UNIVERSITÀ
DEGLI STUDI
DI BRESCIA

Asymptotic growth of codes and related combinatorial problems

by
Stefano Della Fiore

Doctor of Philosophy
Information Engineering

Cycle: XXXV

SSD: ING-INF/03

at the
University of Brescia

Supervisor: Prof. Marco Dalai, University of Brescia, DII department

Preface

All of the work presented henceforth is based on national and international research collaboration, led by Professor Marco Dalai and Simone Costa, Ph.D., at the University of Brescia, by Professor Ugo Vaccaro at the University of Salerno and finally with Professor M. A. Ollis at Emerson College.

Chapter 2 of this thesis is based on the following publications:

- Stefano Della Fiore, Simone Costa and Marco Dalai. Improved Bounds for (b, k)-hashing. IEEE Transactions on Information Theory 68.8 (2022): 4983-4997;
- Stefano Della Fiore, Alessandro Gnutti and Sven Polak. The maximum cardinality of trifferent codes with lengths 5 and 6. Examples and Counterexamples 2 (2022): 100051.

Chapter 3 of this thesis is based on the following publications:

- Stefano Della Fiore, Marco Dalai. A note on $\overline{2}$-separable codes and B_2 codes. Discrete Mathematics 345 (2022): 112751;
- Marco Dalai, Stefano Della Fiore, Adele A. Rescigno and Ugo Vaccaro. Bounds and Algorithms for Frameproof Codes and Related Combinatorial Structures. To appear in IEEE Information Theory Workshop 2023.

Chapter 4 of this thesis is based on the following publication:

- Stefano Della Fiore, Marco Dalai and Ugo Vaccaro. Achievable Rates and Algorithms for Group Testing with Runlength Constraints. IEEE Information Theory Workshop 2022.

Chapter 5 of this thesis is based on the following publication:

- Simone Costa, Marco Dalai and Stefano Della Fiore. Variations on the Erdős distinct-sums problem. Discrete Applied Mathematics 325 (2023): 172-185.

Chapter 6 of this thesis is based on the following publications:

- Simone Costa, Stefano Della Fiore, M. A. Ollis and Sarah Z. Rovner-Frydman. On Sequences in Cyclic Groups with Distinct Partial Sums. The Electronic Journal of Combinatorics (2022): P3-33.
- Simone Costa and Stefano Della Fiore. Weak sequenceability in cyclic groups. Journal of Combinatorial Designs 30.12 (2022): 735-751.

Chapter 7 of this thesis is based on the following paper:

- Simone Costa and Stefano Della Fiore. Bounds on the Higher Degree Erdős-Ginzburg-Ziv Constants over $\mathbb{F}_q^n$. Submitted (arXiv:2211.03682).

I would like to thank all of my co-authors who gave me permission to include the contents of our papers in this thesis.

Proof by analogy is fraud.
–Bjarne Stroustrup–

Abstract

A fundamental problem in Information Theory is studying the asymptotic growth of code sizes. This is often related to problems in extremal combinatorics and to the zero-error transmission capacity of a discrete memoryless noisy channel which is a concept introduced by Shannon [107] in 1956.

In the first part of this thesis, we study the asymptotic rate of (b, k)-hash codes and we provide new upper bounds that improve the best bounds known in the literature for some specific values of b and k. Bounding the size of such codes is a problem of relevant interest in information theory and in computer science since it is related to the zero-error capacity under list decoding of the $b/(k-1)$ channel and with the study of (b, k)-hash families of functions. Moreover, we study some combinatorial structures that are used for traitor tracing in broadcast encryption and collusion resistant fingerprint for copyright protection such as separable codes and frameproof codes. We derive a simple proof, based on information theoretic inequalities, of an upper bound on the largest rates of q-ary $\overline{2}$-separable codes and we show the existence of frameproof codes with small lengths providing a randomized polynomial time algorithm to construct such codes. In addition, we study bounds on the minimum length of superimposed codes introduced in [2], in the context of Non-Adaptive Group Testing algorithms with runlength constraints. We show the existence of superimposed codes using probabilistic methods such as the Lovász Local Lemma and the Expurgation method. Our findings also suggest randomized Las Vegas algorithms for the construction of such codes.

In the second part of this thesis, we focus on various problems with a combinatorial nature. We explore two well-known sum-distinct problems in additive number theory and combinatorial design theory. These problems were first introduced by Erdős in 1955 [101] and Gordon in 1961 [76], and we present new variations on these two classical problems. Additionally, we provide new instances of a conjecture by Alspach and Liversidge [10] about the sequenceability of abelian groups. In particular we focus on cyclic groups of order $n = mt$ when m is prime. A key area of additive group theory and combinatorial number theory is the zero-sum theory, which examines the sum behavior of specific sequences of elements in a finite abelian group. Within this context, we consider a generalization of a problem introduced by Erdős, Gizburg, and Ziv [63] that was recently proposed by Caro and Schmitt [33]. Using both probabilistic methods and the slice rank polynomial method, we present new findings that improve the results obtained in [33].

Contents

CHAPTER 1

Introduction

Extremal Combinatorics deals with problems of determining or estimating the maximum or minimum possible cardinality of a collection of finite objects satisfying certain requirements. Such problems are often related to other areas including Information Theory and Computer Science. A fundamental problem in Information Theory is studying the asymptotic behaviour of code rates. More formally, let n and q be positive integers, a set $\mathcal{C}_n \subseteq \{0, 1, \ldots, q-1\}^n$ is called a q-ary code of length n. Each element of $\mathcal{C}_n$ is called a codeword. An important parameter in coding theory is the *rate* of the code, which is defined as $R_n = \log_q |\mathcal{C}_n|/n$. The asymptotic code rate of $\mathcal{C}_n$ is often investigated for a certain class of codes and it is defined as follows

$$R = \limsup_{n\to\infty} R_n = \limsup_{n\to\infty} \frac{\log_q |\mathcal{C}_n|}{n}\,.$$

In *Chapter 2*, we study (b,k)-hash codes. In particular, we provide new upper bounds on the asymptotic rate of (b,k)-hash codes. Formally, for fixed integers n and $b \geq k$, let $A(b,k,n)$ the largest size of a subset of $\{1,2,\ldots,b\}^n$ such that, for any k distinct elements in the set, there is a coordinate where they all differ. Bounding $A(b,k,n)$ is a problem of relevant interest in information theory and in computer science, relating to the zero-error capacity with list decoding and with the study of (b,k)-hash families of functions. It is known that, for fixed b and k, $A(b,k,n)$ grows exponentially in n. In the first part of Chapter 2, we determine new exponential upper bounds for different values of b and k. A first bound on $A(b,k,n)$ for general b and k was derived by Fredman and Komlós [100] in the '80s and improved for certain $b \neq k$ by Körner and Marton and by Arikan. Only very recently better bounds were derived for general b and k by Guruswami and Riazanov, while stronger results for small values of $b = k$ were obtained by Arikan [15], by Dalai, Guruswami and Radhakrishnan [12], and by Costa and Dalai [42]. In Section 2.2, we strengthen the bounds for some specific values of b and k. Our contribution is a new computational method for obtaining upper bounds on the values of a quadratic form defined over discrete probability distributions in arbitrary dimensions, which emerged as a central ingredient in recent works. The proposed method reduces an infinite-dimensional problem to a finite one, which we manage to further simplify by means of a series of optimality conditions. In the last part of Chapter 2, we prove the non-existence of trifferent codes (3-hash codes) with lengths 5 and 6 and cardinalities 11 and 14 respectively by using an optimized search algorithm.

In *Chapter 3*, we study some combinatorial structures that are used for traitor tracing in broadcast encryption and collusion resistant fingerprints for copyright protection such as separable codes and frameproof codes. In the first part of Chapter 3, we derive, based on information theoretic inequalities, a new upper bound on the largest rates of q-ary $\overline{2}$-separable codes. A q-ary code with codewords of length n is a $\overline{t}$-separable code if for any distinct k codewords and m codewords with $1 \leq k, m \leq t$, there exists a coordinate i, $1 \leq i \leq n$, in which the union of the elements of the k codewords differs from the union of

the elements of the m codewords. In the second part of Chapter 3, we show the existence of q-ary (k,n)-frameproof codes of length $t = O(\frac{k^2}{q}\log n)$ for $q \leq k$, using the Lovász Local Lemma, and of length $t = O(\frac{k}{\log(q/k)}\log(n/k))$ for $q > k$, using the expurgation method. A q-ary (k,n)-frameproof code of length t is a $t \times n$ matrix having entries in $\{0,1,\ldots,q-1\}$ and with the property that for any column $\mathbf{c}$ and any other k columns, there exists a row where the symbols of the k columns are *all* different from the corresponding symbol (in the same row) of the column $\mathbf{c}$. We will discuss how our results improve on known results present in the literature after having proved them. Moreover, for the practically important case of $q \leq k$ (as motivated in [106]) we provide a $O(tn^2)$ randomized algorithm to construct codes of length $t = O(\frac{k^2}{q}\log n)$, that almost matches the lower bound $\Omega(\frac{k^2}{q\log k}\log n)$ on the length of *any* q-ary (k,n)-frameproof code. To the best of our knowledge, this is the first polynomial time algorithm with such a performance.

In *Chapter 4*, we study bounds on the minimum length of (k,n,d)-superimposed codes with runlength constraints introduced in [2]. A (k,n,d)-superimposed code of length t is a $t \times n$ binary matrix such that any two 1's in each column are separated by a run of at least d 0's, and such that for any column $\mathbf{c}$ and any other $k-1$ columns, there exists a row where $\mathbf{c}$ has 1 and all the remaining $k-1$ columns have 0. These codes are used in the context of Non-Adaptive Group Testing algorithms that refer to the scenario in which one has to identify a small subset of defective items that are contained in a much larger set. In general, the goal of Group Testing algorithms is to identify the defective set with as few tests as possible. In the setting of Non-Adaptive Group Testing, the set of items being tested in each test is required to be independent of the outcome of every other test. This restriction is often useful in practice, since this enables parallelization of the testing process. In this chapter, we show the existence of (k,n,d)-superimposed using probabilistic methods such as the Lovász Local Lemma and the Expurgation method. Our findings also suggest randomized Las Vegas algorithms for the construction of such codes.

In *Chapters 5*, *6* and *7*, we consider several problems with a combinatorial flavour. In Chapters 5 and 6 we investigate two known sum-distinct problems in additive number theory and combinatorial design theory. One stated by Erdős [101] in 1955 and the other one by Gordon [76] in 1961, and we propose new variations on these classical problems.

In Chapter 5, we consider the following problem. Let $\{a_1,...,a_n\}$ be a set of positive integers with $a_1 < \cdots < a_n$ such that all 2^n subset sums are distinct. A conjecture by Erdős states that $a_n > c \cdot 2^n$ for some constant c, while the best result known to date is of the form $a_n > c \cdot 2^n/\sqrt{n}$. In this chapter, inspired by an information-theoretic interpretation, we extend the study to vector-valued elements $a_i \in \mathbb{Z}^k$ and we weaken the condition by requiring that only sums corresponding to subsets of size smaller than or equal to λn be distinct. In this case, we derive lower and upper bounds on the smallest possible value of a_n.

In Chapter 6, we investigate the following problem. A subset of an abelian group is *sequenceable* if there is an ordering $(x_1,\ldots,x_k)$ of its elements such that the partial sums $(y_0,y_1,\ldots,y_k)$, given by $y_0 = 0$ and $y_i = \sum_{j=1}^{i} x_i$ for $1 \leq i \leq k$, are distinct, with the possible exception that we may have $y_k = y_0 = 0$. We demonstrate the sequenceability of subsets of size k of $\mathbb{Z}_n \setminus \{0\}$ when $n = mt$ in many cases, including when m is prime for $k \leq 11$ and $t \leq 5$ and for $k = 12$ and $t \leq 4$. We obtain similar, but partial, results for $13 \leq k \leq 15$. This represents progress on a variety of questions and conjectures in the literature concerning the sequenceability of subsets of abelian groups, which we combine and summarize into the conjecture that if a subset of an abelian group does not contain 0 then it is sequenceable. Then, inspired by a graph-theortical interpretation, we propose a

weakening (variation) of this conjecture where we require that the partial sums y_i and y_j are different only whenever i and j are distinct and $|i-j| \leq t$. In this case, we say that a subset A of an abelian group is t-weak sequenceable. The main results presented, in this chapter, about t-weak sequenceability is that any subset A of $\mathbb{Z}_p \setminus \{0\}$ is t-weak sequenceable whenever $t < 7$ or when A does not contain pairs of type $\{x, -x\}$ and $t < 8$.

One significant subfield of additive group theory and combinatorial number theory is the zero-sum theory that studies the sums behavior of suitable sequences of elements in a finite abelian group. Within this context, in Chapter 7 we consider a generalization, recently proposed by Caro and Schmitt [33], of a problem stated by Erdős, Gizburg and Ziv in [63]. The classical Erdős-Ginzburg-Ziv constant of a group G denotes the smallest positive integer ℓ such that any sequence S of length at least ℓ contains a zero-sum subsequence of length $|G|$. In the recent paper, [33], Caro and Schmitt generalized this concept, using the m-th degree symmetric polynomial $e_m(S)$ instead of the sum of the elements of S and considering subsequences of a given length t. In particular, they defined the higher degree Erdős-Ginzburg-Ziv constants $EGZ(t, R, m)$ of a finite commutative ring R and presented several lower and upper bounds to these constants. This chapter aims to provide lower and upper bounds for $EGZ(t, R, m)$ in case $R = \mathbb{F}_q^n$. The lower bounds presented in this chapter have been obtained, respectively, using the Lovász Local Lemma and the Expurgation method and, for sufficiently large n, they beat the lower bound provided by Caro and Schmitt for the same kind of rings. Finally, we will prove an upper bound derived from Tao's Slice Rank method assuming that $q = 3^k$ with $k > 1$, $t = 3$, and $m = 2$.

CHAPTER 2

New bounds on (b, k)-hash codes

In this chapter, all the results presented in Section 2.2 are obtained in collaboration with Marco Dalai and Simone Costa while the results presented in Section 2.3 are obtained in collaboration with Alessandro Gnutti and Sven Polak.

2.1. Introduction

Shannon in his seminal paper of 1956 introduced the concept of zero-error capacity of a discrete finite memoryless noisy channel [107], that is the maximum rate at which information can be transmitted through the channel, using block codes, such that there is zero probability of error. In other words, it is the maximum rate at which messages can be sent through a channel without any errors occurring. In his paper on zero-error theory, Shannon demonstrated that the capacity for zero-error can also be defined using graph theory. Specifically, for each noisy channel, there is a corresponding simple graph that completely defines the channel's zero-error characteristics. The graph-invariant that corresponds to the zero-error capacity of the channel is known as the Shannon capacity of a graph.

A discrete channel is typically characterized by a bipartite graph $H = (X, Y, E)$, where X is the set of channel inputs, Y is the set of channel outputs and E is a subset of pairs $(x, y) \in X \times Y$ that represents the channel links, i.e., if $(x, y) \in E$ then the output y can be received when x has been transmitted over the channel. Starting from this representation of a channel, one can associate to the channel H a confusability graph G_H. In this graph the vertex set is X (the channel inputs) and two vertices $x' \neq x''$ are adjacent if there is a common output $y \in Y$ such that $(x', y), (x'', y) \in E$, so that x' and x'' can be confused with each other. Therefore, the maximum independent set $\alpha(G_H)$ is the maximum number of single letter messages that can be sent without errors. In other words, the receiver knows whether the received message is correct or not. Furthermore, the definition is extended to words of length n by G_H^n, where G_H^n is the n-fold strong product of G_H in which two n-tuples in X^n are adjacent if and only if in every coordinate, they are either equal or adjacent in G_H. Therefore, the graph-theoretic definition of the Shannon capacity is the limit, for $n \to \infty$, of the ratio $\log_2 \alpha(G^n)/n$. The Shannon capacity is in general very difficult to calculate. In fact, the Shannon capacity of the cycle graph C_5 was not determined as $\log_2(\sqrt{5})$ until 1979 by Lovász [92], and the Shannon capacity of C_7 is perhaps one of the most notorious open problems in extremal combinatorics.

In this chapter and in particular in Section 2.2, we study the zero-error capacity under *list decoding* for simple channels where the classical Shannon capacity is trivially zero. The zero-error capacity under list decoding is a concept introduced by Elias in 1988 [60]. For a fixed integer L, the zero-error capacity with list of size L of a channel H is defined as the largest asymptotic rate at which one can communicate over the channel with n independent

This chapter includes research results published in [67], [68], [54].

uses of the channel for $n \to \infty$, so that the receiver can identify the correct message among a list of at most L entries. In other words, the receiver can output L codewords which must include the transmitted one. More formally, given a discrete channel $H = (X, Y, E)$, a subset (code) $C \subseteq X^n$ is said to be a zero-error code with list of size L for channel H if for every subset of $L+1$ codewords in C there exists a coordinate in which the $L+1$ symbols in that coordinate are not adjacent to a common vertex in H. As done for the Shannon capacity, we want to give a definition in graph-theoretical terms of the zero-error capacity under list decoding. First we need to recall the definition of a hypergraph.

DEFINITION 2.1.1. *A hypergraph $\mathcal{H}$ is a family E of subsets of a finite set V where the subsets in E are called hyperedges and the elements of V are called vertices. If all the edges have size d then we say that $\mathcal{H}$ is a d-uniform hypergraph.*

Hence, in graph-theoretical terms, the definition of a zero-error code C with list of size L for a discrete channel $H = (X, Y, E)$ is equivalent to say that C is an independent set in the $(L+1)$-uniform hypergraph defined on the vertex set X^n where the hyperedges correspond to tuples whose i-th symbols are adjacent to a common vertex in H for every i. This definition collapse to the classical zero-error capacity when the list size $L = 1$.

Here we state the following theorem proved by Elias in [60] that provides upper and lower bounds on the zero-error capacity with list of size L of a generic discrete channel.

THEOREM 2.1.1 (Elias [60]). *Let $H = (X, Y, E)$ be a discrete memoryless channel. Let $S_y = \{x \in X : (x, y) \in E\}$, the set of input letters which produce output y. Let Δ be the set of probability vectors p defined on X, and let*

$$P_0 = \min_{p \in \Delta} \max_{y \in Y} \sum_{x \in S_y} p(x)\,. \tag{1}$$

Denote with $C_0(L)$ the zero-error capacity with list of size L for the channel H. Hence

$$-\frac{L+1}{L}\log_2(P_0) - \frac{1}{L}\log_2|Y| \leq C_0(L) \leq -\log_2(P_0)\,. \tag{2}$$

PROOF. The upper bound in equation (2) is obtained using the fact that $C_0(L) \leq C_{0F} = -\log_2(P_0)$, where C_{0F} is the zero-error capacity of the channel H when there is immediate noiseless feedback of each received letter to the transmitter (see [60] for more details). The lower bound in (2) is obtained using a random coding method known as the *Expurgation method*. Let p be a probability vector which attains the minimax value in equation (1). Now, let C be a code of length n and with cardinality M, where each symbol is picked i.i.d. at random with distribution p. For a given subset B of distinct codewords, $|B| = L+1$, let $E_{i,B}$ be the event such that the symbols in the i-th coordinate of the $L+1$ codewords in B all lie in one S_y for some y. Therefore

$$\Pr(E_{i,B}) = \sum_{y \in Y} \left(\sum_{x \in S_y} p(x) \right)^{L+1} \leq |Y| P_0^{L+1}\,,$$

since P_0 is the most probable between the S_y's. Denote with E_B the event such that the $L+1$ codewords in B are not distinguishable at the receiver by using a decoder with list of size L. i.e., $E_B = \cap_{i=1}^{n} E_{i,B}$. Since each symbol in C is picked i.i.d., the probability of each event E_B is upper bounded as follows

$$\Pr(E_B) = \prod_{i=1}^{n} \Pr(E_{i,B}) \leq \left(|Y| P_0^{L+1} \right)^n\,.$$

The number of such events is clearly equal to $\binom{M}{L+1}$. Now, let I_B be the indicator random variable of the event E_B and define the random variable $I = \sum_B I_B$ that represents the number of events E_B that are satisfied. We obtain

$$\mathbb{E}[I] \leq \binom{M}{L+1} \left(|Y|P_0^{L+1}\right)^n .$$

We note that if $\mathbb{E}[I] < M/2$ then there exist at most $M/2$ "*bad*" events E_B that are satisfied. Then, for each of these events E_B we remove one codeword in B. Hence, we are left with a zero-error code C with list of size L for the channel H of cardinality at least $M/2$. The theorem follows since a code of cardinality M and one of cardinality $M/2$ have the same asymptotic rate. □

The lower bound given in equation (2) can alternatively be obtained using the Lovász Local Lemma for the symmetric case. Here we state this lemma that will be used throughout the thesis to provide existential result of certain combinatorial structures.

LEMMA 2.1.1. *[8] Let $E_1, E_2, \ldots, E_m$ be events in an arbitrary probability space. Suppose that each event E_i is mutually independent of a set of all other events E_j but at most D, and that $\Pr(E_i) \leq P$ for all $1 \leq i \leq m$. If*

$$eDP \leq 1$$

then $\Pr(\cap_{i=1}^m \overline{E}_i) > 0$.

Following all the procedure used in the proof of Theorem 2.1.1 and considering the same set of events E_B, we note that the variable P in Lemma 2.1.1 in our case is equal to $\left(|Y|P_0^{L+1}\right)^n$. It can be easily seen that an arbitrary event E_B is mutually independent from all the events E_A, where $A \cap B = \emptyset$. Hence, the quantity D in Lemma 2.1.1 can be upper bounded by $(L+1)\binom{M}{L}$. Therefore we have the following condition that implies the existence of a zero-error code with list of size L, cardinality M and length n for a given channel.

$$eDP = e(L+1)\binom{M}{L} \left(|Y|P_0^{L+1}\right)^n \leq 1 . \tag{3}$$

Rewritten (3) in terms of asymptotic rate, we obtain the exact same lower bound on $C_0(L)$ given in Theorem 2.1.1.

REMARK 2.1.1. *The Expurgation method and the Lovász Local Lemma provide the same asymptotic result (for $n \to \infty$), but for finite code lengths it can be seen that the bound obtained in Theorem 2.1.1 outperforms the one that can be derived from equation* (3) *for all finite n's. We refer the reader to Chapter 7 for a more detailed comparison between these two techniques.*

The smallest non-trivial case for zero error capacity under list decoding is the $3/2$ channel, where $X = Y = \{1, 2, 3\}$ and $(x, y) \in E$ if and only if $x \neq y$. Clearly, since every pair of channel inputs can be confused with each other, the zero-error capacity of this channel is zero. A code that achieve zero-error with list of size 2 for this channel is known as perfect 3-hash code or trifferent code and non-trivial upper and lower bounds on the asymptotic rate of such codes can be obtained thanks to Theorem 2.1.1. By equation (2) we have that $C_0(2)$ for the $3/2$ channel is lower bounded by $\log_2(3) - 3/2$ and upper bounded by $\log_2(3/2)$ since P_0, defined in equation (1), is equal to $2/3$ for this channel. The upper bound $\log_2(3/2)$ is still the best known bound while the best lower bound is $1/4 \log_2(9/5)$ given in [88].

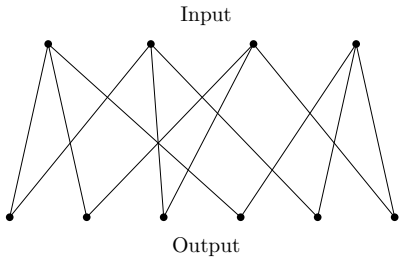


FIGURE 1. A 4/2 channel. Edges represent positive probabilities. Here, zero-error communication is possible when decoding with list-size equal to 2.

In Section 2.2, we study the zero-error capacity under list of size $k-1$ of the $b/(k-1)$ channel, meaning that any $k-1$ of the b inputs share one output but no k distinct inputs do (see Figure 1 for an example). A code C that achieve zero-error capacity under list of size $k-1$ for this channel is called (b,k)-hash code and the required property for C is what is needed for the receiver to always be able to produce a list of $k-1$ codewords of C which must necessarily include the one that was sent; that is, zero-error communication with $(k-1)$-list decoding is possible. Indeed, the condition implies that any k codewords use, in at least one coordinate, k different symbols, and one of them will not be compatible with the received symbol in that coordinate. We refer the reader to [59], [100], [87], [98] for an overview of the more general context of this problem. Some recent important results in a different asymptotic setting can be found in [20]. The problem considered in Section 2.2 has a twofold history that connects it naturally with combinatorial aspects of computer science and information theory. Let b, k, and n be integers and let C be a subset of $\{1,2,\ldots,b\}^n$. The zero-error property required that for any k distinct elements of C we can find a coordinate where they all differ. Such a set can be interpreted, by looking at it coordinate-wise, as a family of n hashing functions on some universe of size $|C|$. The required property then says that the family is a perfect hash family, that is, any k elements in the universe are k-partitioned by at least one function.

We will call any subset C of $\{1,2,\ldots,b\}^n$ with the described property a (b,k)-hash code, for simplicity when $b=k$ we refer to such codes as k-hash codes. For the reasons mentioned above, bounding the size of (b,k)-hash codes is a combinatorial problem that has been of interest in both computer science and information theory.

Finally, in *Section 2.3*, we derive new upper bounds on the cardinality of trifferent codes (3-hash codes). Defining $\mathcal{T}(n)$ as the maximum cardinality of trifferent codes with length n, then it is known that $\mathcal{T}(1)=3$, $\mathcal{T}(2)=4$, $\mathcal{T}(3)=6$ and $\mathcal{T}(4)=9$. $\mathcal{T}(n)$ is unknown for $n \geq 5$. In Section 2.3, we use an optimized search algorithm to show that $\mathcal{T}(5)=10$ and $\mathcal{T}(6)=13$. We prove the the non-existence of trifferent codes with lengths 5 and 6 and cardinalities 11 and 14 respectively by computer, using an optimized search algorithm.

2.2. Improved upper bounds on (b,k)-hash codes

2.2.1. Preliminaries. Denote with $A(b,k,n)$ the largest size of (b,k)-hash codes. It is known that for fixed b and k, $A(b,k,n)$ grows exponentially in n, and a challenging problem consists in bounding the exponent. We will thus study the quantity

$$R_{(b,k)} = \limsup_{n\to\infty} \frac{1}{n} \log A(b,k,n)\,.$$

Note that, throughout the section, all logarithms are to base 2.

Few lower bounds on $R_{(b,k)}$ are known. First results in this sense were given by [100], [59] and a better bound was derived by [88] for $b = k = 3$. More recently, new lower bounds were derived in [119] for infinitely many other values of k. The first, landmark result concerning the upper bounds was obtained by Fredman-Komlós [100], who showed that

$$R_{(b,k)} \leq \frac{b^{\underline{k-1}}}{b^{k-1}} \log(b-k+2)\,, \tag{4}$$

where $b^{\underline{k-1}} = b(b-1)\cdots(b-k+2)$. Progress has since been rare. A generalization of the bound given in equation (4) was derived by Körner and Marton [88] in the form

$$R_{(b,k)} \leq \min_{2\leq j\leq k-2} \frac{b^{\underline{j+1}}}{b^{j+1}} \log \frac{b-j}{k-j-1}\,. \tag{5}$$

Nilli [98] provided an elementary proof of (5) without considerations of graph entropy or hypergraph entropy. This bound was further improved for different values of b and k by Arikan [15]. In the case $b = k$, an improvement was first obtained for $k = 4$ in [16] and then in [12], [50]. The latter only focuses on $b = k = 4$, but the procedure can be extended to general b and k. As shown in the next subsections, it leads to the following bound.

LEMMA 2.2.1. *For general b and k, we have*

$$R_{(b,k)} \leq \left(\frac{1}{\log b} + \frac{b^2}{(b^2-3b+2)\log \frac{b-2}{k-3}} \right)^{-1}. \tag{6}$$

In [80], the authors prove that the Fredman-Komlós bound is not tight for any $b \geq k > 3$; explicit better values were given there for $b = k = 5, 6$, and for larger $b = k$ modulo a conjecture which is proved in [42], where further improvements are also obtained for $b = k = 5, 6$. The case of $b \neq k$ is not described in detail in [80] but, as the authors mention, it is straightforward. We do not write here the bound since it has a complicated expression.

In this subsection, we attack some of the cases which appear not to be optimally handled by those methods. In particular, we build on the results obtained in [42] and add an improvement that leads to better bounds for many pairs of (b, k) values. The results of [42] for $b = k$ were derived following an approach common to many recent works by introducing a symmetrization which reduces to the problem of bounding a quadratic form on probability distributions. We give a more general exposition for the general b, k case, anticipating here the key lemma whose proof we give for completeness in the next subsection. Fix an integer j in the range $2, \ldots, k-2$ and define, for probability vectors $p, q \in \mathbb{R}^b$, the function

$$\Psi_j(p;q) = \frac{1}{(b-j-1)!} \sum_{\sigma} p_{\sigma(1)} p_{\sigma(2)} \cdots p_{\sigma(j)} q_{\sigma(j+1)} + q_{\sigma(1)} q_{\sigma(2)} \cdots q_{\sigma(j)} p_{\sigma(j+1)}, \tag{7}$$

where σ ranges over all permutations of $\{1, 2, \ldots, b\}$. Define then

$$\mathbf{M}_j = \sup_{\lambda} \sum_{p,q} \lambda_p \lambda_q \Psi_j(p;q) \tag{8}$$

where λ ranges over all probability distributions on finite sets of probability vectors in $\mathbb{R}^b$, so that λ_p is the probability associated to the probability vector p. Then, the following bound holds.

LEMMA 2.2.2. *For $j = 2, \ldots, k-2$,*

$$R_{(b,k)} \leq \left(\frac{2}{\mathbf{M}_j \log \frac{b-j}{k-j-1}} + \frac{1}{\log\left(\frac{b}{j-1}\right)} \right)^{-1} . \tag{9}$$

The results in [42] were obtained using in (9), for $b = k$ and $j = k-2$, the upper bound

$$\mathbf{M}_j \leq \max_{p,q} \Psi_j(p; q) . \tag{10}$$

A weakness in this bound comes from the fact that distributions p and q that maximize $\Psi_j(p; q)$ exhibit in many cases some opposing asymmetries, in the sense that they give higher probabilities to different symbols. When used as a replacement for *each* of the pairs of p and q in (8), we have a rather conservative bound, because pairs (p, q) which give high values for $\Psi_j(p; q)$ will give low values for $\Psi_j(p; p)$ and $\Psi_j(q; q)$, and equation (8) contains a weighted contribution from all pairings of p and q. In this subsection, we present a computational method for obtaining more refined bounds on $\mathbf{M}_j$ for general b, k values which lead to improvements on the best-known bounds on $R_{(b,k)}$ for many b, k pairs.

TABLE 1. Upper bounds on $R_{(b,k)}$. All numbers are rounded upwards.

(b,k)	Our method	[15]	[80]	[88]	(b,k)	Our method	[15]	[80]	[88]
$(5,5)$	**0.16894**[1]	0.23560	0.19079	0.19200	$(6,5)$	**0.34512**[1]	0.44149	0.43207	0.44027
$(6,6)$	**0.08475**[1]	0.15484	0.09228	0.09260	$(7,6)$	**0.19897**[2]	0.30554	0.23524	0.23765
$(8,6)$	**0.31799**[2]	0.44888	0.40330	0.41016	$(9,6)$	**0.43237**[2]	0.58303	0.58486	0.59455
$(10,6)$	**0.53909**[2]	0.73304	0.76977	0.78170	$(11,6)$	**0.63766**[2]	0.87038	0.95285	0.96640
$(12,6)$	**0.72848**[2]	0.99588	1.13118	1.14584	$(13,6)$	**0.81227**[2]	1.11084	1.30322	1.31855
$(14,6)$	**0.88978**[2]	1.21657	1.46822	1.48388	$(7,7)$	**0.04090**[1]	0.09747	0.04279	0.04284
$(8,7)$	**0.10865**[2]	0.20340	0.12134	0.12189	$(9,7)$	**0.19054**[2]	0.31204	0.22547	0.22761
$(10,7)$	**0.27741**[2]	0.41982	0.34615	0.35108	$(11,7)$	**0.36424**[2]	0.52472	0.47856	0.48538
$(12,7)$	**0.44850**[2]	0.65160	0.61698	0.62549	$(13,7)$	**0.52902**[2]	0.77148	0.75796	0.76792
$(14,7)$	**0.60538**[2]	0.88384	0.89915	0.91027	$(8,8)$	**0.01889**[1]	0.05769	0.01922	0.01923
$(9,8)$	**0.05616**[1]	0.12874	0.06001	0.06013	$(10,8)$	**0.10791**[2]	0.20754	0.12048	0.12096
$(11,8)$	**0.16878**[2]	0.29023	0.19680	0.19818	$(12,8)$	**0.23451**[2]	0.37434	0.28470	0.28797
$(13,8)$	**0.30214**[2]	0.45827	0.38245	0.38694	$(14,8)$	**0.36974**[2]	0.56612	0.48658	0.49227
$(10,9)$	**0.02773**[1]	0.07668	0.02874	0.02876	$(11,9)$	**0.05796**[2]	0.13098	0.06197	0.06208
$(12,9)$	**0.09730**[2]	0.19157	0.10746	0.10778	$(13,9)$	**0.14332**[2]	0.25611	0.16368	0.16444
$(14,9)$	**0.19382**[2]	0.32294	0.22865	0.23033	$(11,10)$	**0.01321**[1]	0.04289	0.01342	0.01343
$(12,10)$	**0.02978**[1]	0.07806	0.03093	0.03095	$(13,10)$	**0.05342**[2]	0.12009	0.05674	0.05681
$(14,10)$	**0.08332**[2]	0.16726	0.09071	0.09090	$(13,11)$	**0.01476**[1]	0.04400	0.01506	0.01506
$(14,11)$	**0.02815**[2]	0.07141	0.02915	0.02916	$(14,12)$	**0.00712**[1]	0.02361	0.00718	0.00718
$(15,13)$	**0.00335**[1]	0.01218	0.00336	0.00336					

[1]Bounds obtained with the procedure of Subsection 2.2.3, improving the generalization of [42].
[2]Bounds where the procedure of Subsection 2.2.3 reduces to the solution obtained by generalization of [42].

In Table 1 we give a comparison between bounds (6) and (5), the bounds of [15] and [80] and our new bounds for different values of b and k. In Table 2 we show that for some (b, k)-cases the bound (6) is the best bound among all the current known bounds, in particular when b is much larger than k. Finally, in Table 3 we provide some (b, k)-cases where the

bound of [80] is the current best known bound, in particular when b and k are large and nearly equal. Clearly, the cases reported in Tables 2 and 3 are not exhaustive, but they have been properly selected to point out that our method does not always provide the best bounds. The integers in the parentheses for bounds [80], [15] and [88] in Table 2 represent the optimal value of a parameter which has the same role as j in (5). When its value is not reported, as well as in Tables 1 and 3, it is equal to $k-2$ for our bounds and for bounds of [80], [15] and [88]. Instead, for bound (6) it is always equal to 2.

TABLE 2. Upper bounds on $R_{(b,k)}$. All numbers are rounded upwards.

(b,k)	[12]*	[42]*	[15]	[80]	[88]
$(5,4)$	**0.57303**	0.66126	0.61142	0.74834	0.73697(0)
$(6,4)$	**0.77709**	0.87963	0.83904	1.09604	1.00000(0)
$(7,4)$	**0.94372**	1.03711	1.02931	1.40593	1.22239(0)
$(100,6)$	**2.81342**	—	3.61848(2)	4.87959(2)	4.32193(0)
$(100,7)$	**2.67473**	—	3.41158(2)	4.47696(2)	4.05889(0)

Missing values indicate impossibility to compute the bound due to high computational complexity.
*The generalized bound for the (b,k) case.

TABLE 3. Upper bounds on $R_{(b,k)}$. All numbers are rounded upwards.

(b,k)	[80]	[42]*	[15]	[88]
$(9,9)$	$\mathbf{8.4288 \cdot 10^{-3}}$	0.00946	0.03182	$8.4300 \cdot 10^{-3}$
$(10,10)$	$\mathbf{3.6287 \cdot 10^{-3}}$	0.00419	0.01642	$3.6288 \cdot 10^{-3}$
$(11,11)$	$\mathbf{1.53895 \cdot 10^{-3}}$	0.00181	0.00803	$1.53897 \cdot 10^{-3}$
$(12,11)$	$\mathbf{6.13036 \cdot 10^{-3}}$	0.00664	0.02266	$6.13075 \cdot 10^{-3}$
$(12,12)$	$\mathbf{6.44678 \cdot 10^{-4}}$	0.00077	0.00377	$6.44679 \cdot 10^{-4}$
$(13,12)$	$\mathbf{2.75350 \cdot 10^{-3}}$	0.00305	0.01143	$2.75355 \cdot 10^{-3}$
$(13,13)$	$\mathbf{2.672760 \cdot 10^{-4}}$	0.00033	0.00172	$2.672761 \cdot 10^{-4}$
$(14,13)$	$\mathbf{1.218595 \cdot 10^{-3}}$	0.00138	0.00556	$1.218599 \cdot 10^{-3}$

*The generalized bound for the (b,k) case.

The section is structured as follows. In Subsection 2.2.2 we give some background proving Lemmas 2.2.1 and 2.2.2. In Subsection 2.2.3 we present the first part of our computational method to bound $\mathbf{M}_j$ by partitioning the domain of possible p and q distributions and then working on the subdomains. The second part is presented in Subsection 2.2.4, where we derive optimality conditions on p and q over such subdomains, which allow us to reduce the problem to a manageable one that can be solved exactly. Finally, in Subsection 2.2.5 we show that at least some of the bounds that we obtain are not tight, although a quantitative improvement is not explicitly derived.

2.2.2. Background. The best upper bounds on $R_{(b,k)}$ available in the literature can all be seen as different applications of a central idea, which is the study of (b,k)-hashing by comparison with a combination of binary partitions. This mainline of approach to the problem comes from the original work of Fredman and Komlós [100]. A clear and productive formulation of the idea was given by Radhakrishnan in terms of Hansel's lemma [103], which remained the main tool used in all recent results [50], [80] and [42].

We state the Hansel's Lemma for Hypergraphs here for the reader's convenience (see Definition 2.1.1 for the hypergraph's definition).

LEMMA 2.2.3 (Hansel for Hypergraphs [82], [98]). *Let K_r^d be the complete d-uniform hypergraph on r vertices and let $G_1, \ldots, G_m$ be c-partite d-uniform hypergraphs on those vertices such that $\cup_i G_i = K_r^d$. Let $\tau(G_i)$ be the number of non-isolated vertices in G_i. Then*

$$\log \frac{c}{d-1} \sum_{i=1}^{m} \tau(G_i) \geq \log \frac{r}{d-1} \,. \tag{11}$$

Using this main ingredient, we provide here a proof of Lemma 2.2.2, which extends the bound used in [42] to general b and k. We refer the reader to [42] for a more detailed discussion on connections with other previous bounds in the literature.

PROOF OF LEMMA 2.2.2. Given a (b, k)-hash code C of rate R, fix any j elements $x_1, x_2, \ldots, x_j$ in C, with j in the range $2, \ldots, k-2$. For any coordinate i let $G_i^{x_1,\ldots,x_j}$ be the $(b-j)$-partite $(k-j)$-uniform hypergraph with vertex set $C \setminus \{x_1, x_2, \ldots, x_j\}$ and edge set

$$E = \big\{ \{y_1, \ldots, y_{k-j}\} : x_{1,i}, \ldots, x_{j,i}, y_{1,i}, \ldots, y_{k-j,i} \text{ are all distinct} \big\} \,. \tag{12}$$

Since C is a (b, k)-hash code, then $\bigcup_i G_i^{x_1,\ldots,x_j}$ is the complete $(k-j)$-uniform hypergraph on $C \setminus \{x_1, x_2, \ldots, x_j\}$ and so

$$\log \frac{b-j}{k-j-1} \sum_{i=1}^{n} \tau(G_i^{x_1,\ldots,x_j}) \geq \log \frac{|C|-j}{k-j-1} \,. \tag{13}$$

Inequality (13) holds for any choice of $x_1, x_2, \ldots, x_j$, so the main goal is proving that the left hand side is not too large for all possible choices of $x_1, x_2, \ldots, x_j$. The choice can be deterministic or we can take the expectation over any random selection.

First note that if the $x_{1,i}, x_{2,i}, \ldots, x_{j,i}$ are not all distinct (let us say that they "collide") then the hypergraph defined by (12) is empty, that is the corresponding τ in the left hand side of (13) is zero. Otherwise, $\tau(G_i^{x_1,\ldots,x_j})$ depends on the frequency of different symbols in the i-th coordinate of the code. Let f_i be their distribution, meaning that $f_{i,a}$ is the fraction of elements of C whose i-th coordinate is a. Then, we have

$$\tau(G_i^{x_1,\ldots,x_j}) \;=\; \begin{cases} 0 & x_1, \ldots, x_j \text{ collide in coordinate } i \\ \left(\frac{|C|}{|C|-j}\right) \left(1 - \sum_{h=1}^{j} f_{i,x_{h,i}}\right) & \text{otherwise} \end{cases} \,. \tag{14}$$

We partition the code C into subcodes C_ω, $\omega \in \Omega$ in such a way that each subcode has a size which grows unbounded with n and uses in any of its first ℓ coordinates only $j-1$ symbols, where ℓ denotes the length of the prefix. It can be shown, by an easy extension of the method used for the case $b = k$ and $j = k-2$ in [42], that if the original code has rate R, then for any $\epsilon > 0$ one can do this with a choice of $\ell = n(R-\epsilon)/\log\left(\frac{b}{j-1}\right)$ for n large enough. Given such a partition of our code, if we select codewords $x_1, \ldots, x_j$ within the same subcode C_ω, they will collide in the first ℓ coordinates and the corresponding contribution to the left-hand side of (13) will be zero. The next step is to add randomization. Pick randomly one of the subcodes C_ω and randomly select the codewords $x_1, \ldots, x_j$ within C_ω. Then an upper bound on $|C|$ is obtained by taking an expectation on the left-hand side of

(13)

$$\log \frac{|C| - j}{k - j - 1} \leq \log \frac{b - j}{k - j - 1} \mathbb{E}_\omega \left(\mathbb{E} \left[\sum_{i \in [\ell+1, n]} \tau(G_i^{x_1, x_2, \ldots, x_j}) | \omega \right] \right)$$

(15)

$$= \log \frac{b - j}{k - j - 1} \sum_{i \in [\ell+1, n]} \mathbb{E}_\omega (\mathbb{E}[\tau(G_i^{x_1, x_2, \ldots, x_j}) | \omega]).$$

Here, each subcode C_ω is taken with probability $\lambda_\omega = |C_\omega|/|C|$, and $x_1, \ldots, x_j$ are taken uniformly at random (without repetitions) from C_ω.

Let now $f_{i|\omega}$ be the distribution of the i-th coordinate of the subcode C_ω (with components, say, $f_{i,a|\omega}$) . Then, for $i > \ell$, we can write

(16)

$$\mathbb{E}[\tau(G_i^{x_1, \ldots, x_j}) | \omega] = (1 + o(1)) \sum_{\substack{\text{distinct} \\ a_1, \ldots, a_j}} f_{i,a_1|\omega} f_{i,a_2|\omega} \cdots f_{i,a_j|\omega} (1 - f_{i,a_1} - \ldots - f_{i,a_j})$$

where the $o(1)$ is meant as $n \to \infty$ and is due, under the assumption that C_ω grows unbounded with n, to sampling without replacement within C_ω. Now, since $\lambda_\omega = |C_\omega|/|C|$, f_i is actually the expectation of $f_{i|\omega}$ over ω, that is, using a different dummy variable μ to index the subcodes for convenience,

$$f_i = \sum_\mu \lambda_\mu f_{i|\mu} \,.$$

Using this in (16), one notices that when taking a further expectation over ω it is possible to operate a symmetrization in ω and μ. The expectation of (16) over ω can then be written as

(17)

$$\mathbb{E}_\omega[\tau(G_i^{x_1, x_2, \ldots, x_j})] = (1 + o(1)) \frac{1}{2} \sum_{\omega, \mu \in \Omega} \lambda_\omega \lambda_\mu \Psi_j(f_{i|\omega}, f_{i|\mu}) \,,$$

so that

(18)

$$\mathbb{E}_\omega[\tau(G_i^{x_1, x_2, \ldots, x_j})] \leq (1 + o(1)) \frac{1}{2} \mathbf{M}_j \,.$$

This leads to

(19)

$$\log |C| \leq (1 + o(1)) \frac{1}{2} (n - \ell) \mathbf{M}_j \log \frac{b - j}{k - j - 1} \,,$$

from which, using the value of ℓ described above, one deduces

$$R \leq (1 + o(1)) \frac{1}{2} \left[1 - \frac{R}{\log \left(\frac{b}{j-1} \right)} \right] \mathbf{M}_j \log \frac{b - j}{k - j - 1}.$$

Explicitating in R we conclude the proof of the Lemma. □

The first part of the above derivation follows the same method used in [12]. In particular, the proof of Lemma 2.2.1 can be obtained using $j = 2$ and looking at (16) as a quadratic form in $f_{i|\omega}$ with kernel of elements $(1 - f_{i,a_1} - f_{i,a_2})$. The procedure used in [12] can then be applied also for $b \geq k$ with some simple variations.

PROOF OF LEMMA 2.2.1. Set $j = 2$ in (16). Proceeding as in [12], it can be shown that the right hand side, as a quadratic form in $f_{i|\omega}$, is a concave function on the simplex of probability distributions if all the values $f_{i,a}$ are not larger than $1/2$. Assume first that this holds for all $i \in [\ell + 1, n]$. The expectation over ω is then bounded by the value obtained by replacing both $f_{i|\omega}$ and f_i with a uniform distribution, which is easily evaluated to be $(b^2 - 3b + 2)/b^2$. When used in (15) this gives the bound of Lemma 2.2.1. It remains to show that we can assume without loss of generality that $f_{i,a} \leq 1/2$ for all i and a. Again the procedure is a generalization of what was done in [12]. Suppose that there exists a coordinate $i \in \{1, 2, \ldots, n\}$ for which (rename the symbols if needed) $f_{i,1} \geq f_{i,2} \geq \ldots \geq f_{i,b}$ with $f_{i,1} > 1/2$. Note that we must then have $f_{i,1} + f_{i,2} + \ldots + f_{i,k-1} \geq (b+k-3)/(2b-2)$. We can build another (b, k)-hash code C' by removing all the codewords in C for which the symbol in the i-th coordinate is in $\{k, k+1, \ldots, b\}$ and by deleting this coordinate in the remaining codewords. Clearly C' has length $n - 1$ and cardinality $|C'| \geq |C| \cdot (b + k - 3)/(2b - 2)$. This process can be iterated, say t times, in order to get a code $\tilde{C}$ of length $n - t$ in which $f_{i,a} \leq 1/2$ for all $i \in \{1, 2, \ldots, n - t\}$ and for all $a \in \{1, 2, \ldots, b\}$ and such that

$$|\tilde{C}| \geq |C| \left(\frac{b + k - 3}{2b - 2} \right)^t . \tag{20}$$

Let $B(b, k)$ be the right hand side of (6). We can apply the previous part of the proof to $\tilde{C}$ and bound the rate R of C as

$$\begin{aligned} \frac{1}{n} \log |C| &\leq \frac{1}{n} \log |\tilde{C}| + \frac{t}{n} \log \left(\frac{2b - 2}{b + k - 3} \right) \\ &\leq \frac{n - t}{n} B(b, k) + \frac{t}{n} \log \left(\frac{2b - 2}{b + k - 3} \right) + o(1) \\ &\leq B(b, k) - \frac{t}{n} \left[B(b, k) - \log \left(\frac{2b - 2}{b + k - 3} \right) \right] + o(1) . \end{aligned}$$

The proof of the Lemma is concluded if we prove that $B(b, k) > \log \frac{2b-2}{b+k-3}$ for $b \geq k \geq 4$. We verify this inequality considering the following three different ranges of b and k:

(1) Suppose that $12 \leq k \leq b \leq (k - 3)^2$. Then

$$\begin{aligned} B(b, k) &\overset{(i)}{>} \frac{2}{3} \cdot \frac{(b^2 - 3b + 2) \log b \log \left(\frac{b-2}{k-3} \right)}{b^2 \log(b)} > \frac{2}{3} (1 - 3/b) \log \left(\frac{b - 2}{k - 3} \right) \\ &\overset{(ii)}{\geq} \frac{1}{2} \log \left(\frac{b - 2}{k - 3} \right) , \end{aligned}$$

where (i) is true since $\log \left(\frac{b-2}{k-3} \right) \leq 1/2 \log b$ for $b \leq (k-3)^2$, while (ii) since $b \geq 12$. Then, it can be verified that for $b \geq k \geq 12$ we have that

$$\frac{1}{2} \log \left(\frac{b - 2}{k - 3} \right) > \log \left(\frac{2b - 2}{b + k - 3} \right) .$$

(2) Suppose that $b \geq 8k - 22$ and $k \geq 4$. Then

$$B(b,k) > \frac{(b^2-3b+2)\log b \log\left(\frac{b-2}{k-3}\right)}{2b^2\log(b)} > \frac{1}{2}(1-3/b)\log\left(\frac{b-2}{k-3}\right)$$
$$\overset{(i)}{>} \frac{1}{3}\log\left(\frac{b-2}{k-3}\right),$$

where (i) is true since $b > 9$. Then, it can be easily verified that for $b \geq 8k-22$ we have that

$$\frac{1}{3}\log\left(\frac{b-2}{k-3}\right) \geq 1 > \log\left(\frac{2b-2}{b+k-3}\right).$$

(3) All the cases $b \geq k = 4, 5, \ldots, 11$ can be verified manually or by using a symbolic computation software.

Finally, we see that the ranges of b, as functions of k, in the first two cases intersect because

$$(k-3)^2 \geq 8k-22$$

is verified for every $k \geq 12$. Therefore the thesis of the lemma follows. □

2.2.3. Bounding the quadratic form. We now enter the problem of determining better upper bounds on the value of $\mathbf{M}_j$ defined in (8). We consider partitions of $\mathcal{P}_b$, the set of probability distributions on b elements, into disjoint subsets to find upper bounds on the quadratic form (8) in terms of simpler ones. If we have a partition $\{\mathcal{P}_b^0, \mathcal{P}_b^1, \ldots, \mathcal{P}_b^r\}$ of $\mathcal{P}_b$ and we define

$$m_{i,h} = \sup_{p\in\mathcal{P}_b^i, q\in\mathcal{P}_b^h} \Psi_j(p,q), \qquad \eta_i = \sum_{p\in\mathcal{P}_b^i} \lambda_p,$$

then clearly

$$\sum_{p,q} \lambda_p\lambda_q\Psi_j(p,q) \leq \sum_{i,h}\sum_{p\in\mathcal{P}_b^i}\sum_{q\in\mathcal{P}_b^h} \lambda_p\lambda_q m_{i,h} \leq \sum_{i,h} \eta_i\eta_h m_{i,h}. \tag{21}$$

This is a convenient simplification since we have now an r-dimensional problem which we might be able to deal with in some computationally feasible way. We will use this procedure with two different partitions in terms of how balanced or unbalanced the distributions are. We take $b+1$ subsets with some symmetry which allows us to further reduce the complexity.

Partition based on maximum value. We first consider a partition of $\mathcal{P}_b$ in terms of the largest probability value which appears in a distribution. We use a parameter $\epsilon \leq 1/(j+1)$; all quantities will depend on ϵ but we do not write this to avoid cluttering the notation. We define b sets of unbalanced distributions

$$\breve{\mathcal{P}}_b^i = \{p \in \mathcal{P}_b : p_i > 1-\epsilon\}$$

for every $1 \leq i \leq b$, and correspondingly a set of balanced distributions

$$\breve{\mathcal{P}}_b^0 = \{p \in \mathcal{P}_b : p_i \leq 1-\epsilon \ \forall i\}.$$

Note that these are all disjoint sets since $\epsilon < 1/2$ when $j \geq 2$. Following the scheme mentioned above, we can consider the values $m_{i,h}$ and η_i for this specific partition. However, due to symmetry, the values $m_{i,h}$ can be reduced to only four cases, depending on whether p and q are both balanced, one balanced and one unbalanced, or both unbalanced, either on the same coordinate or on different coordinates.

Assuming $1 \leq i, h \leq b$ with $i \neq h$, the following quantities are then well defined and independent of the specific values chosen for i and h

$$\begin{aligned} \breve{M}_1 &= \sup_{p,q \in \breve{\mathcal{P}}_b^0} \Psi_j(p;q) & \breve{M}_2 &= \sup_{p \in \breve{\mathcal{P}}_b^0, q \in \breve{\mathcal{P}}_b^i} \Psi_j(p;q) \\ \breve{M}_3 &= \sup_{p,q \in \breve{\mathcal{P}}_b^i} \Psi_j(p;q) & \breve{M}_4 &= \sup_{p \in \breve{\mathcal{P}}_b^i, q \in \breve{\mathcal{P}}_b^h} \Psi_j(p;q) \end{aligned} \tag{22}$$

These values can then be used in (21) in place of the values $m_{i,h}$.

Partition based on the minimum value. We also consider a partition of $\mathcal{P}_b$ using constraints from below. Again we use a parameter ϵ which will be then tuned. We assume here $\epsilon < 1/b$. Consider now the following disjoint sets of unbalanced distributions

$$\widehat{\mathcal{P}}_b^i = \{p \in \mathcal{P}_b : p_i < \epsilon \, , p_h \geq p_i \ \forall h \, , p_h > p_i \ \forall h < i\}$$

for $1 \leq i \leq b$, that is, distributions in $\widehat{\mathcal{P}}_b^i$ have a minimum component in the i-th coordinate, which is smaller than ϵ, and strictly smaller than any of the preceding components (unless of course $i = 1$). Correspondingly, define a set of balanced distributions as

$$\widehat{\mathcal{P}}_b^0 = \{p \in \mathcal{P}_b : p_i \geq \epsilon \ \forall i\} \ .$$

The symmetry argument mentioned before also applies in this case and we can continue in analogy replacing the $m_{i,h}$ of (21) with the following quantities

$$\begin{aligned} \widehat{M}_1 &= \sup_{p,q \in \widehat{\mathcal{P}}_b^0} \Psi_j(p;q) & \widehat{M}_2 &= \sup_{p \in \widehat{\mathcal{P}}_b^0, q \in \widehat{\mathcal{P}}_b^i} \Psi_j(p;q) \\ \widehat{M}_3 &= \sup_{p,q \in \widehat{\mathcal{P}}_b^i} \Psi_j(p;q) & \widehat{M}_4 &= \sup_{p \in \widehat{\mathcal{P}}_b^i, q \in \widehat{\mathcal{P}}_b^h} \Psi_j(p;q) \end{aligned} \tag{23}$$

where again $1 \leq i, h \leq b$ with $i \neq h$.

Quadratic form. Applying the above scheme with the symmetric partitions we just defined, we can now rewrite the upper bound of equation (21) in the form

$$\sum_{p,q} \lambda_p \lambda_q \Psi_j(p;q) \leq \eta_0^2 M_1 + 2\eta_0 \sum_{i=1}^{b} \eta_i M_2 + \sum_{i=1}^{b} \eta_i^2 M_3 + 2 \sum_{i<h} \eta_i \eta_h M_4 \, , \tag{24}$$

where either the $\widehat{M}_i$'s or the $\breve{M}_i$'s can be used in place of the M_i's.

Call M the maximum value achieved by the right hand side of (24) over all possible probability distributions $\eta = (\eta_0, \eta_1, \ldots, \eta_b)$. We show that under assumptions that are verified in our setting, the value of M can be determined explicitly.

LEMMA 2.2.4. *Let M_1, M_2, M_3 and M_4 be positive numbers such that $M_4 > M_3$ and, for a probability distribution $\eta = (\eta_0, \eta_1, \ldots, \eta_b)$, define the function*

$$f(\eta) = \eta_0^2 M_1 + 2\eta_0 \sum_{i=1}^{b} \eta_i M_2 + \sum_{i=1}^{b} \eta_i^2 M_3 + 2 \sum_{i<h} \eta_i \eta_h M_4 \, .$$

Then

$$M = \max_{\eta} f(\eta) \tag{25}$$

is attained at $\eta_1 = \eta_2 = \ldots = \eta_b$ *and*

$$\eta_0 = \begin{cases} \frac{M_2 - \frac{1}{b}M_3 - \frac{b-1}{b}M_4}{2M_2 - M_1 - \frac{1}{b}M_3 - \frac{b-1}{b}M_4}, & \text{if } M_2 > M_1, M_3, M_4 \\ 0 \text{ or } 1, & \text{otherwise} \end{cases}.$$

PROOF. Since $\sum_{i=1}^{b} \eta_i = (1 - \eta_0)$, f can be written as

$$\eta_0^2 M_1 + 2(1-\eta_0)\eta_0 M_2 + \sum_{i=1}^{b} \eta_i^2 M_3 + 2\sum_{i<h} \eta_i \eta_h M_4.$$

Note that

$$\sum_{i=1}^{b} \eta_i^2 M_3 + 2\sum_{i<h} \eta_i \eta_h M_4 = \sum_{i=1}^{b} \eta_i^2 (M_3 - M_4) + (1-\eta_0)^2 M_4.$$

Since $M_3 < M_4$ and $\sum_{i=1}^{b} \eta_i = 1 - \eta_0$, this sum is maximized when $\eta_1 = \eta_2 = \ldots = \eta_b = (1-\eta_0)/b$. Therefore we have to maximize the quantity

$$\eta_0^2 M_1 + 2(1-\eta_0)\eta_0 M_2 + \frac{1}{b}(1-\eta_0)^2 (M_3 - M_4) + (1-\eta_0)^2 M_4\,,$$

which is just a quadratic in η_0 that achieves its maximum in $[0, 1]$ at the point described in the statement of the Lemma. □

We will describe in the next Subsection our procedure to determine, or upper bound the values $\widehat{M}_i$, $\widetilde{M}_i$. Using these bounds in equation (24) we thus obtain an upper bound on $\mathbf{M}_j$ defined in (8). Applying Lemma 2.2.2 we obtain our main result.

THEOREM 2.2.1. *The bounds of Table 1 hold.*

REMARK 2.2.1. *The bounds on* $R_{(7,7)}$, $R_{(8,8)}$, $R_{(9,8)}$, $R_{(10,9)}$, $R_{(11,10)}$, $R_{(12,10)}$, $R_{(13,11)}$, $R_{(14,12)}$ *and* $R_{(15,13)}$ *are obtained using the partition based on* $\{\widetilde{\mathcal{P}}_b^i\}_{i=0,\ldots,b}$. *The bounds on* $R_{(5,5)}$, $R_{(6,5)}$ *and* $R_{(6,6)}$ *are obtained using the partition based on the minimum value* $\{\widehat{\mathcal{P}}_b^i\}_{i=0,\ldots,b}$.

All other cases, those underlined in Table 1, are obtained computing, as done in [42], the global maximum of Ψ_{k-2}, *which is attained for uniform distributions. Therefore, the partitioning process in these particular cases cannot make any improvements.*

Based on the result in [50], or its generalization given in equation (6) and on Theorem 2.2.1 for $(b, k) = (6, 6)$, we are led to formulate the following conjecture.

CONJECTURE 2.2.1. *For* $b \geq k > 3$,

$$R_{(b,k)} \leq \min_{2 \leq j \leq k-2} \left(\frac{1}{\log \frac{b}{j-1}} + \frac{b^{j+1}}{b^{\underline{j+1}} \log \frac{b-j}{k-j-1}} \right)^{-1}.$$

Note that the conjectured expression can be seen as a modification of the Körner-Marton bound in (5) which takes into account the effects of prefix-based partitions.

2.2.4. Computation of the maximum of the quadratic form. In light of Lemma 2.2.4, the main problem for the computation of M is determining the $\widetilde{M}_i$'s and $\widehat{M}_i$'s defined in equations (22) and (23). This requires determining the maximum values taken by $\Psi_j(p;q)$ for p and q constrained to specific subsets $\breve{\mathcal{P}}_b^i$ or $\widehat{\mathcal{P}}_b^i$. Following a procedure similar to that of [42], here we prove that, under certain conditions, the distributions p and q achieving those maxima have many equal components. This, together with other simplifications that will be presented later, allows us to greatly reduce the complexity in the search for the maxima (see Remarks 2.2.2 and 2.2.3 below). For this purpose we first present three Lemmas, which generalize Lemmas 3, 4 and 5 of [42].

LEMMA 2.2.5 (Extension of Lemma 3 in [42]). *Let ℓ be an integer in $[2, b]$ and, for $i \in [1, \ell]$, consider the nonempty intervals $I_i = [a_i, b_i]$ and $J_i = [c_i, d_i]$. Set $D_p = I_1 \times I_2 \times \cdots \times I_\ell \times \overline{p_{\ell+1}} \times \cdots \times \overline{p_b}$ and $D_q = J_1 \times J_2 \times \cdots \times J_\ell \times \overline{q_{\ell+1}} \times \cdots \times \overline{q_b}$. Consider the set D of pairs of probability vectors (p, q) such that p belongs to D_p and q belongs to D_q. Then if $(\overline{p}; \overline{q})$ is a maximum point for Ψ_j in D then either $\overline{p_i} = \overline{p_h}$ and $\overline{q_i} = \overline{q_h}$ for any $i, h \in [1, \ell]$ or there is a maximum for Ψ_j on the boundary of D (as projected on the first ℓ coordinates).*

Note that, in particular, in the latter case, we have a maximum point $(\overline{p}; \overline{q})$ for Ψ_j with at least one index $i \in [1, \ell]$ such that either $\overline{p_i} \in \{a_i, b_i\}$ or $\overline{q_i} \in \{c_i, d_i\}$.

PROOF. Let us assume that $\overline{P} = (\overline{p}; \overline{q})$ is a maximum point for Ψ_j in D and $\overline{p_1}, \overline{p_2}$, $\ldots, \overline{p_\ell}$ or $\overline{q_1}, \overline{q_2}, \ldots, \overline{q_\ell}$ are not all equal. By symmetry, assume without loss of generality that $\overline{p_1} \neq \overline{p_2}$. Now, if $\overline{P}$ is a maximum for Ψ_j not on the boundary D, then it is a maximum also under the stronger constraints $p_1 + p_2 = c_1$, $q_1 + q_2 = c_2$ where $c_1 = \overline{p_1} + \overline{p_1}$, $c_2 = \overline{q_1} + \overline{q_2}$, and $p_i = \overline{p_i}, q_i = \overline{q_i}$ for $i \in \{3, 4, \ldots, \ell\}$. Then, let us consider the line L of points $P(t)$ such that

$$P(t) = P(0) + t\left(\frac{\overline{p_1} - \overline{p_2}}{2}, \frac{-\overline{p_1} + \overline{p_2}}{2}, 0, \ldots, 0; \frac{\overline{q_1} - \overline{q_2}}{2}, \frac{-\overline{q_1} + \overline{q_2}}{2}, 0, \ldots, 0\right),$$

where $P(0) = (\frac{\overline{p}_1 + \overline{p}_2}{2}, \frac{\overline{p}_1 + \overline{p}_2}{2}, \overline{p}_3, \ldots, \overline{p}_b; \frac{\overline{q}_1 + \overline{q}_2}{2}, \frac{\overline{q}_1 + \overline{q}_2}{2}, \overline{q}_3, \ldots, \overline{q}_b)$, so that $P(1) = \bar{P}$.

It is easy to see that $\Psi_j(P(t))$ is of degree 2 and, if $\overline{P}$ is not on the boundary of D, then, $t = 1$ must be a stationary point for $\Psi_j(P(t))$. Moreover $\Psi_j(P(t))$ is an even function because:

$$\begin{aligned}
\Psi_j(P(-t)) &= P(0) - t\left(\frac{\overline{p_1} - \overline{p_2}}{2}, \frac{-\overline{p_1} + \overline{p_2}}{2}, 0, \ldots, 0; \frac{\overline{q_1} - \overline{q_2}}{2}, \frac{-\overline{q_1} + \overline{q_2}}{2}, 0, \ldots, 0\right) \\
&= P(0) + t\left(\frac{\overline{p_2} - \overline{p_1}}{2}, \frac{-\overline{p_2} + \overline{p_1}}{2}, 0, \ldots, 0; \frac{\overline{q_2} - \overline{q_1}}{2}, \frac{-\overline{q_2} + \overline{q_1}}{2}, 0, \ldots, 0\right) \\
&= \Psi_j(P(t)).
\end{aligned}$$

This means that $\Psi_j(P(t)) = \alpha t^2 + \beta$ for some α and β in $\mathbb{R}$. Therefore $t = 0$ would be another stationary point for $\Psi_j(P(t))$ but this is possible only if $\alpha = 0$ that is $\Psi_j(P(t))$ is a constant.

The thesis follows because, in this case, the maximum is also attained on the boundary of D. □

With essentially the same proof we obtain

LEMMA 2.2.6 (Extension of Lemma 4 in [42]). *Let ℓ be an integer in $[2, b]$ and, for $i \in [1, \ell]$, consider the nonempty intervals $I_i = [a_i, b_i]$. Set $D_p = I_1 \times I_2 \times \cdots \times I_\ell \times \overline{p_{\ell+1}} \times \cdots \times \overline{p_b}$ and $D_q = \overline{q_1} \times \overline{q_2} \times \cdots \times \overline{q_\ell} \times \overline{q_{\ell+1}} \times \cdots \times \overline{q_b}$ where $\overline{q_i} = \overline{q_h}$ for any $i, h \in [1, \ell]$. Consider*

the set D of pairs of probability vectors (p, q) such that p belongs to D_p and q belongs to D_q. Then if $(\overline{p}; \overline{q})$ is a maximum point for Ψ_j in D then either $\overline{p_i} = \overline{p_h}$ for any $i \in [1, \ell]$ or there is a maximum for Ψ_j on the boundary of D.

Note that, in particular, in the latter case, we have a maximum point $(\overline{p}; \overline{q})$ for Ψ_j with at least one index $i \in [1, \ell]$ such that $\overline{p_i} \in \{a_i, b_i\}$.

Now we present a Lemma that allows us to assume that the coordinates of p and q are properly rearranged depending on their values.

LEMMA 2.2.7 (Extension of Lemma 5 in [42]). *If $p_1 \leq p_2$, and $q_1 \leq q_2$, then*

$$\Psi_j(p_1, p_2, p_3, \ldots, p_b; q_1, q_2, q_3, \ldots, q_b) \leq \Psi_j(p_1, p_2, p_3, \ldots, p_b; q_2, q_1, q_3, \ldots, q_b). \tag{26}$$

PROOF. Using the definition of Ψ_j in eq. (7), inequality (26) can be restated by only considering the terms in the summation which differ in the two sides, that is, those corresponding to permutations σ such that $1 \in \{\sigma(1), \ldots, \sigma(j)\}$, $\sigma(j+1) = 2$ and $2 \in \{\sigma(1), \ldots, \sigma(j)\}$, $\sigma(j+1) = 1$. Hence inequality (26) becomes

$$\begin{aligned}
&(p_1 q_2 + p_2 q_1) \sum_{\sigma \in Sym(3,\ldots,b)} p_{\sigma(3)} \cdots p_{\sigma(j+1)} + q_{\sigma(3)} \cdots q_{\sigma(j+1)} \\
&\leq (p_1 q_1 + p_2 q_2) \sum_{\sigma \in Sym(3,\ldots,b)} p_{\sigma(3)} \cdots p_{\sigma(j+1)} + q_{\sigma(3)} \cdots q_{\sigma(j+1)}
\end{aligned}$$

which can be restated as

$$(p_2 - p_1)(q_2 - q_1) \sum_{\sigma \in Sym(3,\ldots,b)} p_{\sigma(3)} \cdots p_{\sigma(j+1)} + q_{\sigma(3)} \cdots q_{\sigma(j+1)} \geq 0$$

This is always true since $p_1 \leq p_2$ and $q_1 \leq q_2$. □

Using the above lemmas, we are able to isolate a relatively small set of possible configurations for the p and q which give the value $\widetilde{M}_1$.

PROPOSITION 2.2.1. *$\widetilde{M}_1$ is attained in one of the following points:*

1) *for $(p; q)$ of the form*

$$(\overbrace{0, \ldots, 0}^{l_1}, \underbrace{\alpha, \ldots, \alpha}_{l_2}, \overbrace{\beta, \ldots, \beta}^{b-l_1-l_2-2}, \gamma, 1-\epsilon; \overbrace{\delta, \ldots, \delta}^{l_1}, \underbrace{0, \ldots, 0}_{l_2}, \overbrace{\eta, \ldots, \eta}^{b-l_1-l_2-2}, 1-\epsilon, \zeta)$$

where $\alpha, \delta > 0$, $\beta, \eta, \gamma, \zeta \geq 0$ and

$$l_2\alpha + (b - l_1 - l_2 - 2)\beta + \gamma + (1-\epsilon) = 1 = l_1\delta + (b - l_1 - l_2 - 2)\eta + (1-\epsilon) + \zeta;$$

2) *for $(p; q)$ of the form*

$$(\overbrace{0, \ldots, 0}^{l_1}, \underbrace{\alpha, \ldots, \alpha}_{l_2}, \overbrace{\beta, \ldots, \beta}^{b-l_1-l_2-1}, \gamma; \overbrace{\delta, \ldots, \delta}^{l_1}, \underbrace{0, \ldots, 0}_{l_2}, \overbrace{\eta, \ldots, \eta}^{b-l_1-l_2-1}, 1-\epsilon)$$

where $\alpha, \delta > 0$, $\beta, \eta, \gamma \geq 0$ and

$$l_2\alpha + (b - l_1 - l_2 - 1)\beta + \gamma = 1 = l_1\delta + (b - l_1 - l_2 - 1)\eta + (1-\epsilon);$$

3) *for* $(p; q)$ *of the form*

$$(\overbrace{0,\dots,0}^{l_1},\underbrace{\alpha,\dots,\alpha}_{l_2},\overbrace{\beta,\dots,\beta}^{b-l_1-l_2};\overbrace{\delta,\dots,\delta}^{l_1},\underbrace{0,\dots,0}_{l_2},\overbrace{\eta,\dots,\eta}^{b-l_1-l_2})$$

where $\alpha, \delta > 0, \quad \beta, \eta \geq 0$ *and*

$$l_2\alpha + (b - l_1 - l_2)\beta = 1 = l_1\delta + (b - l_1 - l_2)\eta.$$

Proof. Remember that the value $\widetilde{M}_1$ is the maximum of Ψ_j over pairs (p, q) with p and q in $\widetilde{\mathcal{P}}_b^0$. Moreover, due to Lemma 2.2.7, we have that p and q do not have a value $1-\epsilon$ in the same coordinate. Similarly, again because of Lemma 2.2.7, either the zeros of p and q are in different positions (i.e. if $p_i = 0$ then $q_i \neq 0$) or for any i at least one between p_i and q_i is zero.

According to the positions where values $1-\epsilon$ and zero can appear as coordinates of p and q, we have that $\widetilde{M}_1$ is attained in one of the following points:

1A) p and q have respectively l_1 and l_2 zeros in different positions, both have a coordinate with value $1-\epsilon$ and those are in different positions:

$$(\overbrace{0,\dots,0}^{l_1},\underbrace{\alpha_1,\dots,\alpha_{l_2}}_{l_2},\overbrace{\beta_1,\dots,\beta_{b-l_1-l_2-2}}^{b-l_1-l_2-2},\gamma,1-\epsilon;\overbrace{\delta_1,\dots,\delta_{l_1}}^{l_1},\underbrace{0,\dots,0}_{l_2},\overbrace{\eta_1,\dots,\eta_{b-l_1-l_2-2}}^{b-l_1-l_2-2},1-\epsilon,\zeta);$$

1B) p and q have respectively l_1 and l_2 zeros in different positions, additional $b-l_1-l_2-2$ zeros in the same positions, both have a coordinate with value $1-\epsilon$ and those are in different positions:

$$(\overbrace{0,\dots,0}^{l_1},\underbrace{\alpha_1,\dots,\alpha_{l_2}}_{l_2},\overbrace{0,\dots,0}^{b-l_1-l_2-2},0,1-\epsilon;\overbrace{\delta_1,\dots,\delta_{l_1}}^{l_1},\underbrace{0,\dots,0}_{l_2},\overbrace{0,\dots,0}^{b-l_1-l_2-2},1-\epsilon,0);$$

2A) p and q have respectively l_1 and l_2 zeros in different positions, p has no coordinate of value $1-\epsilon$ but q has:

$$(\overbrace{0,\dots,0}^{l_1},\underbrace{\alpha_1,\dots,\alpha_{l_2}}_{l_2},\overbrace{\beta_1,\dots,\beta_{b-l_1-l_2-1}}^{b-l_1-l_2-1},\gamma;\overbrace{\delta_1,\dots,\delta_{l_1}}^{l_1},\underbrace{0,\dots,0}_{l_2},\overbrace{\eta_1,\dots,\eta_{b-l_1-l_2-1}}^{b-l_1-l_2-1},1-\epsilon);$$

2B) p and q have respectively l_1 and l_2 zeros in different positions, additional $b-l_1-l_2-1$ zeros in the same positions, p has no coordinate of value $1-\epsilon$ but q has:

$$(\overbrace{0,\dots,0}^{l_1},\underbrace{\alpha_1,\dots,\alpha_{l_2}}_{l_2},\overbrace{0,\dots,0}^{b-l_1-l_2-1},0;\overbrace{\delta_1,\dots,\delta_{l_1}}^{l_1},\underbrace{0,\dots,0}_{l_2},\overbrace{0,\dots,0}^{b-l_1-l_2-1},1-\epsilon);$$

3A) p and q have respectively l_1 and l_2 zeros in different positions and both have no coordinates with value $1-\epsilon$:

$$(\overbrace{0,\dots,0}^{l_1},\underbrace{\alpha_1,\dots,\alpha_{l_2}}_{l_2},\overbrace{\beta_1,\dots,\beta_{b-l_1-l_2}}^{b-l_1-l_2};\overbrace{\delta_1,\dots,\delta_{l_1}}^{l_1},\underbrace{0,\dots,0}_{l_2},\overbrace{\eta_1,\dots,\eta_{b-l_1-l_2}}^{b-l_1-l_2});$$

3B) p and q have respectively l_1 and l_2 zeros in different positions, additional $b-l_1-l_2$ zeros in the same positions and neither has a coordiante of value $1-\epsilon$:

$$(\overbrace{0,\ldots,0}^{l_1},\underbrace{\alpha_1,\ldots,\alpha_{l_2}}_{l_2},\overbrace{0,\ldots,0}^{b-l_1-l_2};\overbrace{\delta_1,\ldots,\delta_{l_1}}^{l_1},\underbrace{0,\ldots,0}_{l_2},\overbrace{0,\ldots,0}^{b-l_1-l_2}).$$

Moreover, in all those cases, the allowed domains for p and q satisfy either the hypothesis of Lemma 2.2.5 or those of Lemma 2.2.6. This means that we can average the α's (i.e. we can assume that all the α's are equal), the β's, the δ's, and the η's. The thesis follows allowing β and η to possibly be zero and noting that the case $1B$ becomes a subcase of $1A$, $2B$ becomes a subcase of $2A$ and $3B$ becomes a subcase of $3A$. □

REMARK 2.2.2. *As seen in Proposition 2.2.1, Lemmas 2.2.5, 2.2.6 and 2.2.7 reduce the maxima candidates to a finite set of possible configurations. Still, the number of such configurations increases with b, and the ensuing optimization problems depend on 4 free variables in the case 1. The direct evaluation of the maxima of Ψ_j on those configurations can in principle be performed by symbolic computation software, but the resources needed are excessive. In the following lemmas, we provide additional simplifications to obtain the exact evaluations of the maxima.*

Due to the following lemma, we can assume that the number of zeros that appear in p (resp. in q) is either $b-2$ or at most $b-j$. Note that this simplification does not decrease the number of free variables but it reduces the total number of cases.

LEMMA 2.2.8 (Extension of Lemma 6 in [42]). *Suppose that $q_1 \leq q_2 \leq \ldots \leq q_{j-1}$. If all the p_i are less than or equal to $1-\alpha$ where $0 \leq \alpha < 1$, then*

$$\begin{aligned}&\Psi_j(p_1,p_2,\ldots,p_{j-1},0,\ldots,0;q_1,q_2,\ldots,q_b)\\ &\qquad\qquad\leq \Psi_j(1-\alpha,\alpha,0,\ldots,0;q_1,q_2,\ldots,q_b).\end{aligned}\tag{27}$$

PROOF. Let $0 \leq \delta \leq p_2$. We first prove that

$$\begin{aligned}&\Psi_j(p_1,p_2,\ldots,p_{j-1},0,\ldots,0;q_1,q_2,\ldots,q_b)\\ &\qquad\leq \Psi_j(p_1+\delta,p_2-\delta,\ldots,p_{j-1},0,\ldots,0;q_1,q_2,\ldots,q_b).\end{aligned}\tag{28}$$

Using the definition of Ψ_j in eq. (7), inequality (28) can be restated by only considering the terms in the summation which differ in the two sides, that is, those corresponding to permutations σ such that $1 \in \{\sigma(1),\ldots,\sigma(j)\}$, $\sigma(j+1)=2$ and $2 \in \{\sigma(1),\ldots,\sigma(j)\}$, $\sigma(j+1)=1$. This gives

$$\begin{aligned}(p_1q_2+p_2q_1)&\sum_{\sigma\in Sym(3,\ldots,b)} q_{\sigma(3)}\cdots q_{\sigma(j+1)}\\ &\leq ((p_1+\delta)q_2+(p_2-\delta)q_1)\sum_{\sigma\in Sym(3,\ldots,b)} q_{\sigma(3)}\cdots q_{\sigma(j+1)}\,.\end{aligned}$$

Rearranging the terms we have

$$\delta(q_2-q_1)\sum_{\sigma\in Sym(3,\ldots,b)} q_{\sigma(3)}\cdots q_{\sigma(j+1)} \geq 0\,.$$

Therefore, inequality (28) is thus satisfied since $q_1 \leq q_2$ and $\delta \geq 0$. Moreover, given $h > i$ and δ such that $0 \leq \delta \leq p_h$, with the same argument we have

$$\begin{aligned}(29)\quad &\Psi_j(p_1, \ldots, p_i, \ldots, p_h, \ldots, p_{j-1}, 0, \ldots, 0; q_1, q_2, \ldots, q_b) \\ &\qquad \leq \Psi_j(p_1, \ldots, p_i + \delta, \ldots, p_h - \delta, \ldots, p_{j-1}, 0, \ldots, 0; q_1, q_2, \ldots, q_b).\end{aligned}$$

Using multiple times inequality (29) we get the following chain of inequalities

$$\begin{aligned}&\Psi_j(p_1, p_2, \ldots, p_{j-1}, 0, \ldots, 0; q_1, q_2, \ldots, q_b) \\ &\qquad \leq \Psi_j(p_1, \alpha, p'_3, \ldots, p'_{j-1}, 0, \ldots, 0; q_1, q_2, \ldots, q_b) \\ &\qquad\qquad \leq \Psi_j(1 - \alpha, \alpha, 0, \ldots, 0; q_1, q_2, \ldots, q_b)\,,\end{aligned}$$

where $p'_3 + \ldots + p'_{j-1} = 1 - p_1 - \alpha$ and $p'_i \in [0, 1 - \alpha]$ for $i = 3, \ldots, j - 1$. □

The following lemma takes care of the cases when there is at least one element greater or equal to $1 - \epsilon$ in p or q vector. If this element is p_1, because of Lemma 2.2.7 we can assume q_1 is the minimum among the q-values if we are maximizing Ψ_j. For the evaluation of $\widetilde{M}_1$, this implies that $q_1 = 0$ whenever $p_1 = 1 - \epsilon$ and vice-versa.

LEMMA 2.2.9. *Assume that* $\epsilon \leq \frac{1}{j+1}$, $p_1 \geq 1 - \epsilon$ *and* $q_1 \leq q_2 \leq \ldots \leq q_b$. *Then*

$$(30)\qquad \Psi_j(p_1, p_2, \ldots, p_b; q_1, q_2, \ldots, q_b) \leq \Psi_j(p_1, p_2, \ldots, p_b; 0, q_1 + q_2, q_3, \ldots, q_b).$$

PROOF. Using the definition of Ψ_j in eq. (7), inequality (30) can be restated by only considering the terms in the summation which differ in the two sides, that is, those corresponding to permutations σ such that $1 \in \{\sigma(1), \ldots, \sigma(j)\}$, $\sigma(j+1) = 2$ and $2 \in \{\sigma(1), \ldots, \sigma(j)\}$, $\sigma(j+1) = 1$ and $\{1, 2\} \subseteq \{\sigma(1), \ldots, \sigma(j)\}$. Hence inequality (30) becomes:

$$\begin{aligned}&(p_1 q_2 + p_2 q_1) \sum_{\sigma \in Sym(3,\ldots,b)} p_{\sigma(3)} \cdots p_{\sigma(j+1)} + q_{\sigma(3)} \cdots q_{\sigma(j+1)} + \\ &(j-1) q_2 q_1 \sum_{\sigma \in Sym(3,\ldots,b)} q_{\sigma(3)} \cdots q_{\sigma(j)} p_{\sigma(j+1)} \\ &\leq p_1(q_1 + q_2) \sum_{\sigma \in Sym(3,\ldots,b)} p_{\sigma(3)} \cdots p_{\sigma(j+1)} + q_{\sigma(3)} \cdots q_{\sigma(j+1)}.\end{aligned}$$

That is

$$\begin{aligned}&p_2 q_1 \sum_{\sigma \in Sym(3,\ldots,b)} p_{\sigma(3)} \cdots p_{\sigma(j+1)} + q_{\sigma(3)} \cdots q_{\sigma(j+1)} + \\ &(j-1) q_2 q_1 \sum_{\sigma \in Sym(3,\ldots,b)} q_{\sigma(3)} \cdots q_{\sigma(j)} p_{\sigma(j+1)} \\ &\leq p_1 q_1 \sum_{\sigma \in Sym(3,\ldots,b)} p_{\sigma(3)} \cdots p_{\sigma(j+1)} + q_{\sigma(3)} \cdots q_{\sigma(j+1)}.\end{aligned}$$

We have

$$\begin{aligned}
&p_2q_1 \sum_{\sigma\in Sym(3,\dots,b)} p_{\sigma(3)}\cdots p_{\sigma(j+1)} + q_{\sigma(3)}\cdots q_{\sigma(j+1)} + \\
&(j-1)q_2q_1 \sum_{\sigma\in Sym(3,\dots,b)} q_{\sigma(3)}\cdots q_{\sigma(j)}p_{\sigma(j+1)} \\
&\overset{(i)}{\leq} q_1\epsilon \sum_{\sigma\in Sym(3,\dots,b)} p_{\sigma(3)}\cdots p_{\sigma(j+1)} + q_{\sigma(3)}\cdots q_{\sigma(j+1)} + \\
&(j-1)q_1\epsilon \sum_{\sigma\in Sym(3,\dots,b)} q_2q_{\sigma(3)}\cdots q_{\sigma(j)} \\
&\overset{(ii)}{\leq} q_1\epsilon \sum_{\sigma\in Sym(3,\dots,b)} p_{\sigma(3)}\cdots p_{\sigma(j+1)} + jq_1\epsilon \sum_{\sigma\in Sym(3,\dots,b)} q_{\sigma(3)}\cdots q_{\sigma(j+1)} \\
&\overset{(iii)}{\leq} (1-\epsilon)q_1 \sum_{\sigma\in Sym(3,\dots,b)} p_{\sigma(3)}\cdots p_{\sigma(j+1)} + q_{\sigma(3)}\cdots q_{\sigma(j+1)} \\
&\overset{(iiii)}{\leq} p_1q_1 \sum_{\sigma\in Sym(3,\dots,b)} p_{\sigma(3)}\cdots p_{\sigma(j+1)} + q_{\sigma(3)}\cdots q_{\sigma(j+1)}
\end{aligned}$$

Inequality (i) holds because $p_2, p_3, \dots, p_b \leq \epsilon$, inequality (ii) because $q_2 \leq q_3 \leq \dots \leq q_b$, inequality (iii) due to the assumption $\epsilon \leq \frac{1}{j+1}$ and inequality $(iiii)$ since $p_1 \geq 1-\epsilon$. □

Thanks to Lemmas 2.2.8 and 2.2.9, we obtain the following proposition.

PROPOSITION 2.2.2. *$\widetilde{M}_1$ is attained in one of the following points:*

1) *for $(p;q)$ of the form*

$$(\overbrace{0,\dots,0}^{l_1},\underbrace{\alpha,\dots,\alpha}_{l_2},\overbrace{\beta,\dots,\beta}^{b-l_1-l_2-2},0,1-\epsilon;\overbrace{\delta,\dots,\delta}^{l_1},\underbrace{0,\dots,0}_{l_2},\overbrace{\eta,\dots,\eta}^{b-l_1-l_2-2},1-\epsilon,0)$$

where $\alpha,\beta,\delta,\eta \geq 0$ and

$$l_2\alpha + (b-l_1-l_2-2)\beta + (1-\epsilon) = 1 = l_1\delta + (b-l_1-l_2-2)\eta + (1-\epsilon);$$

2) *for $(p;q)$ of the form*

$$(\overbrace{0,\dots,0}^{l_1},\underbrace{\alpha,\dots,\alpha}_{l_2},\overbrace{\beta,\dots,\beta}^{b-l_1-l_2-1},0;\overbrace{\delta,\dots,\delta}^{l_1},\underbrace{0,\dots,0}_{l_2},\overbrace{\eta,\dots,\eta}^{b-l_1-l_2-1},1-\epsilon)$$

where $\alpha,\beta,\delta,\eta \geq 0$ and

$$l_2\alpha + (b-l_1-l_2-1)\beta = 1 = l_1\delta + (b-l_1-l_2-1)\eta + (1-\epsilon);$$

3) *for $(p;q)$ of the form*

$$(\overbrace{0,\dots,0}^{l_1},\underbrace{\alpha,\dots,\alpha}_{l_2},\overbrace{\beta,\dots,\beta}^{b-l_1-l_2};\overbrace{\delta,\dots,\delta}^{l_1},\underbrace{0,\dots,0}_{l_2},\overbrace{\eta,\dots,\eta}^{b-l_1-l_2})$$

where $\alpha,\beta,\delta,\eta \geq 0$ and

$$l_2\alpha + (b-l_1-l_2)\beta = 1 = l_1\delta + (b-l_1-l_2)\eta.$$

Moreover, we can assume that the number of zeros that appear in p and in q is either $b-2$ or at most $b-j$.

PROOF. We consider the finite list of cases provided by Proposition 2.2.1 and we relax the domains of p and q allowing α and δ to be 0. Here, due to Lemma 2.2.9, a maximum with exactly one element equal to $1-\epsilon$ in p (resp. q) implies a zero in the same coordinate of q (resp. p). Finally, because of Lemma 2.2.8, a maximum with $b-j+1$ or more coordinates in p (resp. q) equal to zero is also attained in a point of the form $p = (1-\epsilon, \epsilon, 0, \ldots, 0)$ ($q = (1-\epsilon, \epsilon, 0, \ldots, 0)$). □

PROPOSITION 2.2.3. *$\breve{M}_2$ is upper bounded by the global maximum of Ψ_j which is attained in a point $(p; q)$ of the following form:*

$$(\overbrace{0,\ldots,0}^{l_1}, \underbrace{\alpha,\ldots,\alpha}_{l_2}, \overbrace{\beta,\ldots,\beta}^{b-l_1-l_2}; \overbrace{\delta,\ldots,\delta}^{l_1}, \underbrace{0,\ldots,0}_{l_2}, \overbrace{\eta,\ldots,\eta}^{b-l_1-l_2})$$

where $\alpha, \beta, \delta, \eta \geq 0$ and

$$l_2\alpha + (b-l_1-l_2)\beta = 1 = l_1\delta + (b-l_1-l_2)\eta.$$

Moreover, we can assume that the number of zeros that appear in p and in q is either $b-1$ or at most $b-j$.

PROOF. In order to find the global maximum of Ψ_j we need no restriction on the pairs (p, q), i.e., $p \in [0,1]^b$ and $q \in [0,1]^b$. Using Lemmas 2.2.5, 2.2.6, 2.2.7 and 2.2.8, we can easily derived the desired points. □

Now, to provide a list of possible maxima also for the other $\breve{M}_i$ and $\widehat{M}_i$, we need also the following additional lemma.

LEMMA 2.2.10. *Assume that $\epsilon < \frac{1}{2}$, $q_1 \geq 1-\epsilon$ and $0 < \delta \leq \epsilon$, then*

$$\Psi_j(1-\epsilon+\delta, p_2, p_3, \ldots, p_b; q_1, q_2, \ldots, q_b) < \Psi_j(1-\epsilon, p_2+\delta, p_3, \ldots, p_b; q_1, q_2, \ldots, q_b). \quad (31)$$

PROOF. Using the definition of Ψ_j in eq. (7), inequality (31) can be restated by only considering the terms in the summation which differ in the two sides, that is, those corresponding to permutations σ such that $1 \in \{\sigma(1), \ldots, \sigma(j)\}$, $\sigma(j+1) = 2$ and $2 \in \{\sigma(1), \ldots, \sigma(j)\}$, $\sigma(j+1) = 1$ and $\{1, 2\} \subseteq \{\sigma(1), \ldots, \sigma(j)\}$. Therefore we have that

$$\begin{aligned}
&((1-\epsilon+\delta)q_2 + q_1p_2) \sum_{\sigma \in Sym(3,\ldots,b)} p_{\sigma(3)} \cdots p_{\sigma(j+1)} + q_{\sigma(3)} \cdots q_{\sigma(j+1)} + \\
&(j-1)(1-\epsilon+\delta)p_2 \sum_{\sigma \in Sym(3,\ldots,b)} p_{\sigma(3)} \cdots p_{\sigma(j)} q_{\sigma(j+1)} \\
&< ((1-\epsilon)q_2 + q_1(p_2+\delta)) \sum_{\sigma \in Sym(3,\ldots,b)} p_{\sigma(3)} \cdots p_{\sigma(j+1)} + q_{\sigma(3)} \cdots q_{\sigma(j+1)} + \\
&(j-1)(1-\epsilon)(p_2+\delta) \sum_{\sigma \in Sym(3,\ldots,b)} p_{\sigma(3)} \cdots p_{\sigma(j)} q_{\sigma(j+1)}.
\end{aligned}$$

That is

$$\delta(q_1-q_2)\sum_{\sigma\in Sym(3,\dots,b)} p_{\sigma(3)}\cdots p_{\sigma(j+1)}+q_{\sigma(3)}\cdots q_{\sigma(j+1)}+$$
$$(j-1)\delta(1-\epsilon-p_2)\sum_{\sigma\in Sym(3,\dots,b)} p_{\sigma(3)}\cdots p_{\sigma(j)}q_{\sigma(j+1)}>0.$$

Which is satisfied because $q_2<q_1$, $p_2<1-\epsilon$ and $\delta>0$. □

Thanks to Lemma 2.2.10, we obtain the following proposition.

PROPOSITION 2.2.4. *$\widetilde{M}_3$ is attained in a point $(p;q)$ of the following form:*

$$(1-\epsilon,\overbrace{0,\dots,0}^{l_1},\underbrace{\alpha,\dots,\alpha}_{l_2},\overbrace{\beta,\dots,\beta}^{b-l_1-l_2-1};1-\epsilon,\overbrace{\delta,\dots,\delta}^{l_1},\underbrace{0,\dots,0}_{l_2},\overbrace{\eta,\dots,\eta}^{b-l_1-l_2-1})$$

where $\alpha,\beta,\delta,\eta\geq 0$ and

$$l_2\alpha+(b-l_1-l_2-1)\beta=\epsilon=l_1\delta+(b-l_1-l_2-1)\eta.$$

Moreover, we can assume that the number of zeros that appear in p and in q is either $b-2$ or at most $b-j$.

PROOF. In order to find the values $\widetilde{M}_3$ we need to restrict the function Ψ_j to the pairs (p,q) such that p and q belong to $\check{\mathcal{P}}_b^1$ (by symmetry we can fix an arbitrary coordinate).

Using Lemmas 2.2.5, 2.2.6, 2.2.7 and 2.2.8, we see that $\widetilde{M}_3$ is attained in a point of the following form:

$$(\gamma,\overbrace{0,\dots,0}^{l_1},\underbrace{\alpha,\dots,\alpha}_{l_2},\overbrace{\beta,\dots,\beta}^{b-l_1-l_2-1};\zeta,\overbrace{\delta,\dots,\delta}^{l_1},\underbrace{0,\dots,0}_{l_2},\overbrace{\eta,\dots,\eta}^{b-l_1-l_2-1})$$

where $\alpha,\beta,\delta,\eta\geq 0$, $\gamma,\zeta\geq 1-\epsilon$ and

$$\gamma+l_2\alpha+(b-l_1-l_2-1)\beta=1=\zeta+l_1\delta+(b-l_1-l_2-1)\eta.$$

Finally, because of Lemma 2.2.10 a maximum with $\gamma,\zeta\geq 1-\epsilon$ is also attained in a point with $\gamma=\zeta=1-\epsilon$. □

PROPOSITION 2.2.5. *$\widetilde{M}_4$ is attained in one of the following points:*

1) *for $(p;q)$ of the form*

$$(\gamma,\alpha,\dots,\alpha,0;0,\delta,\dots,\delta,\zeta)$$

where $\alpha,\delta\geq 0$, $\gamma,\zeta\geq 1-\epsilon$, and

$$\gamma+(b-2)\alpha=1=(b-2)\delta+\zeta.$$

2) *for $(p;q)$ of the form*

$$(\gamma,\overbrace{0,\dots,0}^{l_1},\underbrace{\alpha,\dots,\alpha}_{b-l_1-2},0;0,\overbrace{\delta,\dots,\delta}^{l_1},\underbrace{\eta,\dots,\eta}_{b-l_1-2},\zeta)$$

where $\alpha,\delta,\eta\geq 0$, $\gamma\geq 1-\epsilon$, $\zeta\in\{1-\epsilon,1\}$, and

$$(b-l_1-2)\alpha+\gamma=1=l_1\delta+(b-l_1-2)\eta+\zeta.$$

3) *for* $(p;q)$ *of the form*

$$(\gamma,\overbrace{0,\dots,0}^{l_1},\underbrace{\alpha,\dots,\alpha}_{l_2},\overbrace{\beta,\dots,\beta}^{b-l_1-l_2-2},0;0,\overbrace{\delta,\dots,\delta}^{l_1},\underbrace{0,\dots,0}_{l_2},\overbrace{\eta,\dots,\eta}^{b-l_1-l_2-2},\zeta)$$

where $\alpha,\beta,\delta,\eta\geq 0$, $\gamma,\zeta\in\{1-\epsilon,1\}$, *and*

$$l_2\alpha+(b-l_1-l_2-2)\beta+\gamma=1=l_1\delta+(b-l_1-l_2-2)\eta+\zeta.$$

Moreover, we can assume that the number of zeros that appear in p *and in* q *is either* $b-1$ *or at most* $b-j$.

Proof. In order to find the values $\breve{M}_4$ we need to restrict the function Ψ_j to the pairs $(p;q)$ such that p belongs to $\breve{\mathcal{P}}_b^1$ and q belongs to $\breve{\mathcal{P}}_b^b$ (by symmetry we can choose, arbitrarily, two different coordinates).

Using Lemmas 2.2.5, 2.2.6, 2.2.7, 2.2.8 and 2.2.9 we see that $\breve{M}_4$ is attained in a point of the following form:

$$(\gamma,\overbrace{0,\dots,0}^{l_1},\underbrace{\alpha,\dots,\alpha}_{l_2},\overbrace{\beta,\dots,\beta}^{b-l_1-l_2-2},0;0,\overbrace{\delta,\dots,\delta}^{l_1},\underbrace{0,\dots,0}_{l_2},\overbrace{\eta,\dots,\eta}^{b-l_1-l_2-2},\zeta)$$

where $\alpha,\beta,\delta,\eta\geq 0$, $\gamma,\zeta\geq 1-\epsilon$, and

$$l_2\alpha+(b-l_1-l_2-2)\beta+\gamma=1=l_1\delta+(b-l_1-l_2-2)\eta+\zeta.$$

Finally, we can split this case into three cases. The first one is for $l_1=l_2=0$, the second one for $l_1>0, l_2=0$ and the third one for $l_1,l_2>0$. By symmetry the case $l_1=0, l_2>0$ is included in the second case. For the second case, by Lemma 2.2.6 it is easy to see that δ or ζ must be on the boundary in order to be a valid point for $\breve{M}_4$. The same argument can be carried out for the third case which implies that $\gamma,\zeta\in\{1-\epsilon,1\}$. □

Proposition 2.2.6. $\widehat{M}_1$ *is attained in a point* $(p;q)$ *of the following form:*

$$(\overbrace{\epsilon,\dots,\epsilon}^{l_1},\underbrace{\alpha,\dots,\alpha}_{l_2},\overbrace{\beta,\dots,\beta}^{b-l_1-l_2};\overbrace{\delta,\dots,\delta}^{l_1},\underbrace{\epsilon,\dots,\epsilon}_{l_2},\overbrace{\eta,\dots,\eta}^{b-l_1-l_2})$$

where $\alpha,\beta,\delta,\eta\geq\epsilon$ *and*

$$l_1\epsilon+\alpha+(b-l_1-l_2)\beta=1=l_2\epsilon+l_1\delta+(b-l_1-l_2)\eta.$$

Proof. In order to find the values $\widehat{M}_1$ we need to restrict the function Ψ_j to the pairs (p,q) such that p and q belong to $\widehat{\mathcal{P}}_b^0$. Using Lemmas 2.2.5, 2.2.6 and 2.2.7 we obtain the thesis. □

Proposition 2.2.7. $\widehat{M}_2$ *is attained in one of the following points:*

1) *for* $(p;q)$ *of the form*

$$(\overbrace{\alpha,\dots,\alpha}^{l_1},\underbrace{\beta,\dots,\beta}_{b-l_1};\overbrace{\eta,\dots,\eta}^{l_1},\underbrace{\epsilon,\dots,\epsilon}_{b-l_1})$$

where $0\leq\alpha\leq\epsilon,\quad \beta\geq 0,\quad \eta\geq\epsilon$, *and*

$$l_1\alpha+(b-l_1)\beta=1=l_1\eta+(b-l_1)\epsilon.$$

2) *for* $(p;q)$ *of the form*

$$(\epsilon, \overbrace{\alpha, \ldots, \alpha}^{l_1}, \underbrace{\beta, \ldots, \beta}_{b-l_1-1}; \zeta, \overbrace{\eta, \ldots, \eta}^{l_1}, \underbrace{\epsilon, \ldots, \epsilon}_{b-l_1-1})$$

where $\alpha, \beta \geq 0, \quad \zeta, \eta \geq \epsilon$, *and*

$$\epsilon + l_1\alpha + (b - l_1 - 1)\beta = 1 = \zeta + l_1\eta + (b - l_1 - 1)\epsilon.$$

3) *for* $(p;q)$ *of the form*

$$(\overbrace{0, \ldots, 0}^{l_1}, \underbrace{\alpha, \ldots, \alpha}_{l_2}, \overbrace{\beta, \ldots, \beta}^{b-l_1-l_2}; \overbrace{\delta, \ldots, \delta}^{l_1}, \underbrace{\eta, \ldots, \eta}_{l_2}, \overbrace{\epsilon, \ldots, \epsilon}^{b-l_1-l_2})$$

where $\alpha, \beta \geq 0, \quad \delta, \eta \geq \epsilon$ *and*

$$l_2\alpha + (b - l_1 - l_2)\beta = 1 = l_1\delta + (b - l_1 - l_2)\eta.$$

Moreover, we can assume that the number of zeros that appear in p *is either* $b - 1$ *or at most* $b - j$.

PROOF. In order to find the values $\widehat{M}_2$ we need to restrict the function Ψ_j to the pairs (p, q) such that p belongs to $\widehat{\mathcal{P}}_b^1$ and q belongs to $\widehat{\mathcal{P}}_b^0$. In addition, we relax the domain of p by removing the constraint on p_1 to be a minimum coordinate., i.e., $p \in [0, \epsilon] \times [0, 1]^{b-1}$. However, this implies that p belongs to $\widehat{\mathcal{P}}_b^i$ for some $i \in [1, b]$. Therefore, by symmetry, we are still considering valid candidates for $\widehat{M}_2$ under this domain.

Using Lemmas 2.2.5, 2.2.6, 2.2.7 and 2.2.8, we see that $\widehat{M}_2$ is attained in a point of the following form:

$$(\gamma, \overbrace{0, \ldots, 0}^{l_1}, \underbrace{\alpha, \ldots, \alpha}_{b-l_1-l_2-1}, \overbrace{\beta, \ldots, \beta}^{l_2}; \zeta, \overbrace{\delta, \ldots, \delta}^{l_1}, \underbrace{\eta, \ldots, \eta}_{b-l_1-l_2-1}, \overbrace{\epsilon, \ldots, \epsilon}^{l_2})$$

where $\alpha, \beta \geq 0, \quad 0 \leq \gamma \leq \epsilon, \quad \zeta, \delta, \eta \geq \epsilon$, and

$$\gamma + (b - l_1 - l_2 - 1)\alpha + l_2\beta = 1 = \zeta + l_1\delta + (b - l_1 - l_2 - 1)\eta + l_2\epsilon.$$

Finally, we can split this case into three cases. The first one is when $l_1 = 0$ and the average between γ and the α-components is less than or equal to ϵ, the second one for $\gamma = \epsilon$ and $l_1 = 0$ while the third one for $\gamma = 0$ and $l_1 \geq 0$. We have not considered the case $\gamma = \epsilon$ and $l_1 > 0$ since it is a subcase of the third one. □

PROPOSITION 2.2.8. *An upper bound on* $\widehat{M}_3$ *is obtained by computing the maximum of* Ψ_j *over points of the following form:*

1) *for* $(p;q)$ *of the form*

$$(\beta, \overbrace{0, \ldots, 0}^{l_1}, \underbrace{\alpha, \ldots, \alpha}_{l_2}, \overbrace{\beta, \ldots, \beta}^{b-l_1-l_2-1}; \eta, \overbrace{\delta, \ldots, \delta}^{l_1}, \underbrace{0, \ldots, 0}_{l_2}, \overbrace{\eta, \ldots, \eta}^{b-l_1-l_2-1})$$

where $\alpha, \delta \geq 0, \quad 0 \leq \beta, \eta \leq \epsilon$ *and*

$$l_2\alpha + (b - l_1 - l_2)\beta = 1 = l_1\delta + (b - l_1 - l_2)\eta.$$

2) *for* $(p;q)$ *of the form*

$$(\gamma,\overbrace{0,\dots,0}^{l_1},\underbrace{\alpha,\dots,\alpha}_{l_2},\overbrace{\beta,\dots,\beta}^{b-l_1-l_2-1};0,\overbrace{\delta,\dots,\delta}^{l_1},\underbrace{0,\dots,0}_{l_2},\overbrace{\eta,\dots,\eta}^{b-l_1-l_2-1})$$

where $\alpha,\beta,\delta,\eta\geq 0,\quad 0\leq\gamma\leq\epsilon$ *and*

$$\gamma+l_2\alpha+(b-l_1-l_2-1)\beta=1=l_1\delta+(b-l_1-l_2-1)\eta.$$

3) *for* $(p;q)$ *of the form*

$$(\gamma,\overbrace{0,\dots,0}^{l_1},\underbrace{\alpha,\dots,\alpha}_{l_2},\overbrace{\beta,\dots,\beta}^{b-l_1-l_2-1};\epsilon,\overbrace{\delta,\dots,\delta}^{l_1},\underbrace{0,\dots,0}_{l_2},\overbrace{\eta,\dots,\eta}^{b-l_1-l_2-1})$$

where $\alpha,\beta,\delta,\eta\geq 0,\quad 0\leq\gamma\leq\epsilon$ *and*

$$\gamma+l_2\alpha+(b-l_1-l_2-1)\beta=1=\epsilon+l_1\delta+(b-l_1-l_2-1)\eta.$$

Moreover, we can assume that the number of zeros that appear in p *and in* q *is either* $b-1$ *or at most* $b-j$.

PROOF. In order to find and upper on the values $\widehat{M}_3$ we need to restrict the function Ψ_j to the pairs (p,q) such that p and q belong to $\widehat{\mathcal{P}}_b^1$ (by symmetry we can fix an arbitrary coordinate). In addition, we relax the domains of p and q by removing the constraints on p_1 and q_1 to be minimum components, i.e., $p,q\in[0,\epsilon]\times[0,1]^{b-1}$.

Using Lemmas 2.2.5, 2.2.6, 2.2.7 and 2.2.8, we see that under this extended domain an upper bound on $\widehat{M}_3$ is attained in a point of the following form:

$$(\gamma,\overbrace{0,\dots,0}^{l_1},\underbrace{\alpha,\dots,\alpha}_{l_2},\overbrace{\beta,\dots,\beta}^{b-l_1-l_2-1};\zeta,\overbrace{\delta,\dots,\delta}^{l_1},\underbrace{0,\dots,0}_{l_2},\overbrace{\eta,\dots,\eta}^{b-l_1-l_2-1})$$

where $\alpha,\beta,\delta,\eta\geq 0,\quad 0\leq\gamma,\zeta\leq\epsilon$ and

$$\gamma+l_2\alpha+(b-l_1-l_2-1)\beta=1=\zeta+l_1\delta+(b-l_1-l_2-1)\eta.$$

Finally, we can split this case into three cases. The first one is when the averages between γ and the β-components and between ζ and the η-components are less than or equal to ϵ, the second one for $0\leq\gamma\leq\epsilon$ and $\zeta=0$, and the third one for $0\leq\gamma\leq\epsilon$ and $\zeta=\epsilon$. By symmetry, the cases in which $\gamma=0$ and $0\leq\zeta\leq\epsilon$ or $\gamma=\epsilon$ and $0\leq\zeta\leq\epsilon$ are included in the second and third cases. □

PROPOSITION 2.2.9. $\widehat{M}_4$ *is upper bounded by the global maximum of* Ψ_j *which is attained in a point* $(p;q)$ *of the following form:*

$$(\overbrace{0,\dots,0}^{l_1},\underbrace{\alpha,\dots,\alpha}_{l_2},\overbrace{\beta,\dots,\beta}^{b-l_1-l_2};\overbrace{\delta,\dots,\delta}^{l_1},\underbrace{0,\dots,0}_{l_2},\overbrace{\eta,\dots,\eta}^{b-l_1-l_2})$$

where $\alpha,\beta,\delta,\eta\geq 0$ *and*

$$l_2\alpha+(b-l_1-l_2)\beta=1=l_1\delta+(b-l_1-l_2)\eta.$$

Moreover, we can assume that the number of zeros that appear in p *and in* q *is either* $b-1$ *or at most* $b-j$.

PROOF. Analogous to the proof of Proposition 2.2.3. □

REMARK 2.2.3. *Each configuration that appears in the list of possible maxima in the previous propositions leads to an optimization problem that depends on at most* 3 *free variables. Therefore, for given* b *and* k*, we can analytically determine, using Mathematica (see [66] for the code used to derive the results in this section), those maxima.*

The previous propositions allow us to determine a finite list of maxima candidates for each $\breve{M}_i$ and $\widehat{M}_i$. We have analytically determined and inspected using Mathematica all the possible maximum points. We have restricted our attention to (b, k)-cases for small b and k in order to avoid excessive computational complexity. It is important to note that for the (b, k)-cases that we have considered (see Propositions 2.2.10 and 2.2.11) the global maximum of Ψ_j, for $j = k - 2$, satisfy the domains of $\breve{M}_2$ and $\widehat{M}_4$. Therefore for these particular cases, we are not upper bounding the values of $\breve{M}_2$ and $\widehat{M}_4$ but, instead, we are computing the exact values. Based on the results of computations, we choose the values of j and ϵ for each (b, k)-case to improve the current best-known bounds on $R_{(b,k)}$. A more careful choice of these parameters could lead to better bounds except for the case $b = k = 6$ (see Remark 2.2.5).

PROPOSITION 2.2.10. *For* $j = k - 2$*, for the values of* ϵ *shown, the* $\breve{M}_i$*'s are as shown in the following table*

(b, k)	ϵ	$\breve{M}_1$	$\breve{M}_2$	$\breve{M}_3$	$\breve{M}_4$
$(7, 7)$	$9/100$	0.085679	0.092593	0.000006	0.000107
$(8, 8)$	$3/25$	0.038453	0.042840	0.000002	0.000022
$(9, 8)$	$1/10$	0.075870	0.076905	0.000001	0.000015
$(10, 9)$	$1/15$	0.036289	0.037935	$3.4 \cdot 10^{-9}$	$8.5 \cdot 10^{-8}$
$(11, 10)$	$1/11$	0.016928	0.018144	$1.4 \cdot 10^{-9}$	$2.7 \cdot 10^{-8}$
$(12, 10)$	$1/20$	0.030945	0.031036	$2.1 \cdot 10^{-11}$	$7.0 \cdot 10^{-9}$
$(13, 11)$	$1/25$	0.015057	0.015473	$7.8 \cdot 10^{-14}$	$3.5 \cdot 10^{-12}$
$(14, 12)$	$1/13$	0.007176	0.007529	$1.2 \cdot 10^{-12}$	$2.6 \cdot 10^{-11}$
$(15, 13)$	$1/12$	0.003360	0.003588	$1.1 \cdot 10^{-13}$	$2.3 \cdot 10^{-12}$

$\breve{M}_1$ *is attained at* $(\frac{1}{b}, \ldots, \frac{1}{b}; \frac{1}{b}, \ldots, \frac{1}{b})$
$\breve{M}_2$ *is attained at* $(1, 0, \ldots, 0; 0, \frac{1}{b-1}, \ldots, \frac{1}{b-1})$
$\breve{M}_3$ *is attained at* $(1 - \epsilon, \frac{\epsilon}{b-1}, \ldots, \frac{\epsilon}{b-1}; 1 - \epsilon, \frac{\epsilon}{b-1}, \ldots, \frac{\epsilon}{b-1})$
$\breve{M}_4$ *is attained at* $(1 - \epsilon, \frac{\epsilon}{b-2}, \ldots, \frac{\epsilon}{b-2}, 0; 0, \frac{\epsilon}{b-2}, \ldots, \frac{\epsilon}{b-2}, 1 - \epsilon)$

PROPOSITION 2.2.11. *For* $j = 3$*,* $(b, k) = (5, 5)$ *and* $\epsilon = \frac{1}{44}(4 + \sqrt{5})$*, the* $\widehat{M}_i$*'s are as shown in the following table*

$\widehat{M}_i$	*Attained at point* $(p; q)$	*Value* $\approx$
$\widehat{M}_1$	$(\epsilon, \frac{1-\epsilon}{b-1}, \ldots, \frac{1-\epsilon}{b-1}; \gamma, \delta, \ldots, \delta), \delta \approx 0.185275$	0.384033
$\widehat{M}_2$	$(0, \frac{1}{b-1}, \ldots, \frac{1}{b-1}; \gamma, \delta, \ldots, \delta), \delta = \epsilon$	0.389226
$\widehat{M}_3$	$(\epsilon, \frac{1-\epsilon}{b-2}, \ldots, \frac{1-\epsilon}{b-2}, 0; \epsilon, \alpha, \ldots, \alpha, \beta), \beta \approx 0.454183$	0.374759
$\widehat{M}_4$	$(0, \frac{1}{b-1}, \ldots, \frac{1}{b-1}; \gamma, \delta, \ldots, \delta), \delta = \epsilon$	0.389226

For $j = 3$*,* $(b, k) = (6, 5)$ *and* $\epsilon = \frac{1}{10}$*, the* $\widehat{M}_i$*'s are as shown in the following table*

$\widehat{M}_i$	*Attained at point* $(p; q)$	*Value* $\approx$
$\widehat{M}_1$	$(\epsilon, \frac{1-\epsilon}{b-1}, \ldots, \frac{1-\epsilon}{b-1}; \gamma, \delta, \ldots, \delta), \delta \approx 0.153159$	0.555625
$\widehat{M}_2$	$(0, \frac{1}{b-1}, \ldots, \frac{1}{b-1}; \gamma, \delta, \ldots, \delta), \delta \approx 0.130217$	0.558467
$\widehat{M}_3$	$(\epsilon, \frac{1-\epsilon}{b-2}, \ldots, \frac{1-\epsilon}{b-2}, 0; \epsilon, \alpha, \ldots, \alpha, \beta), \beta \approx 0.376930$	0.535106
$\widehat{M}_4$	$(0, \frac{1}{b-1}, \ldots, \frac{1}{b-1}; \gamma, \delta, \ldots, \delta), \delta \approx 0.130217$	0.558467

For $j = 4$, $(b, k) = (6, 6)$ and $\epsilon = \frac{1}{20}$, the $\widehat{M}_i$'s are as shown in the following table

$\widehat{M}_i$	*Attained at point* $(p; q)$	*Value* $\approx$
$\widehat{M}_1$	$(\frac{1}{b}, \ldots, \frac{1}{b}; \frac{1}{b}, \ldots, \frac{1}{b})$	0.185185
$\widehat{M}_2$	$(\epsilon, \frac{1-\epsilon}{b-1}, \ldots, \frac{1-\epsilon}{b-1}; \gamma, \delta, \ldots, \delta), \delta \approx 0.147757$	0.178857
$\widehat{M}_3$	$(\epsilon, 0, \frac{1-\epsilon}{b-2}, \ldots, \frac{1-\epsilon}{b-2}; 0, 1, 0, \ldots, 0)$	0.140664
$\widehat{M}_4$	$(1, 0, \ldots, 0; 0, \frac{1}{b-1}, \ldots, \frac{1}{b-1})$	0.192000

REMARK 2.2.4. *The values reported for $\widehat{M}_3$ are not approximate values of the exact values of $\widehat{M}_3$ but upper bounds. We point out that the value $\widehat{M}_1$ for $b = k = 6$ is only attained for uniform distributions. This will be important for a qualitative analysis of our bound on $R_{(b,k)}$ for different values of b and k, see Subsection 2.2.5.*

As a consequence of Propositions 2.2.10, 2.2.11 and equation (24) we are able to evaluate the values of M for both the partitions $\{\check{P}_b^i\}_{i=0,\ldots,b}$ and $\{\widehat{P}_b^i\}_{i=0,\ldots,b}$. Then we state the following theorem

THEOREM 2.2.2. *Using the partition $\{\check{P}_b^i\}_{i=0,\ldots,b}$ we have*

- *for $(b, k) = (7, 7)$ we have that $M \approx 0.0861594$;*
- *for $(b, k) = (8, 8)$ we have that $M \approx 0.0388599$;*
- *for $(b, k) = (9, 8)$ we have that $M \approx 0.0758830$.*
- *for $(b, k) = (10, 9)$ we have that $M \approx 0.0363565$.*
- *for $(b, k) = (11, 10)$ we have that $M \approx 0.0170049$.*
- *for $(b, k) = (12, 10)$ we have that $M \approx 0.0309448$.*
- *for $(b, k) = (13, 11)$ we have that $M \approx 0.0150674$.*
- *for $(b, k) = (14, 12)$ we have that $M \approx 0.0071917$.*
- *for $(b, k) = (15, 13)$ we have that $M \approx 0.0033733$.*

Using the partition $\{\widehat{P}_b^i\}_{i=0,\ldots,b}$ we have

- *for $(b, k) = (5, 5)$ we have that $M \approx 0.3873676$;*
- *for $(b, k) = (6, 5)$ we have that $M \approx 0.5567010$;*
- *for $(b, k) = (6, 6)$ we have that $M = \frac{5}{27} \approx 0.185185$.*

REMARK 2.2.5. *For the underlined (b, k)-cases reported in Table 1, it is interesting to note that the maximum in (10) is only achieved for uniform distributions. This means that, for these particular cases, any new upper bounds that can be found on the quadratic form in equation (17) cannot further improve those bounds. Note that, for $(b, 4)$-cases when $b \geq 4$,*

the maximum of the quadratic form in (17) *is only achieved for uniform distributions if we suppose that the frequency of each symbol in all the coordinates of the code is less than or equal to* $1/2$*. For the special case* $b = k = 6$*, the values we obtained for the* M_i *constants are such that the resulting* η_0 *in the statement of Lemma 2.2.4 is equal to* 1*. That is, the constant* M *is actually* M_1*, which means that in our bound the worst-case scenario is given by the balanced subcodes. The resulting value* $M_1 = 5/27$ *is actually the value attained by* $\Psi_j(p, q)$ *for uniform* p *and* q*. Roughly speaking, this should be interpreted as saying that our procedure is unable to give for* $R_{(6,6)}$ *a bound smaller than* $5/59$ *because such a rate might in principle be achieved if all subcodes have a uniform distribution on each coordinate. However, for such globally balanced codes, one can use a different argument based on the minimum distance of the code to get even stronger upper bounds on* $R_{(b,k)}$*. In the next subsection, we combine the two procedures to deduce a rigorous proof that indeed the bounds shown in Table 1 are not sharp for different values of* b *and* k*.*

2.2.5. A qualitative analysis on $R_{(b,k)}$. In this subsection we show that, at least for the underlined (b, k)-cases in Table 1 and for case $(b, k) = (6, 6)$, the bound in equation (9), for $j = k - 2$ with $\mathbf{M}_{k-2} = \Psi_{k-2}(1/b, \ldots, 1/b;\ 1/b, \ldots, 1/b)$, is not sharp. We also show that, the bound given in equation (6) is not sharp for every $(b, 4)$-cases with $b \geq 5$ and $j = 2$. In this discussion, we use continuity arguments whose quantitative analysis would require long and complicated computations. For this reason, we do not provide explicit numerical improvements on $R_{(b,k)}$ and only show that the bounds on $R_{(b,k)}$ can be improved.

To prove our statement, we invoke an upper bound from [1] on the minimum hamming distance $d_H(C)$ of a b-ary code C with a given rate R. It suffices here to mention that, set $\delta := d_H(C)/n$, this bound is of the form $\delta \leq F(R)$ for a suitable decreasing continuous function F. Due to the monotonicity of F there exists a maximum value of R for which the inequality $R \leq \frac{(b-2)!}{(b-k+1)!b^{k-3}} F(R)$ is satisfied.
Using Mathematica on the specific bound in [1], one finds that

$$R \leq \frac{(b-2)^{\underline{k-3}}}{b^{k-3}} F(R) \implies R < U_{(b,k)}$$

where $(b-2)^{\underline{k-3}} = (b-2)\cdots(b-k+2)$ and $U_{(b,k)}$ takes the values shown in Table 4 for some (b, k) pairs. Note that most of these pairs are actually those underlined in Table 1.

TABLE 4. $U_{(b,k)}$ values

$U_{(6,6)} = 0.08469$	$U_{(7,6)} = 0.13440$	$U_{(8,6)} = 0.18125$	$U_{(9,6)} = 0.22405$
$U_{(10,6)} = 0.26268$	$U_{(11,6)} = 0.29744$	$U_{(12,6)} = 0.32874$	$U_{(13,6)} = 0.35699$
$U_{(14,6)} = 0.38258$	$U_{(8,7)} = 0.07200$	$U_{(9,7)} = 0.10510$	$U_{(10,7)} = 0.13822$
$U_{(11,7)} = 0.17025$	$U_{(12,7)} = 0.20068$	$U_{(13,7)} = 0.22930$	$U_{(14,7)} = 0.25609$
$U_{(10,8)} = 0.05749$	$U_{(11,8)} = 0.08043$	$U_{(12,8)} = 0.10419$	$U_{(13,8)} = 0.12808$
$U_{(14,8)} = 0.15163$	$U_{(11,9)} = 0.03006$	$U_{(12,9)} = 0.04465$	$U_{(13,9)} = 0.06081$
$U_{(14,9)} = 0.07799$	$U_{(13,10)} = 0.02386$	$U_{(14,10)} = 0.03412$	$U_{(14,11)} = 0.01236$

Because of the continuity of F, this implies that there exist $\epsilon_1 > 0$ and $\epsilon_2 > 0$ such that

$$R \leq \left(\frac{(b-2)^{\underline{k-3}}}{b^{k-3}} + \epsilon_1 \right) F(R) + \epsilon_2 \implies R < U_{(b,k)} + 10^{-5}$$

We note that, if $p_1 = p_2 = \cdots = p_b = 1/b$, given $i \neq h \in [1, b]$ and chosen at random $x_1, \ldots, x_{k-4}, z \in [1, b]$ according to the distribution p, the probability that $i, h, x_1, \ldots, x_{k-4}$, z are all different is $(b-2)^{\underline{k-3}}/b^{k-3}$. Therefore, by continuity, there exists $\epsilon_3 > 0$ such that given $i \neq h \in [1, b]$ and chosen at random $x_1, \ldots, x_{k-4}, z \in [1, b]$ according to the distribution p' where $p'_1, p'_2, \ldots, p'_b \in [1/b - \epsilon_3, 1/b + \epsilon_3]$, the probability that $i, h, x_1, \ldots, x_{k-4}, z$ are all different is less than $(b-2)^{\underline{k-3}}/b^{k-3} + \epsilon_1$. Now we divide the coordinates $i \in [1, n]$ into two sets according to whether the distribution f_i has all its values in $[1/b - \epsilon_3, 1/b + \epsilon_3]$ or not. More precisely, we define:

$$U_{\epsilon_3} := \{i \in [1, n] : f_{i,h} \in [1/b - \epsilon_3, 1/b + \epsilon_3],\ \forall h \in [1, b]\}.$$

We can assume, up to reordering the coordinates, that $U_{\epsilon_3} = [1, t]$ for some value t. Here we divide the discussion into two cases, according to the size of t, and we show that in both cases a better bound on $R_{(b,k)}$ can be obtained.

A) Let us assume that $t < n(1 - \epsilon_2)$. As a consequence of Hansel's Lemma, we have the following

$$\begin{aligned} \log(|C|) &\leq (1 + o(1)) \frac{1}{2} \sum_{i \in [\ell+1, n]} \sum_{\omega, \mu \in \Omega} \lambda_\omega \lambda_\mu \Psi_{k-2}(f_{i|\omega}, f_{i|\mu}) \\ &\leq (1 + o(1)) \frac{1}{2} \left[\sum_{i \in [\ell+1, t]} M + \sum_{i \in [t+1, n]} \sum_{\omega, \mu \in \Omega} \lambda_\omega \lambda_\mu \Psi_{k-2}(f_{i|\omega}, f_{i|\mu}) \right] \end{aligned}$$

where M is the upperbound of equation (24) given in Theorem 2.2.2. Due to the following lemma, we are able to provide a better upper bound to the second term of the sum.

LEMMA 2.2.11. *Assume that $f_{i,h} \notin [1/b - \epsilon_3, 1/b + \epsilon_3]$ for some $h \in [1, b]$. Then there exists $M' < M$ such that:*

$$\sum_{\omega, \mu \in \Omega} \lambda_\omega \lambda_\mu \Psi_{k-2}(f_{i|\omega}, f_{i|\mu}) \leq M'.$$

PROOF. Consider first for simplicity the case when $f_{i,h} < 1/b - \epsilon_3$. Let $\Omega' \subseteq \Omega$ be the subset of the ω for which $f_{i,h|\omega} \geq 1/b - \epsilon_3/2$. Then, since

$$f_{i,h} = \sum_{\omega \in \Omega} \lambda_\omega f_{i,h|\omega} \geq \sum_{\omega \in \Omega'} \lambda_\omega f_{i,h|\omega} \geq (1/b - \epsilon_3/2) \sum_{\omega \in \Omega'} \lambda_\omega \,,$$

we deduce that

$$\sum_{\omega \in \Omega'} \lambda_\omega \leq \frac{1/b - \epsilon_3}{1/b - \epsilon_3/2} \,.$$

From Remarks 2.2.1, 2.2.4 and 2.2.5, we know that the maximum of the quadratic form in (17) is only achieved for uniform distributions. This means that $M = \Psi_{k-2}(1/b, \ldots, 1/b; 1/b, \ldots, 1/b)$ for the (b, k)-cases under consideration. Therefore there is some constant $M_{\epsilon_3} < M$ such that if either $f_{i,h|\omega}$ or $f_{i,h|\mu}$ are not Ω', then $\Psi_{k-2}(f_{i|\omega}, f_{i|\mu}) \leq M_{\epsilon_3}$. This implies

$$\sum_{\omega, \mu \in \Omega} \lambda_\omega \lambda_\mu \Psi_{k-2}(f_{i|\omega}, f_{i|\mu}) \leq \left(\frac{1/b - \epsilon_3}{1/b - \epsilon_3/2} \right)^2 M + \left(1 - \left(\frac{1/b - \epsilon_3}{1/b - \epsilon_3/2} \right)^2 \right) M_{\epsilon_3}$$

and hence the statement of the lemma for the case $f_{i,h} < 1/b - \epsilon_3$. A similar proof holds for $f_{i,h} > 1/b + \epsilon_3$. □

In the case $\ell \geq t$, we immediately obtain that $\log(|C|) \leq (n-\ell)\frac{M'}{2}$ which leads to the upperbound $R < \frac{M'}{2+M'}$ that is better than the one shown in Table 1. So we can assume $\ell < t$ and therefore:

$$\log(|C|) \leq (t-\ell)\frac{M}{2} + (n-t)\frac{M'}{2} \leq (n - n\epsilon_2 - \ell)\frac{M}{2} + n\epsilon_2\frac{M'}{2}.$$

Since $\ell = \left\lfloor \frac{nR - 2\log n}{\log(2+\bar{\epsilon})} \right\rfloor = \lfloor nR - 2\log n \rfloor (1 + o(1))$, dividing by n we get:

$$R \leq \frac{1}{2}\left[\frac{M(1-\epsilon_2 - R + 2\frac{\log n}{n})}{1 - R + 2\frac{\log n}{n}} + \frac{M'\epsilon_2}{1 - R + 2\frac{\log n}{n}}\right](1 - R + 2\frac{\log n}{n})(1 + o(1)).$$

Set $M'' = \frac{M(1-\epsilon_2-R)}{1-R} + \frac{M'\epsilon_2}{1-R}$ we have that $M'' < M$ and, taking $n \to \infty$, we obtain:

$$R \leq \frac{M''}{2}(1-R)(1+o(1)).$$

It means that $R < \frac{M''}{2+M''}$ and since $M'' < M$, it follows that the bound is not sharp under the assumption of the case A.

B) Let us assume that $t \geq n(1-\epsilon_2)$. Let us fix two words $u, u' \in C$ at minimum hamming distance and let us choose at random x, y. Because of Hansel Lemma we have that:

$$\log(|C|) \leq \sum_{i=1}^{n} \mathbb{E}[\tau(G_i^{u,u',x_1,\ldots,x_{k-4}})].$$

We recall that $0 \leq \tau(G_i^{u,u',x_1,\ldots,x_{k-4}}) \leq 1$ and, if $u_i \neq u'_i$, $\tau(G_i^{u,u',x_1,\ldots,x_{k-4}})$ is the probability that given $z \notin \{u, u', x_1, \ldots, x_{k-4}\}$ we have that $u_i, u'_i, x_{1i}, x_{(k-4)i}, z_i$ are all different. Since we have chosen at random also $x_1, \ldots, x_{k-4}$, $\mathbb{E}[\tau(G_i^{u,u',x_1,\ldots,x_{k-4}})]$ coincides with the probability that given $x_1, \ldots, x_{k-4}, z \notin \{u, u'\}$ we have that $u_i, u'_i, x_{1i}, x_{(k-4)i}, z_i$ are all different. Therefore $\mathbb{E}[\tau(G_i^{u,u',x_1,\ldots,x_{k-4}})] \leq (b-2)^{\underline{k-3}}/b^{k-3} + \epsilon_1$ for any $i \in [1,t]$ when $u_i \neq u'_i$, otherwise if $u_i = u'_i$ then the expected value is 0. This means that

$$\begin{aligned}\log(|C|) &\leq \left(\frac{(b-2)^{\underline{k-3}}}{b^{k-3}} + \epsilon_1\right)\sum_{i=1}^{t} 1_{u_i \neq u'_i} + \sum_{i=t+1}^{n} 1 \\ &\leq \left(\frac{(b-2)^{\underline{k-3}}}{b^{k-3}} + \epsilon_1\right)\sum_{i=1}^{n} 1_{u_i \neq u'_i} + \sum_{i=n(1-\epsilon_2)}^{n} 1\end{aligned}$$

and hence

$$\log(|C|) \leq \left(\frac{(b-2)^{\underline{k-3}}}{b^{k-3}} + \epsilon_1\right) d_H(u, u') + n\epsilon_2.$$

Dividing by n and remembering that u, u' are at minimal hamming distance, we obtain that:

$$R \leq \left(\frac{(b-2)^{\underline{k-3}}}{b^{k-3}} + \epsilon_1\right)\delta + \epsilon_2 \leq \left(\frac{(b-2)^{\underline{k-3}}}{b^{k-3}} + \epsilon_1\right)F(R) + \epsilon_2.$$

But, because of the definition of ϵ_1 and ϵ_2, this implies that $R < U_{(b,k)} + 10^{-5}$. It can be easily checked that the bound in Theorem 2.2.3 is strictly greater than $U_{(b,k)} + 10^{-5}$ for every (b,k)-cases under consideration and therefore:

THEOREM 2.2.3.

$$R_{(b,k)} < \left(\frac{1}{\log \frac{b}{k-3}} + \frac{b^{k-1}}{b^{\underline{k-1}} \log(b-k+2)} \right)^{-1}$$

for the (b, k)-cases shown in Table 4.

For cases $(b, 4)$ when $b \geq 4$ we know thanks to [12] that the maximum of (16), under the constraint that $f_{i,a} \leq \frac{1}{2}$ for every $i = 1, \ldots, n$ and every $a = 1, \ldots, b$, is only achieved for uniform distributions. Therefore we can use the Plotkin bound instead of the Aaltonen bound in order to prove that bound (6) is not sharp when $k = 4$ and $b \geq 5$.

Let C be a $(b, 4)$-hash code with rate R and suppose that the frequency of the symbols in all the coordinates of C is uniform. Then by Hansel we get

$$R \leq \frac{b-2}{b} \cdot \delta, \tag{32}$$

where $\delta = d_H(C)/n$. The Plotkin bound for q-ary codes with $\delta \leq (b-1)/b$ is the following

$$R \leq \log b \left(1 - \delta \cdot \frac{b}{b-1} \right). \tag{33}$$

Since equation (32) is increasing in δ while (33) is decreasing then we can combine the two bounds to get

$$R \leq \frac{b(b-1)\log b}{(b-1)(b-2) + b^2 \log(b)}. \tag{34}$$

It is easy to see that the bound given in (6) for $k = 4$ is always strictly greater than (34) for every $b > 4$. Then, by a continuity argument (as done previously) one can show that bound (6) for $k = 4$ is not sharp for every $b \geq 5$. Therefore we have the following theorem.

THEOREM 2.2.4. *For every integer $b > 4$*

$$R_{(b,4)} < \left(\frac{1}{\log b} + \frac{b^2}{(b^2 - 3b + 2)\log(b-2)} \right)^{-1}.$$

2.3. A new upper bound on trifferent codes

2.3.1. Preliminaries. Let us recall the definition of k-hash codes from Section 2.1. Let $k \geq 3$ and $n \geq 1$ be integers, and let $\mathcal{C}$ be a subset of $\{0, 1, \ldots, k-1\}^n$ with the property that for any k distinct elements there exists a coordinate in which they all differ. A subset $\mathcal{C}$ with this property is called perfect k-hash code with length n (perfect 3-hash codes are called trifferent codes). The problem of finding upper bounds for the maximum size of perfect k-hash codes is a fundamental problem in theoretical computer science. An elementary double counting argument, as shown in [88], gives the following bound on the cardinality of k-hash codes:

$$|\mathcal{C}| \leq (k-1) \cdot \left(\frac{k}{k-1} \right)^n \text{ for every } k \geq 3\,. \tag{35}$$

In 1984 Fredman and Komlós [100] improved the bound in (35) for every $k \geq 4$ and sufficiently large n, obtaining the following result:

$$|\mathcal{C}| \leq \left(2^{k!/k^{k-1}} \right)^n. \tag{36}$$

Additional refinements of this bound have been progressively achieved over the years. See for example [16, 15, 50] for the case $k = 4$, [42] for the cases $k = 5, 6$, and [88, 80, 67, 68] for $k \geq 5$. For the sake of completeness, we mention that some improvements on the asymptotic probabilistic lower bounds on the maximum size of perfect k-hash codes have been recently obtained in [119] for both small values of k and k sufficiently large.

In contrast, no recent progress has been made to improve the simple bound given in (35) for $k = 3$. This bound has not been outperformed by any algebraic technique, including the recent slice-rank method by Tao [115]. Indeed, Costa and Dalai showed in [41] that the slice-rank method cannot be applied in a *simple way* in order to improve the bound in (35). It is worth to mention that an improvement has been recently obtained in [102], however the authors restrict the codes to be linear, i.e., $\mathcal{C} \subset \mathbb{F}_3^n$ and $\mathcal{C}$ is a subspace of $\mathbb{F}_3^n$.

As a consequence, particular attention is given to the case $k = 3$. Defining $\mathcal{T}(n)$ as the maximum cardinality of trifferent codes with length n, it is easy to verify that $\mathcal{T}(1) = 3$, $\mathcal{T}(2) = 4$ and $\mathcal{T}(3) = 6$. In addition, the authors in [88] showed that the so called *tetra-code* is a trifferent code with length 4 and cardinality 9: this result leads to $\mathcal{T}(4) = 9$. To the best of our knowledge, $\mathcal{T}(n)$ is currently unknown for $n \geq 5$. In this section, we show that $\mathcal{T}(5) = 10$ and $\mathcal{T}(6) = 13$ and we use these results to refine the current best known upper bound on the cardinality of trifferent codes with length $n \geq 5$ (Subsection 2.3.2). The exact value is achieved by implementing an optimized algorithm in GAP which exhibits the non-existence of trifferent codes with lengths 5 and 6 and cardinalities 11 and 14, respectively (the algorithm description is given in Subsection 2.3.3). This section is structured as follows. In Subsection 2.3.2, we provide an improved upper bound on the cardinality of trifferent codes, achieved thanks to a computer testing that shows non-existence of trifferent codes with lengths 5, 6 and cardinalities 11, 13, respectively. In Subsection 2.3.3, the description of the algorithm used to prove the non-existence is reported.

2.3.2. Improved upper bound. The simple recursion used to obtain the bound in (35) for $k = 3$ is:

$$\mathcal{T}(n) \leq \left\lfloor \frac{3}{2} \cdot \mathcal{T}(n-1) \right\rfloor, \tag{37}$$

for every $n \geq 2$, with $\mathcal{T}(1) = 3$. Since $\mathcal{T}(4) = 9$, then $10 \leq \mathcal{T}(5) \leq \left\lfloor \frac{3}{2} \cdot 9 \right\rfloor = 13$. The upper bound is obtained using (37), while the lower bound comes easily from the fact that $\mathcal{T}(n) \geq \mathcal{T}(n-1) + 1$, for every $n \geq 2$. Indeed, when a construction of a trifferent code with length $n - 1$ is known, then it is always possible to trivially add an element of $\{0, 1, 2\}^n$ preserving the trifference property. In Example 2.3.1 we give a construction of a trifferent code with length 5 and cardinality 10 that is built using the tetra-code, see [88] for the definition. The 10 elements of $\{0, 1, 2\}^5$ are represented in columns. For $n = 6$, we have that $13 \leq \mathcal{T}(6) \leq 19$. A trifferent code with length 6 and cardinality 13 is given in Example 2.3.2.

EXAMPLE 2.3.1 ($\mathcal{T}(5) \geq 10$).

$$\left|\begin{array}{cccccccccc} 0 & 0 & 0 & 0 & 1 & 1 & 1 & 2 & 2 & 2 \\ 0 & 0 & 1 & 2 & 0 & 1 & 2 & 0 & 1 & 2 \\ 0 & 0 & 1 & 2 & 2 & 0 & 1 & 1 & 2 & 0 \\ 0 & 0 & 1 & 2 & 1 & 2 & 0 & 2 & 0 & 1 \\ 0 & 1 & 2 & 2 & 2 & 2 & 2 & 2 & 2 & 2 \end{array}\right|$$

EXAMPLE 2.3.2 ($\mathcal{T}(6) \geq 13$).

$$\begin{vmatrix} 0 & 0 & 2 & 2 & 2 & 2 & 2 & 0 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 2 & 2 & 1 & 2 & 2 & 0 & 1 & 1 & 2 & 1 \\ 0 & 1 & 1 & 0 & 2 & 2 & 1 & 2 & 2 & 0 & 1 & 1 & 2 \\ 0 & 1 & 1 & 1 & 0 & 2 & 2 & 2 & 2 & 2 & 0 & 1 & 1 \\ 0 & 1 & 2 & 1 & 1 & 0 & 2 & 2 & 1 & 2 & 2 & 0 & 1 \\ 0 & 1 & 1 & 2 & 1 & 1 & 0 & 2 & 2 & 1 & 2 & 2 & 0 \end{vmatrix}$$

We have designed an algorithm for searching trifferent codes with lengths 5 and 6 and cardinalities 11 and 14, respectively (see Section 2.3.3 for the description of the algorithm). The search ended without returning any trifferent codes, thus proving that $\mathcal{T}(5) \leq 10$ and $\mathcal{T}(6) \leq 13$. Hence, the following theorem holds:

THEOREM 2.3.1. *$\mathcal{T}(5) = 10$ and $\mathcal{T}(6) = 13$.*

This result allows us to focus on the current best known bounds on the maximum cardinality of trifferent codes, which can be expressed as $\mathcal{T}(n) \leq c \cdot (3/2)^n$, where c is a constant and n is sufficiently large. Since finding a better upper bound on the $\limsup_{n\to\infty} \sqrt[n]{\mathcal{T}(n)}$ is a very hard task, it becomes interesting to improve the constant c. The bound shown in (35) gives us $c = 2$, but a better constant can be obtained using (37) and the fact that $\mathcal{T}(4) = 9$, that is $c = 9/(3/2)^4 \approx 1.78$. We are able to improve this constant using Theorem 2.3.1 and (37). These statements directly imply:

COROLLARY 2.3.1.

$$\mathcal{T}(n) \leq \frac{10}{(3/2)^5} \cdot \left(\frac{3}{2}\right)^n \approx 1.32 \cdot \left(\frac{3}{2}\right)^n \quad \textit{for every } n \geq 5,$$
$$\mathcal{T}(n) \leq \frac{13}{(3/2)^6} \cdot \left(\frac{3}{2}\right)^n \approx 1.15 \cdot \left(\frac{3}{2}\right)^n \quad \textit{for every } n \geq 6.$$

Since the floor function is involved in the recursive formula (37), we can improve the constant c by iterating (37) m times starting from a fixed n_0 and a known upper bound on $\mathcal{T}(n_0)$. This results in the following theorem.

THEOREM 2.3.2. *$\mathcal{T}(n) \leq 1.09 \cdot \left(\frac{3}{2}\right)^n$ for every $n \geq 12$.*

PROOF. Fix an integer $n_0 \geq 1$ and consider the following recursive formula that describes a sequence of achievable constants for $\mathcal{T}(n) \leq l(m) \cdot (3/2)^n$ when $n \geq n_0 + m$:

$$l(m) = \left\lfloor l(m-1) \cdot \left(\frac{3}{2}\right)^{n_0+m} \right\rfloor \cdot \left(\frac{3}{2}\right)^{-n_0-m} \quad \textit{for } m \geq 1, \tag{38}$$

where $l(0) = \mathcal{T}(n_0) \cdot (3/2)^{-n_0}$. Taking $n_0 = 6$ and $m = 6$, we obtain the thesis. □

Since the sequence $l(m)$ is non-increasing, we are interested in the $\lim_{m\to\infty} l(m)$. Computing that limit is not trivial, so we use the following recursive relation to obtain a lower bound:

$$d(m) = d(m-1) - \frac{1}{2} \cdot \left(\frac{3}{2}\right)^{-n_0-m} \quad \textit{for } m \geq 1,$$

where $d(0) = \mathcal{T}(n_0) \cdot (3/2)^{-n_0}$. It is easy to see that $l(m) \geq d(m)$ for every $m \geq 0$. Then we have:

$$\lim_{m\to\infty} d(m) = \lim_{m\to\infty} \left(\mathcal{T}(n_0) - \frac{1}{2} \cdot \sum_{i=1}^{m} \left(\frac{2}{3}\right)^i \right) \cdot \left(\frac{3}{2}\right)^{-n_0}$$

$$= (\mathcal{T}(n_0) - 1) \cdot \left(\frac{3}{2}\right)^{-n_0}. \tag{39}$$

REMARK 2.3.1. *Since $\mathcal{T}(4) = 9$, if we fix $n_0 = 4$ then we can substitute them into* (39) *to get that $\lim_{m\to\infty} l(m) \geq \lim_{m\to\infty} d(m) = 8 \cdot (3/2)^{-4} \approx 1.59$. This lower bound is, in any case, greater than the constant that we have found in Corollary 2.3.1.*

2.3.3. An optimized search algorithm. Computing a brute-force search for finding a trifferent code with length n and cardinality M would require to test $\binom{3^n}{M}$ subsets, and for each of them compare $\binom{M}{3}$ triplets: overall, for $(n, M) = (5, 11)$ one would test $\approx 10^{20}$ triplets while for $(n, M) = (6, 14)$ one would test approximately 10^{30} triplets. These numbers are prohibitively large.

Our algorithm dramatically reduces the number of operations, without missing any potential trifferent code. First, we list the elements of $\mathcal{C}_n = \{0, 1, 2\}^n$ in lexicographic order and fix $(i_1, i_2, \ldots, i_M)$ as the indices representing the M elements to test, requiring that $i_1 < i_2 < \ldots < i_M$. Then, let $\mathcal{C}_n^m$ be the code containing the elements associated to the first m indices. Starting from $m = 3$, we check if $\mathcal{C}_n^m$ is trifferent: based on the output, the variable m and the indices are updated accordingly to the pseudocode reported in Algorithm 1.

Algorithm 1 Check if $\mathcal{T}(n) \geq M$.

Require: $(c(1), \ldots, c(3^n)) = \{0, 1, 2\}^n$ ordered lexicographically,
  $(i_1, \ldots, i_M) \leftarrow (1, \ldots, M)$, $m \leftarrow 3$
  repeat
    if $\{c(i_1), \ldots, c(i_m)\}$ **is** trifferent **or** $m < 3$ **then**
      if $m = M$ **then return** True **end if**
      $m \leftarrow m + 1$
    else
      $m' \leftarrow$ **min**$\{m'' : i_{m''} \geq 3^n - M + m''\}$
      if m' **exists then**
        $m \leftarrow m' - 1$, $i_m \leftarrow i_m + 1$
        $i_{t+1} \leftarrow i_t + 1$, *for every* $m \leq t \leq M - 1$
      else
        $i_t \leftarrow i_t + 1$, *for every* $m \leq t \leq M$
      end if
    end if
  until $i_1 \geq 2$
  return False

At each update, $\mathcal{C}_n^m$ is tested: however, only the triplets containing the i_m-th element have to be examined, since all the other triplets have been already verified by construction. This is the first key point of our algorithm.

In addition, we are able to force some restrictions on the set of the indices. Let us first give the following definition.

DEFINITION 2.3.1. *Two codes $C, D \subseteq \mathbb{F}_3^n$ are called* equivalent *if D can be obtained from C by subsequently applying permutations to the coordinate positions and to the symbols $\{0, 1, 2\}$ in each coordinate.*

Given a trifferent code, by symmetry we can find an equivalent code containing the zero vector and a vector of the form $(0, \dots, 0, 1, \dots, 1)$, and not containing nonzero words lexicographically smaller than this vector. To see this, take a nonzero vector in the code that consists of the maximum number of zeros. Now take any column where this vector has a 2, and permute the ones and twos in these columns. Clearly, this new vector is of the form $(0, \dots, 0, 1, \dots, 1)$ and the new equivalent code does not contain any nonzero vector that is lexicographically smaller than this new one. As a consequence, our algorithm stops the search of trifferent codes immediately when $i_1 = 2$, and limits the set of values that the second index can assume, namely, $i_2 \in \{\frac{3^i+1}{2} : i = 1, \dots, n\}$. Furthermore, suppose there exists a trifferent code $\mathcal{C}$ with length n and cardinality M. Let s_0, s_1, s_2 be the number of elements in $\mathcal{C}$ with symbols 0, 1 and 2, respectively, at the first coordinate. It is easy to see that $s_i + s_j \leq \mathcal{T}(n-1)$ for $i \neq j$, so $s_0, s_1, s_2 \geq M - \mathcal{T}(n-1)$. It means that we should have for each symbol 0, 1 and 2 at least $M - \mathcal{T}(n-1)$ elements in $\mathcal{C}$ with that symbol in the first coordinate. As a consequence, recalling that we list the elements of $\mathcal{C}_n$ in lexicographic order, we can force $i_{M-\mathcal{T}(n-1)} \leq 3^{n-1}$ (first coordinate equal to 0), $i_{2(M-\mathcal{T}(n-1))} \leq 2 \cdot 3^{n-1}$ (first coordinate equal to 1), $i_{2\mathcal{T}(n-1)-M+1} > 3^{n-1}$ (first coordinate equal to 1) and finally $i_{\mathcal{T}(n-1)+1} > 2 \cdot 3^{n-1}$ (first coordinate equal to 2). For the sake of readability, the pseudocode reported in Algorithm 1 does not include the restrictions on the set of the indices. However, the code associated to the final version of the algorithm can be found in the Appendix of this section.

We have executed our program for $(n, M) = (5, 11)$ and $(n, M) = (6, 14)$, and no trifferent code has been found. The total number of tested triplets is $\approx 10^7$ for $(n, M) = (5, 11)$ and $\approx 10^{11}$ for $(n, M) = (6, 14)$, thus saving a factor of $\approx 10^{13}$ and $\approx 10^{19}$, respectively, compared to the full brute-force strategy.

As a side note: inspired by a semidefinite programming upper bound for cap sets [75], we could alternatively obtain the upper bound $\mathcal{T}(5) \leq 10$ using the method from [91], in which all extra constraints from Eq. (3) of [91] were included to obtain the bound.

REMARK 2.3.2. *For $(n, M) = (6, 13)$, the search returned a set S of 1046 trifferent codes up to symmetry choices explained above. For any code in S, we generated all equivalent codes and deleted the ones contained in S from S. We had to repeat this 3 times until the set was empty. So there are 3 distinct trifferent (n,M)=(6,13)-codes up to equivalence. These are:*

$$\begin{vmatrix} 0&0&2&2&2&2&2&0&1&1&1&1&1\\ 0&1&0&2&2&2&1&2&0&1&1&1&2\\ 0&1&1&0&2&1&2&2&2&0&1&2&1\\ 0&1&1&1&0&2&2&2&2&2&0&1&1\\ 0&1&1&2&1&0&2&2&2&1&2&0&1\\ 0&1&2&1&1&1&0&2&1&2&2&2&0 \end{vmatrix}, \quad \begin{vmatrix} 0&0&2&2&2&2&2&0&1&1&1&1&1\\ 0&1&0&2&2&2&1&2&2&0&1&1&2&1\\ 0&1&1&0&2&2&1&2&2&2&0&1&1&2\\ 0&1&1&1&0&2&2&2&2&2&0&1&1\\ 0&1&2&1&1&0&2&2&1&2&2&0&1\\ 0&1&1&2&1&1&0&2&2&1&2&2&0 \end{vmatrix}, \quad \begin{vmatrix} 0&0&2&2&2&2&2&0&1&1&1&1&1\\ 0&1&0&2&2&2&1&2&2&0&1&1&2&1\\ 0&1&1&0&2&2&2&2&2&2&0&1&1&1\\ 0&1&1&1&0&2&1&2&2&2&0&1&1&2\\ 0&1&2&1&1&0&2&2&1&2&2&0&1\\ 0&1&1&1&2&1&0&2&2&2&1&2&0 \end{vmatrix}.$$

For each of these codes, in each coordinate position two symbols occur 5 times and one symbol occurs 3 times.

Appendix

We report here the full GAP code used to provide the results shown in the previous section.

```
n := 6; k := 3; M := 14;
possibleDensities := [];
if n = 6 then
    if M = 14 then
        possibleDensities := [[6,4,4], [5,5,4]];
    elif M = 13 then
        possibleDensities := [[7,3,3], [6,4,3], [5,5,3], [5,4,4]];
    fi;
elif n = 5 then
    if M = 10 then
        possibleDensities := [[8,1,1], [7,2,1], [6,3,1], [6,2,2],
                              [5,4,1], [5,3,2], [4,4,2], [4,3,3]];
    elif M = 11 then
        possibleDensities := [[7,2,2], [6,3,2], [5,4,2], [5,3,3], [4,4,3]];
    fi;
elif n = 4 then
    if M = 9 then
        possibleDensities := [[3,3,3]];
    fi;
fi;
symbols := [0..(k-1)];
C:= Tuples(symbols, n);
size := Size(C);
for density in possibleDensities do
    init := [1..density[1]];
    Append(init, [(3^(n-1)+1)..(3^(n-1)+density[2])]);
    Append(init, [(2*3^(n-1)+1)..(2*3^(n-1)+density[3])]);
    finish := [];
    Append(finish, [(3^(n-1)-density[1]+2)..(3^(n-1)+1)]);
    Append(finish, [(2*3^(n-1)-density[2]+2)..(2*3^(n-1)+1)]);
    Append(finish, [(size-density[3]+1)..size]);
    consi2 := 1; m := k;
    repeat
        trifferentSubCode := true;
        for comb in Combinations(init{[1..(m-1)]}, k-1) do
            trifferent := false;
            Append(comb, [init[m]]);
            for j in [1..n] do
                findSymbs := [];
                for i in [1..k] do
                    Append(findSymbs, [Int(C[comb[i]][j])]);
                od;
                if IsEqualSet(findSymbs, symbols) = true then
                    trifferent := true;
                    break;
                fi;
            od;
            trifferentSubCode := trifferentSubCode and trifferent;
            if trifferentSubCode = false then
                break;
```

```
            fi;
        od;
        if trifferentSubCode = true and m >= M then
            break;
        elif trifferentSubCode = true then
            m := m + 1;
        else
            exceed := false;
            for i in [1..M] do
                if init[i] >= finish[i] then
                    if i-1 = 2 then
                        consi2 := consi2 * 3;
                        init[2] := init[2] + consi2;
                    else
                        init[i-1] := init[i-1] + 1;
                    fi;
                    # Here we reset the indexes
                    m := i-1;
                    for j in [i..M] do
                        init[j] := init[j-1] + 1;
                        for l in [1..density[2]] do
                            if init[density[1]+l] < 3^(n-1)+l  then
                                init[density[1]+l] := 3^(n-1)+l;
                            fi;
                        od;
                        for l in [1..density[3]] do
                            if init[M-density[3]+l] < 2*3^(n-1)+l  then
                                init[M-density[3]+l] := 2*3^(n-1)+l;
                            fi;
                        od;
                    od;
                    exceed := true;
                    break;
                fi;
            od;
            if exceed = false then
                init[m] := init[m] + 1;
                for i in [(m+1)..M] do
                    if init[i] = init[i-1] then
                        init[i] := init[i] + 1;
                    fi;
                od;
            fi;
        fi;
    until init[1] >= 2;
od;
```

CHAPTER 3

Codes for multimedia fingerprinting

In this chapter, the results presented in Section 3.2 are obtained in collaboration with Marco Dalai while the results presented in Section 3.3 originate from a work developed at the University of Salerno and are obtained in collaboration with Marco Dalai, Adele A. Rescigno and Ugo Vaccaro.

3.1. Introduction

Separable codes and B_2 codes are combinatorial structures which are used for traitor tracing in broadcast encryption and collusion resistant fingerprints for copyright protection. Separable codes were proposed and applied to identify traitors in an averaging collusion attack in multimedia fingerprint, see [35], [36] and [72]. B_2 codes and 2-separable codes are uniquely decodable in the multiple access communication under the assumption that two accesses use the same codebook, see [49] for new results on separable codes using this general approach.

Separable codes are close related to Frameproof codes that were introduced by Boneh and Shaw [28] in the '90s to protect copyright materials. When a distributor wants to sell copies of a digital product, he chooses t fixed locations in the digital data. For each copy, he associates to each location a q-ary symbol. Such a collection of symbols and locations in each copy is known as a fingerprint, which can be seen as a codeword of length t over an alphabet of size q. The clients do not know the locations and symbols stored in the data, this means they can not remove them. But, instead, some clients can share and compare their copies. In this setting they can recover the locations and the symbols in order to create illegal copies. A set of fingerprints is called to be frameproof if any coalition of at most k clients can not create an illegal copy of the digital data.

One of the main problems in the area of multimedia fingerprinting consist of both providing bounds on the lengths of frameproof codes (this is motivated by the practical consideration that the length of the fingerprint to insert in the digital data represents an obvious overhead that needs to be minimized) *and* computationally efficient procedures to construct frameproof codes of length close to the theoretical optimum. The seminal paper [28] spurred an interesting line of research to investigate the two problems mentioned above. It is impossible here to summarize the many results in the area, and we refer the reader to the papers [19, 24, 34, 37, 79, 106, 110, 111, 112, 113, 117] and references therein quoted for the relevant literature in the area.

In *Section 3.2*, we derive a simple proof, based on information theoretic inequalities, of an upper bound on the largest rates of q-ary $\overline{2}$-separable codes that improves recent results of Wang [118] for any $q \geq 13$. A q-ary code with codewords of length t is a $\overline{k}$-separable code if for any distinct k codewords and m codewords with $1 \leq k, m \leq k$, there exists a coordinate i, $1 \leq i \leq t$, in which the union of the elements of the k codewords differs from the union

This chapter includes research results published in [69].

of the elements of the m codewords. For the case $q = 2$, we recover a result of Lindström [90], but with a much simpler derivation. The method easily extends to give bounds on B_2 codes which, although not improving on Wang's [118] results, use much simpler tools and might be useful for future applications.

In *Section 3.3*, we study upper bounds on the minimum length of frameproof codes introduced by Boneh and Shaw [28] to protect copyrighted materials. A q-ary (k, n)-frameproof code of length t is a $t \times n$ matrix having entries in $\{0, 1, \ldots, q-1\}$ and with the property that for any column $\mathbf{c}$ and any other k columns, there exists a row where the symbols of the k columns are *all* different from the corresponding symbol (in the same row) of the column $\mathbf{c}$. In Section 3.3, we show the existence of q-ary (k, n)-frameproof codes of length $t = O(\frac{k^2}{q} \log n)$ for $q \leq k$, using the Lovász Local Lemma, and of length $t = O(\frac{k}{\log(q/k)} \log(n/k))$ for $q > k$ using the expurgation method. Remarkably, for the practical case of $q \leq k$ our findings give codes whose length almost matches the lower bound $\Omega(\frac{k^2}{q \log k} \log n)$ on the length of *any* q-ary (k, n)-frameproof code and, more importantly, allow us to derive an efficient algorithm of complexity $O(tn^2)$ for the construction of such codes. To the best of our knowledge, this is the first polynomial time, in the code size n, algorithm with such a performance.

3.2. New upper bounds on $\overline{2}$-separable codes and B_2 codes

3.2.1. Preliminaries. Let for notational convenience set $[0, q-1] = \{0, 1, \ldots q-1\}$. We call a q-ary code of length t any subset of $C_t \subseteq [0, q-1]^t$. Let $M = |C_t|$ and write $C_t = \{c_1, c_2, \ldots, c_M\}$. Each c_i is called a codeword and we use the notation $c_i(j)$, for $j = 1, 2, \ldots, t$ for its components. The base-q rate of such a code is defined as $\log_q M/t$. Note that, throughout the section, all logarithms without subscript are to base 2.

We need two definitions.

DEFINITION 3.2.1. *A q-ary code C_t with codewords of length t is a k-frameproof code if for any k codewords and every other codeword, there exists a coordinate i with $1 \leq i \leq t$, in which the symbols of the k codewords do not contain the symbol of the other codeword.*

DEFINITION 3.2.2. *A q-ary code C_t with codewords of length t is a $\overline{k}$-separable code if for any distinct l codewords and m codewords with $1 \leq l, m \leq k$, there exists a coordinate i, $1 \leq i \leq t$, in which the union of the elements of the l codewords differs from the union of the elements of the m codewords.*

Blackburn [24], [25] showed that the rate of k-frameproof codes is upper bounded by $1/k$. Cheng and Miao [36] observed that any k-frameproof code is a $\overline{k}$-separable code and also that any $\overline{k}$-separable code is a $(k-1)$-frameproof code for every $k \geq 2$. This implies that the rate of $\overline{k}$-separable codes is upper bounded by $1/(k-1)$. Interesting results on $\overline{k}$-separable code, with the slightly weaker constraint that only $l = m = k$ is considered in the definition, were recently derived in [49] using an information theoretic approach. With this slightly different definition, an upper bound on the rate of the form $2/k$ was obtained. Since both bounds give the trivial $1/(k-1) = 2/k = 1$ for $k = 2$, other approaches must be adopted for bounding the rate of $\overline{k}$-separable codes, which leads to a rather interesting problem.

A non-trivial bound for q-ary $\overline{2}$-separable codes was derived by Gu, Fan and Miao in [78] and an improvement was recently obtained by Wang [118] for every $3 \leq q \leq 17$ extending a procedure introduced for the binary case by Cohen et al. [38] based on linear programming bounds on codes.

3.2.2. New upper bounds for $\overline{2}$-separable codes. We have the following new bound on the rate of $\overline{2}$-separable codes.

THEOREM 3.2.1. *For integer $q \geq 2$, let C_t be a family of q-ary $\overline{2}$-separable codes. Then*

$$R_s := \limsup_{t\to\infty} \frac{1}{t} \log_q |C_t| \leq \frac{2q-1}{3q-1}\,.$$

This bound improves the one given by Wang [118] when $q \geq 13$. It also improves the bound of Gu et al. [78] for every $q \geq 2$. When $q = 2$, instead, the bound coincides with that of Lindström [90], but with a rather simpler proof.

PROOF OF THEOREM 3.2.1. Let $D = \{(x, y) \in [0, q-1]^2 : x \neq y\} \cup \{0\}$, which implies $|D| = q(q-1)+1$. Define the function $\phi : [0, q-1]^2 \to D$ as

$$\phi(x,y) = \begin{cases} 0, & \text{if } x = y \\ (x,y), & \text{if } x \neq y \end{cases}.$$

For an integer f, we define Φ, the natural extension of ϕ when applied to vectors, that is the function that maps any two vectors $w_1, w_2 \in [0, q-1]^f$ to a vector in D^f according to the rule

$$\Phi(w_1,w_2) = (\phi(w_1(1), w_2(1)), \ldots, \phi(w_1(f), w_2(f))) \in D^f.$$

Let $C_t = \{c_1, c_2, \ldots, c_M\}$ be a q-ary $\overline{2}$-separable code with codewords of length t. We divide each codeword c_i into two sub-blocks, a prefix p_i of length e and a suffix w_i of length f where $t = e + f$. We use here the notation $c_i = (p_i, w_i)$.

Enumerate all the vectors in $[0, q-1]^e$ as $l_1, l_2, \ldots, l_r$, where $r = q^e$, and denote with P_i the set of codewords of C_t which have l_i as the first e components, that is of the form (l_i, w_j). An easy upper bound on M then follows by the Cauchy-Schwarz inequality, namely

$$\frac{M^2}{r} \leq \sum_{i=1}^{r} |P_i|^2. \tag{40}$$

We want a good upper bound on the sum of the ordered pairs in each P_i to get a good upper bound on M. From [78, Theorem 2], we know that the function Φ is injective when we restrict its domain to pairs of suffixes of different vectors taken from the same P_i for all $i = 1, \ldots, r$. Here we provide a short proof. Assume, for the sake of contradiction, there exists four different codewords $(l_h, w_1), (l_h, w_2) \in P_h$, $(l_m, w_3), (l_m, w_4) \in P_m$ such that $\Phi(w_1, w_2) = \Phi(w_3, w_4)$ either when $h = m$ and $(w_1, w_2) \neq (w_3, w_4)$ or when $h \neq m$. For case $h = m$, if $\{w_1, w_2\} \cap \{w_3, w_4\} \neq \emptyset$ then $\Phi(w_1, w_2) = \Phi(w_3, w_4)$ implies a contradiction on the assumption $(w_1, w_2) \neq (w_3, w_4)$. Otherwise, when $\{w_1, w_2\} \cap \{w_3, w_4\} = \emptyset$, the subcodes $C_1 = \{(l_h, w_1), (l_h, w_4)\}$ and $C_2 = \{(l_h, w_2), (l_h, w_3)\}$ do not satisfy the $\overline{2}$-separability property, a contradiction. Instead for case $h \neq m$, $\Phi(w_1, w_2) = \Phi(w_3, w_4)$ implies that the subcodes $C_1 = \{(l_h, w_1), (l_m, w_4)\}$ and $C_2 = \{(l_h, w_2), (l_m, w_3)\}$ do not satisfy the $\overline{2}$-separability property, again a contradiction.

We generalize a smart observation given in [90, eq. (2.9)]. Fix a coordinate ℓ and a subcode P_i in our code C_t, and let $f_0, f_1, \ldots, f_{q-1}$ to be the fractions of symbols that occur in the ℓ-th cooordinate of P_i. Then, when we take all vectors $\Phi(w_j, w_k)$, where w_j and w_k are the suffixes of codewords (not necessarily distinct) that belong to P_i, the frequency of the 0 symbol in the ℓ-th coordinate of these vectors is equal to $f_0^2 + \ldots + f_{q-1}^2$. This summation is always greater than or equal to $1/q$ under the constraint that $\sum_{i=0}^{q-1} f_i = 1$.

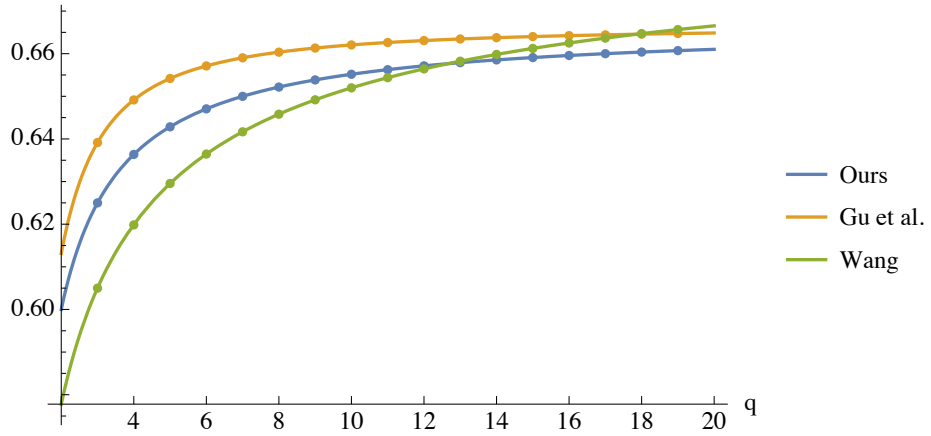


FIGURE 1. Upper bounds on R_s.

So, the fraction of $0'$ in the ℓ-th coordinate of the vectors $\Phi(w_j, w_k)$, where w_j and w_k are suffixes in P_i for each $i = 1, \ldots, r$, is not smaller than $1/q$.

Let $X = (X_1, \ldots, X_f)$ and $Y = (Y_1, \ldots, Y_f)$ be two random variables with joint uniform distributions over the set of ordered pairs of suffixes of vectors taken from the same P_i for each $i = 1, \ldots, r$. Then we have that

$$H(X,Y) = \log\left(\sum_{i=1}^{r} |P_i|^2\right), \tag{41}$$

where H is the Shannon entropy.

We define, for every $i = 1, \ldots, f$, the random variable Z_i by setting $Z_i = \phi(X_i, Y_i)$. Since the function $\Phi(w_1, w_2)$ is injective when $w_1 \neq w_2$ and knowing that $Z = (Z_1, \ldots, Z_f) = \Phi(X, Y)$, then

$$H(X,Y) = H(Z) + \Pr(Z = \underline{0}) \cdot H(X,Y|Z = \underline{0}), \tag{42}$$

where $\underline{0}$ denotes the zero vector.

By the well-known subadditivity property of the entropy function we have

$$H(Z) \leq \sum_{i=1}^{f} H(Z_i) \leq f \left(\max_{\substack{\alpha_0, \ldots, \alpha_{q^2-q} \\ \alpha_0 + \ldots + \alpha_{q^2-q} = 1 \\ \alpha_0 \geq 1/q}} H(\alpha_0, \ldots, \alpha_{q^2-q}) \right) \tag{43}$$

where we abuse the notation using H also for the entropy of a distribution and α_i represents the frequency of the i-th symbol. By the concavity and symmetry of the entropy on its arguments, or using Lagrange multipliers, we find that since $1/q > 1/q^2$ the maximum in (43) is achieved for $\alpha_0 = 1/q$ and $\alpha_1 = \ldots = \alpha_{q^2-q} = 1/q^2$ and takes the following value

$$H(1/q, 1/q^2, \ldots, 1/q^2) = \log q \cdot \frac{2q-1}{q}.$$

By (40) we get

$$\Pr(Z = \underline{0}) = \frac{M}{\sum_{i=1}^{r} |P_i|^2} \leq \frac{r}{M}. \tag{44}$$

The conditional distribution $P(X = w_1, Y = w_2|Z = \underline{0})$ is uniform over its support which has size equal to M. Then

$$H(X, Y|Z = \underline{0}) = \log M. \tag{45}$$

Setting $e = \lfloor \log_q(2M) - \log_q \log M \rfloor$ we have by (44) and (45) that

$$\Pr(Z = \underline{0}) \cdot H(X, Y|Z = \underline{0}) \leq \frac{r}{M} \log M \leq 2. \tag{46}$$

Then by (41), (42), (43) and (46) we have

$$\sum_{i=1}^{r} |P_i|^2 \leq q^{f(2q-1)/q+o(t)} \tag{47}$$

where $o(t)$ is meant as $t \to \infty$.

Finally we are now ready to prove Theorem 3.2.1. By (40) and (47) we have that

$$M^2 \leq q^{f(2q-1)/q+e+o(t)}. \tag{48}$$

Since e is fixed and we know that $t = e + f$, from (48) we get

$$M \leq q^{t\frac{2q-1}{3q-1}+o(t)}$$

and Theorem 3.2.1 follows. □

In Figure 1 we give a comparison between the bounds on the rate of $\overline{2}$-separable codes given in [78], [118] and the one given in Theorem 3.2.1.

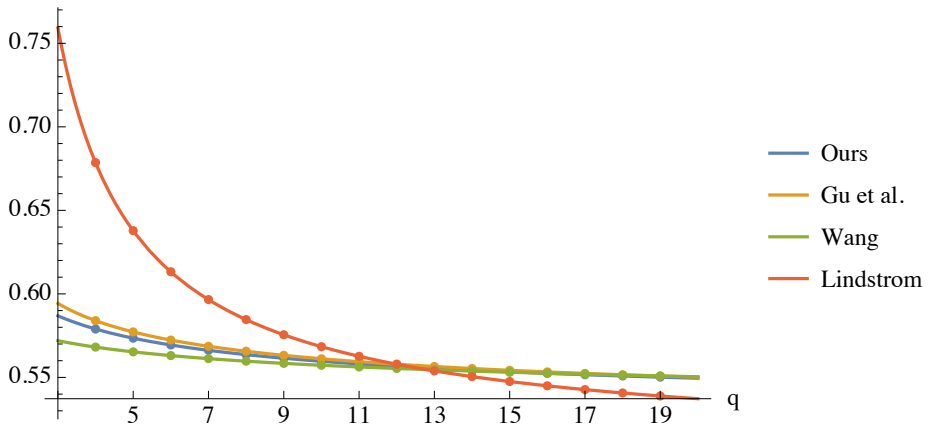


FIGURE 2. Upper bounds on R_b.

3.2.3. Bounds for B_2 codes. The related notion of B_2 codes can be introduced as follows.

DEFINITION 3.2.3. *We say that $C_t = \{c_1, c_2, \ldots, c_M\}$ is a q-ary B_2 code with M codewords of length t and with symbols in the alphabet $[0, q-1]$ if all sums (over the real field) $c_i + c_j$ for $1 \leq i \leq j \leq M$ are different.*

Note that for $q = 2$ this definition is equivalent to the definition of a $\overline{2}$-separable code. Gu et al. in [78] provided non trivial bounds on the rate of q-ary B_2 codes and they also observed that an implicit upper bound can be found in Lindström [90, Theorem 1]. These bounds were improved by Wang [118] for every $2 \leq q \leq 12$.

An immediate extension of the method presented in the previous subsection leads to the following.

THEOREM 3.2.2. *For integer $q \geq 2$, let C_t be a family of q-ary B_2 codes. Then*

$$R_b := \limsup_{t\to\infty} \frac{1}{t} \log_q |C_t| \leq \frac{q + (q-1)\log_q 2}{2q + (q-1)\log_q 2}.$$

For every $3 \leq q \leq 12$ it improves the one given in [78] but not the bound given in [118]. Of course, when $q = 2$, Theorems 3.2.1 and 3.2.2 give the same bound consistently with the fact that any binary $\overline{2}$-separable code is also a B_2 code and vice versa.

PROOF OF THEOREM 3.2.2. In this case, we consider the set $D = \{-q+1, \ldots, -1, 0, 1, \ldots, q-1\}$, so that now $|D| = 2q-1$. For an integer f, we define the function Φ as $\Phi(w_1, w_2) = w_1 - w_2 \in D^f$ where $w_1, w_2 \in [0, q-1]^f$ and the difference is computed in $\mathbb{Z}$.

Let C_t be a q-ary B_2 code and suppose we have constructed the $r = q^e$ subcodes P_i (as done in Theorem 3.2.1). It can be proved, in a similar manner as Theorem 3.2.1, that Φ is injective when we restrict its domain to pairs of suffixes of different vectors taken from the same P_i for all $i = 1, \ldots, r$. Then, the procedure used in Theorem 3.2.1 can be applied to prove Theorem 3.2.2. All the equations from (40) to (48) are verified, also in this case, with the only difference that the cardinality of the set D is $2q-1$ and not $q^2 - q + 1$. □

In Figure 2 we give a comparison between the bounds on the rate of B_2 codes given in [78], [90, Theorem 1], [118] and the one given in Theorem 3.2.2.

3.3. Bounds and algorithms for frameproof codes

3.3.1. Preliminaries. Throughout the section, the logarithms without subscripts are in base two, and we denote with $\ln(\cdot)$ the natural logarithm. Given integers $a < b$, we denote with $[a, b]$ the set $\{a, a+1, \ldots, b\}$. We start by introducing the combinatorial objects we study in this section.

DEFINITION 3.3.1. *Let k, n, $q \geq 2$ be positive integers, $n > k$. A q-ary (k, n)-*frameproof *code is a $t \times n$ matrix M with entries in $[0, q-1]$ such that for any column $\mathbf{c}$ and any other k columns of M we have that, there exists a row $i \in [1, t]$ where the symbols of the k columns are all different from the symbol in the i-th row of the column $\mathbf{c}$. The number of rows t of M is called the length of the q-ary (k, n)-frameproof code.*

In order to provide upper bounds on the minimum length of q-ary (k, n)-frameproof codes we need to recall a strictly related class of codes, named q-ary (k, n)-strongly selective codes, studied in [52] by De Bonis and Vaccaro.

DEFINITION 3.3.2. *Let k, n, and $q \geq 2$ be positive integers, $n \geq k$. A q-ary (k, n)-*strongly selective *code is a $t \times n$ matrix M with entries in $[0, q-1]$ such that for any k-tuple of the columns of M and for any column $\mathbf{c}$ of the given k-tuple, there exists a row $i \in [1, t]$ such that $\mathbf{c}$ has an entry $s \in [1, q-1]$ in row i whereas the entries in row i of all the remaining $k-1$ columns of the k-tuple belong to $[0, q-1] \setminus \{s\}$. The number of rows t of M is called the length of the q-ary (k, n)-strongly selective code.*

Given an integer $q \geq 2$ and a q-ary vector $\mathbf{c} \in [0, q-1]^t$, we denote with $w(\mathbf{c})$ the number of nonzero components of $\mathbf{c}$.

DEFINITION 3.3.3. *A q-ary (k, w, n)-*strongly selective *code is a q-ary (k, n)-strongly selective code with the additional constraint that each column $\mathbf{c}$ has $w(\mathbf{c}) = w$.*

There is a strong relation between q-ary (k,n)-frameproof codes and q-ary $(k+1,n)$-strongly selective codes. In fact, if we denote the minimum length of q-ary (k,n)-frameproof codes by $t_{\mathrm{FP}}(q,k,n)$ and that of q-ary (k,n)-strongly selective codes by $t_{\mathrm{SS}}(q,k,n)$, then the following lemma holds.

LEMMA 3.3.1.

$$t_{SS}(q,k+1,n) \geq t_{FP}(q,k,n) \geq \frac{1}{2} t_{SS}(q,k+1,n)\,.$$

PROOF. The upper bound on $t_{\mathrm{FP}}(q,k,n)$ easily follows by noticing that a q-ary $(k+1,n)$-strongly selective code of length t is a q-ary (k,n)-frameproof code of length t by definition of such codes. Conversely, a q-ary (k,n)-frameproof code $\mathcal{C}$ is not necessarily a q-ary $(k+1,n)$-strongly selective code since we can have a column $\mathbf{c}$ and other k columns in $\mathcal{C}$ where the only rows there exists are those in which the symbols of the k columns do not contain the symbol of the column $\mathbf{c}$ and where this symbol is equal to 0. Therefore, we are satisfying the property for frameproof codes but not the one for strongly selective codes. However, the minimum length $t_{\mathrm{SS}}(q,k+1,n)$ of q-ary $(k+1,n)$-strongly selective codes is at most twice the minimum length $t_{\mathrm{FP}}(q,k,n)$ of q-ary (k,n)-frameproof codes. Indeed, if one is given a q-ary (k,n)-frameproof code $\mathcal{C}$ then one can build a $(k+1,n)$-strongly selective code twice as long as $\mathcal{C}$ by taking the union of the rows of $\mathcal{C}$ and those of the complementary code $\overline{\mathcal{C}}$ obtained by replacing each entry s in $\mathcal{C}$ by $q-1-s$. Hence we obtain the lower bound on $t_{\mathrm{FP}}(q,k,n)$ shown in the statement of the lemma. □

Thanks to Lemma 3.3.1 we can concentrate on finding bounds on the minimum length $t_{\mathrm{SS}}(q,k,n)$ and then obtain, indirectly, bounds on $t_{\mathrm{FP}}(q,k,n)$.

3.3.2. A new randomized algorithm via Lovász Local Lemma. In this section, we provide new upper bounds on the minimum length $t_{\mathrm{SS}}(q,k,n)$ of q-ary (k,n)-strongly selective codes. We will provide two different bounds, one that is derived using the Lovász Local Lemma while the other one using the expurgation method.

In [52], it has been proved the existence of q-ary (k,n)-strongly selective of length

$$t = O\left(\frac{k^2}{v}\log(n/k)\right), \tag{49}$$

where $v = q-1$ for $q \leq k$ and $v = k$ for $q > k$. Their procedure produces a randomized algorithm of complexity $\Theta(n^k)$ to generate q-ary (k,n)-strongly selective codes of length of the same order as the one shown in equation (49). The algorithm is clearly impractical already for small values of k. Here we provide new bounds on $t_{\mathrm{SS}}(q,k,n)$ that are of the same order as the ones provided by [52] but, crucially, this is accompanied with a randomized construction algorithm of complexity $O(tn^2)$. This means that we can construct a q-ary (k,n)-strongly selective codes of length as in (49) in time polynomial in n and k.

The key idea is to use the following matrices (introduced in [85]) where the constraints involve only pairs of columns.

DEFINITION 3.3.4. *Let n, w, λ be positive integers. A q-ary $t \times n$ matrix M, with entries in $[0, q-1]$, is a (λ, w, n)-matrix if the following properties hold true:*
1) each column $\mathbf{c}$ of M has $w(\mathbf{c}) = w$,
2) any pair of columns $\mathbf{c}, \mathbf{d}$ of M have at most λ nonzero symbols in common, that is, there are at most λ rows where columns $\mathbf{c}$ and $\mathbf{d}$ have both the same entry $s \in [1, q-1]$.

These matrices are related to q-ary (k,w,n)-strongly selective codes by the following result.

LEMMA 3.3.2. *If M is a q-ary $t \times n$ (λ, w, n)-matrix with $\lambda = \lfloor (w-1)/(k-1) \rfloor$ then M is a q-ary (k, w, n)-strongly selective code of length t.*

PROOF. Let $\mathbf{c}$ be an arbitrary column of M and let A be the set of row indices in which column $\mathbf{c}$ has nonzero elements. Therefore $|A| = w$. Let K be a set of arbitrary $k-1$ columns of M where $\mathbf{c} \notin K$. Let us denote by $M(A, K)$ the $w \times (k-1)$ submatrix of M constructed by first selecting the $k-1$ columns in K and then selecting the w rows whose indices belong to A. Since M is a (λ, w, n)-matrix we have that the number of nonzero elements that column $\mathbf{c}$ share (in the same rows) with any column in K is at most $\lambda = \left\lfloor \frac{w-1}{k-1} \right\rfloor$. Hence, the total number of nonzero elements in $M(A, K)$ is at most

$$(k-1)\lambda \leq (k-1) \left\lfloor \frac{w-1}{k-1} \right\rfloor \leq w-1 \,.$$

Considering that $M(A, K)$ has $|A| = w$ we have that at least one row in $M(A, K)$ contains only zero elements. Then the lemma follows. □

Now, we want to give a good upper bound on the minimum length of q-ary (λ, w, n)-matrices that will provide us an upper bound on the minimum length of q-ary (k, w, n)-strongly selective codes. We first need to recall the following well-known facts on binomial coefficients:

$$\left(\frac{a}{b}\right)^b \leq \binom{a}{b} \leq \frac{a^b}{b!} \leq \left(\frac{ea}{b}\right)^b , \tag{50}$$

$$\binom{a}{b}\binom{b}{c} = \binom{a}{c}\binom{a-c}{b-c} , \tag{51}$$

and the following useful inequality, proved in [74], for positive integers $c \leq a \leq b$

$$\binom{a}{c} \Big/ \binom{b}{c} \leq \left(\frac{a - \frac{c-1}{2}}{b - \frac{c-1}{2}} \right)^c . \tag{52}$$

Our main tool is the celebrated algorithmic version of the Lovász Local Lemma for the symmetric case as given in [95], see Lemma 2.1.1 for the statement.

We are now ready to state our main lemma.

LEMMA 3.3.3. *There exists a q-ary $t \times n$ (λ, w, n)-matrix with*

$$t = \max \left\{ \lceil 2w - (\lambda+1) \rceil \,, \left\lceil \frac{\lambda}{2} + \frac{1}{q-1} \left(\frac{ew}{\lambda+1} \left(w - \frac{\lambda}{2} \right) (e(2n-4))^{\frac{1}{\lambda+1}} \right) \right\rceil \right\}. \tag{53}$$

PROOF. Let M be a random $t \times n$ q-ary matrix, $t \geq 2w - (\lambda+1)$, where each column $\mathbf{c}$ is picked uniformly at random among the set of all distinct q-ary vectors $\mathbf{c}$ of length t such that $w(\mathbf{c}) = w$. It is easy to see that the number of such vectors is equal to $\binom{t}{w}(q-1)^w$, and therefore

$$\Pr(\mathbf{c}) = \left(\binom{t}{w} (q-1)^w \right)^{-1} .$$

Let $i, j \in [1, n], i \neq j$ and let us consider the event $\overline{E}_{i,j}$ that there exists *at most* λ rows such that both the i-th column and the j-th column of M have the same nonzero symbol in *each* of these rows. We evaluate the probability of the complementary "*bad*" event $E_{i,j}$. Hence $E_{i,j}$ is the event that the i-th and j-th columns $\mathbf{c}_i$ and $\mathbf{c}_j$ have identical non-zero elements

in at least $\lambda+1$ coordinates. We bound $\Pr(E_{i,j})$ by conditioning on the event that $\mathbf{c}_i$ is equal to c.

For a subset $S \subset [1,t]$ of coordinates, let $E^S_{i,j}$ be the event that in each coordinate of S the i-th and j-th column have identical non-zero elements. Finally, let A be the set of coordinates where $\mathbf{c}_i$ is non-zero. Note that for $S \in \binom{A}{\lambda+1}$, i.e. S is a subset of A of size $\lambda+1$, we have

$$\Pr(E^S_{i,j} | \mathbf{c}_i = c) = \frac{\binom{t-(\lambda+1)}{w-(\lambda+1)}(q-1)^{w-(\lambda+1)}}{\binom{t}{w}(q-1)^w}\,.$$

Then

$$\Pr(E_{i,j} | \mathbf{c}_i = c) \le \sum_{S \in \binom{A}{\lambda+1}} \Pr(E^S_{i,j} | \mathbf{c}_i = c) = \binom{w}{\lambda+1} \frac{\binom{t-(\lambda+1)}{w-(\lambda+1)}(q-1)^{w-(\lambda+1)}}{\binom{t}{w}(q-1)^w}. \tag{54}$$

Since the right-hand side of (54) does not depend on the fixed column c, it also holds unconditionally. Hence

$$\Pr(E_{i,j}) \le \binom{w}{\lambda+1} \frac{\binom{t-(\lambda+1)}{w-(\lambda+1)}(q-1)^{w-(\lambda+1)}}{\binom{t}{w}(q-1)^w}. \tag{55}$$

Therefore, by (55) we have

$$\begin{aligned}
\Pr(E_{i,j}) &\le \binom{w}{\lambda+1}\binom{t-(\lambda+1)}{w-(\lambda+1)} \Big/ \binom{t}{w}(q-1)^{\lambda+1} \\
&\overset{(i)}{=} \binom{w}{\lambda+1}\binom{w}{\lambda+1} \Big/ \binom{t}{\lambda+1}(q-1)^{\lambda+1} \\
&\overset{(ii)}{\le} \frac{1}{(q-1)^{\lambda+1}} \binom{w}{\lambda+1} \left(\frac{w-\frac{\lambda}{2}}{t-\frac{\lambda}{2}}\right)^{\lambda+1} \\
&\overset{(iii)}{\le} \frac{1}{(q-1)^{\lambda+1}} \left(\frac{ew}{\lambda+1}\right)^{\lambda+1} \left(\frac{w-\frac{\lambda}{2}}{t-\frac{\lambda}{2}}\right)^{\lambda+1} = P\,,
\end{aligned} \tag{56}$$

where (i) holds due to equality (51), (ii) is true due to inequality (52), and finally (iii) holds thanks to inequalities (50).

The number of events $E_{i,j}$ is equal to $n(n-1)/2$. Let us fix an event $E_{i,j}$, the number of events from which $E_{i,j}$ can be dependent is equal to $D = 2n-4$. Hence, according to Lemma 2.1.1, if P (as defined in (56)) and $D = 2n-4$ satisfy $ePD \le 1$, then the probability that *none* of the "bad" events $E_{i,j}$ occurs is strictly positive. One can see that by setting t as in the second term of the maximum in (53) one indeed obtains

$$ePD = \frac{e(2n-4)}{(q-1)^{\lambda+1}} \left(\frac{ew}{\lambda+1}\right)^{\lambda+1} \left(\frac{w-\frac{\lambda}{2}}{t-\frac{\lambda}{2}}\right)^{\lambda+1} \le 1.$$

Hence, from Lemma 2.1.1 one can construct a q-ary (λ, w, n)-matrix M whose number of rows t satisfies equality (53) since we also need to consider the initial assumption $t \ge 2w-(\lambda+1)$ so that all the computation carried out in this lemma are meaningful. □

Now, thanks to Lemmas 3.3.2 and 3.3.3, we can prove the following result.

THEOREM 3.3.1. *There exists a randomized algorithm to construct a q-ary (k, w, n)-strongly selective code with length*

(57)

$$t \leq 1 + \max\left\{2w - \frac{w-1}{k-1}, \frac{w-1}{2(k-1)} + \frac{ew(k-1)}{(q-1)(w-1)}\left(w - \frac{w-1}{2(k-1)} + \frac{1}{2}\right)(e(2n-4))^{\frac{k-1}{w-1}}\right\}.$$

The algorithm requires, on average, time $O(tn^2)$ to construct the code.

PROOF. The upper bound on t shown in the statement of the lemma is derived by substituting the value of $\lambda = \lfloor (w-1)/(k-1) \rfloor$ of Lemma 3.3.2 into equation (53) of Lemma 3.3.3, and by using the inequalities $\frac{w-1}{k-1} - 1 \leq \left\lfloor \frac{w-1}{k-1} \right\rfloor \leq \frac{w-1}{k-1}$. The time complexity $O(tn^2)$ comes from Lemma 2.1.1 by noticing that $m/D = n(n-1)/(4n-8) \leq n/3$. Moreover, the algorithm that one obtains from [95] requires to randomly generate a matrix, checking if the $\Theta(n^2)$ events $\overline{E}_{i,j}$ are satisfied, and resample *only on non-satisfied* events. This means that we need to check if the i-th column and the j-th column of the matrix have at most $\left\lfloor \frac{w-1}{k-1} \right\rfloor$ nonzero elements in common, that can be done with at most $O(t)$ operations, and resample only over non-satisfied events. Then we need to check only the events that involve columns that have been resampled. Altogether, by Lemma 2.1.1 this procedure requires $O(tn^2 + n \cdot m/D \cdot t) = O(tn^2)$ elementary operations. □

REMARK 3.3.1. *Before optimizing (57) over the parameter w, we would like to stress that Theorem 3.3.1 is not a mere technical intermediate result, but might be important in several practical scenarios. For instance, it has been shown in [52] that q-ary (k, n)-strongly selective codes can be used to solve important communication problems arising in multiple-channel wireless networks. In the scenario considered in [52], one has a set of n uncoordinated stations, attempting transmission over a set of $q-1$ independent channels. Transmission is successful if and only if no two stations attempt to transmit over the same channel at the same time instant. The idea in [52] is the following: Each station is assigned a distinct codeword of a q-ary (k, n)-strongly selective code, and such a codeword corresponds to the transmission schedule of the associated station. The presence of a symbol $s \in [0, q-1]$ in the i-th coordinate of a given codeword $\mathbf{c}$ naturally translates as the "instruction", to the station possessing codeword $\mathbf{c}$, to stay "silent" in the i-th step of the communication protocol if $s = 0$, and to transmit over the j-th channel in the i-th step if $s = j \neq 0$. Under the hypothesis that at any given time at most k stations are "active", the authors of [52] proved that q-ary (k, n)-strongly selective codes naturally correspond to conflict resolution protocols in multiple-channel wireless networks. Now, in many situations, it is important not only to minimize the length of the protocol (i.e., the number of time instants before all stations transmit successfully) but it is important also to restrict the number of attempted transmissions by each station (to save energy, for example, see [74] for more). Therefore q-ary (k, w, n)-strongly selective codes, where each codeword has w non-zero components, could be useful in these instances. We remark that the techniques of [52] are not able to deal with this hard constraint on the number of attempted transmissions by each station, nor suggest efficient algorithms for the construction of q-ary (k, n)-strongly selective codes, as our technique does.*

We optimize w in equation (57) to get a randomized algorithm for (unconstrained) q-ary (k, n)-strongly selective codes.

COROLLARY 3.3.1. *Let $w = \lceil 1 + (k-1)\ln(2en) \rceil$, then the algorithm described in Theorem 3.3.1 constructs a q-ary (k, w, n)-strongly selective code that is, clearly, a q-ary (k, n)-strongly selective code of length t upper bounded as*

$$t \leq \max\left\{ 2(k-1)\ln(2en) - \ln(n), \frac{\ln(n)}{2} + \frac{e^2(k-1)^2}{q-1}\ln(2en) + \frac{7e^2(k-1)}{2(q-1)} \right\} + O(1).$$

PROOF. Fixing w as in the statement of the corollary and using the following inequalities

$$1 + (k-1)\ln(2en) \leq \lceil 1 + (k-1)\ln(2en) \rceil \leq 2 + (k-1)\ln(2en)$$

by Theorem 3.3.1, considering only the second term of the maximum, we have that

$$\begin{aligned} t &\leq 1 + \frac{1 + (k-1)\ln(2en)}{2(k-1)} + \frac{e}{(q-1)\ln(2en)} \\ &\quad (2 + (k-1)\ln(2en)) \left(\frac{3}{2} + (k-1)\ln(2en) \right) (2en)^{\frac{1}{\ln(2en)}} \\ &\leq \frac{\ln(n)}{2} + \frac{e^2(k-1)^2}{q-1}\ln(2en) + \frac{7e^2(k-1)}{2(q-1)} + O(1)\,, \end{aligned}$$

since $k \geq 2$, $\ln(2en) \geq 2$ and $(2en)^{\frac{1}{\ln(2en)}} = e$. Then, the corollary follows since we also need to consider the first term of the maximum of Theorem 3.3.1. □

Therefore due to Lemma 3.3.1 and Corollary 3.3.1 we obtain the main result of this section.

THEOREM 3.3.2. *There exists a randomized algorithm to construct a q-ary (k, n)-frame proof code with length*

$$t \leq \max\left\{ 2k\ln(2en) - \ln(n), \frac{\ln(n)}{2} + \frac{e^2k^2}{q-1}\ln(2en) + \frac{7e^2k}{2(q-1)} \right\} + O(1).$$

The algorithm requires, on average, time $O(tn^2)$ to construct the code.

To properly judge the value of Theorem 3.3.2, we recall the following result that provides a lower bound on the length of any q-ary (k, n)-frameproof code.

THEOREM 3.3.3. *[51, 52, 106] Given positive integers q, k, and n, with $q \geq 2$ and $2 \leq k \leq \sqrt{n}$, the minimum length of any q-ary (k, n)-frameproof code satisfies*

$$t_{FP}(q, k, n) = \Omega\left(\frac{k^2}{q \log k} \log \frac{n}{k} \right). \tag{58}$$

Therefore, one can see that the construction method provided by Theorem 3.3.2, besides being quite efficient, produces codes of almost optimal length.

We can also prove the following result.

THEOREM 3.3.4. *Let M be a q-ary (k, n)-frameproof code of* minimum *length t. Then*

$$\left\lceil \frac{n}{q-1} \right\rceil \geq t \geq \left\lceil \frac{1}{q} \min\left\{ n, \frac{15 + \sqrt{33}}{24} k^2 \right\} \right\rceil. \tag{59}$$

PROOF. We can define a map from M to a binary (k, n)-strongly selective code of length t' by mapping each symbol $i \in [0, q-1]$ into $\mathbf{e}_{i+1}$, where $\mathbf{e}_i$ is the binary column vector that has 1 in the i-th component and 0 elsewhere. Therefore $t' = qt$. Now, the right-hand

side inequality of (59) follows since $t' \geq \min\left\{n, \frac{15+\sqrt{33}}{24}k^2\right\}$ by [105, Theorem 2]. To prove the left-hand side inequality of (59), simply observe that by taking any n columns from the side-by-side concatenation of $(q-1)$ many $\lceil n/(q-1)\rceil \times \lceil n/(q-1)\rceil$ diagonal matrices, where the i-th matrix has symbol $i \in [1, q-1]$ on its diagonal, and 0 elsewhere, one gets a q-ary (k,n)-frameproof code of length $\lceil n/(q-1)\rceil$. □

3.3.3. New improved upper bounds on $t_{\mathbf{FP}}(q,k,n)$ via Expurgation Method. In this Section, we will provide an existential upper bound on the minimum length of q-ary (k,n)-frameproof codes that improves the best results known in the literature. We first recall such known results.

THEOREM 3.3.5. *[113] There exists a q-ary (k,n)-frameproof code of length*

$$t \leq -k \ln\left(n\frac{k!}{k!-1}\right) \Big/ \ln\left(1-\left(1-\frac{1}{q}\right)^k\right).$$

We note that in the original paper [113], this bound is stated in terms of bounds on the length of separating hash families. However, it is well known that a separating hash family of type $(t,n,q,\{1,k\})$ is equivalent to a q-ary (k,n)-frameproof code of length t.

THEOREM 3.3.6. *For k sufficiently large and $q \leq 0.3118 \cdot k(1+o(1))$, where $o(1)$ is meant for $k \to \infty$, the bound given in Theorem 3.3.2 is better than the one of Theorem 3.3.5.*

PROOF. The bound given in Theorem 3.3.5 can be lower bounded as follows

$$\begin{aligned} -(1+o(1))k\ln n \Big/ \ln\left(1-\left(1-\frac{1}{q}\right)^k\right) \geq \\ -(1+o(1))k\ln n \Big/ \ln\left(1-\left(1-e^{-k/q}\right)\right) \geq \\ (1+o(1))\left(e^{k/q}-1\right)k\ln n\,, \end{aligned}$$

since $(1+x) \leq e^x$ and $\ln(1+x) \geq \frac{x}{1+x}$ for all $x > -1$. Then, for $q \leq k$, the bound given in Theorem 3.3.2 can be stated as follows

$$(1+o(1))\frac{e^2k^2}{q-1}\ln(n)\,.$$

Let us take $q = \alpha k(1+o(1))$, where α is a real in $(0,1]$, then we need to study the following inequality to compare the two bounds

$$e^2 \leq \alpha\left(e^{\frac{1}{\alpha}}-1\right).$$

Since the right-hand side of this inequality is a strictly decreasing function in α for $\alpha > 0$, we can compute numerically the range of α for which the inequality is satisfied, that is, $(0, 0.3118]$. □

In [106], the authors provide the following bound that improves the one of Theorem 3.3.5 whenever $q \leq k$ and k is sufficiently large.

THEOREM 3.3.7. *[106] If $q \leq k$, then there exists a q-ary (k,n)-frameproof code of length*

$$t \leq \frac{-k\ln n-(k+1)\ln 2}{\ln\left[1-\left(1-\frac{q-1}{k+1}\right)\left(\frac{q-1}{k+1}\right)^k-\frac{q-1}{k+1}\left(1-\frac{1}{k+1}\right)^k\right]}.$$

Our result employs the so-called expurgation method or deletion method, the same technique of [113], but with a more careful optimization of the parameters. Therefore, we are able to improve the bound of Theorem 3.3.5 for every value of the parameters k, q, and n. Here we state the following theorem.

THEOREM 3.3.8. *There exists a (k,n)-frameproof code of length t, where t is the minimum integer such that the following inequality holds*

$$(k+1)\binom{n\left(1+\frac{1}{k}\right)}{k}(1-p_{q,k})^t \leq 1\,,$$

where

$$p_{q,k} := \begin{cases} \left(1-\frac{1}{q}\right)^k & \text{for } q > k, \\ \left(1-\frac{q-1}{k+1}\right)\left(\frac{q-1}{k+1}\right)^k + \frac{q-1}{k+1}\left(1-\frac{1}{k+1}\right)^k & \text{otherwise.} \end{cases}$$

PROOF. Let M be a q-ary $t \times (n+\ell)$ matrix, where each element is picked i.i.d. at random in the set $[0, q-1]$ with distribution $\mu = (\mu_0, \mu_1, \ldots, \mu_{q-1})$ that will be fixed later. For a given index $i \in [1,n]$ and a set of column-indices B, $|B| = k-1$, $i \notin B$, let $E_{i,B}$ be the event such that for every row in which $\mathbf{c}_i$ (the i-th column) has a symbol s, there exists an index $j \in B$ such that $\mathbf{c}_j$ has symbol s in that same row. Therefore the probability of each event $E_{i,B}$ can be upper bounded as $\Pr(E_{i,B}) \leq \left(1-\sum_{i=0}^{q-1}\mu_i\,(1-\mu_i)^k\right)^t$. The number of such events is equal to $(n+\ell)\binom{n+\ell-1}{k}$. Now, let $X_{i,B}$ be the indicator random variable of the event $E_{i,B}$ and define the random variable $X = \sum_{i,B} X_{i,B}$ that represents the number of events $E_{i,B}$ that are satisfied. Hence, taking $\mu_i = 1/q$ for every $i \in [0, q-1]$ (uniform distribution) when $q > k$ and $\mu_i = 1/(k+1)$ for every $i \in [1, q-1]$, $\mu_0 = 1-(q-1)/(k+1)$ when $q \leq k$, we obtain

$$\mathbb{E}[X] \leq (n+\ell)\binom{n+\ell-1}{k}(1-p_{q,k})^t\,.$$

We note that if $\mathbb{E}[X] < \ell+1$ then there exists at most ℓ "*bad*" events $E_{i,B}$ that are satisfied. Then, for each of these events $E_{i,B}$ we remove one column with index in $\{i\} \cup B$. Hence we are left with a q-ary matrix with t rows and at least n columns that satisfy the frameproof property. Therefore we obtain a (k,n)-frameproof code with length t. Thus the theorem follows taking $\ell = \lfloor n/k \rfloor$. □

COROLLARY 3.3.2. *Using the inequalities in equation* (50)*, we have that, from Theorem 3.3.8, the length of (k,n)-frameproof codes is upper bounded as follows*

$$t \leq \frac{-k\ln\left(n\frac{k+1}{k}\right) - \ln\left(\frac{k+1}{k!}\right)}{\ln\left(1-p_{q,k}\right)}\,,$$

where $p_{q,k}$ is the same quantity defined in Theorem 3.3.8.

THEOREM 3.3.9. *The bound of Corollary 3.3.2 improves the one of Theorem 3.3.5 for every $n \geq k \geq 2$ and $q > k$.*

PROOF. We need to prove the following inequality

$$\frac{-k\ln\left(n\frac{k+1}{k}\right) - \ln\left(\frac{k+1}{k!}\right)}{\ln\left(1-p_{q,k}\right)} < \frac{-k\ln\left(n\frac{k!}{k!-1}\right)}{\ln\left(1-\left(1-\frac{1}{q}\right)^k\right)}\,. \tag{60}$$

Since for $q > k$, $p_{q,k} = (1 - 1/q)^k$, we can rearrange and simplify the terms in (60) to obtain the following equivalent inequality.

$$\left(\frac{k+1}{k}\right)^k \frac{k+1}{k!} < \left(\frac{k!}{k!-1}\right)^k . \tag{61}$$

Now, since $\left(1 + \frac{1}{k}\right)^k \leq e$ and $k! \geq e\left(\frac{k}{e}\right)^k$, we get

$$\left(\frac{k+1}{k}\right)^k \frac{k+1}{k!} \leq \left(\frac{e}{k}\right)^k (k+1) .$$

To prove inequality (61), it suffices to show that

$$\left(\frac{e}{k}\right)^k (k+1) < 1 , \tag{62}$$

since the right-hand side of (61) is greater than 1 for every k.

It can be seen that the left-hand side of (62) is a decreasing function in k for $k \geq 2$. The first integer k for which inequality (62) holds is $k = 5$. Then, the theorem follows since inequality (61) also holds for $k = 2, 3, 4$ by direct computation. □

THEOREM 3.3.10. *The bound of Corollary 3.3.2 improves the one of Theorem 3.3.7 for every $n \geq k \geq 2$ and $q \leq k$.*

PROOF. Clearly, we need to prove the following inequality

$$\frac{-k \ln\left(n\frac{k+1}{k}\right) - \ln\left(\frac{k+1}{k!}\right)}{\ln\left(1 - p_{q,k}\right)} < \frac{-k \ln n - (k+1)\ln 2}{\ln\left[1 - \left(1 - \frac{q-1}{k+1}\right)\left(\frac{q-1}{k+1}\right)^k - \frac{q-1}{k+1}\left(1 - \frac{1}{k+1}\right)^k\right]} . \tag{63}$$

For $q \leq k$, the denominators in (63) are equal by definition of $p_{q,k}$. Therefore, we can rearrange and simplify the terms to obtain the following inequality.

$$\left(\frac{k+1}{k}\right)^k \frac{k+1}{k!} < 2^{k+1} . \tag{64}$$

Proceeding as in the proof of Theorem 3.3.9, the left-hand side of (64) is a decreasing function in k for $k \geq 2$ while the right-hand side of (64) is increasing in k. By inspection, it is easy to see that inequality (64) holds even for $k = 2$. □

CHAPTER 4

Group Testing with runlength constraints

In this chapter, all the results are obtained in collaboration with Marco Dalai and Ugo Vaccaro.

4.1. Introduction

Group Testing refers to the scenario in which one has a population I of individuals, and an unknown subset P of I, commonly referred to as "positives". The goal is to determine the unknown elements of P by performing tests on arbitrary subsets A of I (called *pools*), and the outcome of the test is assumed to return the value 1 (positive) if A contains at least one element of the unknown set P, the value 0 (negative), otherwise. The problem was first introduced by Dorfman [56] during WWII, in the context of mass blood testing. Since then, Group Testing techniques have found applications in a large variety of areas, ranging from DNA sequencing to quality control, data security to network analysis, and much more. We refer the reader to the excellent monographs [57, 5] for an account of the vast literature on the subject.

Group Testing procedures can be adaptive or non-adaptive. In adaptive Group Testing, the tests are performed sequentially, and the content of the pool tested at the generic step i might depend on the previous $i-1$ test outcomes. Conversely, in non-adaptive Group Testing all pools are a-priori set, and tests are carried out in parallel. Non-adaptive Group Testing (NAGT) schemes typically require more tests to discover the positives, but they are faster since tests can be performed in parallel. To combine the advantages of both techniques, while mitigating their limitations, it is sometimes preferable to implement a hybrid approach, where a first screening is performed via a NAGT algorithm, followed by a simple one-by-one testing of the members that are identified in the first stage as potentially positives. This latter approach is usually called Two-Stage Group Testing [29].

In NAGT, the algorithm to determine the positives is usually represented by means of a $t \times n$ binary matrix M, where each row of M represents a test while each column is associated to a distinct member of the population $I = \{1, 2, \ldots, n\}$. More precisely, we have $M_{ij} = 1$ if and only if the member $j \in I$ belongs to the i-th test. In general, one assumes a known upper bound k on the cardinality of the unknown set of positives P. Having said that, the property one usually requires for M to represent a correct (and efficiently decodable) NAGT is the following [57]: for any k-tuple of the n columns of M we demand that for any column $\mathbf{c}$ of the given k-tuple, there exists a row $i \in \{1, \ldots, t\}$ such that $\mathbf{c}$ has symbol 1 in row i and all the remaining $k-1$ columns of the k-tuple have a 0 in the same row i. This condition renders matrices M with such a property equivalent to the well known superimposed codes introduced in the seminal paper by Kautz and Singleton [85] and, independently, by Erdös *et al.* in [64].

This chapter includes research results published in [53].

Motivated by applications in topological DNA-based data storage, the authors of [2] introduced an interesting new variant of NAGT, in which the associated test matrix M has to satisfy additional constraints, in order to comply with the biological constraints of the problem they want to solve. Informally, one of the main problems studied in [2] is to show the existence of a superimposed code M with a "small" number t of rows and satisfying the following additional property: any two 1's in each column are separated by a run of at least d 0's. We refer the reader to [2] for the rationale behind this run-length constraint. The main achievability result obtained in [2] says that codes with these properties exist for $t = \Theta(dk \log(n/k) + k^2 \log(n/k))$.

In *Section 4.2*, we study bounds on the minimum length of (k, n, d)-superimposed codes introduced by Agarwal *et al.* [2], in the context of Non-Adaptive Group Testing algorithms with runlength constraints. A (k, n, d)-superimposed code of length t is a $t \times n$ binary matrix such that any two 1's in each column are separated by a run of at least d 0's, and such that for any column $\mathbf{c}$ and any other $k-1$ columns, there exists a row where $\mathbf{c}$ has 1 and all the remaining $k-1$ columns have 0. Agarwal *et al.* [2] proved the existence of such codes with $t = \Theta(dk \log(n/k) + k^2 \log(n/k))$. Here we investigate more in detail the coefficients in front of these two main terms as well as the role of lower order terms. We show that improvements can be obtained over the construction in [2] by using different constructions and by an appropriate exploitation of the Lovász Local Lemma in this context. Our findings also suggest $O(n^k)$ randomized Las Vegas algorithms for the construction of such codes. We also extend our results to Two-Stage Group Testing algorithms with runlength constraints.

4.2. New lower bounds on (k, n, d)-superimposed codes

4.2.1. Preliminaries. Throughout the section, the logarithms without subscripts are in base two, and we denote with $\ln(\cdot)$ the natural logarithm. For notation convenience we denote with $[a, b]$ the set $\{a, a+1, \ldots, b\}$.

DEFINITION 4.2.1. *[2] Let k, n, d be positive integers, $k \leq n$. A* (k, n, d)-superimposed *code is a $t \times n$ binary matrix M such that any two 1's in each column of M are separated by a run of at least d 0's, and for any k-tuple of the columns of M we have that for any column $\mathbf{c}$ of the given k-tuple, there exists a row $i \in [1, t]$ such that $\mathbf{c}$ has symbol 1 in row i and all the remaining $k-1$ columns of the k-tuple are equal to 0. The number of rows t of M is called the length of the (k, n, d)-superimposed code.*

DEFINITION 4.2.2. *A* (k, n, d, w)-superimposed *code is a (k, n, d)-superimposed with the additional constraint that each column has weight w (number of ones).*

First, we need the following enumerative lemma.

LEMMA 4.2.1. *Let $S \subseteq \{0,1\}^t$ be the set of all distinct binary vectors of length t such that each vector has Hamming weight $w \geq 1$ and any two 1's in each vector are separated by a run of at least d 0's. If $t \geq (w-1)d + w$, then*

$$|S| = \binom{t - (w-1)d}{w}.$$

PROOF. Let A be the set of all distinct binary vectors of length $t - (w-1)d$ and weight w. One can see that $|S| = |A|$ since each element of S can be obtained from an element $a \in A$ by adding between each pair of consecutive ones in a exactly d 0's. Conversely, each element of A can be obtained from an element $s \in S$ by removing between each pair of consecutive ones in s exactly d 0's. □

We also need the following technical lemma and an easy corollary, which have been proved in [74]. We report here the proofs for the reader's convenience.

LEMMA 4.2.2. *Let a, b, c be positive integers such that $c \leq a \leq b$. We have that*

$$\frac{a}{b} \cdot \frac{a-c}{b-c} \leq \left(\frac{a - \frac{c}{2}}{b - \frac{c}{2}} \right)^2 .$$

PROOF. Clearly $a(a-c)c^2 \leq b(b-c)c^2$. Then adding the quantity $4ab(a-c)(b-c)$ to both members implies that $a(a-c)(2b-c)^2 \leq b(b-c)(2a-c)^2$. Therefore Lemma 4.2.2 follows. □

COROLLARY 4.2.1. *Let a, b, c be positive integers such that $c \leq a \leq b$. We have that*

$$\frac{\binom{a}{c}}{\binom{b}{c}} \leq \left(\frac{a - \frac{c-1}{2}}{b - \frac{c-1}{2}} \right)^c . \tag{65}$$

PROOF. Expanding the LHS of (65) we get

$$\frac{\binom{a}{c}}{\binom{b}{c}} = \frac{a}{b} \cdot \frac{a-1}{b-1} \cdots \frac{a-c+1}{b-c+1} . \tag{66}$$

Let us group the terms in (66) into pairs as follows

$$\frac{a-i}{b-i} \cdot \frac{a-(c-i-1)}{b-(c-i-1)} \text{ for } i = 0, \ldots, \left\lceil \frac{c-1}{2} \right\rceil - 1 . \tag{67}$$

If c is odd then we leave alone the term $(a - \frac{c-1}{2})/(b - \frac{c-1}{2})$. By Lemma 4.2.2, each term in (67) can be upper bounded by

$$\frac{a-i}{b-i} \cdot \frac{a-(c-i-1)}{b-(c-i-1)} \leq \left(\frac{a - \frac{c-1}{2}}{b - \frac{c-1}{2}} \right)^2 .$$

Hence Corollary 4.2.1 follows. □

4.2.2. New upper bounds. The main tool to prove Theorem 4.2.1 is the Lovász Local Lemma for the symmetric case, see Lemma 2.1.1 for the statement. We are ready to state our main result.

THEOREM 4.2.1. *There exists a (k, n, d, w)-superimposed code of length t, where t is the minimum integer such that the following inequality holds*

$$ek \left[\binom{n}{k} - \binom{n-k+1}{k} \right] \left(\frac{w(k-1) - \frac{w-1}{2}}{t - (w-1)d - \frac{w-1}{2}} \right)^w \leq 1. \tag{68}$$

PROOF. Let M be a $t \times n$ binary matrix, where each column $\mathbf{c}$ is picked uniformly at random between the set of all distinct binary vectors of length t such that each column has weight w and any two 1's in each column of M are separated by a run of at least d 0's. Therefore by Lemma 4.2.1 we have that

$$\Pr(\mathbf{c}) = \binom{t - (w-1)d}{w}^{-1} .$$

For a given index $i \in [1, n]$ and a set of column-indices B, $|B| = k-1$, $i \notin B$, let $E_{i,B}$ be the event such that for every row in which $\mathbf{c}_i$ (the i-th column) has 1, there exists an index $j \in B$ such that $\mathbf{c}_j$ has 1 in that same row. We can write this event in terms of supports

as $\mathrm{Supp}(\mathbf{c}_i) \subseteq \mathrm{Supp}(\mathbf{c}_B)$. There are $n\binom{n-1}{k-1}$ such events. We can express the probability of such an event as follows

$$\Pr(E_{i,B}) = \sum_{c'=(c'_1,\ldots,c'_{k-1})} \Pr(\mathbf{c}_B = c') \cdot \Pr(\mathrm{Supp}(\mathbf{c}_i) \subseteq \mathrm{Supp}(\mathbf{c}_B) | \mathbf{c}_B = c'), \tag{69}$$

where we have denoted with $\mathbf{c}_B$ the vector $(\mathbf{c}_{j_1}, \ldots, \mathbf{c}_{j_{k-1}})$ in which $j_1, \ldots, j_{k-1}$ are the elements of B. The sum in (69) is over all the possible configurations of $k-1$ vectors of length t, weight w and the distance between ones in each column is at least d. Then, we can upper bound (69) by the maximum of $\Pr(\mathrm{Supp}(\mathbf{c}_i) \subseteq \mathrm{Supp}(\mathbf{c}_B) | \mathbf{c}_B = c')$ over all $k-1$ vectors $c' = (c'_1, \ldots, c'_{k-1})$. Therefore, we can consider the worst-case scenario where the $k-1$ columns of M with indices in B maximize this probability. It can be seen that the maximum is achieved when the $w(k-1)$ ones of the $k-1$ columns indexed by B are placed in $w(k-1)$ different rows. Hence,

$$\Pr(E_{i,B}) \leq \frac{\binom{w(k-1)}{w}}{\binom{t-(w-1)d}{w}} . \tag{70}$$

Using Corollary 4.2.1 we upper bound (70) as follows

$$\Pr(E_{i,B}) \leq \left(\frac{w(k-1) - \frac{w-1}{2}}{t - (w-1)d - \frac{w-1}{2}} \right)^w . \tag{71}$$

Proceeding as in [74], it can be proved that an arbitrary event $E_{i,A}$ is mutually independent from all the events $E_{j,C}$, where $C \subseteq [1,n] \setminus (A \cup \{i\})$ and $j \notin C$. Since the number of events $E_{j,C}$ is equal to

$$\binom{n-k}{k-1}(n-k+1) = k\binom{n-k+1}{k},$$

each event $E_{i,A}$ is dependent of at most

$$D := k\left[\binom{n}{k} - \binom{n-k+1}{k}\right] \tag{72}$$

other events. If the probability that none of the events $E_{i,A}$ occurs is strictly positive then there exists a matrix M that is a (k,n,d,w)-superimposed code of length t. Therefore, using Lemma 2.1.1 and taking P equal to the RHS of (71) and D as defined in equation (72), Theorem 4.2.1 follows. □

Remark 4.2.1. *We note that in Theorem 4.2.1 we could use the union bound instead of the Local Lemma. Since the total number of events is $n\binom{n-1}{k-1}$, we have that there exists a (k,n,d,w)-superimposed code of length t, provided that*

$$n\binom{n-1}{k-1}\left(\frac{w(k-1) - \frac{w-1}{2}}{t - (w-1)d - \frac{w-1}{2}} \right)^w < 1 . \tag{73}$$

In [2] the authors proved that a (k,n,d,w)-superimposed code of length t exists, provided that

$$n\binom{n-1}{k-1}\left(\frac{w(k-1)}{t - (2d+1)(w-1)} \right)^w < 1 . \tag{74}$$

It is clear that our bound given in Remark 4.2.1 is better than the bound given in (74) since

$$\frac{w(k-1)-\frac{w-1}{2}}{t-(w-1)d-\frac{w-1}{2}} \leq \frac{w(k-1)}{t-(2d+1)(w-1)}$$

for all positive integers w, k, d.

If we compare the bounds of Theorem 4.2.1 and Remark 4.2.1 then it has been proved in [74] that

$$ek\left[\binom{n}{k}-\binom{n-k+1}{k}\right] \leq n\binom{n-1}{k-1} \tag{75}$$

for all $k \leq 0.667\sqrt{n}$. Therefore when k is much smaller than n (which is indeed the case in circumstances of interest), the Local Lemma performs better than the union bound. It is important to note that a conjecture of Erdős, Frankl and Füredi [64] says that for $k \geq \sqrt{n}$ optimal superimposed codes have length equal to n. The current best known result has been proved in [105] which states that if $k \geq 1.157\sqrt{n}$ then the minimum length of superimposed codes is equal to n.

COROLLARY 4.2.2. *There exists a (k, n, d, w)-superimposed code of length t, where*

$$t \leq \left\lceil (w-1)d+\frac{w-1}{2}+\left(w(k-1)-\frac{w-1}{2}\right)\cdot \left(\min\left\{n\binom{n-1}{k-1}, ek\left[\binom{n}{k}-\binom{n-k+1}{k}\right]\right\}\right)^{\frac{1}{w}}\right\rceil . \tag{76}$$

PROOF. It easily follows rearranging the terms in equation (68) and in equation (73). □

COROLLARY 4.2.3. *There exists a (k, n, d)-superimposed code of length t with $k \leq n/e$, where*

$$t \leq \ln 2 \cdot dk\log(n/k) + e^2 \cdot k^2\log(n/k) - \frac{\left(3e^2-\ln 2\right)}{2}k\log(n/k) - d + O(1)\,.$$

PROOF. Substitute $w = k\ln(n/k)$ in (76) and upper bound

$$\min\left\{n\binom{n-1}{k-1}, ek\left[\binom{n}{k}-\binom{n-k+1}{k}\right]\right\} < k\left(\frac{en}{k}\right)^k .$$

Therefore we obtain

$$t \leq d\left(k\ln(n/k)-1\right)+\frac{k}{2}\ln(n/k)+e\cdot(ke^k)^{\frac{1}{k\ln(n/k)}}k\left(k-\frac{3}{2}\right)\ln(n/k)+O(1). \tag{77}$$

Hence Corollary 4.2.3 follows since $n \geq ek$ and $k^{1/k} \leq \frac{1}{\ln 2}$ for every integer $k \geq 1$. □

We note that in the explicit bound given in Corollary 4.2.3 the leading coefficient of the term $k\log(n/k)$ can be improved, for $k \leq 0.667\sqrt{n}$, by using a better estimation of the minimum in equation (76) that comes from the use of the Local Lemma.

By exploiting the celebrated result by Moser and Tardos [95], this directly implies a $O(n^k)$ randomized Las Vegas algorithm to construct the codes of Corollary 4.2.3

From the inequality (74) we can derive an explicit upper bound on the length of the codes whose existence was showed in [2] when $w = k\ln(n/k)$ by upper bounding $n\binom{n-1}{k-1}$ with $k\left(\frac{en}{k}\right)^k$. We report here the obtained result.

THEOREM 4.2.2. *[2] There exists a (k, n, d)-superimposed code of length t, where*

$$t \leq 2d\,(k\ln(n/k) - 1) + k\ln(n/k) + e \cdot (ke^k)^{\frac{1}{k\ln(n/k)}} k(k-1)\ln(n/k) + O(1).$$

It is clear that our result given in equation (77) improves the one of Theorem 4.2.2.

REMARK 4.2.2. *We note that it was proved in [2] that every (k, n, d)-superimposed code of length t must satisfy*

$$t \geq \min\left\{n, 1 + (k-1)(d+1)\right\}.$$

This implies that if $k \geq \frac{n-1}{d+1} + 1$ then $t = n$, so we cannot construct a (k, n, d)-superimposed code of length t that is better than the identity matrix of size $n \times n$.

By Remark 4.2.2, it is clear that the constraint $k \leq n/e$ in Corollary 4.2.3 is reasonable since $1 + (k-1)(d+1) \geq ek$ for every $k, d \geq 2$.

We also note that a simple generalization of the method given by Cheng et al. in [37] provide the following result.

THEOREM 4.2.3. *There exists a (k, n, d)-superimposed code of length t, $t \leq \frac{1}{B_k}\,(k\log(n/k) + \log(ke^k))$, where*

$$B_k = \max_{q \geq 2} B_{k,q}\,, \tag{78}$$

$$B_{k,q} = \frac{-\log\left[1 - \left(1 - \frac{1}{q}\right)^{k-1}\right]}{q + d}\,.$$

For $k \to \infty$, the point q that maximize (78) is linear in k.

The proof of Theorem 4.2.3 is similar to the one in [37], we only need to ensure that when we construct a binary matrix M starting from a random q-ary matrix each column $\mathbf{c}$ of M has a run of at least d 0's between any two 1's. This can be done by mapping each q-ary symbol into a binary vector of length $q + d$ where the last d elements are fixed to 0.

If we lower bound B_k with $B_{k,q}$ for the choice $q = \frac{1}{\ln 2}(k-1)$ then, for k sufficiently large, Theorem 4.2.3 gives the following explicit bound on the minimum length t of (k, n, d)-superimposed codes

$$t \leq dk\log(n/k) + \frac{1}{\ln 2} \cdot k(k-1)\log(n/k) + \left(\frac{1}{\ln 2}(k-1) + d\right)\log\left(ke^k\right) + O(1). \tag{79}$$

One can see that this bound already improves, for k sufficiently large, the one given in Theorem 4.2.2 but not the one obtained in Corollary 4.2.3 for $k < d$.

4.2.3. Selectors. Selectors were introduced in [29] and they can be seen as a generalization of superimposed codes. Like superimposed codes, selectors find applications in many circumstances, like Group Testing [29], efficient conflict resolution in the transmission model of [86], etc.. In this subsection, we introduce selectors in which the weight of each column is equal to some fixed value w and where any two 1's in each column of M are separated by a run of at least d 0's, so that they can be applied to the scenario of [2]. Successively, we will show that selectors can be used to construct efficient two-stage procedure for Group Testing with runlength constraints, that require a much smaller number of tests, with respect to the NAGT considered in [2] and in the previous subsection of the present section. Let us start by giving some definitions.

DEFINITION 4.2.3. *Let k, n, d, p be positive integers, $1 \leq p \leq k \leq n$. A (k, n, d, p)-*selector *is a $t \times n$ binary matrix M such that any two 1's in each column of M are separated by a run of at least d 0's, and for any k-tuple of the columns of M we have that at least p rows of the identity matrix of size $k \times k$ are contained in that k-tuple of columns. The number of rows t of M is called the length of the (k, n, d, p)-selector.*

One can see that for $p = k$ we get the definition of (k, n, d)-superimposed codes studied in Subsection 4.2.1.

DEFINITION 4.2.4. *A (k, n, d, p, w)-*selector *is a (k, n, d, p)-selector with the additional constraint that each column has weight w.*

It can be seen (see [74, Lemma 2]) that Definition 4.2.3 is equivalent to requiring that for any k-tuple of columns of a (k, n, d, p)-selector and any $k-p+1$ columns among the selected k-tuple, there exists a row of the identity matrix of size $k \times k$ where the 1 is contained in one of the $k - p + 1$ columns. Therefore, thanks to this equivalence, we can generalize the proof of Theorem 4.2.1 to obtain the following.

THEOREM 4.2.4. *There exists a (k, n, d, p, w)-selector of length t, where t is the minimum integer such that the following inequality holds*

$$e\binom{k}{p-1}\left[\binom{n}{k} - \binom{n-k}{k}\right] \cdot \left(\frac{w(k-1) - \frac{w-1}{2}}{t - (w-1)d - \frac{w-1}{2}}\right)^{w(k-p+1)} \leq 1. \tag{80}$$

PROOF. Let M be a $t \times n$ binary matrix, where each column $\mathbf{c}$ is picked uniformly at random between the set of all distinct binary vectors of length t such that each column has weight w and with distance between ones in each column at least d. As in Theorem 4.2.1, by Lemma 4.2.1 we have that

$$\Pr(\mathbf{c}) = \binom{t - (w-1)d}{w}^{-1}.$$

For a given pair of sets B_1, $B_2 \subseteq [1, n]$ where $|B_1| = k-p+1$, $|B_2| = p-1$ and $B_1 \cap B_2 = \emptyset$, let E_{B_1,B_2} be the event such that for each column $\mathbf{c}_i$ with $i \in B_1$ and every row r where $\mathbf{c}_i(r) = 1$ there exists an index $j \in (B_1 \cup B_2 \setminus \{i\})$ such that $\mathbf{c}_j$ has 1 in that same row r. There are $\binom{k}{p-1}\binom{n}{k}$ such events. Then, by the same argument used in the proof of Theorem 4.2.1 we can easily upper bound the probability of such events as follows

$$\Pr(E_{B_1,B_2}) \leq \left(\frac{\binom{w(k-1)}{w}}{\binom{t-(w-1)d}{w}}\right)^{k-p+1}. \tag{81}$$

Using Corollary 4.2.1 we upper bound (81) as follows

$$\Pr(E_{B_1,B_2}) \leq \left(\frac{w(k-1) - \frac{w-1}{2}}{t - (w-1)d - \frac{w-1}{2}}\right)^{w(k-p+1)}. \tag{82}$$

Let us fix an arbitrary event E_{A_1,A_2} then it is easy to see that it is mutually independent from all the events $E_{A'_1,A'_2}$ such that $A'_1 \subseteq [1, n] \setminus (A_1 \cup A_2)$, $A'_2 \subseteq [1, n] \setminus (A_1 \cup A_2 \cup A'_1)$. The number of events $E_{A'_1,A'_2}$ is equal to $\binom{k}{p-1}\binom{n-k}{k}$. Therefore each event E_{A_1,A_2} is dependent of at most

$$D := \binom{k}{p-1}\left[\binom{n}{k} - \binom{n-k}{k}\right] \tag{83}$$

other events. If the probability that none of the events E_{A_1,A_2} occurs is strictly positive then there exists a matrix M that is a (k,n,d,p,w)-selector of length t. Using Lemma 2.1.1 and taking P equal to the RHS of (82) and D as defined in equation (83), Theorem 4.2.4 follows. □

COROLLARY 4.2.4. *There exists a (k,n,d,p,w)-selector of length t, where*

$$t \leq \left\lceil (w-1)d + \frac{w-1}{2} + \left(w(k-1) - \frac{w-1}{2} \right) \cdot \left(e \binom{k}{p-1} \left[\binom{n}{k} - \binom{n-k}{k} \right] \right)^{\frac{1}{w(k-p+1)}} \right\rceil . \tag{84}$$

PROOF. It follows rearranging the terms in equation (80). □

Again, by exploiting the result by Moser and Tardos [95], we get a $O(n^k)$ randomized Las Vegas algorithm to construct the codes of Corollary 4.2.4

Thanks to Corollary 4.2.4 we obtain the following upper bound on the minimum length of (k,n,d,p)-selectors.

COROLLARY 4.2.5. *There exists a (k,n,d,p)-selector of length t with $k \leq n/e$, where*

$$t \leq \ln 2 \cdot \frac{dk}{k-p+1} \log(n/k) + \ln 2 \cdot e^{3+\frac{1}{e}} \frac{k^2}{k-p+1} \log(n/k) + O(k \log(n/k)) .$$

PROOF. Substituting $w = \frac{k}{k-p+1} \ln(n/k)$ in (84) and using the well-known inequality $\binom{m}{s} \leq \left(\frac{em}{s}\right)^s$, we get

$$t \leq \frac{dk}{k-p+1} \ln(n/k) + e \left[e^{1+\frac{p}{k}} \left(\frac{k}{p-1} \right)^{\frac{p-1}{k}} \right]^{\frac{1}{\ln(n/k)}} \frac{k^2}{k-p+1} \ln(n/k) + O(k \ln(n/k)) .$$

Hence Corollary 4.2.5 follows since $p \leq k$, $n \geq ek$ and since the function $x^{1/x}$ takes its maximum at $x = e$. □

4.2.4. Application of (k,n,d,p)-selectors to two-stage Group Testing. We need the following result, whose proof for "classical" selectors (that is, for selectors without the runlength constraint studied in this subsection) is implicit in the discussion before Theorem 3 of [29]. It is trivial to see that the proof carries out also in the present scenario.

LEMMA 4.2.3. *Let M be a (k,n,d,p)-selector with t rows, and let $\mathbf{f}$ be the $t \times 1$ columns vector obtained by the bitwise OR of at most q, $q \leq p-1$, columns $\mathbf{c}_{i_1}, \ldots, \mathbf{c}_{i_q}$ of M. Then, apart from $\mathbf{c}_{i_1}, \ldots, \mathbf{c}_{i_q}$, there are at most other $k-q-1$ columns of M whose 1's are in a subset of the positions in which the vector $\mathbf{f}$ also has 1's.*

Now we proceed as follows. Let k be an upper bound on the number of possible positives in the Group Testing problem. We perform all the tests corresponding to the rows of a $(2k,n,d,k+1)$-selector M, as explained in the introduction. More precisely, the generic i-th pool T_i, for $i = 1, \ldots, t$, contains all elements $j \in [1,n]$ for which $M_{ij} = 1$. After having performed (in parallel) all tests on pools $T_1, \ldots, T_t$, we get a "sindrome" vector $\mathbf{f}$ (of dimension $t \times 1$) equal to the bitwise OR of the (at most) k columns that correspond to the unknown positive elements. The number of columns of M that are "covered" by $\mathbf{f}$ (that is, that have their 1's in a subset of the positions in which the vector $\mathbf{f}$ also has 1's) is upper

bounded by $2k$ (by Lemma 4.2.3). In other words, there are at most $s \leq 2k$ potentially positive elements, and the true positive are among them. Hence, one can test individually those s elements to discover the true positives. Altogether, we have used $t + 2k$ tests.

By using Corollary 4.2.5 to estimate t, we get that we can discover all the positive elements by performing a number of tests upper bounded by a quantity that is

$$2d \ln(n/k) + O(k \ln(n/k)). \tag{85}$$

The bound (85) shows that our two-stage Group Testing algorithm outperforms both the NAGT algorithm presented in [2] and also our improved one given in the previous subsection of the present section. It is interesting to notice that the bound (85) is information-theoretic optimal, for $d = O(k)$, and that this optimality can be achieved by introducing the least amount of adaptivity in the testing algorithm.

CHAPTER 5

A famous sum-distinct problem by Erdős

In this chapter, all the results are obtained in collaboration with Marco Dalai and Simone Costa.

5.1. Introduction

For any $n \geq 1$, consider sets $\{a_1, ..., a_n\}$ of positive integers with $a_1 < \cdots < a_n$ whose subset sums are all distinct. A famous conjecture, due to Paul Erdős, is that $a_n \geq c \cdot 2^n$ for some constant $c > 0$. Using the variance method, Erdős and Moser [101] (see also [8]) were able to prove that

$$a_n \geq 1/4 \cdot n^{-1/2} \cdot 2^n.$$

No advances have been made so far in removing the term $n^{-1/2}$ from this lower bound, but there have been several improvements on the constant factor, including the works of Dubroff, Fox and Xu [58], Guy [81], Elkies [61], Bae [18], and Aliev [6]. In particular, the best currently known lower bound states that

$$a_n \geq (1 + o(1))\sqrt{\frac{2}{\pi}}\frac{1}{\sqrt{n}}2^n\,.$$

Two simple proofs of this result, first obtained unpublished by Elkies and Gleason, are presented in [58]. In the other direction, the best-known construction is due to Bohman [27], who showed that there exist arbitrarily large such sets with $a_n \leq 0.22002 \cdot 2^n$.

Remark 5.1.1. *In Chapter 3 (Section 3.2), we studied B_2 codes that are subsets of $\{0, \ldots, q-1\}^n$ with the property that all the vector sums over real field between pairs of codewords are different. The notion of B_2 codes was introduced by Sidon for integers in [108]. The problem introduced in this chapter, instead, deal with a distinct-sum problem over the integers with the additional constraint that all the subset-sums have to be different (not only the subsets of cardinality 2).*

5.2. A variation on the Erdős distinct-sums problem

In this section, we propose a generalization of the problem in two directions. One is that the distinct-sums condition is weakened by only requiring that the sums of up to λn elements of the set be distinct, a direction with connections with the recent study independently proposed in [17]. The second is that the integers a_i be replaced by elements in $\mathbb{Z}^k$ for some $k \geq 1$. For these cases we derive both upper and lower bounds on the smallest possible value of the largest component among all of the a_i's, that is on the smallest cube which contains all the a_i elements.

This variation on the problem is inspired by an information-theoretic interpretation, namely in the setting of signaling over a multiple access channel. Looking at the original

This chapter includes research results published in [45] and [44].

problem, we can interpret the a_i integers as pulse amplitudes that n transmitters can transmit over an additive channel to send one bit of information each, for example, to signal to the base station that they want to start a communication session. The requirement that all subset sums be distinct expresses the desire that the base station be able to infer any possible subset of active users. In this setting, a natural assumption to consider is that only a maximum fraction of the users might actually be active at the same time, and that signals be vector-valued rather than scalars since the channel would be used over an interval of time sending a sequence of pulses (codewords) rather than a single pulse.

5.2.1. Preliminaries. More formally, we consider the following problem.

PROBLEM 5.2.1. *Let $\mathcal{F}_{\lambda,n}$ be the family of all subsets of $\{1,\dots,n\}$ whose size is smaller than or equal to λn. We are interested in the minimum M such that there exists a sequence $\Sigma = (a_1,\dots,a_n)$ in $\mathbb{Z}^k$, $a_i \in [0,M]^k$ $\forall i$, (i.e. Σ is M-bounded) such that for all distinct $A_1, A_2 \in \mathcal{F}_{\lambda,n}$, $S(A_1) \neq S(A_2)$, where*

$$S(A) = \sum_{i\in A} a_i\,.$$

In the following, we will call such sequences $\mathcal{F}_{\lambda,n}$-sum distinct.

Throughout the section, the logarithms are in base two and we denote the open interval with endpoints x and y by (x,y) and the closed interval by $[x,y]$.

The section is organized as follows. Subsection 5.2.2 is devoted to lower bounds on the values of M in Problem 5.2.1. We show that for $\lambda \geq 1/2$, both the isoperimetric approach (see [58]) and the variance method can be applied to obtain non-trivial lower bounds. Then, in Subsection 5.2.3, we derive three upper bounds using, respectively, the combinatorial nullstellensatz, the probabilistic method, and a direct construction.

5.2.2. Lower bounds. In this subsection we will derive three different lower bounds on M. Firstly, we provide a very elementary (but still interesting since, for $\lambda < 1/2$ we have no better results) lower bound.

PROPOSITION 5.2.1. *Let $\Sigma = (a_1,\dots,a_n)$ be an $\mathcal{F}_{\lambda,n}$-sum distinct sequence in $\mathbb{Z}^k$ that is M-bounded. Then*

$$M \geq (1+o(1)) \cdot \begin{cases} \frac{1}{\lceil \lambda n\rceil \sqrt[2k]{2\pi n\lambda(1-\lambda)}} 2^{nh(\lambda)/k} & \text{if } \lambda < 1/2; \\ \frac{1}{\lceil \lambda n\rceil} \cdot 2^{(n-1)/k} & \text{if } 1/2 \leq \lambda < 1; \\ \frac{1}{n} \cdot 2^{n/k} & \text{if } \lambda = 1; \end{cases}$$

where $h(\lambda) = -\lambda\log\lambda - (1-\lambda)\log(1-\lambda)$ is the binary entropy function.

PROOF. The maximum possible sum we can get on some coordinates is at most $\lceil \lambda n\rceil M$. Then by the pigeonhole principle, for values of $\lambda \in (0,1/2)$, we have that

$$M^k \geq \frac{1}{\lceil \lambda n\rceil^k} \sum_{i=0}^{\lceil \lambda n\rceil} \binom{n}{i} \geq \frac{1}{\lceil \lambda n\rceil^k \sqrt{2\pi n\lambda(1-\lambda)}} 2^{nh(\lambda)/k}\,.$$

This leads to the asymptotic bound as $n \to \infty$

$$M \geq (1+o(1)) \frac{1}{\lceil \lambda n\rceil \sqrt[2k]{2\pi n\lambda(1-\lambda)}} 2^{nh(\lambda)/k}.$$

For values of $\lambda \in [1/2, 1]$ the lower bound on M can be easily derived noticing that the sum $\sum_{i=0}^{\lceil \lambda n \rceil} \binom{n}{i}$ is greater than or equal to 2^{n-1} for $\lambda \in [1/2, 1)$ and it is equal to 2^n for $\lambda = 1$. Therefore, we have that

$$M \geq (1 + o(1)) \cdot \begin{cases} \frac{1}{\lceil \lambda n \rceil} \cdot 2^{(n-1)/k} & \text{if } 1/2 \leq \lambda < 1; \\ \frac{1}{n} \cdot 2^{n/k} & \text{if } \lambda = 1. \end{cases} \tag{86}$$

□

Now, if $\lambda \geq 1/2$, we see that it is possible to improve on the term $C_n = 1/\lceil \lambda n \rceil$ in (86) using the Harper isoperimetric inequality (see [83]) as done in [58] for $\lambda = 1$. In particular, we see that the same bound obtained for $\lambda = 1$ also holds for all $\lambda > 1/2$. For $\lambda = 1/2$, instead, a weakening by a factor of 2 appears, which can be explained in terms of the concentration of measure around the average value of the sums.

THEOREM 5.2.1. *[Harper vertex-isoperimetric inequality] Let $\mathcal{G}$ be a family of subsets of $[1, n]$ with cardinality $\sum_{i=0}^{k} \binom{n}{i} \leq |\mathcal{G}| \leq 2^{n-1}$ then $|\partial\mathcal{G}| \geq \binom{n}{k+1}$ where $\partial\mathcal{G} = \{F \mid F \in \mathcal{P}([1, n]), \min_{Y \in \mathcal{G}} |F \Delta Y| = 1\}$ is called the border of $\mathcal{G}$.*

Inspired by [58], we obtain the following theorem.

THEOREM 5.2.2. *Let $\Sigma = (a_1, \ldots, a_n)$ be an $\mathcal{F}_{\lambda,n}$-sum distinct sequence in $\mathbb{Z}$ that is M-bounded. Then*

$$M \geq (1 + o(1)) \cdot \begin{cases} \frac{1}{\sqrt{2\pi n}} \cdot 2^n & \text{if } \lambda = 1/2; \\ \sqrt{\frac{2}{\pi n}} \cdot 2^n & \text{if } \lambda \in (1/2, 1]. \end{cases}$$

PROOF. Assume that there exists an $\mathcal{F}_{\lambda,n}$-sum distinct sequence $\Sigma = (a_1, a_2, \ldots, a_n)$ and, without loss of generality, that $a_1 < a_2 < \cdots < a_n$. Let $\mathcal{G}$ be a set of vectors $\epsilon = (\epsilon_1, \ldots, \epsilon_n)$ such that $\epsilon_i \in \{-1/2, 1/2\}$ and the dot product $\epsilon \cdot \Sigma < 0$ $\forall \epsilon \in \mathcal{G}$. Clearly $|\mathcal{G}| = 2^{n-1}$ by symmetry. Then by Theorem 5.2.1 we know that $|\partial\mathcal{G}| \geq \binom{n}{\lceil n/2 \rceil}$. If we take $\eta \in \partial\mathcal{G}$ then $0 < \eta \cdot \Sigma < a_n$. We can express $\partial\mathcal{G} = \partial\mathcal{G}_1 \cup \partial\mathcal{G}_2$ where

$$\partial\mathcal{G}_1 = \{\eta \in \partial\mathcal{G} : \operatorname{supp}(\eta + 1/2) \leq \lfloor \lambda n \rfloor\}$$

and

$$\partial\mathcal{G}_2 = \{\eta \in \partial\mathcal{G} : \operatorname{supp}(\eta + 1/2) \geq \lfloor \lambda n \rfloor + 1\}.$$

If $\lambda \in (1/2, 1]$, then we have that

$$|\partial\mathcal{G}_1| \geq \binom{n}{\lceil n/2 \rceil} - |\partial\mathcal{G}_2|. \tag{87}$$

Because of the definition of $\partial\mathcal{G}_2$

$$|\partial\mathcal{G}_2| \leq \sum_{i=\lfloor \lambda n \rfloor + 1}^{n} \binom{n}{i} \leq 2^{h(\lambda) n}.$$

Since in this case $h(\lambda) < 1$, from (87) we obtain

$$|\partial\mathcal{G}_1| \geq (1 + o(1)) \binom{n}{\lceil n/2 \rceil}.$$

Again, by the pigeonhole principle there exists $\eta_1, \eta_2 \in \partial\mathcal{G}_1$ such that

$$|(\eta_1 - \eta_2) \cdot \Sigma| < a_n / |\partial\mathcal{G}_1| \leq (1 + o(1)) a_n / \binom{n}{\lceil n/2 \rceil}.$$

Finally, by the hypothesis of sum-distinctness we have that $|(\eta_1 - \eta_2) \cdot \Sigma| \geq 1$, and hence

$$a_n > (1 + o(1))\binom{n}{\lceil n/2 \rceil} = (1 + o(1))\sqrt{\frac{2}{\pi n}} \cdot 2^n.$$

For $\lambda = 1/2$ we need a tweak. In this case we see that either $\partial\mathcal{G}_1$ or $\partial\mathcal{G}_2$ is greater than or equal to $(1/2)\binom{n}{\lceil n/2 \rceil}$. Here we note that, since Σ is $\mathcal{F}_{1/2,n}$-sum distinct, it is also $\overline{\mathcal{F}_{1/2,n}}$-sum distinct, where $\overline{\mathcal{F}_{1/2,n}}$ is the complement of $\mathcal{F}_{1/2,n}$ in the power set $\mathcal{P}([1, n])$. Therefore we can assume, without loss of generality, that $\partial\mathcal{G}_1$ is greater than or equal to $(1/2)\binom{n}{\lceil n/2 \rceil}$. Proceeding as in the previous case, here we obtain that

$$a_n > (1/2)\binom{n}{\lceil n/2 \rceil} = (1 + o(1))\frac{1}{\sqrt{2\pi n}} \cdot 2^n.$$

□

REMARK 5.2.1. *A simple extension of Theorem 5.2.2 to the case $k > 1$ leads, for $\lambda > 1/2$, to the bound*

$$M \geq (1 + o(1)) \sqrt[k]{\frac{2}{\pi}} n^{\frac{1}{2k} - 1} 2^{n/k}.$$

Although a more refined reasoning might lead to better results, we did not manage to obtain something which could compete with Theorem 5.2.3 below.

Now we see that, using the variance method (see [8], [101] or [81]), it is possible to improve the bound of Remark 5.2.1 whenever $k > 1$.

THEOREM 5.2.3. *Let $\lambda \geq 1/2$ and let $\Sigma = (a_1, \ldots, a_n)$ be an $\mathcal{F}_{\lambda,n}$-sum distinct sequence in $\mathbb{Z}^k$ that is M-bounded. Then*

$$M \geq (1 + o(1)) \cdot \begin{cases} \sqrt{\frac{4}{\pi n(k+2)}} \cdot \Gamma(k/2 + 1)^{1/k} \cdot 2^{n/k} & \text{if } \lambda = 1; \\ \sqrt{\frac{4}{\pi n(k+2)}} \cdot \Gamma(k/2 + 1)^{1/k} \cdot 2^{(n-1)/k} & \text{if } 1/2 \leq \lambda < 1; \end{cases}$$

where Γ is the gamma function.

PROOF. Let $\Sigma = (a_1, \ldots, a_n)$ be an M-bounded and $\mathcal{F}_{\lambda,n}$-sum distinct sequence in $\mathbb{Z}^k$ where $\lambda \geq 1/2$. Consider a random variable $X = \sum_{i=1}^n \epsilon_i a_i$ where the random vectors $(\epsilon_1, \epsilon_2, \ldots, \epsilon_n)$ are uniformly distributed over the set $\{\epsilon \in \{-1/2, 1/2\}^n : \operatorname{supp}(\epsilon + 1/2) \leq \lambda n\}$. We denote with μ and σ^2 respectively the expected value and the variance of the random variable X.

We know that $\sigma^2 = \mathbb{E}[|X|^2] - |\mathbb{E}[X]|^2 \leq \mathbb{E}[|X|^2]$. Expanding $\mathbb{E}[|X|^2]$ we get

$$\mathbb{E}[|X|^2] = 1/4 \sum_{i=1}^n |a_i|^2 + 2 \sum_{i<j} \mathbb{E}[\epsilon_i \epsilon_j](a_i \cdot a_j), \tag{88}$$

where $\mathbb{E}[\epsilon_i \epsilon_j]$ does not depend on the specific values chosen for i and j. Then for each $i \neq j$ the following inequality holds

$$\begin{aligned} \mathbb{E}[\epsilon_i \epsilon_j] &= 1/4 \cdot \frac{\sum_{i=0}^{\lfloor \lambda n \rfloor} \binom{n-2}{i} + \sum_{i=0}^{\lfloor \lambda n \rfloor - 2} \binom{n-2}{i} - 2 \sum_{i=0}^{\lfloor \lambda n \rfloor - 1} \binom{n-2}{i}}{\sum_{i=0}^{\lfloor \lambda n \rfloor} \binom{n}{i}} \\ &= 1/4 \cdot \frac{\binom{n-2}{\lfloor \lambda n \rfloor} - \binom{n-2}{\lfloor \lambda n \rfloor - 1}}{\sum_{i=0}^{\lfloor \lambda n \rfloor} \binom{n}{i}} \\ &\leq 0\,, \end{aligned} \tag{89}$$

where the inequality holds since $\lambda \geq 1/2$. By (88), (89), since $|a_i|^2 \leq kM^2$, we have that

$$\sigma^2 \leq \mathbb{E}[|X|^2] \leq \frac{knM^2}{4}\,. \tag{90}$$

Now we want to provide a lower bound on σ^2. We know, by the sum-distinctness property of Σ, that each possible value of X, has a probability of happening equal to $1/|\mathcal{F}_{\lambda,n}|$. Therefore, considered the possible outcomes $s_1, s_2, \ldots, s_{|\mathcal{F}_{\lambda,n}|}$ of the random variable X and its mean μ, the variance can be expressed as follows

$$\sigma^2 = \frac{1}{|\mathcal{F}_{\lambda,n}|} \sum_{i=1}^{|\mathcal{F}_{\lambda,n}|} |s_i - \mu|^2.$$

Thus, we can lower bound the variance by the minimum value that the above expression can take for distinct values of the s_i's on a discrete grid when we relax the constraint that μ be their average. For any fixed μ, the sum is minimized when the s_i's are packed as close as possible around μ, that is, if $d = \max_i |s_i - \mu|$, then no point in the grid at a distance $d' < d$ from μ is left unused (otherwise we can move one of the s_i's closer to μ and make the sum smaller). Let R be the radius of a ball of volume $|\mathcal{F}_{\lambda,n}|$, that is,

$$R = \frac{\Gamma(k/2+1)^{1/k}}{\sqrt{\pi}} |\mathcal{F}_{\lambda,n}|^{1/k}. \tag{91}$$

By considering unit-volume non-overlapping cubes around each point in the grid, we deduce that $d \geq R' = R - \sqrt{k}$, so that we have an s_i in any discrete point at distance $d' < R'$ from μ. So, we have

$$\sigma^2 \geq \frac{1}{|\mathcal{F}_{\lambda,n}|} \sum_{|s-\mu|<R'} |s - \mu|^2$$

where s runs over all points in the ball on a discrete grid with spacing 1. If we thus scale everything down by R', renaming $\tilde{s}$ and $\tilde{\mu}$ the scaled quantities, we find

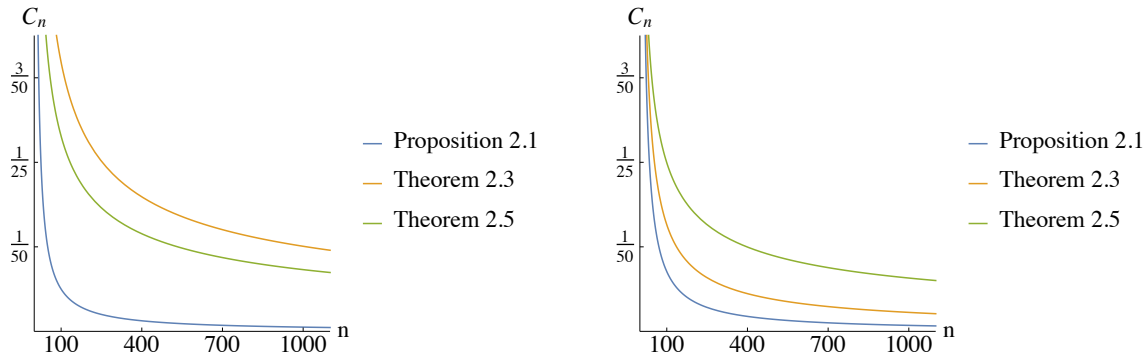
$$\begin{aligned}\sigma^2 &\geq \frac{R'^2}{|\mathcal{F}_{\lambda,n}|} \sum_{|\tilde{s}-\tilde{\mu}|<1} |\tilde{s} - \tilde{\mu}|^2 \\ &= \frac{R'^{2+k}}{|\mathcal{F}_{\lambda,n}|} \sum_{|\tilde{s}-\tilde{\mu}|<1} |\tilde{s} - \tilde{\mu}|^2 \frac{1}{R'^k}\end{aligned}$$

where now $\tilde{s}$ runs over all points in the ball on a discrete grid with spacing $1/R'$. For fixed k, as $n \to \infty$ R' grows to infinity with $R' = (1 + o(1))R$, and the sum in the last expression behaves as a Riemann approximation for an integral over a unit ball. So, asymptotically as $n \to \infty$ we have

$$\sigma^2 \geq (1 + o(1)) \frac{R^{2+k}}{|\mathcal{F}_{\lambda,n}|} \int_{|\tilde{x}-\tilde{\mu}|\leq 1} |\tilde{x} - \tilde{\mu}|^2 \, d\tilde{x}\,.$$

Integrating in polar coordinates, using the $(k-1)$-dimensional volume of the $(k-1)$-dimensional sphere of radius ρ, $S_{k-1}(\rho) = \frac{k\pi^{k/2}}{\Gamma(k/2+1)}\rho^{k-1}$, we obtain

$$\begin{aligned}\sigma^2 &\geq (1 + o(1)) \frac{R^{2+k}}{|\mathcal{F}_{\lambda,n}|} \int_0^1 S_{k-1}(\rho)\rho^2 d\rho \\ &\geq (1 + o(1)) \frac{R^{2+k}}{|\mathcal{F}_{\lambda,n}|} \frac{k\pi^{k/2}}{\Gamma(k/2+1)(k+2)}.\end{aligned}$$



(A) $k = 1$ (B) $k > 1$

FIGURE 1. Representation of the sub-exponential factor C_n of the lower bounds for $1/2 \leq \lambda \leq 1$.

Using (91) and (90) we obtain the thesis. □

5.2.3. Upper bounds. The goal of this subsection is to provide upper bounds on M. We remark that the best known upper bound for the classical Erdős distinct-sums problem (see Bohman [27]) is always (i.e. for any λ) an upper bound on M for the $\mathcal{F}_{\lambda,n}$ distinct-sums problem. Now we will see that this bound can be improved in several situations.

5.2.3.1. *One dimensional Upper Bounds.* In this paragraph, we consider the one dimensional case that is $k = 1$. In this case, we can provide an upper bound by using Alon's combinatorial nullstellensatz. This Theorem has been applied in several Combinatorial Number Theory problems; we refer to [84] (see also [39]) for applications in the similar context of Alspach's partial sums conjecture and to [40] for background on that problem. We report here the theorem for the reader's convenience.

THEOREM 5.2.4. *[7, Theorem 1.2] Let $\mathbb{F}$ be a field and let $f = f(x_1, \ldots, x_k)$ be a polynomial in $\mathbb{F}[x_1, \ldots, x_k]$. Suppose the degree of f is $\sum_{i=1}^{k} t_i$, where each t_i is a nonnegative integer, and suppose the coefficient of $\prod_{i=1}^{k} x_i^{t_i}$ in f is nonzero. Then, if $A_1, \ldots, A_k$ are subsets of $\mathbb{F}$ with $|A_i| > t_i$, there are $a_1 \in A_1, \ldots, a_k \in A_k$ so that $f(a_1, \ldots, a_k) \neq 0$.*

Before providing our upper bound, we need an enumerative lemma. The bound that we will derive is non-trivial, i.e., it is better than the one derived from the powers of two sequence, for $\lambda < \bar{\lambda} \approx 0.113546$, so we assume for simplicity that $\lambda < 1/3$.

We define for convenience

$$f(\lambda) = H(\lambda, \lambda, 1 - 2\lambda),$$

where $H(p_1, \ldots, p_h) = \sum_{i=1}^{h} -p_i \log p_i$ is the Shannon entropy of a probability vector $(p_1, \ldots, p_h)$.

LEMMA 5.2.1. *Let $\mathcal{C}_{\bar{i}}$ be the family of the unodered pairs $\{A_1, A_2\}$ of subsets of $[1, n]$ such that, given an element $\bar{i} \in [1, n]$:*

- *$A_1 \cap A_2 = \emptyset$;*
- *The element $\bar{i}$ belongs to $A_1 \cup A_2$;*

- *The cardinalities of A_1 and A_2 are smaller than or equal to λn.*

Then, for $\lambda < 1/3$, we have the following upper bound on the cardinality of $\mathcal{C}_{\bar{i}}$

$$|\mathcal{C}_{\bar{i}}| < \lambda^3 n^2 \cdot 2^{f(\lambda)n}.$$

PROOF. Suppose, without loss of generality, that $\bar{i} \in A_1$. Then we can upper bound the size of $\mathcal{C}_{\bar{i}}$ as follows

$$|\mathcal{C}_{\bar{i}}| \leq \sum_{i=1}^{\lfloor \lambda n \rfloor} \sum_{j=0}^{\lfloor \lambda n \rfloor} \binom{n-1}{i-1, j, n-i-j}$$

where i represents the cardinality of A_1 while j that of A_2. Using the fact that $\binom{n-1}{i-1,j,n-i-j} \leq \lambda \cdot \binom{n}{i,j,n-i-j}$ for each $i \in [1, \lambda n]$ and $j \in [0, \lambda n]$, we get

$$|\mathcal{C}_{\bar{i}}| < \lambda^3 n^2 \binom{n}{\lfloor \lambda n \rfloor, \lfloor \lambda n \rfloor, n - 2\lfloor \lambda n \rfloor},$$

since the multinomial coefficient is maximized when all numbers are as equal as possibile. Then, by a well-known entropy bound on the multinomial coefficient (see [47, Lemma 2.2]) we have that

$$|\mathcal{C}_{\bar{i}}| < \lambda^3 n^2 \cdot 2^{nH(\frac{\lfloor \lambda n \rfloor}{n}, \frac{\lfloor \lambda n \rfloor}{n}, 1 - 2\frac{\lfloor \lambda n \rfloor}{n})} \leq \lambda^3 n^2 \cdot 2^{nH(\lambda, \lambda, 1-2\lambda)}$$

where the last inequality holds because, for $\lambda < 1/3$, $f(\lambda)$ is an increasing function. □

We are now ready to state our bound.

THEOREM 5.2.5. *For any $\lambda < 1/3$, there exists a sequence $\Sigma = (a_1, \ldots, a_n)$ of $(\lambda^3 n^2 2^{f(\lambda)n})$-bounded positive integers that is $\mathcal{F}_{\lambda,n}$-sum distinct.*

PROOF. For any pair $(A_1, A_2) \in \mathcal{F}^2_{\lambda,n}$, we define the linear polynomial

$$l_{A_1,A_2}(x_1, \ldots, x_n) := \sum_{i \in A_1} x_i - \sum_{j \in A_2} x_j.$$

Now, let us denote by $\mathcal{P}_{\lambda,n}$ the family of the pairs (A_1, A_2) of elements of $\mathcal{F}_{\lambda,n}$ such that $A_1 \cap A_2 = \emptyset$ and $\min(A_1) < \min(A_2)$. Then we set

$$q_{\mathcal{F}_{\lambda,n}}(x_1, \ldots, x_n) := \prod_{(A_1,A_2) \in \mathcal{P}_{\lambda,n}} l_{A_1,A_2}(x_1, \ldots, x_n).$$

We note that, for any pair $(A'_1, A'_2) \in \mathcal{F}^2_{\lambda,n}$ such that $A'_1 \neq A'_2$, the linear polynomial $l_{A'_1,A'_2}(x_1, \ldots, x_n)$ is equal to $\pm l_{A_1,A_2}(x_1, \ldots, x_n)$ for some $(A_1, A_2) \in \mathcal{P}_{\lambda,n}$. Therefore $\Sigma = (a_1, \ldots, a_n)$ is $\mathcal{F}_{\lambda,n}$-sum distinct if and only if $q_{\mathcal{F}_{\lambda,n}}(a_1, \ldots, a_n) \neq 0$.

Since $\mathbb{Z}[x_1, \ldots, x_n]$ is an integral domain, $q_{\mathcal{F}_{\lambda,n}}$ is not constantly zero. Therefore there exist $t_1, \ldots, t_n$, where each t_i is a nonnegative integer, such that the coefficient of $\prod_{i=1}^{n} x_i^{t_i}$ in $q_{\mathcal{F}_{\lambda,n}}$ is nonzero. Since $q_{\mathcal{F}_{\lambda,n}}$ is homogeneous, we also have that its degree is $\sum_{i=1}^{n} t_i$. Let us consider $\bar{i}$ such that $t_{\bar{i}} = \max_i t_i$. The term $x_{\bar{i}}^{t_{\bar{i}}}$ originates from the factor $r_{\bar{i}}$ of $q_{\mathcal{F}_{\lambda,n}}$ defined by the product

$$r_{\bar{i}}(x_1, \ldots, x_n) := \prod_{(A_1,A_2) \in \mathcal{P}_{\lambda,n} :\ \bar{i} \in A_1 \cup A_2} l_{A_1,A_2}(x_1, \ldots, x_n).$$

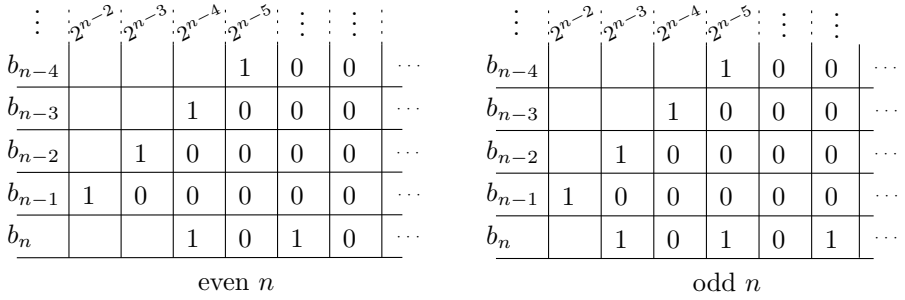


FIGURE 2. Binary representation of the b_n integers used in Lemma 5.2.2.

Hence, because of Lemma 5.2.1, we have that $t_{\bar{i}} < \lambda^3 n^2 \cdot 2^{f(\lambda)n}$. This means that the hypotheses of Theorem 5.2.4 are satisfied whenever $M \geq \lambda^3 n^2 \cdot 2^{f(\lambda)n} > \max_i t_i$ and hence, under this constraint, there exist $a_1 \in [1, M], \ldots, a_n \in [1, M]$ such that $q_{\mathcal{F}_{\lambda,n}}(a_1, \ldots, a_n) \neq 0$. □

We recall that the result of Theorem 5.2.5 is non-trivial only when $\lambda < \bar{\lambda} \approx 0.113546$. Now, we investigate the range $\lambda \in [\bar{\lambda}, 1/4)$.

5.2.3.2. *Direct constructions.* Here we provide a direct construction that improves the constant of Bohman [27] bound.

LEMMA 5.2.2. *Let us consider the sequence* $\widetilde{\Sigma}_n = (b_1, \ldots, b_n)$ *where*

$$b_i := \begin{cases} 2^{i-1} & i = 1, 2 \ldots n-1 \\ \sum_{j=0}^{j<n/2-1} 2^{2j} & i = n; \end{cases}$$

Then, given two subsets A_1, A_2 *of* $[1, n]$ *such that* $|A_1| + |A_2| < n/2$,

$$S(A_1) = \sum_{i \in A_1} b_i \neq \sum_{j \in A_2} b_j = S(A_2).$$

The structure of the set $\widetilde{\Sigma}_n$ is better understood by writing a table of the binary representations of the integers b_n, as shown in Figure 2.

PROOF. Let us suppose, by contradiction, that there exist n, A_1 and A_2 with $|A_1| + |A_2| < n/2$ such that $S(A_1) = S(A_2)$, and let us consider the smallest n for which this holds.

We note that if two sets A_1 and A_2 have the same sum, then also $A_1 \setminus (A_1 \cap A_2)$ and $A_2 \setminus (A_1 \cap A_2)$ have the same sum. Therefore we may also assume that A_1 and A_2 are disjoint. Since a simple check shows that the thesis is true for $n \leq 5$, n must be bigger than 5. Moreover, since $\widetilde{\Sigma}_n \setminus \{b_n\}$ is clearly sum-distinct, we can assume without loss of generality that $n \in A_1$. Therefore we have

$$b_n + \sum_{i \in A_1 \setminus \{n\}} b_i = \sum_{j \in A_2} b_j.$$

which can be rewritten as

$$\sum_{i=0}^{i<n/2-1} 2^{2i} + \sum_{i \in A_1 \setminus \{n\}} 2^{i-1} = \sum_{j \in A_2} 2^{j-1}. \tag{92}$$

Now we divide the proof in two cases, according to whether n is even or n is odd. The binary representations shown in Figure 2 might be useful as a complement in some steps of the discussion.

Consider the case of even n. First observe that in this case equation (92) can rewritten by replacing n with $n-1$ in the upper extreme of the first summation, that is,

$$\sum_{i=0}^{i<(n-1)/2-1} 2^{2i} + \sum_{i\in A_1\setminus\{n\}} 2^{i-1} = \sum_{j\in A_2} 2^{j-1}. \tag{93}$$

We now claim that $n-1 \in A_2$. Indeed, if $n-1$ is neither in A_1 nor in A_2, we see that equation (93) provides a counterexample which is already contained in $\widetilde{\Sigma}_{n-1}$. Formally, the sets $A_1' = A_1 \setminus \{n\} \cup \{n-1\}$ and $A_2' = A_2$ give a counterexample for $\widetilde{\Sigma}_{n-1}$ satisfying $|A_1'| + |A_2'| = |A_1| + |A_2| < (n-1)/2$, because $|A_1| + |A_2| < n/2$ with even n. This contradicts the minimality of n. It is easy to see that $n-1 \in A_1$ is impossible, since we would have $S(A_2) \leq b_1 + \ldots + b_{n-2} < b_{n-1}$. This implies that $n-1 \in A_2$. As a consequence, $n-2$ must be in A_1, for otherwise we would have $S(A_1) \leq b_n + b_1 + b_2 + \ldots + b_{n-3} < 2(b_1 + b_2 + \ldots + b_{n-3}) < b_{n-1} \leq S(A_2)$. So A_1 contains both n and $n-2$, while A_2 contains $n-1$, and we have

$$\sum_{i=0}^{i<(n-1)/2-1} 2^{2i} + 2^{n-3} + \sum_{i\in A_1\setminus\{n,n-2\}} 2^{i-1} = 2^{n-2} + \sum_{j\in A_2\setminus\{n-1\}} 2^{j-1}.$$

Defining now $A_1' = A_1 \setminus \{n, n-2\} \cup \{n-1\}$ and $A_2' = A_2 \setminus \{n-1\} \cup \{n-2\}$, again these two sets give a valid counterexample in $\widetilde{\Sigma}_{n-1}$, contradicting the minimality of n.

Consider now the case of odd n. In this case we can rewrite (92) as

$$2^{n-3} + \sum_{i=0}^{i<(n-1)/2-1} 2^{2i} + \sum_{i\in A_1\setminus\{n\}} 2^{i-1} = \sum_{j\in A_2} 2^{j-1}.$$

We notice that A_2 must contain either $n-2$ or $n-1$, but not both, because $b_1 + b_2 + \ldots + b_{n-3} < b_n$ but at the same time $b_1 + b_2 + \ldots + b_{n-3} + b_n < b_{n-2} + b_{n-1}$. Also note that $n-1$ cannot be in A_1, for the same reason mentioned in the case of even n. So, we are left with the following cases to consider:

a) $n-2 \in A_2$, $n-1 \notin A_1 \cup A_2$ and

$$2^{n-3} + \sum_{i=0}^{i<(n-1)/2-1} 2^{2i} + \sum_{i\in A_1\setminus\{n\}} 2^{i-1} = \sum_{j\in A_2\setminus\{n-2\}} 2^{j-1} + 2^{n-3},$$

In this case, by defining $A_2' = A_2 \setminus \{n-2\}$ $A_1' = A_1 \setminus \{n\} \cup \{n-1\}$ we see that these two sets of indices satisfy $|A_1'| + |A_2'| < (n-1)/2$ and give a counterexample in $\widetilde{\Sigma}_{n-1}$, which contradicts the minimality of n.

b) $n-2 \in A_1$, $n-1 \in A_2$ and

$$2 \cdot 2^{n-3} + \sum_{i=0}^{i<(n-1)/2-1} 2^{2i} + \sum_{i\in A_1\setminus\{n,n-2\}} 2^{i-1} = \sum_{j\in A_2\setminus\{n-1\}} 2^{j-1} + 2^{n-2},$$

Here we obtain a counterexample valid for $\widetilde{\Sigma}_{n-1}$ by setting $A_1' = A_1 \setminus \{n, n-2\} \cup \{n-1\}$ and $A_2' = A_2 \setminus \{n-1\}$.

c) $n-2 \notin A_1 \cup A_2$, $n-1 \in A_2$ and

$$2^{n-3} + \sum_{i=0}^{i<(n-1)/2-1} 2^{2i} + \sum_{i \in A_1 \setminus \{n\}} 2^{i-1} = \sum_{j \in A_2 \setminus \{n-1\}} 2^{j-1} + 2^{n-2}\,.$$

In this case we note that $n-3$ must be in A_1, for otherwise $S(A_1) \leq b_n + b_1 + \ldots + b_{n-4} < b_n + b_{n-3} < b_{n-1} \leq S(A_2)$ (see Figure 2). We can then define $A_1' = A_1' \setminus \{n, n-3\} \cup \{n-1\}$ and $A_2' = A_2 \setminus \{n-1\} \cup \{n-3\}$ and again obtain a valid counterexample in $\widetilde{\Sigma}_{n-1}$ which contradicts the minimality of n. □

REMARK 5.2.2. *We note that the condition $|A_1|+|A_2| < n/2$ in the statement of Lemma 5.2.2 is tight, when n is even and greater than or equal to 6, because if we take $A_1 = \{b_n\}$ and $A_2 = \{b_{2i+1} : i = 0, \ldots, n/2-2\}$ then, clearly, $|A_1| + |A_2| = n/2$ and $S(A_1) = S(A_2)$.*

The following corollary follows.

COROLLARY 5.2.1. *If $\lambda < 1/4$, $\widetilde{\Sigma}_n$ is $\mathcal{F}_{\lambda,n}$-sum distinct.*

The meaning of this Corollary is that it is possible to add one more element to the sequence of powers of two in such a way that it remains $\mathcal{F}_{\lambda,n}$-sum distinct. With the same procedure we can also prove the following statement:

LEMMA 5.2.3. *Let us consider the sequence $\widetilde{\Sigma}_n = (b_1, \ldots, b_n)$ where, as in Lemma 5.2.2, we have that*

$$b_i := \begin{cases} 2^{i-1} & i = 1, 2 \ldots n-1 \\ \sum_{j=0}^{j<n/2-1} 2^{2j} & i = n; \end{cases}$$

Then, given two subsets A_1, A_2 of $[1, n]$ such that $|A_1| + |A_2| < (n-1)/2$,

$$S(A_1) = \sum_{i \in A_1} b_i \neq \sum_{j \in A_2} b_j + 2^{n-1} = S(A_2) + 2^{n-1}.$$

PROOF. We note that the set $\widetilde{\Sigma}_n \cup \{2^{n-1}\}$ is $\widetilde{\Sigma}_{n+1}$ whenever n is odd. Therefore, in this case, a contradiction to the statements leads to a contradiction to Lemma 5.2.2 and we can assume n to be even.

Hence, we suppose now we have a counterexample with n even. We would have that $b_n = \sum_{i=0,\ i \equiv 0 \pmod 2}^{n-4} 2^i$ and n must belong to A_1. It follows that

$$\sum_{i=0,\ i \equiv 0 \pmod 2}^{n-4} 2^i + \sum_{i \in A_1 \setminus \{n\}} b_i = \sum_{j \in A_2} b_j + 2^{n-1}.$$

Here we note that, since

$$2^{n-1} = 2^{n-2} + 2^{n-2} > b_n + \sum_{i=0}^{n-3} 2^i = b_n + \sum_{i=1}^{n-2} b_i,$$

$n-1$ must also belong to A_1. In this case we would have that:

$$b_n + 2^{n-2} + \sum_{i \in A_1 \setminus \{n, n-1\}} b_i = \sum_{j \in A_2} b_j + 2^{n-1}.$$

We remark that the $(n+1)$-th element of the sequence $\widetilde{\Sigma}_{n+1}$ is $\sum_{i=0,\ i \equiv 0 \pmod 2}^{n-2} 2^i$ that is $b_n + 2^{n-2}$. It follows that the set $(\widetilde{\Sigma}_n \setminus \{b_n\}) \cup \{2^{n-1}, b_n + 2^{n-2}\}$ is $\widetilde{\Sigma}_{n+1}$ that would be a

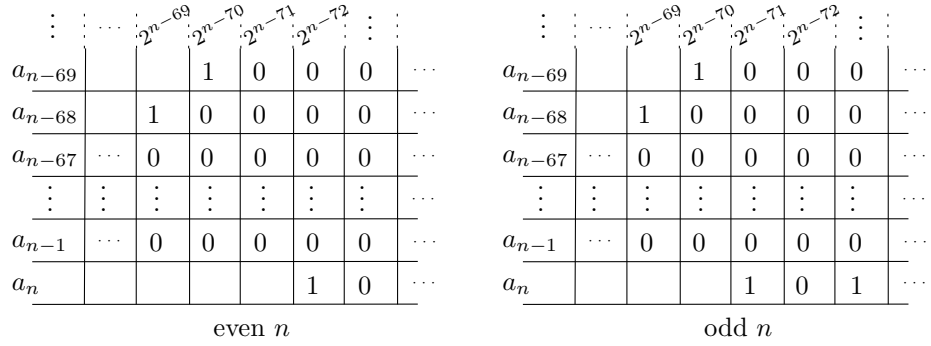


FIGURE 3. Binary representation of the a_n integers used in Proposition 5.2.2.

counterexample to Lemma 5.2.2. Therefore, also for n even, we would obtain a contradiction to Lemma 5.2.2 and thus the statement is verified. □

The ideas of Lemmas 5.2.2 and 5.2.3 can be adapted to the following sum-distinct sequence.

THEOREM 5.2.6 ([93]). *Given $n \geq 67$, there exists a sum-distinct sequence $\overline{\Sigma_n}$ of integers such that $c_{1,n} < c_{2,n} < \cdots < c_{n,n}$, $0,22 \cdot 2^n < c_{n,n} < 0,22096 \cdot 2^n$ and such that, denoted by $(\overline{c_1}, \overline{c_2}, \ldots, \overline{c_{67}})$ the sequence for $n = 67$, we have*

$$c_{i,n} = \begin{cases} 2^{i-1} \text{ if } i \leq n-67; \\ 2^{n-67} \cdot \overline{c_{i-(n-67)}} \text{ otherwise.} \end{cases}$$

Now we show that it is possible to add one more element also to this sequence in such a way that it remains $\mathcal{F}_{\lambda,n}$-sum distinct. We observe that the proof of our result does not depend on the specific $\bar{c}_i$ values which appear in Theorem 5.2.6. Indeed, it suffices to analyze only less significant bits in the binary representation of the $c_{i,n}$'s, which are all zeros for $i \geq n-66$.

PROPOSITION 5.2.2. *Let $\Sigma = (a_1, \ldots, a_n)$ be the sequence of integers defined by*

$$a_i := \begin{cases} c_{i,n-1} & i = 1 \ldots, n-1 \\ \sum_{j=0}^{j<(n-68)/2-1} 2^{2j} & i = n \end{cases}$$

Then, if $\lambda < 1/4$ and n is big enough, Σ is $\mathcal{F}_{\lambda,n}$-sum distinct.

The structure of the set Σ in Proposition 5.2.2 is better understood by writing a table of the binary representations of the integers a_n, as shown in Figure 3.

PROOF. Let us suppose, by contradiction, that there exists two disjoint sets A_1 and A_2 in $\mathcal{F}_{\lambda,n}$ such that $S(A_1) = S(A_2)$. We note that, if $n \notin A_1 \cup A_2$, we would have two distinct sets of elements of $\overline{\Sigma_{n-1}}$ with the same sums which is in contradiction with the fact that, due to Theorem 5.2.6, $\overline{\Sigma_{n-1}}$ is sum-distinct. Therefore, we may assume, without loss of generality, that $n \in A_1$. It follows that

$$a_n + \sum_{i \in A_1 \setminus \{n\}} a_i = \sum_{j \in A_2} a_j.$$

Set $n' := n - 68$. As a generalization of the method used in Lemma 5.2.2, we first look at the equation modulo some appropriate power of 2, namely $2^{n'-1}$ in this case, and then

consider possible reminders in the binary expressions for the sums. We set then $A'_1 := (A_1 \setminus [n', n]) \cup \{n'\}$, $A'_2 := A_2 \setminus [n', n]$, and we redefine $a_{n'}$ as $a_{n'} := \sum_{i=0}^{i<n'/2-1} 2^{2i}$. Since $S(A_1) = S(A_2)$ and $S(A'_2) \leq a_1 + a_2 + \ldots + a_{n'-1} < 2^{n'-1}$ we have that either $S(A'_1) = S(A'_2)$ or $S(A'_1) = S(A'_2) + 2^{n'-1}$. Also, since $n' \in A'_1$ we have that both A'_1 and A'_2 are not empty.

Here, in the first case, if n is big enough, we would have that

$$|A'_1| + |A'_2| \leq |A_1| + |A_2| \leq 2\lambda n < n'/2.$$

This would imply that $\widetilde{\Sigma}_{n'}$ is a contradiction to the statement of Lemma 5.2.2 considered for sets A'_1, A'_2 and for n'.

Similarly, in the second case, if n is big enough, we would have that

$$|A'_1| + |A'_2| \leq |A_1| + |A_2| \leq 2\lambda n < (n' - 1)/2.$$

Here we would have that $\widetilde{\Sigma}_{n'}$ is a contradiction to the statement of Lemma 5.2.3 considered for sets A'_1, A'_2 and for n'.

Since we obtain a contradiction in all cases, Σ is $\mathcal{F}_{\lambda,n}$-sum distinct. □

In case $\lambda < 1/8$ we can even add two elements to the sequence $\overline{\Sigma}$ dividing again the coefficient by 2. At this purpose we need another technical lemma.

LEMMA 5.2.4. *Let us consider the sequence $(d_1, \ldots, d_n)$ where $d_i := 2^{i-1}$.*

Then, given three subsets A_1, A_2, A_3 of $[1, n]$ such that $S(A_1) + S(A_2) = S(A_3)$ we have that

$$|A_1| + |A_2| \geq |A_3|.$$

PROOF. Assume A_1, A_2 and A_3 form a counterexample with minimum possible value of $|A_1| + |A_2|$. By the uniqueness of the binary representation, it is clear that $Y := A_1 \cap A_2 \neq \emptyset$. Also, we note that $n \notin Y$. Then we have

$$\begin{aligned}\sum_{i \in A_1} 2^{i-1} + \sum_{i \in A_2} 2^{i-1} &= \sum_{i \in A_1 \setminus Y} 2^{i-1} + \sum_{i \in A_2 \setminus Y} 2^{i-1} + 2\sum_{i \in Y} 2^{i-1} \\ &= \sum_{i \in A'_1} 2^{i-1} + \sum_{i \in A'_2} 2^{i-1}\end{aligned}$$

where $A'_1 = A_1 \cup A_2 \setminus Y$ and $A'_2 = Y + 1$ is obtained by adding 1 to each element of Y. But here $|A'_1| + |A'_2| = |A_1 \cup A_2| < |A_1| + |A_2|$, contradicting the assumption that the chosen counterexample minimizes $|A_1| + |A_2|$. □

PROPOSITION 5.2.3. *Let n be a positive integer, let us set $n' = \lfloor (n - 69)/2 \rfloor$ and let $\Sigma = (a_1, \ldots, a_n)$ be the sequence of integers defined by*

$$a_i := \begin{cases} \sum_{j=\lceil n'/2 \rceil - 1}^{j<(n-69)/2-1} 2^{2j} & \text{if } i = n; \\ \sum_{j=0}^{j<n'/2-1} 2^{2j} & \text{if } i = n-1; \\ c_{i,n-2} & \text{otherwise.} \end{cases}$$

Then, if $\lambda < 1/8$ and n is big enough, Σ is $\mathcal{F}_{\lambda,n}$-sum distinct.

The structure of the set Σ in Proposition 5.2.3 is better understood by writing a table of the binary representations of the integers a_n. In Figure 4 we show the table only for even n and n' (the other configurations of n and n' can be easily derived).

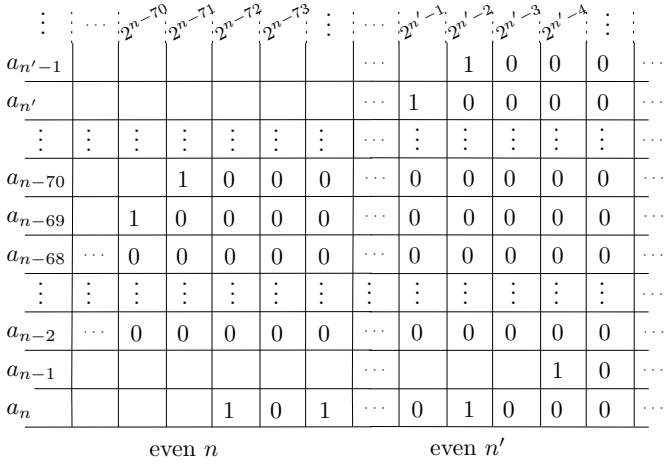


FIGURE 4. Binary representation of the a_n integers used in Proposition 5.2.3 when n and n' are even.

PROOF. Let us suppose, by contradiction, that there exists A_1 and A_2 in $\mathcal{F}_{\lambda,n}$ such that $S(A_1) = \sum_{i\in A_1} a_i = \sum_{j\in A_1} a_j = S(A_2)$. Since $\overline{\Sigma_{n-2}}$ is sum distinct, we may assume, without loss of generality, that $n-1 \in A_1$ or $n \in A_1$ and $n-1 \notin A_1, A_2$. Indeed, if both n and $n-1$ do not belong to $A_1 \cup A_2$ we would have two distinct sets of elements of $\overline{\Sigma_{n-2}}$ with the same sums which is in contradiction with Theorem 5.2.6.

In the first case we may assume due to Proposition 5.2.2 that $n \notin A_1$ and hence we have

$$a_{n-1} + \sum_{i\in A_1\setminus\{n,n-1\}} a_i = \sum_{j\in A_2} a_j.$$

As done in Proposition 5.2.2, we first look at the equation modulo some appropriate power of 2, namely $2^{n'-2}$ in this case, and then consider possible reminders in the binary expressions for the sums. We set $A_1' := (A_1 \setminus [n'-1, n]) \cup \{n'\}$, $A_2' := A_2 \setminus [n'-1, n]$ and we rename $a_{n'}$ by setting $a_{n'} := \sum_{i=0}^{i<n'/2-1} 2^{2i}$ where we recall that $n' = \lfloor (n-69)/2 \rfloor$. Since $S(A_1) = S(A_2)$ and $S(A_2') \leq a_1 + a_2 + \ldots + a_{n'-2} < 2^{n'-2}$ we have that either $S(A_1') = S(A_2')$ or $S(A_1') = S(A_2') + 2^{n'-2}$. In the first case this leads to contradict the statement of Lemma 5.2.2 considered for the sets A_1', A_2' and for n'. In the second case, we get a contradiction to the statement of Lemma 5.2.2 considered for the sets A_1', $A_2' \cup \{n'-1\}$ and for n'.

Let us assume now that $n \in A_1$ and $n-1 \notin A_1, A_2$, that is:

$$a_n + \sum_{i\in A_1\setminus\{n,n-1\}} a_i = \sum_{j\in A_2} a_j. \tag{94}$$

Here we note that by setting $A_3 := \{2i+1 : 0 \leq i < n'/2 - 1\}$ and by adding a_{n-1} to both sides of equation (94) we get

$$a_n + a_{n-1} + \sum_{i\in A_1\setminus\{n,n-1\}} a_i = \sum_{j\in A_2} a_j + \sum_{j\in A_3} a_j, \tag{95}$$

because clearly $a_{n-1} = \sum_{j\in A_3} a_j$.

Since $|A_2| < \frac{1}{8}n$, there exists $h \in [n'-1, n-69]$ that is not in A_2 and for which we have that $a_h > a_{n-1}$. This implies that

$$2^h > \sum_{\substack{j\in A_2\\ j<h}} a_j + a_h > \sum_{\substack{j\in A_2\\ j<h}} a_j + a_{n-1} = \sum_{\substack{j\in A_2\\ j<h}} a_j + \sum_{j\in A_3} a_j. \tag{96}$$

Considering the binary representation of the natural numbers there exists a set A_2'' such that

$$\sum_{\substack{j\in A_2,\\ j<h}} a_j + \sum_{j\in A_3} a_j = \sum_{j\in A_2''} 2^{j-1}. \tag{97}$$

Set $A_1'' := (A_1 \setminus \{n\}) \cup \{n-1\}$ and redefine a_{n-1} by setting $a_{n-1} = \sum_{i=0}^{i<(n-69)/2-1} 2^{2i}$. Then thanks to the upper bound of equation (96) we know that $A_2'' \subseteq [1, h]$ and hence $a_j = 2^{j-1}$ for $j \in A_2''$ and equation (95) can be rewritten as:

$$\sum_{i\in A_1''} a_i = \sum_{j\in A_2''} a_j + \sum_{\substack{j\in A_2,\\ j>h}} a_j. \tag{98}$$

Set $A_2''' := A_2'' \cup (A_2 \setminus [1, h])$. Since A_2'' and $A_2 \setminus [1, h]$ are disjoint, equation (98) becomes

$$\sum_{i\in A_1''} a_i = \sum_{j\in A_2'''} a_j.$$

Now it follows from Lemma 5.2.4 that $|A_2''| \leq |A_2 \setminus [h, n]| + |A_3|$. Therefore we have that

$$|A_2'''| = |A_2''| + |A_2 \setminus [1, h]| \leq |A_2| + |A_3|.$$

Moreover, since, $|A_2| \leq \lambda n < \frac{1}{8}(n-1)$ for n big enough and $|A_3| < \frac{1}{4}(n-1)$, we obtain that $|A_2'''| < \frac{1}{8}(n-1)+\frac{1}{4}(n-1)$. We also have that, for n big enough, $|A_1''| = |A_1| \leq \lambda n < \frac{1}{8}(n-1)$. Here we note that $|A_1''| + |A_2'''| < \frac{1}{2}(n-1)$ but this is in contradiction with the statement of Proposition 5.2.2 considered for the sets A_1'', A_2''' and for $n-1$. □

As a consequence, we have the following result.

THEOREM 5.2.7. *Let $\lambda < 1/4$, (resp. $\lambda < 1/8$) then, if n is big enough, there exists a sequence $\Sigma = (a_1, \ldots, a_n)$ of $\left(\frac{0{,}22096}{2} \cdot 2^n\right)$-bounded integers (resp. $\left(\frac{0{,}22096}{4} \cdot 2^n\right)$-bounded integers) that is $\mathcal{F}_{\lambda,n}$-sum distinct.*

5.2.3.3. *Multi-Dimensional upper bounds.* In this paragraph we consider the general case $k \geq 1$. First of all, we note that both Theorem 5.2.5 and Theorem 5.2.7 can be used to obtain an upper bound for the M of Problem 5.2.1 also in $\mathbb{Z}^k$.

PROPOSITION 5.2.4. *Let $\bar{\Sigma}$ be an integer M-bounded, $\mathcal{F}_{\lambda',n'}$-sum distinct sequence of length n'. Then there exists an M-bounded sequence Σ in $\mathbb{Z}^k$ of length n that is $\mathcal{F}_{\lambda,n}$-sum distinct where $n = kn'$ and $\lambda = \lambda'/k$.*

PROOF. We set $\bar{\Sigma}_j$ to be the sequence in $\mathbb{Z}^k$ whose j-th projection is $\bar{\Sigma}$ and that is zero on the other coordinates. It suffices to consider the sequence $\Sigma = (\bar{\Sigma}_1, \bar{\Sigma}_2, \ldots, \bar{\Sigma}_k)$. Clearly Σ is a sequence in $\mathbb{Z}^k$ of length n. It is also easy to see that, the existence of A_1, A_2 in $\mathcal{F}_{\lambda,n}$ such that $S(A_1) = S(A_2)$ would imply the existence of A_1', A_2' in $\mathcal{F}_{\lambda',n'}$ such that $S(A_1') = S(A_2')$ for $\bar{\Sigma}$. But, since $\bar{\Sigma}$ is an $\mathcal{F}_{\lambda',n'}$-sum distinct sequence, it follows that Σ is $\mathcal{F}_{\lambda,n}$-sum distinct. □

On the other hand, assuming $k > 1$, these results can be improved for several values of λ using the probabilistic method (see [8]). If $k = 1$, instead, the probabilistic method fails to beat the upper bound of Theorem 5.2.5 (see Remark 5.2.3).

We first need another enumerative lemma.

LEMMA 5.2.5. *Let $\mathcal{C}$ be the family of the unordered pairs $\{A_1, A_2\}$ of subsets of $[1, n]$ such that:*

- *$A_1 \cap A_2 = \emptyset$;*
- *The cardinalities of A_1 and A_2 are smaller than or equal to λn.*

Then, for $\lambda < 1/3$, we have the following upper bound on the cardinality of $\mathcal{C}$

$$|\mathcal{C}| < \frac{\lambda^2 n^2}{2} \cdot 2^{f(\lambda)n}.$$

PROOF. It can be easily derived from the proof of Lemma 5.2.1. □

THEOREM 5.2.8. *Let*

$$C_{\lambda,n} = \sqrt[k]{\frac{\lambda^2 n^2}{2\tau_\lambda} 2^{f(\lambda)\tau_\lambda}} \text{ and } \tau_\lambda = \left\lceil \frac{1}{2^{f(\lambda)} - 1} \right\rceil.$$

Then there exists a sequence $\Sigma = (a_1, \ldots, a_n)$, for n big enough, of $\left(C_{\lambda,n} \cdot 2^{f(\lambda)n/k}\right)$-bounded elements of $\mathbb{Z}^k$ that is $\mathcal{F}_{\lambda,n}$-sum distinct.

PROOF. We recall that, if two sets A_1 and A_2 have the same sum, then also $A_1 \setminus (A_1 \cap A_2)$ and $A_2 \setminus (A_1 \cap A_2)$ have the same sum. Therefore, a sequence Σ is $\mathcal{F}_{\lambda,n}$-sum distinct whenever $S(A_1) \neq S(A_2)$ for any $A_1, A_2 \in \mathcal{F}_{\lambda,n}$ such that $A_1 \cap A_2 = \emptyset$. Moreover, since $A_1 \neq A_2$, we can assume without loss of generality that A_2 is not the empty set.

Now we choose, uniformly at random, the sequence Σ' with elements in $[1, M]^k$ and of length n' (whose value will be specified later). Let X be a random variable that represents the numbers of pairs of elements of $\mathcal{F}_{\lambda,n'}$ such that $A_1 \cap A_2 = \emptyset$, $S(A_1) = S(A_2)$ and A_2 is not the empty set.

Then we need to estimate

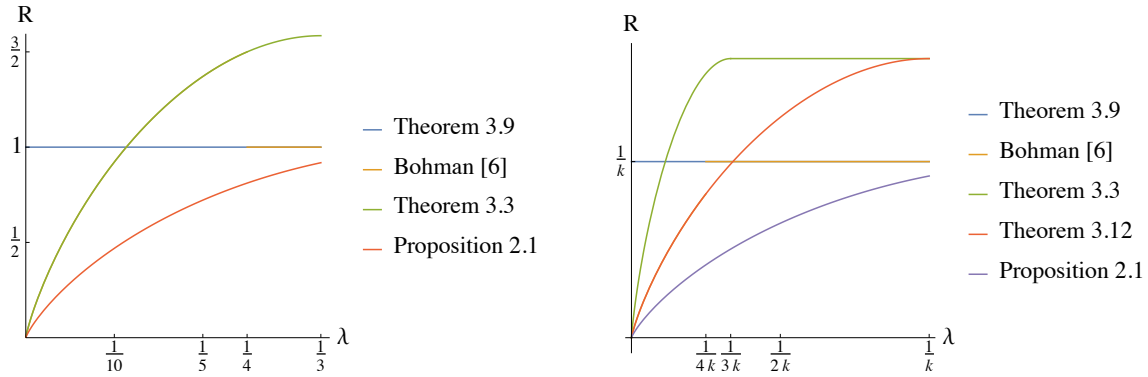
$$\begin{aligned}\mathbb{E}[X] &= \mathbb{E}(|\{\{A_1, A_2\} : S(A_1) = S(A_2), A_1, A_2 \in \mathcal{F}_{\lambda,n'}, A_1 \cap A_2 = \emptyset \neq A_2\}|) \\ &= \sum_{\{A_1,A_2\}:\ A_1,A_2 \in \mathcal{F}_{\lambda,n'}, A_1 \cap A_2 = \emptyset \neq A_2} p[S(A_1) = S(A_2)].\end{aligned}$$

Since $A_1 \cap A_2 = \emptyset$, the value of $S(A_1)$ is independent from the value of $S(A_2)$. Then the probability $p[S(A_1) = S(A_2)]$ is the following

$$p[S(A_1) = S(A_2)] = \sum_{s \in \mathbb{Z}^k} p[S(A_1) = s] \cdot p[S(A_2) = s].$$

We recall that $A_1 \cap A_2 = \emptyset \neq A_2$ and hence there exists $i \in A_2 \setminus A_1$. Clearly, A_2 can sum to s only if $a_i = s - S(A_2 \setminus \{i\})$ that happens with probability at most $1/M^k$. This means that

$$\begin{aligned}\mathbb{E}[X] &\leq \sum_{\{A_1,A_2\}:\ A_1,A_2 \in \mathcal{F}_{\lambda,n}, A_1 \cap A_2 = \emptyset \neq A_2} \left(\sum_{s \in \mathbb{Z}^k} p[S(A_1) = s](1/M^k) \right) \\ &= \frac{1}{M^k} |\{\{A_1, A_2\} :\ A_1, A_2 \in \mathcal{F}_{\lambda,n}, A_1 \cap A_2 = \emptyset \neq A_2\}|.\end{aligned}$$



(A) $k = 1$ (B) $k > 1$

FIGURE 5. Exponent of the upper and lower bounds for $k = 1$ and for $k > 1$. Here the bounds of Bohman [27], Theorem 5.2.5 and Theorem 5.2.7 have been extended via Proposition 5.2.4.

Therefore, according to Lemma 5.2.5, we have that

$$\mathbb{E}[X] < \frac{1}{M^k}(\lambda n')^2 \cdot 2^{f(\lambda)n'-1}. \tag{99}$$

This means that, in case $(1/M^k)(\lambda n')^2 \cdot 2^{f(\lambda)n'-1} \leq t$, there exists a sequence $\Sigma' = (a_1, \ldots, a_{n'})$ of elements in $\mathbb{Z}^k$ with at most t pairs $\{A_1, A_2\}$ that have the same sum and satisfy the assumptions. Hence, we can remove t elements from Σ' and obtain a new sequence $\Sigma = (a_1, \ldots, a_n)$, with $n = n' - t$ elements, that is $\mathcal{F}_{\lambda,n}$-sum distinct. Since $n' = n + t$ and due to inequality (99), Σ exists whenever

$$M \geq (1 + o(1)) \sqrt[k]{\frac{\lambda^2 n^2}{2} \frac{2^{f(\lambda)t}}{t}} \cdot 2^{f(\lambda)n/k}. \tag{100}$$

It can be seen that the function $g_\lambda(t) := \frac{2^{f(\lambda)t}}{t}$ is strictly convex for $t > 0$ and the minimum integer m for which $g_\lambda(m+1) \geq g_\lambda(m)$ is equal to τ_λ. Therefore $t = \tau_\lambda = \left\lceil \frac{1}{2^{f(\lambda)}-1} \right\rceil$ is the best choice in order to optimize the inequality (100). □

REMARK 5.2.3. *We note that for $k = 1$ and n sufficiently large the upper bound given in Theorem 5.2.5 improves the one given in Theorem 5.2.8 since*

$$\lambda < \frac{2^{f(\lambda)\tau_\lambda}}{2\tau_\lambda},$$

for every $0 < \lambda \leq 1/3$.

CHAPTER 6

Sequenceability of cyclic groups

In this chapter, the results presented in Section 6.2 are obtained in collaboration with Simone Costa, M. A. Ollis and Sarah Z. Rovner-Frydman. All the results presented in Section 6.3 are obtained with Simone Costa.

6.1. Introduction

Given a subset of an abelian group, is it possible to order the elements of the subset in such a way that the partial sums of the ordering are distinct? This type of problem goes back at least fifty years and there are several conjectures on the topic, described below. The successful resolution, or partial resolution, of these conjectures, has implications in the study of graph decompositions and embeddings and in the construction of Heffter arrays and other combinatorial designs.

We introduce some definitions and notation to make the previous question precise. Let G be an abelian group and let S be a subset of $G \setminus \{0\}$ of size k.

Let $\boldsymbol{x} = (x_1, x_2, \ldots, x_k)$ be an ordering of the elements of S and define its partial sums $\boldsymbol{y} = (y_0, y_1, \ldots, y_k)$ by $y_0 = 0$ and $y_i = x_1 + \cdots + x_i$ for $i > 0$. Denote the sum of the elements of S by ΣS. As G is abelian, for any ordering of the elements of S the final partial sum y_k is equal to ΣS.

If the elements of $\boldsymbol{y}$ are distinct, then $\boldsymbol{x}$ is a *sequencing* of S. If the elements of $\boldsymbol{y}$ are distinct with the exception that $y_0 = 0 = y_k$, then $\boldsymbol{x}$ is a *rotational sequencing* or *R-sequencing* of S. We sometimes refer to a sequencing as a *linear sequencing* to emphasize the distinction from rotational sequencings. As G is abelian, a subset S cannot have both a linear and a rotational sequencing. If S has one or the other, call it *sequenceable*. If every subset $S \subseteq G \setminus \{0\}$ is sequenceable then G is *strongly sequenceable*.

This nomenclature is consistent with the definition of sequencing and R-sequencing introduced by Gordon in 1961 and Friedlander, Gordon and Miller in 1978 respectively for the case $S = G \setminus \{0\}$ [71, 76]. Replacing "R-" with the more descriptive "rotational" was suggested by Ahmed, Azimli, Anderson and Preece in 2011 [3]. The term "strongly sequenceable" was first used in the literature by Alspach and Liversidge in 2020, where they say that Alspach and Kalinowski have posed the problem of determining which groups are strongly sequenceable and also make a conjecture that would imply that every finite abelian group is strongly sequenceable.

We now come to the main conjecture.

Conjecture 6.1.1. *Every abelian group is strongly sequenceable.*

Conjecture 6.1.1 is the amalgamation of several questions and conjectures. In 1971, Graham asked whether every subset S of $\mathbb{Z}_n$, the additively written cyclic group of order n, with $0 \notin S$ and $\Sigma S = 0$, has a rotational sequencing when n is prime [77]. Independently of this, in 2016 Archdeacon, Dinitz, Mattern and Stinson conjectured that any subset S of

This chapter includes research results published in [43].

$\mathbb{Z}_n \setminus \{0\}$ with $\Sigma S = 0$ has a rotational sequencing [13]. In 2005, Bode and Harborth published the first results on *Alspach's conjecture* that every subset S of $\mathbb{Z}_n \setminus \{0\}$ with $\Sigma S \neq 0$ has a linear sequencing [26]. In 2018, Costa, Morini, Pasotti and Pellegrini suggested that these conjectures may be generalized from subsets of $\mathbb{Z}_n$ to finite subsets of arbitrary (including infinite) abelian groups [40].

Costa, Morini, Pasotti and Pellegrini also put forward a weaker version of Conjecture 6.1.1 that is sufficient for some applications to Heffter arrays, a combinatorial structure introduced by Archdeacon in [14]:

CONJECTURE 6.1.2. *Let G be an abelian group and let S be a finite subset of $G \setminus \{0\}$ such that $\Sigma S = 0$ and $|S \cap \{x, -x\}| \leq 1$ for any $x \in G$. Then S has a rotational sequencing.*

As suggested by the discussion of nomenclature above, the case $S = G \setminus \{0\}$ was considered earlier (mostly) than these conjectures. Gordon posed and solved the question in this instance for linear sequenceability in 1961. Friedlander, Gordon and Miller conjectured the rotational sequenceability version in 1978 [71] and this was recently resolved by Alspach, Kreher and Pastine [9].

THEOREM 6.1.1. *Let G be an abelian group of order n and $S \subseteq G \setminus \{0\}$ with $|S| = k$. Then S is sequenceable in the following cases:*

(1) $k \leq 9$ [10],
(2) $k = 10$ *when n is prime* [84],
(3) $k = n - 3$ *when n is prime and* $\Sigma S \neq 0$ [84],
(4) $k = n - 2$ *when G is cyclic and* $\Sigma S \neq 0$ [26],
(5) $k = n - 1$ [9, 76],
(6) $n \leq 21$ [40],
(7) $n \leq 23$ *and* $\sum S = 0$ [40], *and*
(8) $n \leq 25$ *for G cyclic and* $\sum S = 0$ [13].

Furthermore, if G is a torsion-free abelian group, then any subset S of $G \setminus \{0\}$ whose size is at most 11 *is sequenceable* [39].

This chapter is organized as follows. In *Section 6.2*, we demonstrate the sequenceability of subsets of size k of $\mathbb{Z}_n \setminus \{0\}$ when $n = mt$ in many cases, when m is prime and for $k \leq 11$ and $t \leq 5$ and for $k = 12$ and $t \leq 4$. We obtain similar, but partial, results for $13 \leq k \leq 15$. This represents progress on a variety of questions and conjectures in the literature concerning the sequenceability of subsets of abelian groups, which we combine and summarize into the conjecture that if a subset of an abelian group does not contain 0 then it is sequenceable. If the elements of a sequenceable set A do not sum to 0 then there exists a simple path P in the Cayley graph $Cay[G : \pm A]$ such that $\Delta(P) = \pm A$. In *Section 6.3*, inspired by this graph-theoretical interpretation, we propose a weakening of a conjecture given by Alspach and Liversidge [10]. The goal is to find an ordering whose partial sums define a walk W of girth bigger than t (for a given $t < k$) and such that $\Delta(W) = \pm A$. In this case, we say that the set A is *t-weakly sequenceable*. The main result presented in Section 6.3 is that any subset A of $\mathbb{Z}_p \setminus \{0\}$ is t-weakly sequenceable whenever $t < 7$ or when A does not contain pairs of type $\{x, -x\}$ and $t < 8$.

REMARK 6.1.1. *In Chapter 5, we studied a distinct-sum problem over the integers with the constraint that all the subset-sums have to be different. In this Chapter, instead, we consider sequences of distinct elements that belong to the cyclic group $\mathbb{Z}_n$ with the property that the partial sums have to be different. So we are both weakening the subset-sums constraint and strengthening the requirements since we need to work in a cyclic group.*

6.2. On sequences in cyclic groups with distinct partial sums

The main purpose of this section is to prove more instances of Conjecture 6.1.1. In the next subsection we adapt the polynomial method used in [84] so that it may be used to prove instances of the conjecture in cyclic groups of order pt, where p is prime and t is small. This requires computing coefficients of monomials in various polynomials, the results of which are summarized in Subsection 6.2.2. As well as composite orders, we are able to push k higher in the prime case. In sum, we prove:

THEOREM 6.2.1. *Let $n = pt$ with p prime. Then subsets S of size k of $\mathbb{Z}_n \setminus \{0\}$ are sequenceable in the following cases:*

1. *$k \leq 11$ and $t \leq 5$,*
2. *$k = 12$ and $t \leq 4$,*
3. *$k = 13$ and $t \in \{2, 3\}$, provided S contains at least one element not in the subgroup of order p,*
4. *$k = 14$ and $t = 2$, provided S contains at least one element not in the subgroup of order p, and*
5. *$k = 15$ and $t = 2$, provided S does not contain exactly 0, 1, 2 or 15 elements of the subgroup of order p.*

6.2.1. Applying the polynomial method. The method relies on the Non-Vanishing Corollary to the Combinatorial Nullstellensatz (see [7, 94]).

THEOREM 6.2.2. (Non-Vanishing Corollary) *Let F be a finite field and let $f(x_1, x_2, \ldots, x_k)$ be a polynomial in $F[x_1, x_2, \ldots, x_k]$. Suppose the degree $deg(f)$ of f is $\sum_{i=1}^{k} \gamma_i$, where each γ_i is a nonnegative integer, and suppose the coefficient of $\prod_{i=1}^{k} x_i^{\gamma_i}$ in f is nonzero. If $C_1, C_2, \ldots, C_k$ are subsets of F with $|C_i| > \gamma_i$, then there are $c_1 \in C_1, \ldots, c_k \in C_k$ such that $f(c_1, c_2, \ldots, c_k) \neq 0$.*

In the notation of the Non-Vanishing Corollary, call the monomial $x_1^{|C_1|-1} \cdots x_k^{|C_k|-1}$ the *bounding monomial*. The corollary can be rephrased as requiring the polynomial to include a monomial of maximum degree that divides the bounding monomial (where by "include" we mean that it has a nonzero coefficient).

To use the Non-Vanishing Corollary we require a polynomial for which the nonzeros correspond to successful solutions to the case of the problem under consideration.

We work in the group $\mathbb{Z}_p \times \mathbb{Z}_t$, where p is prime and $p \nmid t$. This means that p is coprime with t, hence $\mathbb{Z}_p \times \mathbb{Z}_t \cong \mathbb{Z}_{pt}$. The set $\mathbb{Z}_p$ is a field, and this plays the role of the field F in the Non-Vanishing Corollary.

Let $\pi_2 : \mathbb{Z}_p \times \mathbb{Z}_t \to \mathbb{Z}_t$ be the projection map that picks out the second coordinate of an element and for a subset $S \subseteq (\mathbb{Z}_p \times \mathbb{Z}_t) \setminus \{(0,0)\}$ let $\pi_2(S)$ be the multiset $\{\pi_2(s) : s \in S\}$. Define the *type* of S to be the sequence $\boldsymbol{\lambda} = (\lambda_0, \ldots, \lambda_{t-1})$, where λ_i is the number of times that i appears in $\pi_2(S)$.

Let T be a multiset of elements from $\mathbb{Z}_t \setminus \{0\}$ with size k. Let $\boldsymbol{a} = (a_1, \ldots, a_k)$ be an arrangement of the elements of T with partial sums $\boldsymbol{b} = (b_0, b_1, \ldots, b_k)$. If, for each i, the element i appears at most r times in $\mathbf{b}$, then $\mathbf{a}$ is a *quotient sequencing* of T with respect to r. In our setting, given some $S \subseteq (\mathbb{Z}_p \times \mathbb{Z}_t) \setminus \{(0,0)\}$ for which we wish to find a sequencing, we shall be interested in quotient sequencings of $\pi_2(S)$ with respect to p.

When $S = G \setminus \{0\}$, quotient sequencings have been a useful tool in the construction of sequencings from the earliest papers on the subject; see [99] for a summary of the history.

Given $S \subseteq (\mathbb{Z}_p \times \mathbb{Z}_t) \setminus \{(0,0)\}$ we first construct a quotient sequencing of $\pi_2(S)$ with respect to p. We then use the polynomial method to show that there is a sequencing for S that projects elementwise onto that quotient sequencing. Given such a quotient sequencing $\boldsymbol{a} = (a_1, \ldots, a_k)$ with partial sums $\boldsymbol{b} = (b_0, b_1, \ldots, b_k)$, let

$$\boldsymbol{x_a} = ((x_1, a_1), (x_2, a_2), \ldots, (x_k, a_k))$$

be a putative arrangement of the elements of S with partial sums

$$\boldsymbol{y_a} = ((y_0, b_0), (y_1, b_1), \ldots, (y_k, b_k)).$$

Define a polynomial in variables $x_1, x_2, \ldots, x_k$ by

$$p_{\boldsymbol{a}} = \prod_{\substack{1 \le i < j \le k \\ a_i = a_j}} (x_j - x_i) \prod_{\substack{0 \le i < j \le k \\ b_i = b_j \\ j \ne i+1 \\ (i,j) \ne (0,k)}} (y_j - y_i)$$

where the variable x_i ranges over the values $\{c : (c, a_i) \in S\}$ for each i.

We claim that an assignment of the variables makes $\boldsymbol{x_a}$ a sequencing of S if and only if this polynomial is nonzero.

The first product compares elements in the sequencing: it contains a factor that is zero if and only if $(x_i, a_i) = (x_j, a_j)$ for some i, j. The second product does a similar task for the partial sums when the first two conditions on the product are considered. The second two conditions reduce the degree of the polynomial, which is generally a positive effect as it makes it easier to meet the degree condition in the Non-Vanishing Corollary and reduces the amount of work required to calculate a coefficient. The condition $j \ne i + 1$ is permissible, because we know that $(y_i, b_i) \ne (y_{i+1}, b_{i+1})$ by the assumption that $(0,0) \notin S$. The condition $(i,j) \ne (0,k)$ is permissible as we know that $(y_0, b_0) = (0,0)$ and $(y_k, b_k) = \Sigma S$: the polynomial will detect linear or rotational sequencings according to whether ΣS is nonzero or zero respectively.

For each i, the number of possible values for x_i is $|\{c : (c, a_i) \in S\}|$. Therefore the bounding monomial for use with the Non-Vanishing Corollary is given by $x_1^{|C_1|-1} \cdots x_k^{|C_k|-1}$, where C_i is the set of elements in S that are in the coset $\overline{(0, a_i)}$ with respect to the subgroup $\mathbb{Z}_p \times \{0\}$.

EXAMPLE 6.2.1. *Let $G = \mathbb{Z}_p \times \mathbb{Z}_2$ with $p > 2$ and p prime. Suppose $S \subseteq G \setminus \{(0,0)\}$ with $|S| = 5$ and of type $(3,2)$. The sequence $\boldsymbol{a} = (0,1,0,0,1)$ has partial sums $(0,0,1,1,1,0)$ and so is a quotient sequencing of $\pi_2(S)$ with respect to p. We desire a sequencing of S of the form*

$$((x_1, 0), (x_2, 1), (x_3, 0), (x_4, 0), (x_5, 1)).$$

The polynomial is

$$\begin{aligned} p_{\boldsymbol{a}} &= (x_3 - x_1)(x_4 - x_1)(x_4 - x_3)(x_5 - x_2)(y_5 - y_1)(y_4 - y_2) \\ &= (x_3 - x_1)(x_4 - x_1)(x_4 - x_3)(x_5 - x_2)(x_2 + x_3 + x_4 + x_5)(x_3 + x_4). \end{aligned}$$

To apply the Non-Vanishing Corollary we need a monomial of this polynomial which divides the bounding monomial $x_1^2 x_2 x_3^2 x_4^2 x_5$ with a nonzero coefficient. One such is $x_1^2 x_3^2 x_4 x_5$, which has coefficient -1. Hence whenever S has this form it has a sequencing.

Noting that $G \cong \mathbb{Z}_{2p}$, we can rephrase this as showing that a subset S of $\mathbb{Z}_{2p} \setminus \{0\}$ has a sequencing whenever $|S| = 5$ and S has exactly 3 even elements.

When $t = 1$ we always have $a_i = 0 = a_j$ and $b_i = 0 = b_j$ and the polynomial $p_{\boldsymbol{a}}$ reduces to the one used in [84] to investigate Alspach's Conjecture in $\mathbb{Z}_p$ for p prime:

$$p_{\boldsymbol{a}} = \prod_{1 \le i < j \le k} (x_j - x_i) \prod_{\substack{0 \le i < j \le k \\ j \ne i+1 \\ (i,j) \ne (0,k)}} (y_j - y_i).$$

As noted in the introduction, that paper was concerned only with the case $\Sigma S \neq 0$, but the above discussion shows that the same calculations also prove Theorem 6.1.1.3 when $\Sigma S = 0$.

The polynomial method approach may also be used for Conjecture 6.1.2. While the same polynomial suffices, we can reduce the degree slightly by considering this alternative:

$$q_{\boldsymbol{a}} = \prod_{\substack{1 \le i < j \le k \\ a_i = a_j}} (x_j - x_i) \prod_{\substack{0 \le i < j \le k \\ b_i = b_j \\ j \notin \{i+1, i+2\} \\ (i,j) \ne (0,k)}} (y_j - y_i).$$

The difference compared to $p_{\boldsymbol{a}}$ is that we have removed factors of the form $(y_{i+2} - y_i)$. In the context of Conjecture 6.1.2 we know that a factor of this form is nonzero when y_i and y_{i+2} are in the same coset because $(x_{i+1}, a_{i+1}) \neq -(x_i, a_i)$. However, in the next subsection all computations use $p_{\boldsymbol{a}}$ rather than $q_{\boldsymbol{a}}$.

6.2.2. Computational results. We begin with the case $t = 1$; that is, groups of prime order.

THEOREM 6.2.3. *Let p be prime and let $S \subseteq \mathbb{Z}_p \setminus \{0\}$ with $|S| \in \{11, 12\}$. Then S is sequenceable.*

PROOF. First, consider the case $|S| = 11$. The polynomial $p_{\boldsymbol{a}}$ for this situation has degree 109 and to use the Non-Vanishing Corollary we require a monomial that divides the bounding monomial $x_1^{10} x_2^{10} \cdots x_{11}^{10}$ of degree 110, which gives eleven possible monomials. Over the integers, the coefficient on $x_1^9 x_2^{10} \cdots x_{11}^{10}$ is

$$-18128730243333160 = -2^3 \cdot 5 \cdot 11 \cdot 3019 \cdot 13647452681$$

and the coefficient on $x_1^{10} x_2^9 x_3^{10} \cdots x_{11}^{10}$ is

$$-46383022877233608 = -2^3 \cdot 3^2 \cdot 644208651072689$$

(in each case the right-hand side gives the prime factorization).

The two integers have no odd prime factors in common. Therefore, for any odd prime p (in particular, for any prime greater than 11, which is the current concern) the coefficient in $\mathbb{Z}_p$ is nonzero for at least one of these two monomials. The Non-Vanishing Corollary gives the result.

We use the same approach for $|S| = 12$. The polynomial $p_{\boldsymbol{a}}$ now has degree 131 and the prime factorizations of the coefficients on the monomials $x_1^{10} x_2^{11} \cdots x_{12}^{11}$ and $x_1^{11} x_2^{10} x_3^{11} \cdots x_{12}^{11}$ are

$$2^4 \cdot 3 \cdot 29 \cdot 12953077208391719881 \quad \text{and} \quad 2^3 \cdot 3 \cdot 277 \cdot 1901 \cdot 786640832519761$$

and the result follows. □

The program used for the computation used in the proof of Theorem 6.2.3 was independent of those used in [84]. This new program recalculated the coefficients obtained in that paper, obtaining the same results.

Moving on to $t > 1$, the method described in the previous subsection divides the proof into a case for each type. For each case, the first step of the process is to find a quotient sequencing that matches the type. There are typically many of these. We tend to choose a quotient sequencing whose partial sums are distributed among the elements of $\mathbb{Z}_t$ as evenly as possible, as this both reduces the degree of $p_{\boldsymbol{a}}$ and minimizes the smallest value of p with respect to which it is a quotient sequencing.

For many types of S, we find a quotient sequencing for which the degree of $p_{\boldsymbol{a}}$ is significantly lower than the degree of the bounding monomial. This gives the scope to prove slightly stronger results with less computation.

Suppose that we have set a quotient sequencing $\boldsymbol{a} = (a_1, \ldots, a_k)$. Take ℓ with $1 \leq \ell \leq k$ and assume $x_\ell = c$ for some constant c such that $(c, a_\ell) \in S$. Then we define the following non-homogeneous polynomial that is nonzero if and only if there is a sequencing of S that has quotient sequencing $\boldsymbol{a}$ and with (c, a_ℓ) in position ℓ:

$$p'_{\boldsymbol{a}} = \prod_{\substack{1 \leq i < j \leq k \\ a_i = a_j \\ i,j \neq \ell}} (x_j - x_i) \prod_{\substack{0 \leq i < j \leq k \\ b_i = b_j \\ j \neq i+1 \\ (i,j) \neq (0,k)}} (y_j - y_i).$$

As we are interested in terms of maximum degree, we may replace factors in $p'_{\boldsymbol{a}}$ that include c as a summand by the same factor with c removed.

This process reduces the complexity of the initial polynomial $p_{\boldsymbol{a}}$, which is an advantage for computing coefficients. It also reduces the degree of the bounding monomial as there is one fewer element available in the coset $\overline{(0, a_\ell)}$. This can mean that the Non-Vanishing Corollary does not apply and that we therefore cannot make this step.

The process may be repeated by choosing multiple elements to fix as arbitrary constants. However, we must ensure that there are no relations between the constants and their positions that could lead to the polynomial returning a nonzero for a non-sequencing, which could happen if a factor is a linear combination of constants with no variables. We achieve this by never fixing both x_ℓ and $x_{\ell'}$ with $\ell' \in \{\ell - 1, \ell + 1\}$, which means that every factor retains at least one variable.

In general, we keep fixing elements until there are no more that we may fix without becoming unable to apply the Non-Vanishing Corollary.

EXAMPLE 6.2.2. *Let $G = \mathbb{Z}_p \times \mathbb{Z}_2$ with $p > 3$ and p prime. Suppose $S \subseteq G \setminus \{(0,0)\}$ with $|S| = 7$ and of type $(5, 2)$. The sequence $\boldsymbol{a} = (0, 0, 1, 0, 0, 0, 1)$ has partial sums $(0, 0, 0, 1, 1, 1, 1, 0)$ and so is a quotient sequencing of $\pi_2(S)$ with respect to p. We desire a sequencing of S of the form*

$$((x_1, 0), (x_2, 0), (x_3, 1), (x_4, 0), (x_5, 0), (x_6, 0), (x_7, 1))$$

with partial sums

$$((y_0, 0), (y_1, 0), (y_2, 0), (y_3, 1), (y_4, 1)(y_5, 1), (y_6, 1), (y_7, 0)).$$

The polynomial is

$$\begin{aligned} p_{\boldsymbol{a}} &= (x_2 - x_1)(x_4 - x_1)(x_5 - x_1)(x_6 - x_1)(x_4 - x_2)(x_5 - x_2)(x_6 - x_2)(x_7 - x_3) \\ &\quad (x_5 - x_4)(x_6 - x_4)(x_6 - x_5)(y_2 - y_0)(y_7 - y_1)(y_7 - y_2)(y_5 - y_3)(y_6 - y_3)(y_6 - y_4) \\ &= (x_2 - x_1)(x_4 - x_1)(x_5 - x_1)(x_6 - x_1)(x_4 - x_2)(x_5 - x_2)(x_6 - x_2)(x_7 - x_3) \\ &\quad (x_5 - x_4)(x_6 - x_4)(x_6 - x_5)(x_1 + x_2)(x_2 + x_3 + x_4 + x_5 + x_6 + x_7) \\ &\quad (x_3 + x_4 + x_5 + x_6 + x_7)(x_4 + x_5)(x_4 + x_5 + x_6)(x_5 + x_6). \end{aligned}$$

Since the polynomial $p_{\boldsymbol{a}}$ has degree 17 and the bounding monomial $x_1^4x_2^4x_3x_4^4x_5^4x_6^4x_7$ has degree 22, we can fix $x_3 = c_1$ and $x_6 = c_2$, where $(c_1, 1), (c_2, 0) \in S$, without violating the constraint on the degree of the polynomial which has to be less than or equal to the degree of the bounding monomial to satisfy the hypotheses of the Non-Vanishing Corollary. Therefore we get the following simplified polynomial of degree 12

$$\begin{aligned} p'_{\boldsymbol{a}} &= (x_2 - x_1)(x_4 - x_1)(x_5 - x_1)(x_4 - x_2)(x_5 - x_2)(x_5 - x_4)(x_1 + x_2)(x_4 + x_5) \\ &\quad (x_2 + c_1 + x_4 + x_5 + c_2 + x_7)(c_1 + x_4 + x_5 + c_2 + x_7)(x_4 + x_5 + c_2)(x_5 + c_2). \end{aligned}$$

To apply the Non-Vanishing Corollary we need a monomial of this polynomial which divides the new bounding monomial $x_1^3x_2^3x_4^3x_5^3$ with a nonzero coefficient. Since the degree of $p'_{\boldsymbol{a}}$ is equal to the degree of the new bounding monomial, the only feasible monomial is $x_1^3x_2^3x_4^3x_5^3$, which has coefficient -2. Hence whenever S has this form it has a sequencing.

The following result completes the proof of Theorem 6.2.1.

THEOREM 6.2.4. *Let $n = pt$ with p prime. Then subsets S of size k of $\mathbb{Z}_n \setminus \{0\}$ are sequenceable in the following cases:*

1. *$k \leq 11$ and $t \in \{2, 3, 4, 5\}$,*
2. *$k = 12$ and $t \in \{2, 3, 4\}$,*
3. *$k = 13$ and $t \in \{2, 3\}$, provided S contains at least one element not in the subgroup of order p,*
4. *$k = 14$ and $t = 2$, provided S contains at least one element not in the subgroup of order p, and*
5. *$k = 15$ and $t = 2$, provided S does not contain exactly 0, 1, 2 or 15 elements of the subgroup of order p.*

PROOF. We can suppose that $k \geq 10$ since by [10] we know that the subsets S of size $k \leq 9$ in an arbitrary abelian group are sequenceable. Then, in all of the cases stated in the theorem, we can use the Non-Vanishing Corollary since $\mathbb{Z}_p \times \mathbb{Z}_t \cong \mathbb{Z}_{pt}$ except for $p = t = 5$ which has been treated separately. In that case we have checked computationally that each subset of size 10 and 11 of $\mathbb{Z}_{25} \setminus \{0\}$ is sequenceable. All of the other results are obtained using the Python framework SageMath [55] mainly because it has efficient libraries to handle multivariate polynomials. The polynomial multiplication was carried out by multiplying pairs of factors and then all the resulting terms together. The specific order of the products is described by the pseudo-code in Algorithm 2.

In addition, after each multiplication, we only keep the terms that divide the bounding monomial. If we are searching for the coefficient of a specific monomial then we can also lower bound the exponents of each term because at some point of the computation the degrees of the variables x_i's cannot be too small. For the sake of readability, the pseudo-code reported in Algorithm 2 does not include the restrictions on the exponents of each monomial. However, the code associated with the final version of the algorithm is given in the Appendix of this section.

All the tables reporting the monomials' coefficients for each case listed in Theorem 6.2.4 can be found at

`https://arxiv.org/abs/2203.16658`.

All of the computations were completed in less than 5 days on a PC with a 4.6 GHz AMD Ryzen 9 processor and 128 GB of RAM. □

Algorithm 2 Polynomial multiplication

Require:
$G = \mathbb{Z}_p \times \mathbb{Z}_t$, p prime, $t \geq 1$ and p coprime with t
$S \subseteq G \setminus \{(0,0)\}$, $|S| = k$
$\boldsymbol{a} = (a_1, a_2, \ldots, a_k)$ with partial sums $\boldsymbol{b} = (b_0, b_1, \ldots, b_k)$
$p \leftarrow 1$
for $1 \leq i < j \leq k$ **do**
  $f \leftarrow 1$
  if $a_i = a_j$ **then**
    $f \leftarrow f \cdot (x_j - x_i)$
  end if
  if $b_{i-1} = b_j$ **and** $(i-1, j) \neq (0, k)$ **then**
    $f \leftarrow f \cdot (x_i + \cdots + x_j)$
  end if
  $p \leftarrow p \cdot f$
end for
return p

TABLE 1. Monomials and their coefficients sufficient for the proof of Theorem 6.2.4 in the case $|S| = 10$ and $t = 2$.

$\boldsymbol{\lambda}$	**a**	deg	monomial/s	coefficient/s
$(10,0)$	$(0,0,0,0,0,0,0,0,0,0)$	89	$x_1^8x_2^9x_3^9x_4^9x_5^9x_6^9x_7^9x_8^9x_9^9x_{10}^9$ $x_1^9x_2^8x_3^9x_4^9x_5^9x_6^9x_7^9x_8^9x_9^9x_{10}^9$	$2^5 \cdot 7 \cdot 11^2 \cdot 21966239$ $2 \cdot 13 \cdot 211 \cdot 256046627$
$(9,1)$	$(0,0,0,0,0,1,0,0,0,0)$	52	$x_2^2x_3^4x_4^7x_5^8x_7^7x_8^8x_9^8x_{10}^8$	$-1 \cdot 2^2$
$(8,2)$	$(0,1,0,0,0,0,1,0,0,0)$	45	$x_1x_3x_4^7x_5^7x_6^7x_7x_8^7x_9^7x_{10}^7$	$-1 \cdot 2 \cdot 3 \cdot 7$
$(7,3)$	$(0,0,0,0,1,0,0,0,1,1)$	42	$x_2^6x_3^6x_4^6x_5^2x_6^6x_7^6x_8^6x_9^2x_{10}^2$	$-1 \cdot 2 \cdot 3 \cdot 7$
$(6,4)$	$(0,0,0,1,0,0,0,1,1,1)$	39	$x_1^5x_2^5x_3^5x_4^3x_5^5x_6^5x_7^3x_8^3x_9^3x_{10}^2$	$2 \cdot 5$
$(5,5)$	$(0,0,0,1,0,0,1,1,1,1)$ $(0,1,0,1,0,1,0,1,0,1)$	40 40	$x_1^4x_2^4x_3^4x_4^4x_5^4x_6^4x_7^4x_8^4x_9^4x_{10}^4$ $x_1^4x_2^4x_3^4x_4^4x_5^4x_6^4x_7^4x_8^4x_9^4x_{10}^4$	$2^2 \cdot 157$ $5 \cdot 19 \cdot 41 \cdot 83$
$(4,6)$	$(0,1,0,1,1,1,1,0,1,0)$	41	$x_1^2x_2^5x_3^3x_4^5x_5^5x_6^5x_7^5x_8^3x_9^5x_{10}^3$ $x_1^3x_2^4x_3^3x_4^5x_5^5x_6^5x_7^5x_8^3x_9^5x_{10}^3$	$2^4 \cdot 3 \cdot 5 \cdot 13$ $2 \cdot 3 \cdot 463$
$(3,7)$	$(0,0,1,0,1,1,1,1,1,1)$	46	$x_2^2x_3^6x_4^2x_5^6x_6^6x_7^6x_8^6x_9^6x_{10}^6$	$-1 \cdot 2^3 \cdot 3^2$
$(2,8)$	$(0,1,0,1,1,1,1,1,1,1)$	51	$x_1x_2x_3x_4^6x_5^7x_6^7x_7^7x_8^7x_9^7x_{10}^7$ $x_1x_3x_4^7x_5^7x_6^7x_7^7x_8^7x_9^7x_{10}^7$	$-1 \cdot 2 \cdot 1277$ $-1 \cdot 2 \cdot 17^2$
$(1,9)$	$(1,0,1,1,1,1,1,1,1,1)$	60	$x_1^2x_3^2x_4^8x_5^8x_6^8x_7^8x_8^8x_9^8x_{10}^8$ $x_1^2x_3^3x_4^7x_5^8x_6^8x_7^8x_8^8x_9^8x_{10}^8$	$2 \cdot 17^2$ $2^2 \cdot 647$
$(0,10)$	$(1,1,1,1,1,1,1,1,1,1)$	69	$x_1^2x_2^2x_3^4x_4^7x_5^9x_6^9x_7^9x_8^9x_9^9x_{10}^9$ $x_1^2x_2^2x_3^4x_4^9x_5^7x_6^9x_7^9x_8^9x_9^9x_{10}^9$	$2 \cdot 3 \cdot 733$ $2^5 \cdot 3^2 \cdot 5$

Appendix

We report here the full SageMath code used to provide the results of the previous section.

```
import numpy as np
import gc
import math
import time

def poldeg(seq_type,qs,bs):
    deg = 0
    occ = np.zeros(k, dtype=int)
    for i in range(0, k-1):
        for j in range(i+1, k):
            if qs[j] == qs[i]:
                occ[i] = occ[i] + 1
                occ[j] = occ[j] + 1
                deg = deg + 1
            if bs[j+1] == bs[i] and (i != 0 or j != k-1):
                for l in range(i, j+1):
                    occ[l] = occ[l] + 1
                deg = deg + 1
    return deg, occ

def remTerms(f, ubound, occs):
    R = f.parent()
    d = f.dict()
    k = len(ubound)
    dd = {ee: c for ee, c in d.items() if all(ee[i] <= ubound[i] and
          ee[i] >= ubound[i]-occs[i] for i in range(0, k))}
    return R(dd)

k = 10
dataset = {"(6,4)": {"(0,0,0,1,0,0,0,1,1,1)":
                     {"(5,5,5,3,5,5,3,3,3,2)": 10}}}
R = PolynomialRing(ZZ,k,"x")
vars = R.gens()
print("Variables: ", vars, "\n")

allCorrect = True

for typ, coset in dataset.items():

    seq_type = [int(x) for x in typ.strip(')][(').split(',')]
    t = len(seq_type)
    print("Type: ", seq_type, "\n")

    for qseq, monomials in coset.items():
        qs = [int(x) for x in qseq.strip(')][(').split(',')]
        seq_test = [qs.count(i) for i in range(0, t)]
```

```
        bs = np.mod(np.cumsum(qs), t)
        bs = np.insert(bs, 0, 0)
        pdeg, occs = poldeg(seq_type, qs, bs)
        print("Quotient sequence: ", qs)
        print("Cumsum quotient sequence: ", bs)
        print("Polynomial degree: ", pdeg)
        print("Variables occurrence: ", occs)

        for monomial, coeff in monomials.items():
            coccs = occs.copy()
            bounding_exponents =
                    [int(x) for x in monomial.strip(')][(').split(',')]
            print("Exponents of the monomial: ", bounding_exponents)
            check_degree = True
            for i in range(0, k):
                if bounding_exponents[i] > seq_type[qs[i]]-1:
                    check_degree = False
                    break
            p = 1
            nitems = 0
            for i in range(0, k-1):
                for j in range(i+1, k):
                    remove = False
                    f1 = 1
                    f2 = 1
                    if qs[j] == qs[i]:
                        f1 = (vars[j] - vars[i])
                        coccs[i] = coccs[i] - 1
                        coccs[j] = coccs[j] - 1
                        remove = True
                        nitems = nitems + 1
                    if bs[j+1] == bs[i] and (i != 0 or j != k-1):
                        f2 = sum(vars[k] for k in range(i, j+1))
                        for l in range(i, j+1):
                            coccs[l] = coccs[l] - 1
                        remove = True
                        nitems = nitems + 1
                    ff = f1 * f2
                    p = p * ff
                    if remove == True:
                        p = remTerms(p, bounding_exponents, coccs)
            print("Monomial: ", p)
            pcoeff = p.lc()
            print("Coefficient: ", factor(pcoeff))
            testcorr = (p.total_degree() == pdeg and coeff == pcoeff and
                        seq_type==seq_test and check_degree)
            print("Is correct? ", testcorr, "\n")
            allCorrect = allCorrect and testcorr
```

6.3. Weak sequenceability in cyclic groups

6.3.1. Preliminaries. We recall and change, for notational convenience, some definitions and notation used in Section 6.2. Let G be an abelian group and let A be a subset of $G \setminus \{0\}$ whose cardinality is equal to k. Let $\boldsymbol{\omega} = (a_1, a_2, \ldots, a_k)$ be an ordering of the elements of A and we define its partial sums $\boldsymbol{s} = (s_0, s_1, \ldots, s_k)$ by $s_0 = 0$ and $s_i = a_1 + \cdots + a_i$ for $i > 0$. We denote the sum of the elements of A by ΣA. As G is abelian, for any ordering of the elements of A the final partial sum s_k is equal to ΣA. Then, as done in Section 6.2, we give the following definitions.

Definition 6.3.1.

- *The ordering $\boldsymbol{\omega}$ is said to be a* sequencing *(or a* linear sequencing*) of A if the elements of $\boldsymbol{s}$ are distinct;*
- *the ordering $\boldsymbol{\omega}$ is said to be an* R-sequencing *(or a* rotational sequencing*) of A if the elements of $\boldsymbol{s}$ are distinct with the exception that $s_0 = 0 = s_k$;*
- *a subset A of an abelian group is said to be* sequenceable *if it admits a sequencing or an R-sequencing;*
- *an abelian group G is said to be* strongly sequenceable *if every subset A of $G \setminus \{0\}$ is sequenceable.*

We remark that a set A can have a linear sequencing only if $\Sigma A \neq 0$. On the other hand, A can have a rotational sequencing only when $\Sigma A = 0$.

Inspired by the graph-theoretical interpretation, we propose the following weakening of the concept of sequenceability.

Definition 6.3.2.

- *Given a positive integer t and a set A whose cardinality is $k > t$, the ordering $\boldsymbol{\omega}$ is said to be a* t-weak sequencing *of A if the elements of $\boldsymbol{s} = (s_0, s_1, \ldots, s_k)$ are such that $s_i \neq s_j$ whenever $i \neq j$ and $|i - j| \leq t$;*
- *a subset A of an abelian group is said to be* t-weakly sequenceable *if it admits a t-weak sequencing;*
- *an abelian group G is said to be* strongly t-weakly sequenceable *if every subset A of $G \setminus \{0\}$ whose cardinality is bigger than t is t-weakly sequenceable.*

Note that this notion is related with that of sequenceability of triple systems introduced in [11] and [89] (see also [48] and the references therein).

Here, if a set A admits a t-weak sequencing and $\Sigma A \neq 0$, then the partial sums $(s_0, s_1, \ldots, s_k)$ define a walk in $Cay[G : \pm A]$ whose girth is strictly bigger than t. Exploiting this interpretation, we can state the analogy of Conjecture 6.1.1 for weak sequenceability.

Conjecture 6.3.1. *Let t be a positive integer, G be an abelian group and let A be a finite subset of $G \setminus \{0\}$ whose cardinality is $k > t$. Then A is t-weakly sequenceable. Equivalently, we conjecture that any abelian group G is strongly t-weakly sequenceable.*

Then, as done with Conjecture 6.1.1, we propose a variation of Conjecture 6.1.2 for the weak sequenceability.

Conjecture 6.3.2. *Let t be a positive integer, G be an abelian group and let A be a finite subset of $G \setminus \{0\}$ such that $|A \cap \{x, -x\}| \leq 1$ for any $x \in G$ and $|A| > t$. Then A is t-weakly sequenceable.*

In this section, we will work on these weak forms of Conjectures 6.1.1 and 6.1.2. In particular, when G is the field $\mathbb{Z}_p$, we will use a polynomial approach whose starting point is the same as [84]. Here, after some manipulations, we surprisingly obtain a polynomial whose expression does not depend on the cardinality of A and this allows us to have a result that is very general on the parameter $k = |A|$. On the other hand, since the degree of this polynomial increases very quickly in t, we can resolve computationally, using SageMath [55], only the cases where t is smaller than 7 and 8, respectively, for Conjectures 6.3.1 and 6.3.2. These results will be presented in Subsection 6.3.2. We also remark that the polynomial method provides better results than the ones that can be obtained by using the direct construction. Indeed, in the third subsection of this section we will show how a direct approach, similar to that of [40], can effectively solve only very small values of t: we can prove, directly and with a great effort, Conjectures 6.3.1 and 6.3.2 only when t is smaller respectively than 4 and 5.

Finally, in the last subsection, we will outline a probabilistic approach. We will start from the result of [13] that almost all the sets are sequenceable (fixed $|A|$ and asymptotically in $|G|$) and we will prove the existence of sequences that are not too far from being t-weak sequencings.

6.3.2. Applying the polynomial method. In this subsection, we apply a method that relies on the Non-Vanishing Corollary of the Combinatorial Nullstellensatz, see Theorem 6.2.2. Given a prime p (in the following p will be always assumed to be a prime), this corollary allows us to obtain a non-zero point to suitable polynomials on $\mathbb{Z}_p$ derived starting from the ones defined in [84]. Then, after some manipulations, surprisingly, we obtain a polynomial whose expression does not depend on the cardinality of A and this allows us to have a result that is very general on the parameter $k = |A|$.

In the notation of the Non-Vanishing Corollary, we call the monomial $x_1^{|C_1|-1} \cdots x_k^{|C_k|-1}$ the *bounding monomial*. The corollary can be rephrased as requiring the polynomial to include a monomial of maximum degree that divides the bounding monomial (where by "include" we mean that it has a nonzero coefficient).

To use the Non-Vanishing Corollary we require a polynomial for which the non-zeros correspond to successful solutions to the case of the problem under consideration. We recall that in order to attack Conjecture 6.1.1, the following polynomial was defined in [84]:

$$F_k(x_1, \cdots, x_k) := \prod_{1 \le i < j \le k} (x_j - x_i) \prod_{\substack{0 \le i < j \le k \\ j \ne i+1, (i,j) \ne (0,k)}} (x_{i+1} + \cdots + x_j).$$

It is clear that, given $A = \{a_1, \ldots, a_k\} \subseteq \mathbb{Z}_p \setminus \{0\}$ of cardinality k, $F_k(a_1, \ldots, a_k) \ne 0$ if and only if the sequence $(a_1, \ldots, a_k)$ is a solution to Conjecture 6.1.1 for the set A. In other words A is sequenceable if and only if there exists an ordering that we denote, up to relabeling, with $(a_1, \ldots, a_k)$ such that $F_k(a_1, \ldots, a_k) \ne 0$.

6.3.2.1. *Polynomial method for Conjecture 6.3.1.* In addition to requiring that $x_i - x_j \ne 0$ for $1 \le i < j \le k$, we seek an ordering to have no two of its partial sums s_i, s_j equal for $1 \le i < j \le k$ and $|i - j| \le t$ (here there is the weakening of Conjecture 6.1.1). Hence, modifying the expression of F_k, we define, for $t < k$, the following polynomial:

$$P_{k,t}(x_1, \cdots, x_k) := \prod_{1 \le i < j \le k} (x_j - x_i) \prod_{\substack{0 \le i < j \le k \\ j - i \le t, j \ne i+1}} (x_{i+1} + \cdots + x_j).$$

In this case we have that a set $A = \{a_1, \dots, a_k\} \subseteq \mathbb{Z}_p$ of cardinality k is t-weakly sequenceable if and only if there exists an ordering $(a_1, \dots, a_k)$ of its elements such that $P_{k,t}(a_1, \dots, a_k) \neq 0$.

Now, given a set $A = \{a_1, \dots, a_k\}$ of k elements, the idea is to fix, *a priori*, the first h elements $(a_1, \dots, a_h)$, where h is not too big, of the ordering in such a way that none of its partial sums s_i, s_j are equal for $1 \leq i < j \leq h$ and $|i - j| \leq t$. This can be expressed by requiring that $P_{h,t}(a_1, \cdots, a_h) \neq 0$ and we show that this can be done under the hypothesis of the following Proposition.

PROPOSITION 6.3.1. *Let $A = \{a_1, \dots, a_k\} \subseteq \mathbb{Z}_p \setminus \{0\}$ be a set of cardinality k and let h and t be positive integers such that $h \leq k - (t-1)$. Then there exists an ordering of h-elements of A that we denote, up to relabeling, with $(a_1, \dots, a_h)$, such that*

$$P_{h,t}(a_1, \cdots, a_h) \neq 0.$$

PROOF. Given k and t, we prove this statement by induction on h.

BASE CASE: Let $h = 1$. Since $P_{1,t}(x) = 1$ for any t and for any $x \in A$, the statement is realized for $h = 1$.

INDUCTIVE CASE: Let us assume the statement for $h \in \{1, \dots, m\}$ and let us prove it for $h = m + 1$ where $m + 1 \leq k - (t-1)$. Since the statement is true for $h = m$, there exists an m-tuple $(a_1, \dots, a_m)$ such that

$$P_{m,t}(a_1, \cdots, a_m) \neq 0.$$

We note that

$$\frac{P_{m+1,t}(a_1, \dots, a_m, x)}{P_{m,t}(a_1, \dots, a_m)} = \prod_{1 \leq i < m+1} (x - a_i) \prod_{\substack{0 \leq i < m \\ m+1-i \leq t}} (a_{i+1} + \cdots + a_m + x).$$

Here, any element x of $A \setminus \{a_1, \dots, a_m\}$ satisfies $\prod_{1 \leq i < m+1}(x - a_i) \neq 0$. Hence, to have $\frac{P_{m+1,t}(a_1,\dots,a_m,x)}{P_{m,t}(a_1,\dots,a_m)} \neq 0$, it suffice to find x such that $\prod_{\max(0,m+1-t) \leq i < m}(a_{i+1} + \cdots + a_m + x) \neq 0$.

Note that for each relation $a_{i+1} + \cdots + a_m + x = 0$ there is at most one solution $x \in A \setminus \{a_1, \dots, a_m\}$. Since those relations are at most $t - 1$, we have at most $t - 1$ values x in $A \setminus \{a_1, \dots, a_m\}$ such that $\prod_{\max(0,m+1-t) \leq i < m}(a_{i+1} + \cdots + a_m + x) = 0$. We recall that $m + 1 \leq k - (t-1)$ that is

$$|A \setminus \{a_1, \dots, a_m\}| = k - m \geq t > t - 1.$$

This means that there exists $a_{m+1} \in A \setminus \{a_1, \dots, a_m\}$ such that

$$\frac{P_{m+1,t}(a_1, \dots, a_m, a_{m+1})}{P_{m,t}(a_1, \dots, a_m)} = \prod_{1 \leq i < m+1} (a_{m+1} - a_i) \prod_{\max(0,m+1-t) \leq i < m} (a_{i+1} + \cdots + a_{m+1}) \neq 0.$$

Since $\mathbb{Z}_p$ is a field and due to the inductive hypothesis $P_{m,t}(a_1, \dots, a_m) \neq 0$, we also have that

$$\frac{P_{m+1,t}(a_1, \dots, a_m, a_{m+1})}{P_{m,t}(a_1, \dots, a_m)} \cdot P_{m,t}(a_1, \dots, a_m) = P_{m+1,t}(a_1, \dots, a_{m+1}) \neq 0$$

which completes the proof. □

In the following we assume that we have fixed, according to Proposition 6.3.1, $\{a_1, \dots, a_h\} \subseteq A$ such that $P_{h,t}(a_1, \dots, a_h) \neq 0$. We note that every $x \in A \setminus \{a_1, \dots, a_h\}$ is such

that $x - a_i \neq 0$ for any $i \in \{1, \dots, h\}$. Therefore, it is left to find a nonzero point for the polynomial

$$\frac{P_{k,t}(a_1, \dots, a_h, x_{h+1}, \dots, x_k)}{P_{h,t}(a_1, \dots, a_h) \prod_{1 \leq i \leq h < j \leq k} (x_j - a_i)}.$$

Since the free variables are now $x_{h+1}, \dots, x_k$, we set $\ell := k - h$ and $y_i := x_{i+h}$; here the constraint $h \leq k - (t-1)$ of Proposition 6.3.1 becomes $\ell \geq t - 1$. Then we denote by $H_{k,t,\ell}$ the polynomial

$$H_{k,t,\ell}(y_1, \dots, y_\ell) := \frac{P_{k,t}(a_1, \dots, a_{k-\ell}, y_1, \dots, y_\ell)}{P_{k-\ell,t}(a_1, \dots, a_{k-\ell}) \prod_{1 \leq i \leq k-\ell;\ 1 \leq j \leq \ell} (y_j - a_i)}. \tag{101}$$

Assuming now that $k - \ell \geq t - 1$, that is, $k - (t-1) \geq \ell \geq t - 1$, we obtain the following expression:

$$H_{k,t,\ell}(y_1, \cdots, y_\ell) =$$

$$P_{\ell,t}(y_1, \dots, y_\ell) \prod_{0 \leq i \leq t-1;\ 1 \leq j \leq t-i-1} (a_{k-\ell} + a_{k-\ell-1} + \cdots + a_{k-\ell-i} + y_1 + y_2 + \cdots + y_j). \tag{102}$$

Now our aim is to apply the Non-Vanishing Corollary (i.e. Theorem 6.2.2) to the polynomial $H_{k,t,\ell}$. For this purpose it is enough to consider the terms of $H_{k,t,\ell}$ of maximal degree in the variables $y_1, \dots, y_\ell$ that are the ones where no a_i appears. We denote by $Q_{k,t,\ell}$ the polynomial given by those terms, that is,

$$Q_{k,t,\ell} := P_{\ell,t}(y_1, \dots, y_\ell) \prod_{\substack{0 \leq i \leq t-1 \\ 1 \leq j \leq t-i-1}} (y_1 + y_2 + \cdots + y_j). \tag{103}$$

Now we can state the following simple but very powerful remark.

REMARK 6.3.1. *The expression of $Q_{k,t,\ell}$ does not depend on k. In the following, we just denote this polynomial by $Q_{t,\ell}$.*

Indeed Remark 6.3.1 means that, after these manipulations, we are left to consider a polynomial that does not depend on $k = |A|$ and hence we have chances to get a result that is very general on k.

To apply the Non-Vanishing Corollary, we also need to know the degree of $Q_{t,\ell}$ (and hence that of $H_{k,t,\ell}$) in order to compare it with the one of the bounding monomial.

LEMMA 6.3.1. *We have*

$$\deg(Q_{t,\ell}) = (t-1)\ell + \frac{\ell(\ell-1)}{2}.$$

PROOF. It is more convenient to consider the degree of the polynomial $H_{k,t,\ell}$ defined in eq. (102) since that of $Q_{t,\ell}$ is the same.

We note that in $H_{k,t,\ell}$, each variable y_j is the ending point of $t-1$ terms whose length is $i+1$ and that are of the form $(y_j + y_{j-1} + \cdots + y_{j-i})$ or, if $i \geq j$, $(y_j + y_{j-1} + \cdots + y_1 + a_{k-\ell} + \cdots + a_{k-\ell-(i-j)})$.

The other terms of $H_{k,t,\ell}$ are those of the form $(y_j - y_i)$ where $\ell \geq j > i \geq 1$. Therefore we have that

$$\deg(H_{k,t,\ell}) = (t-1)\ell + \frac{\ell(\ell-1)}{2}.$$

□

To apply Theorem 6.2.2 we need to find a nonzero coefficient of some monomials of type $\prod_{i=1}^{\ell} y_i^{\gamma_i}$ in $Q_{t,\ell}$ where each γ_i is smaller than the number of choices for y_i, i.e. $\gamma_i \leq \ell - 1$. Note that this is possible only if $\deg(Q_{t,\ell}) \leq \ell(\ell-1)$: indeed this is the degree of the bounding monomial. Therefore we need that

$$(t-1)\ell + \frac{\ell(\ell-1)}{2} \leq \ell(\ell-1),$$

that is, $2t - 1 \leq \ell$. Recalling that we are assuming $k - (t-1) \geq \ell \geq t-1$, the conditions on ℓ to apply Theorem 6.2.2 to the polynomial $H_{k,t,\ell}$ defined in eq. (102) are that

$$k - (t-1) \geq \ell \geq 2t - 1. \tag{104}$$

From the previous discussion, it follows that

PROPOSITION 6.3.2. *Let t, ℓ be positive integers such that $\ell \geq 2t-1$. Let us also suppose that the coefficient of $\Pi_{i=1}^{\ell} y_i^{\gamma_i}$ in $Q_{t,\ell}$ is nonzero in $\mathbb{Z}_p$ where $\gamma_i \leq \ell - 1$ for every $i \in \{1, \ldots, \ell\}$.*

Then, any subset A of $\mathbb{Z}_p \setminus \{0\}$ whose cardinality is $k \geq \ell + (t-1)$ is t-weakly sequenceable.

REMARK 6.3.2. *Since to apply Proposition 6.3.1 we need $\ell \geq t-1$, it is not guaranteed that we can find ℓ such that $k - \ell \geq t - 1$. If this condition it is not satisfied, we can still define the polynomial $H_{k,t,\ell}$ via equation* (101) *even though equations* (102) *and* (103) *do not hold. Then, since given t those cases are only a finite number, we can apply directly the Non-Vanishing Corollary to equation* (101).

Now we are ready to prove the main result of this subsection

THEOREM 6.3.1. *Let $t \leq 6$ be a positive integer, then for any prime p the field $\mathbb{Z}_p$ is strongly t-weakly sequenceable.*

PROOF. Since a strongly t-weakly sequenceable group is also strongly $(t-1)$-weakly sequenceable, we can suppose that $t = 6$. By [45] we know that each subset $A \subseteq \mathbb{Z}_p \setminus \{0\}$ of cardinality $k \leq 12$ is sequenceable, therefore we can suppose that $k \geq 13$. We divide the proof considering two different ranges of k.

For each $13 \leq k \leq 15$ and for $k = 16$ when p is coprime with $379 \cdot 167938950753577$, the polynomial $H_{k,t,\ell}$, defined in eq. (101), for $\ell \in \{2t-1, 2t\}$ has monomials with non-zero coefficients that divide the bounding monomial $y_1^{\ell-1} y_2^{\ell-1} \cdots y_\ell^{\ell-1}$ (see Table 2). Then thanks to the Non-Vanishing Corollary each subset $A \subseteq \mathbb{Z}_p$, $|A| \leq 15$ (or 16 under the above assumption), is sequenceable.

For $k \geq 17$ and for $k = 16$ when p is coprime with $3^4 \cdot 5 \cdot 47 \cdot 97 \cdot 271 \cdot 15985681$, we consider the polynomials $Q_{t,\ell}$ defined in eq. (103) for $\ell \in \{11, 12\}$. Since these polynomials have monomials that divide the bounding monomial with non-zero coefficients (see Table 3), and since $k \geq \ell + t - 1$, we can apply Proposition 6.3.2 to obtain that each subset $A \subseteq \mathbb{Z}_p$, $|A| \geq 17$ (or 16 under the above assumption), is sequenceable. □

TABLE 2. Monomials and their coefficients sufficient for the proof of Theorem 6.3.1 in the case $A \subseteq \mathbb{Z}_p$, $|A| \leq 16$.

k	ℓ	deg	monomial/s	coefficient/s
16	12	125	$y_1^5 y_2^{10} y_3^{11} y_4^{11} y_5^{11} y_6^{11} y_7^{11} y_8^{11} y_9^{11} y_{11}^{11} y_{11}^{11} y_{12}^{11}$	$-379 \cdot 167938950753577$
15	11	109	$y_1^9 y_2^{10} y_3^{10} y_4^{10} y_5^{10} y_6^{10} y_7^{10} y_8^{10} y_9^{10} y_{10}^{10} y_{11}^{10}$	$-3^4 \cdot 5 \cdot 47 \cdot 97 \cdot 271 \cdot 15985681$
			$y_1^{10} y_2^9 y_3^{10} y_4^{10} y_5^{10} y_6^{10} y_7^{10} y_8^{10} y_9^{10} y_{10}^{10} y_{11}^{10}$	$-2^2 \cdot 3 \cdot 401 \cdot 1305987719053$

14	11	107	$y_1^7y_2^{10}y_3^{10}y_4^{10}y_5^{10}y_6^{10}y_7^{10}y_8^{10}y_9^{10}y_{10}^{10}y_{11}^{10}$	$-2^2\cdot 3\cdot 5\cdot 7^2\cdot 37\cdot 433\cdot 81945547$
			$y_1^8y_2^9y_3^{10}y_4^{10}y_5^{10}y_6^{10}y_7^{10}y_8^{10}y_9^{10}y_{10}^{10}y_{11}^{10}$	$-3\cdot 5\cdot 555349\cdot 496867859$
13	11	104	$y_1^5y_2^9y_3^{10}y_4^{10}y_5^{10}y_6^{10}y_7^{10}y_8^{10}y_9^{10}y_{10}^{10}y_{11}^{10}$	$-2\cdot 11\cdot 946021\cdot 34341337$
			$y_1^6y_2^8y_3^{10}y_4^{10}y_5^{10}y_6^{10}y_7^{10}y_8^{10}y_9^{10}y_{10}^{10}y_{11}^{10}$	$-7\cdot 211\cdot 73019\cdot 7962769$

TABLE 3. Monomials and their coefficients sufficient for the proof of Theorem 6.3.1 in the case $A\subseteq\mathbb{Z}_p$, $|A|\geq 16$

ℓ	deg	monomial/s	coefficient/s
11	110	$y_1^{10}y_2^{10}y_3^{10}y_4^{10}y_5^{10}y_6^{10}y_7^{10}y_8^{10}y_9^{10}y_{10}^{10}y_{11}^{10}$	$-3^4\cdot 5\cdot 47\cdot 97\cdot 271\cdot 15985681$
12	126	$y_1^6y_2^{10}y_3^{11}y_4^{11}y_5^{11}y_6^{11}y_7^{11}y_8^{11}y_9^{11}y_{11}^{11}y_{11}^{11}y_{12}^{11}$	$-379\cdot 167938950753577$

6.3.2.2. *Polynomial method for Conjecture 6.3.2.* We recall that, in order to attack Conjecture 6.1.2, in [84] the following polynomial was defined:

$$\overline{F}_k(x_1,\cdots,x_k):=\frac{F_k(x_1,\cdots,x_k)}{\prod_{1\leq i<k}(x_i+x_{i+1})}.$$

Indeed, given $A=\{a_1,\ldots,a_k\}\subseteq\mathbb{Z}_p\setminus\{0\}$ of cardinality k and such that $|A\cap\{x,-x\}|\leq 1$ for any $x\in\mathbb{Z}_p$, we do not need to impose that x_i+x_{i+1} is different from zero. Therefore $\overline{F}_k(a_1,\ldots,a_k)\neq 0$ if and only if the sequence $(a_1,\ldots,a_k)$ is a solution to Conjecture 6.1.2 for the set A. Under the above assumptions, we can also say that A is sequenceable if and only if there exists an ordering that we denote, up to relabeling, with $(a_1,\ldots,a_k)$ such that $\overline{F}_k(a_1,\ldots,a_k)\neq 0$.

Reasoning in a similar way, with respect to Conjecture 6.3.2, we define, for $t<k$, the following polynomial:

$$\overline{P}_{k,t}(x_1,\cdots,x_k):=\frac{P_{k,t}(x_1,\cdots,x_k)}{\prod_{1\leq i<k}(x_i+x_{i+1})}.$$

In this case we have that a set $A=\{a_1,\ldots,a_k\}\subseteq\mathbb{Z}_p$ of cardinality k and such that $|A\cap\{x,-x\}|\leq 1$ for any $x\in\mathbb{Z}_p$ is t-weakly sequenceable if and only if there exists an ordering $(a_1,\ldots,a_k)$ of its elements such that $\overline{P}_{k,t}(a_1,\ldots,a_k)\neq 0$.

Then, with the same proof of Proposition 6.3.1, and keeping in mind that we do not need to impose that $x_i+x_{i+1}\neq 0$, we obtain the next result.

PROPOSITION 6.3.3. *Let $A=\{a_1,\ldots,a_k\}\subseteq\mathbb{Z}_p\setminus\{0\}$ be a set of cardinality k such that $|A\cap\{x,-x\}|\leq 1$ for any $x\in\mathbb{Z}_p$, and let h and t be positive integers. Then, if $h\leq k-(t-2)$, there exists an ordering of h-elements of A that we denote, up to relabeling, with $(a_1,\ldots,a_h)$, such that*

$$\overline{P}_{h,t}(a_1,\cdots,a_h)\neq 0.$$

Here we can assume that we have fixed, according to Proposition 6.3.3, $\{a_1,\ldots,a_h\}\subseteq A$ such that $\overline{P}_{h,t}(a_1,\ldots,a_h)\neq 0$. Then, proceeding as we did with Conjecture 6.3.1, we have that if we set $\ell=k-h$ and $\ell\geq t-2$ it is enough to find $y_1,\ldots,y_\ell$ in $A\setminus\{a_1,\ldots,a_{k-\ell}\}$ such that $\overline{H}_{k,t,\ell}(y_1,\ldots,y_\ell)\neq 0$, where

$$\overline{H}_{k,t,\ell}(y_1,\ldots,y_\ell):=\frac{H_{k,t,\ell}(y_1,\ldots,y_\ell)}{(y_1+a_{k-\ell})\prod_{1\leq i<k}(y_i+y_{i+1})}. \tag{105}$$

Assuming now that $k-\ell \geq t-1$, that is, $k-(t-1) \geq \ell \geq t-2$, we obtain the following expression:

$$\overline{H}_{k,t,\ell}(y_1, \cdots, y_\ell) =$$

$$\overline{P}_{\ell,t}(y_1, \ldots, y_\ell) \prod_{\substack{0 \leq i \leq t-1;\ 1 \leq j \leq t-i-1 \\ i+j>1}} (a_{k-\ell} + a_{k-\ell-1} + \cdots + a_{k-\ell-i} + y_1 + y_2 + \cdots + y_j). \tag{106}$$

Here our aim is to apply the Non-Vanishing Corollary (i.e. Theorem 6.2.2) to the polynomial $\overline{H}_{k,t,\ell}$. For this purpose it is enough to consider the terms of $\overline{H}_{k,t,\ell}$ of maximal degree in the variables $y_1, \ldots, y_\ell$ which are those where no a_i appears. We denote by $\overline{Q}_{k,t,\ell}$ the polynomial given by those terms, that is,

$$\overline{Q}_{k,t,\ell} := \overline{P}_{\ell,t}(y_1, \ldots, y_\ell) \prod_{\substack{0 \leq i \leq t-1;\ 1 \leq j \leq t-i-1 \\ i+j>1}} (y_1 + y_2 + \cdots + y_j). \tag{107}$$

Also in this case we can state this simple but very powerful remark.

Remark 6.3.3. *The expression of $\overline{Q}_{k,t,\ell}$ does not depend on k. In the following, we just denote this polynomial by $\overline{Q}_{t,\ell}$.*

In this case the degree of $\overline{Q}_{t,\ell}$ (and that of $\overline{H}_{k,t,\ell}$) is

$$\deg(\overline{Q}_{t,\ell}) = (t-2)\ell + \frac{\ell(\ell-1)}{2}.$$

This means that in order to apply the Non-Vanishing Corollary (i.e. Theorem 6.2.2) to the polynomial $\overline{H}_{k,t,\ell}$ defined in eq. (106), we need that

$$k-(t-1) \geq \ell \geq 2t-3. \tag{108}$$

From the previous discussion, we obtain the next result.

Proposition 6.3.4. *Let t, ℓ be positive integers such that $\ell \geq 2t-3$. Let us also suppose that the coefficient of $\Pi_{i=1}^{\ell} y_i^{\gamma_i}$ in $\overline{Q}_{t,\ell}$ is nonzero in $\mathbb{Z}_p$, where $\gamma_i \leq \ell - 1$ for every $i \in \{1, \ldots, \ell\}$.*

Then any subset A of $\mathbb{Z}_p \setminus \{0\}$ such that $|A \cap \{x, -x\}| \leq 1$ for every $x \in \mathbb{Z}_p$ and whose cardinality is $k \geq \ell + (t-1)$ is t-weakly sequenceable.

Now we are ready to prove our main result about Conjecture 6.3.2

Theorem 6.3.2. *Let $t \leq 7$ be a positive integer and A be a finite subset of $\mathbb{Z}_p \setminus \{0\}$ such that $|A \cap \{x, -x\}| \leq 1$ for any $x \in \mathbb{Z}_p$ and $|A| > t$. Then A is t-weakly sequenceable.*

Proof. Since a t-weakly sequenceable set A is also $(t-1)$-weakly sequenceable, we can suppose that $t = 7$. By [45] we know that each subset $A \subseteq \mathbb{Z}_p \setminus \{0\}$ of cardinality $k \leq 12$ is sequenceable, therefore we can assume that $k \geq 13$ and thus $p > 13$. We divide the proof considering two different ranges of k.

For each $13 \leq k \leq 16$ and for $k = 17$ when p is coprime with $2 \cdot 7 \cdot 13 \cdot 4679 \cdot 3953841444019$, the polynomial $\overline{H}_{k,t,\ell}$, defined in eq. (105), for $\ell \in \{2t-3, 2t-2\}$ has monomials with non-zero coefficients that divide the bounding monomial $y_1^{\ell-1} y_2^{\ell-1} \cdots y_\ell^{\ell-1}$ (see Table 4). Then thanks to the Non-Vanishing Corollary each subset $A \subseteq \mathbb{Z}_p \setminus \{0\}$, $|A| \leq 16$ (or 17 under the assumption above), that satisfies the hypothesis of Theorem 6.3.2, is sequenceable.

For $k \geq 18$ and for $k = 17$ when p is coprime with $13 \cdot 67 \cdot 451441944254443$, we consider the polynomials $\overline{Q}_{t,\ell}$ defined in eq. (107) for $\ell \in \{11, 12\}$. Since these polynomials have

monomials that divide the bounding monomial with non-zero coefficients (see Table 5), and since $k \geq \ell + t - 1$, we can apply Proposition 6.3.4 to prove Theorem 6.3.2 for $k \geq 18$ (or 17 under the assumption above). □

TABLE 4. Monomials and their coefficients sufficient for the proof of Theorem 6.3.1 in the case $A \subseteq \mathbb{Z}_p$, $|A| \leq 17$.

k	ℓ	deg	monomial/s	coefficient/s
17	12	125	$y_1^5y_2^{10}y_3^{11}y_4^{11}y_5^{11}y_6^{11}y_7^{11}y_8^{11}y_9^{11}y_{11}^{11}y_{11}^{11}y_{12}^{11}$	$2 \cdot 7 \cdot 13 \cdot 4679 \cdot 3953841444019$
16	11	109	$y_1^9y_2^{10}y_3^{10}y_4^{10}y_5^{10}y_6^{10}y_7^{10}y_8^{10}y_9^{10}y_{10}^{10}y_{11}^{10}$	$13 \cdot 67 \cdot 451441944254443$
			$y_1^{10}y_2^9y_3^{10}y_4^{10}y_5^{10}y_6^{10}y_7^{10}y_8^{10}y_9^{10}y_{10}^{10}y_{11}^{10}$	$3^2 \cdot 281 \cdot 1163 \cdot 112116705839$
15	11	107	$y_1^7y_2^{10}y_3^{10}y_4^{10}y_5^{10}y_6^{10}y_7^{10}y_8^{10}y_9^{10}y_{10}^{10}y_{11}^{10}$	$2^2 \cdot 59 \cdot 708923 \cdot 1059330263$
			$y_1^8y_2^9y_3^{10}y_4^{10}y_5^{10}y_6^{10}y_7^{10}y_8^{10}y_9^{10}y_{10}^{10}y_{11}^{10}$	$7 \cdot 149 \cdot 239 \cdot 4073 \cdot 212718109$
14	11	104	$y_1^5y_2^9y_3^{10}y_4^{10}y_5^{10}y_6^{10}y_7^{10}y_8^{10}y_9^{10}y_{10}^{10}y_{11}^{10}$	$2^3 \cdot 41 \cdot 7682093 \cdot 13267117$
			$y_1^6y_2^8y_3^{10}y_4^{10}y_5^{10}y_6^{10}y_7^{10}y_8^{10}y_9^{10}y_{10}^{10}y_{11}^{10}$	$2^2 \cdot 16834339 \cdot 679071929$
13	11	100	$y_1^2y_2^8y_3^{10}y_4^{10}y_5^{10}y_6^{10}y_7^{10}y_8^{10}y_9^{10}y_{10}^{10}y_{11}^{10}$	$3^3 \cdot 708569 \cdot 33345973$
			$y_1^3y_2^7y_3^{10}y_4^{10}y_5^{10}y_6^{10}y_7^{10}y_8^{10}y_9^{10}y_{10}^{10}y_{11}^{10}$	$3 \cdot 19 \cdot 7829 \cdot 31223 \cdot 121843$

TABLE 5. Monomials and their coefficients sufficient for the proof of Theorem 6.3.1 in the case $A \subseteq \mathbb{Z}_p$, $|A| \geq 17$

ℓ	deg	monomial/s	coefficient/s
11	110	$y_1^{10}y_2^{10}y_3^{10}y_4^{10}y_5^{10}y_6^{10}y_7^{10}y_8^{10}y_9^{10}y_{10}^{10}y_{11}^{10}$	$13 \cdot 67 \cdot 451441944254443$
12	126	$y_1^6y_2^{10}y_3^{11}y_4^{11}y_5^{11}y_6^{11}y_7^{11}y_8^{11}y_9^{11}y_{11}^{11}y_{11}^{11}y_{12}^{11}$	$2 \cdot 7 \cdot 13 \cdot 4679 \cdot 3953841444019$

6.3.3. Direct construction(s). In this subsection we want to attack Conjecture 6.3.1 with a direct construction. Even though we are able to solve it only for $t = 3$, for this value we obtain a solution in any cyclic group. Then we outline the proof of a similar statement for Conjecture 6.3.2. Indeed, in a very similar way, it is possible to prove that the latter conjecture holds, in cyclic groups, for $t \leq 4$.

First of all, we note that with the same proof of Proposition 6.3.1, we obtain the following.

PROPOSITION 6.3.5. *Let $A = \{a_1, \ldots, a_k\} \subseteq \mathbb{Z}_n \setminus \{0\}$ be a set of cardinality k and let h and t be positive integers such that $h \leq k - (t-1)$. Then there is an ordering of h-elements of A that we denote, up to relabeling, with $(a_1, \ldots, a_h)$, such that for any $0 \leq i < j \leq \min(h, i+t)$*

$$s_i = a_1 + a_2 + \cdots + a_i \neq a_1 + a_2 + \cdots + a_j = s_j.$$

Moreover, if n is even and $n/2 \in A$, we can assume $a_1 = n/2$.

Here we can not apply directly Proposition 6.3.1 because $\mathbb{Z}_n$ is not necessary a field. However, with this new proposition we obtain the main result of this subsection.

THEOREM 6.3.3. *Let $t \leq 3$ be a positive integer. Then the cyclic group $\mathbb{Z}_n$ is strongly t-weakly sequenceable for any positive integer n.*

PROOF. As usual it is enough to consider only the case $t = 3$ and let $A = \{a_1, \dots, a_k\}$ be a subset of $\mathbb{Z}_n \setminus \{0\}$. Here we can assume $k > 9$ because, due to the result of [10], Conjecture 6.1.1 holds for sets of cardinality at most 9. According to Proposition 6.3.5, for $h = k - 4$, there is an ordering of h elements of A that we denote, up to relabeling, with $(a_1, \dots, a_h)$ such that $s_i \neq s_j$ whenever $0 \leq i < j \leq \min(h, i + t)$. Moreover, if n is even and $n/2 \in A$, we can assume $a_1 = n/2$.

We then need to order the last four elements $a_{k-3}, a_{k-2}, a_{k-1}, a_k$. We divide the proof into two cases.

CASE 1: $a_{k-3} + a_{k-2} + a_{k-1} = 0$. Here we first assume that $-a_k \notin \{a_{k-3}, a_{k-2}, a_{k-1}\}$. In this case we look for an ordering of type

$$(a_1, \dots, a_{k-5}, a_{k-4}, y_1, y_2, a_k, y_3),$$

where $y_1, y_2, y_3 \in \{a_{k-3}, a_{k-2}, a_{k-1}\}$. Indeed there exists $y_1 \in \{a_{k-3}, a_{k-2}, a_{k-1}\}$ such that

$$\begin{cases} y_1 + a_{k-4} \neq 0; \\ y_1 + a_{k-4} + a_{k-5} \neq 0. \end{cases}$$

Then we can easily check that all the partial sums s_i and s_j such that $0 \leq i < j \leq \min(k, i+t)$ are different.

Let us now assume that $-a_k = a_{k-3}$. Here if $a_k \neq a_{k-4} + a_{k-5}$ we can choose an ordering of type

$$(a_1, \dots, a_{k-5}, a_{k-4}, -a_k, y_1, a_k, y_2),$$

where $y_1, y_2 \in \{a_{k-2}, a_{k-1}\}$. Indeed there exists $y_1 \in \{a_{k-2}, a_{k-1}\}$ such that

$$y_1 - a_k + a_{k-4} \neq 0.$$

Then we can easily check that all the partial sums s_i and s_j such that $0 \leq i < j \leq \min(k, i+t)$ are different.

Let us now assume that $-a_k = a_{k-3}$ and $a_k = a_{k-4} + a_{k-5}$. Here we have that

$$\{a_{k-3}, a_{k-2}, a_{k-1}, a_k\} = \{-(a_{k-4} + a_{k-5}), a_{k-2}, a_{k-1}, a_{k-4} + a_{k-5}\}$$

and we look for an ordering of type

$$(a_1, \dots, a_{k-5}, a_{k-4}, y_1, a_{k-4} + a_{k-5}, y_2, -(a_{k-4} + a_{k-5})),$$

where $y_1, y_2 \in \{a_{k-2}, a_{k-1}\}$. We first note that we can choose $y_1 \in \{a_{k-2}, a_{k-1}\}$ such that

$$\begin{cases} y_1 + a_{k-4} \neq 0; \\ y_1 + 2a_{k-4} + a_{k-5} \neq 0. \end{cases}$$

Indeed, if such y_1 does not exist, we would have that

$$\{a_{k-3}, a_{k-2}, a_{k-1}, a_k\} = \{-(a_{k-4} + a_{k-5}), -a_{k-4}, -2a_{k-4} - a_{k-5}, a_{k-4} + a_{k-5}\}.$$

We recall that also $a_{k-3} + a_{k-2} + a_{k-1} = 0$ and hence it would follows that $-4a_{k-4} - 2a_{k-5} = 0$. This means that $-2a_{k-4} - a_{k-5}$ is an involution and hence, because $\mathbb{Z}_n$ is cyclic, $-2a_{k-4} - a_{k-5} \in \{0, n/2\}$. Since $-2a_{k-4} - a_{k-5} \in \{a_{k-2}, a_{k-1}\}$ this is in contradiction with the choice of the first element of the ordering. Then we can easily check that all the partial sums s_i and s_j such that $0 \leq i < j \leq \min(k, i + t)$ are different.

CASE 2: Since we have already considered CASE 1, here we can assume, without loss of generality, that all the triples of elements do not sum to zero. Moreover, let us assume that $a_{k-3} + a_{k-2} = 0$. Here we can choose an ordering of type

$$(a_1, \dots, a_{k-5}, a_{k-4}, y_1, z_1, y_2, z_2),$$

where $y_1, y_2 \in \{a_{k-3}, a_{k-2}\}$ and $z_1, z_2 \in \{a_{k-1}, a_k\}$. Indeed there exist $y_1 \in \{a_{k-3}, a_{k-2}\}$ and $z_1 \in \{a_{k-1}, a_k\}$ such that

$$\begin{cases} y_1 + a_{k-4} + a_{k-5} \neq 0; \\ z_1 + y_1 + a_{k-4} \neq 0. \end{cases}$$

Then we can easily check that all the partial sums s_i and s_j such that $0 \leq i < j \leq \min(k, i+t)$ are different.

Finally, let us assume that all the triples and all the pairs of elements from $\{a_{k-3}, a_{k-2}, a_{k-1}, a_k\}$ do not sum to zero. Here, due to the pigeonhole principle, we can choose an ordering of type

$$(a_1, \ldots, a_{k-5}, a_{k-4}, y_1, y_2, y_3, y_3),$$

where y_1, y_2 are such that

$$\begin{cases} y_1 + a_{k-4} \neq 0; \\ y_1 + a_{k-4} + a_{k-5} \neq 0; \\ y_2 + y_1 + a_{k-4} \neq 0. \end{cases}$$

Then we can easily check that all the partial sums s_i and s_j such that $0 \leq i < j \leq \min(k, i+t)$ are different. □

Moreover, with a very similar but more tedious proof, one could get an analogous result about Conjecture 6.3.2.

THEOREM 6.3.4. *Let $t \leq 4$ be a positive integer and A be a finite subset of $\mathbb{Z}_n \setminus \{0\}$ such that $|A \cap \{x, -x\}| \leq 1$ for any $x \in \mathbb{Z}_p$ and $|A| > t$. Then A is t-weakly sequenceable.*

This Theorem can be proved by fixing the first $k-6$ elements of the ordering and then choosing a_{k-5} in such a way that $2a_{k-5} + 2a_{k-6} + a_{k-7} \neq 0$ and s_{k-5} is different from s_{k-8} and s_{k-9}. Then we can proceed, similarly to what we did for Theorem 6.3.3, by considering two cases according to whether $a_{k-4} + a_{k-3} + a_{k-2} + a_{k-1} = 0$ or not. However, we prefer not to write a complete proof of this statement since we believe it goes beyond the scope of this subsection and we have the feeling that it is not very deep from the mathematical point of view.

6.3.4. A probabilistic approach. In this subsection, we prove that a randomly chosen subset $A \subseteq \mathbb{Z}_n \setminus \{0\}$ of cardinality k is t-weakly sequenceable when tk is small with respect to n and $t \geq 2$. This result corresponds to Theorem 4.2 of [13] in the case of weak sequenceability. In addition we also prove that for every $A \subseteq \mathbb{Z}_n \setminus \{0\}$ of cardinality k there exists an ordering $\boldsymbol{\omega}$ of A with at most $t-2$ pairs of partial sums s_i, s_j such that $s_i = s_j$ and $|j - i| \leq t$.

DEFINITION 6.3.3. *Let $\mathcal{A}_{n,k}$ be the set of all subsets of cardinality k of $\mathbb{Z}_n \setminus \{0\}$ that are t-weakly sequenceable. We say that* almost all k-subsets *of $\mathbb{Z}_n$ are t-weakly sequenceable if*

$$\lim_{n \to \infty} \frac{|\mathcal{A}_{n,k}|}{\binom{n-1}{k}} = 1\,.$$

PROPOSITION 6.3.6. *Let us choose an ordered sequence $\boldsymbol{\omega} = (a_1, a_2, \ldots, a_k)$ of distinct elements of $\mathbb{Z}_n \setminus \{0\}$ uniformly at random. The probability that $\boldsymbol{\omega}$ is a t-weak sequencing of the set $\{a_1, a_2, \ldots, a_k\}$ is greater than or equal to $1 - \frac{(t-1)(k-2)}{n-2}$.*

PROOF. Let q be the probability that $\boldsymbol{\omega}$ is not a t-weak sequencing of $\{a_1, \ldots, a_k\}$. Then, letting $\boldsymbol{s} = (s_0, s_1, \ldots, s_k)$ denote the partial sums of $\boldsymbol{\omega}$, we get

$$q \leq \sum_{\substack{0 \leq i < j \leq k \\ j-i \leq t, j \neq i+1}} \mathbb{P}(s_j = s_i) = \sum_{\substack{0 \leq i < j \leq k \\ j-i \leq t, j \neq i+1}} \mathbb{P}(a_{i+1} + \ldots + a_j = 0)$$

$$= \sum_{\substack{0 \leq i < j \leq k \\ j-i \leq t, j \neq i+1}} \sum_{s=0}^{n-1} \mathbb{P}(a_{i+1} + \ldots + a_{j-1} = s) \cdot \mathbb{P}(a_j = -s | a_{i+1} + \ldots + a_{j-1} = s)\,.$$

We can upper bound $\mathbb{P}(a_j = -s | a_{i+1} + \ldots + a_{j-1} = s)$ by $1/(n-j+i)$ for each $s \in \mathbb{Z}_n$ since there is at most one possible outcome for $a_j \in \mathbb{Z}_n \setminus \{0, a_{i+1}, \ldots, a_{j-1}\}$ that makes the sum $a_{i+1} + \ldots + a_j = 0$. Hence

$$q \leq \sum_{\substack{0 \leq i < j \leq k \\ j-i \leq t, j \neq i+1}} \frac{1}{n-j+i} = \sum_{l=2}^{t} \sum_{\substack{0 \leq i < j \leq k \\ j-i=l}} \frac{1}{n-j+i} = \sum_{l=2}^{t} \frac{k-l}{n-l} \leq \frac{(t-1)(k-2)}{n-2}\,,$$

where we used the fact that $(k-l)/(n-l) \leq (k-2)/(n-2)$ for every $n > k \geq 2$ and $l \geq 2$. □

THEOREM 6.3.5. *Almost all k-subsets of $\mathbb{Z}_n$ are t-weakly sequenceable when $tk = o(n)$ for $n \to \infty$.*

PROOF. By Proposition 6.3.6 it is easy to see that the probability a randomly chosen subset of $\mathbb{Z}_n \setminus \{0\}$ of cardinality k is not t-weakly sequenceable is at most $\frac{(t-1)(k-2)}{n-2}$. □

PROPOSITION 6.3.7. *Let A be a subset of cardinality k of $\mathbb{Z}_n \setminus \{0\}$ and let us choose uniformly at random an ordering $\boldsymbol{\omega} = (a_1, a_2, \ldots, a_k)$ of A. Denoting the partial sums of $\boldsymbol{\omega}$ by $\boldsymbol{s} = (s_0, s_1, \ldots, s_k)$, let X be the random variable that represents the number of pairs (i, j) such that $s_i = s_j$ with $0 \leq i < j \leq k$ and $j - i \leq t$, where $2 \leq t < k$.*

Then the expected value $\mathbb{E}(X)$ is smaller than $t - 1$.

PROOF. Proceeding as in Proposition 6.3.6 we get

$$\mathbb{E}(X) = \sum_{\substack{0 \leq i < j \leq k \\ j-i \leq t, j \neq i+1}} \mathbb{P}(s_j = s_i) = \sum_{\substack{0 \leq i < j \leq k \\ j-i \leq t, j \neq i+1}} \mathbb{P}(a_{i+1} + \ldots + a_j = 0)$$

$$\leq \sum_{\substack{0 \leq i < j \leq k \\ j-i \leq t, j \neq i+1}} \frac{1}{k-j+i+1} = \sum_{l=2}^{t} \frac{k-l}{k-l+1} < t-1\,.$$

□

From Proposition 6.3.7 the following result is immediate.

THEOREM 6.3.6. *For every $A \subseteq \mathbb{Z}_n \setminus \{0\}$ and $2 \leq t < |A|$, there exists an ordering of A with less than $t - 1$ pairs of equal partial sums $s_i = s_j$ where $|j - i| \leq t$.*

Appendix

We report here the full SageMath code used to provide the results of the previous section. We have omitted to report the function *remTerms* since is the same function stated in the Appendix of Section 6.2.

```
import numpy as np, gc, math, time

def poldeg(l):
    deg = 0; occ = np.zeros(l, dtype=int)
    for i in range(0, l-1):
        for j in range(i+1, l):
            occ[i] += 1
            occ[j] += 1
            deg += 1
            if j - i + 1 <= t:
                for k in range(i, j+1):
                    occ[k] += 1
                deg += 1
    for i in range(0, t-1):
        for k in range(0, i+1):
            occ[k] += t-i-1
        deg += t-i-1
    return deg, occ
t = 6; l = 2*t-1; p=1
R = PolynomialRing(ZZ,l,"x")
vars = R.gens()
print("Variables: ", vars, "\n")
deg, occs = poldeg(l)
print("Deg: ", deg, " Occs: ", occs)
bounding_exponents = np.ones(l, dtype=int) * (l-1)
print(list(bounding_exponents))
for i in range(0, l-1):
    for j in range(i+1, l):
        f1 = vars[j]-vars[i]
        occs[i] -= 1; occs[j] -= 1
        f2 = 1
        if j - i + 1 <= t:
            f2 = sum(vars[k] for k in range(i, j+1))
            for k in range(i, j+1):
                occs[k] -= 1
        ff = f1 * f2; p = p * ff
        p = remTerms(p, bounding_exponents, occs)
        print(p.total_degree(), " / ", deg)
    if i < t-1:
        print(sum(vars[k] for k in range(0, i+1)), "^", t-i-1)
        for s in range(0, t-i-1):
            f3 = sum(vars[k] for k in range(0, i+1))
            for k in range(0, i+1):
                occs[k] -= 1
            p = p * f3
            p = remTerms(p, bounding_exponents, occs)
            print("2) ", p.total_degree(), " / ", deg)
print("Degree: ", p.total_degree())
print(p)
print(factor(p.lc()))
```

CHAPTER 7

Higher Degree Erdős-Ginzburg-Ziv Constants

In this chapter, all the results are obtained in collaboration with Simone Costa.

7.1. Introduction

One significant subfield of additive group theory and combinatorial number theory is the zero-sum theory that studies the sums behavior of suitable sequences of elements in an abelian finite group G (see, for instance, the surveys [31, 73]). In this context, a typical kind of problem considers the existence of constants ℓ such that any sequence of elements of G whose length is bigger than ℓ satisfies an additive property $\mathcal{P}$. Among these constants, an important role is taken by the classical Erdős-Ginzburg-Ziv constant of a group G that denotes the smallest positive integer ℓ such that any sequence of length $|S| \geq \ell$ contains a zero-sum subsequence of length $|G|$. This constant has been well studied in the literature, we refer to the survey paper [73]. Here we recall that in [63], Erdős, Ginzburg and Ziv completely determined its value over cyclic groups and that in [70] and in [96], respectively Fox, Sauermann and Naslund, derived nontrivial upper bounds on groups of type $\mathbb{F}_p^n$, they assumed a slightly different definition of Erdős-Ginzburg-Ziv constant. Using this definition Sidorenko [109] showed the equivalence between this generalized Erdős-Ginzburg-Ziv constant over $\mathbb{Z}_2^d$ and the problem of finding the lowest redundancy of a linear binary code of a given length which does not contain words of a specific hamming weight.

In the recent paper [33], Caro and Schmitt generalized this concept, using the m-th degree symmetric polynomial $e_m(g_1, \ldots, g_t) = \sum_{1 \leq i_1 < \cdots < i_m \leq t} \prod_{j=1}^{m} g_{i_j}$ instead of the sum of the elements of S and considering subsequences of a given length t (see also [4, 21, 22] and [23] that considered some related problems). In particular, they defined the higher degree Erdős-Ginzburg-Ziv constants $EGZ(t, R, m)$ as follows. For a finite commutative ring R, $EGZ(t, R, m)$ is the smallest positive integer ℓ such that every sequence S over R of length $|S| \geq \ell$ contains a subsequence S' of length t for which $e_m(S')$ evaluates to the zero-element in R. If such ℓ does not exists, $EGZ(t, R, m)$ is set to ∞.

They also present several lower and upper bounds to these constants solving the case where R is $\mathbb{Z}_2$ and the case where R is $\mathbb{Z}_{p^s}$ if t and m are powers of the same prime. For a generic finite commutative ring R, their best lower bound is expressed in term of the generalized Davenport constant $D(R, m)$ of the ring R (see Caro, Girard and Schmitt, [32]) that is the smallest integer ℓ such that any sequence S over R of length $|S| \geq \ell$ contains a subsequence S' of length $|S'| \geq m$ for which $e_m(S')$ equals the zero element of R. Indeed they prove that

$$EGZ(t, R, m) \geq t + D(R, m) - m. \tag{109}$$

This chapter aims to determine lower and upper bounds for $EGZ(t, R, m)$ in case $R = \mathbb{F}_q^n$ for some prime power q (in the following we will always use the letter q for a prime power and p for a prime). The chapter is organized as follows. In Section 7.2.1 we will present two lower bounds obtained, respectively, using Lovász Local Lemma and the Expurgation method. Here we will also compare our lower bounds with each other. Then, in Section 7.2.2, we will show that, for sufficiently large n, our bounds improve the ones given by Caro and Schmitt in the same context. Finally, in Section 7.2.3, we will apply Tao's Slice Rank method to provide an upper bound to $EGZ(3, R, 2)$ in case $R = \mathbb{F}_q^n$ and $q = 3^k$ for $k > 1$. In particular, here, we will apply the asymptotic rank

theory developed by Tao and Sawin in [116] and we will prove, purely theoretically, the existence of a nontrivial upper bound. In addition, for $k = 2, 3, 4, 5$, we provide explicit numerical upper bounds.

7.2. Bounds on the Higher Degree Erdős-Ginzburg-Ziv Constants

7.2.1. Lower bounds. In this subsection, we will present two kinds of probabilistic lower bounds on the Erdős-Ginzburg-Ziv constants of rings of type $\mathbb{F}_q^n$. Both those bounds exploit the following upper bound on the probability that a given t-sequence S of elements in $\mathbb{F}_q^n$ is such that $e_m(S) = 0$. The following proposition easily follows by Schwartz–Zippel lemma [104], we report here a proof for the reader convenience.

PROPOSITION 7.2.1. *Let us choose, uniformly at random, a sequence $S = (g_1, g_2, \dots, g_t)$ of $t \geq m$ elements in $\mathbb{F}_q^n$. Then*

$$\mathbb{P}[e_m(S) = 0] \leq \left(\frac{m}{q}\right)^n.$$

PROOF. We prove this result first assuming $n = 1$, by induction on m.

BASE STEP. Let us consider the case $m = 1$. Let us assume we have already chosen, uniformly at random, the first $t-1$ elements $g_1, \dots, g_{t-1}$ of S then we note that the equation

$$e_1(g_1, \dots, g_{t-1}, x) = g_1 + g_2 + \cdots + g_{t-1} + x = 0$$

has only one solution in $\mathbb{F}_q$. It means that

$$\mathbb{P}[e_1(S) = 0] \leq \frac{1}{|\mathbb{F}_q|} = \frac{1}{q}.$$

INDUCTIVE STEP. Here we assume the thesis is true for $m-1$ and we prove it for m. We note that

$$e_m(g_1, \dots, g_{t-1}, g_t) = e_m(g_1, \dots, g_{t-1}) + g_t e_{m-1}(g_1, \dots, g_{t-1}).$$

Therefore, we can upper bound the probability that, chosen, uniformly at random the elements $g_1, \dots, g_t$, $e_m(g_1, \dots, g_t) = 0$ as follows

$$\begin{aligned}\mathbb{P}[e_m(g_1, \dots, g_t) = 0] \\ \leq \mathbb{P}[e_{m-1}(g_1, \dots, g_{t-1}) = 0] + \mathbb{P}[e_m(g_1, \dots, g_t) = 0 | e_{m-1}(g_1, \dots, g_{t-1}) \neq 0].\end{aligned}$$

Here we note that, if $e_{m-1}(g_1, \dots, g_{t-1}) \neq 0$, there is exactly one $x \in \mathbb{F}_q$ such that

$$e_m(g_1, \dots, g_{t-1}, x) = e_m(g_1, \dots, g_{t-1}) + x e_{m-1}(g_1, \dots, g_{t-1}) = 0.$$

It follows that

$$\mathbb{P}[e_m(g_1, \dots, g_t) = 0 | e_{m-1}(g_1, \dots, g_{t-1}) \neq 0] \leq \frac{1}{q}.$$

Moreover, due to the inductive hypothesis, we have that $\mathbb{P}[e_{m-1}(g_1, \dots, g_{t-1}) = 0] \leq \frac{m-1}{q}$. Therefore the inductive claim is proved, since:

$$\mathbb{P}[e_m(g_1, \dots, g_t) = 0] \leq \frac{m-1}{q} + \frac{1}{q} = \frac{m}{q}.$$

It means that, in $\mathbb{F}_q$, if we choose uniformly at random a sequence S of $t \geq m$ elements then

$$\mathbb{P}[e_m(S) = 0] \leq \frac{m}{q}.$$

Now we note that, if we consider a sequence a sequence S of $t \geq m$ elements in $\mathbb{F}_q^n$, then $e_m(S) = 0$ if and only if each of the n projections $\pi_i(S)$ of S over the i-th coordinate satisfies $e_m(\pi_i(S)) = 0$. Since those projections are independent, it follows that

$$\mathbb{P}[e_m(S) = 0] = \prod_{i=1}^{n} \mathbb{P}[e_m(\pi_i(S)) = 0] \leq \left(\frac{m}{q}\right)^n.$$

□

7.2.1.1. *Lovász Local Lemma.* We provide a first new lower bound on $EGZ(t, \mathbb{F}_q^n, m)$ by exploiting the so-called Lovász Local Lemma, see also the work [23] of Bitz, Griffith and He for a similar application of this method. Here we restate the lemma (in the symmetric case), already stated in Chapter 2, for the reader's convenience.

LEMMA 7.2.1 ([65] (see also [8])). *Let $E_1, E_2, \ldots, E_k$ be events in an arbitrary probability space. Suppose that each event E_i is mutually independent of the set of all other events E_j but at most D, and that $\mathbb{P}[E_i] \leq P$ for all $1 \leq i \leq k$. If*

$$eDP \leq 1$$

then $\mathbb{P}[\cap_{i=1}^k \overline{E_i}] > 0$.

Now, we are ready to state the following theorem.

THEOREM 7.2.1. *Let ℓ be such that*

$$e\left[\binom{\ell}{t} - \binom{\ell - t}{t}\right]\left(\frac{m}{q}\right)^n \leq 1$$

where $\binom{\ell-t}{t}$ is set to zero if $\ell < 2t$. Then $EGZ(t, \mathbb{F}_q^n, m) > \ell$.

PROOF. Here we need to prove the existence of a sequence S of length ℓ for which any subsequence S' of length t is such that $e_m(S') \neq 0$.

Let us choose, uniformly at random, a sequence S of length ℓ in $\mathbb{F}_q^n$. For a given subsequence S' of length t contained in S, let $E_{S'}$ be the event such that $e_m(S') = 0$. Clearly, there are $\binom{\ell}{t}$ such events. Due to Proposition 7.2.1, we know that

$$\mathbb{P}[E_{S'}] \leq \left(\frac{m}{q}\right)^n \quad \text{for all} \quad S' \subseteq S, |S'| = t.$$

It is easy to see that each event $E_{S'}$ is mutually independent from all the events $E_{S''}$ where $S'' \subseteq S \backslash S'$ and $|S''| = t$. Therefore each event $E_{S'}$ is dependent by at most

$$\binom{\ell}{t} - \binom{\ell - t}{t}$$

other events. Hence, due to Lemma 7.2.1 we obtain the thesis. □

7.2.1.2. *Expurgation.* Now we provide a second lower bound that, in some regime of the parameters turns out to improve that of Subsection 7.2.1.1. The method we use here is sometimes called Expurgation in the literature. We refer the reader to the book [8, Chapter 3 (Alterations)].

THEOREM 7.2.2. *Let ℓ be such that*

$$\binom{\ell + s}{t}\left(\frac{m}{q}\right)^n < s + 1$$

for some $s \geq 0$. Then $EGZ(t, \mathbb{F}_q^n, m) > \ell$.

PROOF. We first note that the thesis is equivalent to prove the existence of a sequence S of length ℓ for which any subsequence S' of length t is such that $e_m(S') \neq 0$.

Here we choose, uniformly at random, a sequence T of length $\ell + s$ and we evaluate the expected value of the random variable X given by the number of subsequences T' of T of length t and such that $e_m(T') = 0$. Because of Proposition 7.2.1, we have that

$$\mathbb{E}(X) \leq \sum_{T' \subseteq T : |T'| = t} \left(\frac{m}{q}\right)^n = \binom{\ell + s}{t}\left(\frac{m}{q}\right)^n.$$

Moreover, due to the hypothesis, we have that

$$\mathbb{E}(X) < s + 1.$$

It follows that there exists a set T of length $\ell + s$ with at most s subsequences T' such that $e_m(T') = 0$ that we call bad subsequences. If we remove from T one element from each bad subsequence we

have removed at most s elements and we are left with a sequence S of length at least ℓ for which any subsequence S' of length t is such that $e_m(S') \neq 0$. Clearly, we may assume, without loss of generality, that the length of S is exactly ℓ obtaining the thesis. □

In the following proposition, we show that when $t \leq c\sqrt{\ell}$ for some constant c, the bound given in Theorem 7.2.1 is better than the one given in Theorem 7.2.2 with $s = 0$.

PROPOSITION 7.2.2. *Let ℓ and t be positive integers such that $\ell \geq 2t$. Then*

$$e\left[\binom{\ell}{t} - \binom{\ell - t}{t}\right] \leq \binom{\ell}{t} \tag{110}$$

for every $t \leq \sqrt{\frac{\ell+1}{e+1}}$.

PROOF. Inequality (110) can be easily restated as

$$\left(1 - \frac{t}{\ell}\right) \cdot \left(1 - \frac{t}{\ell - 1}\right) \cdots \left(1 - \frac{t}{\ell - t + 1}\right) \geq 1 - \frac{1}{e}. \tag{111}$$

Then lower bounding each factor on the LHS of equation (111) by $\left(1 - \frac{t}{\ell - t + 1}\right)$ we get

$$\prod_{i=0}^{t-1} \left(1 - \frac{t}{\ell - i}\right) \geq \left(1 - \frac{t}{\ell - t + 1}\right)^t.$$

Using Bernoulli's inequality $(1 + x)^r \geq 1 + rx$ we obtain that

$$\left(1 - \frac{t}{\ell - t + 1}\right)^t \geq 1 - \frac{t^2}{\ell - t + 1}.$$

For $(e + 1)t^2 \leq \ell + 1$, the following inequality

$$1 - \frac{t^2}{\ell - t + 1} \geq 1 - \frac{1}{e}$$

is satisfied. Hence we proved the proposition. □

An immediate corollary of this proposition is that, if t is fixed and ℓ is big enough,

$$e\left[\binom{\ell}{t} - \binom{\ell - t}{t}\right] \left(\frac{m}{q}\right)^n < 1$$

for any ℓ such that

$$\binom{\ell}{t} \left(\frac{m}{q}\right)^n < 1.$$

Equivalently we can say that in this regime the bound provided by Lovász Local Lemma is better than that of Theorem 7.2.2 with $s = 0$.

Since finding the optimal s in the bound given in Theorem 7.2.2 is not easy even for small values of t, we are interested in studying the optimal s when $\ell \to \infty$ and $t = o(\ell)$. It can be seen that in this case, the optimal value of s is equal to $\ell/(t - 1)$. This can be easily proved observing that

$$\binom{\ell + s}{t} = \frac{(\ell + s)^t}{t!}(1 + o(1))$$

and deriving in s the function

$$\frac{(\ell + s)^t}{t!(1 + s)}(1 + o(1)).$$

In this regime, we provide the following proposition which implies that the bound given in Theorem 7.2.2 with $s = \ell/(t - 1)$ provides a better result than the one given in Theorem 7.2.1 for sufficiently large ℓ's.

PROPOSITION 7.2.3. *If $t = o(\sqrt{\ell})$ then we have that*

$$\lim_{\ell\to\infty} \binom{\frac{t}{t-1}\ell}{t} \frac{1}{\frac{\ell}{t-1}+1} \Bigg/ e\left[\binom{\ell}{t} - \binom{\ell-t}{t}\right] \leq \frac{1}{t}. \tag{112}$$

PROOF. First, we lower bound the denominator on the LHS of (112) as follows

$$e\left[\binom{\ell}{t} - \binom{\ell-t}{t}\right] = e\binom{\ell}{t}\left(1 - \prod_{i=0}^{t-1}\left(1 - \frac{t}{\ell-i}\right)\right) \geq e\binom{\ell}{t}\left(1 - \left(1-\frac{t}{\ell}\right)^t\right).$$

Since $(1-t/\ell)^t \leq e^{-t^2/\ell} = 1 - t^2/\ell + o(t^2/\ell)$ and since $t^2 = o(\ell)$ we obtain that

$$e\binom{\ell}{t}\left(1 - \left(1-\frac{t}{\ell}\right)^t\right) \geq e\binom{\ell}{t}\frac{t^2}{\ell}(1+o(1)) = et\binom{\ell-1}{t-1}(1+o(1)).$$

Then, we upper bound the numerator on the LHS of (112) as follows

$$\binom{\frac{t}{t-1}\ell}{t}\frac{1}{\frac{\ell}{t-1}+1} = \binom{\frac{t}{t-1}\ell - 1}{t-1}\frac{\frac{t}{t-1}\ell}{t}\frac{1}{\frac{\ell}{t-1}+1} \leq \binom{\frac{t}{t-1}\ell}{t-1}.$$

Hence, using the estimates for the numerator and the denominator we have that the limit in the statement of the proposition is upper bounded by

$$\lim_{\ell\to\infty} \binom{\frac{t}{t-1}\ell}{t-1} \Bigg/ et\binom{\ell-1}{t-1}(1+o(1)) = \frac{1}{et}\left(\frac{t}{t-1}\right)^{t-1} \leq \frac{1}{t}$$

where we used the fact that $\left(1+\frac{1}{t-1}\right)^{t-1} \leq e$. □

An immediate corollary of this proposition is that, if t is fixed and ℓ is big enough,

$$\binom{\ell + \ell/(t-1)}{t}\left(\frac{m}{q}\right)^n < 1 + \ell/(t-1)$$

for any ℓ such that

$$e\left[\binom{\ell}{t} - \binom{\ell-t}{t}\right]\left(\frac{m}{q}\right)^n \leq 1.$$

Equivalently we can say that, in this regime, the bound provided by Theorem 7.2.2 with $s = \ell/(t-1)$ is better than that of Lovász Local Lemma.

REMARK 7.2.1. *We have been able to compute the optimal value of s in the expurgation bound (Theorem 7.2.2) only for small values of t, i.e., $t = 2, 3, 4, 5$. In all these cases and the regime considered in Theorem 7.2.3 the expurgation bound performs better than the bound given in Theorem 7.2.1 obtained using the Lovász Local Lemma. In view of these results, we are inclined to conjecture that the expurgation bound provides the best bound for every $\ell \geq t \geq 2$. However, since we did not succeed to prove this conjecture, we considered useful to report also the bound given in Theorem 7.2.1.*

7.2.2. Comparision with Caro and Schmitt's bounds. In this subsection, we discuss the bounds we have obtained in comparison to that of Caro and Schmitt. In particular, in [32] (see Theorems 3.1 and 3.4), it was proved that for rings of type $\mathbb{F}_p^n$ (where p is a prime) the following bounds on $D(\mathbb{F}_p^n, m)$ hold:

$$nmp - (n-1)m \geq D(\mathbb{F}_p^n, m) \geq np - (n-1)m. \tag{113}$$

It follows that the lower bound of Caro and Schmitt (109) becomes

$$EGZ(t, \mathbb{F}_p^n, m) \geq t + n(p-m). \tag{114}$$

Now we consider our lower bound of Theorem 7.2.2 with $s = 0$ in the case $q = p$. Note that this is not, in general, our best lower bound but it is the easiest to consider. We have that $EGZ(t, \mathbb{F}_p^n, m) \geq \ell$, if ℓ is such that

$$\binom{\ell}{t}\left(\frac{m}{p}\right)^n < 1.$$

We note that $\frac{\ell^t}{t!} > \binom{\ell}{t}$ and hence $EGZ(t, \mathbb{F}_p^n, m) \geq \ell$ for any ℓ such that

$$\frac{\ell^t}{t!}\left(\frac{m}{p}\right)^n < 1$$

that is

$$\frac{\ell^t}{t!} < \left(\frac{p}{m}\right)^n$$

and hence

$$EGZ(t, \mathbb{F}_p^n, m) \geq (t!)^{\frac{1}{t}}\left(\frac{p}{m}\right)^{\frac{n}{t}}. \tag{115}$$

Now, since (115) is, when $p > m$, exponential in n, it is clear that asymptotically in n, it improves the lower bound of equation (114).

REMARK 7.2.2. *From equation* (115)*, we also have that, if $p > m$, for sufficiently large n:*

$$EGZ(t, \mathbb{F}_p^n, m) \geq (t!)^{\frac{1}{t}}\left(\frac{p}{m}\right)^{\frac{n}{t}} > t + nm(p-1) \geq t + D(\mathbb{F}_p^n, m) - m$$

where the last inequality follows from the upper bound of equation (113)*. This means that, for these kinds of parameters it does not yield a Caro-Gao-type relation (see [31, 73]), i.e. it does not hold the equality in equation* (109)*.*

We also note that the bound of equation (115) can be trivially improved for several values of $q = p^k$. Indeed, if $\binom{t}{m} \not\equiv 0 \pmod p$ we have that $EGZ(t, \mathbb{F}_q^n, m) = \infty$. It suffices to consider the infinite constant sequence such that $g_i = 1$ for any $i \in \mathbb{N}$. In this case we have that, for any subsequence S' of length t, $e_m(S') = \binom{t}{m} \not\equiv 0 \pmod p$. On the other hand, this is a subset of the parameters for which our bounds of Subsection 7.2.1 (and in particular equation (115)) hold. Moreover, we will show in the upcoming subsection that, at least when $m = 2, t = 3$ and $q = 3^k$, it is possible to provide nontrivial upper bounds.

Finally, we also note that the bounds here presented can be easily generalized to rings of type $\mathbb{F}_{q_1} \times \mathbb{F}_{q_2} \times \cdots \times \mathbb{F}_{q_n}$ (similarly to those of [33] that Caro and Schmitt stated for rings of type $\mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \cdots \times \mathbb{Z}_{m_n}$) but, since we believe this is not a substantial improvement, we prefer to keep the notation of this note as simple as possible and to explicitly consider only rings of type $\mathbb{F}_q^n$.

7.2.3. Upper bound via slice rank. In this subsection we provide an upper bound to $EGZ(3, \mathbb{F}_q^n, 2)$ with $q = 3^k$ (in this subsection we always consider q to be of that form). Even though this is a very special case, providing upper bounds seems to be a hard task. The approach used here is the so-called Slice Rank method, introduced by Terence Tao in [114] and revisited by Tao and Sawin in [116] (see also [42] for a discussion on the method) in order to generalize the polynomial approach introduced in [46] and in [62]. Our application of the method is somehow reminiscent of works on the classical Erdős-Ginzburg-Ziv constants of Fox and Sauermann [70] and Naslund [96].

We begin by recalling some definitions and lemmas from [114] and [116].

DEFINITION 7.2.1. *A function $T : A^k \to \mathbb{F}$ is said to be a slice if it can be written in the form*

$$T(x_1, \ldots, x_k) = T_1(x_i)T_2(x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_k)$$

where $T_1 : A \to \mathbb{F}$ and $T_2 : A^{k-1} \to \mathbb{F}$.

DEFINITION 7.2.2. *The Slice Rank $srk(T)$ of a general function $T : A^k \to \mathbb{F}$ is the smallest number m such that T is a linear combination of m slices.*

LEMMA 7.2.2 ([114]). *Let A be a finite set and $\mathbb{F}$ be a field. Let $T(x,y,z)$ be a function $A\times A\times A\to\mathbb{F}$ such that $T(x,y,z)\neq 0$ if and only if $x=y=z$. Then $srk(T)=|A|$.*

Now we consider a sequence $S=(g_1,g_2,\ldots,g_\ell)$ of elements in $\mathbb{F}_q^n$ with $q=3^k$ such that every triple of elements g_1',g_2',g_3' of S satisfies $e_2(g_1',g_2',g_3')=g_1'g_2'+g_2'g_3'+g_3'g_1'\neq 0$. We note that S can not have elements repeated more than twice since $g_1'g_2'+g_2'g_3'+g_3'g_1'=0$ whenever $g_1'=g_2'=g_3'$. It means that we can split S into two parts S_1 and S_2 that are both sets of elements in $\mathbb{F}_q^n$. We can also assume that $|S_1|\geq|S|/2$. Now we split S_1 in $n+1$ sets $S_1^0,S_1^1,\ldots,S_1^n$ where $g_i\in S_1^j$ if g_i has exactly j coordinates equal to zero. We note that there exists j such that

$$|S_1^j|\geq\frac{|S_1|}{n+1}\geq\frac{|S|}{2(n+1)}$$

and hence $|S|\leq 2(n+1)|S_1^j|$. Clearly, to upper bound the length of the sequence S, it suffices to bound the cardinality of S_1^j considered as a set (it has no repetitions). Since it does not admit repeated elements, we already have that

$$|S_1^j|\leq q^n. \tag{116}$$

We will see that it is possible, if $q=3^k>3$, to improve this bound (even though not explicitly).

In order to apply Lemma 7.2.2, we want to consider a function that is zero whenever we consider three different elements of S_1^j. In particular, given $x,y,z\in\mathbb{F}_q^n$ we consider

$$P(x,y,z)=\prod_{i=1}^{n}(1-(x_iy_i+y_iz_i+z_ix_i)^{q-1}).$$

LEMMA 7.2.3. *Let us consider the function $P(x,y,z)$ on the restricted domain $S_1^j\times S_1^j\times S_1^j\to\mathbb{F}_q$ where $q=3^k$. Then $P(x,y,z)\neq 0$ if and only if $x=y=z$.*

PROOF. Here we have that, if x,y,z are in S_1^j, then $P(x,y,z)\neq 0$ if and only if $x=y=z$. Indeed, if x,y, and z are three different elements of S_1^j, they are such that $xy+yz+zx\neq 0$ and hence $x_iy_i+y_iz_i+z_ix_i\neq 0$ for at least one $i\in[1,n]$. This means that $1-(x_iy_i+y_iz_i+z_ix_i)^{q-1}=0$ and hence $P(x,y,z)=0$.

We note that also if we consider an element $x\in S_1^j$ repeated twice and $z\neq x$, we have that $P(x,x,z)=0$. Indeed, since x and z have the same number of zero components, there exists i such that $x_i\neq 0$ and $x_i\neq z_i$. Here we have that

$$x_ix_i+x_iz_i+z_ix_i=x_i^2+2x_iz_i=x_i(x_i-z_i)\neq 0$$

since both x_i-z_i and x_i are nonzero. It follows that $P(x,x,z)=0$. Similarly, we prove that also $P(z,x,x)=0$ and $P(x,z,x)=0$.

Finally, we consider an element x repeated three times. In this case, we have that

$$P(x,x,x)=\prod_{i=1}^{n}(1-(x_ix_i+x_ix_i+x_ix_i)^{q-1})=\prod_{i=1}^{n}(1-(3x_ix_i)^{q-1})=1\neq 0.$$

□

As a corollary of Lemmas 7.2.2 and 7.2.3 we have that:

COROLLARY 7.2.1.

$$|S|\leq 2(n+1)|S_1^j|=2(n+1)srk(P|_{S_1^j\times S_1^j\times S_1^j}).$$

Now the goal is to upper bound the $srk(P|_{S_1^j\times S_1^j\times S_1^j})$. The following Lemma will help us to make the first step in this direction.

LEMMA 7.2.4 ([114]). *Let A be a finite set, $A_1\subseteq A$ and $\mathbb{F}$ be a field. Let $T(x,y,z)$ be a function $A\times A\times A\to\mathbb{F}$. Then*

$$srk(T|_{A_1\times A_1\times A_1})\leq srk(T).$$

We immediately get the following corollary:

COROLLARY 7.2.2. *Considering the function P on the domain $\mathbb{F}_q^n \times \mathbb{F}_q^n \times \mathbb{F}_q^n$, we have that*

$$|S| \leq 2(n+1)|S_1^j| = 2(n+1)srk(P).$$

Now we aim to prove that $srk(P)$ is smaller than $a^{n+o(n)}$ for some constant a strictly smaller than $q = 3^k$.

For this purpose, we recall the asymptotic rank theory studied by Tao and Sawin in [116] in the special case of polynomial function (we do not need to consider the very general case of tensor Slice Rank).

Given a polynomial $p(x, y, z)$ whose degree in each variables is at most δ, we define Γ as the subset of $\{0, 1, \dots, \delta\}^3$ of the triples (d_1, d_2, d_3) such that $x^{d_1}y^{d_2}z^{d_3}$ has a nonzero coefficient in p.

PROPOSITION 7.2.4 ([116]). *Let $p(x, y, z)$ be a polynomial and let Γ be its support. Then:*

$$srk(\prod_{i=1}^{n} p(x_i, y_i, z_i)) \leq \exp((H(\Gamma) + o(1))n)$$

where

$$H(\Gamma) := \sup_{(X_1,\dots,X_k)} \min(h(X_1), \dots, h(X_k)),$$

$(X_1, \dots, X_k)$ takes values in Γ and $h(X)$ is the Shannon entropy of the random variable X defined as $-\sum_{\gamma\in\Gamma'} \mathbb{P}[X = \gamma] \log(\mathbb{P}[X = \gamma])$ and Γ' is the support of X.

In our case, we will not find the exact value of $H(\Gamma)$ but we will prove that $H(\Gamma) < \log(q) = \log(3^k)$, providing then an upper bound of type $\exp((H(\Gamma) + o(1))n) = \exp(H(\Gamma))^{(n+o(n))}$ where $\exp(H(\Gamma))$ is strictly smaller than $q = 3^k$. For this purpose, we will recall the following theorem from [30].

THEOREM 7.2.3 (Theorem 8 of [30]). *Let Γ be a finite subset of $S \times S \times S$ for some set S and let $\sigma \in Sym(3)$ be a permutation such that for each $a = (a_1, a_2, a_3) \in \Gamma$ also $\sigma(a) = (a_{\sigma(1)}, a_{\sigma(2)}, a_{\sigma(3)}) \in \Gamma$. Then there is a random variable Y taking values in Γ such that for all $y \in \Gamma$ we have that $\mathbb{P}[Y = y] = \mathbb{P}[Y = \sigma(y)]$ and*

$$\min(h(Y_1), h(Y_2), h(Y_3)) = H(\Gamma).$$

This theorem essentially ensures us that the value $H(\Gamma)$ is attained as a minimum of the entropy of the marginal variables of some random variable Y and that this variable is invariant under permutations that fix Γ. We are now ready to state and prove the main result of this subsection.

THEOREM 7.2.4. *Let $q = p^k$, then, if $p \neq 3$, we have that*

$$EGZ(3, \mathbb{F}_q^n, 2) = \infty.$$

If, instead, $p = 3$, we obtain the upper bound

$$EGZ(3, \mathbb{F}_q^n, 2) \leq a^{n+o(n)}$$

where $a = q = 3$ if $k = 1$ and $a < q = 3^k$ otherwise.

PROOF. We note that, if $p \neq 3$, $\binom{3}{2} = 3 \not\equiv 0 \pmod p$. In this case we consider the infinite constant sequence such that $g_i = 1$ for any $i \in \mathbb{N}$. Here we have that, for any subsequence S' of length 3, $e_2(S') = \binom{3}{2} = 3 \not\equiv 0 \pmod p$ and hence $EGZ(3, \mathbb{F}_q^n, 2) = \infty$ whenever $q = p^k$ and $p \neq 3$.

Now we assume p to be 3. If $k = 1$ the upper bound of this theorem follows directly from equation (116).

Otherwise, if $k > 1$, we set $p(x, y, z) = (1 - (xy + yz + zx)^{q-1})$ and we note that

$$P(x, y, z) = \prod_{i=1}^{n} p(x_i, y_i, z_i).$$

Therefore we can use Proposition 7.2.4 to evaluate $srk(P)$. To determine Γ, we develop the product. Here we have that

$$p(x,y,z) = x^0y^0z^0 - \left(\sum_{b+c+d=q-1, b,c,d\geq 0} \binom{q-1}{b,c,d} x^{b+c}y^{b+d}z^{d+c} \right).$$

It follows that $\Gamma \subset S^3$ where $S = \{0,1,\ldots,q-1\}$. Hence the marginal variables Y_1, Y_2 and Y_3 of Theorem 7.2.3 have all support $S = \{0,1,\ldots,q-1\}$.

We remark that given a random variable Y_1 whose support is the discrete set $\{0,1,\ldots,q-1\}$, as a consequence of the concavity of the entropy function and due to Jensen's inequality, $h(Y_1) = \log(q) = \log(3^k)$ if and only if Y_1 has uniform distribution over $\{0,1,\ldots,q-1\}$. It follows that, given a random variable Y whose support is Γ, $\min(h(Y_1), h(Y_2), h(Y_3)) = \log(q)$ if and only if Y_1, Y_2 and Y_3 have all uniform distributions over $\{0,1,\ldots,q-1\}$. Equivalently, $H(\Gamma) = \log(q)$ if and only if there exists a random variable Y that assume values over Γ (that satisfies the symmetric hypothesis of Theorem 7.2.3) and such that Y_1, Y_2 and Y_3 have all uniform distributions over $\{0,1,\ldots,q-1\}$.

Now we assume, by contradiction, that there exists such a variable Y and we set:

$$p_i = \mathbb{P}[Y = (i, q-1, q-1-i)] \text{ for } i = 0,1,\ldots,q-1.$$

Now since Y_1 has uniform distribution we have that

$$\begin{cases} \mathbb{P}[Y_1 = 1] = 1/q; \\ \mathbb{P}[Y_1 = 3] = 1/q; \\ \mathbb{P}[Y_1 = q-1] = 1/q. \end{cases} \tag{117}$$

It is easy to see that

$$\mathbb{P}[Y_1 = 1] = \mathbb{P}[Y = (1, q-1, q-2)] + \mathbb{P}[Y = (1, q-2, q-1)] = 2p_1$$

where the last equality holds due to Theorem 7.2.3.

We note that the coefficient of $x^3y^{q-2}z^{q-3}$ (and that of $x^3y^{q-3}z^{q-2}$) in p is

$$\binom{q-1}{2,1,q-4} = \frac{(q-1)(q-2)(q-3)}{2} \equiv 0 \pmod 3$$

and hence $(3, q-2, q-3), (3, q-3, q-2) \notin \Gamma$. It means that

$$\mathbb{P}[Y_1 = 3] = \mathbb{P}[Y = (3, q-1, q-4)] + \mathbb{P}[Y = (3, q-4, q-1)] = 2p_3.$$

Finally, we observe that

$$\mathbb{P}[Y_1 = q-1] = \sum_{i=0}^{q-1} \mathbb{P}[Y = (q-1, i, q-1-i)]$$

and, due to Theorem 7.2.3,

$$\mathbb{P}[Y_1 = q-1] = p_0 + 2p_1 + 2p_3 + 2p_2 + \sum_{i=4}^{q-5} p_i.$$

Hence system (117) can be rewritten as

$$\begin{cases} 2p_1 = 1/q; \\ 2p_3 = 1/q; \\ p_0 + 2p_1 + 2p_3 + 2p_2 + \sum_{i=4}^{q-5} p_i = 1/q. \end{cases} \tag{118}$$

Since $2p_1 = 1/q$ and $2p_3 = 1/q$ the last equation can be written as

$$p_0 + 2/q + 2p_2 + \sum_{i=4}^{q-5} p_i = 1/q.$$

But this would imply that

$$p_0 + 2p_2 + \sum_{i=4}^{q-5} p_i = -1/q < 0$$

that is a contradiction. It means that it does not exist any variable Y such that Y_1, Y_2 and Y_3 have all uniform distributions over $\{0, 1, \ldots, q-1\}$. Therefore $H(\Gamma) < \log(q)$ and due to Proposition 7.2.4 we have that

$$srk(P) = srk(\prod_{i=1}^{n} p(x_i, y_i, z_i)) \leq \exp((H(\Gamma) + o(1))n).$$

Let now $S = (g_1, g_2, \ldots, g_\ell)$ be a sequence of elements in $\mathbb{F}_q^n$ such that every subsequence of length three g_1', g_2', g_3' of S satisfies $g_1'g_2' + g_2'g_3' + g_3'g_1' \neq 0$. Then, recalling Corollary 7.2.2, we have that

$$|S| \leq 2(n+1)srk(P) \leq \exp((H(\Gamma) + o(1))n).$$

Hence the claim follows by setting $a = \exp(H(\Gamma))$. □

REMARK 7.2.3. *We observe that, in the previous theorem, for $q = 3$ we obtain a weaker bound than for the other cases of q. Indeed, in this case*

$$\Gamma = \{(0,0,0), (2,2,0), (0,2,2), (2,0,2), (2,1,1), (1,2,1), (1,1,2)\}$$

and one can easily check that defining Y that has, neatly, the distribution

$$(1/4, 1/12, 1/12, 1/12, 1/6, 1/6, 1/6)$$

over Γ, Y_1, Y_2 and Y_3 have all uniform distributions. It follows that, in this case, $H(\Gamma) = \log(3)$ and hence our proof fails to provide a better upper bound for $q = 3$.

We note that, to compute $H(\Gamma)$ in the previous theorem, we need to solve a convex optimization problem. Using standard mathematical software we have been able to find an upper bound for $H(\Gamma)$ only in the following cases.

q	9	27	81	243
$H(\Gamma)$	2.118	3.082	4.07	5.074

For the other values of q (i.e. $q > 243$) we have not been able to explicitly evaluate $H(\Gamma)$ since it seems that there are too many variables for this problem to be treated even with the help of a computer. Hence we do not provide an explicit upper bound on $EGZ(3, \mathbb{F}_q^n, 2)$ for $q > 243$. Also developing the product that defines P and trying to group the slices as done by Naslund and Sawin in [97] appears not helpful in this problem. On the other hand, we believe it is interesting that we can prove, just theoretically, the upper bound of Theorem 7.2.4.

Bibliography

[1] Matti Aaltonen. "A new upper bound on nonbinary block codes". In: *Discrete Mathematics* 83 (2-3 Aug. 1990), pp. 139–160.

[2] Abhishek Agarwal et al. "Group Testing with Runlength Constraints for Topological Molecular Storage". In: *IEEE International Symposium on Information Theory - Proceedings* 2020-June (June 2020), pp. 132–137.

[3] A. Ahmed, M. Azimli, and I. Anderson. "Rotational terraces from rectangular arrays." In: *Bulletin Inst. Combin. Appl.* (2011), pp. 4–12.

[4] Tanbir Ahmed et al. "Power Sum Polynomials as Relaxed EGZ Polynomials." In: *Integers* 19 (2019), A49.

[5] Matthew Aldridge, Oliver Johnson, and Jonathan Scarlett. "Group testing: An information theory perspective". In: *Foundations and Trends in Communications and Information Theory* 15 (3-4 Dec. 2019), pp. 196–392.

[6] Iskander Aliev. "Siegel's Lemma and Sum-Distinct Sets". In: *Discrete & Computational Geometry 2008 39:1* 39 (1 Mar. 2008), pp. 59–66.

[7] Noga Alon. "Combinatorial Nullstellensatz". In: *Combinatorics, Probability and Computing* 8 (1-2 1999), pp. 7–29.

[8] Noga. Alon and Joel H. Spencer. *The probabilistic method*. Wiley, 2016, p. 375. ISBN: 978-1-119-06195-3.

[9] B. Alspach, D. L. Kreher, and A. Pastine. "he Friedlander-Gordon-Miller Conjecture is true". In: *Australasian Journal of Combinatorics* (2017), pp. 11–24.

[10] B. Alspach and G. Liversidge. "On strongly sequenceable abelian groups". In: *The Art of Discrete and Applied Mathematics* 3 (1 July 2020), #P1.02–#P1.02.

[11] Brian Alspach, Donald L. Kreher, and Adrian Pastine. "Sequencing partial Steiner triple systems". In: *Journal of Combinatorial Designs* 28 (4 Apr. 2020), pp. 327–343.

[12] "An improved bound on the zero-error list-decoding capacity of the 4/3 channel". In: *IEEE International Symposium on Information Theory - Proceedings* (Aug. 2017), pp. 1658–1662.

[13] D. Archdeacon et al. "On Partial Sums in Cyclic Groups". In: *Journal of Combinatorial Mathematics and Combinatorial Computing* 98 (Jan. 2015).

[14] Dan Archdeacon. "Heffter Arrays and Biembedding Graphs on Surfaces". In: *The Electronic Journal of Combinatorics* 22 (1 Mar. 2015), P1.74–P1.74.

[15] Erdal Arikan. "An improved graph-entropy bound for perfect hashing". In: *IEEE International Symposium on Information Theory - Proceedings* (1994), p. 314.

[16] Erdal Arikan. "An Upper Bound on the Zero-Error List-Coding Capacity". In: *IEEE Transactions on Information Theory* 40 (4 1994), pp. 1237–1240.

[17] Maria Axenovich, Yair Caro, and Raphael Yuster. *Sum-distinguishing number of sparse hypergraphs*. 2021.

[18] Jaegug Bae. "On subset-sum-distinct sequences". In: *Analytic Number Theory* (1996), pp. 31–37.

[19] Alexander Barg, G Robert Blakley, and Gregory A Kabatiansky. “Digital fingerprinting codes: Problem statements, constructions, identification of traitors”. In: *IEEE Transactions on Information Theory* 49.4 (2003), pp. 852–865.

[20] Siddharth Bhandari and Jaikumar Radhakrishnan. “Bounds on the Zero-Error List-Decoding Capacity of the q/(q - 1) Channel”. In: *IEEE Transactions on Information Theory* 68 (1 Jan. 2022), pp. 238–247.

[21] Arie Bialostocki and Tran Dinh Luong. “An Analogue of the Erdős–Ginzburg–Ziv Theorem for Quadratic Symmetric Polynomials”. In: *Integers* (2009).

[22] Arie Bialostocki and Tran Dinh Luong. “Cubic symmetric polynomials yielding variations of the Erdős–Ginzburg–Ziv theorem”. In: *Acta Mathematica Hungarica* 142.1 (2014), pp. 152–166.

[23] Jared Bitz, Sarah Griffith, and Xiaoyu He. “Exponential lower bounds on the generalized Erdős–Ginzburg–Ziv constant”. In: *Discrete Mathematics* 343.12 (2020), p. 112083.

[24] Simon R. Blackburn. “Frameproof Codes”. In: *SIAM Journal on Discrete Mathematics* 16 (3 Aug. 2006), pp. 499–510.

[25] Simon R. Blackburn. “Probabilistic Existence Results for Separable Codes”. In: *IEEE Transactions on Information Theory* 61 (11 Nov. 2015), pp. 5822–5827.

[26] Jens P. Bode and Heiko Harborth. “Directed paths of diagonals within polygons”. In: *Discrete Mathematics* 299 (1-3 Aug. 2005), pp. 3–10.

[27] Tom Bohman. “A construction for sets of integers with distinct subset sums”. In: *The Electronic Journal of Combinatorics* 5 (1 1998), R3–R3.

[28] Dan Boneh and James Shaw. “Collusion-secure fingerprinting for digital data”. In: *IEEE Transactions on Information Theory* 44 (5 1998), pp. 1897–1905.

[29] Annalisa De Bonis, Leszek Gasieniec, and Ugo Vaccaro. “Optimal Two-Stage Algorithms for Group Testing Problems”. In: *SIAM Journal on Computing* 34 (5 July 2006), pp. 1253–1270.

[30] Sander Borst. “Using the slice rank for finding upper bounds on the size of cap sets”. In: *Bachelor thesis* (2018).

[31] Yair Caro. “Zero-sum problems—a survey”. In: *Discrete Mathematics* 152.1-3 (1996), pp. 93–113.

[32] Yair Caro, Benjamin Girard, and John Schmitt. “Higher Degree Davenport Constants over Finite Commutative Rings”. In: *Integers* (Feb. 2021), #A120.

[33] Yair Caro and John R Schmitt. “Higher Degree Erdos-Ginzburg-Ziv Constants”. In: *Integers* (July 2022), #A102.

[34] Yeow Meng Chee and Xiande Zhang. “Improved constructions of frameproof codes”. In: *IEEE transactions on information theory* 58.8 (2012), pp. 5449–5453.

[35] Minquan Cheng, Lijun Ji, and Ying Miao. “Separable codes”. In: *IEEE Transactions on Information Theory* 58 (3 Mar. 2012), pp. 1791–1803.

[36] Minquan Cheng and Ying Miao. “On anti-collusion codes and detection algorithms for multimedia fingerprinting”. In: *IEEE Transactions on Information Theory* 57 (7 July 2011), pp. 4843–4851.

[37] Yongxi Cheng, Ding Zhu Du, and Guohui Lin. “On the upper bounds of the minimum number of rows of disjunct matrices”. In: *Optimization Letters 2008 3:2* 3 (2 Nov. 2008), pp. 297–302.

[38] G. érard Cohen, Simon Litsyn, and Gilles Zémor. “Binary B2-Sequences : A New Upper Bound”. In: *Journal of Combinatorial Theory, Series A* 94 (1 Apr. 2001), pp. 152–155.

[39] S. Costa and M. A. Pellegrini. "Some new results about a conjecture by Brian Alspach". In: *Archiv der Mathematik* 115 (5 Nov. 2020), pp. 479–488.

[40] S. Costa et al. "A problem on partial sums in abelian groups". In: *Discrete Mathematics* 341 (3 Mar. 2018), pp. 705–712.

[41] Simone Costa and Marco Dalai. "A gap in the slice rank of k-tensors". In: *Journal of Combinatorial Theory, Series A* 177 (Jan. 2021), p. 105335.

[42] Simone Costa and Marco Dalai. "New bounds for perfect k-hashing". In: *Discrete Applied Mathematics* 289 (Jan. 2021), pp. 374–382.

[43] Simone Costa, Marco Dalai, and Stefano Della Fiore. "Variations on the Erdős distinct-sums problem". In: *Discrete Applied Mathematics* 325 (2023), pp. 172–185.

[44] Simone Costa and Stefano Della Fiore. "Weak sequenceability in cyclic groups". In: *Journal of Combinatorial Designs* 30.12 (2022), pp. 735–751.

[45] Simone Costa et al. "On Sequences in Cyclic Groups with Distinct Partial Sums". In: *The Electronic Journal of Combinatorics* 29 (3 Aug. 2022), P3.33–P3.33.

[46] Ernie Croot, Vsevolod F Lev, and Péter Pál Pach. "Progression-free sets in are exponentially small". In: *Annals of Mathematics* (2017), pp. 331–337.

[47] I. Csiszár and P.C. Shields. "Information Theory and Statistics: A Tutorial". In: *Foundations and Trends® in Communications and Information Theory* 1.4 (2004), pp. 417–528.

[48] D. R. Stinson D. L. Kreher and S. Veitch. "Block-avoiding point sequencings of directed triple systems". In: *Discrete Mathematics* 343 (4 Apr. 2020), p. 111773.

[49] Arkadii D'Yachkov et al. "Separable Codes for the Symmetric Multiple-Access Channel". In: *IEEE Transactions on Information Theory* 65 (6 June 2019), pp. 3738–3750.

[50] Marco Dalai, Venkatesan Guruswami, and Jaikumar Radhakrishnan. "An Improved Bound on the Zero-Error List-Decoding Capacity of the 4/3 Channel". In: *IEEE Transactions on Information Theory* 66 (2 Feb. 2020), pp. 749–756.

[51] Annalisa De Bonis and Ugo Vaccaro. "A new kind of selectors and their applications to conflict resolution in wireless multichannels networks". In: (2017), pp. 45–61.

[52] Annalisa De Bonis and Ugo Vaccaro. "A new kind of selectors and their applications to conflict resolution in wireless multichannels networks". In: *Theoretical Computer Science* 806 (2020), pp. 219–235.

[53] Stefano Della Fiore, Marco Dalai, and Ugo Vaccaro. "Achievable Rates and Algorithms for Group Testing with Runlength Constraints". In: (2022), pp. 576–581.

[54] Stefano Della Fiore, Alessandro Gnutti, and Sven Polak. "The maximum cardinality of trifferent codes with lengths 5 and 6". In: *Examples and Counterexamples* 2 (2022), p. 100051.

[55] Sage Developers. *Sage Mathematics Software*. 2022.

[56] Robert Dorfman. "The Detection of Defective Members of Large Populations". In: *The Annals of Mathematical Statistics* 14.4 (1943), pp. 436–440.

[57] Ding Zhu Du and Frank K. Hwang. "Pooling designs and nonadaptive group testing: Important tools for dna sequencing". In: *Pooling Designs And Nonadaptive Group Testing: Important Tools For Dna Sequencing* (Jan. 2006), pp. 1–237.

[58] Quentin Dubroff, Jacob Fox, and Max Wenqiang Xu. "A Note on the Erdös Distinct Subset Sums Problem". In: *SIAM Journal on Discrete Mathematics* 35 (1 Mar. 2021), pp. 322–324.

[59] Peter Elias. "Zero Error Capacity Under List Decoding". In: *IEEE Transactions on Information Theory* 34 (5 1988), pp. 1070–1074.

[60] Peter Elias. “Zero error capacity under list decoding”. In: *IEEE Transactions on Information Theory* 34.5 (1988), pp. 1070–1074.

[61] Noam D. Elkies. “An improved lower bound on the greatest element of a sum-distinct set of fixed order”. In: *Journal of Combinatorial Theory, Series A* 41 (1 Jan. 1986), pp. 89–94.

[62] Jordan S Ellenberg and Dion Gijswijt. “On large subsets of with no three-term arithmetic progression”. In: *Annals of Mathematics* (2017), pp. 339–343.

[63] Paul Erdos, Abraham Ginzburg, and Abraham Ziv. “Theorem in the additive number theory”. In: *Bull. Res. Council Israel F* 10 (1961), pp. 41–43.

[64] P. Erdös, P. Frankl, and Z. Füredi. “Families of finite sets in which no set is covered by the union of r others”. In: *Israel Journal of Mathematics 1985 51:1* 51 (1 Dec. 1985), pp. 79–89.

[65] Paul Erdős and László Lovász. “Problems and results on 3-chromatic hypergraphs and some related questions”. In: *Colloquia Mathematica Societatis Janos Bolyai 10. Infinite and Finite Sets, Keszthely (Hungary)*. Citeseer. 1973.

[66] Stefano Della Fiore, Simone Costa, and Marco Dalai. *GAP Code*. URL: `https://www.stefano-dellafiore.me/additional_material_bk_hashing.zip`.

[67] Stefano Della Fiore, Simone Costa, and Marco Dalai. “Improved Bounds for (b, k)-Hashing”. In: *IEEE Transactions on Information Theory* 68 (8 Aug. 2022), pp. 4983–4997.

[68] Stefano Della Fiore, Simone Costa, and Marco Dalai. “New upper bounds for (b, k)-hashing”. In: *IEEE International Symposium on Information Theory - Proceedings* 2021-July (July 2021), pp. 256–261.

[69] Stefano Della Fiore and Marco Dalai. “A note on 2-separable codes and B2 codes”. In: *Discrete Mathematics* 345 (3 Mar. 2022), p. 112751.

[70] Jacob Fox and Lisa Sauermann. “Erd\H {o}s-Ginzburg-Ziv Constants by Avoiding Three-Term Arithmetic Progressions”. In: *The Electronic Journal of Combinatorics* 25.2 (2018), pp. 2–14.

[71] Richard Friedlander, Basil Gordon, and Michael Miller. “On a group sequencing problem of Ringel”. In: *Congr Numer* 21 (Jan. 1978).

[72] Fei Gao and Gennian Ge. “New bounds on separable codes for multimedia fingerprinting”. In: *IEEE Transactions on Information Theory* 60 (9 2014), pp. 5257–5262.

[73] Weidong Gao and Alfred Geroldinger. “Zero-sum problems in finite abelian groups: a survey”. In: *Expositiones Mathematicae* 24.4 (2006), pp. 337–369.

[74] Luisa Gargano, Adele Anna Rescigno, and Ugo Vaccaro. “Low-weight superimposed codes and related combinatorial structures: Bounds and applications”. In: *Theoretical Computer Science* 806 (Feb. 2020), pp. 655–672.

[75] D.C. Gijswijt. “Matrix Algebras and Semidefinite Programming Techniques for Codes”. University of Amsterdam, 2005.

[76] Basil Gordon. “Sequences in groups with distinct partial products.” In: *Pacific Journal of Mathematics* 11.4 (1961), pp. 1309–1313.

[77] R. L. Graham. “On sums of integers taken from a fixed sequence”. In: *Proceedings, Washington State University Conference on Number Theory* (1971), pp. 22–40.

[78] Yujie Gu, Jinping Fan, and Ying Miao. “Improved Bounds for Separable Codes and B2 Codes”. In: *IEEE Communications Letters* 24 (1 Jan. 2020), pp. 15–19.

[79] Chuan Guo, Douglas R Stinson, and Tran Van Trung. “On tight bounds for binary frameproof codes”. In: *Designs, Codes and Cryptography* 77.2 (2015), pp. 301–319.

[80] Venkatesan Guruswami and Andrii Riazanov. "Beating Fredman-Komlós for perfect k-hashing". In: *Journal of Combinatorial Theory, Series A* 188 (May 2022), p. 105580.

[81] Richard K. Guy. "Sets of Integers Whose Subsets Have Distinct Sums". In: *North-Holland Mathematics Studies* 60 (C Jan. 1982), pp. 141–154.

[82] G. Hansel. "Nombre minimal de contacts de fermeture nécessaire pour réaliser une fonction booléenne symétrique de n variables". In: *C.R. Acad. Sci. Paris* (1964), pp. 6037–6040.

[83] Harper. "Optimal numberings and isoperimetric problems on graphs". In: *Journal of Combinatorial Theory* 1 (3 Jan. 1966), pp. 385–393.

[84] Jacob Hicks, M. A. Ollis, and John R. Schmitt. "Distinct partial sums in cyclic groups: polynomial method and constructive approaches". In: *Journal of Combinatorial Designs* 27 (6 June 2019), pp. 369–385.

[85] W. H. Kautz and R. C. Singleton. "Nonrandom Binary Superimposed Codes". In: *IEEE Transactions on Information Theory* 10 (4 1964), pp. 363–377.

[86] Janos Komlos and Albert G. Greenberg. "An Asymptotically Nonadaptive Algorithm for Conflict Resolution in Multiple-Access Channels". In: *IEEE Transactions on Information Theory* 31 (2 1985), pp. 302–306.

[87] J. Korner. "Fredman–Komlós bounds and information theory". In: *SIAM Journal on Algebraic Discrete Methods* 7 (4 July 2006), pp. 560–570.

[88] J. Korner and K. Marton. "New Bounds for Perfect Hashing via Information Theory". In: *European Journal of Combinatorics* 9 (6 Nov. 1988), pp. 523–530.

[89] Donald L Kreher and Douglas R Stinson. "Block-avoiding sequencings of points in Steiner triple systems". In: *The Australasian Journal of Combinatorics* 74.3 (2019).

[90] Bernt Lindström. "On B2-sequences of vectors". In: *Journal of Number Theory* 4 (3 June 1972), pp. 261–265.

[91] Bart Litjens, Sven Polak, and Alexander Schrijver. "Semidefinite bounds for nonbinary codes based on quadruples". In: *Designs, Codes and Cryptography 2016 84:1* 84 (1 May 2016), pp. 87–100.

[92] László Lovász. "On the Shannon capacity of a graph". In: *IEEE Transactions on Information theory* 25.1 (1979), pp. 1–7.

[93] W. F. Lunnon. "Integer Sets with Distinct Subset-Sums". In: *Mathematics of Computation* 50.181 (1988), pp. 297–320.

[94] Mateusz Michalek. "A Short Proof of Combinatorial Nullstellensatz". In: *The American Mathematical Monthly* 117.9 (2010), pp. 821–823.

[95] R. A. Moser and G. Tardos. "A constructive proof of the general lovasz local lemma". In: *Journal of the ACM (JACM)* 57 (2 Feb. 2010).

[96] Eric Naslund. "Exponential bounds for the Erdős-Ginzburg-Ziv constant". In: *Journal of Combinatorial Theory, Series A* 174 (2020), p. 105185.

[97] Eric Naslund and Will Sawin. "Upper bounds for sunflower-free sets". In: *Forum of Mathematics, Sigma*. Vol. 5. Cambridge University Press. 2017.

[98] A. Nilli. "Perfect Hashing and Probability". In: *Combinatorics, Probability and Computing* 3 (3 1994), pp. 407–409.

[99] M. A. Ollis. "Sequenceable Groups and Related Topics". In: *The Electronic Journal of Combinatorics* (2009), DS10: May 31–2013.

[100] "On the Size of Separating Systems and Families of Perfect Hash Functions". In: *SIAM Journal on Matrix Analysis and Applications* 5 (1 July 2006), pp. 61–68.

[101] Erdos Paul. "Problems and results in additive number theory". In: *Colloque sur la Theorie des Nombres* (1955), pp. 122–137.

[102] Cosmin Pohoata and Dmitriy Zakharov. "On the trifference problem for linear codes". In: *IEEE Transactions on Information Theory* (2022).

[103] J. Radhakrishnan. *Entropy and Counting*. URL: `https://www.tcs.tifr.res.in/~jaikumar/Papers/EntropyAndCounting.pdf`.

[104] J. T. Schwartz. "Fast Probabilistic Algorithms for Verification of Polynomial Identities". In: *J. ACM* 27.4 (Oct. 1980), pp. 701–717. ISSN: 0004-5411.

[105] Chong Shangguan and Gennian Ge. "New bounds on the number of tests for disjunct matrices". In: *IEEE Transactions on Information Theory* 62 (12 Dec. 2016), pp. 7518–7521.

[106] Chong Shangguan et al. "New bounds for frameproof codes". In: *IEEE Transactions on Information Theory* 63.11 (2017), pp. 7247–7252.

[107] Claude Shannon. "The zero error capacity of a noisy channel". In: *IRE Transactions on Information Theory* 2.3 (1956), pp. 8–19.

[108] Simon Sidon. "Ein Satz über trigonometrische Polynome und seine Anwendung in der Theorie der Fourier-Reihen". In: *Mathematische Annalen* 106.1 (1932), pp. 536–539.

[109] Alexander Sidorenko. "On generalized Erdős–Ginzburg–Ziv constants for Z2d". In: *Journal of Combinatorial Theory, Series A* 174 (2020), p. 105254.

[110] Jessica N Staddon, Douglas R Stinson, and Ruizhong Wei. "Combinatorial properties of frameproof and traceability codes". In: *IEEE transactions on information theory* 47.3 (2001), pp. 1042–1049.

[111] Douglas R Stinson and Ruizhong Wei. "Combinatorial properties and constructions of traceability schemes and frameproof codes". In: *SIAM Journal on Discrete Mathematics* 11.1 (1998), pp. 41–53.

[112] Douglas R Stinson, Ruizhong Wei, and Kejun Chen. "On generalized separating hash families". In: *Journal of Combinatorial Theory, Series A* 115.1 (2008), pp. 105–120.

[113] Douglas R Stinson and Gregory M Zaverucha. "Some improved bounds for secure frameproof codes and related separating hash families". In: *IEEE Transactions on Information Theory* 54.6 (2008), pp. 2508–2514.

[114] Terence Tao. "A symmetric formulation of the Croot-Lev-Pach-Ellenberg-Gijswijt capset bound". In: *Tao's blog post* (2016).

[115] Terence Tao. *A symmetric formulation of the Croot–Lev-Pach-Ellenberg-Gijswijt capset bound*. 2016.

[116] Terence Tao and Will Sawin. "Notes on the "slice rank" of tensors". In: *Tao's blog post* (2016).

[117] Tran van Trung. "A tight bound for frameproof codes viewed in terms of separating hash families". In: *Designs, codes and cryptography* 72.3 (2014), pp. 713–718.

[118] Xin Wang. "Improved upper bounds for parent-identifying set systems and separable codes". In: *Designs, Codes, and Cryptography* 89 (1 Jan. 2021), pp. 91–104.

[119] Chaoping Xing and Chen Yuan. "Beating the probabilistic lower bound on perfect hashing". In: *Proceedings of the 2021 ACM-SIAM Symposium on Discrete Algorithms* (2021), pp. 33–41.

Acknowledgements

Firstly, I would like to express my sincere gratitude to my advisor Prof. Marco Dalai and my co-advisor Simone Costa for their continuous support during my PhD studies, and for their patience, motivation, and immense knowledge.

I would like to thank my parents for supporting me spiritually throughout these years and my life in general. Thank you both for giving me strength to reach my dreams. A special thank to Veronica, my partner, for the patience and support that she always gave to me and for having celebrated every success with me.

Last but not least a thank goes to all my family and friends that have always supported and encouraged me in difficult moments.