An overview of the Graham's rearrangement conjecture

Stefano Della Fiore

Università degli studi di Brescia
Dipartimento di Ingegneria dell'Informazione

YoungPeople4Math, SemMat, Brescia, 2025

Graham's rearrangement conjecture

Let A be a finite subset of an abelian group.

An ordering $a_1, a_2, \ldots, a_{|A|}$ of A is *valid* if the partial sums

$$a_1, a_1 + a_2, \ldots, a_1 + a_2 + \ldots + a_{|A|}$$

are all distinct. Moreover, this ordering is called a *sequencing* if it is valid and $a_i + \ldots + a_j \neq 0$ for any $(i, j) \neq (1, |A|)$.

Conjecture (Graham (1971); Erdős and Graham (1980))

Let p be a prime. Then every subset $A \subseteq \mathbb{Z}_p \setminus \{0\}$ has a valid ordering.

Graham's rearrangement conjecture

Let A be a finite subset of an abelian group.

An ordering $a_1, a_2, \ldots, a_{|A|}$ of A is *valid* if the partial sums

$$a_1, a_1 + a_2, \ldots, a_1 + a_2 + \ldots + a_{|A|}$$

are all distinct. Moreover, this ordering is called a *sequencing* if it is valid and $a_i + \ldots + a_j \neq 0$ for any $(i, j) \neq (1, |A|)$.

Conjecture (Graham (1971); Erdős and Graham (1980))

Let p be a prime. Then every subset $A \subseteq \mathbb{Z}_p \setminus \{0\}$ has a valid ordering.

Graham's rearrangement conjecture

Example

Let $p = 5$ and $A = \{1, 2, 3, 4\} \subset \mathbb{Z}_5$. The ordering $1, 2, 3, 4$ is not valid since $1 = 1 + 2 + 3$ while the ordering $1, 3, 4, 2$ is valid since the partial sums are $1, 4, 3, 0$.

The only valid orderings of A beginning with 1 are $1, 3, 4, 2$ and $1, 2, 4, 3$ (with partial sums $1, 3, 2, 0$).

Conjecture (Alspach (∼2001))

Let G be an abelian group. Then every finite subset $A \subseteq G \setminus \{0\}$ has a valid ordering.

Graham's rearrangement conjecture

Example

Let $p = 5$ and $A = \{1, 2, 3, 4\} \subset \mathbb{Z}_5$. The ordering $1, 2, 3, 4$ is not valid since $1 = 1 + 2 + 3$ while the ordering $1, 3, 4, 2$ is valid since the partial sums are $1, 4, 3, 0$.

The only valid orderings of A beginning with 1 are $1, 3, 4, 2$ and $1, 2, 4, 3$ (with partial sums $1, 3, 2, 0$).

Conjecture (Alspach ($\sim$2001))

Let G be an abelian group. Then every finite subset $A \subseteq G \setminus \{0\}$ has a valid ordering.

Graham's rearrangement conjecture

Example

Let $p = 5$ and $A = \{1, 2, 3, 4\} \subset \mathbb{Z}_5$. The ordering $1, 2, 3, 4$ is not valid since $1 = 1 + 2 + 3$ while the ordering $1, 3, 4, 2$ is valid since the partial sums are $1, 4, 3, 0$.

The only valid orderings of A beginning with 1 are $1, 3, 4, 2$ and $1, 2, 4, 3$ (with partial sums $1, 3, 2, 0$).

Conjecture (Alspach (∼2001))

Let G be an abelian group. Then every finite subset $A \subseteq G \setminus \{0\}$ has a valid ordering.

Some motivation

This problem has connections to:

- Heffter arrays
- Non-zero sum Heffter arrays
- Graph decomposition
- Graceful labelings
- ...

Old and new results over $\mathbb{Z}_p$

Progress before 2024:

- Many authors (2005–2020): The conjecture holds for $|A| \leq 12$.
- Müyesser and Pokrovskiy (2022): The conjecture holds for $|A| \geq p - p^{1/1000}$. Earlier authors proved it for $|A| \geq p - 3$.

Theorem (N. Kravitz (July 2024) – W. Sawin (2015))

Let p be a prime. Then every subset $A \subseteq \mathbb{Z}_p \setminus \{0\}$ of size $|A| \leq \log p / 2 \log\log p$ has a valid ordering.

Theorem (B. Bedert and N. Kravitz (Sept. 2024))

Let p be a large prime. Then every subset $A \subseteq \mathbb{Z}_p \setminus \{0\}$ of size $|A| \leq e^{c(\log p)^{1/4}}$ has a valid ordering.

Old and new results over $\mathbb{Z}_p$

Progress before 2024:

- Many authors (2005–2020): The conjecture holds for $|A| \leq 12$.
- Müyesser and Pokrovskiy (2022): The conjecture holds for $|A| \geq p - p^{1/1000}$. Earlier authors proved it for $|A| \geq p - 3$.

Theorem (N. Kravitz (July 2024) – W. Sawin (2015))

Let p be a prime. Then every subset $A \subseteq \mathbb{Z}_p \setminus \{0\}$ of size $|A| \leq \log p / 2 \log\log p$ has a valid ordering.

Theorem (B. Bedert and N. Kravitz (Sept. 2024))

Let p be a large prime. Then every subset $A \subseteq \mathbb{Z}_p \setminus \{0\}$ of size $|A| \leq e^{c(\log p)^{1/4}}$ has a valid ordering.

Old and new results over $\mathbb{Z}_p$

Progress before 2024:

- Many authors (2005–2020): The conjecture holds for $|A| \leq 12$.
- Müyesser and Pokrovskiy (2022): The conjecture holds for $|A| \geq p - p^{1/1000}$. Earlier authors proved it for $|A| \geq p - 3$.

Theorem (N. Kravitz (July 2024) – W. Sawin (2015))

Let p be a prime. Then every subset $A \subseteq \mathbb{Z}_p \setminus \{0\}$ of size $|A| \leq \log p / 2 \log\log p$ has a valid ordering.

Theorem (B. Bedert and N. Kravitz (Sept. 2024))

Let p be a large prime. Then every subset $A \subseteq \mathbb{Z}_p \setminus \{0\}$ of size $|A| \leq e^{c(\log p)^{1/4}}$ has a valid ordering.

The Polynomial Method – ACN

Theorem (Well-known)

Let $f \in \mathbb{F}[x]$ be a polynomial of degree t. If $S \subseteq \mathbb{F}$ satisfies $|S| \geq t+1$, then there exists an $s \in S$ such that $f(s) \neq 0$.

Generalization to multivariate polynomials.

Theorem (N. Alon (1999))

Let $f \in \mathbb{F}[x_1, \ldots, x_n]$ be a polynomial of degree $t_1 + \ldots + t_n$. Given $S_1, \ldots, S_n$ non-empty subset of $\mathbb{F}$ such that $|S_i| \geq t_i + 1$, there exists $s_1 \in S_1, \ldots, s_n \in S_n$ for which

$$f(s_1, \ldots, s_n) \neq 0\,,$$

as long as the coefficient of $x_1^{t_1} \cdots x_n^{t_n}$ is non-zero.

Let p be prime and take $A \subseteq \mathbb{Z}_p \setminus \{0\}$. To use the ACN, we take each $S_i \subseteq A$ and we need a polynomial f that is nonzero exactly when $x_1, \ldots, x_{|A|}$ is a sequencing of A.

The Polynomial Method – ACN

Theorem (Well-known)

Let $f \in \mathbb{F}[x]$ be a polynomial of degree t. If $S \subseteq \mathbb{F}$ satisfies $|S| \geq t+1$, then there exists an $s \in S$ such that $f(s) \neq 0$.

Generalization to multivariate polynomials.

Theorem (N. Alon (1999))

Let $f \in \mathbb{F}[x_1, \ldots, x_n]$ be a polynomial of degree $t_1 + \ldots + t_n$. Given $S_1, \ldots, S_n$ non-empty subset of $\mathbb{F}$ such that $|S_i| \geq t_i + 1$, there exists $s_1 \in S_1, \ldots, s_n \in S_n$ for which

$$f(s_1, \ldots, s_n) \neq 0\,,$$

as long as the coefficient of $x_1^{t_1} \cdots x_n^{t_n}$ is non-zero.

Let p be prime and take $A \subseteq \mathbb{Z}_p \setminus \{0\}$. To use the ACN, we take each $S_i \subseteq A$ and we need a polynomial f that is nonzero exactly when $x_1, \ldots, x_{|A|}$ is a sequencing of A.

The Polynomial Method – ACN

Theorem (Well-known)

Let $f \in \mathbb{F}[x]$ be a polynomial of degree t. If $S \subseteq \mathbb{F}$ satisfies $|S| \geq t+1$, then there exists an $s \in S$ such that $f(s) \neq 0$.

Generalization to multivariate polynomials.

Theorem (N. Alon (1999))

Let $f \in \mathbb{F}[x_1, \ldots, x_n]$ be a polynomial of degree $t_1 + \ldots + t_n$. Given $S_1, \ldots, S_n$ non-empty subset of $\mathbb{F}$ such that $|S_i| \geq t_i + 1$, there exists $s_1 \in S_1, \ldots, s_n \in S_n$ for which

$$f(s_1, \ldots, s_n) \neq 0\,,$$

as long as the coefficient of $x_1^{t_1} \cdots x_n^{t_n}$ is non-zero.

Let p be prime and take $A \subseteq \mathbb{Z}_p \setminus \{0\}$. To use the ACN, we take each $S_i \subseteq A$ and we need a polynomial f that is nonzero exactly when $x_1, \ldots, x_{|A|}$ is a sequencing of A.

HOS polynomial

Let $A \subseteq \mathbb{Z}_p \setminus \{0\}$ of size k. Hicks, Ollis and Schmitt introduced the following homogeneous polynomial

$$f(x_1, \ldots, x_k) = \prod_{1 \le i < j \le k} (x_j - x_i) \prod_{\substack{1 \le i < j \le k \\ (i,j) \neq (1,k)}} (x_i + \ldots + x_j)$$

To apply the ACN we need a nonzero coefficient on a monomial in f that divides $x_1^{k-1} \cdots x_k^{k-1}$ which has clearly degree $k(k-1)$. Since $\deg(f) = k(k-1) - 1$ there are k monomials that could work.

HOS polynomial

Let $A \subseteq \mathbb{Z}_p \setminus \{0\}$ of size k. Hicks, Ollis and Schmitt introduced the following homogeneous polynomial

$$f(x_1, \dots, x_k) = \boxed{\prod_{1 \le i < j \le k} (x_j - x_i)} \prod_{\substack{1 \le i < j \le k \\ (i,j) \ne (1,k)}} (x_i + \dots + x_j)$$

To apply the ACN we need a nonzero coefficient on a monomial in f that divides $x_1^{k-1} \cdots x_k^{k-1}$ which has clearly degree $k(k-1)$. Since $\deg(f) = k(k-1) - 1$ there are k monomials that could work.

HOS polynomial

Let $A \subseteq \mathbb{Z}_p \setminus \{0\}$ of size k. Hicks, Ollis and Schmitt introduced the following homogeneous polynomial

$$f(x_1, \ldots, x_k) = \prod_{1 \le i < j \le k} (x_j - x_i) \prod_{\substack{1 \le i < j \le k \\ (i,j) \neq (1,k)}} (x_i + \ldots + x_j)$$

To apply the ACN we need a nonzero coefficient on a monomial in f that divides $x_1^{k-1} \cdots x_k^{k-1}$ which has clearly degree $k(k-1)$. Since $\deg(f) = k(k-1) - 1$ there are k monomials that could work.

$\mathbb{Z}_p$ results

Theorem (J. Hicks, M. A. Ollis and J. R. Schmitt (2018))

Let p be a prime. Then every subset $A \subseteq \mathbb{Z}_p \setminus \{0\}$, $|A| \leq 10$, has a valid ordering.

Theorem (S. Costa, S. D. F., M. A. Ollis and S. R-Frydman (2022))

Let p be a prime. Then every subset $A \subseteq \mathbb{Z}_p \setminus \{0\}$, $|A| = 11, 12$, has a valid ordering.

For $A \subseteq \mathbb{Z}_p \setminus \{0\}$, $|A| = 12$ we have

monomial	coefficient
$x_1^{10} x_2^{11} x_3^{11} \cdots x_{12}^{11}$	$2^4 \cdot 3 \cdot 29 \cdot 1295307720839171988\,1$
$x_1^{11} x_2^{10} x_3^{11} \cdots x_{12}^{11}$	$2^3 \cdot 3 \cdot 277 \cdot 1901 \cdot 786640832519761$

$\mathbb{Z}_p$ results

Theorem (J. Hicks, M. A. Ollis and J. R. Schmitt (2018))

Let p be a prime. Then every subset $A \subseteq \mathbb{Z}_p \setminus \{0\}$, $|A| \leq 10$, has a valid ordering.

Theorem (S. Costa, S. D. F., M. A. Ollis and S. R-Frydman (2022))

Let p be a prime. Then every subset $A \subseteq \mathbb{Z}_p \setminus \{0\}$, $|A| = 11, 12$, has a valid ordering.

For $A \subseteq \mathbb{Z}_p \setminus \{0\}$, $|A| = 12$ we have

monomial	coefficient
$x_1^{10}x_2^{11}x_3^{11}\cdots x_{12}^{11}$	$2^4 \cdot 3 \cdot 29 \cdot 1295307720839171988l$
$x_1^{11}x_2^{10}x_3^{11}\cdots x_{12}^{11}$	$2^3 \cdot 3 \cdot 277 \cdot 1901 \cdot 786640832519761$

$\mathbb{Z}_p$ results

Theorem (J. Hicks, M. A. Ollis and J. R. Schmitt (2018))

Let p be a prime. Then every subset $A \subseteq \mathbb{Z}_p \setminus \{0\}$, $|A| \leq 10$, has a valid ordering.

Theorem (S. Costa, S. D. F., M. A. Ollis and S. R-Frydman (2022))

Let p be a prime. Then every subset $A \subseteq \mathbb{Z}_p \setminus \{0\}$, $|A| = 11, 12$, has a valid ordering.

For $A \subseteq \mathbb{Z}_p \setminus \{0\}$, $|A| = 12$ we have

monomial	coefficient
$x_1^{10}x_2^{11}x_3^{11}\cdots x_{12}^{11}$	$2^4 \cdot 3 \cdot 29 \cdot 1295307720839171 9881$
$x_1^{11}x_2^{10}x_3^{11}\cdots x_{12}^{11}$	$2^3 \cdot 3 \cdot 277 \cdot 1901 \cdot 786640832519761$

Sets of size tending to infinity

Theorem (N. Kravitz (July 2024) – W. Sawin (2015))

Let p be a prime. Then every subset $A \subseteq \mathbb{Z}_p \setminus \{0\}$ of size $|A| \leq \log p / 2 \log\log p$ has a valid ordering.

Proof sketch.

Rectification step: The Pigeonhole Principle provides a $\lambda \in \mathbb{Z}_p \setminus \{0\}$ such that $\lambda \cdot A$ is contained in $(-p/4|A|, p/4|A|)$. Since the subset sums in $\lambda \cdot A$ have no "wrap-around" we can work in $\mathbb{Z}$.

By induction on $|A|$, one can prove that every finite subset $A \subseteq \mathbb{Z} \setminus \{0\}$ has a valid ordering.

Sets of size tending to infinity

Theorem (N. Kravitz (July 2024) – W. Sawin (2015))

Let p be a prime. Then every subset $A \subseteq \mathbb{Z}_p \setminus \{0\}$ of size $|A| \leq \log p / 2 \log\log p$ has a valid ordering.

Proof sketch.

Rectification step: The Pigeonhole Principle provides a $\lambda \in \mathbb{Z}_p \setminus \{0\}$ such that $\lambda \cdot A$ is contained in $(-p/4|A|, p/4|A|)$. Since the subset sums in $\lambda \cdot A$ have no "wrap-around" we can work in $\mathbb{Z}$.

By induction on $|A|$, one can prove that every finite subset $A \subseteq \mathbb{Z} \setminus \{0\}$ has a valid ordering.

Sets of size quasi-polynomial

Theorem (B. Bedert and N. Kravitz (Sept. 2024))

Let p be a large prime. Then every subset $A \subseteq \mathbb{Z}_p \setminus \{0\}$ of size $|A| \leq e^{c(\log p)^{1/4}}$ has a valid ordering.

New Idea.

A set A to be not rectificable has to contain a large "dissociated set". A dissociated set D, $|D| = r$, is a set in which all the 2^r subset sums are distinct.

The dimension $dim(B)$ of a set B is the maximum size of a dissociated subset of B.

Theorem

Let $A \subseteq \mathbb{Z}_p$, $|A| \leq e^{c(\log p)^{1/4}}$. Then for some $\lambda \in \mathbb{Z}_p \setminus \{0\}$, $\lambda \cdot A = \cup_{j=1}^{s} D_j \cup E$ where each $|D_j|$ has size at least $c'(\log p)^{3/4}$ and E is rectifiable.

Sets of size quasi-polynomial

Theorem (B. Bedert and N. Kravitz (Sept. 2024))

Let p be a large prime. Then every subset $A \subseteq \mathbb{Z}_p \setminus \{0\}$ of size $|A| \le e^{c(\log p)^{1/4}}$ has a valid ordering.

New Idea.

A set A to be not rectificable has to contain a large "dissociated set". A dissociated set D, $|D| = r$, is a set in which all the 2^r subset sums are distinct.

The dimension $dim(B)$ of a set B is the maximum size of a dissociated subset of B.

Theorem

Let $A \subseteq \mathbb{Z}_p$, $|A| \le e^{c(\log p)^{1/4}}$. Then for some $\lambda \in \mathbb{Z}_p \setminus \{0\}$, $\lambda \cdot A = \cup_{j=1}^{s} D_j \cup E$ where each $|D_j|$ has size at least $c'(\log p)^{3/4}$ and E is rectifiable.

Sets of size quasi-polynomial

Theorem (B. Bedert and N. Kravitz (Sept. 2024))

Let p be a large prime. Then every subset $A \subseteq \mathbb{Z}_p \setminus \{0\}$ of size $|A| \leq e^{c(\log p)^{1/4}}$ has a valid ordering.

New Idea.

A set A to be not rectificable has to contain a large "dissociated set". A dissociated set D, $|D| = r$, is a set in which all the 2^r subset sums are distinct.

The dimension $dim(B)$ of a set B is the maximum size of a dissociated subset of B.

Theorem

Let $A \subseteq \mathbb{Z}_p$, $|A| \leq e^{c(\log p)^{1/4}}$. Then for some $\lambda \in \mathbb{Z}_p \setminus \{0\}$, $\lambda \cdot A = \cup_{j=1}^{s} D_j \cup E$ where each $|D_j|$ has size at least $c'(\log p)^{3/4}$ and E is rectifiable.

Finding the orderings - Probabilistic method

Goal: Find a valid ordering consisting of the positive elements of E, then the elements of the dissociated sets D_j's and then the negative elements of E.

Recall that the subset sums of a dissociated set are all distinct. In a random ordering of a R-element dissociated set, the length-k prefix sum assumes each of $\binom{R}{k}$ possible values with equal probability. This probability is very small as long as k is not too close to 0 or R.

- Inductively order the set E
- Randomly split the dissociated sets and then permute the newly splitted sets
- Randomly order each dissociated set

Finding the orderings - Probabilistic method

Goal: Find a valid ordering consisting of the positive elements of E, then the elements of the dissociated sets D_j's and then the negative elements of E.

Recall that the subset sums of a dissociated set are all distinct. In a random ordering of a R-element dissociated set, the length-k prefix sum assumes each of $\binom{R}{k}$ possible values with equal probability. This probability is very small as long as k is not too close to 0 or R.

- Inductively order the set E
- Randomly split the dissociated sets and then permute the newly splitted sets
- Randomly order each dissociated set

Finding the orderings - Probabilistic method

Goal: Find a valid ordering consisting of the positive elements of E, then the elements of the dissociated sets D_j's and then the negative elements of E.

Recall that the subset sums of a dissociated set are all distinct. In a random ordering of a R-element dissociated set, the length-k prefix sum assumes each of $\binom{R}{k}$ possible values with equal probability. This probability is very small as long as k is not too close to 0 or R.

- Inductively order the set E
- Randomly split the dissociated sets and then permute the newly splitted sets
- Randomly order each dissociated set

Our results

Generalizing the procedure of Bedert and Kravitz we get

Theorem (S. Costa, S. D. F. and E. Engel (2025+))

There exists a $c > 0$ such that every subset $A \subseteq \mathbb{Z}_p \rtimes_\varphi H \setminus \{id\}$ where $\varphi : H \to Aut(\mathbb{Z}_p)$ satisfies $\varphi(h) \in \{id, -id\}$ for each $h \in H$, where H is abelian and and all of its subsets have a sequencing, and where

$$|A| \leqslant e^{c(\log p)^{1/4}},$$

A has a sequencing.

A question

- Can we do better than $e^{c(\log p)^{1/4}}$ (quasi-polynomial)?

Our results

Generalizing the procedure of Bedert and Kravitz we get

Theorem (S. Costa, S. D. F. and E. Engel (2025+))

There exists a $c > 0$ such that every subset $A \subseteq \mathbb{Z}_p \rtimes_\varphi H \setminus \{id\}$ where $\varphi : H \to Aut(\mathbb{Z}_p)$ satisfies $\varphi(h) \in \{id, -id\}$ for each $h \in H$, where H is abelian and and all of its subsets have a sequencing, and where

$$|A| \leqslant e^{c(\log p)^{1/4}},$$

A has a sequencing.

A question

- Can we do better than $e^{c(\log p)^{1/4}}$ (quasi-polynomial)?

Thank you.