Sharper upper bounds for q-ary B_2 codes from Toeplitz SDPs

Stefano Della Fiore

Department of Information Engineering
University of Brescia

ISIT 2026

July 3, Guangzhou, China

B_2 codes

Code setting

We consider a q-ary code of length n:

$$C \subseteq [q]^n, \qquad [q] = \{0, 1, \ldots, q-1\}.$$

B_2 property

Let $c_i, c_j, c_k, c_\ell \in C$:

$$c_i + c_j = c_k + c_\ell \quad \Longrightarrow \quad \{i, j\} = \{k, \ell\}$$

where the sum is performed over $\mathbb{Z}^n$.

- Unique recovery of an unordered pair from its sum.
- Asymptotic rate: $R = \limsup_{n\to\infty} \frac{1}{n} \log_q |C_n|$.
- Additive collisions become entropy inequalities.

B_2 codes

Code setting

We consider a q-ary code of length n:

$$C \subseteq [q]^n, \qquad [q] = \{0, 1, \ldots, q-1\}.$$

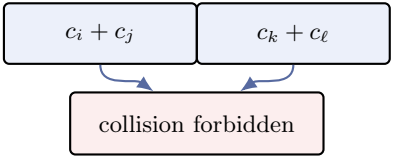
B_2 property

Let $c_i, c_j, c_k, c_\ell \in C$:

$$c_i + c_j = c_k + c_\ell \quad \Longrightarrow \quad \{i, j\} = \{k, \ell\}$$

where the sum is performed over $\mathbb{Z}^n$.

- Unique recovery of an unordered pair from its sum.
- Asymptotic rate: $R = \limsup_{n\to\infty} \frac{1}{n} \log_q |C_n|$.
- Additive collisions become entropy inequalities.



injectivity of
the sum map

B_2 codes

Code setting

We consider a q-ary code of length n:

$$C \subseteq [q]^n, \qquad [q] = \{0, 1, \ldots, q-1\}.$$

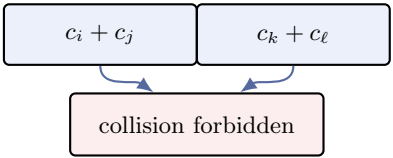
B_2 property

Let $c_i, c_j, c_k, c_\ell \in C$:

$$c_i + c_j = c_k + c_\ell \quad \Longrightarrow \quad \{i, j\} = \{k, \ell\}$$

where the sum is performed over $\mathbb{Z}^n$.

- Unique recovery of an unordered pair from its sum.
- Asymptotic rate: $R = \limsup_{n\to\infty} \frac{1}{n} \log_q |C_n|$.
- Additive collisions become entropy inequalities.



injectivity of
the sum map

B_2 codes

Code setting

We consider a q-ary code of length n:

$$C \subseteq [q]^n, \qquad [q] = \{0, 1, \ldots, q-1\}.$$

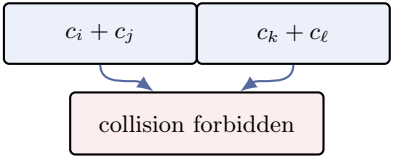
B_2 property

Let $c_i, c_j, c_k, c_\ell \in C$:

$$c_i + c_j = c_k + c_\ell \quad \Longrightarrow \quad \{i, j\} = \{k, \ell\}$$

where the sum is performed over $\mathbb{Z}^n$.

- Unique recovery of an unordered pair from its sum.
- Asymptotic rate: $R = \limsup_{n\to\infty} \frac{1}{n} \log_q |C_n|$.
- Additive collisions become entropy inequalities.



injectivity of
the sum map

Talk outline

1. Local entropy problem: the difference $D = X - Y$.
2. Fourier positivity and Toeplitz PSD constraints.
3. Prefix–suffix proof for q-ary B_2 codes.
4. Constant-weight adaptation via distance distributions.
5. Numerical comparison of the resulting bounds.

Talk outline

1. Local entropy problem: the difference $D = X - Y$.
2. Fourier positivity and Toeplitz PSD constraints.
3. Prefix–suffix proof for q-ary B_2 codes.
4. Constant-weight adaptation via distance distributions.
5. Numerical comparison of the resulting bounds.

Talk outline

1. Local entropy problem: the difference $D = X - Y$.
2. Fourier positivity and Toeplitz PSD constraints.
3. Prefix–suffix proof for q-ary B_2 codes.
4. Constant-weight adaptation via distance distributions.
5. Numerical comparison of the resulting bounds.

Talk outline

1. Local entropy problem: the difference $D = X - Y$.
2. Fourier positivity and Toeplitz PSD constraints.
3. Prefix–suffix proof for q-ary B_2 codes.
4. Constant-weight adaptation via distance distributions.
5. Numerical comparison of the resulting bounds.

Talk outline

1. Local entropy problem: the difference $D = X - Y$.
2. Fourier positivity and Toeplitz PSD constraints.
3. Prefix–suffix proof for q-ary B_2 codes.
4. Constant-weight adaptation via distance distributions.
5. Numerical comparison of the resulting bounds.

The local object: the i.i.d. difference distribution

Let X, Y be i.i.d. on $[0, q-1]$ with pmf $P = (p_0, \dots, p_{q-1})$, and set

$$D = X - Y, \qquad D \in \{-(q-1), \dots, q-1\}.$$

Autocorrelation

$$r_k = \mathbb{P}(D = k) = \sum_{i=0}^{q-1-k} p_i p_{i+k}, \quad 0 \le k \le q-1,$$

$$r_{-k} = r_k, \qquad r_0 = \sum_i p_i^2 \ge \frac{1}{q}.$$

The key local quantity is $\mathrm{H}(D)$.

The local object: the i.i.d. difference distribution

Let X, Y be i.i.d. on $[0, q-1]$ with pmf $P = (p_0, \dots, p_{q-1})$, and set

$$D = X - Y, \qquad D \in \{-(q-1), \dots, q-1\}.$$

Autocorrelation

$$r_k = \mathbb{P}(D = k) = \sum_{i=0}^{q-1-k} p_i p_{i+k}, \quad 0 \le k \le q-1,$$

$$r_{-k} = r_k, \qquad r_0 = \sum_i p_i^2 \ge \frac{1}{q}.$$

The key local quantity is $\mathrm{H}(D)$.

The local object: the i.i.d. difference distribution

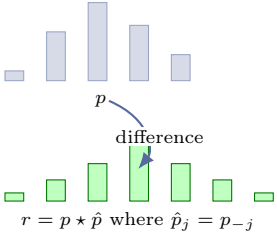
Let X, Y be i.i.d. on $[0, q-1]$ with pmf $P = (p_0, \dots, p_{q-1})$, and set

$$D = X - Y, \qquad D \in \{-(q-1), \dots, q-1\}.$$

Autocorrelation

$$r_k = \mathbb{P}(D = k) = \sum_{i=0}^{q-1-k} p_i p_{i+k}, \quad 0 \le k \le q-1,$$

$$r_{-k} = r_k, \qquad r_0 = \sum_i p_i^2 \ge \frac{1}{q}.$$



The key local quantity is $\mathrm{H}(D)$.

Fourier positivity: more structure than $r_0 \geq 1/q$

The characteristic function of D is

$$R(\theta) = \mathbb{E}\left[e^{i\theta(X-Y)}\right] = \left|\sum_{j=0}^{q-1} p_j e^{ij\theta}\right|^2 \geq 0.$$

Equivalently,

$$R(\theta) = \sum_{k=-(q-1)}^{q-1} r_k e^{ik\theta}$$

is a nonnegative trigonometric polynomial.

Old relaxation

Only used

$$r_0 \geq \frac{1}{q}.$$

This gives the coarse entropy upper bound $\bar{h}_q$.

New relaxation

Keep the full Fourier positivity:

$$r \in \Delta, \quad r_{-k} = r_k,$$
$$R(\theta) \geq 0 \quad \forall \theta.$$

Fourier positivity: more structure than $r_0 \geq 1/q$

The characteristic function of D is

$$R(\theta) = \mathbb{E}\left[e^{i\theta(X-Y)}\right] = \left|\sum_{j=0}^{q-1} p_j e^{ij\theta}\right|^2 \geq 0.$$

Equivalently,

$$R(\theta) = \sum_{k=-(q-1)}^{q-1} r_k e^{ik\theta}$$

is a nonnegative trigonometric polynomial.

Old relaxation

Only used

$$r_0 \geq \frac{1}{q}.$$

This gives the coarse entropy upper bound $\bar{h}_q$.

New relaxation

Keep the full Fourier positivity:

$$r \in \Delta, \quad r_{-k} = r_k,$$
$$R(\theta) \geq 0 \quad \forall \theta.$$

Fourier positivity: more structure than $r_0 \geq 1/q$

The characteristic function of D is

$$R(\theta) = \mathbb{E}\left[e^{i\theta(X-Y)}\right] = \left|\sum_{j=0}^{q-1} p_j e^{ij\theta}\right|^2 \geq 0.$$

Equivalently,

$$R(\theta) = \sum_{k=-(q-1)}^{q-1} r_k e^{ik\theta}$$

is a nonnegative trigonometric polynomial.

Old relaxation

Only used

$$r_0 \geq \frac{1}{q}.$$

This gives the coarse entropy upper bound $\bar{h}_q$.

New relaxation

Keep the full Fourier positivity:

$$r \in \Delta, \quad r_{-k} = r_k,$$
$$R(\theta) \geq 0 \quad \forall \theta.$$

Fourier positivity: more structure than $r_0 \geq 1/q$

The characteristic function of D is

$$R(\theta) = \mathbb{E}\left[e^{i\theta(X-Y)}\right] = \left|\sum_{j=0}^{q-1} p_j e^{ij\theta}\right|^2 \geq 0.$$

Equivalently,

$$R(\theta) = \sum_{k=-(q-1)}^{q-1} r_k e^{ik\theta}$$

is a nonnegative trigonometric polynomial.

Old relaxation

Only used

$$r_0 \geq \frac{1}{q}.$$

This gives the coarse entropy upper bound $\bar{h}_q$.

New relaxation

Keep the full Fourier positivity:

$$r \in \Delta, \quad r_{-k} = r_k,$$
$$R(\theta) \geq 0 \quad \forall \theta.$$

The entropy convex program

Define

$$h_q^\star = \sup \mathrm{H}(X - Y),$$

where the supremum is over all i.i.d. q-ary X, Y.

Fourier relaxation

$$\begin{aligned} h_q^{\mathrm{F}} = \max_r \quad & -\sum_{k=-(q-1)}^{q-1} r_k \log r_k \\ \text{s.t.} \quad & r_k \geq 0, \quad \sum_k r_k = 1, \quad r_{-k} = r_k, \\ & r_0 \geq \frac{1}{q}, \quad \sum_k r_k e^{ik\theta} \geq 0 \quad \forall \theta. \end{aligned}$$

Theorem (Entropy relaxation)

$$h_q^\star \leq h_q^{\mathrm{F}} \leq \bar{h}_q.$$

The entropy convex program

Define

$$h_q^\star = \sup \mathrm{H}(X - Y),$$

where the supremum is over all i.i.d. q-ary X, Y.

Fourier relaxation

$$\begin{aligned} h_q^{\mathrm{F}} = \max_r \quad & -\sum_{k=-(q-1)}^{q-1} r_k \log r_k \\ \text{s.t.} \quad & r_k \geq 0, \quad \sum_k r_k = 1, \quad r_{-k} = r_k, \\ & r_0 \geq \frac{1}{q}, \quad \sum_k r_k e^{ik\theta} \geq 0 \quad \forall \theta. \end{aligned}$$

Theorem (Entropy relaxation)

$$h_q^\star \leq h_q^{\mathrm{F}} \leq \bar{h}_q.$$

The entropy convex program

Define

$$h_q^\star = \sup \mathrm{H}(X - Y),$$

where the supremum is over all i.i.d. q-ary X, Y.

Fourier relaxation

$$\begin{aligned} h_q^{\mathrm{F}} = \max_r \quad & -\sum_{k=-(q-1)}^{q-1} r_k \log r_k \\ \text{s.t.} \quad & r_k \geq 0, \quad \sum_k r_k = 1, \quad r_{-k} = r_k, \\ & r_0 \geq \frac{1}{q}, \quad \sum_k r_k e^{ik\theta} \geq 0 \quad \forall \theta. \end{aligned}$$

Theorem (Entropy relaxation)

$$h_q^\star \leq h_q^{\mathrm{F}} \leq \bar{h}_q.$$

Toeplitz SDP and Gram interpretation

Set $r_k = 0$ for $|k| \geq q$ and define

$$T^{(N)}(r) = (r_{i-j})_{0 \leq i,j \leq N-1}.$$

Toeplitz formulation

Fourier positivity is equivalent to

$$T^{(N)}(r) \succeq 0 \quad \text{for all } N \geq 1.$$

Thus $h_q^{\mathrm{F}} = h_q^{\mathrm{SDP}}$.

Why PSD appears

Let $\tilde{p}^{(i)}$ be shifted copies of p. Then

$$\langle \tilde{p}^{(i)}, \tilde{p}^{(j)} \rangle = r_{i-j}.$$

Hence $T^{(N)}(r)$ is a Gram matrix.

Toeplitz SDP and Gram interpretation

Set $r_k = 0$ for $|k| \geq q$ and define

$$T^{(N)}(r) = (r_{i-j})_{0 \leq i,j \leq N-1}.$$

Toeplitz formulation

Fourier positivity is equivalent to

$$T^{(N)}(r) \succeq 0 \quad \text{for all } N \geq 1.$$

Thus $h_q^{\mathrm{F}} = h_q^{\mathrm{SDP}}$.

Why PSD appears

Let $\tilde{p}^{(i)}$ be shifted copies of p. Then

$$\langle \tilde{p}^{(i)}, \tilde{p}^{(j)} \rangle = r_{i-j}.$$

Hence $T^{(N)}(r)$ is a Gram matrix.

Toeplitz SDP and Gram interpretation

Set $r_k = 0$ for $|k| \geq q$ and define

$$T^{(N)}(r) = (r_{i-j})_{0 \leq i,j \leq N-1}.$$

Toeplitz formulation

Fourier positivity is equivalent to

$$T^{(N)}(r) \succeq 0 \quad \text{for all } N \geq 1.$$

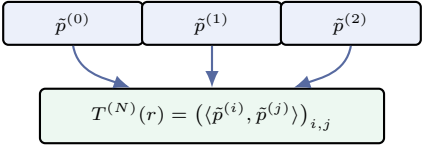
Thus $h_q^{\mathrm{F}} = h_q^{\mathrm{SDP}}$.

Why PSD appears

Let $\tilde{p}^{(i)}$ be shifted copies of p. Then

$$\langle \tilde{p}^{(i)}, \tilde{p}^{(j)} \rangle = r_{i-j}.$$

Hence $T^{(N)}(r)$ is a Gram matrix.



q-ary result: improved rate upper bound

Theorem (Main q-ary upper bound)

For integer $q \geq 2$, the asymptotic rate R_b of q-ary B_2 codes satisfies

$$R_b \leq \frac{h_q^{\mathrm{F}}}{\log q + h_q^{\mathrm{F}}},$$

where h_q^{F} is the Fourier–Toeplitz entropy bound.

Numerical certification

Impose $T^{(N)}(r) \succeq 0$ only for $N \leq N_{\max}$:

$$h_q^\star \leq h_q^{\mathrm{F}} \leq h_{q,N_{\max}}, \qquad R_b \leq \frac{h_{q,N_{\max}}}{\log q + h_{q,N_{\max}}}.$$

The truncation is a relaxation, hence the values are still certified upper bounds.

q-ary result: improved rate upper bound

Theorem (Main q-ary upper bound)

For integer $q \geq 2$, the asymptotic rate R_b of q-ary B_2 codes satisfies

$$R_b \leq \frac{h_q^{\mathrm{F}}}{\log q + h_q^{\mathrm{F}}},$$

where h_q^{F} is the Fourier–Toeplitz entropy bound.

Numerical certification

Impose $T^{(N)}(r) \succeq 0$ only for $N \leq N_{\max}$:

$$h_q^\star \leq h_q^{\mathrm{F}} \leq h_{q,N_{\max}}, \qquad R_b \leq \frac{h_{q,N_{\max}}}{\log q + h_{q,N_{\max}}}.$$

The truncation is a relaxation, hence the values are still certified upper bounds.

q-ary result: improved rate upper bound

Theorem (Main q-ary upper bound)

For integer $q \geq 2$, the asymptotic rate R_b of q-ary B_2 codes satisfies

$$R_b \leq \frac{h_q^{\mathrm{F}}}{\log q + h_q^{\mathrm{F}}},$$

where h_q^{F} is the Fourier–Toeplitz entropy bound.

Numerical certification

Impose $T^{(N)}(r) \succeq 0$ only for $N \leq N_{\max}$:

$$h_q^\star \leq h_q^{\mathrm{F}} \leq h_{q,N_{\max}}, \qquad R_b \leq \frac{h_{q,N_{\max}}}{\log q + h_{q,N_{\max}}}.$$

The truncation is a relaxation, hence the values are still certified upper bounds.

Proof architecture: prefix–suffix decomposition

Split each codeword into prefix length e and suffix length $f = n - e$:

$$c = (\ell, w), \qquad \ell \in [0, q-1]^e, \quad w \in [0, q-1]^f.$$

Group codewords by prefix:

$$P_i = \{(\ell_i, w) : w \in W_i\}, \qquad |P_i| = M_i.$$

Choose uniformly at random an ordered pair (X, Y) inside the same prefix classes:

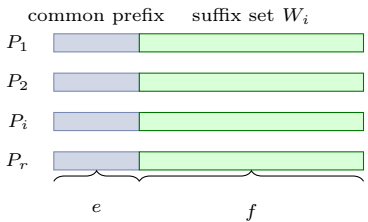
$$\mathrm{H}(X, Y) = \log \sum_i M_i^2.$$

Proof architecture: prefix–suffix decomposition

Split each codeword into prefix length e and suffix length $f = n - e$:

$$c = (\ell, w), \qquad \ell \in [0, q-1]^e, \quad w \in [0, q-1]^f.$$

Group codewords by prefix:



$$P_i = \{(\ell_i, w) : w \in W_i\}, \qquad |P_i| = M_i.$$

Choose uniformly at random an ordered pair (X, Y) inside the same prefix classes:

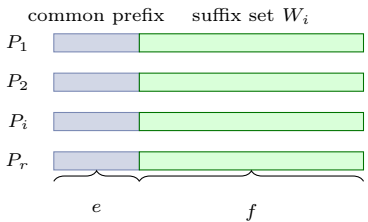
$$\mathrm{H}(X, Y) = \log \sum_i M_i^2.$$

Proof architecture: prefix–suffix decomposition

Split each codeword into prefix length e and suffix length $f = n - e$:

$$c = (\ell, w), \qquad \ell \in [0, q-1]^e, \quad w \in [0, q-1]^f.$$

Group codewords by prefix:



$$P_i = \{(\ell_i, w) : w \in W_i\}, \qquad |P_i| = M_i.$$

Choose uniformly at random an ordered pair (X, Y) inside the same prefix classes:

$$\mathrm{H}(X, Y) = \log \sum_i M_i^2.$$

Key injectivity lemma

Lemma

If C is B_2, then $(w_1, w_2) \mapsto w_1 - w_2$ is injective on ordered pairs of distinct suffixes drawn inside prefix classes.

Assume two suffix differences coincide:

$$w_1 - w_2 = w_3 - w_4.$$

Then

$$w_1 + w_4 = w_2 + w_3.$$

If prefixes are ℓ_h and ℓ_m, this gives

$$(\ell_h, w_1) + (\ell_m, w_4) = (\ell_h, w_2) + (\ell_m, w_3),$$

a forbidden B_2 collision.
Only diagonal pairs $X = Y$ are not covered by injectivity and must be controlled separately.

Key injectivity lemma

Lemma

If C is B_2, then $(w_1, w_2) \mapsto w_1 - w_2$ is injective on ordered pairs of distinct suffixes drawn inside prefix classes.

Assume two suffix differences coincide:

$$w_1 - w_2 = w_3 - w_4.$$

Then

$$w_1 + w_4 = w_2 + w_3.$$

If prefixes are ℓ_h and ℓ_m, this gives

$$(\ell_h, w_1) + (\ell_m, w_4) = (\ell_h, w_2) + (\ell_m, w_3),$$

a forbidden B_2 collision.
Only diagonal pairs $X = Y$ are not covered by injectivity and must be controlled separately.

Key injectivity lemma

Lemma

If C is B_2, then $(w_1, w_2) \mapsto w_1 - w_2$ is injective on ordered pairs of distinct suffixes drawn inside prefix classes.

Assume two suffix differences coincide:

$$w_1 - w_2 = w_3 - w_4.$$

Then

$$w_1 + w_4 = w_2 + w_3.$$

If prefixes are ℓ_h and ℓ_m, this gives

$$(\ell_h, w_1) + (\ell_m, w_4) = (\ell_h, w_2) + (\ell_m, w_3),$$

a forbidden B_2 collision.
Only diagonal pairs $X = Y$ are not covered by injectivity and must be controlled separately.

Key injectivity lemma

Lemma

If C is B_2, then $(w_1, w_2) \mapsto w_1 - w_2$ is injective on ordered pairs of distinct suffixes drawn inside prefix classes.

Assume two suffix differences coincide:

$$w_1 - w_2 = w_3 - w_4.$$

Then

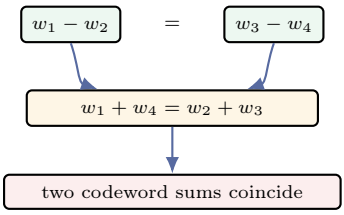
$$w_1 + w_4 = w_2 + w_3.$$

If prefixes are ℓ_h and ℓ_m, this gives

$$(\ell_h, w_1) + (\ell_m, w_4) = (\ell_h, w_2) + (\ell_m, w_3),$$

a forbidden B_2 collision.

Only diagonal pairs $X = Y$ are not covered by injectivity and must be controlled separately.



Key injectivity lemma

Lemma

If C is B_2, then $(w_1, w_2) \mapsto w_1 - w_2$ is injective on ordered pairs of distinct suffixes drawn inside prefix classes.

Assume two suffix differences coincide:

$$w_1 - w_2 = w_3 - w_4.$$

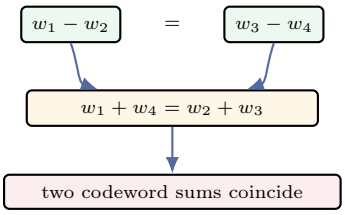
Then

$$w_1 + w_4 = w_2 + w_3.$$

If prefixes are ℓ_h and ℓ_m, this gives

$$(\ell_h, w_1) + (\ell_m, w_4) = (\ell_h, w_2) + (\ell_m, w_3),$$

a forbidden B_2 collision.
Only diagonal pairs $X = Y$ are not covered by injectivity and must be controlled separately.



Entropy accounting in the proof

Let $Z = X - Y \in \mathbb{Z}^f$ be the suffix difference. The injectivity lemma gives

$$\mathrm{H}(X, Y) = \mathrm{H}(Z) + \mathbb{P}(Z = 0)\, \mathrm{H}(X, Y \mid Z = 0).$$

Zero term

With

$$e = \left\lfloor \log_q(2M) - \log_q \log M \right\rfloor,$$

one has

$$\mathbb{P}(Z = 0)\, \mathrm{H}(X, Y \mid Z = 0) \le 2.$$

Difference entropy

By subadditivity,

$$\mathrm{H}(Z) \le \sum_{j=1}^{f} \mathrm{H}(Z_j) \le f h_q^{\mathrm{F}}.$$

Combine with Cauchy–Schwarz, $M^2/r \le \sum_i M_i^2$, and let $n \to \infty$.

Entropy accounting in the proof

Let $Z = X - Y \in \mathbb{Z}^f$ be the suffix difference. The injectivity lemma gives

$$\mathrm{H}(X, Y) = \mathrm{H}(Z) + \mathbb{P}(Z = 0)\, \mathrm{H}(X, Y \mid Z = 0).$$

Zero term

With

$$e = \left\lfloor \log_q(2M) - \log_q \log M \right\rfloor,$$

one has

$$\mathbb{P}(Z = 0)\, \mathrm{H}(X, Y \mid Z = 0) \le 2.$$

Difference entropy

By subadditivity,

$$\mathrm{H}(Z) \le \sum_{j=1}^{f} \mathrm{H}(Z_j) \le f h_q^{\mathrm{F}}.$$

Combine with Cauchy–Schwarz, $M^2/r \le \sum_i M_i^2$, and let $n \to \infty$.

Entropy accounting in the proof

Let $Z = X - Y \in \mathbb{Z}^f$ be the suffix difference. The injectivity lemma gives

$$\mathrm{H}(X, Y) = \mathrm{H}(Z) + \mathbb{P}(Z = 0)\, \mathrm{H}(X, Y \mid Z = 0).$$

Zero term

With

$$e = \left\lfloor \log_q(2M) - \log_q \log M \right\rfloor,$$

one has

$$\mathbb{P}(Z = 0)\, \mathrm{H}(X, Y \mid Z = 0) \le 2.$$

Difference entropy

By subadditivity,

$$\mathrm{H}(Z) \le \sum_{j=1}^{f} \mathrm{H}(Z_j) \le f h_q^{\mathrm{F}}.$$

Combine with Cauchy–Schwarz, $M^2/r \le \sum_i M_i^2$, and let $n \to \infty$.

Entropy accounting in the proof

Let $Z = X - Y \in \mathbb{Z}^f$ be the suffix difference. The injectivity lemma gives

$$\mathrm{H}(X, Y) = \mathrm{H}(Z) + \mathbb{P}(Z = 0)\, \mathrm{H}(X, Y \mid Z = 0).$$

Zero term

With

$$e = \left\lfloor \log_q(2M) - \log_q \log M \right\rfloor,$$

one has

$$\mathbb{P}(Z = 0)\, \mathrm{H}(X, Y \mid Z = 0) \le 2.$$

Difference entropy

By subadditivity,

$$\mathrm{H}(Z) \le \sum_{j=1}^{f} \mathrm{H}(Z_j) \le f h_q^{\mathrm{F}}.$$

Combine with Cauchy–Schwarz, $M^2/r \le \sum_i M_i^2$, and let $n \to \infty$.

Numerical impact for q-ary B_2 codes

	$q = 9$	10	11	12	13
New	**0.55792**	**0.55611**	**0.55457**	**0.55323**	**0.55206**
Lindström	0.57551	0.56839	0.56264	0.55789	0.55390
Earlier bound	0.56149	0.55966	0.55807	0.55668	0.55545
Wang	0.55841	0.55727	0.55626	0.55536	0.55454

Lower-bound

The classical Sidon-set construction, combined with the base-q representation of integers, yields the general asymptotic lower bound

$$R_b \geq \frac{1}{2}.$$

Numerical impact for q-ary B_2 codes

	$q = 9$	10	11	12	13
New	**0.55792**	**0.55611**	**0.55457**	**0.55323**	**0.55206**
Lindström	0.57551	0.56839	0.56264	0.55789	0.55390
Earlier bound	0.56149	0.55966	0.55807	0.55668	0.55545
Wang	0.55841	0.55727	0.55626	0.55536	0.55454

Lower-bound

The classical Sidon-set construction, combined with the base-q representation of integers, yields the general asymptotic lower bound

$$R_b \geq \frac{1}{2}.$$

Constant-weight binary B_2 codes

Let $C^{(w)} \subseteq \{0,1\}^n$ be B_2 with constant weight

$$w = \alpha n(1 + o(1)), \qquad 0 < \alpha < 1.$$

Define the distance distribution

$$B_{2i}^{(w)} = \frac{1}{|C^{(w)}|} \left| \{(x, y) \in C^{(w)} \times C^{(w)} : d(x, y) = 2i\} \right|.$$

If $d(x, y) = 2i$, then $x - y \in \{-1, 0, 1\}^n$ has

$$i \text{ entries } +1, \quad i \text{ entries } -1, \quad n - 2i \text{ zeros.}$$

The number of such difference vectors is

$$\binom{n}{i}\binom{n-i}{i} = \binom{n}{2i}\binom{2i}{i}.$$

Constant-weight binary B_2 codes

Let $C^{(w)} \subseteq \{0,1\}^n$ be B_2 with constant weight

$$w = \alpha n(1 + o(1)), \qquad 0 < \alpha < 1.$$

Define the distance distribution

$$B_{2i}^{(w)} = \frac{1}{|C^{(w)}|} \left| \{(x, y) \in C^{(w)} \times C^{(w)} : d(x, y) = 2i\} \right|.$$

If $d(x, y) = 2i$, then $x - y \in \{-1, 0, 1\}^n$ has

i entries $+1$, i entries -1, $n - 2i$ zeros.

$+1$	$+1$	0	0	-1	0	-1	0

$x - y$

The number of such difference vectors is

$$\binom{n}{i}\binom{n-i}{i} = \binom{n}{2i}\binom{2i}{i}.$$

Constant-weight binary B_2 codes

Let $C^{(w)} \subseteq \{0,1\}^n$ be B_2 with constant weight

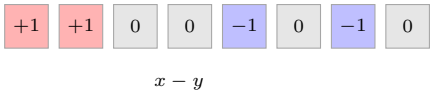
$$w = \alpha n(1 + o(1)), \qquad 0 < \alpha < 1.$$

Define the distance distribution

$$B_{2i}^{(w)} = \frac{1}{|C^{(w)}|} \left| \{(x, y) \in C^{(w)} \times C^{(w)} : d(x, y) = 2i\} \right|.$$

If $d(x, y) = 2i$, then $x - y \in \{-1, 0, 1\}^n$ has

$$i \text{ entries } +1, \quad i \text{ entries } -1, \quad n - 2i \text{ zeros.}$$



The number of such difference vectors is

$$\binom{n}{i}\binom{n-i}{i} = \binom{n}{2i}\binom{2i}{i}.$$

Constant-weight binary B_2 codes

Let $C^{(w)} \subseteq \{0,1\}^n$ be B_2 with constant weight

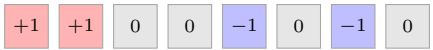
$$w = \alpha n(1 + o(1)), \qquad 0 < \alpha < 1.$$

Define the distance distribution

$$B_{2i}^{(w)} = \frac{1}{|C^{(w)}|} \left| \{(x, y) \in C^{(w)} \times C^{(w)} : d(x, y) = 2i\} \right|.$$

If $d(x, y) = 2i$, then $x - y \in \{-1, 0, 1\}^n$ has

$$i \text{ entries } +1, \quad i \text{ entries } -1, \quad n - 2i \text{ zeros.}$$



$x - y$

The number of such difference vectors is

$$\binom{n}{i}\binom{n-i}{i} = \binom{n}{2i}\binom{2i}{i}.$$

Cohen–Litsyn–Zémor method in constant weight

The B_2 property again gives injectivity of $(x, y) \mapsto x - y$ for $x \neq y$. For $i = \xi n(1 + o(1))$:

Upper estimate from injectivity

$$\frac{1}{n} \log B_{2\xi n}^{(w)} \leq h(2\xi) + 2\xi - R + o(1).$$

What is missing

To turn this into a rate bound, we need a *forced populated shell*: a distance $2i$ at which the average distance distribution cannot be too small.

This is where Litsyn's constant-weight LP bound enters.

Cohen–Litsyn–Zémor method in constant weight

The B_2 property again gives injectivity of $(x, y) \mapsto x - y$ for $x \neq y$. For $i = \xi n(1 + o(1))$:

Upper estimate from injectivity

$$\frac{1}{n} \log B_{2\xi n}^{(w)} \leq h(2\xi) + 2\xi - R + o(1).$$

What is missing

To turn this into a rate bound, we need a *forced populated shell*: a distance $2i$ at which the average distance distribution cannot be too small.

This is where Litsyn's constant-weight LP bound enters.

Cohen–Litsyn–Zémor method in constant weight

The B_2 property again gives injectivity of $(x, y) \mapsto x - y$ for $x \neq y$. For $i = \xi n(1 + o(1))$:

Upper estimate from injectivity

$$\frac{1}{n} \log B_{2\xi n}^{(w)} \leq h(2\xi) + 2\xi - R + o(1).$$

What is missing

To turn this into a rate bound, we need a *forced populated shell*: a distance $2i$ at which the average distance distribution cannot be too small.

This is where Litsyn's constant-weight LP bound enters.

Cohen–Litsyn–Zémor method in constant weight

The B_2 property again gives injectivity of $(x, y) \mapsto x - y$ for $x \neq y$. For $i = \xi n(1 + o(1))$:

Upper estimate from injectivity

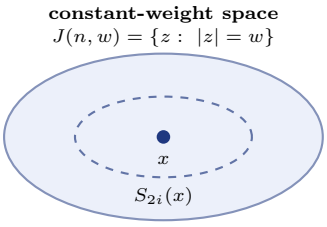
$$\frac{1}{n} \log B_{2\xi n}^{(w)} \leq h(2\xi) + 2\xi - R + o(1).$$

What is missing

To turn this into a rate bound, we need a *forced populated shell*: a distance $2i$ at which the average distance distribution cannot be too small.

This is where Litsyn's constant-weight LP bound enters.

Where the Litsyn lower estimate comes from



Inside $J(n,w)$ the distance-$2i$ shell around x is obtained by

$$\underbrace{i \text{ ones}}_{1\to 0} \qquad \text{and} \qquad \underbrace{i \text{ zeros}}_{0\to 1}.$$

Hence the natural shell mass is

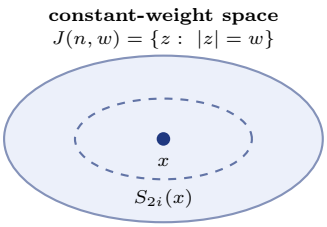
$$\frac{|S_{2i}(x)|}{|J(n,w)|} = \frac{\binom{w}{i}\binom{n-w}{i}}{\binom{n}{w}}.$$

LP input on the Johnson scheme

The constant-weight linear-programming bound forces, for some $2\xi \le \delta_{\mathrm{LP}}(R,\alpha)$,

$$B_{2\xi n}^{(w)} \gtrsim |C^{(w)}| \, \frac{\binom{w}{\xi n}\binom{n-w}{\xi n}}{\binom{n}{w}} \cdot n^{-O(1)}.$$

Where the Litsyn lower estimate comes from



Inside $J(n,w)$ the distance-$2i$ shell around x is obtained by

$$\underbrace{i \text{ ones}}_{1\to 0} \quad \text{and} \quad \underbrace{i \text{ zeros}}_{0\to 1}.$$

Hence the natural shell mass is

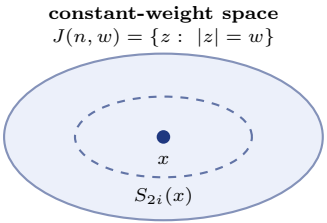
$$\frac{|S_{2i}(x)|}{|J(n,w)|} = \frac{\binom{w}{i}\binom{n-w}{i}}{\binom{n}{w}}.$$

LP input on the Johnson scheme

The constant-weight linear-programming bound forces, for some $2\xi \le \delta_{\mathrm{LP}}(R,\alpha)$,

$$B_{2\xi n}^{(w)} \gtrsim |C^{(w)}| \, \frac{\binom{w}{\xi n}\binom{n-w}{\xi n}}{\binom{n}{w}} \cdot n^{-O(1)}.$$

Where the Litsyn lower estimate comes from



Inside $J(n,w)$ the distance-$2i$ shell around x is obtained by

$$\underbrace{i \text{ ones}}_{1\to 0} \qquad \text{and} \qquad \underbrace{i \text{ zeros}}_{0\to 1}.$$

Hence the natural shell mass is

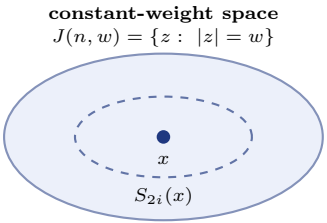
$$\frac{|S_{2i}(x)|}{|J(n,w)|} = \frac{\binom{w}{i}\binom{n-w}{i}}{\binom{n}{w}}.$$

LP input on the Johnson scheme

The constant-weight linear-programming bound forces, for some $2\xi \le \delta_{\mathrm{LP}}(R,\alpha)$,

$$B_{2\xi n}^{(w)} \gtrsim |C^{(w)}| \, \frac{\binom{w}{\xi n}\binom{n-w}{\xi n}}{\binom{n}{w}} \cdot n^{-O(1)}.$$

Where the Litsyn lower estimate comes from



Inside $J(n,w)$ the distance-$2i$ shell around x is obtained by

$$\underbrace{i \text{ ones}}_{1\to 0} \qquad \text{and} \qquad \underbrace{i \text{ zeros}}_{0\to 1}.$$

Hence the natural shell mass is

$$\frac{|S_{2i}(x)|}{|J(n,w)|} = \frac{\binom{w}{i}\binom{n-w}{i}}{\binom{n}{w}}.$$

LP input on the Johnson scheme

The constant-weight linear-programming bound forces, for some $2\xi \le \delta_{\mathrm{LP}}(R,\alpha)$,

$$B_{2\xi n}^{(w)} \gtrsim |C^{(w)}| \, \frac{\binom{w}{\xi n}\binom{n-w}{\xi n}}{\binom{n}{w}} \cdot n^{-O(1)}.$$

LP shell mass on the exponential scale

Let $R = \frac{1}{n}\log|C^{(w)}|$ and $w = \alpha n(1+o(1))$.

Constant-weight LP distance bound

$$\delta_{\mathrm{LP}}(R,\alpha) = \min_{\substack{0\le\beta\le\alpha \\ h(\beta)=R}} 2\,\frac{\alpha(1-\alpha)-\beta(1-\beta)}{1+2\sqrt{\beta(1-\beta)}}.$$

Litsyn lower shell estimate

For some $2\xi \le \delta_{\mathrm{LP}}(R,\alpha)$,

$$\frac{1}{n}\log B_{2\xi n}^{(w)} \ge R - h(\alpha) + \alpha h\left(\frac{\xi}{\alpha}\right) + (1-\alpha)h\left(\frac{\xi}{1-\alpha}\right) + o(1).$$

B_2 upper shell estimate

$$\frac{1}{n}\log B_{2\xi n}^{(w)} \le h(2\xi) + 2\xi - R + o(1).$$

Comparing the two estimates gives the implicit rate inequality.

LP shell mass on the exponential scale

Let $R = \frac{1}{n}\log|C^{(w)}|$ and $w = \alpha n(1+o(1))$.

Constant-weight LP distance bound

$$\delta_{\mathrm{LP}}(R,\alpha) = \min_{\substack{0\le\beta\le\alpha \\ h(\beta)=R}} 2\,\frac{\alpha(1-\alpha)-\beta(1-\beta)}{1+2\sqrt{\beta(1-\beta)}}.$$

Litsyn lower shell estimate

For some $2\xi \le \delta_{\mathrm{LP}}(R,\alpha)$,

$$\frac{1}{n}\log B_{2\xi n}^{(w)} \ge R - h(\alpha) + \alpha h\left(\frac{\xi}{\alpha}\right) + (1-\alpha)h\left(\frac{\xi}{1-\alpha}\right) + o(1).$$

B_2 upper shell estimate

$$\frac{1}{n}\log B_{2\xi n}^{(w)} \le h(2\xi) + 2\xi - R + o(1).$$

Comparing the two estimates gives the implicit rate inequality.

LP shell mass on the exponential scale

Let $R = \frac{1}{n}\log|C^{(w)}|$ and $w = \alpha n(1+o(1))$.

Constant-weight LP distance bound

$$\delta_{\mathrm{LP}}(R,\alpha) = \min_{\substack{0\le\beta\le\alpha \\ h(\beta)=R}} 2\,\frac{\alpha(1-\alpha)-\beta(1-\beta)}{1+2\sqrt{\beta(1-\beta)}}.$$

Litsyn lower shell estimate

For some $2\xi \le \delta_{\mathrm{LP}}(R,\alpha)$,

$$\frac{1}{n}\log B_{2\xi n}^{(w)} \ge R - h(\alpha) + \alpha h\left(\frac{\xi}{\alpha}\right) + (1-\alpha)h\left(\frac{\xi}{1-\alpha}\right) + o(1).$$

B_2 upper shell estimate

$$\frac{1}{n}\log B_{2\xi n}^{(w)} \le h(2\xi) + 2\xi - R + o(1).$$

Comparing the two estimates gives the implicit rate inequality.

LP shell mass on the exponential scale

Let $R = \frac{1}{n}\log|C^{(w)}|$ and $w = \alpha n(1+o(1))$.

Constant-weight LP distance bound

$$\delta_{\mathrm{LP}}(R,\alpha) = \min_{\substack{0\le\beta\le\alpha \\ h(\beta)=R}} 2\,\frac{\alpha(1-\alpha)-\beta(1-\beta)}{1+2\sqrt{\beta(1-\beta)}}.$$

Litsyn lower shell estimate

For some $2\xi \le \delta_{\mathrm{LP}}(R,\alpha)$,

$$\frac{1}{n}\log B_{2\xi n}^{(w)} \ge R - h(\alpha) + \alpha h\left(\frac{\xi}{\alpha}\right) + (1-\alpha)h\left(\frac{\xi}{1-\alpha}\right) + o(1).$$

B_2 upper shell estimate

$$\frac{1}{n}\log B_{2\xi n}^{(w)} \le h(2\xi) + 2\xi - R + o(1).$$

Comparing the two estimates gives the implicit rate inequality.

LP shell mass on the exponential scale

Let $R = \frac{1}{n}\log|C^{(w)}|$ and $w = \alpha n(1 + o(1))$.

Constant-weight LP distance bound

$$\delta_{\mathrm{LP}}(R,\alpha) = \min_{\substack{0\le\beta\le\alpha \\ h(\beta)=R}} 2\,\frac{\alpha(1-\alpha)-\beta(1-\beta)}{1+2\sqrt{\beta(1-\beta)}}.$$

Litsyn lower shell estimate

For some $2\xi \le \delta_{\mathrm{LP}}(R,\alpha)$,

$$\frac{1}{n}\log B_{2\xi n}^{(w)} \ge R - h(\alpha) + \alpha h\left(\frac{\xi}{\alpha}\right) + (1-\alpha)h\left(\frac{\xi}{1-\alpha}\right) + o(1).$$

B_2 upper shell estimate

$$\frac{1}{n}\log B_{2\xi n}^{(w)} \le h(2\xi) + 2\xi - R + o(1).$$

Comparing the two estimates gives the implicit rate inequality.

Constant-weight theorem and comparison

Define

$$\Psi_\alpha(\xi) = \frac{1}{2}\left[h(2\xi) + 2\xi + h(\alpha) - \alpha h\left(\frac{\xi}{\alpha}\right) - (1-\alpha)h\left(\frac{\xi}{1-\alpha}\right)\right].$$

Theorem (Constant-weight upper bound)

For every $\alpha \in (0,1)$,

$$r_{B_2}^{\mathrm{cw}}(\alpha) \le \rho(\alpha),$$

where $\rho(\alpha)$ is the largest real solution of

$$R = \Psi_\alpha\left(\frac{\delta_{\mathrm{LP}}(R,\alpha)}{2}\right).$$

Monotonicity step

$$\Psi'_\alpha(\xi) = \log\left(\frac{1-2\xi}{\sqrt{(\alpha-\xi)(1-\alpha-\xi)}}\right) \ge 0.$$

Constant-weight theorem and comparison

Define

$$\Psi_\alpha(\xi) = \frac{1}{2}\left[h(2\xi) + 2\xi + h(\alpha) - \alpha h\left(\frac{\xi}{\alpha}\right) - (1-\alpha)h\left(\frac{\xi}{1-\alpha}\right)\right].$$

Theorem (Constant-weight upper bound)

For every $\alpha \in (0,1)$,

$$r_{B_2}^{\mathrm{cw}}(\alpha) \le \rho(\alpha),$$

where $\rho(\alpha)$ is the largest real solution of

$$R = \Psi_\alpha\left(\frac{\delta_{\mathrm{LP}}(R,\alpha)}{2}\right).$$

Monotonicity step

$$\Psi'_\alpha(\xi) = \log\left(\frac{1-2\xi}{\sqrt{(\alpha-\xi)(1-\alpha-\xi)}}\right) \ge 0.$$

Constant-weight theorem and comparison

Define

$$\Psi_\alpha(\xi) = \frac{1}{2}\left[h(2\xi) + 2\xi + h(\alpha) - \alpha h\left(\frac{\xi}{\alpha}\right) - (1-\alpha)h\left(\frac{\xi}{1-\alpha}\right)\right].$$

Theorem (Constant-weight upper bound)

For every $\alpha \in (0,1)$,

$$r_{B_2}^{\mathrm{cw}}(\alpha) \le \rho(\alpha),$$

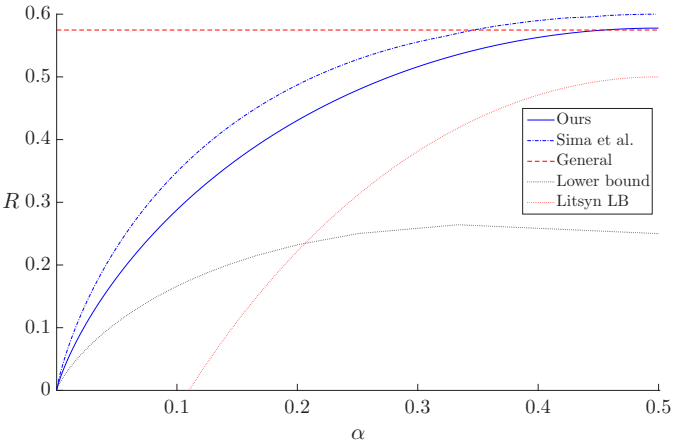
where $\rho(\alpha)$ is the largest real solution of

$$R = \Psi_\alpha\left(\frac{\delta_{\mathrm{LP}}(R,\alpha)}{2}\right).$$

Monotonicity step

$$\Psi'_\alpha(\xi) = \log\left(\frac{1-2\xi}{\sqrt{(\alpha-\xi)(1-\alpha-\xi)}}\right) \ge 0.$$

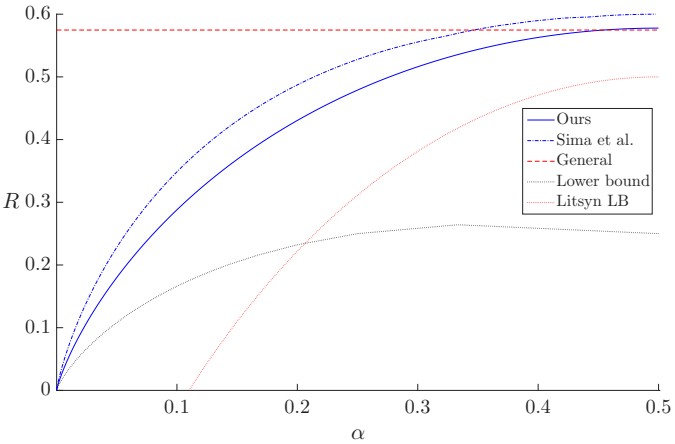
Constant-weight numerical comparison



Observed behavior

- The new curve is below Sima et al. over $\alpha \in (0, 1/2]$.
- It also beats the general B_2 upper bound for $w \leq 0.459n$.
- The lower bounds remains far below the upper bounds: there is room for sharper techniques.

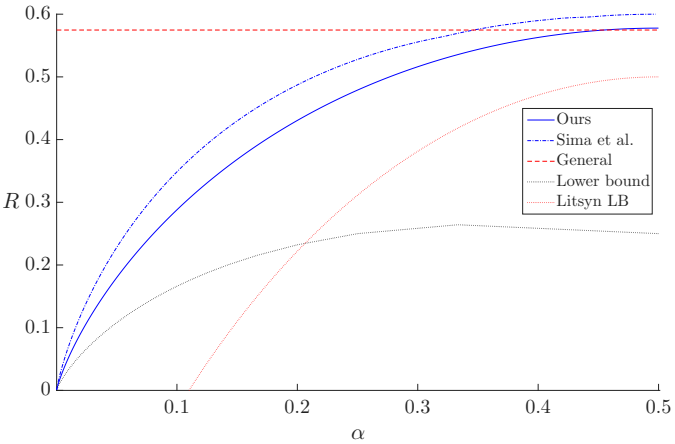
Constant-weight numerical comparison



Observed behavior

- The new curve is below Sima et al. over $\alpha \in (0, 1/2]$.
- It also beats the general B_2 upper bound for $w \leq 0.459n$.
- The lower bounds remains far below the upper bounds: there is room for sharper techniques.

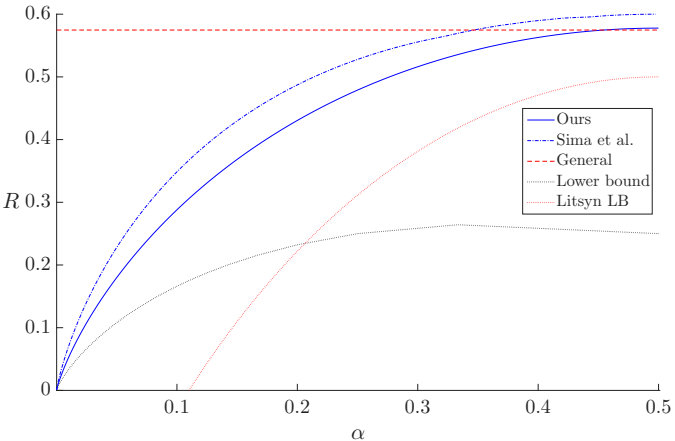
Constant-weight numerical comparison



Observed behavior

- The new curve is below Sima et al. over $\alpha \in (0, 1/2]$.
- It also beats the general B_2 upper bound for $w \leq 0.459n$.
- The lower bounds remains far below the upper bounds: there is room for sharper techniques.

Constant-weight numerical comparison



Observed behavior

- The new curve is below Sima et al. over $\alpha \in (0, 1/2]$.
- It also beats the general B_2 upper bound for $w \leq 0.459n$.
- The lower bounds remains far below the upper bounds: there is room for sharper techniques.

Thank you.