Product Expansion of Random Codes via Analytic Techniques



Eshan Chattopadhyay



Noam Ringach



Nicholas Spooner

Part 1: Error-correcting codes

Error-correcting codes

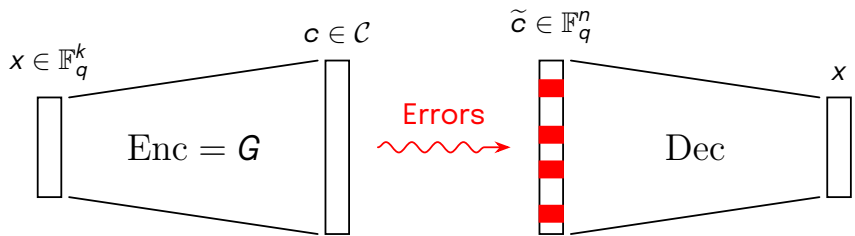
Definition

- A linear ***error-correcting code*** is a subspace $\mathcal{C} \subseteq \mathbb{F}_q^n$ of dimension k, rate $r = k/n$, distance $d = \min_{c \neq c' \in \mathcal{C}} |c - c'|$, and rel distance $\delta = d/n$.

Error-correcting codes

Definition

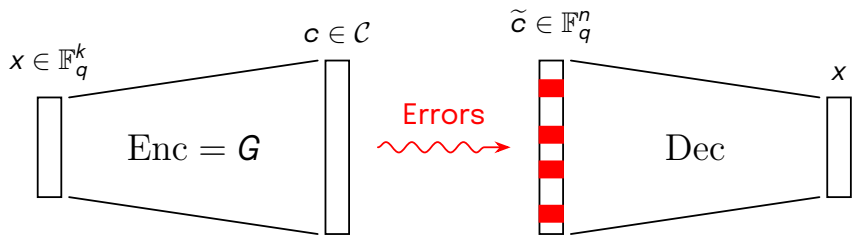
- A linear ***error-correcting code*** is a subspace $\mathcal{C} \subseteq \mathbb{F}_q^n$ of dimension k, rate $r = k/n$, distance $d = \min_{c \neq c' \in \mathcal{C}} |c - c'|$, and rel distance $\delta = d/n$.



Error-correcting codes

Definition

- A linear ***error-correcting code*** is a subspace $\mathcal{C} \subseteq \mathbb{F}_q^n$ of dimension k, rate $r = k/n$, distance $d = \min_{c \neq c' \in \mathcal{C}} |c - c'|$, and rel distance $\delta = d/n$.
- $\mathcal{C}$ is ***"good"*** when $r, \delta = \Theta(1)$ as $n \to \infty$.



Locally testable codes (LTCs)

Locally testable codes (LTCs)

Locally testable code (LTC)

A ***LTC*** is a code $\mathcal{C}$ with a randomized tester $\mathrm{Test} : \mathbb{F}_q^\ell \to \{\mathsf{Accept}, \mathsf{Reject}\}$ s.t.

Locally testable codes (LTCs)

Locally testable code (LTC)

A ***LTC*** is a code $\mathcal{C}$ with a randomized tester $\mathrm{Test} : \mathbb{F}_q^\ell \to \{\mathsf{Accept}, \mathsf{Reject}\}$ s.t.

- Test has oracle access to a word $w \in \mathbb{F}_q^n$ and can make ℓ queries.

Locally testable codes (LTCs)

Locally testable code (LTC)

A ***LTC*** is a code $\mathcal{C}$ with a randomized tester $\mathrm{Test} : \mathbb{F}_q^\ell \to \{\mathsf{Accept}, \mathsf{Reject}\}$ s.t.

- Test has oracle access to a word $w \in \mathbb{F}_q^n$ and can make ℓ queries.
- **Completeness:** If $w \in \mathcal{C}$, then $\mathrm{Test}(w) = \mathsf{Accept}$ w.p. 1.

Locally testable codes (LTCs)

Locally testable code (LTC)

A ***LTC*** is a code $\mathcal{C}$ with a randomized tester $\mathrm{Test} : \mathbb{F}_q^\ell \to \{\mathsf{Accept}, \mathsf{Reject}\}$ s.t.

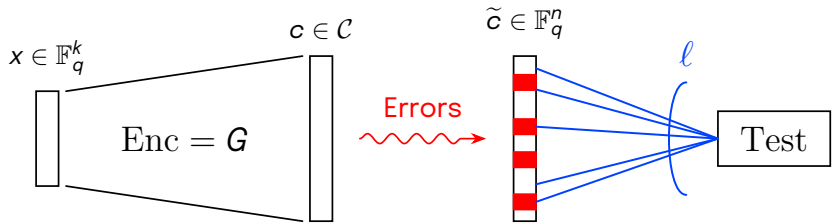
- Test has oracle access to a word $w \in \mathbb{F}_q^n$ and can make ℓ queries.
- **Completeness:** If $w \in \mathcal{C}$, then $\mathrm{Test}(w) = \mathsf{Accept}$ w.p. 1.
- **Soundness:** If $w \notin \mathcal{C}$, then $\Pr[\mathrm{Test}(w) = \mathsf{Reject}] \geq s \cdot \mathrm{Dist}(w, \mathcal{C})/n$.

Locally testable codes (LTCs)

Locally testable code (LTC)

A ***LTC*** is a code $\mathcal{C}$ with a randomized tester $\mathrm{Test} : \mathbb{F}_q^\ell \to \{\mathsf{Accept}, \mathsf{Reject}\}$ s.t.

- Test has oracle access to a word $w \in \mathbb{F}_q^n$ and can make ℓ queries.
- **Completeness:** If $w \in \mathcal{C}$, then $\mathrm{Test}(w) = \mathsf{Accept}$ w.p. 1.
- **Soundness:** If $w \notin \mathcal{C}$, then $\Pr[\mathrm{Test}(w) = \mathsf{Reject}] \geq s \cdot \mathrm{Dist}(w, \mathcal{C})/n$.



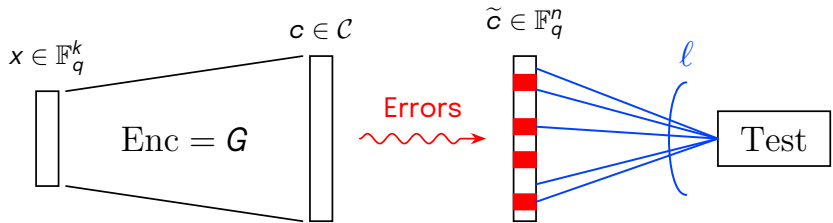
Locally testable codes (LTCs)

Locally testable code (LTC)

A ***LTC*** is a code $\mathcal{C}$ with a randomized tester $\mathrm{Test} : \mathbb{F}_q^\ell \to \{\mathsf{Accept}, \mathsf{Reject}\}$ s.t.

- Test has oracle access to a word $w \in \mathbb{F}_q^n$ and can make ℓ queries.
- **Completeness:** If $w \in \mathcal{C}$, then $\mathrm{Test}(w) = \mathsf{Accept}$ w.p. 1.
- **Soundness:** If $w \notin \mathcal{C}$, then $\Pr[\mathrm{Test}(w) = \mathsf{Reject}] \geq s \cdot \mathrm{Dist}(w, \mathcal{C})/n$.

$\mathcal{C}$ is a ***"good"*** LTC if $r, \delta, \ell, s = \Theta(1)$.



Locally testable codes (LTCs)

Locally testable code (LTC)

A ***LTC*** is a code $\mathcal{C}$ with a randomized tester $\mathrm{Test} : \mathbb{F}_q^\ell \to \{\text{Accept}, \text{Reject}\}$ s.t.

- Test has oracle access to a word $w \in \mathbb{F}_q^n$ and can make ℓ queries.
- **Completeness:** If $w \in \mathcal{C}$, then $\mathrm{Test}(w) = \text{Accept}$ w.p. 1.
- **Soundness:** If $w \notin \mathcal{C}$, then $\Pr[\mathrm{Test}(w) = \text{Reject}] \geq s \cdot \mathrm{Dist}(w, \mathcal{C})/n$.

$\mathcal{C}$ is a ***"good"*** LTC if $r, \delta, \ell, s = \Theta(1)$.

Good LTCs and quantum LTCs have been used for:

- classical probabilistically checkable proofs (PCPs) [Dinur, '07]

Locally testable codes (LTCs)

Locally testable code (LTC)

A ***LTC*** is a code $\mathcal{C}$ with a randomized tester $\mathrm{Test} : \mathbb{F}_q^\ell \to \{\text{Accept}, \text{Reject}\}$ s.t.

- Test has oracle access to a word $w \in \mathbb{F}_q^n$ and can make ℓ queries.
- **Completeness:** If $w \in \mathcal{C}$, then $\mathrm{Test}(w) = \text{Accept}$ w.p. 1.
- **Soundness:** If $w \notin \mathcal{C}$, then $\Pr[\mathrm{Test}(w) = \text{Reject}] \geq s \cdot \mathrm{Dist}(w, \mathcal{C})/n$.

$\mathcal{C}$ is a ***"good"*** LTC if $r, \delta, \ell, s = \Theta(1)$.

Good LTCs and quantum LTCs have been used for:

- classical probabilistically checkable proofs (PCPs) [Dinur, '07]
- qIOPs for QMA [Sun, Vidick, '26]

Locally testable codes (LTCs)

Locally testable code (LTC)

A ***LTC*** is a code $\mathcal{C}$ with a randomized tester $\mathrm{Test} : \mathbb{F}_q^\ell \to \{\mathsf{Accept}, \mathsf{Reject}\}$ s.t.

- Test has oracle access to a word $w \in \mathbb{F}_q^n$ and can make ℓ queries.
- **Completeness:** If $w \in \mathcal{C}$, then $\mathrm{Test}(w) = \mathsf{Accept}$ w.p. 1.
- **Soundness:** If $w \notin \mathcal{C}$, then $\Pr[\mathrm{Test}(w) = \mathsf{Reject}] \geq s \cdot \mathrm{Dist}(w, \mathcal{C})/n$.

$\mathcal{C}$ is a ***"good"*** LTC if $r, \delta, \ell, s = \Theta(1)$.

Good LTCs and quantum LTCs have been used for:

- classical probabilistically checkable proofs (PCPs) [Dinur, '07]
- qIOPs for QMA [Sun, Vidick, '26]

Could be used to construct:

Locally testable codes (LTCs)

Locally testable code (LTC)

A ***LTC*** is a code $\mathcal{C}$ with a randomized tester $\mathrm{Test} : \mathbb{F}_q^\ell \to \{\mathsf{Accept}, \mathsf{Reject}\}$ s.t.

- Test has oracle access to a word $w \in \mathbb{F}_q^n$ and can make ℓ queries.
- **Completeness:** If $w \in \mathcal{C}$, then $\mathrm{Test}(w) = \mathsf{Accept}$ w.p. 1.
- **Soundness:** If $w \notin \mathcal{C}$, then $\Pr[\mathrm{Test}(w) = \mathsf{Reject}] \geq s \cdot \mathrm{Dist}(w, \mathcal{C})/n$.

$\mathcal{C}$ is a ***"good"*** LTC if $r, \delta, \ell, s = \Theta(1)$.

Good LTCs and quantum LTCs have been used for:

- classical probabilistically checkable proofs (PCPs) [Dinur, '07]
- qIOPs for QMA [Sun, Vidick, '26]

Could be used to construct:

- Linear-sized PCPs

Locally testable codes (LTCs)

Locally testable code (LTC)

A ***LTC*** is a code $\mathcal{C}$ with a randomized tester $\mathrm{Test} : \mathbb{F}_q^\ell \to \{\mathsf{Accept}, \mathsf{Reject}\}$ s.t.

- Test has oracle access to a word $w \in \mathbb{F}_q^n$ and can make ℓ queries.
- **Completeness:** If $w \in \mathcal{C}$, then $\mathrm{Test}(w) = \mathsf{Accept}$ w.p. 1.
- **Soundness:** If $w \notin \mathcal{C}$, then $\Pr[\mathrm{Test}(w) = \mathsf{Reject}] \geq s \cdot \mathrm{Dist}(w, \mathcal{C})/n$.

$\mathcal{C}$ is a ***"good"*** LTC if $r, \delta, \ell, s = \Theta(1)$.

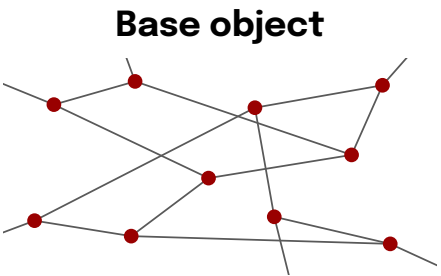
Good LTCs and quantum LTCs have been used for:

- classical probabilistically checkable proofs (PCPs) [Dinur, '07]
- qIOPs for QMA [Sun, Vidick, '26]

Could be used to construct:

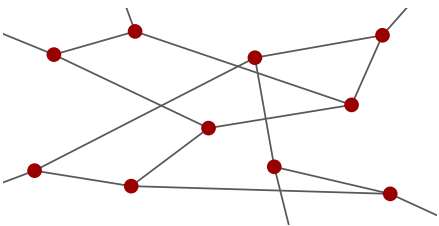
- Linear-sized PCPs
- Quantum PCPs

A common lifting strategy



A common lifting strategy

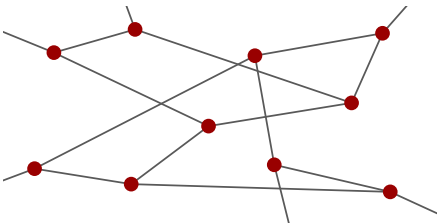
Base object



- Asymptotically increasing size

A common lifting strategy

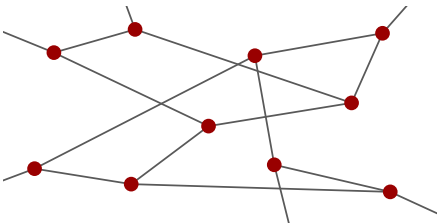
Base object



- Asymptotically increasing size
- Explicit

A common lifting strategy

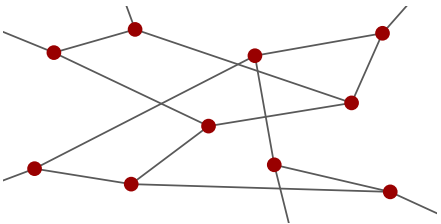
Base object



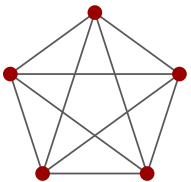
- Asymptotically increasing size
- Explicit
- Good enough properties

A common lifting strategy

Base object



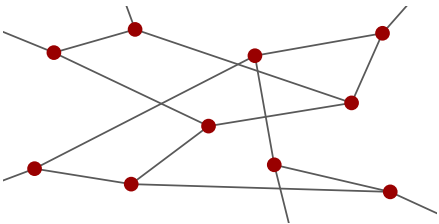
Gadget



- Asymptotically increasing size
- Explicit
- Good enough properties

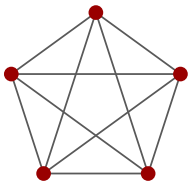
A common lifting strategy

Base object



- Asymptotically increasing size
- Explicit
- Good enough properties

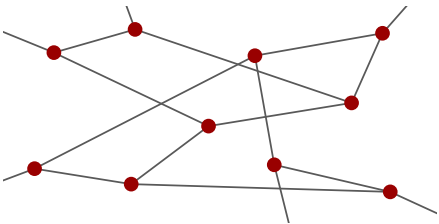
Gadget



- Constant size

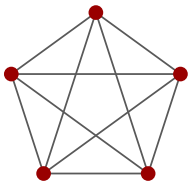
A common lifting strategy

Base object



- Asymptotically increasing size
- Explicit
- Good enough properties

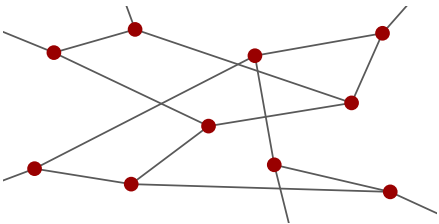
Gadget



- Constant size
- Existential

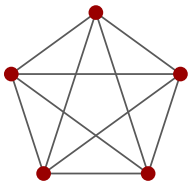
A common lifting strategy

Base object



- Asymptotically increasing size
- Explicit
- Good enough properties

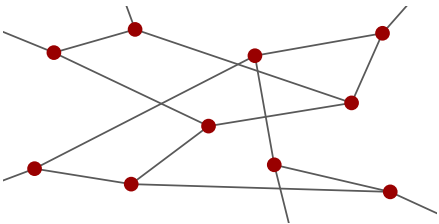
Gadget



- Constant size
- Existential
- Has desired properties

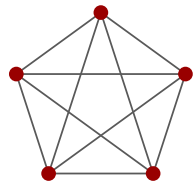
A common lifting strategy

Base object



- Asymptotically increasing size
- Explicit
- Good enough properties

Gadget



- Constant size
- Existential
- Has desired properties

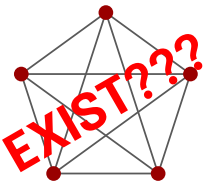
Combine to “lift” properties of gadget to a large object

A common lifting strategy

Base object

- Asymptotically increasing size
- Explicit
- Good enough properties

Gadget



- Constant size
- Existential
- Has desired properties

Combine to “lift” properties of gadget to a large object

LTC constructions

LTC constructions

Theorem [Dinur, Evra, Livne, Lubotzky, Mozes, '22]

Families of **good LTCs exist**: $r, \delta, \ell, s = \Theta(1)$.

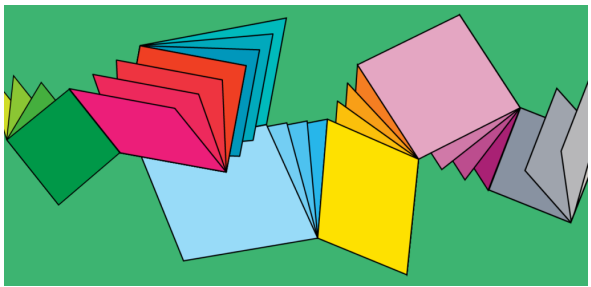
- **Large object:** 2-dimensional cubical complex with good expansion
- **Gadget object:** Tensor of two random linear codes $\mathcal{C}_1 \otimes \mathcal{C}_2$.

LTC constructions

Theorem [Dinur, Evra, Livne, Lubotzky, Mozes, '22]

Families of **good LTCs exist**: $r, \delta, \ell, s = \Theta(1)$.

- **Large object:** 2-dimensional cubical complex with good expansion
- **Gadget object:** Tensor of two random linear codes $\mathcal{C}_1 \otimes \mathcal{C}_2$.



https://blog.simons.berkeley.edu/2022/09/the-blooming-of-the-c3-ltc-flowers/

LTC constructions

Theorem [Dinur, Evra, Livne, Lubotzky, Mozes, '22]

Families of **good LTCs exist**: $r, \delta, \ell, s = \Theta(1)$.

- **Large object:** 2-dimensional cubical complex with good expansion
- **Gadget object:** Tensor of two random linear codes $\mathcal{C}_1 \otimes \mathcal{C}_2$.

Theorem [Dinur, Lin, Vidick, '24]

Families of **quantum LTCs exist:** $r, \ell = \Theta(1), \delta, s = 1/\operatorname{polylog}(n)$.

- **Large object:** 4-dimensional cubical complex witih good expansion
- **Gadget object:** Tensor of four random linear codes $\mathcal{C}_1 \otimes \mathcal{C}_2 \otimes \mathcal{C}_3 \otimes \mathcal{C}_4$.

LTC constructions

Theorem [Dinur, Evra, Livne, Lubotzky, Mozes, '22]

Families of **good LTCs exist**: $r, \delta, \ell, s = \Theta(1)$.

- **Large object:** 2-dimensional cubical complex with good expansion
- **Gadget object:** Tensor of two random linear codes $\mathcal{C}_1 \otimes \mathcal{C}_2$.

Theorem [Gay, Jeronimo, '26], [Bafna, Li, Nguyen, '26], [Chen, Huang, Liu, Tang, '26]

Families of **good quantum LTCs exist.**

- **Large object:** 4-dimensional cubical complex witih good expansion
- **Gadget object:** Tensor of four clever RS codes $\mathcal{C}_1 \otimes \mathcal{C}_2 \otimes \mathcal{C}_3 \otimes \mathcal{C}_4$.

Can we ask for more?



Can we ask for more?

Some other desired properties:

- **Multiplication** (coordinate-wise product of codewords is in a related code)
- Transversal **quantum gates**
- Global **symmetries/automorphisms**

Can we ask for more?

Some other desired properties:

- **Multiplication** (coordinate-wise product of codewords is in a related code)
- Transversal **quantum gates**
- Global **symmetries/automorphisms**

Required for constructions of linear-sized PCPs and qPCPs

Can we ask for more?

Some other desired properties:

- **Multiplication** (coordinate-wise product of codewords is in a related code)
- Transversal **quantum gates**
- Global **symmetries/automorphisms**

Required for constructions of linear-sized PCPs and qPCPs

Bottleneck

We have a **restricted understanding of the gadget codes.** Prevents:

- Specifying symmetries of the code
- Using other base graphs (e.g, simplicial complexes)

Tensor codes

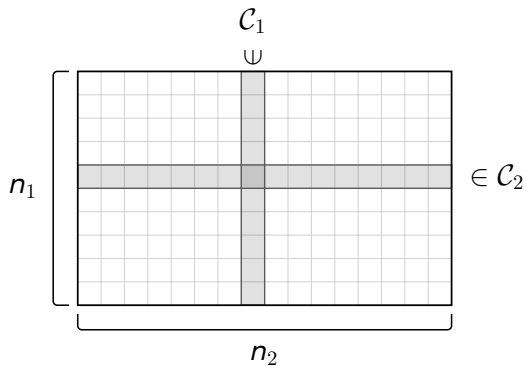
Definition (D=2)

For two codes $\mathcal{C}_1 \subseteq \mathbb{F}_q^{n_1}$ and $\mathcal{C}_2 \subseteq \mathbb{F}_q^{n_2}$, their ***tensor code*** $\mathcal{C}_1 \otimes \mathcal{C}_2 \subseteq \mathbb{F}_q^{n_1 \times n_2}$ has columns in $\mathcal{C}_1$ and rows in $\mathcal{C}_2$.

Tensor codes

Definition (D=2)

For two codes $\mathcal{C}_1 \subseteq \mathbb{F}_q^{n_1}$ and $\mathcal{C}_2 \subseteq \mathbb{F}_q^{n_2}$, their ***tensor code*** $\mathcal{C}_1 \otimes \mathcal{C}_2 \subseteq \mathbb{F}_q^{n_1 \times n_2}$ has columns in $\mathcal{C}_1$ and rows in $\mathcal{C}_2$.



Tensor codes

Definition (D=2)

For two codes $\mathcal{C}_1 \subseteq \mathbb{F}_q^{n_1}$ and $\mathcal{C}_2 \subseteq \mathbb{F}_q^{n_2}$, their ***tensor code*** $\mathcal{C}_1 \otimes \mathcal{C}_2 \subseteq \mathbb{F}_q^{n_1 \times n_2}$ has columns in $\mathcal{C}_1$ and rows in $\mathcal{C}_2$.

Definition (General)

For D codes $\mathcal{C}_1 \subseteq \mathbb{F}_q^n, \ldots, \mathcal{C}_D \subseteq \mathbb{F}_q^n$, their ***tensor code*** $\mathcal{C}_1 \otimes \cdots \otimes \mathcal{C}_D \subseteq \mathbb{F}_q^{[n]^D}$ has every i-axis parallel line in $\mathcal{C}_i$.

Tensor codes

Definition (D=2)

For two codes $\mathcal{C}_1 \subseteq \mathbb{F}_q^{n_1}$ and $\mathcal{C}_2 \subseteq \mathbb{F}_q^{n_2}$, their ***tensor code*** $\mathcal{C}_1 \otimes \mathcal{C}_2 \subseteq \mathbb{F}_q^{n_1 \times n_2}$ has columns in $\mathcal{C}_1$ and rows in $\mathcal{C}_2$.

Definition (General)

For D codes $\mathcal{C}_1 \subseteq \mathbb{F}_q^n, \ldots, \mathcal{C}_D \subseteq \mathbb{F}_q^n$, their ***tensor code*** $\mathcal{C}_1 \otimes \cdots \otimes \mathcal{C}_D \subseteq \mathbb{F}_q^{[n]^D}$ has every i-axis parallel line in $\mathcal{C}_i$.

Fact

For codes $(\mathcal{C}_i)_{i \in [D]}$ where $\mathcal{C}_i$ is an $[n, k_i, d_i]$ code, their tensor code $\mathcal{C} = \mathcal{C}_1 \otimes \cdots \otimes \mathcal{C}_D$ is an $[n^D, k_1 k_2 \cdots k_D, d_1 d_2 \cdots d_D]$ code.

Product expansion

Product expansion

Definition

Property of gadgets necessary for LTC constructions

Product expansion

Definition

Property of gadgets necessary for LTC constructions

- ε-closed sets

Product expansion

Definition

Property of gadgets necessary for LTC constructions

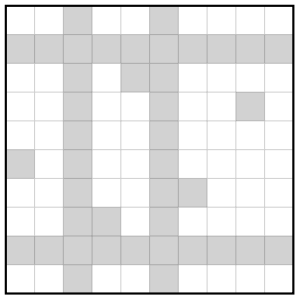
- ε-closed sets
- Extendable sets

ε-closed sets

ε-closed sets

Definition

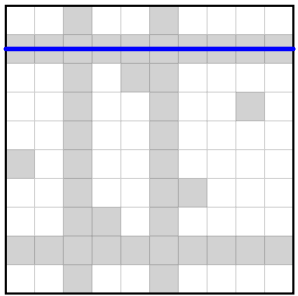
$M \subseteq [n]^D$ is ε-***closed*** if $\forall$ i-axis parallel lines ℓ, either $\ell \subseteq M$ or $|\ell \cap M| \leq \varepsilon n$.



ε-closed sets

Definition

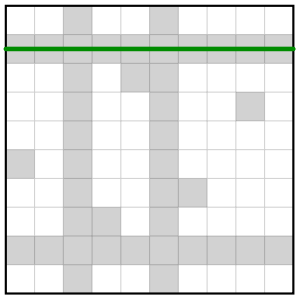
$M \subseteq [n]^D$ is ε-***closed*** if $\forall$ i-axis parallel lines ℓ, either $\ell \subseteq M$ or $|\ell \cap M| \leq \varepsilon n$.



ε-closed sets

Definition

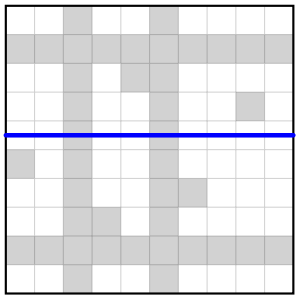
$M \subseteq [n]^D$ is ε-***closed*** if $\forall$ i-axis parallel lines ℓ, either $\ell \subseteq M$ or $|\ell \cap M| \leq \varepsilon n$.



ε-closed sets

Definition

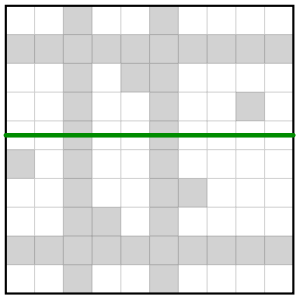
$M \subseteq [n]^D$ is ε-***closed*** if $\forall$ i-axis parallel lines ℓ, either $\ell \subseteq M$ or $|\ell \cap M| \leq \varepsilon n$.



ε-closed sets

Definition

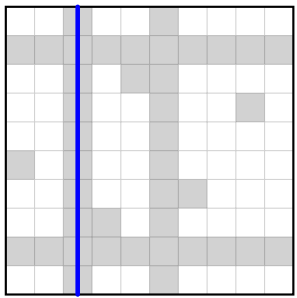
$M \subseteq [n]^D$ is ε-***closed*** if $\forall$ i-axis parallel lines ℓ, either $\ell \subseteq M$ or $|\ell \cap M| \leq \varepsilon n$.



ε-closed sets

Definition

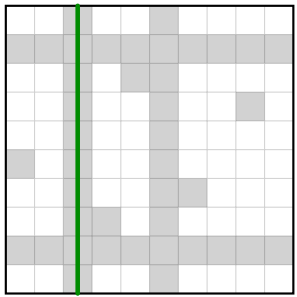
$M \subseteq [n]^D$ is ε-***closed*** if $\forall$ i-axis parallel lines ℓ, either $\ell \subseteq M$ or $|\ell \cap M| \leq \varepsilon n$.



ε-closed sets

Definition

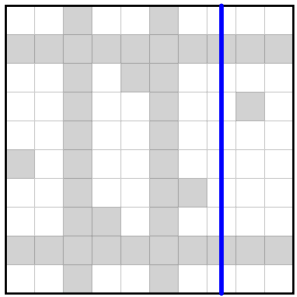
$M \subseteq [n]^D$ is ε-***closed*** if $\forall$ i-axis parallel lines ℓ, either $\ell \subseteq M$ or $|\ell \cap M| \leq \varepsilon n$.



ε-closed sets

Definition

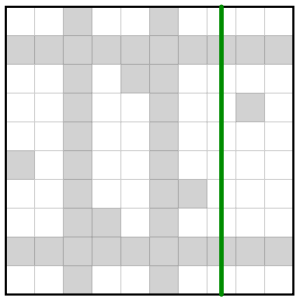
$M \subseteq [n]^D$ is ε-***closed*** if $\forall$ i-axis parallel lines ℓ, either $\ell \subseteq M$ or $|\ell \cap M| \leq \varepsilon n$.



ε-closed sets

Definition

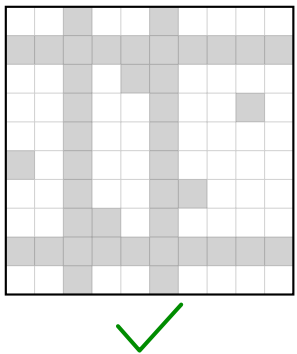
$M \subseteq [n]^D$ is ε-***closed*** if $\forall$ i-axis parallel lines ℓ, either $\ell \subseteq M$ or $|\ell \cap M| \leq \varepsilon n$.



ε-closed sets

Definition

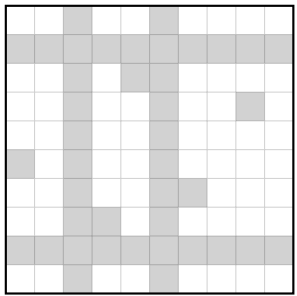
$M \subseteq [n]^D$ is ε-***closed*** if $\forall$ i-axis parallel lines ℓ, either $\ell \subseteq M$ or $|\ell \cap M| \leq \varepsilon n$.

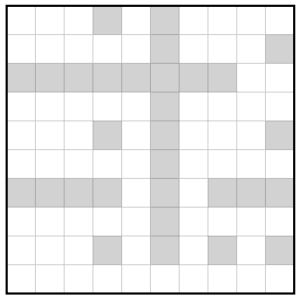


ε-closed sets

Definition

$M \subseteq [n]^D$ is ε-***closed*** if $\forall$ i-axis parallel lines ℓ, either $\ell \subseteq M$ or $|\ell \cap M| \leq \varepsilon n$.

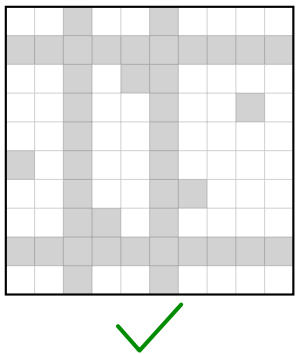


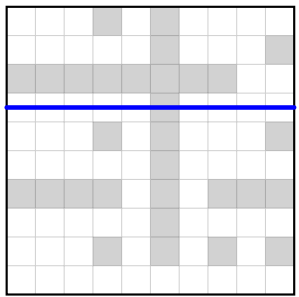


ε-closed sets

Definition

$M \subseteq [n]^D$ is ε-***closed*** if $\forall$ i-axis parallel lines ℓ, either $\ell \subseteq M$ or $|\ell \cap M| \leq \varepsilon n$.

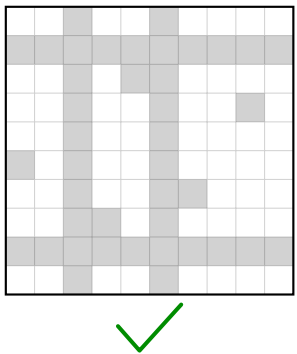


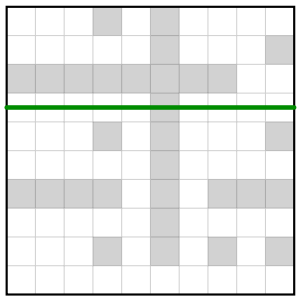


ε-closed sets

Definition

$M \subseteq [n]^D$ is ε-***closed*** if $\forall$ i-axis parallel lines ℓ, either $\ell \subseteq M$ or $|\ell \cap M| \leq \varepsilon n$.

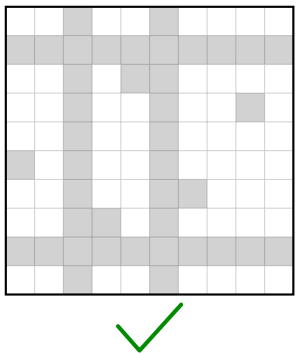


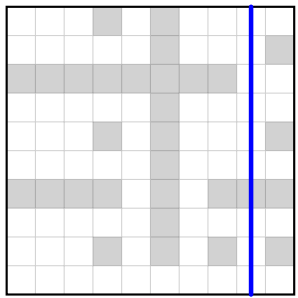


ε-closed sets

Definition

$M \subseteq [n]^D$ is ε-***closed*** if $\forall$ i-axis parallel lines ℓ, either $\ell \subseteq M$ or $|\ell \cap M| \leq \varepsilon n$.

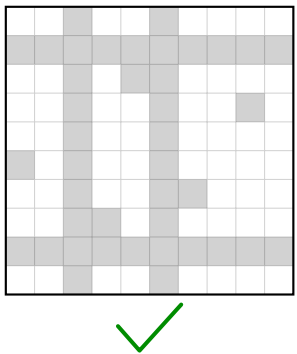


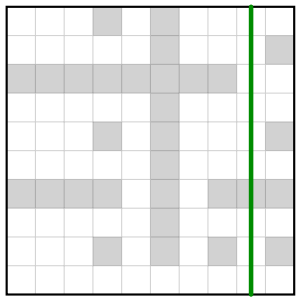


ε-closed sets

Definition

$M \subseteq [n]^D$ is ε-***closed*** if $\forall$ i-axis parallel lines ℓ, either $\ell \subseteq M$ or $|\ell \cap M| \leq \varepsilon n$.

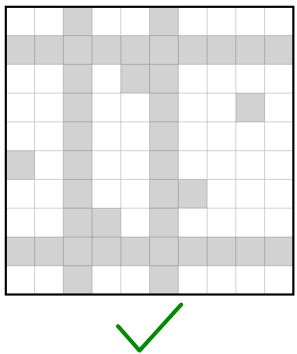


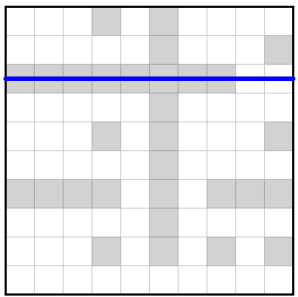


ε-closed sets

Definition

$M \subseteq [n]^D$ is ε-***closed*** if $\forall$ i-axis parallel lines ℓ, either $\ell \subseteq M$ or $|\ell \cap M| \leq \varepsilon n$.

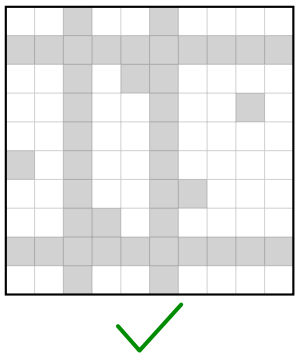


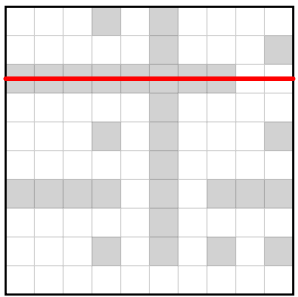


ε-closed sets

Definition

$M \subseteq [n]^D$ is ε-***closed*** if $\forall$ i-axis parallel lines ℓ, either $\ell \subseteq M$ or $|\ell \cap M| \leq \varepsilon n$.

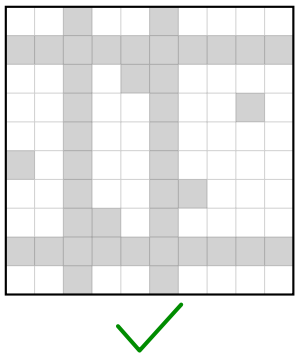


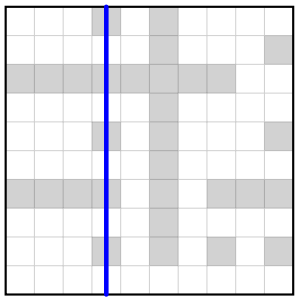


ε-closed sets

Definition

$M \subseteq [n]^D$ is ε-***closed*** if $\forall$ i-axis parallel lines ℓ, either $\ell \subseteq M$ or $|\ell \cap M| \leq \varepsilon n$.

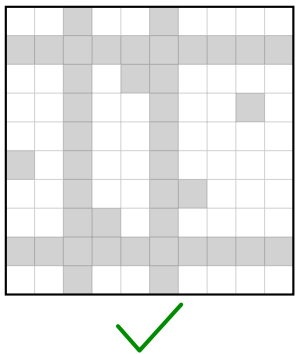


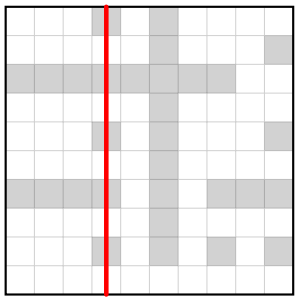


ε-closed sets

Definition

$M \subseteq [n]^D$ is ε-***closed*** if $\forall$ i-axis parallel lines ℓ, either $\ell \subseteq M$ or $|\ell \cap M| \leq \varepsilon n$.

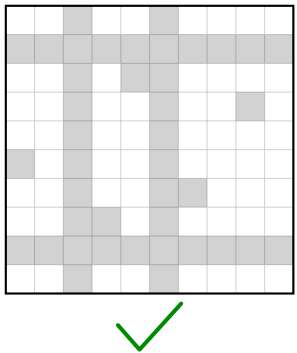




ε-closed sets

Definition

$M \subseteq [n]^D$ is ε-***closed*** if $\forall$ i-axis parallel lines ℓ, either $\ell \subseteq M$ or $|\ell \cap M| \leq \varepsilon n$.



Product expansion

Definition

Property of gadgets necessary for LTC constructions

- ε-closed sets ✓
- Extendable sets

Extendable sets

Extendable sets

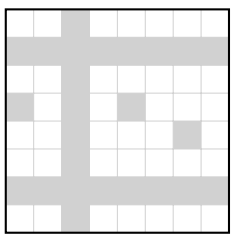
Definition

A set $M \subseteq [n]^D$ is ***extendable*** if $\forall\, c_M \in \mathbb{F}_q^M$ s.t. $\forall\, i$-axis parallel lines $\ell \subseteq M$ have $c_M|_\ell \in \mathcal{C}_i$, there exists a global codeword $c \in \mathcal{C}_1 \otimes \cdots \otimes \mathcal{C}_D$ s.t. $c|_M = c_M$.

Extendable sets

Definition

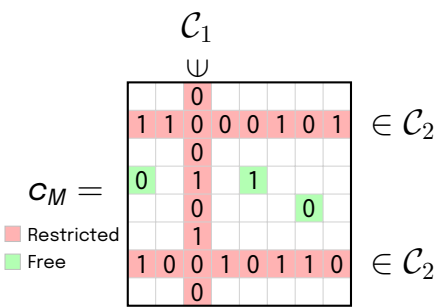
A set $M \subseteq [n]^D$ is ***extendable*** if $\forall\, c_M \in \mathbb{F}_q^M$ s.t. $\forall\, i$-axis parallel lines $\ell \subseteq M$ have $c_M|_\ell \in \mathcal{C}_i$, there exists a global codeword $c \in \mathcal{C}_1 \otimes \cdots \otimes \mathcal{C}_D$ s.t. $c|_M = c_M$.



Extendable sets

Definition

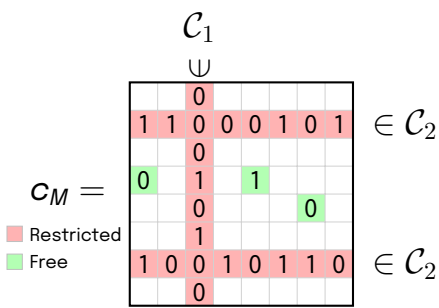
A set $M \subseteq [n]^D$ is ***extendable*** if $\forall\, c_M \in \mathbb{F}_q^M$ s.t. $\forall\, i$-axis parallel lines $\ell \subseteq M$ have $c_M|_\ell \in \mathcal{C}_i$, there exists a global codeword $c \in \mathcal{C}_1 \otimes \cdots \otimes \mathcal{C}_D$ s.t. $c|_M = c_M$.



Extendable sets

Definition

A set $M \subseteq [n]^D$ is ***extendable*** if $\forall\, c_M \in \mathbb{F}_q^M$ s.t. $\forall\, i$-axis parallel lines $\ell \subseteq M$ have $c_M|_\ell \in \mathcal{C}_i$, there exists a global codeword $c \in \mathcal{C}_1 \otimes \cdots \otimes \mathcal{C}_D$ s.t. $c|_M = c_M$.



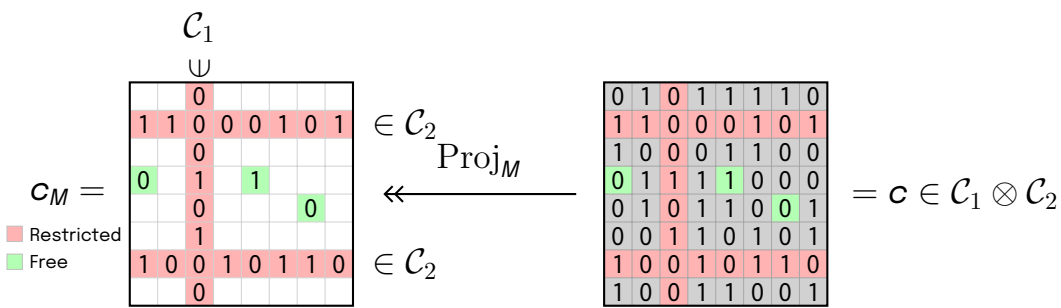


$= c \in \mathcal{C}_1 \otimes \mathcal{C}_2$

Extendable sets

Definition

A set $M \subseteq [n]^D$ is ***extendable*** if $\forall\, c_M \in \mathbb{F}_q^M$ s.t. $\forall$ i-axis parallel lines $\ell \subseteq M$ have $c_M|_\ell \in \mathcal{C}_i$, there exists a global codeword $c \in \mathcal{C}_1 \otimes \cdots \otimes \mathcal{C}_D$ s.t. $c|_M = c_M$.



Product expansion

Definition

Property of gadgets necessary for LTC constructions

- ε-closed sets ✓
- Extendable sets ✓

Product expansion

Definition

- A collection $\mathcal{C}_1, \ldots, \mathcal{C}_D$ is ε-***product expanding*** if every ε-closed set $M \subseteq [n]^D$ is extendable.

Product expansion

Definition

- A collection $\mathcal{C}_1, \ldots, \mathcal{C}_D$ is ***ε-product expanding*** if every ε-closed set $M \subseteq [n]^D$ is extendable.
- A collection $\mathcal{C}_1, \ldots, \mathcal{C}_D$ is ***two-sided ε-product expanding*** if both $\mathcal{C}_1, \ldots, \mathcal{C}_D$ and $\mathcal{C}_1, ^{\perp} \ldots, \mathcal{C}_D^{\perp}$ are ε-product expanding.

Product expansion

Definition

- A collection $\mathcal{C}_1, \ldots, \mathcal{C}_D$ is ***ε-product expanding*** if every ε-closed set $M \subseteq [n]^D$ is extendable.
- A collection $\mathcal{C}_1, \ldots, \mathcal{C}_D$ is ***two-sided ε-product expanding*** if both $\mathcal{C}_1, \ldots, \mathcal{C}_D$ and $\mathcal{C}_1, ^{\perp} \ldots, \mathcal{C}_D^{\perp}$ are ε-product expanding.

The possible labelings of any sufficiently closed set depend ONLY on internal parity checks

Part 2: Results

Product expansion of random linear codes

Product expansion of random linear codes

Theorem [Kalachev, Panteleev, '25]

With explicit good LTCs of [DELLM]: Two-sided ε-product expanding codes $\mathcal{C}_1, \ldots, \mathcal{C}_D \subseteq \mathbb{F}_{2^t}^n$ **exist** for large enough $n \in \mathbb{N}$, $t = (n+1)^D$, and constant $\varepsilon > 0$.

Product expansion of random linear codes

Theorem [Kalachev, Panteleev, '25]

With explicit good LTCs of [DELLM]: Two-sided ε-product expanding codes $\mathcal{C}_1, \ldots, \mathcal{C}_D \subseteq \mathbb{F}_{2^t}^n$ **exist** for large enough $n \in \mathbb{N}$, $t = (n+1)^D$, and constant $\varepsilon > 0$.

Theorem 1 [Chattopadhyay, R, Spooner, '26]

Without any explicit objects: Two-sided ε-product expanding codes $\mathcal{C}_1, \ldots, \mathcal{C}_D \subseteq \mathbb{F}_p^n$ **exist** for large enough $n \in \mathbb{N}$, $p = O(2^{n^D} n^D \log n)$, and const $\varepsilon > 0$.

Product expansion of random linear codes

Theorem [Kalachev, Panteleev, '25]

With explicit good LTCs of [DELLM]: Two-sided ε-product expanding codes $\mathcal{C}_1, \ldots, \mathcal{C}_D \subseteq \mathbb{F}_{2^t}^n$ **exist** for large enough $n \in \mathbb{N}$, $t = (n+1)^D$, and constant $\varepsilon > 0$.

Theorem 1 [Chattopadhyay, R, Spooner, '26]

Without any explicit objects: Two-sided ε-product expanding codes $\mathcal{C}_1, \ldots, \mathcal{C}_D \subseteq \mathbb{F}_p^n$ **exist** for large enough $n \in \mathbb{N}$, $p = O(2^{n^D} n^D \log n)$, and const $\varepsilon > 0$.

Didn't we just do the same thing... but worse?

Product expansion of symmetric codes

Product expansion of symmetric codes

Theorem [Bafna, Li, Nguyen, '26], [Gay, Jeronimo, '26], [Chen, Huang, Liu, Tang, '26]

The tensor of **projective Reed-Solomon codes** $\mathcal{C}_1 \otimes \cdots \otimes \mathcal{C}_D$ of **coprime lengths** evaluated on **roots of unity over** $\mathbb{F}_{2^t}$ is two-sided ε-product expanding for some constant $\varepsilon > 0$.

Product expansion of symmetric codes

Theorem [Bafna, Li, Nguyen, '26], [Gay, Jeronimo, '26], [Chen, Huang, Liu, Tang, '26]

The tensor of **projective Reed-Solomon codes** $\mathcal{C}_1 \otimes \cdots \otimes \mathcal{C}_D$ of **coprime lengths** evaluated on **roots of unity over** $\mathbb{F}_{2^t}$ is two-sided ε-product expanding for some constant $\varepsilon > 0$.

Theorem 2 [Chattopadhyay, R, Spooner, '26]

Two-sided ε-product expanding codes $\mathcal{C}_1 \otimes \mathcal{C}_2 \subseteq \mathbb{F}_p^{n^2}$ with the local symmetries of [RSV'19] of rate $1/2$ **exist** for large enough **prime** $n \in \mathbb{N}$, $p = O(2^{n^2} n^2 \log n)$, and constant $\varepsilon > 0$.

Plan

Before lunch

Theorem 1

Without any explicit objects: Two-sided ε-product expanding codes $\mathcal{C}_1, \ldots, \mathcal{C}_D \subseteq \mathbb{F}_p^n$ **exist** for large enough $n \in \mathbb{N}$, $p = O(2^{n^D} n^D \log n)$, and const $\varepsilon > 0$.

After lunch (whiteboard)

Theorem 2

Two-sided ε-product expanding codes $\mathcal{C}_1 \otimes \mathcal{C}_2 \subseteq \mathbb{F}_p^{n^2}$ with the local symmetries of [RSV'19] of rate $1/2$ **exist** for large enough **prime** $n \in \mathbb{N}$, $p = O(2^{n^2} n^2 \log n)$, and constant $\varepsilon > 0$.

Part 3: Techniques

Maximal extendability

Maximal extendability

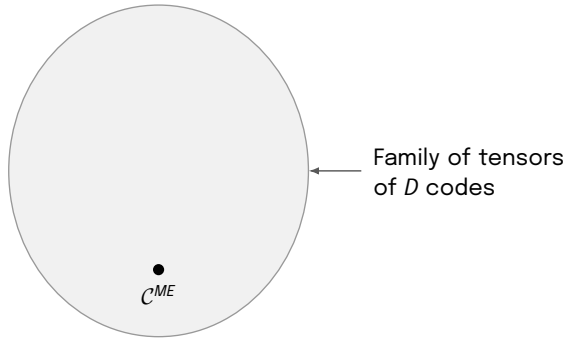
Definition

A tensor code $\mathcal{C} = \mathcal{C}_1 \otimes \cdots \otimes \mathcal{C}_D$ is ***maximally extendable*** if for any other $\mathcal{C}' = \mathcal{C}'_1 \otimes \cdots \otimes \mathcal{C}'_D$ s.t. $\dim(\mathcal{C}'_i) = \dim(\mathcal{C}_i)$ with $M \subseteq [n]^D$ extendable in $\mathcal{C}'$, then M is also extendable in $\mathcal{C}$.

Maximal extendability

Definition

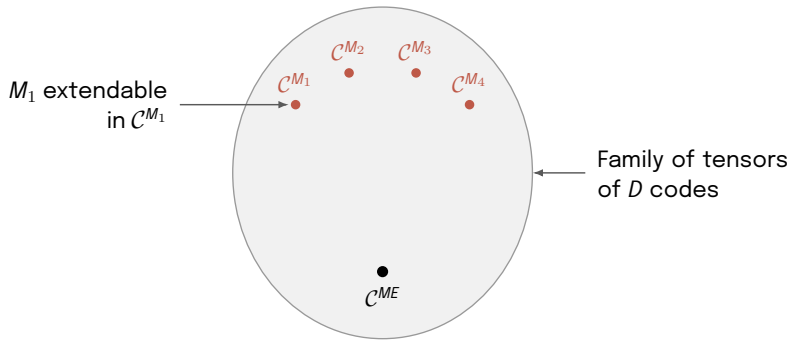
A tensor code $\mathcal{C} = \mathcal{C}_1 \otimes \cdots \otimes \mathcal{C}_D$ is ***maximally extendable*** if for any other $\mathcal{C}' = \mathcal{C}'_1 \otimes \cdots \otimes \mathcal{C}'_D$ s.t. $\dim(\mathcal{C}'_i) = \dim(\mathcal{C}_i)$ with $M \subseteq [n]^D$ extendable in $\mathcal{C}'$, then M is also extendable in $\mathcal{C}$.



Maximal extendability

Definition

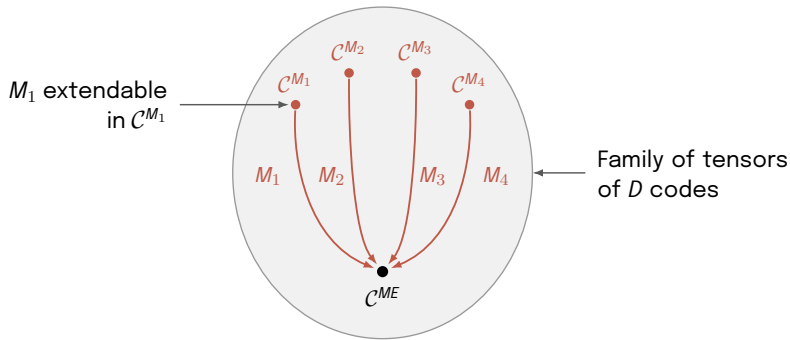
A tensor code $\mathcal{C} = \mathcal{C}_1 \otimes \cdots \otimes \mathcal{C}_D$ is ***maximally extendable*** if for any other $\mathcal{C}' = \mathcal{C}'_1 \otimes \cdots \otimes \mathcal{C}'_D$ s.t. $\dim(\mathcal{C}'_i) = \dim(\mathcal{C}_i)$ with $M \subseteq [n]^D$ extendable in $\mathcal{C}'$, then M is also extendable in $\mathcal{C}$.



Maximal extendability

Definition

A tensor code $\mathcal{C} = \mathcal{C}_1 \otimes \cdots \otimes \mathcal{C}_D$ is ***maximally extendable*** if for any other $\mathcal{C}' = \mathcal{C}'_1 \otimes \cdots \otimes \mathcal{C}'_D$ s.t. $\dim(\mathcal{C}'_i) = \dim(\mathcal{C}_i)$ with $M \subseteq [n]^D$ extendable in $\mathcal{C}'$, then M is also extendable in $\mathcal{C}$.



Maximal extendability

Definition

A tensor code $\mathcal{C} = \mathcal{C}_1 \otimes \cdots \otimes \mathcal{C}_D$ is ***maximally extendable*** if for any other $\mathcal{C}' = \mathcal{C}'_1 \otimes \cdots \otimes \mathcal{C}'_D$ s.t. $\dim(\mathcal{C}'_i) = \dim(\mathcal{C}_i)$ with $M \subseteq [n]^D$ extendable in $\mathcal{C}'$, then M is also extendable in $\mathcal{C}$.

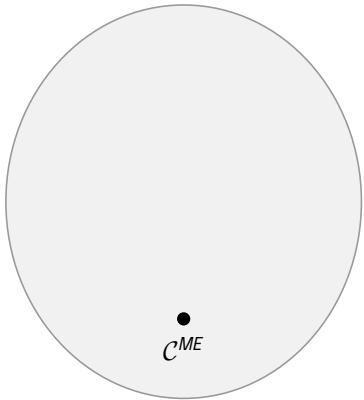
Theorem [Panteleev, Kalachev, '24], [Kalachev, Panteleev, '25]

For uniformly random codes $\mathcal{C}_1, \ldots, \mathcal{C}_D \subseteq \mathbb{F}_{2^t}^n$ with $\dim(\mathcal{C}_i) = k_i$, the tensor code $\mathcal{C}_1 \otimes \cdots \otimes \mathcal{C}_D$ is **maximally extendable w.h.p.**as $t \to \infty$.

Comparing strategies

Comparing strategies

[KP25]
One witness for all sets

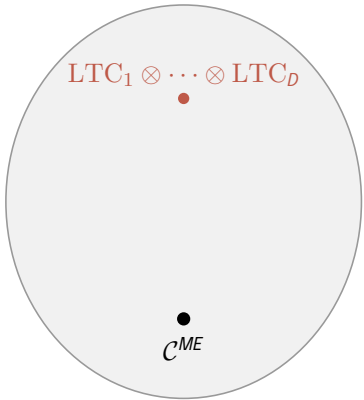


- Exists maximally extendable $\mathcal{C}^{ME}$

Comparing strategies

[KP25]

One witness for all sets

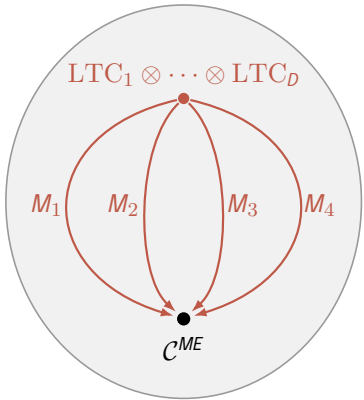


- Exists maximally extendable $\mathcal{C}^{ME}$
- Product of good LTCs is ε-PE

Comparing strategies

[KP25]

One witness for all sets



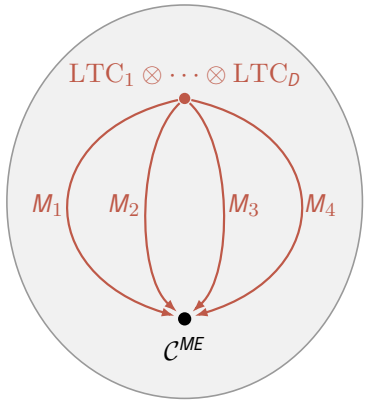
$\exists \mathcal{C} \ \ \forall \varepsilon$-closed M

- Exists maximally extendable $\mathcal{C}^{ME}$
- Product of good LTCs is ε-PE
- $\mathcal{C}^{ME}$ is ε-PE

Comparing strategies

[KP25]

One witness for all sets

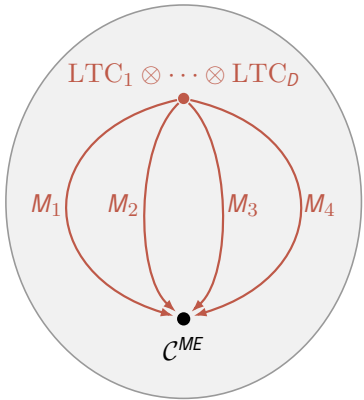


$\exists \mathcal{C} \quad \forall \varepsilon$-closed M

- Exists maximally extendable $\mathcal{C}^{ME}$
- Product of good LTCs is ε-PE
- $\mathcal{C}^{ME}$ is ε-PE
- Dual of product of random codes is product of random codes, so union bound to get two-sided ε-PE

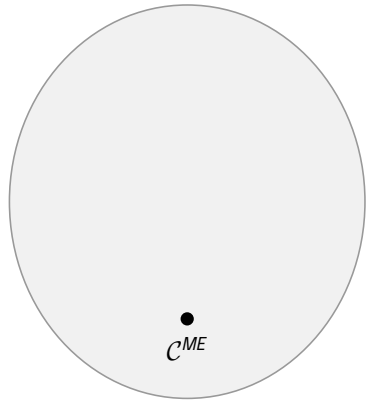
Comparing strategies

[KP25]
One witness for all sets



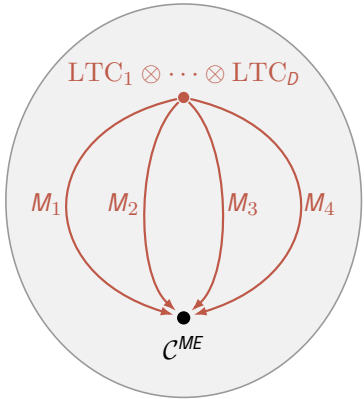
$\exists \mathcal{C} \quad \forall \varepsilon$-closed M

Our approach
A witness for each set



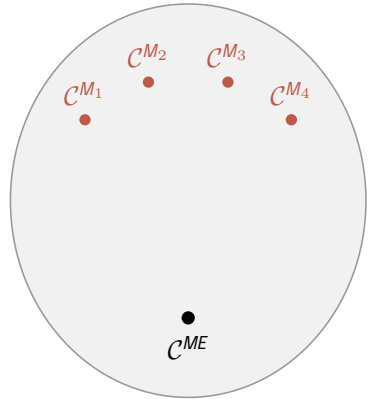
Comparing strategies

[KP25]
One witness for all sets



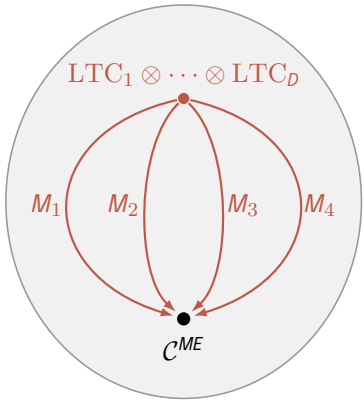
$\exists \mathcal{C} \quad \forall \varepsilon$-closed M

Our approach
A witness for each set



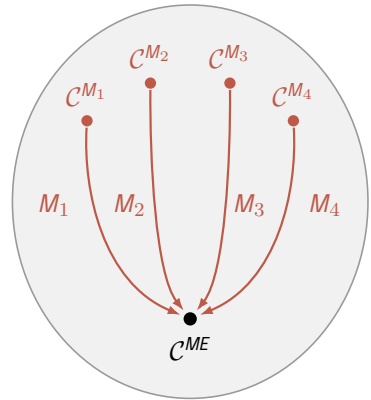
Comparing strategies

[KP25]
One witness for all sets



$\exists \mathcal{C} \ \ \forall \varepsilon$-closed M

Our approach
A witness for each set



$\forall \varepsilon$-closed M $\ \exists \mathcal{C}^M$

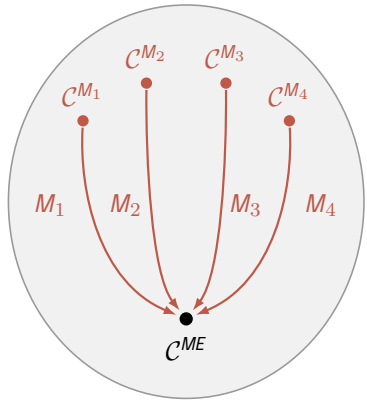
Comparing strategies

By not using explicit good LTCs, we:

- Develop new techniques to analyze **random codes over $\mathbb{R}$ and $\mathbb{C}$**

Our approach

A witness for each set



$\forall\, \varepsilon$-closed M $\exists\, \mathcal{C}^M$

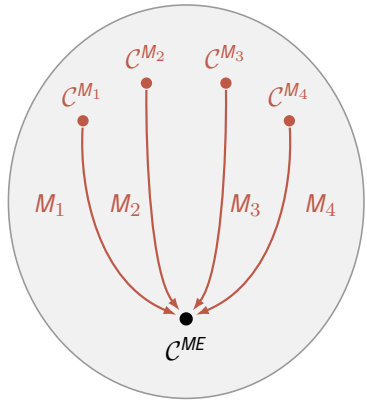
Comparing strategies

By not using explicit good LTCs, we:

- Develop new techniques to analyze **random codes over $\mathbb{R}$ and $\mathbb{C}$**
- Develop new model of codes over $\mathbb{F}$ generated by **Rademacher matrices**

Our approach

A witness for each set



$\forall\, \varepsilon$-closed M $\exists\, \mathcal{C}^M$

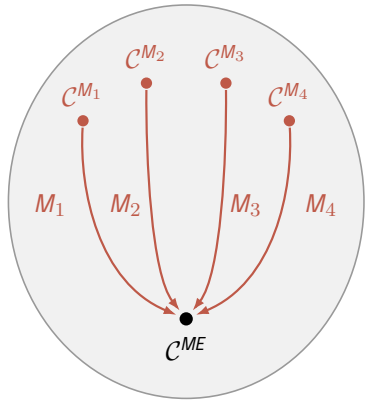
Comparing strategies

By not using explicit good LTCs, we:

- Develop new techniques to analyze **random codes over $\mathbb{R}$ and $\mathbb{C}$**
- Develop new model of codes over $\mathbb{F}$ generated by **Rademacher matrices**
  - Connect to weak Wigner words [Wig'55], **walks on bipartite graphs**

Our approach

A witness for each set



$\forall\, \varepsilon$-closed M $\exists\, \mathcal{C}^M$

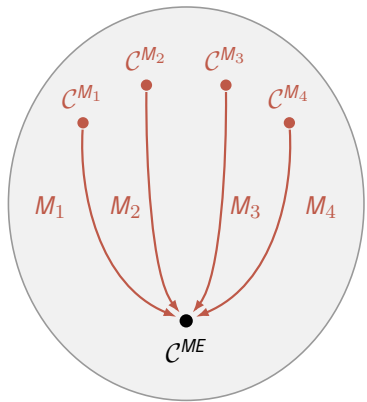
Comparing strategies

By not using explicit good LTCs, we:

- Develop new techniques to analyze **random codes over $\mathbb{R}$ and $\mathbb{C}$**
- Develop new model of codes over $\mathbb{F}$ generated by **Rademacher matrices**
  - Connect to weak Wigner words [Wig'55], **walks on bipartite graphs**
- Remove explicit good LTC bottleneck, allowing for:

Our approach

A witness for each set



$\forall\, \varepsilon$-closed M $\exists\, \mathcal{C}^M$

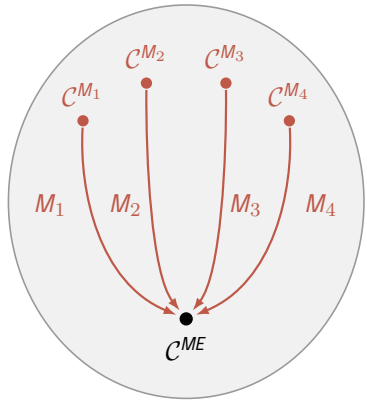
Comparing strategies

By not using explicit good LTCs, we:

- Develop new techniques to analyze **random codes over $\mathbb{R}$ and $\mathbb{C}$**
- Develop new model of codes over $\mathbb{F}$ generated by **Rademacher matrices**
  - Connect to weak Wigner words [Wig'55], **walks on bipartite graphs**
- Remove explicit good LTC bottleneck, allowing for:
  - Analysis of codes with **symmetries**

Our approach

A witness for each set

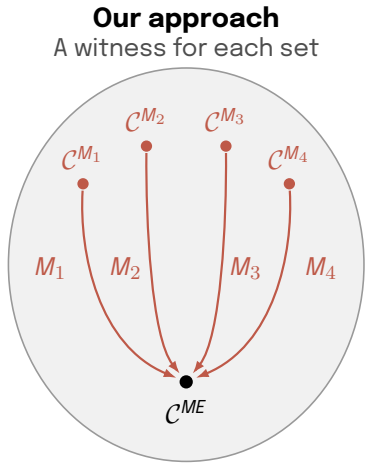


$\forall\, \varepsilon$-closed M $\exists\, \mathcal{C}^M$

Comparing strategies

By not using explicit good LTCs, we:

- Develop new techniques to analyze **random codes over $\mathbb{R}$ and $\mathbb{C}$**
- Develop new model of codes over $\mathbb{F}$ generated by **Rademacher matrices**
  - Connect to weak Wigner words [Wig'55], **walks on bipartite graphs**
- Remove explicit good LTC bottleneck, allowing for:
  - Analysis of codes with **symmetries**
  - Analysis of codes for **non-cubical complexes**



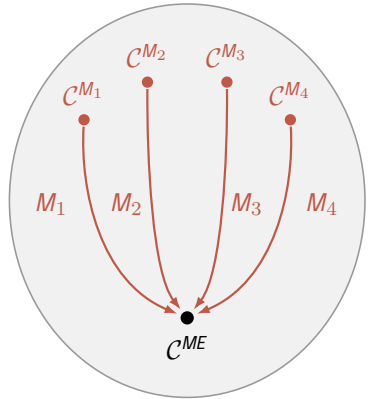
Comparing strategies

By not using explicit good LTCs, we:

- Develop new techniques to analyze **random codes over $\mathbb{R}$ and $\mathbb{C}$**
- Develop new model of codes over $\mathbb{F}$ generated by **Rademacher matrices**
  - Connect to weak Wigner words [Wig'55], **walks on bipartite graphs**
- Remove explicit good LTC bottleneck, allowing for:
  - Analysis of codes with **symmetries**
  - Analysis of codes for **non-cubical complexes**
- **Natural** probabilistic/existential proof

Our approach

A witness for each set



$\forall\, \varepsilon$-closed M $\exists\, \mathcal{C}^M$

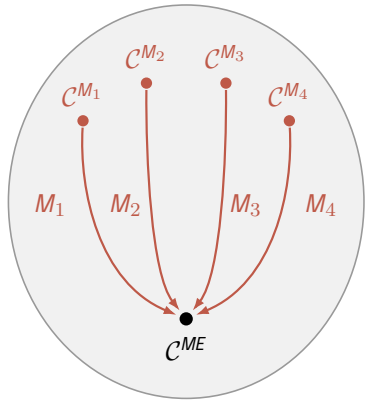
Comparing strategies

Goal

For every fixed ε-closed $M \subseteq [n]^D$, show that there exists $\mathcal{C}^M = \mathcal{C}_1 \otimes \cdots \otimes \mathcal{C}_D$ such that M **is extendable in** $\mathcal{C}^M$ **(over** $\mathbb{R}$**).**

Our approach

A witness for each set



$\forall\, \varepsilon$-closed M $\exists\, \mathcal{C}^M$

Proof overview

Goal

For every fixed ε-closed $M \subseteq [n]^D$, show that there exists $\mathcal{C}^M = \mathcal{C}_1 \otimes \cdots \otimes \mathcal{C}_D$ such that M **is extendable in** $\mathcal{C}^M$ **(over** $\mathbb{R}$**).**

Proof overview

Goal

For every fixed ε-closed $M \subseteq [n]^D$, show that there exists $\mathcal{C}^M = \mathcal{C}_1 \otimes \cdots \otimes \mathcal{C}_D$ such that M **is extendable in** $\mathcal{C}^M$ **(over** $\mathbb{R}$**).**

1. Sample $\mathcal{C}_1, \ldots, \mathcal{C}_D$ randomly by (left) generator matrices $G_1, \ldots, G_D$ with random Rademacher entries $(\sigma_{r,t}^{(j)})_{j \in [D], r \in [k_j], t \in [n]} \sim \{-1, 1\}$, so $\mathcal{C}_i = \mathrm{Im}(G_i)$.

Proof overview

Goal

For every fixed ε-closed $M \subseteq [n]^D$, show that there exists $\mathcal{C}^M = \mathcal{C}_1 \otimes \cdots \otimes \mathcal{C}_D$ such that M **is extendable in** $\mathcal{C}^M$ **(over** $\mathbb{R}$**).**

1. Sample $\mathcal{C}_1, \ldots, \mathcal{C}_D$ randomly by (left) generator matrices $G_1, \ldots, G_D$ with random Rademacher entries $(\sigma^{(j)}_{r,t})_{j \in [D], r \in [k_j], t \in [n]} \sim \{-1, 1\}$, so $\mathcal{C}_i = \mathrm{Im}(G_i)$.
2. M is extendable $\iff \mathrm{Proj}_M$ is surjective.

Proof overview

Goal

For every fixed ε-closed $M \subseteq [n]^D$, show that there exists $\mathcal{C}^M = \mathcal{C}_1 \otimes \cdots \otimes \mathcal{C}_D$ such that M **is extendable in** $\mathcal{C}^M$ **(over** $\mathbb{R}$**).**

1. Sample $\mathcal{C}_1, \ldots, \mathcal{C}_D$ randomly by (left) generator matrices $G_1, \ldots, G_D$ with random Rademacher entries $(\sigma^{(j)}_{r,t})_{j \in [D], r \in [k_j], t \in [n]} \sim \{-1, 1\}$, so $\mathcal{C}_i = \mathrm{Im}(G_i)$.
2. M is extendable $\iff \mathrm{Proj}_M$ is surjective.
3. $\iff$ its dual ***extension map*** τ_M is injective.

Proof overview

Goal

For every fixed ε-closed $M \subseteq [n]^D$, show that there exists $\mathcal{C}^M = \mathcal{C}_1 \otimes \cdots \otimes \mathcal{C}_D$ such that M **is extendable in** $\mathcal{C}^M$ **(over** $\mathbb{R}$**).**

1. Sample $\mathcal{C}_1, \ldots, \mathcal{C}_D$ randomly by (left) generator matrices $G_1, \ldots, G_D$ with random Rademacher entries $(\sigma^{(j)}_{r,t})_{j\in[D], r\in[k_j], t\in[n]} \sim \{-1, 1\}$, so $\mathcal{C}_i = \mathrm{Im}(G_i)$.
2. M is extendable $\iff \mathrm{Proj}_M$ is surjective.
3. $\iff$ its dual ***extension map*** τ_M is injective.
4. $\iff \|K\|_{\mathrm{op}} < 1$ where $K = \tau_M^\top \tau_M - \mathrm{Id}$ since $\|\tau_M(x)\|^2 \geq (1 - \|K\|_{\mathrm{op}}) \|x\|^2$.

Proof overview

Goal

For every fixed ε-closed $M \subseteq [n]^D$, show that there exists $\mathcal{C}^M = \mathcal{C}_1 \otimes \cdots \otimes \mathcal{C}_D$ such that M **is extendable in** $\mathcal{C}^M$ **(over** $\mathbb{R}$**).**

1. Sample $\mathcal{C}_1, \ldots, \mathcal{C}_D$ randomly by (left) generator matrices $G_1, \ldots, G_D$ with random Rademacher entries $(\sigma^{(j)}_{r,t})_{j \in [D], r \in [k_j], t \in [n]} \sim \{-1, 1\}$, so $\mathcal{C}_i = \mathrm{Im}(G_i)$.
2. M is extendable $\iff \mathrm{Proj}_M$ is surjective.
3. $\iff$ its dual ***extension map*** τ_M is injective.
4. $\iff \|K\|_{\mathrm{op}} < 1$ where $K = \tau_M^\top \tau_M - \mathrm{Id}$ since $\|\tau_M(x)\|^2 \geq (1 - \|K\|_{\mathrm{op}}) \|x\|^2$.
5. So just need $\mathbb{E}_\sigma[\|K\|_{\mathrm{op}}] < 1 \iff$ bounding $\mathbb{E}$ of a **Rademacher polynomials.**

Proof overview

Goal

For every fixed ε-closed $M \subseteq [n]^D$, show that there exists $\mathcal{C}^M = \mathcal{C}_1 \otimes \cdots \otimes \mathcal{C}_D$ such that M **is extendable in** $\mathcal{C}^M$ **(over** $\mathbb{R}$**).**

1. Sample $\mathcal{C}_1, \ldots, \mathcal{C}_D$ randomly by (left) generator matrices $G_1, \ldots, G_D$ with random Rademacher entries $(\sigma^{(j)}_{r,t})_{j \in [D], r \in [k_j], t \in [n]} \sim \{-1, 1\}$, so $\mathcal{C}_i = \mathrm{Im}(G_i)$.
2. M is extendable $\iff \mathrm{Proj}_M$ is surjective.
3. $\iff$ its dual ***extension map*** τ_M is injective.
4. $\iff \|K\|_{\mathrm{op}} < 1$ where $K = \tau_M^\top \tau_M - \mathrm{Id}$ since $\|\tau_M(x)\|^2 \geq (1 - \|K\|_{\mathrm{op}}) \|x\|^2$.
5. So just need $\mathbb{E}_\sigma[\|K\|_{\mathrm{op}}] < 1 \iff$ bounding $\mathbb{E}$ of a **Rademacher polynomials.**
6. $\iff$ Bound number of **non-backtracking walks on a bipartite graph with even edge traversals** adhering to M.

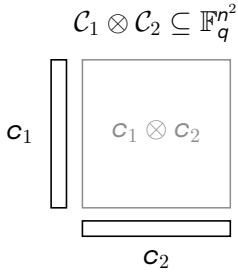
Proof overview

Goal

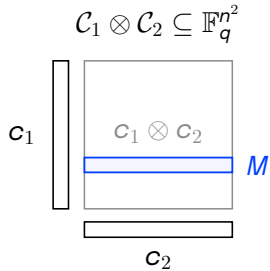
For every fixed ε-closed $M \subseteq [n]^D$, show that there exists $\mathcal{C}^M = \mathcal{C}_1 \otimes \cdots \otimes \mathcal{C}_D$ such that M **is extendable in** $\mathcal{C}^M$ **(over** $\mathbb{R}$**).**

1. Sample $\mathcal{C}_1, \ldots, \mathcal{C}_D$ randomly by (left) generator matrices $G_1, \ldots, G_D$ with random Rademacher entries $(\sigma^{(j)}_{r,t})_{j \in [D], r \in [k_j], t \in [n]} \sim \{-1, 1\}$, so $\mathcal{C}_i = \mathrm{Im}(G_i)$.
2. M is extendable $\iff \mathrm{Proj}_M$ is surjective.
3. $\iff$ its dual ***extension map*** τ_M is injective.
4. $\iff \|K\|_{\mathrm{op}} < 1$ where $K = \tau_M^\top \tau_M - \mathrm{Id}$ since $\|\tau_M(x)\|^2 \geq (1 - \|K\|_{\mathrm{op}}) \|x\|^2$.
5. So just need $\mathbb{E}_\sigma[\|K\|_{\mathrm{op}}] < 1 \iff$ bounding $\mathbb{E}$ of a **Rademacher polynomials.**
6. $\iff$ Bound number of **non-backtracking walks on a bipartite graph with even edge traversals** adhering to M.

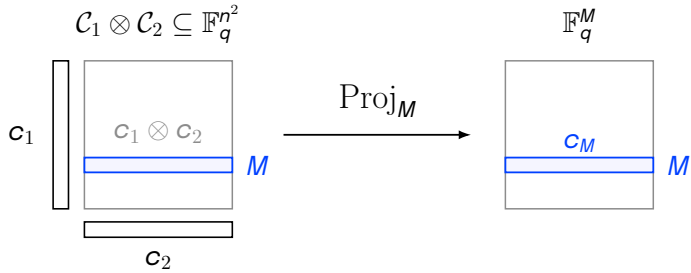
Behavior of τ_M



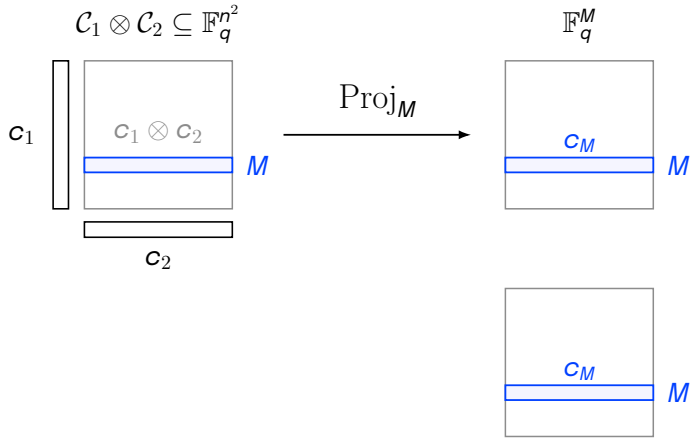
Behavior of τ_M



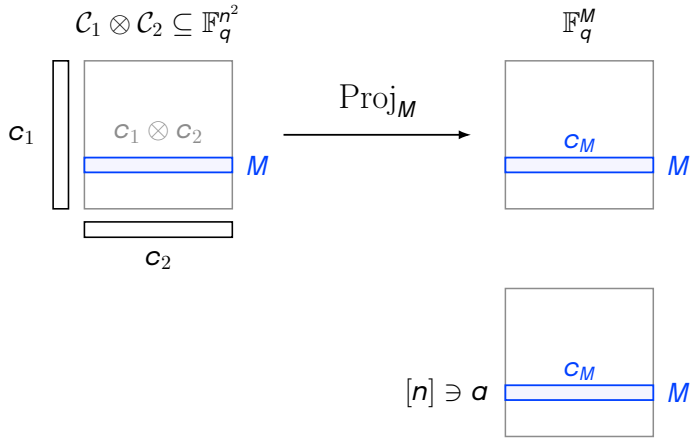
Behavior of τ_M



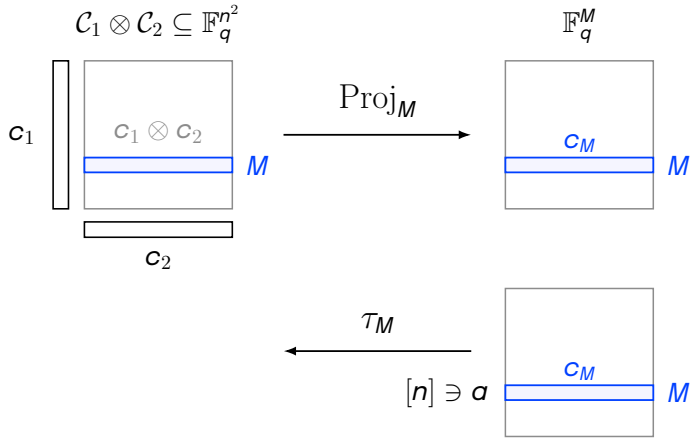
Behavior of τ_M



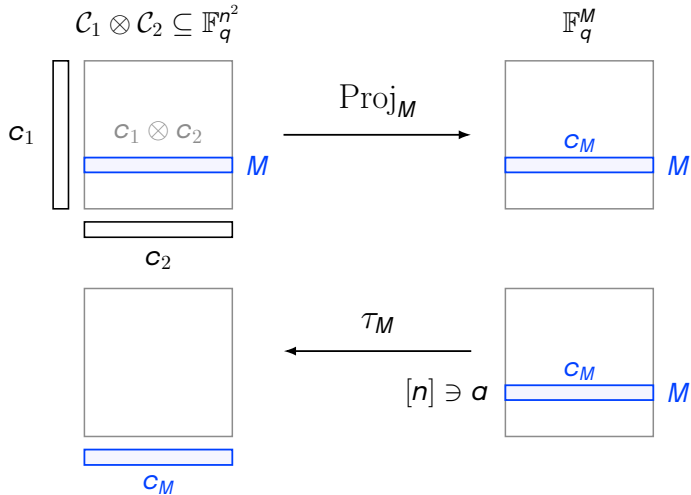
Behavior of τ_M



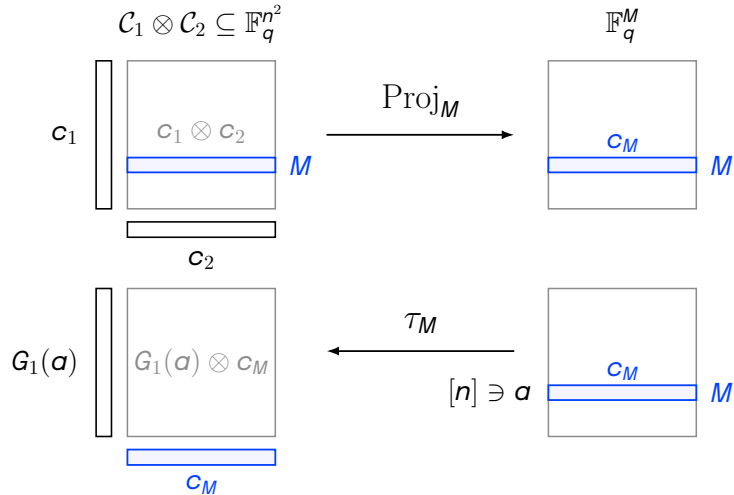
Behavior of τ_M



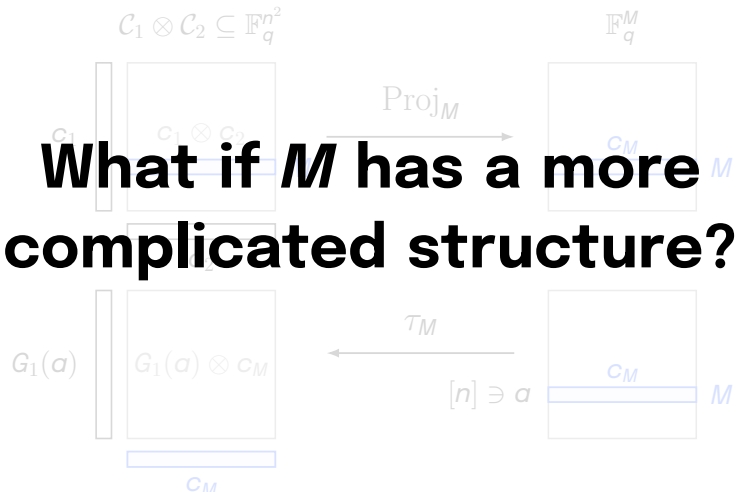
Behavior of τ_M



Behavior of τ_M



Behavior of τ_M



What if M has a more complicated structure?

Maximal planes

Definition

For a set of free coordinates $I \subseteq [D]$, we define the ***axis-parallel plane*** at the **anchor** $a \in [n]^{I^c}$ as $\mathcal{P}(I, a) = \{x \in [n]^D : \forall j \in I^c,\ x_j = a_j\}$.

Maximal planes

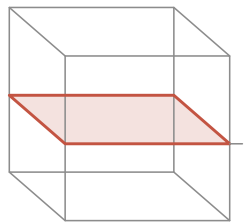
Definition

For a set of free coordinates $I \subseteq [D]$, we define the ***axis-parallel plane*** at the **anchor** $a \in [n]^{I^c}$ as $\mathcal{P}(I, a) = \{x \in [n]^D : \forall j \in I^c,\ x_j = a_j\}$.
$P = \mathcal{P}(I, a)$ ***maximal*** for $M \subseteq [n]^D$ if $P \subseteq M$ and no other plane in M contains P.

Maximal planes

Definition

For a set of free coordinates $I \subseteq [D]$, we define the ***axis-parallel plane*** at the **anchor** $a \in [n]^{I^c}$ as $\mathcal{P}(I, a) = \{x \in [n]^D : \forall j \in I^c,\ x_j = a_j\}$.
$P = \mathcal{P}(I, a)$ ***maximal*** for $M \subseteq [n]^D$ if $P \subseteq M$ and no other plane in M contains P.



$P_1 = \mathcal{P}(\{1, 2\}, (5))$

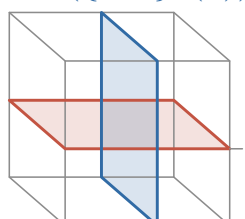
$M = P_1$

Maximal planes

Definition

For a set of free coordinates $I \subseteq [D]$, we define the ***axis-parallel plane*** at the **anchor** $a \in [n]^{I^c}$ as $\mathcal{P}(I, a) = \{x \in [n]^D : \forall j \in I^c,\ x_j = a_j\}$.
$P = \mathcal{P}(I, a)$ ***maximal*** for $M \subseteq [n]^D$ if $P \subseteq M$ and no other plane in M contains P.

$P_2 = \mathcal{P}(\{2, 3\}, (6))$



$P_1 = \mathcal{P}(\{1, 2\}, (5))$

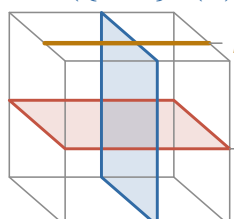
$M = P_1 \cup P_2$

Maximal planes

Definition

For a set of free coordinates $I \subseteq [D]$, we define the ***axis-parallel plane*** at the **anchor** $a \in [n]^{I^c}$ as $\mathcal{P}(I, a) = \{x \in [n]^D : \forall j \in I^c,\ x_j = a_j\}$.
$P = \mathcal{P}(I, a)$ ***maximal*** for $M \subseteq [n]^D$ if $P \subseteq M$ and no other plane in M contains P.

$P_2 = \mathcal{P}(\{2, 3\}, (6))$



$P_3 = \mathcal{P}(\{1\}, (8, 10))$

$P_1 = \mathcal{P}(\{1, 2\}, (5))$

$M = P_1 \cup P_2 \cup P_3$

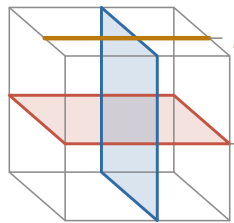
Maximal planes

Definition

For a set of free coordinates $I \subseteq [D]$, we define the ***axis-parallel plane*** at the **anchor** $a \in [n]^{I^c}$ as $\mathcal{P}(I, a) = \{x \in [n]^D : \forall j \in I^c,\ x_j = a_j\}$.
$P = \mathcal{P}(I, a)$ ***maximal*** for $M \subseteq [n]^D$ if $P \subseteq M$ and no other plane in M contains P.

τ_M acts by summing extension across all maximal planes

$P_2 = \mathcal{P}(\{2, 3\}, (6))$



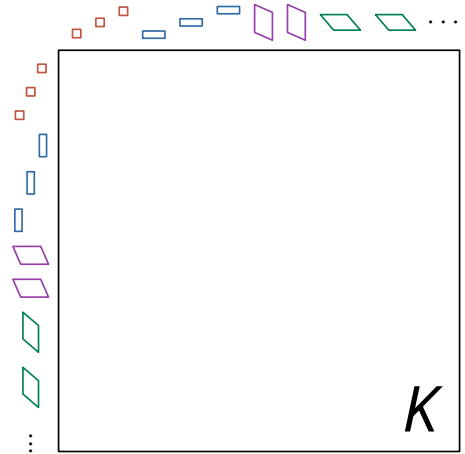
$P_3 = \mathcal{P}(\{1\}, (8, 10))$

$P_1 = \mathcal{P}(\{1, 2\}, (5))$

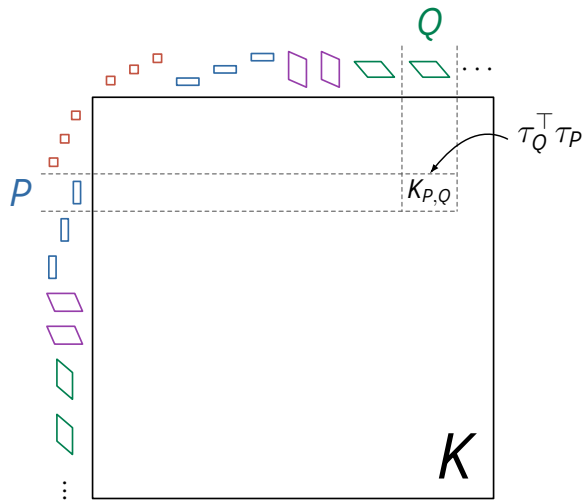
$M = P_1 \cup P_2 \cup P_3$

Structure of $K = \tau_M^\top \tau_M - \mathrm{Id}$

Structure of $K = \tau_M^\top \tau_M - \mathrm{Id}$



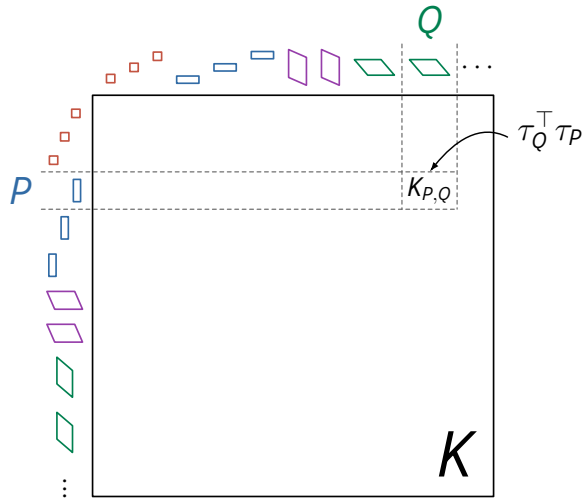
Structure of $K = \tau_M^\top \tau_M - \mathrm{Id}$



Structure of $K = \tau_M^\top \tau_M - \mathrm{Id}$

Goal:

Show $\mathbb{E}_\sigma[\|K\|_{\mathrm{op}}] < 1$

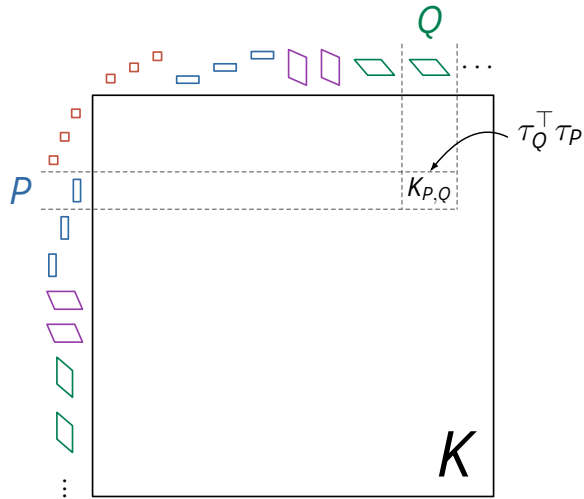


Structure of $K = \tau_M^\top \tau_M - \mathrm{Id}$

Goal:

Show $\mathbb{E}_\sigma[\|K\|_{\mathrm{op}}] < 1$

Idea 1:



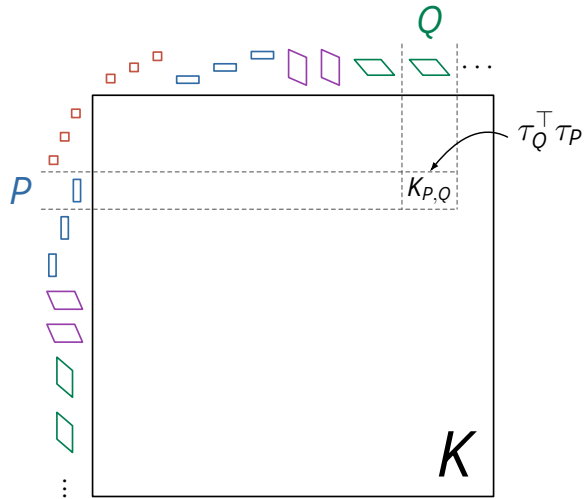
Structure of $K = \tau_M^\top \tau_M - \mathrm{Id}$

Goal:

Show $\mathbb{E}_\sigma[\|K\|_{\mathrm{op}}] < 1$

Idea 1:

1. $\mathbb{E}_\sigma[\|K_{P,Q}\|_{\mathrm{op}}] = O(1)$
   - Not too hard



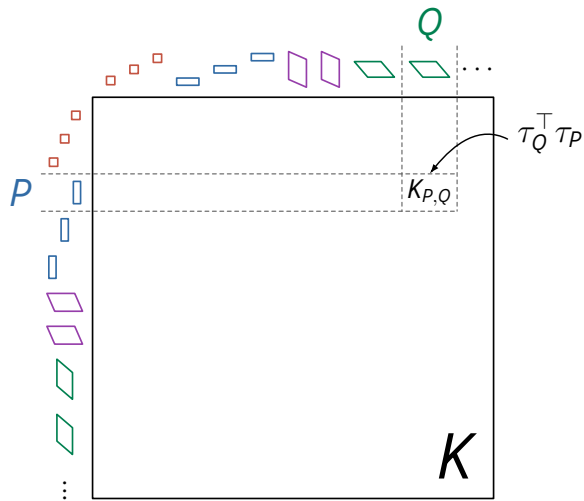
Structure of $K = \tau_M^\top \tau_M - \mathrm{Id}$

Goal:

Show $\mathbb{E}_\sigma[\|K\|_{\mathrm{op}}] < 1$

Idea 1:

1. $\mathbb{E}_\sigma[\|K_{P,Q}\|_{\mathrm{op}}] = O(1)$
   - Not too hard
2. $\|K\|_{\mathrm{op}} \leq \sum_{P,Q} \|K_{P,Q}\|_{\mathrm{op}}$



Structure of $K = \tau_M^\top \tau_M - \mathrm{Id}$

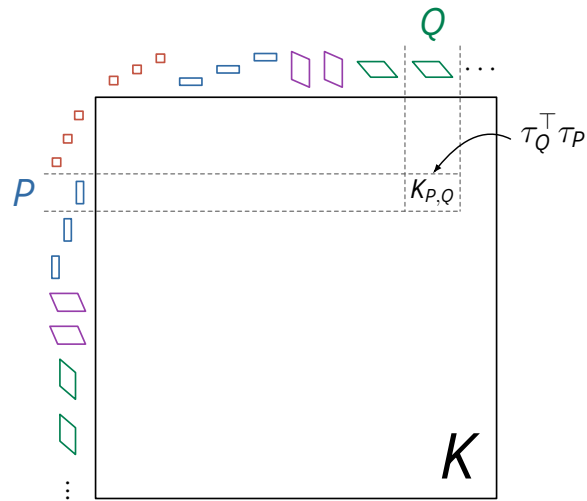
Goal:

Show $\mathbb{E}_\sigma[\|K\|_{\mathrm{op}}] < 1$

Idea 1:

1. $\mathbb{E}_\sigma[\|K_{P,Q}\|_{\mathrm{op}}] = O(1)$
   - Not too hard
2. $\|K\|_{\mathrm{op}} \leq \sum_{P,Q} \|K_{P,Q}\|_{\mathrm{op}}$

But M can contain $O(n^D)$ planes!

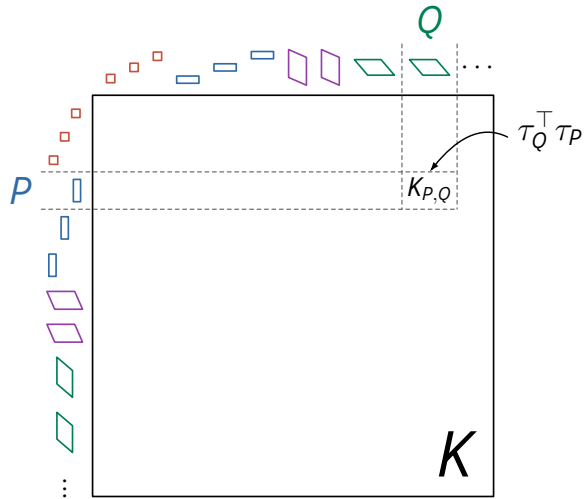


Structure of $K = \tau_M^\top \tau_M - \mathrm{Id}$

Goal:

Show $\mathbb{E}_\sigma[\|K\|_{\mathrm{op}}] < 1$

Idea 2:



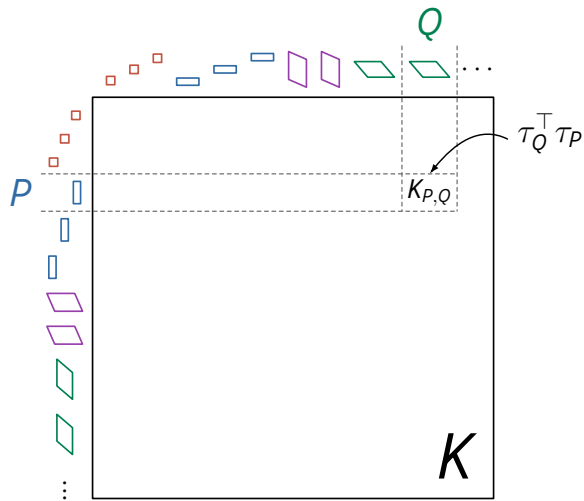
Structure of $K = \tau_M^\top \tau_M - \mathrm{Id}$

Goal:

Show $\mathbb{E}_\sigma[\|K\|_{\mathrm{op}}] < 1$

Idea 2:

1. Combine plane blocks $K_{P,Q}$ into direction blocks $K_{I,J}$.



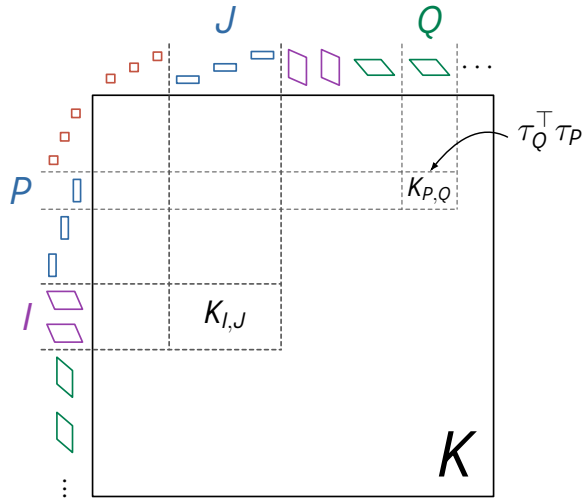
Structure of $K = \tau_M^\top \tau_M - \mathrm{Id}$

Goal:

Show $\mathbb{E}_\sigma[\|K\|_{\mathrm{op}}] < 1$

Idea 2:

1. Combine plane blocks $K_{P,Q}$ into direction blocks $K_{I,J}$.



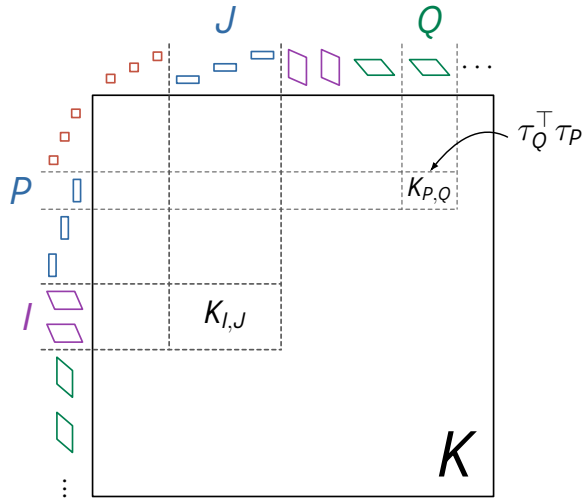
Structure of $K = \tau_M^\top \tau_M - \mathrm{Id}$

Goal:

Show $\mathbb{E}_\sigma[\|K\|_{\mathrm{op}}] < 1$

Idea 2:

1. Combine plane blocks $K_{P,Q}$ into direction blocks $K_{I,J}$.
2. $\mathbb{E}_\sigma[\|K_{I,J}\|_{\mathrm{op}}] = O(1)$
   - Hard!



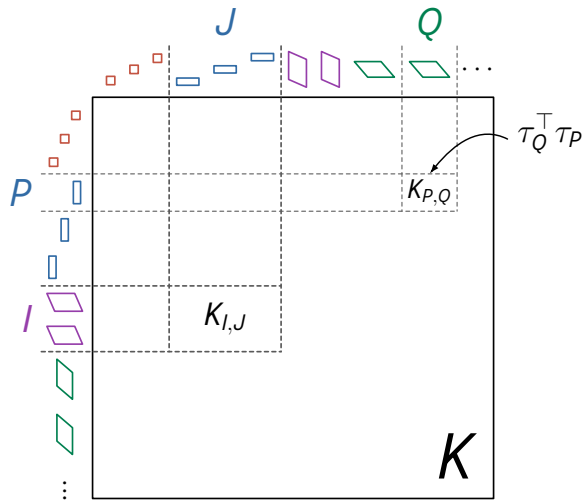
Structure of $K = \tau_M^\top \tau_M - \mathrm{Id}$

Goal:

Show $\mathbb{E}_\sigma[\|K\|_{\mathrm{op}}] < 1$

Idea 2:

1. Combine plane blocks $K_{P,Q}$ into direction blocks $K_{I,J}$.
2. $\mathbb{E}_\sigma[\|K_{I,J}\|_{\mathrm{op}}] = O(1)$
   - Hard!
3. $\|K\|_{\mathrm{op}} \leq \sum_{I,J} \|K_{I,J}\|_{\mathrm{op}}$



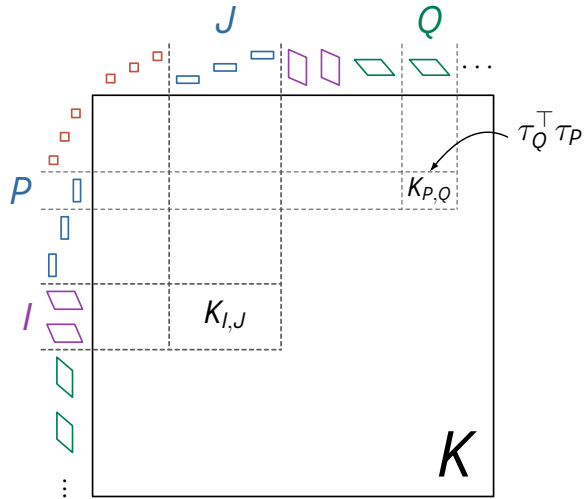
Structure of $K = \tau_M^\top \tau_M - \mathrm{Id}$

Goal:

Show $\mathbb{E}_\sigma[\|K\|_{\mathrm{op}}] < 1$

Idea 2:

1. Combine plane blocks $K_{P,Q}$ into direction blocks $K_{I,J}$.
2. $\mathbb{E}_\sigma[\|K_{I,J}\|_{\mathrm{op}}] = O(1)$
   - Hard!
3. $\|K\|_{\mathrm{op}} \leq \sum_{I,J} \|K_{I,J}\|_{\mathrm{op}}$
4. Only 4^D pairs $I, J \subseteq [D]$!



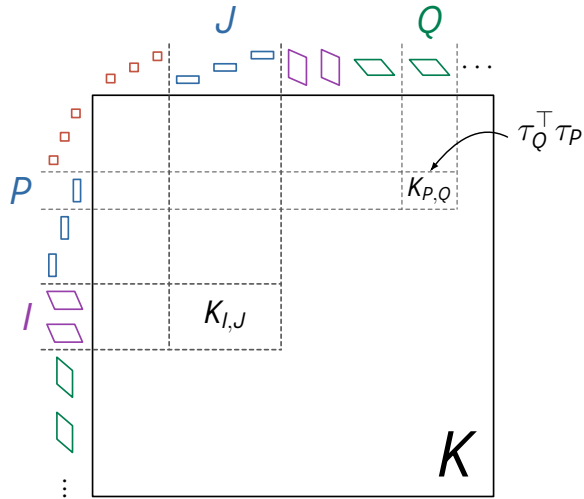
Structure of $K = \tau_M^\top \tau_M - \mathrm{Id}$

New goal:

Show $\mathbb{E}_\sigma[\|K_{I,J}\|_{\mathrm{op}}] < 4^{-D}$

Idea 2:

1. Combine plane blocks $K_{P,Q}$ into direction blocks $K_{I,J}$.
2. $\mathbb{E}_\sigma[\|K_{I,J}\|_{\mathrm{op}}] = O(1)$
   - Hard!
3. $\|K\|_{\mathrm{op}} \leq \sum_{I,J} \|K_{I,J}\|_{\mathrm{op}}$
4. Only 4^D pairs $I, J \subseteq [D]$!



Bounding $\left\|K_{I,J}\right\|_{\mathbf{op}}$

Goal: Show $\mathbb{E}_{\sigma}[\left\|K_{I,J}\right\|_{\mathsf{op}}] < 4^{-D}$

Bounding $\left\|K_{I,J}\right\|_{\mathbf{op}}$

Goal: Show $\mathbb{E}_\sigma[\left\|K_{I,J}\right\|_{\mathrm{op}}] < 4^{-D}$

$$K_{I,J} = \sum_{\varnothing \neq E \subseteq (I \cup J)^c} K^E_{I,J},$$

and $\left\|K_{I,J}\right\|_{\mathrm{op}} \leq \sum_{\varnothing \neq E \subseteq (I \cup J)^c} \left\|K^E_{I,J}\right\|_{\mathrm{op}}$.

Bounding $\left\|K_{I,J}\right\|_{\mathbf{op}}$

Goal: Show $\mathbb{E}_\sigma[\left\|K_{I,J}\right\|_{\mathrm{op}}] < 4^{-D}$

$$K_{I,J} = \sum_{\varnothing \neq E \subseteq (I \cup J)^c} K^E_{I,J},$$

and $\left\|K_{I,J}\right\|_{\mathrm{op}} \leq \sum_{\varnothing \neq E \subseteq (I \cup J)^c} \left\|K^E_{I,J}\right\|_{\mathrm{op}}$.
At most 2^D **possible** E, so **suffices to show**

$$\mathop{\mathbb{E}}_{\sigma}[\left\|K^E_{I,J}\right\|_{\mathrm{op}}] < 8^{-D}.$$

Bounding $\left\|K^E_{I,J}\right\|_{\mathsf{op}}$ with bipartite walks

Goal: Show $\mathbb{E}_\sigma[\left\|K^E_{I,J}\right\|_{\mathsf{op}}] < 8^{-D}$

For $I \subseteq [D]$ define ***anchor set*** $\Omega_I(M) = \{a \in [n]^{I^c} : \mathcal{P}(I, a) \subseteq M\}$

Bounding $\left\|K^E_{I,J}\right\|_{\text{op}}$ with bipartite walks

Goal: Show $\mathbb{E}_\sigma[\left\|K^E_{I,J}\right\|_{\text{op}}] < 8^{-D}$

For $I \subseteq [D]$ define ***anchor set*** $\Omega_I(M) = \{a \in [n]^{I^c} : \mathcal{P}(I,a) \subseteq M\}$

$$\left\|K^E_{I,J}\right\|^m_{\text{op}} \lesssim \sum_{\substack{x_1,\dots,x_m \in \Omega_I(M) \\ y_1,\dots,y_m \in \Omega_J(M)}} \sum_{\substack{r_j \in [k_j]^{2m} \\ j \in [|E|]}} \left(\prod_{j=1}^{|E|} k_j^{-2m}\right) \left(\prod_{j=1}^{|E|} \Phi_j(x,y,r_j)\right)$$

Bounding $\left\|K^E_{I,J}\right\|_{\text{op}}$ with bipartite walks

Goal: Show $\mathbb{E}_\sigma[\left\|K^E_{I,J}\right\|_{\text{op}}] < 8^{-D}$

For $I \subseteq [D]$ define ***anchor set*** $\Omega_I(M) = \{a \in [n]^{I^c} : \mathcal{P}(I, a) \subseteq M\}$

$$\left\|K^E_{I,J}\right\|^m_{\text{op}} \lesssim \sum_{\substack{x_1,\dots,x_m \in \Omega_I(M) \\ y_1,\dots,y_m \in \Omega_J(M)}} \sum_{\substack{r_j \in [k_j]^{2m} \\ j \in [|E|]}} \left(\prod_{j=1}^{|E|} k_j^{-2m}\right) \left(\prod_{j=1}^{|E|} \Phi_j(x, y, r_j)\right)$$

and ***sign monomials*** Φ_j

$$\Phi_j(x, y, r_j) = \prod_{t=1}^{m} \left(\sigma^{(j)}_{r_{j,2t-1}, x_{t,j}} \sigma^{(j)}_{r_{j,2t-1}, y_{t,j}} \sigma^{(j)}_{r_{j,2t}, y_{t,j}} \sigma^{(j)}_{r_{j,2t}, x_{t+1,j}} \mathbf{1}\{x_{t,j} \neq y_{t,j} \text{ and } y_{t,j} \neq x_{t+1,j}\}\right)$$

Bounding $\left\|K^E_{I,J}\right\|_{\text{op}}$ with bipartite walks

Goal: Show $\mathbb{E}_\sigma[\left\|K^E_{I,J}\right\|_{\text{op}}] < 8^{-D}$

For $I \subseteq [D]$ define ***anchor set*** $\Omega_I(M) = \{a \in [n]^{I^c} : \mathcal{P}(I, a) \subseteq M\}$

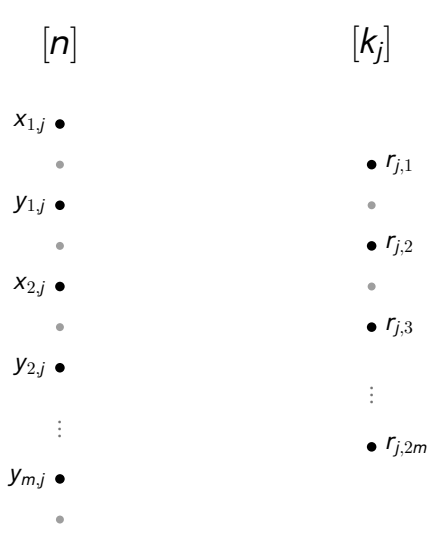
$$\left\|K^E_{I,J}\right\|^m_{\text{op}} \lesssim \sum_{\substack{x_1,\dots,x_m \in \Omega_I(M) \\ y_1,\dots,y_m \in \Omega_J(M)}} \sum_{\substack{r_j \in [k_j]^{2m} \\ j \in [|E|]}} \left(\prod_{j=1}^{|E|} k_j^{-2m}\right) \left(\prod_{j=1}^{|E|} \Phi_j(x, y, r_j)\right)$$

and ***sign monomials*** Φ_j

$$\Phi_j(x, y, r_j) = \prod_{t=1}^{m} \left(\sigma^{(j)}_{r_{j,2t-1}, x_{t,j}} \sigma^{(j)}_{r_{j,2t-1}, y_{t,j}} \sigma^{(j)}_{r_{j,2t}, y_{t,j}} \sigma^{(j)}_{r_{j,2t}, x_{t+1,j}} \mathbf{1}\{x_{t,j} \neq y_{t,j} \text{ and } y_{t,j} \neq x_{t+1,j}\}\right)$$

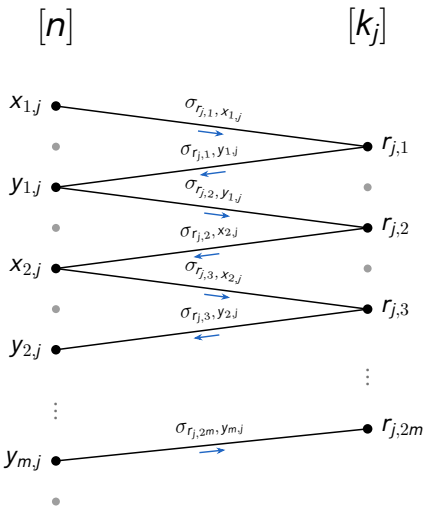
This is hard to interpret...

Bounding $\left\| K^E_{I,J} \right\|_{\mathbf{op}}$ with bipartite walks



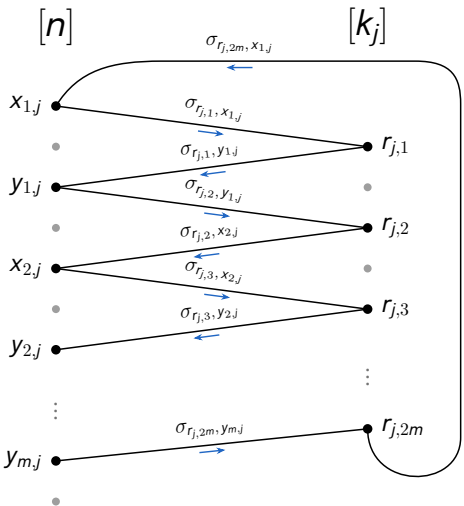
- Each vertex represents an index

Bounding $\left\| K^E_{I,J} \right\|_{\mathbf{op}}$ with bipartite walks



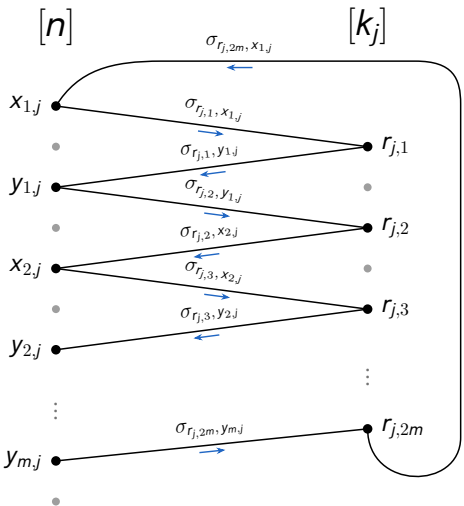
- Each vertex represents an index
- Each edge represents a sign

Bounding $\left\| K^E_{I,J} \right\|_{\text{op}}$ with bipartite walks



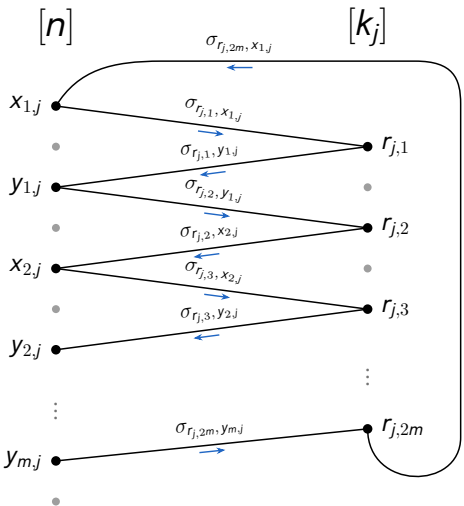
- Each vertex represents an index
- Each edge represents a sign
- The walk is closed

Bounding $\left\|K^E_{I,J}\right\|_{\text{op}}$ with bipartite walks



- Each vertex represents an index
- Each edge represents a sign
- The walk is closed
- $\mathbb{E}$ of prod of signs $= 1$ iff signs have **even multiplicity**

Bounding $\left\|K^E_{I,J}\right\|_{\text{op}}$ with bipartite walks

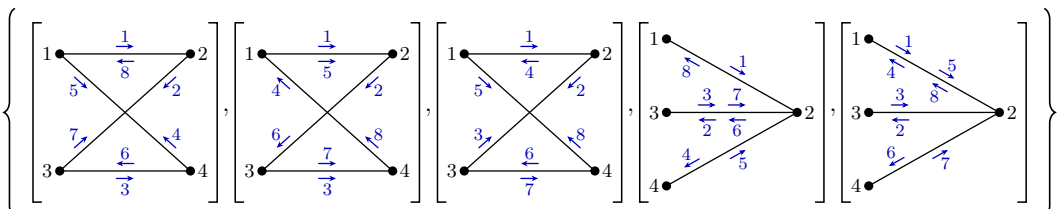


- Each vertex represents an index
- Each edge represents a sign
- The walk is closed
- $\mathbb{E}$ of prod of signs $= 1$ iff signs have **even multiplicity**
- Bound $\#$ **closed walks with even traversals**

Bounding even traversal closed walks

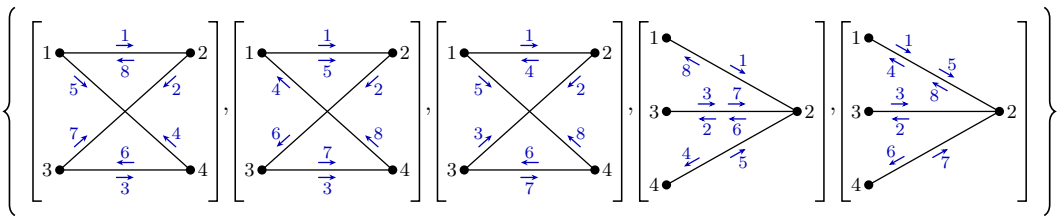
Bounding even traversal closed walks

- Group bipartite walks into ***equivalence classes*** by shape of walk.



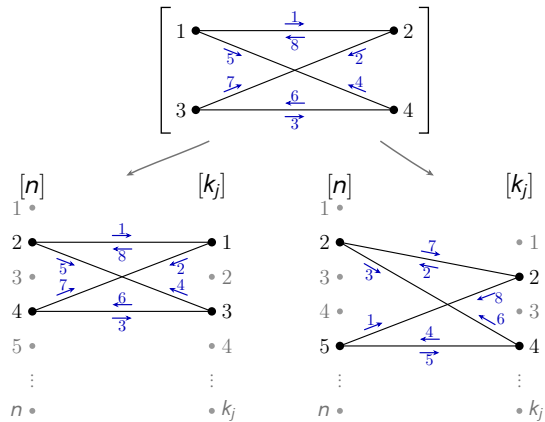
Bounding even traversal closed walks

- Group bipartite walks into ***equivalence classes*** by shape of walk.
- Bound number of equivalence classes by [Wig'55, FK'81; AZ'06].

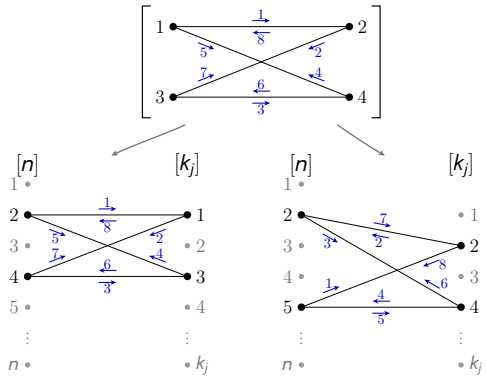


Bounding even traversal closed walks

- Group bipartite walks into ***equivalence classes*** by shape of walk.
- Bound number of equivalence classes by [Wig'55, FK'81; AZ'06].
- Bound size of each equivalence class using ε-closedness of M.



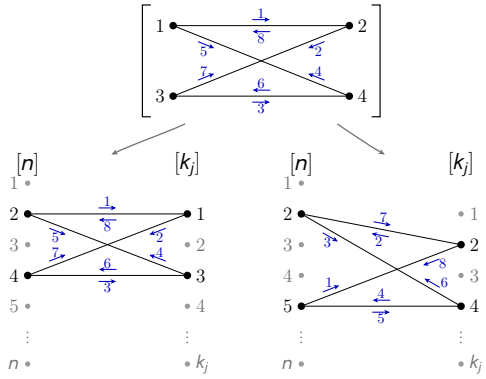
Bounding the size of equivalence classes



Bounding the size of equivalence classes

Need to choose:

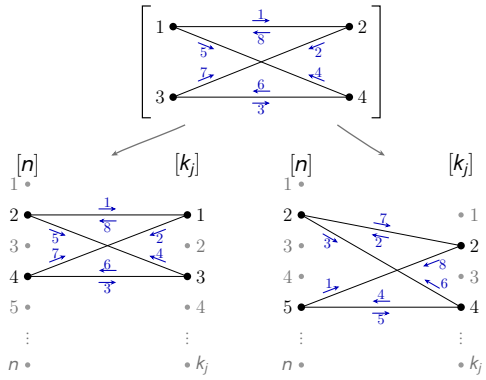
- $x_1, \ldots, x_m \in \Omega_I(M); y_1, \ldots, y_m \in \Omega_J(M)$



Bounding the size of equivalence classes

Need to choose:

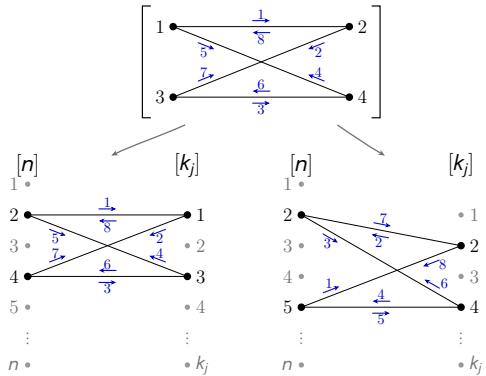
- $x_1, \ldots, x_m \in \Omega_I(M); y_1, \ldots, y_m \in \Omega_J(M)$
- $r_j \in [k_j]^{2m}$ for $j \in [|E|]$



Bounding the size of equivalence classes

Need to choose:

- $x_1, \ldots, x_m \in \Omega_I(M); y_1, \ldots, y_m \in \Omega_J(M)$
- $r_j \in [k_j]^{2m}$ for $j \in [|E|]$
- S.t. walk of $\Phi_j(x, y, r_j)$ has given shape

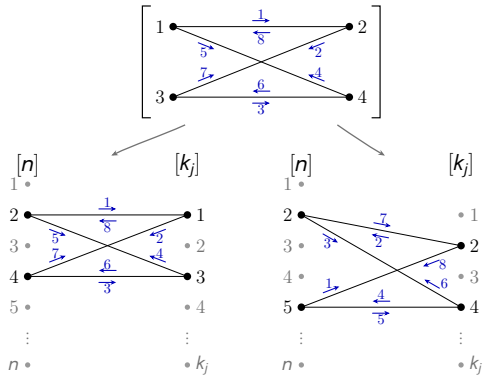


Bounding the size of equivalence classes

Need to choose:

- $x_1, \ldots, x_m \in \Omega_I(M); y_1, \ldots, y_m \in \Omega_J(M)$
- $r_j \in [k_j]^{2m}$ for $j \in [|E|]$
- S.t. walk of $\Phi_j(x, y, r_j)$ has given shape

To bound number choices:



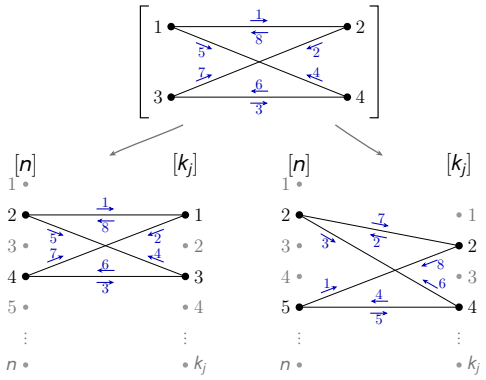
Bounding the size of equivalence classes

Need to choose:

- $x_1, \ldots, x_m \in \Omega_I(M); y_1, \ldots, y_m \in \Omega_J(M)$
- $r_j \in [k_j]^{2m}$ for $j \in [|E|]$
- S.t. walk of $\Phi_j(x, y, r_j)$ has given shape

To bound number choices:

- Let R be # unique right vertices in walk



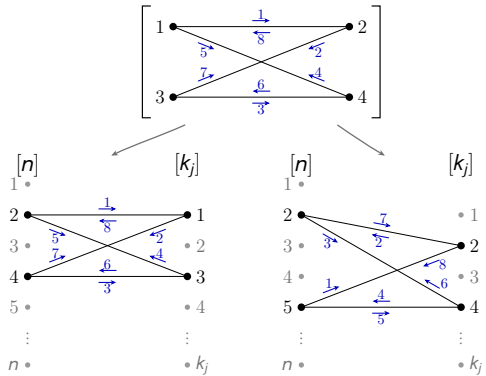
Bounding the size of equivalence classes

Need to choose:

- $x_1, \ldots, x_m \in \Omega_I(M); y_1, \ldots, y_m \in \Omega_J(M)$
- $r_j \in [k_j]^{2m}$ for $j \in [|E|]$
- S.t. walk of $\Phi_j(x, y, r_j)$ has given shape

To bound number choices:

- Let R be # unique right vertices in walk
- Let L be # unique left vertices in walk



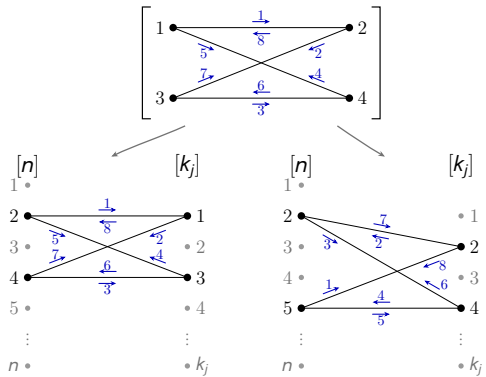
Bounding the size of equivalence classes

Need to choose:

- $x_1, \ldots, x_m \in \Omega_I(M); y_1, \ldots, y_m \in \Omega_J(M)$
- $r_j \in [k_j]^{2m}$ for $j \in [|E|]$
- S.t. walk of $\Phi_j(x, y, r_j)$ has given shape

To bound number choices:

- Let R be # unique right vertices in walk
- Let L be # unique left vertices in walk
- Take any k_j^{R} possible r_j



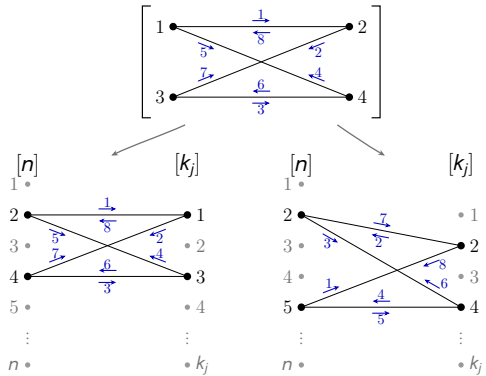
Bounding the size of equivalence classes

Need to choose:

- $x_1, \ldots, x_m \in \Omega_I(M); y_1, \ldots, y_m \in \Omega_J(M)$
- $r_j \in [k_j]^{2m}$ for $j \in [|E|]$
- S.t. walk of $\Phi_j(x, y, r_j)$ has given shape

To bound number choices:

- Let R be # unique right vertices in walk
- Let L be # unique left vertices in walk
- Take any k_j^{R} possible r_j
- Use M is ε-closed and shape of walk to get only $n^{\mathsf{L}}\varepsilon^{\mathsf{L}/|E|}$ choices of x and y



Part 4: Future directions

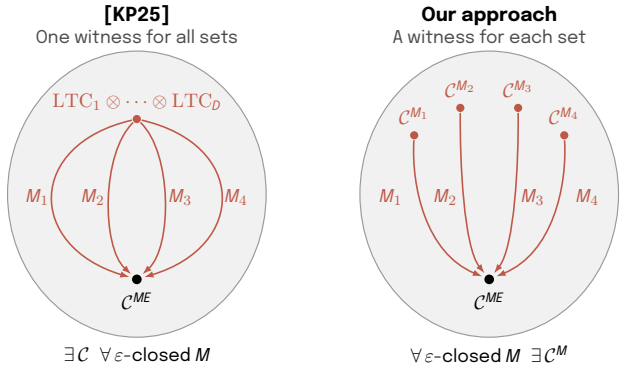
Future directions

Future directions

- Extend techniques to other base graphs (e.g., simplicial complexes)
  - Shown coboundary expansion of HDX $\iff$ ε-closed extendable

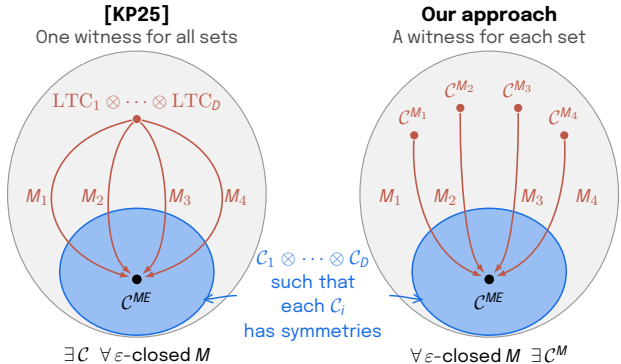
Future directions

- Extend techniques to other base graphs (e.g., simplicial complexes)
- Obtain more symmetries of the gadget codes (beyond [RSV'19])



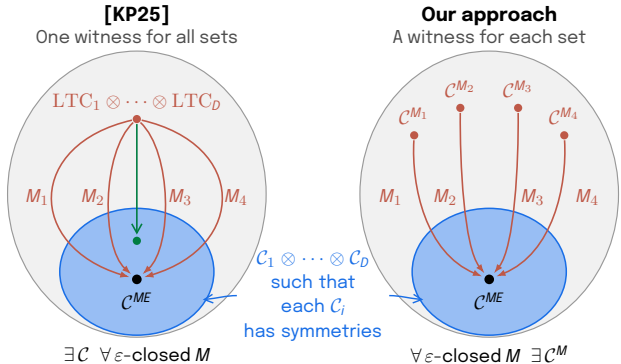
Future directions

- Extend techniques to other base graphs (e.g., simplicial complexes)
- Obtain more symmetries of the gadget codes (beyond [RSV'19])



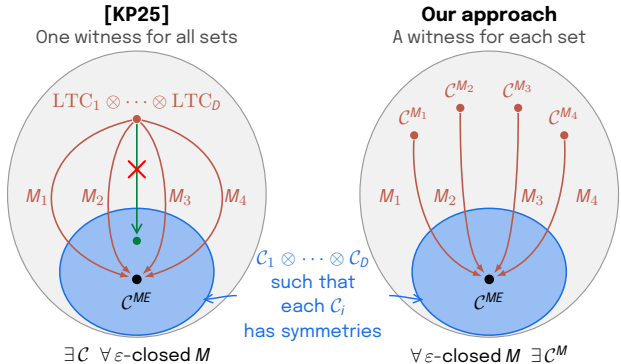
Future directions

- Extend techniques to other base graphs (e.g., simplicial complexes)
- Obtain more symmetries of the gadget codes (beyond [RSV'19])



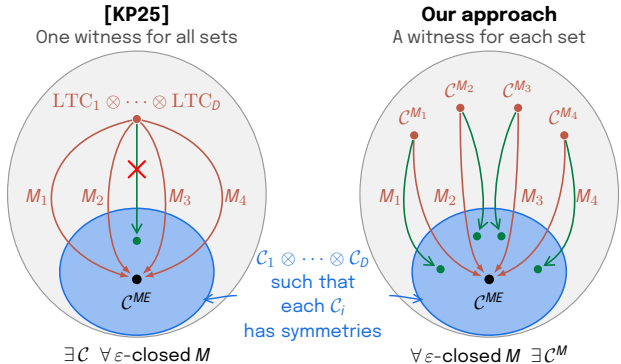
Future directions

- Extend techniques to other base graphs (e.g., simplicial complexes)
- Obtain more symmetries of the gadget codes (beyond [RSV'19])



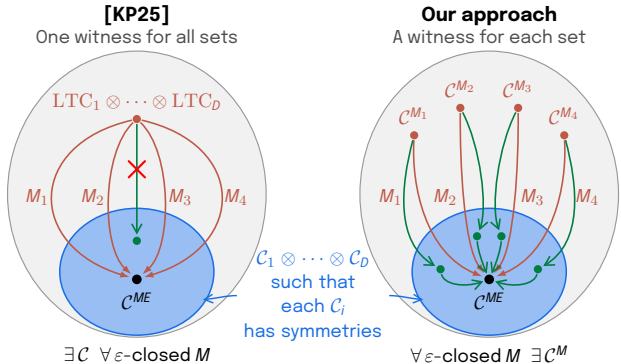
Future directions

- Extend techniques to other base graphs (e.g., simplicial complexes)
- Obtain more symmetries of the gadget codes (beyond [RSV'19])



Future directions

- Extend techniques to other base graphs (e.g., simplicial complexes)
- Obtain more symmetries of the gadget codes (beyond [RSV'19])



Future directions

- Extend techniques to other base graphs (e.g., simplicial complexes)
- Obtain more symmetries of the gadget codes (beyond [RSV'19])
- Reduce field characteristic from $O(2^{n^D} n^D \log n)$ to 2

Future directions

- Extend techniques to other base graphs (e.g., simplicial complexes)
- Obtain more symmetries of the gadget codes (beyond [RSV'19])
- Reduce field characteristic from $O(2^{n^D} n^D \log n)$ to 2

Conjecture (Generalized Chebotarev's theorem)

For a constant $D \in \mathbb{N}$, there exist constants $\varepsilon > 0$ and $\varepsilon' \in \left[\varepsilon^{1/D}, \frac{1}{2^D}\right)$, such that for any large enough prime k, the following is true: Let $\omega = e^{2\pi i/k}$ be a primitive k-th root of unity and $F \in \mathbb{C}^{k\times k}$ be the DFT matrix, so $F_{r,i} = \omega^{ri}$ for $r, i \in \mathbb{Z}/(k)$. Define its D-wise tensor $\Phi = F^{\otimes D} \in \mathbb{C}^{k^D \times k^D}$, so

$$\Phi_{\boldsymbol{r},\boldsymbol{i}} = (F_{:,i_1} \otimes F_{:,i_2} \otimes \cdots \otimes F_{:,i_D})_{\boldsymbol{r}} = \omega^{\sum_{j=1}^{D} r_j i_j}$$

for $\boldsymbol{i}, \boldsymbol{r} \in (\mathbb{Z}/(k))^D$. Let $M \subseteq (\mathbb{Z}/(k))^D$ be ε-sparse. Then there exist sets $A_1, A_2, \ldots, A_D \subseteq \mathbb{Z}/(k)$ such that $|A_i| \le \varepsilon' k$ for all i and $\Phi_{A_1\times A_2\times\cdots\times A_D,M}$ has rank $|M|$ (full column rank).

Thank you!

