Expanders, Extractors, Condensers

and Other Mysteries

Noam Ringach, 5/2/25

Randomness in Computation

Randomness in Computation

- Randomized algorithms are everywhere!

Randomness in Computation

- Randomized algorithms are everywhere!
- Many use randomness to sample a random object (e.g., graph, function, etc…) that has a "nice" property with 99% probability.

Randomness in Computation

- Randomized algorithms are everywhere!
- Many use randomness to sample a random object (e.g., graph, function, etc…) that has a "nice" property with 99% probability.
- **BUT** perfect randomness doesn't exist in the real world!

Randomness in Computation

- Randomized algorithms are everywhere!
- Many use randomness to sample a random object (e.g., graph, function, etc…) that has a "nice" property with 99% probability.
- **BUT** perfect randomness doesn't exist in the real world!
- Can get around this by explicitly constructing objects that look "pseudorandom" and have these nice properties.

Pseudorandomness

Pseudorandomness

Existence

Show that a random object (e.g., graphs, functions, …) has very nice properties via the probabilistic method (usually easy).

Pseudorandomness

Existence

Show that a random object (e.g., graphs, functions, …) has very nice properties via the probabilistic method (usually easy).

Explicit construction

Explicitly (in polynomial time) construct a deterministic object with those properties (HARD).

Part 0: Introduction to Expanders

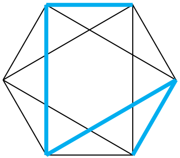
Types of Expanders

Goal

Have similar connectivity to a complete graph while having low degree (sparse).

Types of Expanders

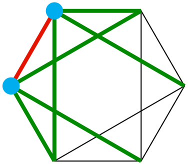
Spectral



Random walks mix well. Adjacency matrix has $\lambda_2 \leq 2\sqrt{D-1}$

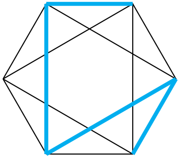
Types of Expanders

Edge



Large fraction of edges from a set leave the set.

Spectral

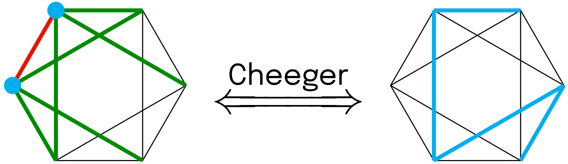


Random walks mix well. Adjacency matrix has $\lambda_2 \leq 2\sqrt{D-1}$

Types of Expanders

Edge

Spectral

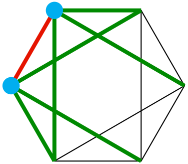


Large fraction of edges from a set leave the set.

Random walks mix well. Adjacency matrix has $\lambda_2 \leq 2\sqrt{D-1}$

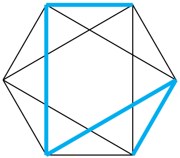
Types of Expanders

Edge



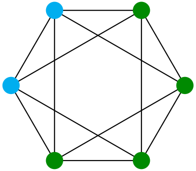
Large fraction of edges from a set leave the set.

Spectral



Random walks mix well. Adjacency matrix has $\lambda_2 \leq 2\sqrt{D-1}$

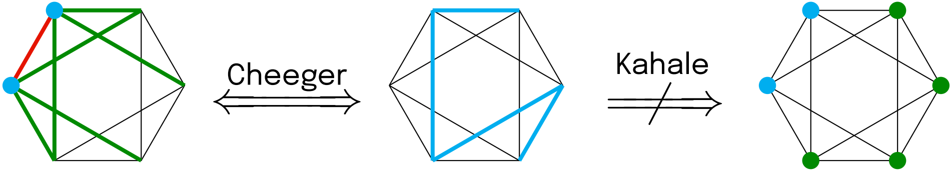
Vertex



Small sets have almost as many neighbors as possible.

Types of Expanders

Edge | Spectral | Vertex



Edge: Large fraction of edges from a set leave the set.

Spectral: Random walks mix well. Adjacency matrix has $\lambda_2 \leq 2\sqrt{D-1}$

Vertex: Small sets have almost as many neighbors as possible.

Vertex Expanders

Vertex Expanders

Vertex Expander

- A D-regular graph $G = (V, E)$ is a *(K, ε)-expander* if for every set $S \subseteq V$ of size at most K, the neighborhood $\Gamma(S)$ has size at least $(1 - \varepsilon) \cdot D \cdot |S|$.

Vertex Expanders

Vertex Expander

- A D-regular graph $G = (V, E)$ is a *(K, ε)-expander* if for every set $S \subseteq V$ of size at most K, the neighborhood $\Gamma(S)$ has size at least $(1 - \varepsilon) \cdot D \cdot |S|$.
- When $\varepsilon \approx 0.01$, we call G a *lossless expander*.

Vertex Expanders

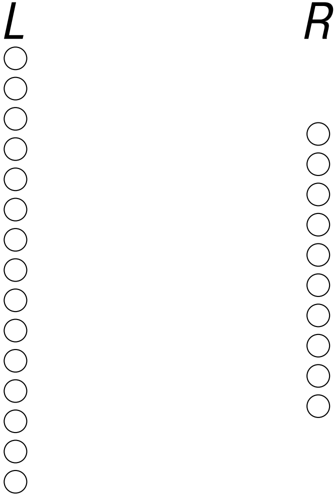
Vertex Expander

- A D-regular graph $G = (V, E)$ is a *(K, ε)-expander* if for every set $S \subseteq V$ of size at most K, the neighborhood $\Gamma(S)$ has size at least $(1 - \varepsilon) \cdot D \cdot |S|$.
- When $\varepsilon \approx 0.01$, we call G a *lossless expander*.

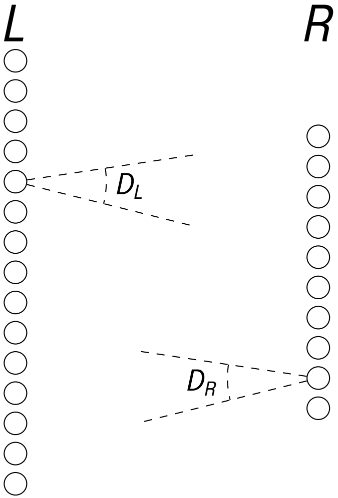
Theorem (Kahale'95)

There exist Ramanujan graphs (optimal spectral expanders) that are only $(K = \Omega(|V|), \varepsilon > 1/2)$-vertex expanders.

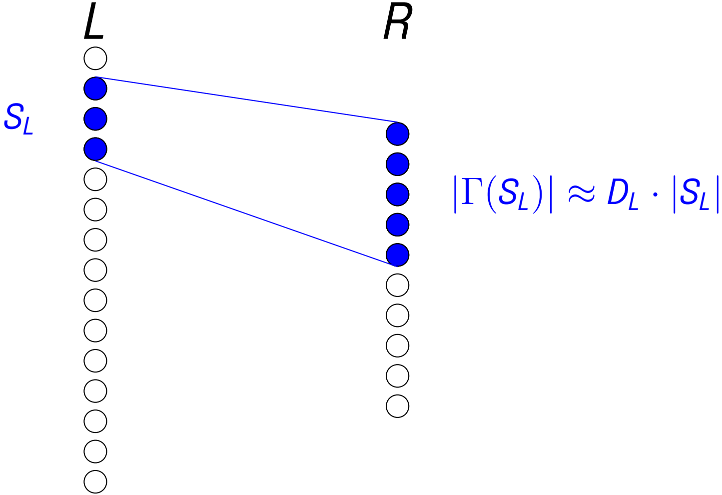
Vertex Expanders



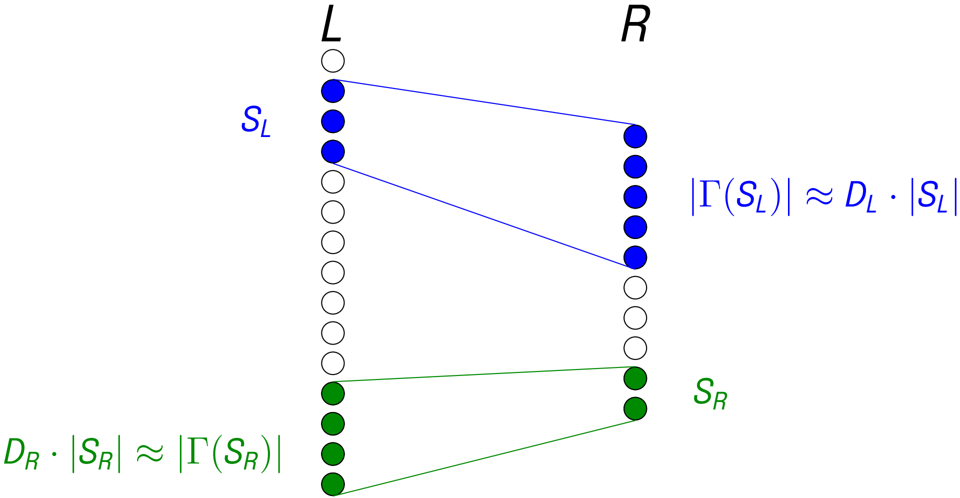
Vertex Expanders



Vertex Expanders



Vertex Expanders



Vertex Expanders

Bipartite Vertex Expander

Vertex Expanders

Bipartite Vertex Expander

- A (D_L, D_R)-biregular graph $G = (L \sqcup R, E)$ is a *one-sided (K_L, ε_L)-lossless expander* if for all $S \subseteq L$ s.t. $|S| \leq K_L$ then $|\Gamma(S)| \geq (1 - \varepsilon_L) \cdot D_L \cdot |S|$.

Vertex Expanders

Bipartite Vertex Expander

- A (D_L, D_R)-biregular graph $G = (L \sqcup R, E)$ is a *one-sided (K_L, ε_L)-lossless expander* if for all $S \subseteq L$ s.t. $|S| \leq K_L$ then $|\Gamma(S)| \geq (1 - \varepsilon_L) \cdot D_L \cdot |S|$.
- G is a *two-sided $(K_L, \varepsilon_L, K_R, \varepsilon_R)$-lossless expander* if, moreover, for all $S \subseteq R$ s.t. $|S| \leq K_R$ then $|\Gamma(S)| \geq (1 - \varepsilon_R) \cdot D_R \cdot |S|$.

Vertex Expanders

Bipartite Vertex Expander

- A (D_L, D_R)-biregular graph $G = (L \sqcup R, E)$ is a *one-sided (K_L, ε_L)-lossless expander* if for all $S \subseteq L$ s.t. $|S| \leq K_L$ then $|\Gamma(S)| \geq (1 - \varepsilon_L) \cdot D_L \cdot |S|$.
- G is a *two-sided $(K_L, \varepsilon_L, K_R, \varepsilon_R)$-lossless expander* if, moreover, for all $S \subseteq R$ s.t. $|S| \leq K_R$ then $|\Gamma(S)| \geq (1 - \varepsilon_R) \cdot D_R \cdot |S|$.

With $N = |L|$ and $M = |R|$, we can view G instead as its neighborhood function:

$$\Gamma : [N] \times [D_L] \to [M]$$

Vertex Expanders

Bipartite Vertex Expander

- A (D_L, D_R)-biregular graph $G = (L \sqcup R, E)$ is a *one-sided (K_L, ε_L)-lossless expander* if for all $S \subseteq L$ s.t. $|S| \leq K_L$ then $|\Gamma(S)| \geq (1 - \varepsilon_L) \cdot D_L \cdot |S|$.
- G is a *two-sided $(K_L, \varepsilon_L, K_R, \varepsilon_R)$-lossless expander* if, moreover, for all $S \subseteq R$ s.t. $|S| \leq K_R$ then $|\Gamma(S)| \geq (1 - \varepsilon_R) \cdot D_R \cdot |S|$.

Balanced and Unbalanced Bipartite Expanders

Vertex Expanders

Bipartite Vertex Expander

- A (D_L, D_R)-biregular graph $G = (L \sqcup R, E)$ is a *one-sided (K_L, ε_L)-lossless expander* if for all $S \subseteq L$ s.t. $|S| \leq K_L$ then $|\Gamma(S)| \geq (1 - \varepsilon_L) \cdot D_L \cdot |S|$.
- G is a *two-sided $(K_L, \varepsilon_L, K_R, \varepsilon_R)$-lossless expander* if, moreover, for all $S \subseteq R$ s.t. $|S| \leq K_R$ then $|\Gamma(S)| \geq (1 - \varepsilon_R) \cdot D_R \cdot |S|$.

Balanced and Unbalanced Bipartite Expanders

- If $M = O(N)$, we say G is *balanced*.

Vertex Expanders

Bipartite Vertex Expander

- A (D_L, D_R)-biregular graph $G = (L \sqcup R, E)$ is a *one-sided (K_L, ε_L)-lossless expander* if for all $S \subseteq L$ s.t. $|S| \leq K_L$ then $|\Gamma(S)| \geq (1 - \varepsilon_L) \cdot D_L \cdot |S|$.
- G is a *two-sided $(K_L, \varepsilon_L, K_R, \varepsilon_R)$-lossless expander* if, moreover, for all $S \subseteq R$ s.t. $|S| \leq K_R$ then $|\Gamma(S)| \geq (1 - \varepsilon_R) \cdot D_R \cdot |S|$.

Balanced and Unbalanced Bipartite Expanders

- If $M = O(N)$, we say G is *balanced*.
- If $M = O(N^\delta)$, for some $0 < \delta < 1$, we say G is *unbalanced*.

Bipartite Vertex Expanders are Useful

Unbalanced

- Condenser and extractor constructions [Ta-Shma, Umans, Zuckerman'01;Ta-Shma, Umans'06; Guruswami, Umans, Vadhan'09; Dvir, Kopparty, Saraf, Sudan'13]
- Derandomization [Doron, Tell'23]
- Probabilistic data structures [Upfal, Wigderson'87; Buhrman, Miltersen, Radhakrishnan, Venkatesh'02]
- Complexity lower bounds [Ben-Sasson, Wigderson'01; …; Alekhnovich, Ben-Sasson, Razborov, Wigderson'04]

Bipartite Vertex Expanders are Useful

Balanced

- Classical codes [Sipser, Spielman'96; Luby, Mitzenmacher, Shokrollahi, Spielman'01; Tanner'03]
- Quantum codes* [Lin, Hsieh'22]
- Distributed routing algorithms* [Pele, Upfal'89; …; Hoory, Magen, Pitassi'06]

*Uses two-sided expansion

An Abridged History of Vertex Expanders

D_L-regular $G = ([N] \sqcup [M], E)$ with max expanding set size K_L and K_R and factor ε

Reference(s)	M	$D_L(\downarrow)$	$K_L(\uparrow)$	$K_R(\uparrow)$	$\varepsilon(\downarrow)$

An Abridged History of Vertex Expanders

D_L-regular $G = ([N] \sqcup [M], E)$ with max expanding set size K_L and K_R and factor ε

Reference(s)	M	$D_L(\downarrow)$	$K_L(\uparrow)$	$K_R(\uparrow)$	$\varepsilon(\downarrow)$
Existential	$O(N)$	$O(1)$	$O(N)$	$O(M)$	0.01

An Abridged History of Vertex Expanders

D_L-regular $G = ([N] \sqcup [M], E)$ with max expanding set size K_L and K_R and factor ε

Reference(s)	M	$D_L (\downarrow)$	$K_L (\uparrow)$	$K_R (\uparrow)$	$\varepsilon (\downarrow)$
Existential	$O(N)$	$O(1)$	$O(N)$	$O(M)$	0.01
CRVW'02; CRT'23; Gol'23	$O(N)$	$O(1)$	$O(N)$	$\varnothing$	0.01

An Abridged History of Vertex Expanders

D_L-regular $G = ([N] \sqcup [M], E)$ with max expanding set size K_L and K_R and factor ε

Reference(s)	M	$D_L(\downarrow)$	$K_L(\uparrow)$	$K_R(\uparrow)$	$\varepsilon(\downarrow)$
Existential	$O(N)$	$O(1)$	$O(N)$	$O(M)$	0.01
CRVW'02; CRT'23; Gol'23	$O(N)$	$O(1)$	$O(N)$	$\varnothing$	0.01
HLMRZ'25	$O(N)$	$O(1)$	$O(N)$	$O(M)$	0.01

An Abridged History of Vertex Expanders

D_L-regular $G = ([N] \sqcup [M], E)$ with max expanding set size K_L and K_R and factor ε

Reference(s)	M	$D_L (\downarrow)$	$K_L (\uparrow)$	$K_R (\uparrow)$	$\varepsilon (\downarrow)$
Existential	$O(N)$	$O(1)$	$O(N)$	$O(M)$	0.01
CRVW'02; CRT'23; Gol'23	$O(N)$	$O(1)$	$O(N)$	$\varnothing$	0.01
HLMRZ'25	$O(N)$	$O(1)$	$O(N)$	$O(M)$	0.01
Existential	$O(N^{\delta})$	$O(\log(N))$	$O(N^{0.9\delta})$	$O(M)$	0.01

An Abridged History of Vertex Expanders

D_L-regular $G = ([N] \sqcup [M], E)$ with max expanding set size K_L and K_R and factor ε

Reference(s)	M	$D_L (\downarrow)$	$K_L (\uparrow)$	$K_R (\uparrow)$	$\varepsilon (\downarrow)$
Existential	$O(N)$	$O(1)$	$O(N)$	$O(M)$	0.01
CRVW'02; CRT'23; Gol'23	$O(N)$	$O(1)$	$O(N)$	$\varnothing$	0.01
HLMRZ'25	$O(N)$	$O(1)$	$O(N)$	$O(M)$	0.01
Existential	$O(N^{\delta})$	$O(\log(N))$	$O(N^{0.9\delta})$	$O(M)$	0.01
TUZ'01	$O(N^{\delta})$	$2^{O((\log \log N)^2)}$	$O(N^{0.9\delta})$	$\varnothing$	0.01

An Abridged History of Vertex Expanders

D_L-regular $G = ([N] \sqcup [M], E)$ with max expanding set size K_L and K_R and factor ε

Reference(s)	M	$D_L (\downarrow)$	$K_L (\uparrow)$	$K_R (\uparrow)$	$\varepsilon (\downarrow)$
Existential	$O(N)$	$O(1)$	$O(N)$	$O(M)$	0.01
CRVW'02; CRT'23; Gol'23	$O(N)$	$O(1)$	$O(N)$	$\varnothing$	0.01
HLMRZ'25	$O(N)$	$O(1)$	$O(N)$	$O(M)$	0.01
Existential	$O(N^\delta)$	$O(\log(N))$	$O(N^{0.9\delta})$	$O(M)$	0.01
TUZ'01	$O(N^\delta)$	$2^{O((\log\log N)^2)}$	$O(N^{0.9\delta})$	$\varnothing$	0.01
TU'06	$O(N^\delta)$	$2^{O((\log\log N)^{1.01})}$	$O(N^{0.9\delta})$	$\varnothing$	0.01

An Abridged History of Vertex Expanders

D_L-regular $G = ([N] \sqcup [M], E)$ with max expanding set size K_L and K_R and factor ε

Reference(s)	M	$D_L (\downarrow)$	$K_L (\uparrow)$	$K_R (\uparrow)$	$\varepsilon (\downarrow)$
Existential	$O(N)$	$O(1)$	$O(N)$	$O(M)$	0.01
CRVW'02; CRT'23; Gol'23	$O(N)$	$O(1)$	$O(N)$	$\varnothing$	0.01
HLMRZ'25	$O(N)$	$O(1)$	$O(N)$	$O(M)$	0.01
Existential	$O(N^\delta)$	$O(\log(N))$	$O(N^{0.9\delta})$	$O(M)$	0.01
TUZ'01	$O(N^\delta)$	$2^{O((\log\log N)^2)}$	$O(N^{0.9\delta})$	$\varnothing$	0.01
TU'06	$O(N^\delta)$	$2^{O((\log\log N)^{1.01})}$	$O(N^{0.9\delta})$	$\varnothing$	0.01
GUV'09, KT'22	$O(N^\delta)$	$\mathrm{polylog}(N)$	$O(N^{0.9\delta})$	$\varnothing$	0.01

An Abridged History of Vertex Expanders

D_L-regular $G = ([N] \sqcup [M], E)$ with max expanding set size K_L and K_R and factor ε

Reference(s)	M	$D_L (\downarrow)$	$K_L (\uparrow)$	$K_R (\uparrow)$	$\varepsilon (\downarrow)$
Existential	$O(N)$	$O(1)$	$O(N)$	$O(M)$	0.01
CRVW'02; CRT'23; Gol'23	$O(N)$	$O(1)$	$O(N)$	$\varnothing$	0.01
HLMRZ'25	$O(N)$	$O(1)$	$O(N)$	$O(M)$	0.01
Existential	$O(N^\delta)$	$O(\log(N))$	$O(N^{0.9\delta})$	$O(M)$	0.01
TUZ'01	$O(N^\delta)$	$2^{O((\log\log N)^2)}$	$O(N^{0.9\delta})$	$\varnothing$	0.01
TU'06	$O(N^\delta)$	$2^{O((\log\log N)^{1.01})}$	$O(N^{0.9\delta})$	$\varnothing$	0.01
GUV'09, KT'22	$O(N^\delta)$	$\mathrm{polylog}(N)$	$O(N^{0.9\delta})$	$\varnothing$	0.01
Us (on KT'22)	$O(N^\delta)$	$\mathrm{polylog}(N)$	$O(N^{0.9\delta})$	$O(\min(M, \frac{N}{M}))$	0.01

Part 1: Two-Sided Lossless Expanders in the Unbalanced Setting [CGRZ'24]

Part 1 Outline

- Main results
- Construction of the KT graph
- Right to left expansion
- Tightness
- Open Questions

Main Results

Theorem (CGRZ'24)

The KT graph is a right lossless expander. I.e., for infinitely many N and all constant $0 < \delta < 0.99$, there exists an explicit (D_L, D_R)-biregular two-sided $(K_L, \varepsilon_L = 0.01, K_R, \varepsilon_R = 0.01)$-lossless expander where

Main Results

Theorem (CGRZ'24)

The KT graph is a right lossless expander. I.e., for infinitely many N and all constant $0 < \delta < 0.99$*, there exists an explicit* (D_L, D_R)*-biregular two-sided* $(K_L, \varepsilon_L = 0.01, K_R, \varepsilon_R = 0.01)$*-lossless expander where*

- $D_L = \mathrm{polylog}(N)$

Main Results

Theorem (CGRZ'24)

The KT graph is a right lossless expander. I.e., for infinitely many N and all constant $0 < \delta < 0.99$, there exists an explicit (D_L, D_R)-biregular two-sided $(K_L, \varepsilon_L = 0.01, K_R, \varepsilon_R = 0.01)$-lossless expander where

- $D_L = \mathrm{polylog}(N)$
- $M \approx N^\delta$

Main Results

Theorem (CGRZ'24)

The KT graph is a right lossless expander. I.e., for infinitely many N and all constant $0 < \delta < 0.99$*, there exists an explicit* (D_L, D_R)*-biregular two-sided* $(K_L, \varepsilon_L = 0.01, K_R, \varepsilon_R = 0.01)$*-lossless expander where*

- $D_L = \mathrm{polylog}(N)$
- $M \approx N^{\delta}$
- $K_L = N^{0.99\delta}$ *(from KT'22)*

Main Results

Theorem (CGRZ'24)

The KT graph is a right lossless expander. I.e., for infinitely many N and all constant $0 < \delta < 0.99$, there exists an explicit (D_L, D_R)-biregular two-sided $(K_L, \varepsilon_L = 0.01, K_R, \varepsilon_R = 0.01)$-lossless expander where

- $D_L = \mathrm{polylog}(N)$
- $M \approx N^{\delta}$
- $K_L = N^{0.99\delta}$ (from KT'22)
- If $\delta \leq \frac{1}{2}$, then $K_R = O\left(\frac{M}{D_L}\right)$

Main Results

Theorem (CGRZ'24)

The KT graph is a right lossless expander. I.e., for infinitely many N and all constant $0 < \delta < 0.99$, there exists an explicit (D_L, D_R)-biregular two-sided $(K_L, \varepsilon_L = 0.01, K_R, \varepsilon_R = 0.01)$-lossless expander where

- $D_L = \mathrm{polylog}(N)$
- $M \approx N^{\delta}$
- $K_L = N^{0.99\delta}$ *(from KT'22)*
- *If* $\delta \leq \frac{1}{2}$, *then* $K_R = O\left(\frac{M}{D_L}\right)$
- *If* $\delta > \frac{1}{2}$, *then* $K_R = O\left(\frac{N}{MD_L}\right)$

Main Results

Theorem (CGRZ'24)

The KT graph is a right lossless expander. I.e., for infinitely many N and all constant $0 < \delta < 0.99$, *there exists an explicit* (D_L, D_R)*-biregular two-sided* $(K_L, \varepsilon_L = 0.01, K_R, \varepsilon_R = 0.01)$*-lossless expander where*

- $D_L = \mathrm{polylog}(N)$
- $M \approx N^\delta$
- $K_L = N^{0.99\delta}$ *(from KT'22)*
- *If* $\delta \le \frac{1}{2}$, *then* $K_R = O\left(\frac{M}{D_L}\right)$
- *If* $\delta > \frac{1}{2}$, *then* $K_R = O\left(\frac{N}{MD_L}\right)$

Remark

When $M \le \sqrt{N}$, have that $K_R = O(M/D_L)$ is optimal. Otherwise since $ND_L = MD_R$, for a subset $|S_R| = \omega(M/D_L)$ we would have $|\Gamma(S_R)| = \omega(M/D_L) \cdot D_R = \omega(N)$.

Main Results

Theorem (CGRZ'24)

The KT graph is a right lossless expander. I.e., for infinitely many N and all constant $0 < \delta < 0.99$, there exists an explicit (D_L, D_R)-biregular two-sided $(K_L, \varepsilon_L = 0.01, K_R, \varepsilon_R = 0.01)$-lossless expander where

- $D_L = \mathrm{polylog}(N)$
- $M \approx N^{\delta}$
- $K_L = N^{0.99\delta}$ (from KT'22)
- If $\delta \leq \frac{1}{2}$, then $K_R = O\left(\frac{M}{D_L}\right)$
- If $\delta > \frac{1}{2}$, then $K_R = O\left(\frac{N}{MD_L}\right)$

Theorem (CGRZ'24)

When $M > \sqrt{N}$, our construction cannot achieve K_R larger than $O\left(\frac{N}{MD_L}\right)$.

Part 1 Outline

- ~~Main results~~
- Construction of the KT graph
- Right to left expansion
- Tightness
- Open Questions

Construction of the KT Graph

Notation

For $n \in \mathbb{N}$ and a prime power q, define

- Polynomials of deg $< n$: $P_{<n} = \{f \in \mathbb{F}_q[x] \mid \deg(f) < n\}$
- Iterated derivative: $f^{(i)}(x) = \frac{\mathrm{d}^i}{\mathrm{d}x^i} f(x) \in \mathbb{F}_q[x]$

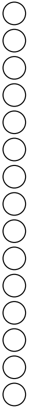
Construction of the KT Graph

Given $n, s, q \in \mathbb{N}$ such that $s = \delta n$ for $\delta < 1$ and prime $q > n$, construct:

Construction of the KT Graph

Given $n, s, q \in \mathbb{N}$ such that $s = \delta n$ for $\delta < 1$ and prime $q > n$, construct:

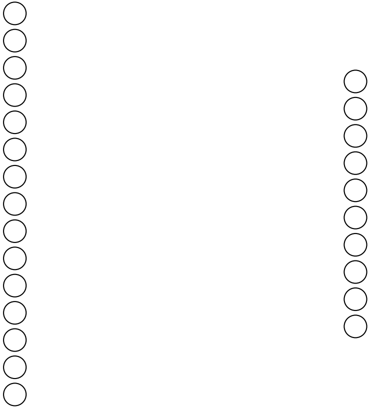
$$L = \mathbb{F}_q^n = P_{<n}$$



Construction of the KT Graph

Given $n, s, q \in \mathbb{N}$ such that $s = \delta n$ for $\delta < 1$ and prime $q > n$, construct:

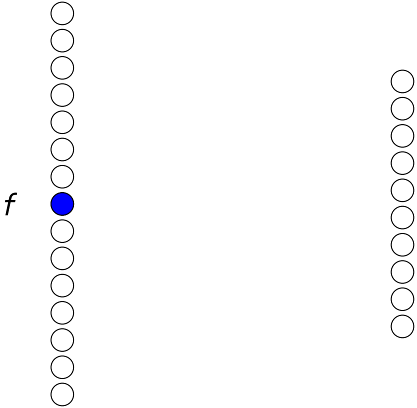
$$L = \mathbb{F}_q^n = P_{<n} \qquad R = \mathbb{F}_q^{s+2}$$



Construction of the KT Graph

Given $n, s, q \in \mathbb{N}$ such that $s = \delta n$ for $\delta < 1$ and prime $q > n$, construct:

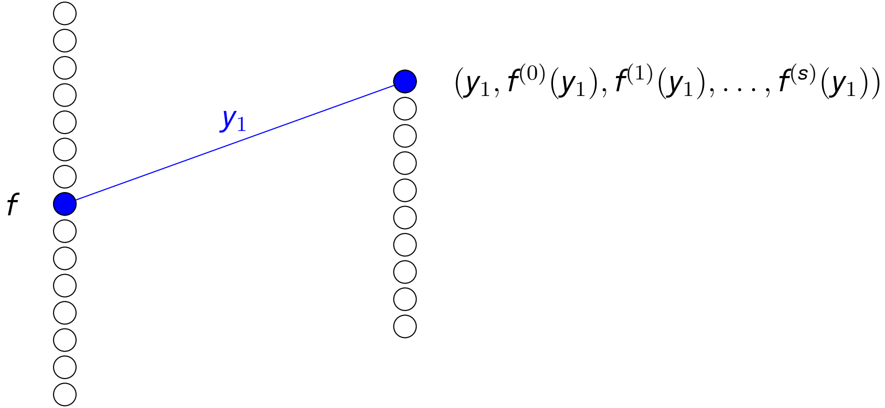
$$L = \mathbb{F}_q^n = P_{<n} \qquad R = \mathbb{F}_q^{s+2}$$



Construction of the KT Graph

Given $n, s, q \in \mathbb{N}$ such that $s = \delta n$ for $\delta < 1$ and prime $q > n$, construct:

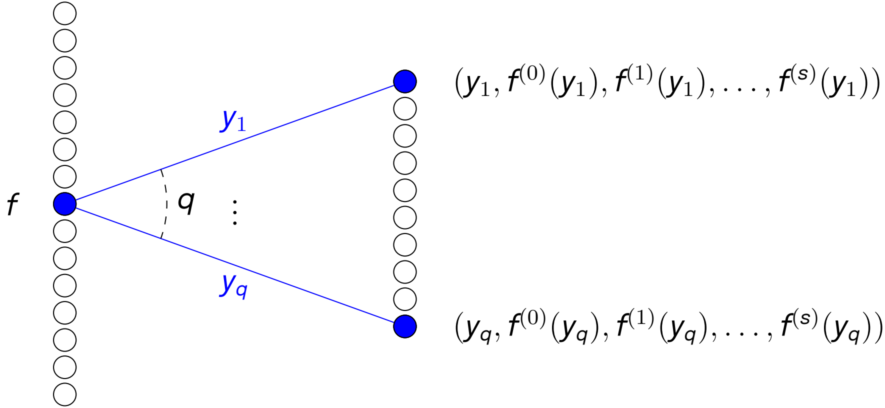
$$L = \mathbb{F}_q^n = P_{<n} \qquad R = \mathbb{F}_q^{s+2}$$



Construction of the KT Graph

Given $n, s, q \in \mathbb{N}$ such that $s = \delta n$ for $\delta < 1$ and prime $q > n$, construct:

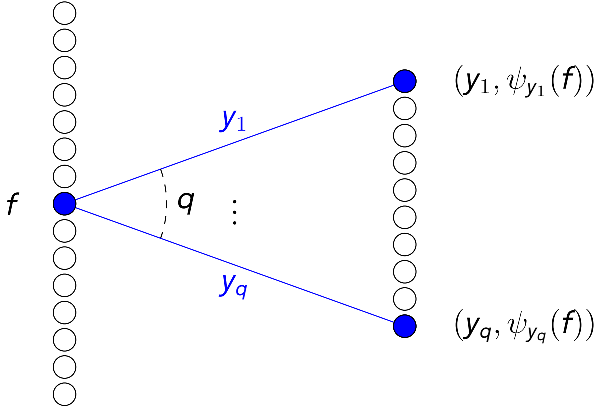
$$L = \mathbb{F}_q^n = P_{<n} \qquad R = \mathbb{F}_q^{s+2}$$



Construction of the KT Graph

Given $n, s, q \in \mathbb{N}$ such that $s = \delta n$ for $\delta < 1$ and prime $q > n$, construct:

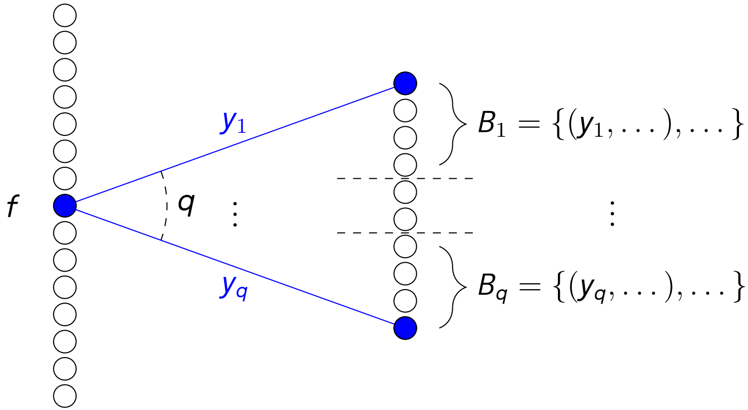
$$L = \mathbb{F}_q^n = P_{<n} \qquad R = \mathbb{F}_q^{s+2}$$



Construction of the KT Graph

Given $n, s, q \in \mathbb{N}$ such that $s = \delta n$ for $\delta < 1$ and prime $q > n$, construct:

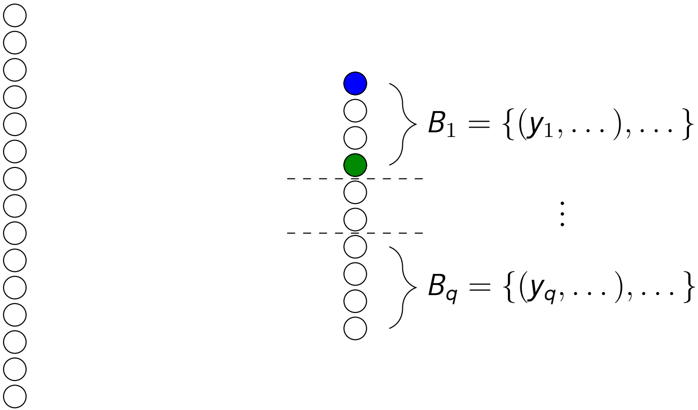
$$L = \mathbb{F}_q^n = P_{<n} \qquad R = \mathbb{F}_q^{s+2}$$



Construction of the KT Graph

Given $n, s, q \in \mathbb{N}$ such that $s = \delta n$ for $\delta < 1$ and prime $q > n$, construct:

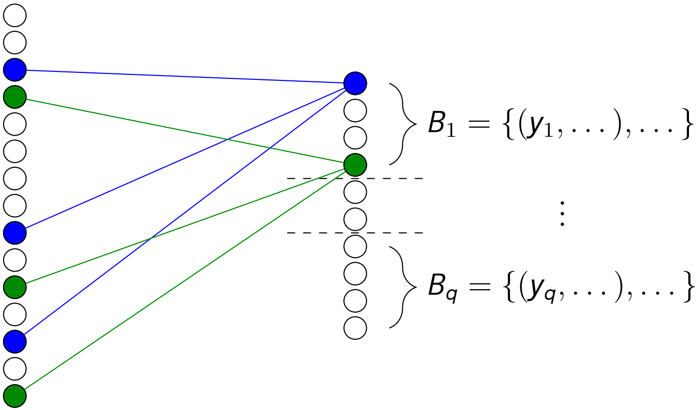
$$L = \mathbb{F}_q^n = P_{<n} \qquad R = \mathbb{F}_q^{s+2}$$



Construction of the KT Graph

Given $n, s, q \in \mathbb{N}$ such that $s = \delta n$ for $\delta < 1$ and prime $q > n$, construct:

$$L = \mathbb{F}_q^n = P_{<n} \qquad R = \mathbb{F}_q^{s+2}$$



Part 1 Outline

- ~~Main results~~
- ~~Construction of the KT graph~~
- Right to left expansion
- Tightness
- Open Questions

Right to Left Expansion

Right to Left Expansion

Theorem

If $n \geq s+1$, then G is a right (K_R, ε_R)-lossless expander with $K_R = \gamma q^{s+1}$ and $\varepsilon_R = \gamma \cdot q^{\max(2s+2-n,0)}$ where γ is arbitrary.

Right to Left Expansion

Theorem

If $n \geq s+1$, then G is a right (K_R, ε_R)-lossless expander with $K_R = \gamma q^{s+1}$ and $\varepsilon_R = \gamma \cdot q^{\max(2s+2-n,0)}$ where γ is arbitrary.

$$\underline{n > 2s+2}$$

$$\gamma = 0.01$$

Right to Left Expansion

Theorem

If $n \geq s + 1$, then G is a right (K_R, ε_R)-lossless expander with $K_R = \gamma q^{s+1}$ and $\varepsilon_R = \gamma \cdot q^{\max(2s+2-n,0)}$ where γ is arbitrary.

$$\underline{n > 2s + 2}$$

$$\gamma = 0.01$$

$$\varepsilon_R = 0.01$$

Right to Left Expansion

Theorem

If $n \geq s+1$, then G is a right (K_R, ε_R)-lossless expander with $K_R = \gamma q^{s+1}$ and $\varepsilon_R = \gamma \cdot q^{\max(2s+2-n,0)}$ where γ is arbitrary.

$$\underline{n > 2s+2}$$

$$\gamma = 0.01$$

$$\varepsilon_R = 0.01$$

$$K_R = 0.01 \cdot q^{s+1} = O\left(\frac{M}{D_L}\right)$$

Right to Left Expansion

Theorem

If $n \geq s+1$, then G is a right (K_R, ε_R)-lossless expander with $K_R = \gamma q^{s+1}$ and $\varepsilon_R = \gamma \cdot q^{\max(2s+2-n,0)}$ where γ is arbitrary.

$\underline{n > 2s+2}$

$\underline{n \leq 2s+2}$

$$\gamma = 0.01$$

$$\varepsilon_R = 0.01$$

$$K_R = 0.01 \cdot q^{s+1} = O\left(\frac{M}{D_L}\right)$$

Right to Left Expansion

Theorem

If $n \geq s+1$, then G is a right (K_R, ε_R)-lossless expander with $K_R = \gamma q^{s+1}$ and $\varepsilon_R = \gamma \cdot q^{\max(2s+2-n,0)}$ where γ is arbitrary.

<u>$n > 2s+2$</u>

$$\gamma = 0.01$$

$$\varepsilon_R = 0.01$$

$$K_R = 0.01 \cdot q^{s+1} = O\left(\frac{M}{D_L}\right)$$

<u>$n \leq 2s+2$</u>

$$\gamma = 0.01 \cdot q^{n-(2s+2)}$$

Right to Left Expansion

Theorem

If $n \geq s+1$, then G is a right (K_R, ε_R)-lossless expander with $K_R = \gamma q^{s+1}$ and $\varepsilon_R = \gamma \cdot q^{\max(2s+2-n,0)}$ where γ is arbitrary.

$\underline{n > 2s+2}$

$$\gamma = 0.01$$

$$\varepsilon_R = 0.01$$

$$K_R = 0.01 \cdot q^{s+1} = O\left(\frac{M}{D_L}\right)$$

$\underline{n \leq 2s+2}$

$$\gamma = 0.01 \cdot q^{n-(2s+2)}$$

$$\varepsilon_R = 0.01$$

Right to Left Expansion

Theorem

If $n \geq s+1$, then G is a right (K_R, ε_R)-lossless expander with $K_R = \gamma q^{s+1}$ and $\varepsilon_R = \gamma \cdot q^{\max(2s+2-n,0)}$ where γ is arbitrary.

$\underline{n > 2s+2}$

$$\gamma = 0.01$$
$$\varepsilon_R = 0.01$$
$$K_R = 0.01 \cdot q^{s+1} = O\left(\frac{M}{D_L}\right)$$

$\underline{n \leq 2s+2}$

$$\gamma = 0.01 \cdot q^{n-(2s+2)}$$
$$\varepsilon_R = 0.01$$
$$K_R = 0.01 \cdot q^{n-(2s+2)} q^{s+1}$$
$$= O\left(\frac{N}{MD_L}\right)$$

Right to Left Expansion

Theorem

If $n \geq s+1$, then G is a right (K_R, ε_R)-lossless expander with $K_R = \gamma q^{s+1}$ and $\varepsilon_R = \gamma \cdot q^{\max(2s+2-n,0)}$ where γ is arbitrary.

$n > 2s+2$

$$\gamma = 0.01$$
$$\varepsilon_R = 0.01$$
$$K_R = 0.01 \cdot q^{s+1} = O\left(\frac{M}{D_L}\right)$$

$n \leq 2s+2$

$$\gamma = 0.01 \cdot q^{n-(2s+2)}$$
$$\varepsilon_R = 0.01$$
$$K_R = 0.01 \cdot q^{n-(2s+2)} q^{s+1} = O\left(\frac{N}{MD_L}\right)$$

Right to Left Expansion

Theorem

If $n \geq s+1$, then G is a right (K_R, ε_R)-lossless expander with $K_R = \gamma q^{s+1}$ and $\varepsilon_R = \gamma \cdot q^{\max(2s+2-n,0)}$ where γ is arbitrary.

Right to Left Expansion

Theorem

If $n \geq s+1$, then G is a right (K_R, ε_R)-lossless expander with $K_R = \gamma q^{s+1}$ and $\varepsilon_R = \gamma \cdot q^{\max(2s+2-n,0)}$ where γ is arbitrary.

Lemma

The KT graph G is right-regular with degree $D_R = q^{n-(s+1)}$.

Right to Left Expansion

Theorem

If $n \geq s+1$, then G is a right (K_R, ε_R)-lossless expander with $K_R = \gamma q^{s+1}$ and $\varepsilon_R = \gamma \cdot q^{\max(2s+2-n,0)}$ where γ is arbitrary.

Lemma

The KT graph G is right-regular with degree $D_R = q^{n-(s+1)}$.

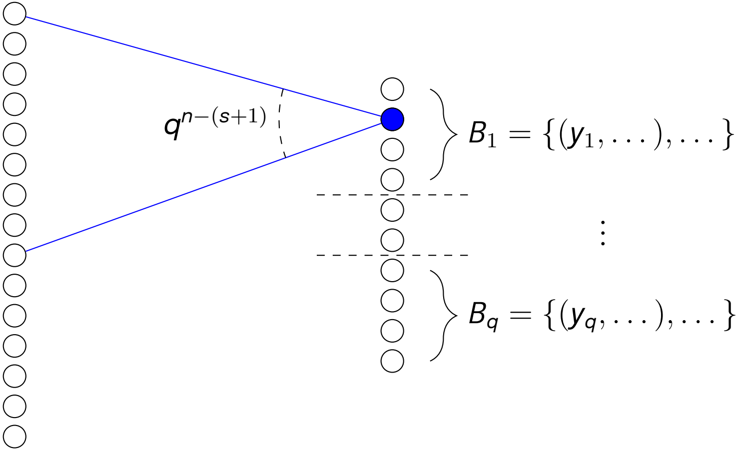
Lemma

For any pair of right vertices $w \in B_i$ and $w' \in B_j$ for $i \neq j$:

$$|\Gamma(w) \cap \Gamma(w')| \leq \begin{cases} q^{n-(2s+2)} & n \geq 2s+2 \\ 1 & n \leq 2s+2 \end{cases}$$

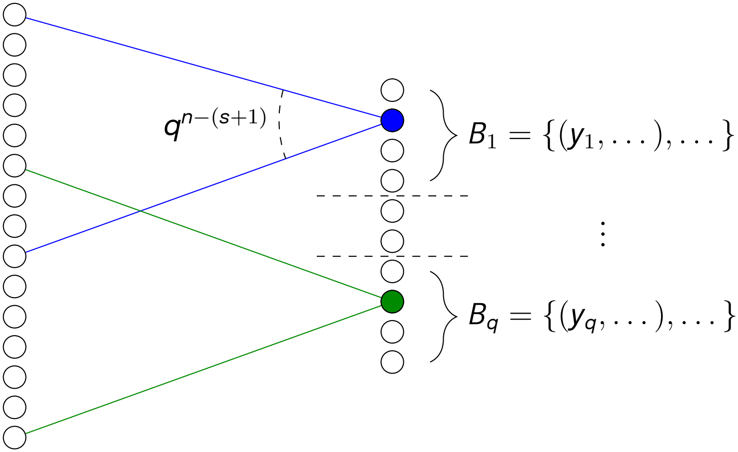
Right to Left Expansion

$$L = \mathbb{F}_q^n = P_{<n} \qquad R = \mathbb{F}_q^{s+2}$$



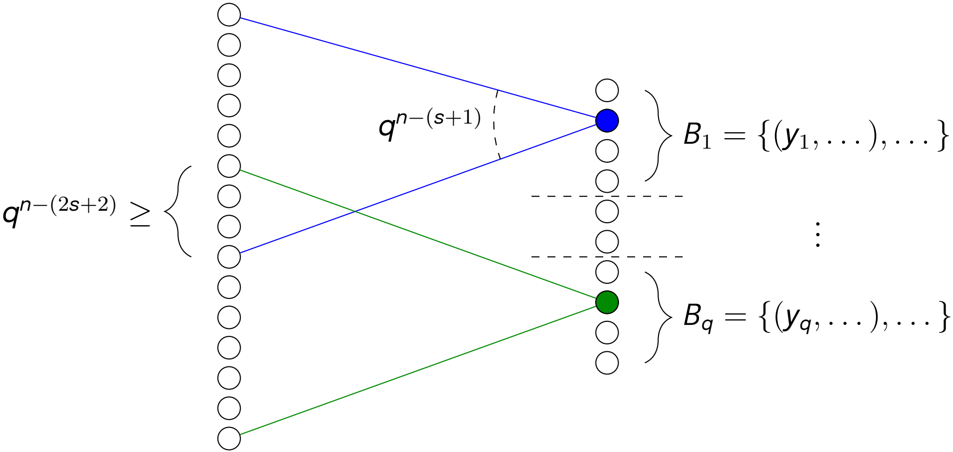
Right to Left Expansion

$$L = \mathbb{F}_q^n = P_{<n} \qquad R = \mathbb{F}_q^{s+2}$$



Right to Left Expansion

$$L = \mathbb{F}_q^n = P_{<n} \qquad R = \mathbb{F}_q^{s+2}$$



Right to Left Expansion

Theorem

If $n \geq s + 1$, then G is a right (K_R, ε_R)-lossless expander with $K_R = \gamma q^{s+1}$ and $\varepsilon_R = \gamma \cdot q^{\max(2s+2-n,0)}$ where γ is arbitrary.

Right to Left Expansion

Theorem

If $n \geq s + 1$, then G is a right (K_R, ε_R)-lossless expander with $K_R = \gamma q^{s+1}$ and $\varepsilon_R = \gamma \cdot q^{\max(2s+2-n,0)}$ where γ is arbitrary.

Proof.

Right to Left Expansion

Theorem

If $n \geq s+1$, then G is a right (K_R, ε_R)-lossless expander with $K_R = \gamma q^{s+1}$ and $\varepsilon_R = \gamma \cdot q^{\max(2s+2-n,0)}$ where γ is arbitrary.

Proof.

- Assume $T \subseteq R = \mathbb{F}_q^{s+2}$, $|T| = K_R$ is evenly spread among q buckets.

Right to Left Expansion

Theorem

If $n \geq s+1$, then G is a right (K_R, ε_R)-lossless expander with $K_R = \gamma q^{s+1}$ and $\varepsilon_R = \gamma \cdot q^{\max(2s+2-n,0)}$ where γ is arbitrary.

Proof.

- Assume $T \subseteq R = \mathbb{F}_q^{s+2}$, $|T| = K_R$ is evenly spread among q buckets.
- Use two levels of inclusion-exclusion to bound left neighborhood.

Right to Left Expansion

Theorem

If $n \geq s+1$, then G is a right (K_R, ε_R)-lossless expander with $K_R = \gamma q^{s+1}$ and $\varepsilon_R = \gamma \cdot q^{\max(2s+2-n,0)}$ where γ is arbitrary.

Proof.

- Assume $T \subseteq R = \mathbb{F}_q^{s+2}$, $|T| = K_R$ is evenly spread among q buckets.
- Use two levels of inclusion-exclusion to bound left neighborhood.
- First level given by $D_R \cdot |T|$.

Right to Left Expansion

Theorem

If $n \geq s+1$, then G is a right (K_R, ε_R)-lossless expander with $K_R = \gamma q^{s+1}$ and $\varepsilon_R = \gamma \cdot q^{\max(2s+2-n,0)}$ where γ is arbitrary.

Proof.

- Assume $T \subseteq R = \mathbb{F}_q^{s+2}$, $|T| = K_R$ is evenly spread among q buckets.
- Use two levels of inclusion-exclusion to bound left neighborhood.
- First level given by $D_R \cdot |T|$.
- Bound on second level given by left overlap lemma.

Hermite Interpolation

Hermite Interpolation

Problem

Hermite Interpolation

Problem

- Given data: m evaluation points $y_1, \ldots, y_m \in \mathbb{F}_q$ and $s+1$ derivatives $\{(z_{0,j}, \ldots, z_{s,j})\}_{j=1}^{m}$ at each point. In total $m(s+1)$ data points.

Hermite Interpolation

Problem

- Given data: m evaluation points $y_1, \ldots, y_m \in \mathbb{F}_q$ and $s+1$ derivatives $\{(z_{0,j}, \ldots, z_{s,j})\}_{j=1}^{m}$ at each point. In total $m(s+1)$ data points.
- Want to find lowest degree $f \in \mathbb{F}_q[x]$ such that $f^{(i)}(y_j) = z_{i,j}$ for $i \in \{0, \ldots, s\}$ and $j \in [m]$.

Hermite Interpolation

Problem

- Given data: m evaluation points $y_1, \dots, y_m \in \mathbb{F}_q$ and $s+1$ derivatives $\{(z_{0,j}, \dots, z_{s,j})\}_{j=1}^{m}$ at each point. In total $m(s+1)$ data points.
- Want to find lowest degree $f \in \mathbb{F}_q[x]$ such that $f^{(i)}(y_j) = z_{i,j}$ for $i \in \{0, \dots, s\}$ and $j \in [m]$.

Hermite Interpolation

Problem

- Given data: m evaluation points $y_1, \ldots, y_m \in \mathbb{F}_q$ and $s+1$ derivatives $\{(z_{0,j}, \ldots, z_{s,j})\}_{j=1}^{m}$ at each point. In total $m(s+1)$ data points.
- Want to find lowest degree $f \in \mathbb{F}_q[x]$ such that $f^{(i)}(y_j) = z_{i,j}$ for $i \in \{0, \ldots, s\}$ and $j \in [m]$.

Theorem (Hermite ineterpolation)

There exists a unique $f \in P_{<m(s+1)}$ satisfying the requirements.

Hermite Interpolation

Problem

- Given data: m evaluation points $y_1, \ldots, y_m \in \mathbb{F}_q$ and $s+1$ derivatives $\{(z_{0,j}, \ldots, z_{s,j})\}_{j=1}^{m}$ at each point. In total $m(s+1)$ data points.
- Want to find lowest degree $f \in \mathbb{F}_q[x]$ such that $f^{(i)}(y_j) = z_{i,j}$ for $i \in \{0, \ldots, s\}$ and $j \in [m]$.

Theorem (Hermite ineterpolation)

There exists a unique $f \in P_{<m(s+1)}$ satisfying the requirements.

Theorem (Generalized Hermite interpolation)

For $n \geq m(s+1)$, there exist exactly $q^{n-m(s+1)}$ satisfactory polynomials in $P_{<n}$.

Right-Regularity

Lemma

The KT graph G is right-regular with degree $D_R = q^{n-(s+1)}$.

Right-Regularity

Lemma

The KT graph G is right-regular with degree $D_R = q^{n-(s+1)}$.

Proof.

Immediate by Hermite interpolation

Left Neighborhood Overlap

Lemma

For any $w_1 \in B_1$ *and* $w_2 \in B_2$*, have that* $|\Gamma(w_1) \cap \Gamma(w_2)| \leq q^{\max((n-(2s+2),0)}$.

Left Neighborhood Overlap

Lemma

For any $w_1 \in B_1$ and $w_2 \in B_2$, have that $|\Gamma(w_1) \cap \Gamma(w_2)| \leq q^{\max((n-(2s+2),0)}$.

Proof.

Left Neighborhood Overlap

Lemma

For any $w_1 \in B_1$ and $w_2 \in B_2$, have that $|\Gamma(w_1) \cap \Gamma(w_2)| \leq q^{\max((n-(2s+2)),0)}$.

Proof.

- Define $\psi_{y_1,y_2} : \mathbb{F}_q^n \to \mathbb{F}_q^{2s+2}$ as $\psi_{y_1,y_2}(f) = \psi_{y_1}(f) \circ \psi_{y_2}(f)$, so it's $\mathbb{F}_q$-linear.

Left Neighborhood Overlap

Lemma

For any $w_1 \in B_1$ and $w_2 \in B_2$, have that $|\Gamma(w_1) \cap \Gamma(w_2)| \leq q^{\max((n-(2s+2),0)}$.

Proof.

- Define $\psi_{y_1,y_2} : \mathbb{F}_q^n \to \mathbb{F}_q^{2s+2}$ as $\psi_{y_1,y_2}(f) = \psi_{y_1}(f) \circ \psi_{y_2}(f)$, so it's $\mathbb{F}_q$-linear.
- For $w_1 = (y_1, z_1)$ and $w_2 = (y_2, z_2)$ where $y_1, y_2 \in \mathbb{F}_q$ and $z_1, z_2 \in \mathbb{F}_q^{s+1}$, we have $|\Gamma(w_1) \cap \Gamma(w_2)| = \left|\psi_{y_1,y_2}^{-1}(z_1, z_2)\right|$.

Left Neighborhood Overlap

Lemma

For any $w_1 \in B_1$ and $w_2 \in B_2$, have that $|\Gamma(w_1) \cap \Gamma(w_2)| \leq q^{\max((n-(2s+2),0)}$.

Proof.

- Define $\psi_{y_1,y_2} : \mathbb{F}_q^n \to \mathbb{F}_q^{2s+2}$ as $\psi_{y_1,y_2}(f) = \psi_{y_1}(f) \circ \psi_{y_2}(f)$, so it's $\mathbb{F}_q$-linear.
- For $w_1 = (y_1, z_1)$ and $w_2 = (y_2, z_2)$ where $y_1, y_2 \in \mathbb{F}_q$ and $z_1, z_2 \in \mathbb{F}_q^{s+1}$, we have $|\Gamma(w_1) \cap \Gamma(w_2)| = \left|\psi_{y_1,y_2}^{-1}(z_1, z_2)\right|$.
- When $n \geq 2s + 2$, Hermite interpolation implies $\left|\psi_{y_1,y_2}^{-1}(z_1, z_2)\right| = q^{n-(2s+2)}$.

Left Neighborhood Overlap

Lemma

For any $w_1 \in B_1$ *and* $w_2 \in B_2$*, have that* $|\Gamma(w_1) \cap \Gamma(w_2)| \le q^{\max((n-(2s+2),0)}$.

Proof.

- Define $\psi_{y_1,y_2} : \mathbb{F}_q^n \to \mathbb{F}_q^{2s+2}$ as $\psi_{y_1,y_2}(f) = \psi_{y_1}(f) \circ \psi_{y_2}(f)$, so it's $\mathbb{F}_q$-linear.
- For $w_1 = (y_1, z_1)$ and $w_2 = (y_2, z_2)$ where $y_1, y_2 \in \mathbb{F}_q$ and $z_1, z_2 \in \mathbb{F}_q^{s+1}$, we have $|\Gamma(w_1) \cap \Gamma(w_2)| = \left|\psi_{y_1,y_2}^{-1}(z_1, z_2)\right|$.
- When $n \le 2s + 2$, Hermite interpolation implies $\left|\psi_{y_1,y_2}^{-1}(z_1, z_2)\right| \le 1$.

Part 1 Outline

- ~~Main results~~
- ~~Construction of the KT graph~~
- ~~Right to left expansion~~
- Tightness
- Open Questions

Tightness

Remark

When $M \leq \sqrt{N}$, the max size of right sets $K_R = O(M/D_L)$ that can expand losslessly is optimal.

Tightness

Theorem

When $M > \sqrt{N}$, the KT graph cannot achieve K_R larger than $O\left(\frac{N}{MD_L}\right)$. That is, when $s + 1 < n < 2s + 2$, the tradeoff $K_R = \varepsilon_R \cdot q^{n-(s+1)}$ is optimal.

Tightness

Theorem

For $s+1 < n < 2s+2$ *and* $0 < \gamma \leq 2$, *there exists* $T \subseteq R$ *such that* $|T| = \gamma q^{n-(s+1)} = K_R$ *and* $|\Gamma(T)| = \left(1 - \frac{\gamma}{4}\right) D_R \, |T|$.

Tightness

Theorem

For $s+1 < n < 2s+2$ *and* $0 < \gamma \leq 2$, *there exists* $T \subseteq R$ *such that* $|T| = \gamma q^{n-(s+1)} = K_R$ *and* $|\Gamma(T)| = \left(1 - \frac{\gamma}{4}\right) D_R\, |T|$.

Lemma (Can achieve worst left overlap)

Let $y_1, y_2 \in \mathbb{F}_q$ *such that* $y_1 \neq y_2$. *Then there exist* $T_1 \subseteq B_{y_1}$ *and* $T_2 \subseteq B_{y_2}$ *such that* $|T_1| = |T_2| = \frac{K_R}{2}$ *and* $|\Gamma(T_1) \cap \Gamma(T_2)| = |T_1| \cdot |T_2|$.

Tightness

Theorem

For $s+1<n<2s+2$ and $0<\gamma\leq 2$, there exists $T\subseteq R$ such that $|T|=\gamma q^{n-(s+1)}=K_R$ and $|\Gamma(T)|=\left(1-\frac{\gamma}{4}\right)D_R\,|T|$.

Lemma (Can achieve worst left overlap)

Let $y_1,y_2\in\mathbb{F}_q$ such that $y_1\neq y_2$. Then there exist $T_1\subseteq B_{y_1}$ and $T_2\subseteq B_{y_2}$ such that $|T_1|=|T_2|=\frac{K_R}{2}$ and $|\Gamma(T_1)\cap\Gamma(T_2)|=|T_1|\cdot|T_2|$.

Proof.

Let $T=T_1\cup T_2$ and use inclusion-exclusion to compute

$$|\Gamma(T)|=D_R\cdot(|T_1|+|T_2|)-|T_1|\cdot|T_2|=\left(1-\frac{\gamma}{4}\right)D_R\,|T|$$

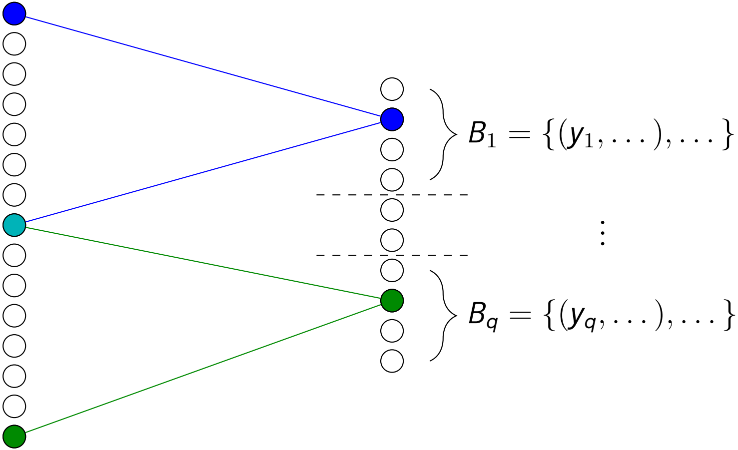
Constructing Worst-Case Right Sets

Lemma (Can achieve worst left overlap)

Let $y_1, y_2 \in \mathbb{F}_q$ *such that* $y \neq y'$. *Then there exist* $T_1 \subseteq B_{y_1}$ *and* $T_2 \subseteq B_{y_2}$ *such that* $|T_1| = |T_2| = \frac{K_R}{2}$ *and* $|\Gamma(T_1) \cap \Gamma(T_2)| = |T_1| \cdot |T_2|$.

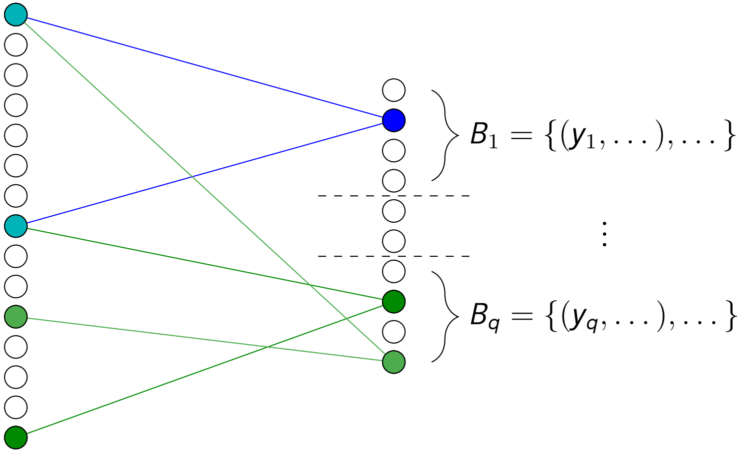
Constructing Worst-Case Right Sets

$L = \mathbb{F}_q^n = P_{<n}$ $\qquad$ $R = \mathbb{F}_q^{s+2}$



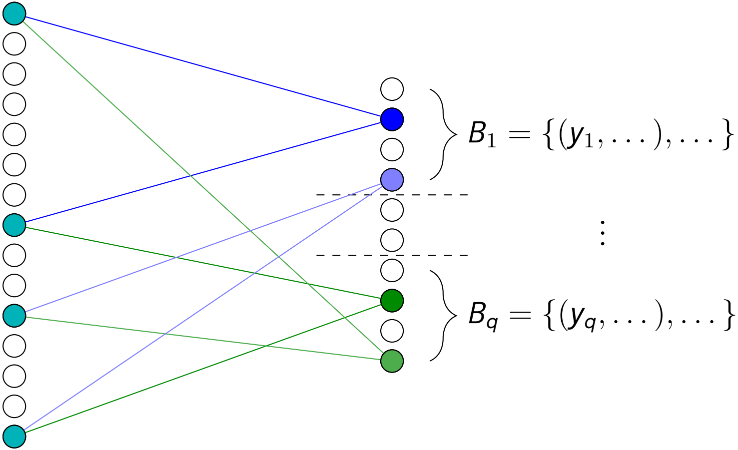
Constructing Worst-Case Right Sets

$L = \mathbb{F}_q^n = P_{<n}$ $\qquad$ $R = \mathbb{F}_q^{s+2}$



Constructing Worst-Case Right Sets

$L = \mathbb{F}_q^n = P_{<n}$ $\qquad$ $R = \mathbb{F}_q^{s+2}$



Constructing Worst-Case Right Sets

Lemma (Can achieve worst left overlap)

Let $y_1, y_2 \in \mathbb{F}_q$ such that $y \neq y'$. Then there exist $T_1 \subseteq B_{y_1}$ and $T_2 \subseteq B_{y_2}$ such that $|T_1| = |T_2| = \frac{K_R}{2}$ and $|\Gamma(T_1) \cap \Gamma(T_2)| = |T_1| \cdot |T_2|$.

Observation

To construct such T_1, T_2, suffices to construct $S_1, S_2 \subseteq \mathbb{F}_q^{s+1}$ with $|S_1| = |S_2| = \frac{K_R}{2}$ such that $S_1 \times S_2 \subseteq \psi_{y_1,y_2}(P_{<n})$ by letting $T_1 = \{(y_1, s_1)\}_{s_1 \in S_1}$ and $T_2 = \{(y_2, s_2)\}_{s_2 \in S_2}$.

Constructing Worst-Case Right Sets

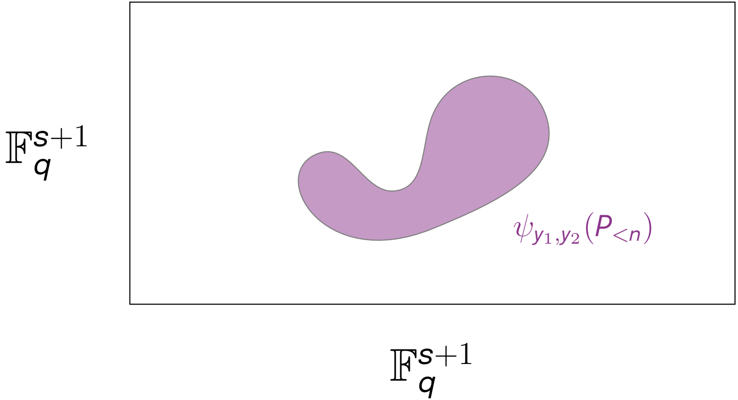
Goal

Construct $S_1, S_2 \subseteq \mathbb{F}_q^{s+1}$ with $|S_1| = |S_2| = \frac{K_R}{2}$ such that $S_1 \times S_2 \subseteq \psi_{y_1,y_2}(P_{<n})$.

Constructing Worst-Case Right Sets

Goal

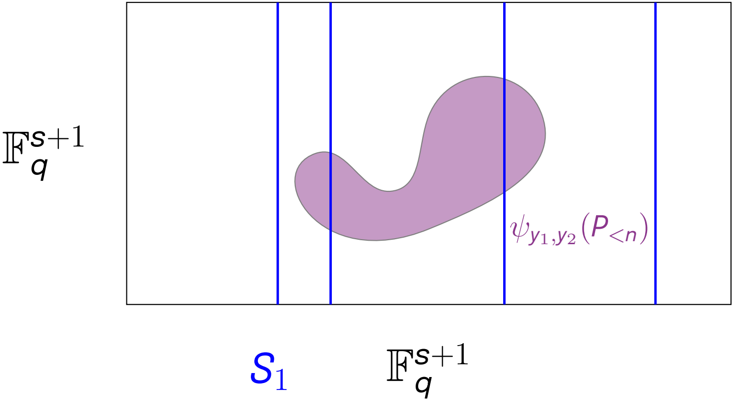
Construct $S_1, S_2 \subseteq \mathbb{F}_q^{s+1}$ with $|S_1| = |S_2| = \frac{K_R}{2}$ such that $S_1 \times S_2 \subseteq \psi_{y_1,y_2}(P_{<n})$.



Constructing Worst-Case Right Sets

Goal

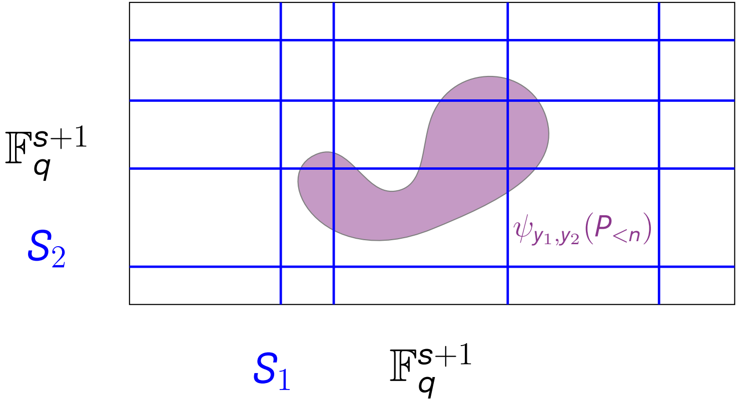
Construct $S_1, S_2 \subseteq \mathbb{F}_q^{s+1}$ with $|S_1| = |S_2| = \frac{K_R}{2}$ such that $S_1 \times S_2 \subseteq \psi_{y_1,y_2}(P_{<n})$.



Constructing Worst-Case Right Sets

Goal

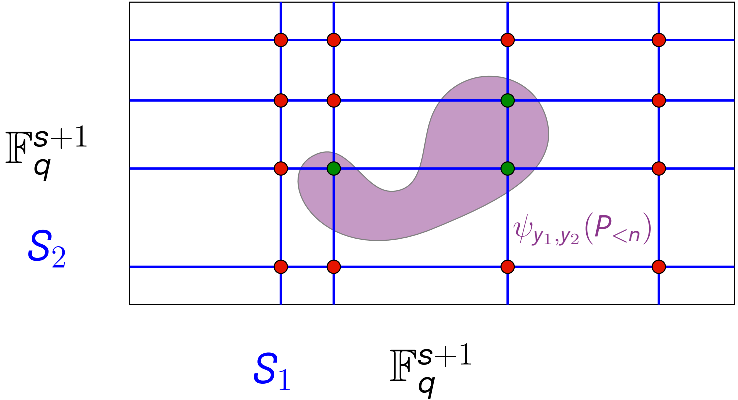
Construct $S_1, S_2 \subseteq \mathbb{F}_q^{s+1}$ with $|S_1| = |S_2| = \frac{K_R}{2}$ such that $S_1 \times S_2 \subseteq \psi_{y_1,y_2}(P_{<n})$.



Constructing Worst-Case Right Sets

Goal

Construct $S_1, S_2 \subseteq \mathbb{F}_q^{s+1}$ with $|S_1| = |S_2| = \frac{K_R}{2}$ such that $S_1 \times S_2 \subseteq \psi_{y_1,y_2}(P_{<n})$.



Constructing Worst-Case Right Sets

Goal

Construct $S_1, S_2 \subseteq \mathbb{F}_q^{s+1}$ with $|S_1| = |S_2| = \frac{K_R}{2}$ such that $S_1 \times S_2 \subseteq \psi_{y_1,y_2}(P_{<n})$.

Lemma

For $s+1 < n < 2s+2$, we have

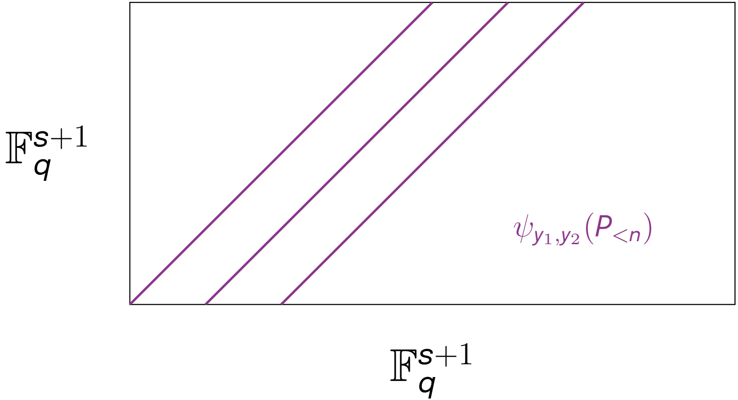
$$\psi_{y_1,y_2}(P_{<d}) = \bigcup_{h \in P_{n-(s+1)}} \{(\psi_{y_1}(f), \psi_{y_2}(f + \sigma(h))) \mid f \in P_{<s+1}\},$$

where $\sigma : P_{n-(s+1)} \to P_{<s+1}$ is an injective homomorphism.

Constructing Worst-Case Right Sets

Goal

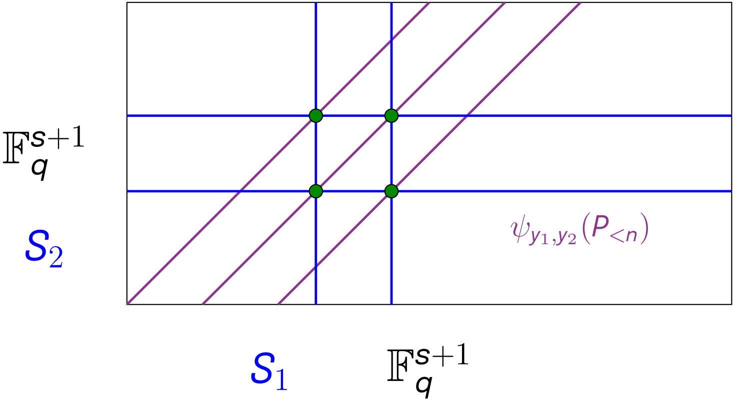
Construct $S_1, S_2 \subseteq \mathbb{F}_q^{s+1}$ with $|S_1| = |S_2| = \frac{K_R}{2}$ such that $S_1 \times S_2 \subseteq \psi_{y_1,y_2}(P_{<n})$.



Constructing Worst-Case Right Sets

Goal

Construct $S_1, S_2 \subseteq \mathbb{F}_q^{s+1}$ with $|S_1| = |S_2| = \frac{K_R}{2}$ such that $S_1 \times S_2 \subseteq \psi_{y_1,y_2}(P_{<n})$.



Constructing Worst-Case Right Sets

Lemma (Can achieve worst left overlap)

Let $y_1, y_2 \in \mathbb{F}_q$ such that $y \neq y'$. Then there exist $T_1 \subseteq B_{y_1}$ and $T_2 \subseteq B_{y_2}$ such that $|T_1| = |T_2| = \frac{K_R}{2}$ and $|\Gamma(T_1) \cap \Gamma(T_2)| = |T_1| \cdot |T_2|$.

Theorem

When $M > \sqrt{N}$, the KT graph cannot achieve K_R larger than $O\left(\frac{N}{MD_L}\right)$. That is, when $s+1 < n < 2s+2$, the tradeoff $K_R = \varepsilon_R \cdot q^{n-(s+1)}$ is optimal.

Part 1 Outline

- ~~Main results~~
- ~~Construction of the KT graph~~
- ~~Right to left expansion~~
- ~~Tightness~~
- Open Questions

Open Questions

Open Questions

Reference(s)	M	$D_L(\downarrow)$	$K_L(\uparrow)$	$K_R(\uparrow)$	$\varepsilon(\downarrow)$
Existential	$O(N)$	$O(1)$	$O(N)$	$O(M)$	0.01
HLMRZ'25	$O(N)$	$O(1)$	$O(N)$	$O(M)$	0.01
Existential	$O(N^\delta)$	$O(\log(N))$	$O(N^{0.9\delta})$	$O(M)$	0.01
Us (on KT'22)	$O(N^\delta)$	$\mathrm{polylog}(N)$	$O(N^{0.9\delta})$	$O(\min(M, \frac{N}{M}))$	0.01

Open Questions

Reference(s)	M	$D_L(\downarrow)$	$K_L(\uparrow)$	$K_R(\uparrow)$	$\varepsilon(\downarrow)$
Existential	$O(N)$	$O(1)$	$O(N)$	$O(M)$	0.01
HLMRZ'25	$O(N)$	$O(1)$	$O(N)$	$O(M)$	0.01
Existential	$O(N^\delta)$	$O(\log(N))$	$O(N^{0.9\delta})$	$O(M)$	0.01
Us (on KT'22)	$O(N^\delta)$	$\mathrm{polylog}(N)$	$O(N^{0.9\delta})$	$O(\min(M, \frac{N}{M}))$	0.01
Existential	$O(N)$	$O(1)$	$O(N)$	$O(M)$	$O(1/D_L)$

Open Questions

Reference(s)	M	$D_L(\downarrow)$	$K_L(\uparrow)$	$K_R(\uparrow)$	$\varepsilon(\downarrow)$
Existential	$O(N)$	$O(1)$	$O(N)$	$O(M)$	0.01
HLMRZ'25	$O(N)$	$O(1)$	$O(N)$	$O(M)$	0.01
Existential	$O(N^\delta)$	$O(\log(N))$	$O(N^{0.9\delta})$	$O(M)$	0.01
Us (on KT'22)	$O(N^\delta)$	$\mathrm{polylog}(N)$	$O(N^{0.9\delta})$	$O(\min(M, \frac{N}{M}))$	0.01
Existential	$O(N)$	$O(1)$	$O(N)$	$O(M)$	$O(1/D_L)$
Existential	$O(N^\delta)$	$O(1)$	$O(N^{0.3\delta})$	$O(M)$	0.01

Open Questions

- When $M > \sqrt{N}$, improve our K_R to $O(M/D_L)$ with different constructions?
- Explicitly construct balanced ultra-lossless expanders with $\varepsilon = O(1/D_L)$?
- Explicitly construct unbalanced expanders with $D_L = O(1)$ for $K_L = O(N^{0.3\delta})$?

Open Questions

- When $M > \sqrt{N}$, improve our K_R to $O(M/D_L)$ with different constructions?
- Explicitly construct balanced ultra-lossless expanders with $\varepsilon = O(1/D_L)$?
- Explicitly construct unbalanced expanders with $D_L = O(1)$ for $K_L = O(N^{0.3\delta})$?
- The KT graph is based on multiplicity codes while the GUV graph is based on Parvaresh-Vardy codes since they have good list-recoverability. Recent work [Chen, Zhang'25] gives better bounds on list-recoverability for folded RS codes. Use to build better condensers?

Part 2: Other Projects & Future Directions

Vertex Expanders

Bipartite Vertex Expander

- A (D_L, D_R)-biregular graph $G = (L \sqcup R, E)$ is a *one-sided (K_L, ε_L)-lossless expander* if for all $S \subseteq L$ s.t. $|S| \leq K_L$ then $|\Gamma(S)| \geq (1 - \varepsilon_L) \cdot D_L \cdot |S|$.
- G is a *two-sided $(K_L, \varepsilon_L, K_R, \varepsilon_R)$-lossless expander* if, moreover, for all $S \subseteq R$ s.t. $|S| \leq K_R$ then $|\Gamma(S)| \geq (1 - \varepsilon_R) \cdot D_R \cdot |S|$.

With $N = |L|$ and $M = |R|$, we can view G instead as its neighborhood function:

$$\Gamma : [N] \times [D_L] \to [M]$$

Vertex Expanders

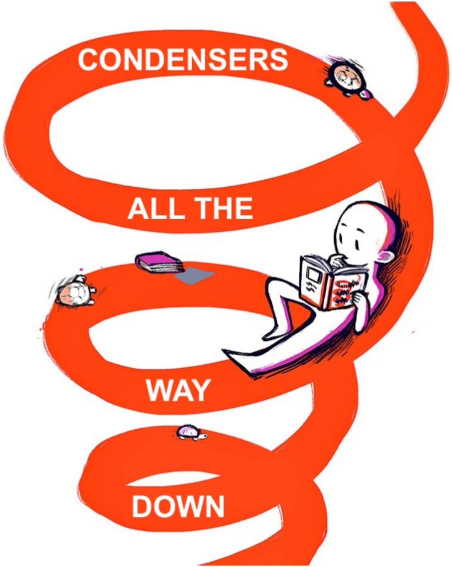
Bipartite Vertex Expander

- A (D_L, D_R)-biregular graph $G = (L \sqcup R, E)$ is a *one-sided (K_L, ε_L)-lossless expander* if for all $S \subseteq L$ s.t. $|S| \leq K_L$ then $|\Gamma(S)| \geq (1 - \varepsilon_L) \cdot D_L \cdot |S|$.
- G is a *two-sided $(K_L, \varepsilon_L, K_R, \varepsilon_R)$-lossless expander* if, moreover, for all $S \subseteq R$ s.t. $|S| \leq K_R$ then $|\Gamma(S)| \geq (1 - \varepsilon_R) \cdot D_R \cdot |S|$.

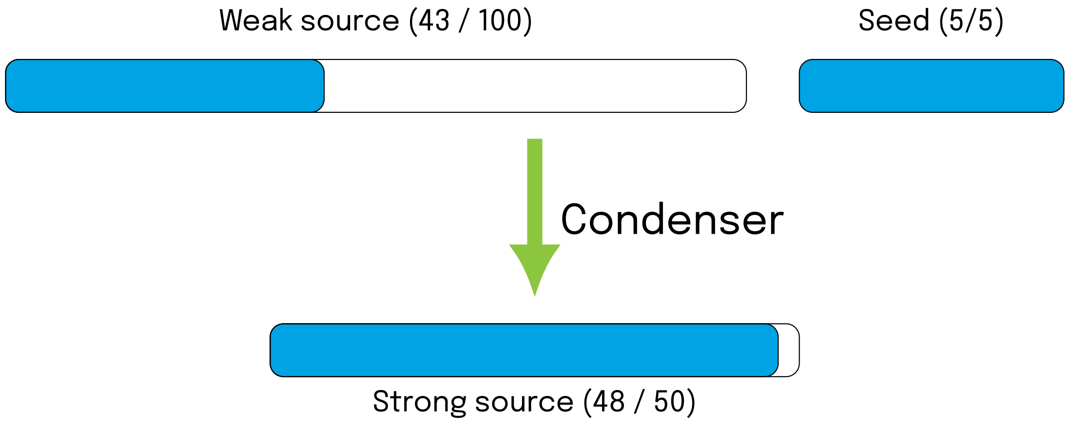
With $n = \log |L|$, $m = \log |R|$, and $d = \log D_L$, we can view G instead as its neighborhood function:

$$\Gamma : \{0,1\}^n \times \{0,1\}^d \to \{0,1\}^m$$

It Was Condensers All Along!



Seeded Condensers

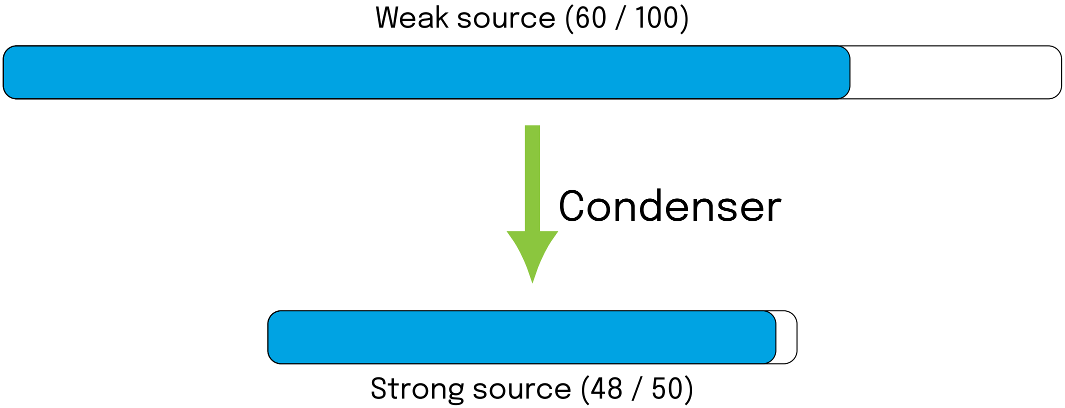


Seeded Condensers

Expanders give condensers

If G is a *one-sided* (K_L, ε)*-expander*, then Γ is a *lossless condenser* for sources with min-entropy at most k and its output ε-close in TV distance to a source with min-entropy at least $k + d$.

What If You Don’t Have Access to a Seed?



What If You Don’t Have Access to a Seed?

NO!

What If You Don't Have Access to a Seed?

NO!

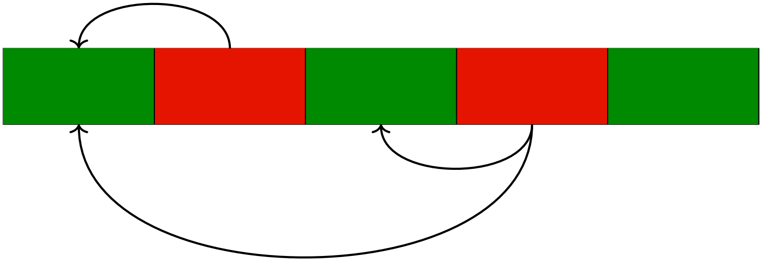
Solution: Distributions must be structured.

oNOSFs

oNOSFs

Online Non-Oblivious Symbol Fixing Sources (oNOSFs)

- ℓ blocks each of length n.
- g uniform "good" blocks, and $\ell - g$ "bad" blocks that are arbitrary functions the of good blocks that **appear before them**.



oNOSFs

Theorem (CGR, FOCS'24)

- ***Can't*** *condense* (g, ℓ)*-oNOSFs beyond* ***rate*** $\frac{\mathbf{1}}{\lfloor \boldsymbol{\ell}/\boldsymbol{g} \rfloor}$.
- ***Can*** *condense* (g, ℓ)*-oNOSFs to* ***rate*** $\frac{\mathbf{1}}{\lfloor \boldsymbol{\ell}/\boldsymbol{g} \rfloor}$ *when* $n \geq 2^{\omega(\ell)}$.

oNOSFs

Theorem (CGR, FOCS'24)

- ***Can't*** *condense* (g, ℓ)*-oNOSFs beyond* ***rate*** $\frac{\mathbf{1}}{\lfloor \boldsymbol{\ell/g} \rfloor}$.
- ***Can*** *condense* (g, ℓ)*-oNOSFs to* ***rate*** $\frac{\mathbf{1}}{\lfloor \boldsymbol{\ell/g} \rfloor}$ *when* $n \geq 2^{\omega(\ell)}$.

Theorem (CGRS'25)

- *Construct* ***explicit*** *condensers as above when* $n \geq 2^{\omega(\ell)}$.
- *Show there* ***exist*** *condensers up to rate* $\frac{1}{\lfloor \ell/g \rfloor}$ *when* $n = O(1)$ *(large).*

oNOSFs

Theorem (CGR, FOCS'24)

- ***Can't*** *condense* (g, ℓ)*-oNOSFs beyond* ***rate*** $\boldsymbol{\frac{1}{\lfloor \ell/g \rfloor}}$.
- ***Can*** *condense* (g, ℓ)*-oNOSFs to* ***rate*** $\boldsymbol{\frac{1}{\lfloor \ell/g \rfloor}}$ *when* $n \geq 2^{\omega(\ell)}$.

Theorem (CGRS'25)

- *Construct* ***explicit*** *condensers as above when* $n \geq 2^{\omega(\ell)}$.
- *Show there* ***exist*** *condensers up to rate* $\frac{1}{\lfloor \ell/g \rfloor}$ *when* $n = O(1)$ *(large).*
- ***Convert*** *leader election protocols into extractors for oNOSFs.*

oNOSFs

Theorem (CGR, FOCS'24)

- ***Can't*** *condense* (g,ℓ)*-oNOSFs beyond* ***rate*** $\boldsymbol{\frac{1}{\lfloor \ell/g \rfloor}}$.
- ***Can*** *condense* (g,ℓ)*-oNOSFs to* ***rate*** $\boldsymbol{\frac{1}{\lfloor \ell/g \rfloor}}$ *when* $n \geq 2^{\omega(\ell)}$.

Theorem (CGRS'25)

- *Construct* ***explicit*** *condensers as above when* $n \geq 2^{\omega(\ell)}$.
- *Show there* ***exist*** *condensers up to rate* $\frac{1}{\lfloor \ell/g \rfloor}$ *when* $n = O(1)$ *(large).*
- ***Convert*** *leader election protocols into extractors for oNOSFs.*
- ***Construct*** *protocols to extract from oNOSFs with* $g \geq \ell - O(\ell/\log^* \ell)$.

New coin flipping protocol bounds

New coin flipping protocol bounds

Theorem (RSZ'02)

- *Upper bound on # of people needed to bias a coin flipping protocol.*

New coin flipping protocol bounds

Theorem (RSZ'02)

- *Upper bound on # of people needed to bias a coin flipping protocol.*

Theorem (CGRS'25)

New coin flipping protocol bounds

Theorem (RSZ'02)

- *Upper bound on # of people needed to bias a coin flipping protocol.*

Theorem (CGRS'25)

- ***Smaller** upper bound on # of people needed to bias a protocol.*

New coin flipping protocol bounds

Theorem (RSZ'02)

- *Upper bound on # of people needed to bias a coin flipping protocol.*

Theorem (CGRS'25)

- ***Smaller** upper bound on # of people needed to bias a protocol.*
- *Construct **explicit** protocol that handles more adversaries than previously possible.*

Open Questions

oNOSFs:

1. Find explicit constructions for oNOSFs with constant block length.

Open Questions

oNOSFs:

1. Find explicit constructions for oNOSFs with constant block length.
2. Determine possibility of condensing from oNOBFs (oNOSFs with block length 1).

Open Questions

oNOSFs:

1. Find explicit constructions for oNOSFs with constant block length.
2. Determine possibility of condensing from oNOBFs (oNOSFs with block length 1).

Coin flipping protocols

Open Questions

oNOSFs:

1. Find explicit constructions for oNOSFs with constant block length.
2. Determine possibility of condensing from oNOBFs (oNOSFs with block length 1).

Coin flipping protocols

1. There's a gap between the number of adversaries our explicit protocol can handle and how many we know can bias any protocol. What's the truth?

Open Questions

oNOSFs:

1. Find explicit constructions for oNOSFs with constant block length.
2. Determine possibility of condensing from oNOBFs (oNOSFs with block length 1).

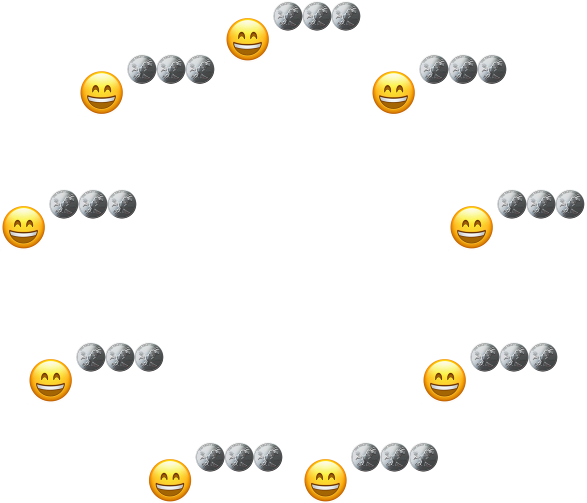
Coin flipping protocols

1. There's a gap between the number of adversaries our explicit protocol can handle and how many we know can bias any protocol. What's the truth?
2. (Dis)prove: For $f : \{0,1\}^\ell \to \{0,1\}^m$, there exist $b = O\left(\frac{\ell}{\log(\ell)}\right)$ bad players that can simultaneously bias $0.01m$ of the output coordinates.

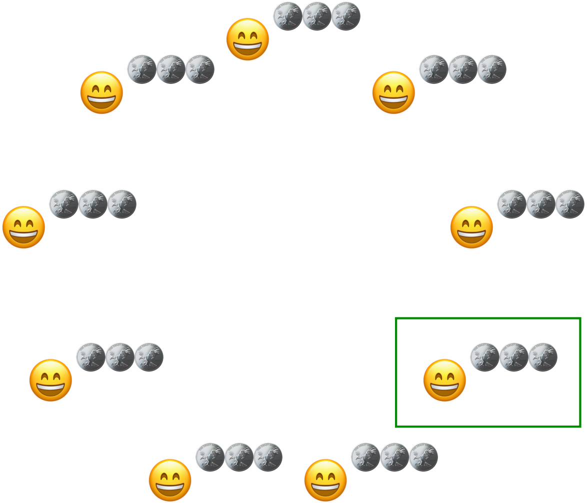
Thank you!

- Committee
- Family
- Friends
- Office mates
- Cornell TCS

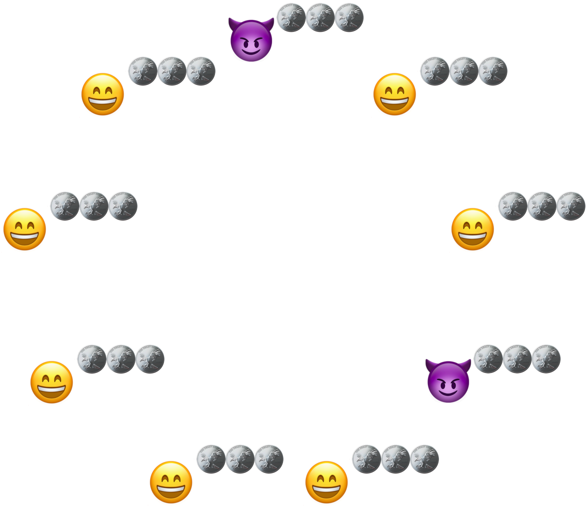
Leader Election Protocols



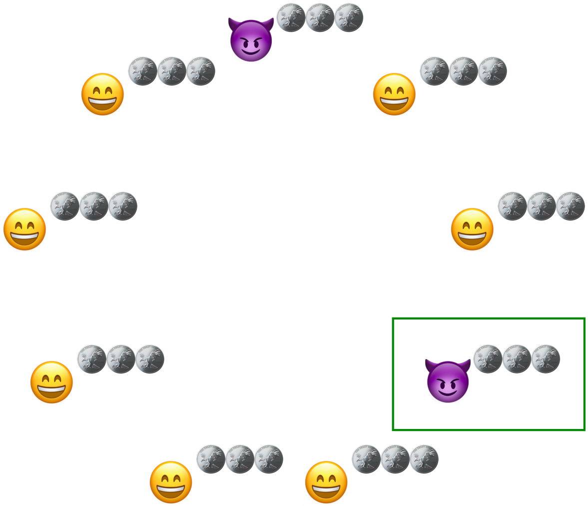
Leader Election Protocols



Leader Election Protocols

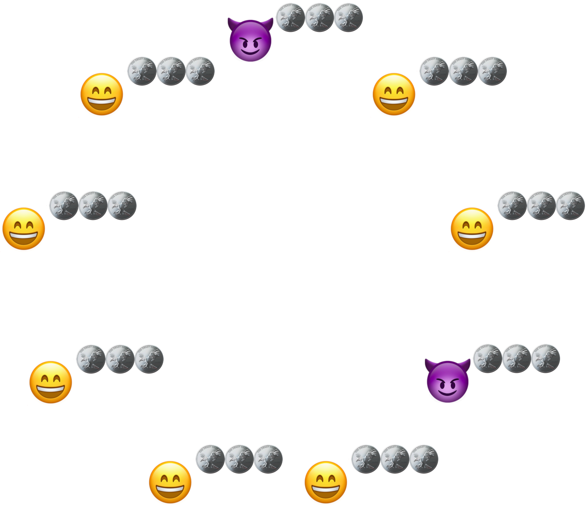


Leader Election Protocols



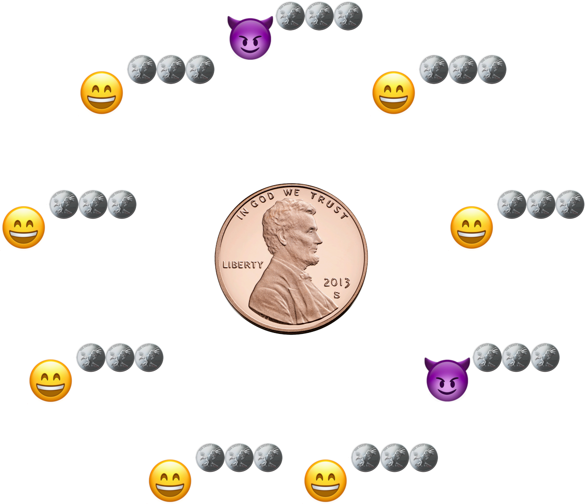
Leader Election Protocols

- ℓ players
- b adversarial
- n bits each
- r rounds
- Common channel
- No crypto



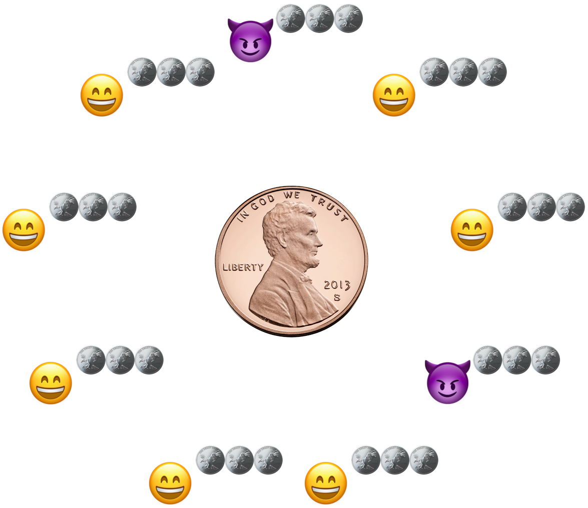
Coin flipping protocols

- ℓ players
- b adversarial
- n bits each
- r rounds
- Common channel
- No crypto



Coin flipping protocols

- ℓ players
- b adversarial
- n bits each
- r rounds
- Common channel
- No crypto
- Leader election $\Longrightarrow$ coin flipping



Protocols

Leader election protocol

- A *leader election protocol* π is a function on ℓ players each with n bits that lasts r rounds and chooses a player at the end of the r rounds.
- π is *resilient* to $b = b(\ell)$ bad players (arbitrary functions of good players in the current and past rounds) if a good player is chosen w.p. $\Omega(1)$.

Protocols

Leader election protocol

- A *leader election protocol* π is a function on ℓ players each with n bits that lasts r rounds and chooses a player at the end of the r rounds.
- π is *resilient* to $b = b(\ell)$ bad players (arbitrary functions of good players in the current and past rounds) if a good player is chosen w.p. $\Omega(1)$.

Coin flipping protocol

A *coin flipping protocol* instead outputs a value in $\{0, 1\}$. Resilient to b bad players if both $\{0, 1\}$ occur w.p. $\Omega(1)$.

Protocols

Leader election protocol

- A *leader election protocol* π is a function on ℓ players each with n bits that lasts r rounds and chooses a player at the end of the r rounds.
- π is *resilient* to $b = b(\ell)$ bad players (arbitrary functions of good players in the current and past rounds) if a good player is chosen w.p. $\Omega(1)$.

Coin flipping protocol

A *coin flipping protocol* instead outputs a value in $\{0, 1\}$. Resilient to b bad players if both $\{0, 1\}$ occur w.p. $\Omega(1)$.

Remark

By adding one more round, can convert leader election to coin flipping.

New coin flipping protocol bounds

Theorem (RSZ'02)

- *Any r-round coin flipping protocol with* $n = 1$ *bit per round can be biased by* $\boldsymbol{O}\left(\frac{\ell}{\log^{(2r-1)}(\ell)}\right)$ *players.*
- *To handle* $b = \Theta(\ell)$ *bad players, need* $\boldsymbol{r \geq \frac{1}{2}\log^*(\ell) - \log^*\log^*(\ell)}$.

Theorem (CGRS'25)

- *Any r-round protocl with* $n = 1$ *biased by* $\boldsymbol{O}\left(\frac{\ell}{\log^{(r)}(\ell)}\right)$ *players.*
- *To handle* $b = \Theta(\ell)$ *bad players, need* $\boldsymbol{r \geq \log^*(\ell) - O(1)}$.
- *For* $r \geq 2$*, exists explicit protocol that can handle* $\boldsymbol{b = O\left(\frac{\ell}{\log(\ell)(\log^{(r)}(\ell))^2}\right)}$.

GUV and KT

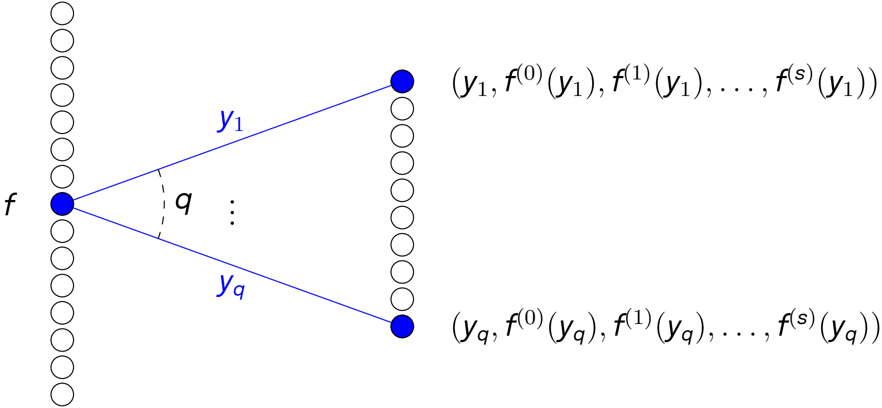
GUV and KT

Do other list-recoverable codes give expanders with better parameters?

GUV and KT

The KT graph is constructed based on multiplicity codes.

$$L = \mathbb{F}_q^n = P_{<n} \qquad R = \mathbb{F}_q^{s+2}$$



GUV and KT

The GUV graph is constructed based on Parvaresh-Vardy codes.

$$L = \mathbb{F}_q^n = P_{<n} \qquad R = \mathbb{F}_q^{s+2}$$