Lecture IV: Quantum Expander Codes

Before we can talk about quantum expander codes, we need to define (classical) expander codes.

We start by recalling the definition of expander graphs.

Def : Expander graph

Let $G=(V,E)$ be a graph on n vertices. We say that the graph is a (ε,δ)-expander if

$$\boxed{\begin{array}{l}\text{for all } S\subset V \text{ with } |S|\leq \varepsilon n\\ |\{y : \exists x\in S \text{ s.t. } (x,y)\in E\}|>\delta|S|\end{array}}$$

That is, every subset S of vertices of size at most εn has a neighbourhood of size greater than $\delta|S|$.

Now suppose $G = (\{A, B\}, E)$

is a bipartite graph where the vertices

of A are a-regular and the

vertices of B are b-regular.

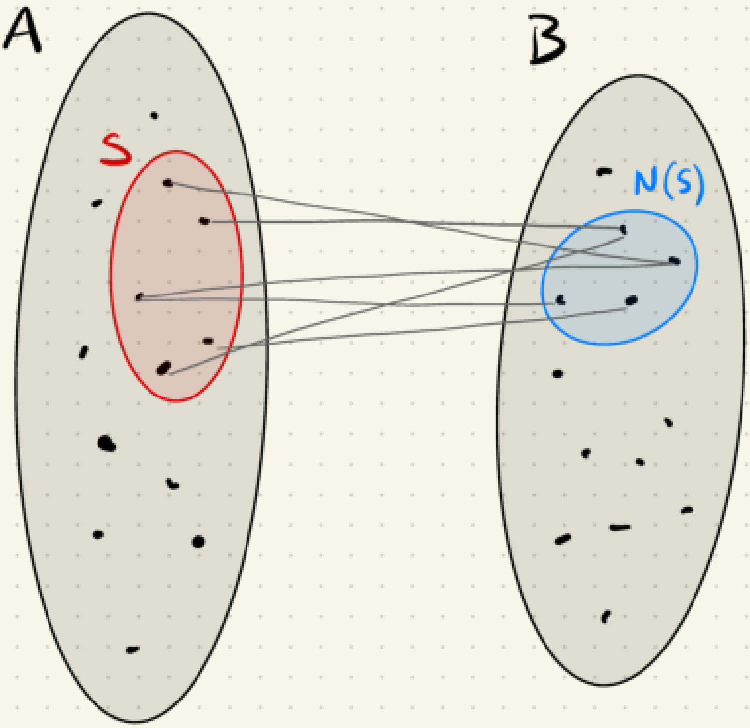
We call such graphs (a,b)-regular

We say that G is an

$(a, b, \varepsilon, \delta)$-expander if it is

(a,b)-regular and

$$\boxed{\begin{array}{l} \forall S \subseteq A \text{ with } |S| \leq \varepsilon |A| \\ |\{y : \exists x \in S \text{ s.t. } (x,y) \in E\}| > \delta |S| \end{array}}$$



Neighborhood

$$N(S) = \{ y \in B : \exists x \in S \text{ s.t. } (x,y) \in E \}$$

We are interested in families of graphs of increasing size, where each graph in the family is an $(a, b, \varepsilon, \delta)$-expander.

Def: Expander code

Let $G = (\{A, B\}, E)$ be an (a,b)-regular graph with $|A| = n$ and $|B| = an/b$.

Let $\mathcal{C}$ (the local code) be a linear code on b bits. Let

$\{1, 2, \ldots, n\}$

$$f(i,j) : [an/b] \times [b] \to [n]$$

be a bijective function defined such that, for each $u_i \in B$ the neighbourhood of u_i,

$$N(u_i) = \{ v_{f(i,1)}, \ldots, v_{f(i,b)} \}.$$

The expander code defined by G and $\mathcal{C}$ is the linear code on n bits whose codewords are the vectors $(v_1, v_2, \dots, v_n)$ such that, for $i \in [an/b]$, $(v_{f(i,1)}\, v_{f(i,2)}, \dots, v_{f(i,b)})$ is a codeword of $\mathcal{C}$.

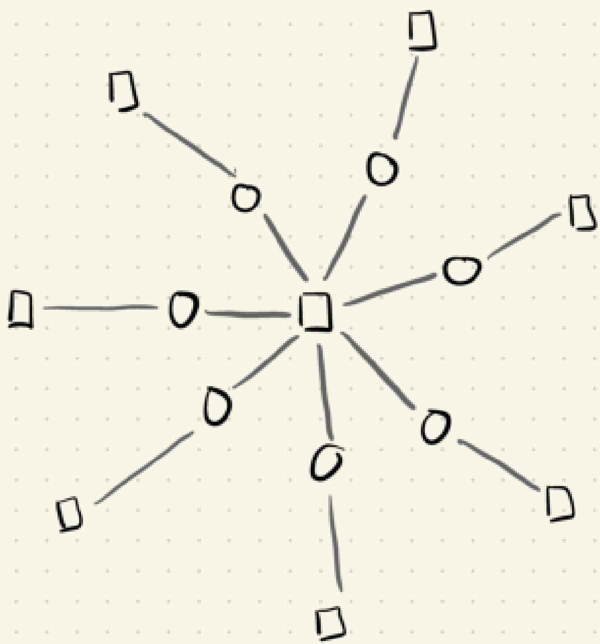
Def: relative distance of an $[n,k,d]$ linear code.

$$\boxed{d_r = d/n}$$

Example

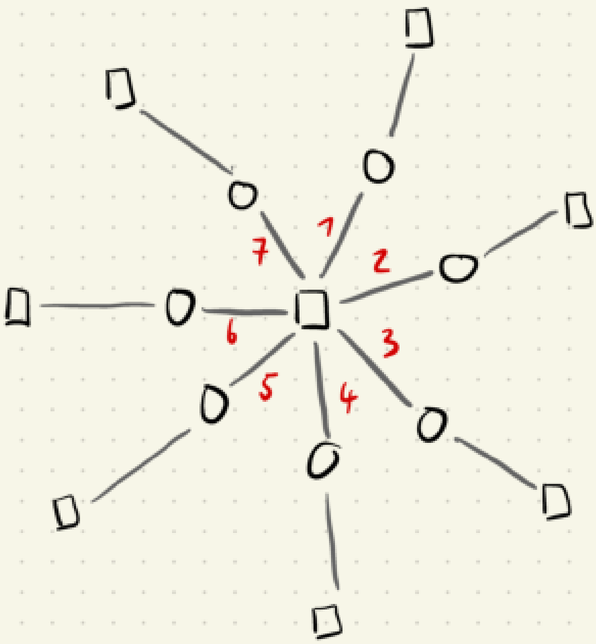
Let G be a $(2,7)$-regular graph. Denote the A vertices by ○ and the B vertices by □.

Locally, the graph looks like



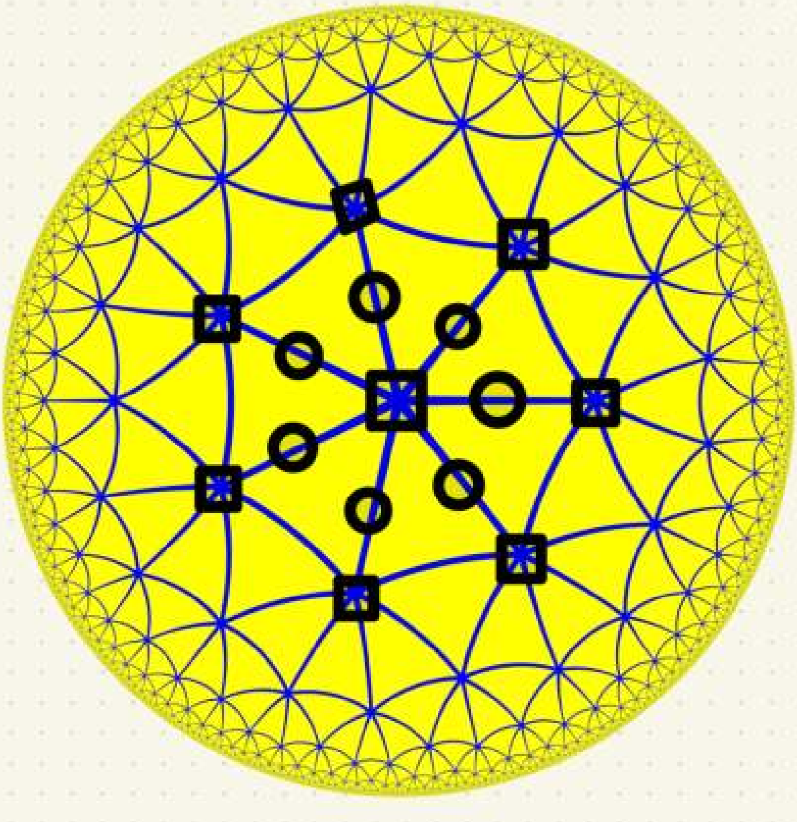
Let $\mathcal{C}$ be the $[7,4,3]$ Hamming code.

$$H = \begin{array}{c} \begin{bmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix} \\ \begin{array}{ccccccc} 1 & 2 & 3 & 4 & 5 & 6 & 7 \end{array} \end{array}$$



The codewords of the expander code defined by G and $\mathcal{C}$ must locally be codewords of $\mathcal{C}$ e.g. $(1110000)^T$.

An example of such a graph G is the edge-vertex incidence graph of a certain hyperbolic tiling.



Theorem: Let G be an $(a, b, \alpha, \frac{a}{\gamma b})$-expander and let $\mathcal{C}$ be a linear code on b bits with encoding rate $r > (a-1)/a$, and minimum relative distance γ.

Recall
$|A| = n$
$|B| = \frac{an}{b}$

[That is, the code has parameters

$$[\, b, k > \left(\frac{a-1}{a}\right) b, d = \gamma b \,].]$$

Then the expander code defined by G and $\mathcal{C}$ has encoding rate at least $ar - (a-1)$ and minimum relative distance at least α.

Proof

To find k we count the number of parity checks.

Each vertex in B imposes

$$b - rb = b(1-r) \text{ parity checks.}$$

Assuming all checks are independent, we have

$$k = n - \frac{an}{b} b(1-r)$$

$$= n - an(1-r) = n(1-a(1-r))$$

$$= n(ar - (a-1))$$

So the encoding rate

$\frac{k}{n}$ is at least $ar - (a-1)$.

Now to prove the distance

suppose that $\underline{v}$ is a codeword

of (Hamming) weight $\leq \alpha n$.

Let V be the set of bits $= 1$

in $\underline{v}$. As G is (a,b)-regular,

there are $a|V|$ edges leaving

the corresponding A vertices in G.

The expansion property implies

that these edges are incident

to more than $\frac{a}{\gamma b} |V|$

B vertices in G.

So the set of 1 bits are incident

to more than $\frac{a}{\gamma b} |V|$ parity checks.

The average number of bits per B vertex

is less than $a|V| \,/\, \frac{a}{\gamma b} |V|$

$$= \gamma b$$

There must be at least one B

vertex that achieves the average

and therefore we have a B vertex with fewer than γb 1 bits incident to it. But the local code $\mathcal{C}$ has distance $= \gamma b$ and so $\underline{v}$ cannot satisfy the checks of the local code at this B vertex and is therefore not a valid codeword of the expander code.

□

Families of graphs exist that satisfy the constraints of the Theorem & so expander codes provide a construction of good LDPC codes w/ parameters $[n, \Theta(n), \Theta(n)]$.

Theorem: There exist families of qLDPC codes with parameters

$$[[N, \Theta(N), \Theta(\sqrt{N})]].$$

Proof: We apply the hypergraph product construction to the a family of good expander codes defined by a family of (a,b)-regular graphs and a local code $\mathcal{C}$ with encoding rate r.

Let G_i be the ith graph and H_i be the ith parity check matrix. We can choose $H_i \in \mathcal{M}_{m_i \times n_i}(\mathbb{F}_2)$ such that it is (b,a)-LDPC and full rank (ie $k^T = 0$).

The expander code has parameters

$[n_i, (ar-(a-1))n_i, \alpha n_i]$.

Consider the code $HGP(H_i, H_i)$.

Applying our previous results we conclude:

- $HGP(H_i, H_i)$ is $(a+b, \max\{a,b\})$ – qLDPC.

- $HGP(H_i, H_i)$ has $N = n_i^2 + m_i^2$

- $HGP(H_i, H_i)$ has $K = k^2$
$$= (ar - (a-1)n_i)^2$$

- $HGP(H_i, H_i)$ has $D = d = \alpha n_i$

$\square$

This family of qLDPC codes is known as quantum expander codes.

Expander codes can be decoded in linear time using a simple algorithm called FLIP.

Quantum expander codes can also be decoded in linear time using a generalisation of FLIP called small set flip.

Q. expander codes were also the first known family of codes to enable fault-tolerant q. computation w/ constant (space) overhead.

References

- Sipser and Spielman
  "Expander Codes"

  Beautiful paper ↑

- Leverrier, Tillich, and Zémor
  "Quantum Expander Codes"

  arXiv: 1504.00822