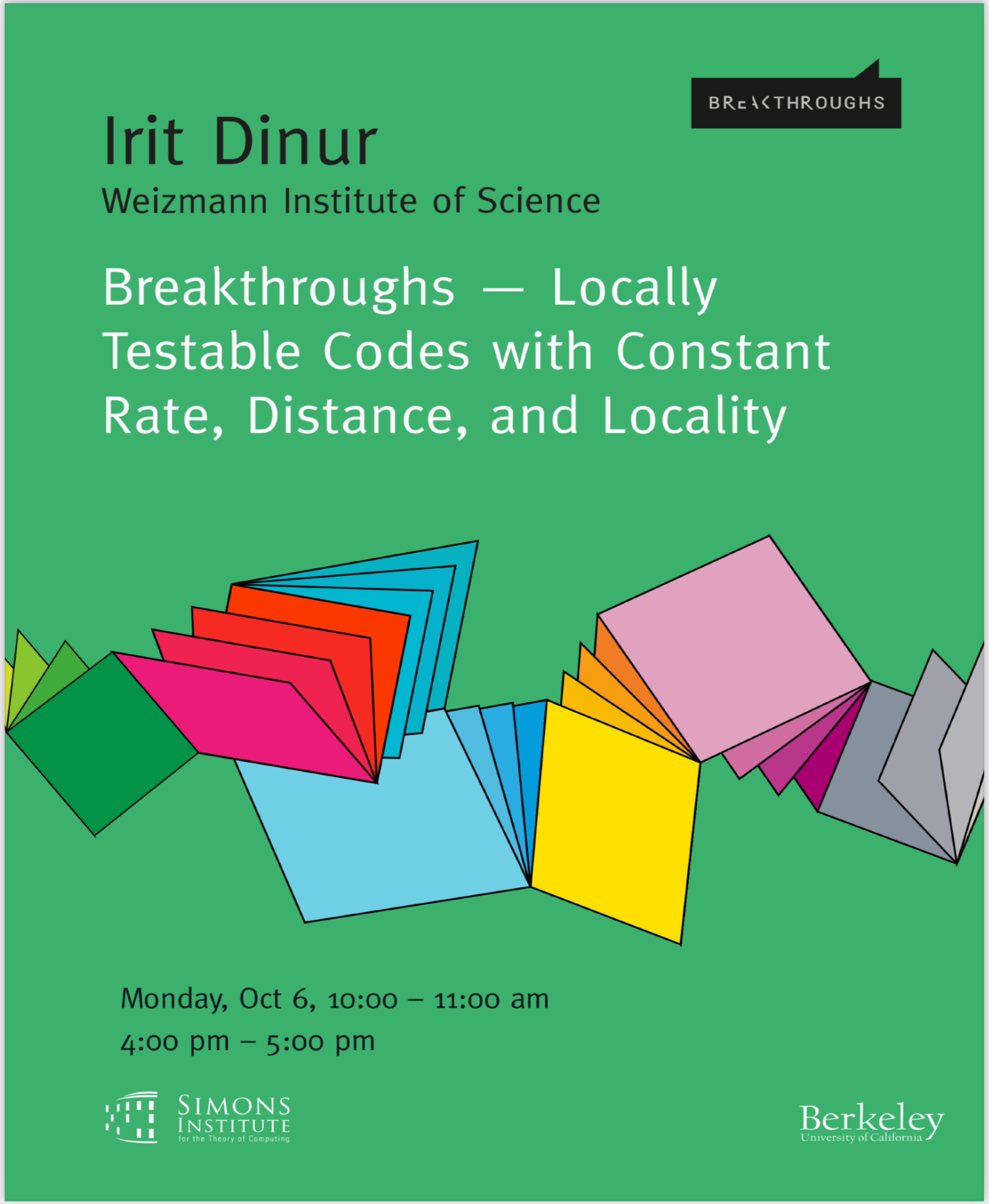


Joint with

Shai Evra

Ron Livne

Alexander Lubotzky

Shahar Mozes

Locally Testable Codes

A linear error-correcting code is a linear subspace $C \subseteq \{0,1\}^n$

Rate = $\dfrac{dim(C)}{n}$, Distance = $min_{w \in C \setminus \{0\}} \dfrac{|\{i : w_i \neq 0\}|}{n}$

A code C is locally testable with q queries if there is a tester T that has query access to a given word w, reads q randomized bits from w and accepts / rejects, such that

- If $w \in C$ then Pr[T accepts] $= 1$
- If $w \notin C$ then Pr[T rejects] $\geq const \cdot dist(w, C)$

q = the locality of the tester

Historical background

- LTCs were studied implicitly in early PCP works [BlumLubyRubinfeld 1990, BabaiFortnowLund 1990, ..]
- Formally defined in works on low degree tests [Friedl-Sudan, Rubinfeld-Sudan] ~ 1995
- Spielman in his PhD thesis (1996), writes:

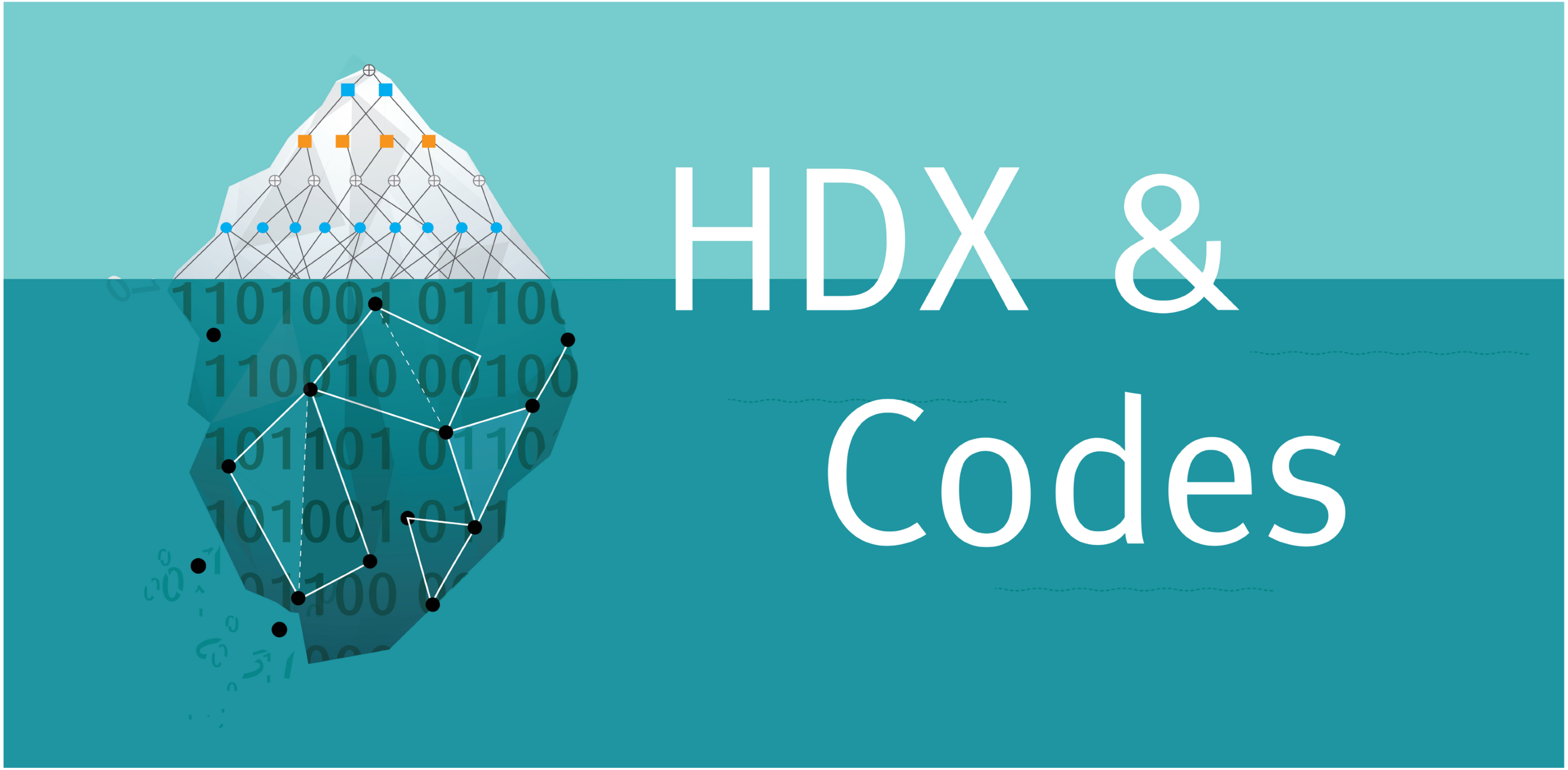
  “A checker would be able to read only a constant number of bits of a received signal and then estimate the chance that a decoder will be able to correct the errors, then the checker can instantly request a retransmission of that block, before the decoder has wasted its time trying to decode the message. Unfortunately all known codes with local-checkers have rate approaching zero."

- A systematic study of LTCs was initiated by Goldreich and Sudan in 2002.
  “what is the highest possible rate of an LTC?”

Historical background

- Sequence of works (BenSasson-Sudan-Vadhan-Wigderson2003, BenSasson-Goldreich-Harsha-Sudan-Vadhan2004, Ben-Sasson-Sudan2005, Dinur2005) achieved rate = 1/polylog & constant locality+distance
- "$\mathbf{c}^3$ LTCs" (**c**onstant rate, **c**onstant distance, **c**onstant locality) - experts doubt existence. Restricted lower bounds are shown [BenSasson-Harsha-Rashkhodnikova2005, Babai-Shpilka-Stefankovic2005, BenSasson-Guruswami-Kaufman-Sudan-Viderman2010, D.-Kaufman2011]
- Fix rate to constant, get locality $(\log n)^{\log \log n}$: [Kopparty-Meir-RonZewi-Saraf2017, Gopi-Kopparty-OliveiraRonZewi-Saraf2018] (forget about PCPs, inject expanders)
- Affine invariance [Kaufman-Sudan2007,...]: what makes properties testable?
- High dimensional expansion: local to global features [Garland 1973, Kaufman-Kazhdan-Lubotzky 2014, Evra-Kaufman 2016, Oppenheim 2017, D.-Kaufman 2017, D.-Harsha-Kaufman-LivniNavon-TaShma 2019, Dikstein-D.-Harsha-Kaufman-RonZewi 2019, Anari-Liu-OveisGharan-Vinzant2019]

We even had a summer cluster at the Simons Institute in 2019



Main Result

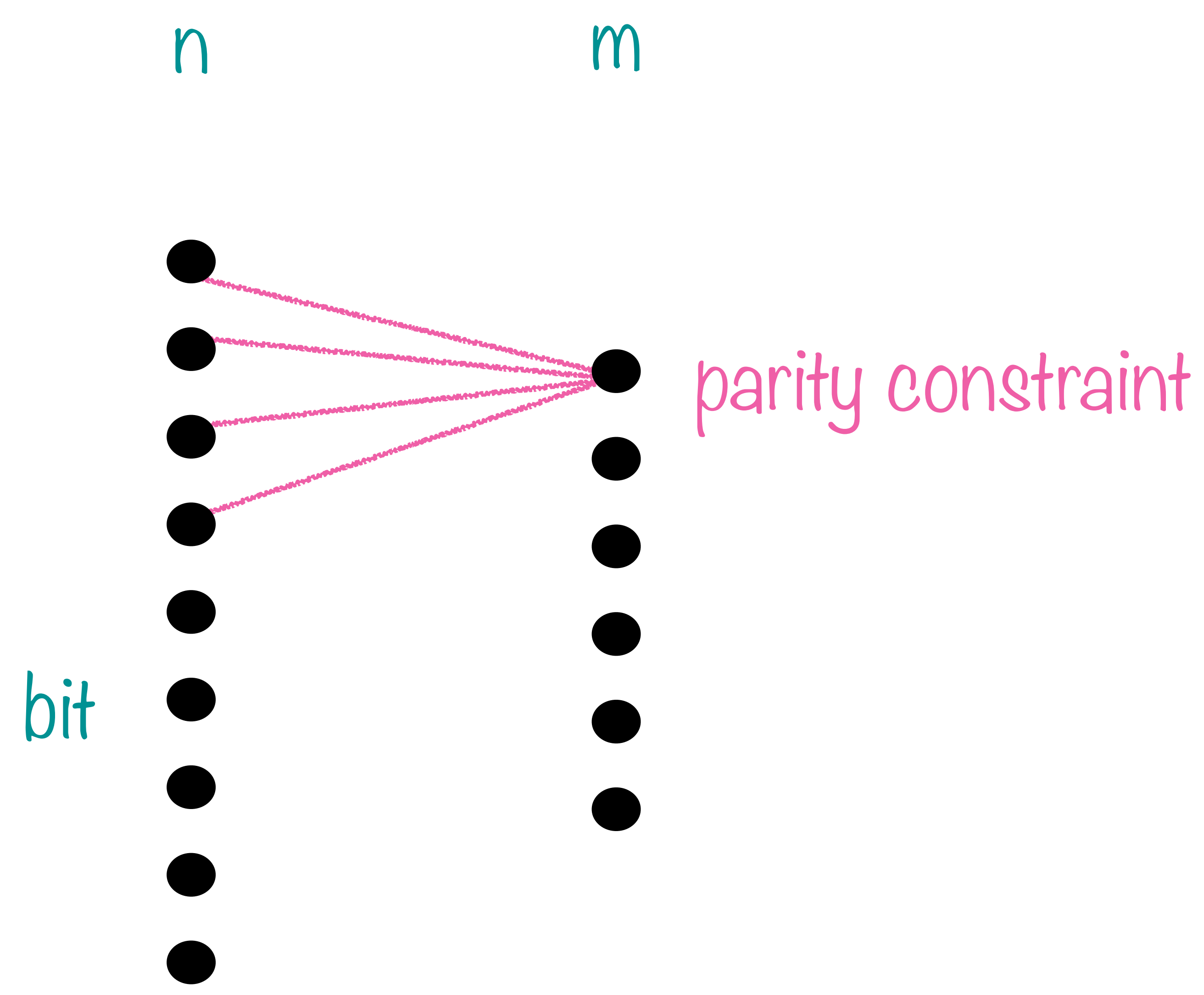
There exist $r, \delta > 0$ and $q \in \mathbb{N}$ and an explicit construction of an infinite family of error-correcting codes $\{C_n\}_n$ with rate $\geq r$, distance $\geq \delta$ and locally testable with q queries.

Plan of talk

1. Expander codes
2. New: left-right Cayley complex, "a graph-with-squares"
3. Define the code on the complex / graph-with-squares
4. Properties of the code

Expander Codes

- Gallager (1963): A random LDPC code has good rate & distance
- Tanner (1981): Place a small base-code $C_0 \subseteq \{0,1\}^d$ on each constraint node. Consider various bipartite graph structures
- Sipser & Spielman (1996): Explicit expander-codes: Tanner codes using edges of an (explicit) expander



factor graph

$$C = \{ w \in \{0,1\}^n : \forall\, v \in [m] \ \sum_{i \sim v} w_i = 0 \bmod 2 \}$$

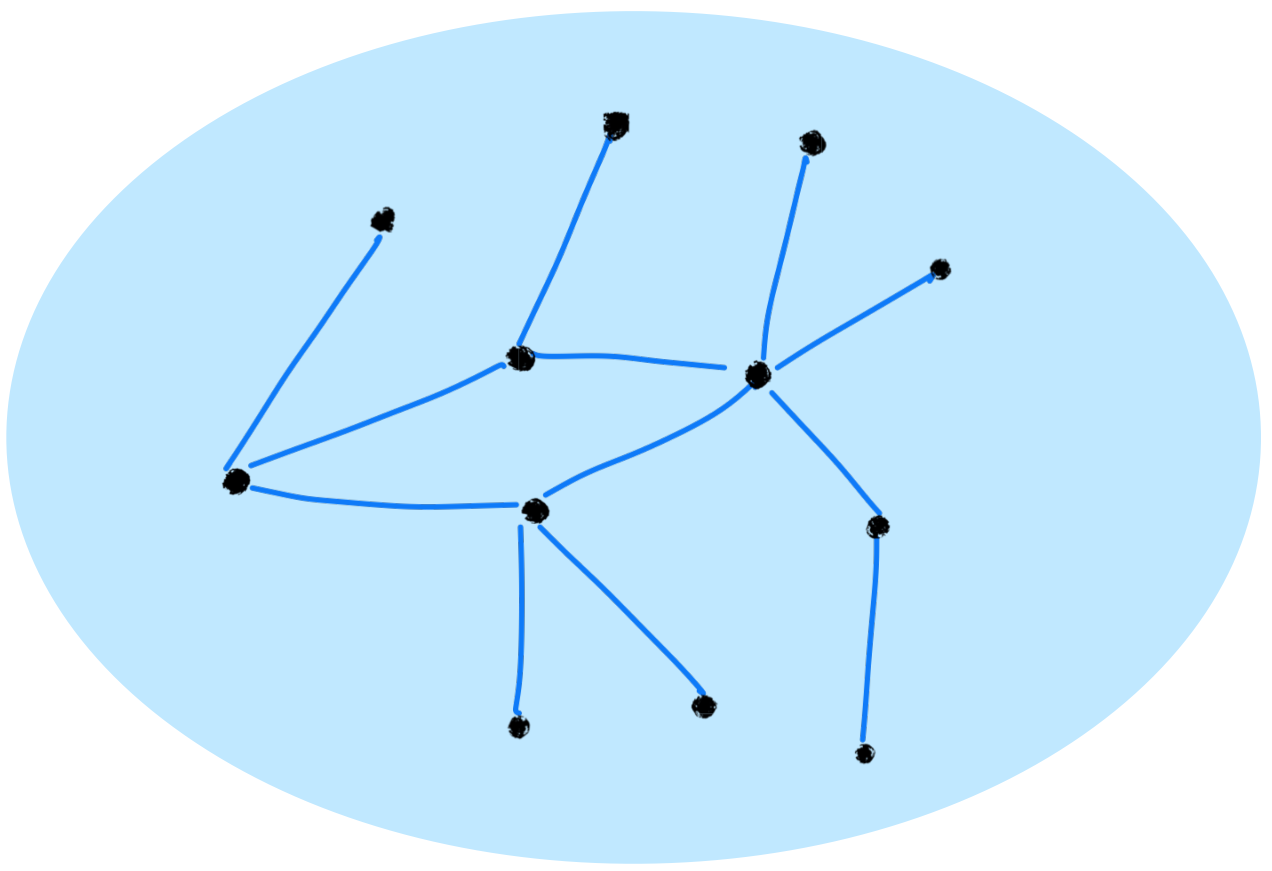
$$C = \{ w \in \{0,1\}^n : \forall\, v \in [m] \ w|_{nbrs(v)} \in C_0 \}$$

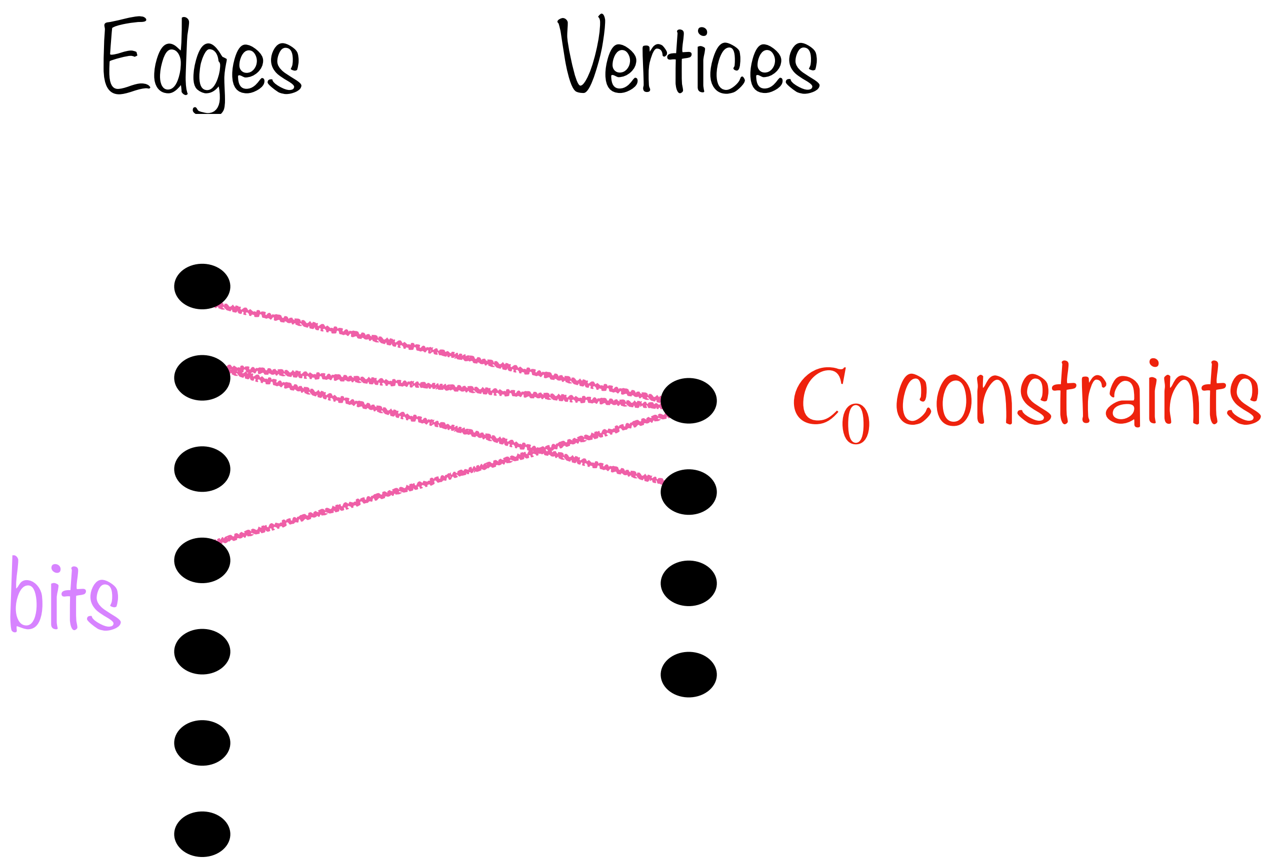
Expander Codes [SS'96]

Given

1. A d-regular $\lambda-$expander graph G on n vertices
2. A base code $C_0 \subseteq \{0,1\}^d$ with rate r_0, distance δ_0

Let $C[G, C_0] = \{w : E \to \{0,1\} : \forall v, w|_{edges(v)} \in C_0\}$



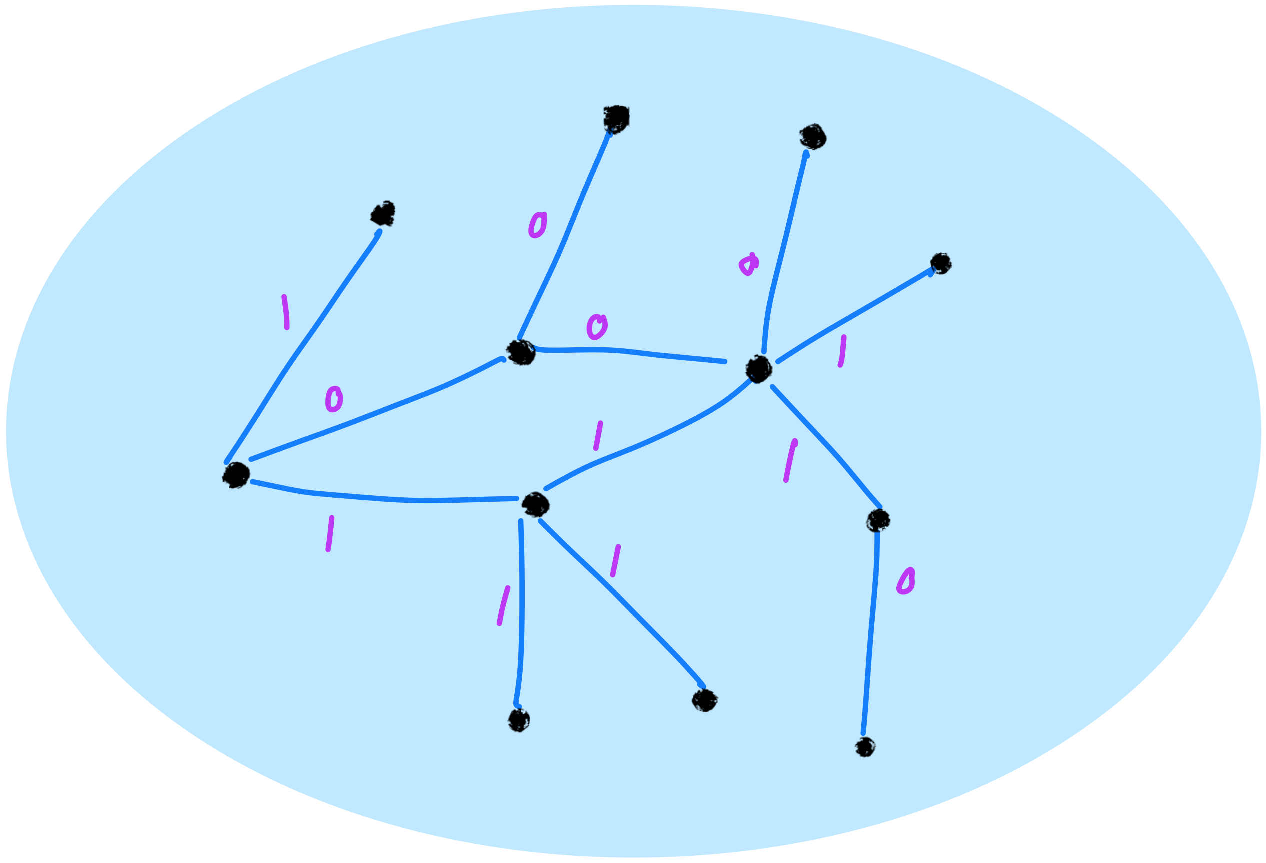


Expander Codes [SS'96]

Given

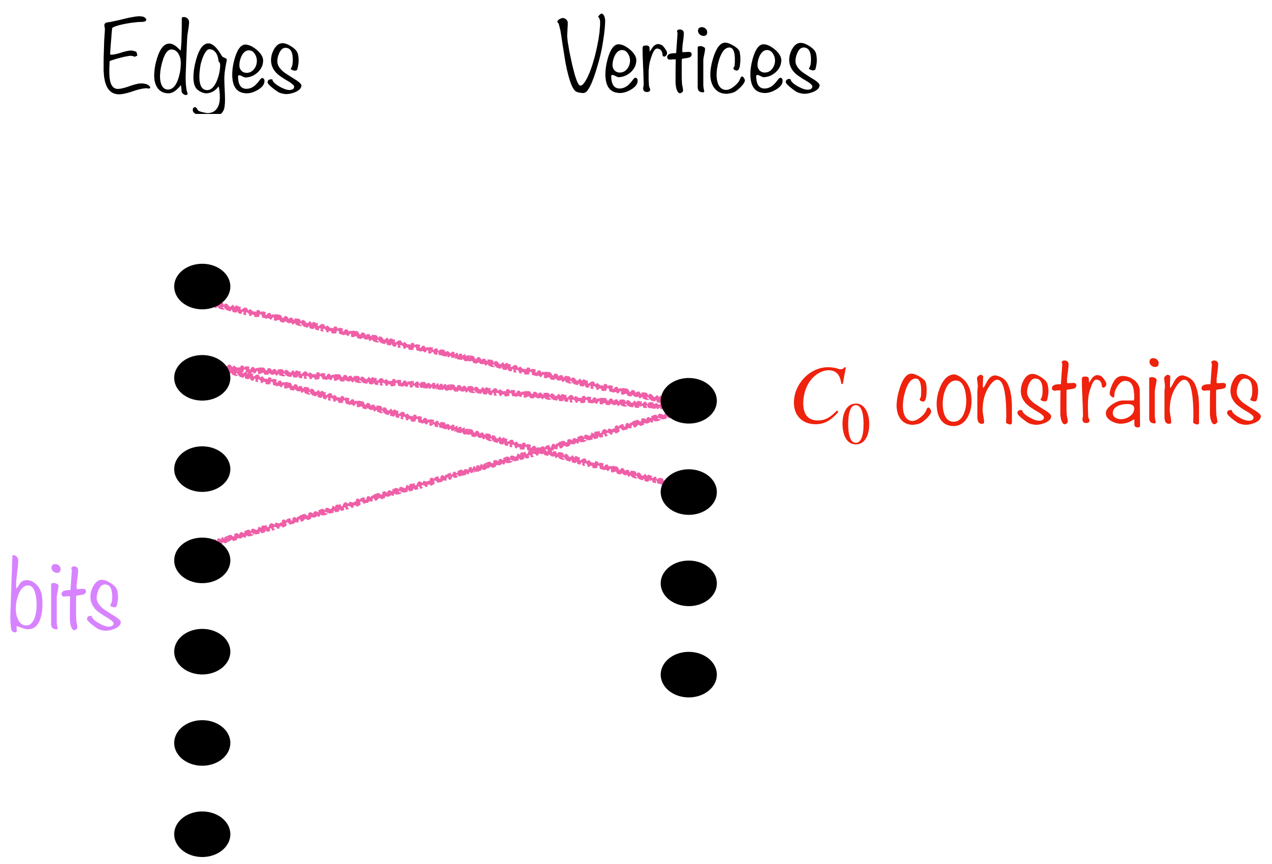
1. A d-regular $\lambda-$expander graph G on n vertices
2. A base code $C_0 \subseteq \{0,1\}^d$ with rate r_0, distance δ_0

Let $C[G, C_0] = \{w : E \to \{0,1\} : \forall v, w|_{edges(v)} \in C_0\}$



- Dim(C) $\geq$ #bits - #constraints =

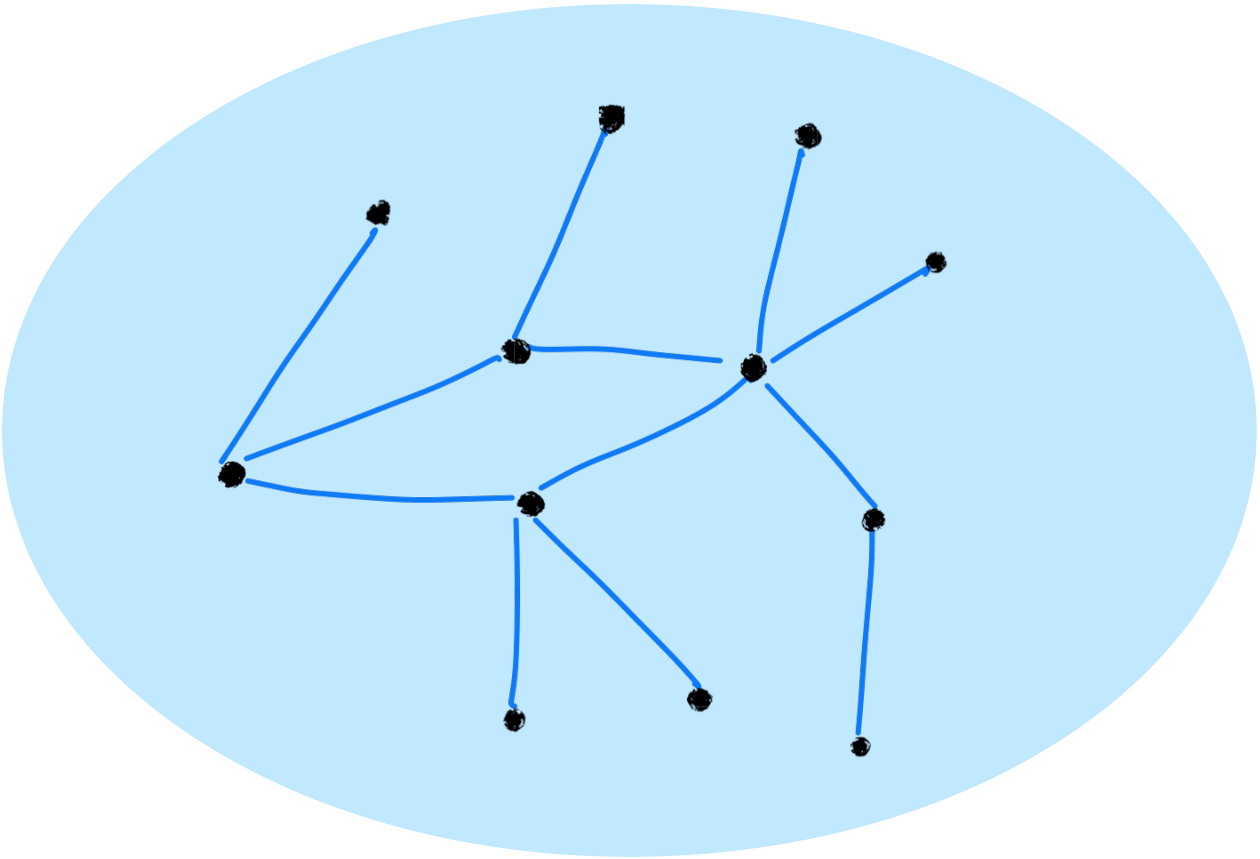
  $|E| - |V| \cdot (1 - r_0)d = |E|(2r_0 - 1)$ rate positive if $r_0 > 1/2$
- Distance $\geq \delta_0(\delta_0 - \lambda)$
- Linear time decoding !
- Locally testable?



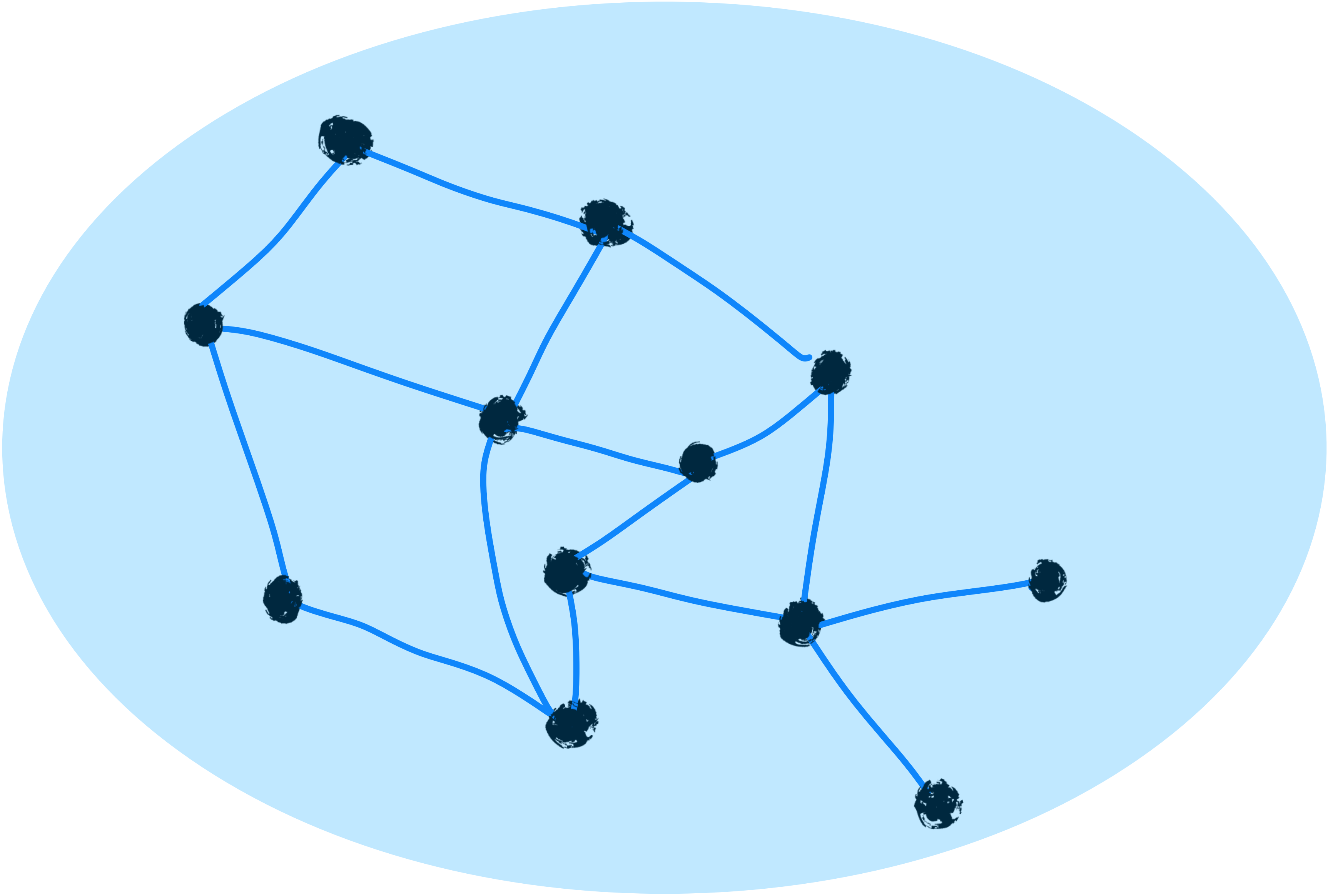
Expander Codes [SS'96]

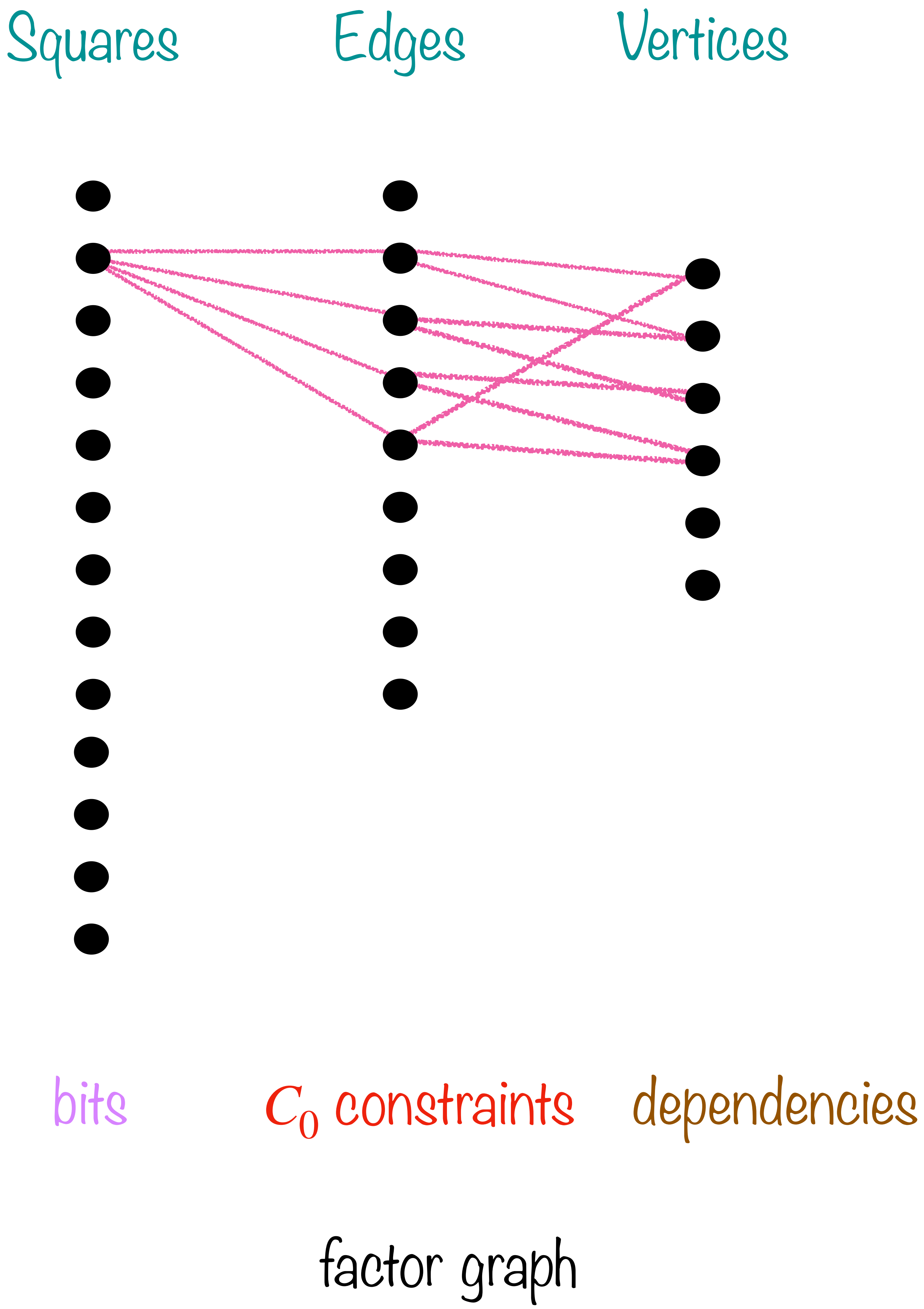
are typically not locally testable

- No need to put same base code at each vertex
- Remove one constraint from the base-code of v_0
- New codewords are far from old code, but violate only one constraint

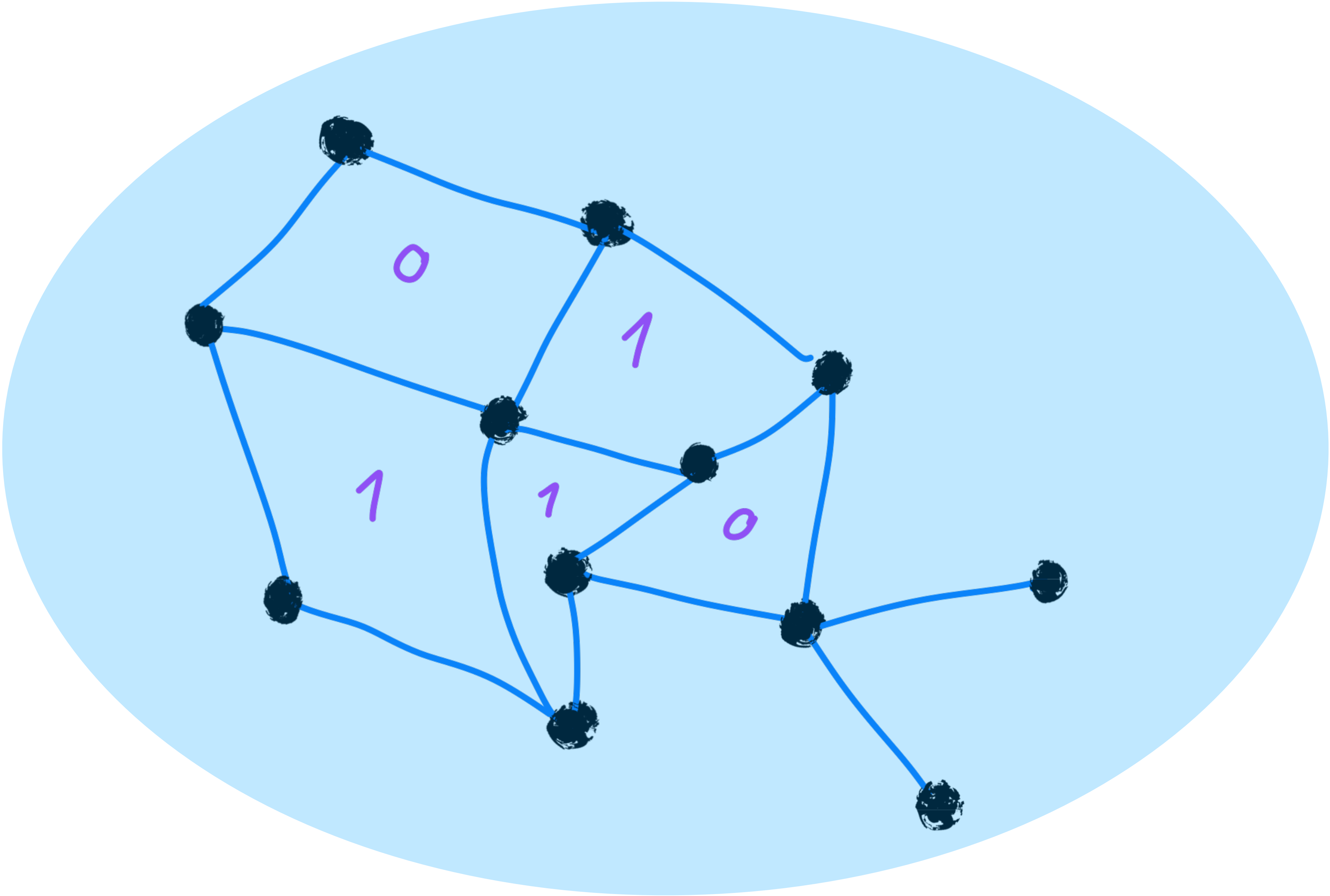


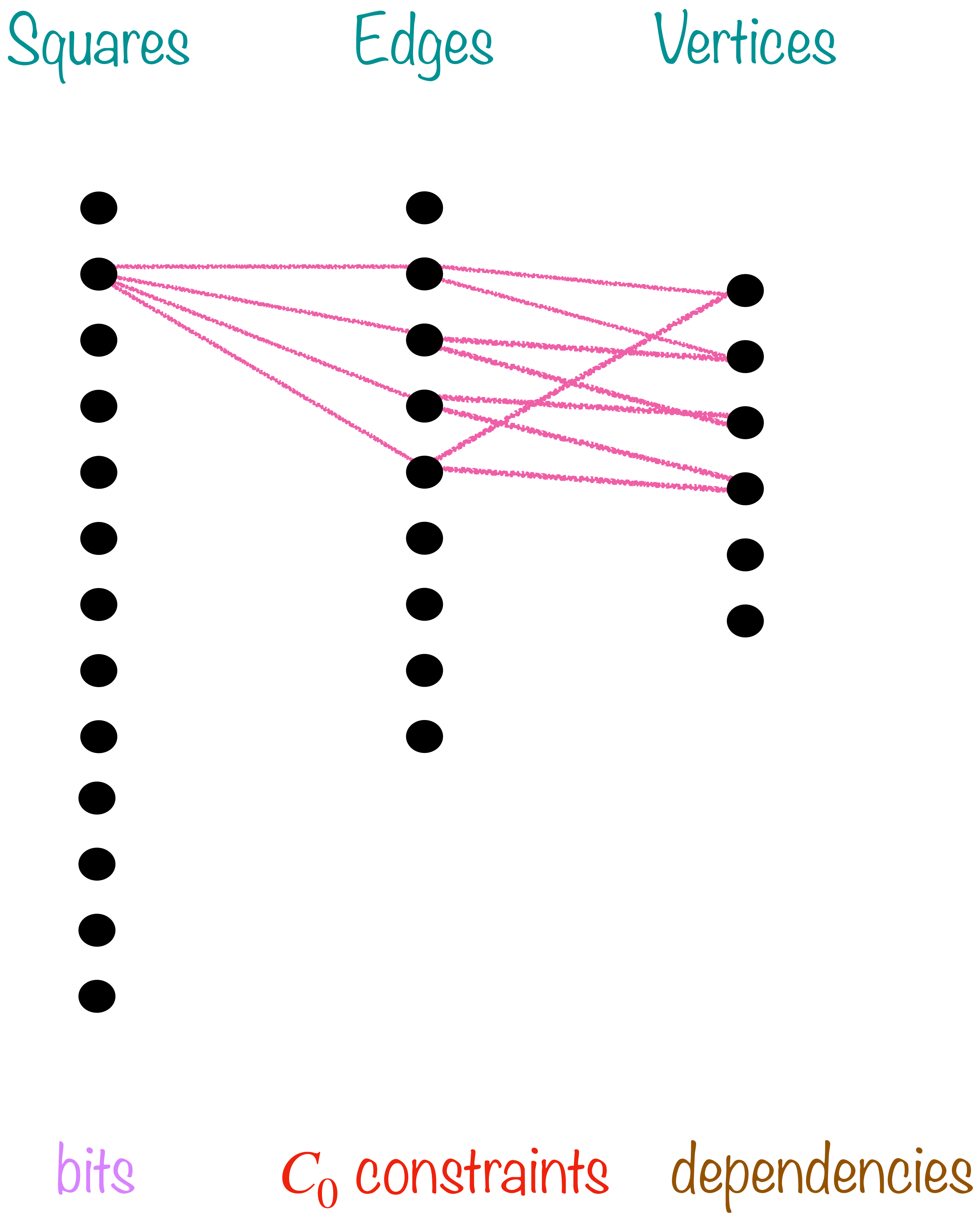
Expander Codes, one level up





Expander Codes, one level up





factor graph

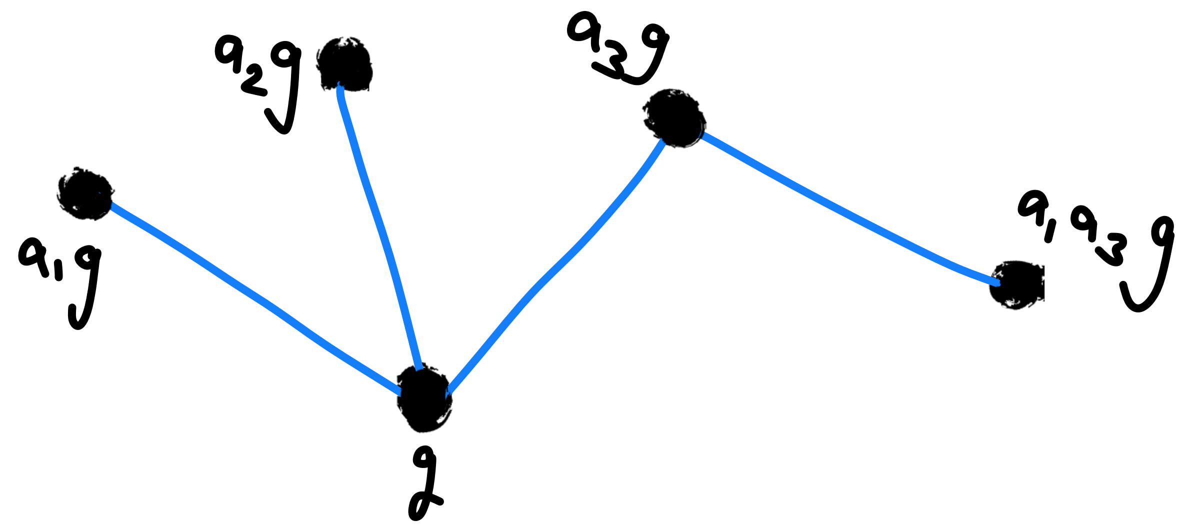
Left-right Cayley Complex

"a graph with squares"

Let G be a finite group,

Let $A \subset G$ be closed under taking inverses, i.e. such that $a \in A \;\rightarrow\; a^{-1} \in A$

Cay(G,A) is a graph with vertices G, and edges $E_A = \{\{g, ag\} : g \in G, a \in A\}$

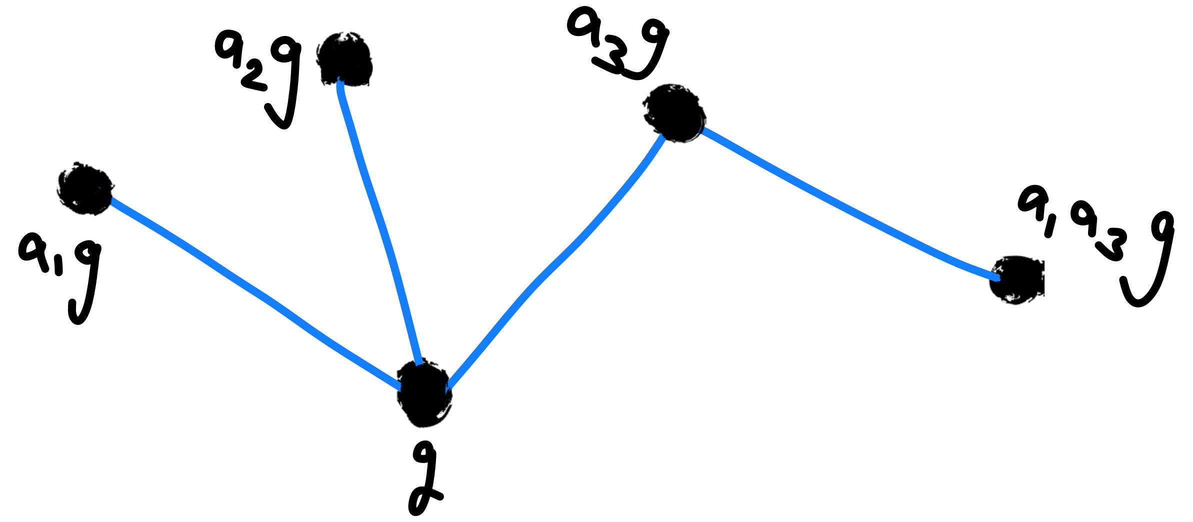


Left-right Cayley Complex

"a graph with squares"

Let G be a finite group,

Let $A, B \subset G$ be closed under taking inverses



Left-right Cayley Complex

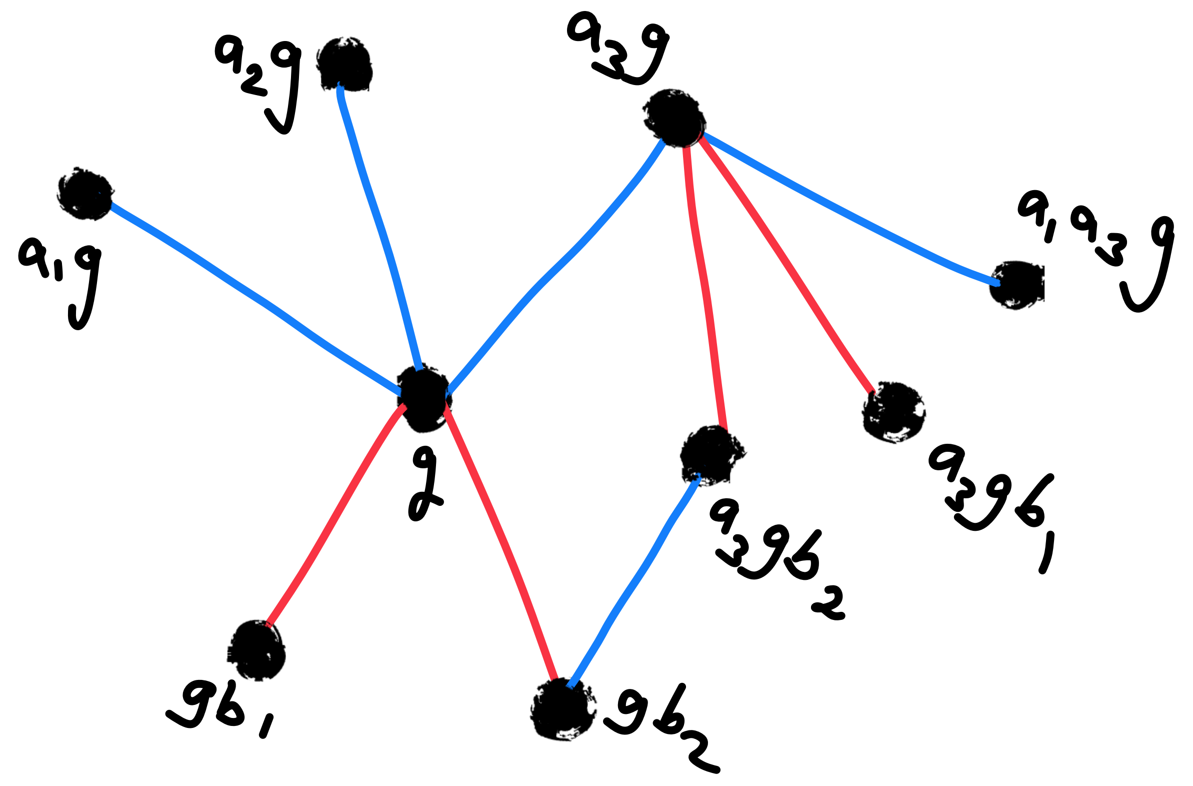
"a graph with squares"

Let G be a finite group,

Let $A, B \subset G$ be closed under taking inverses

Cay(G,A) is a graph with vertices G, and edges $E_A = \{\{g, ag\} : g \in G, a \in A\}$ (left *)

Cay(G,B) is a graph with vertices G, and edges $E_B = \{\{g, gb\} : g \in G, b \in B\}$ (right *)



Left-right Cayley Complex

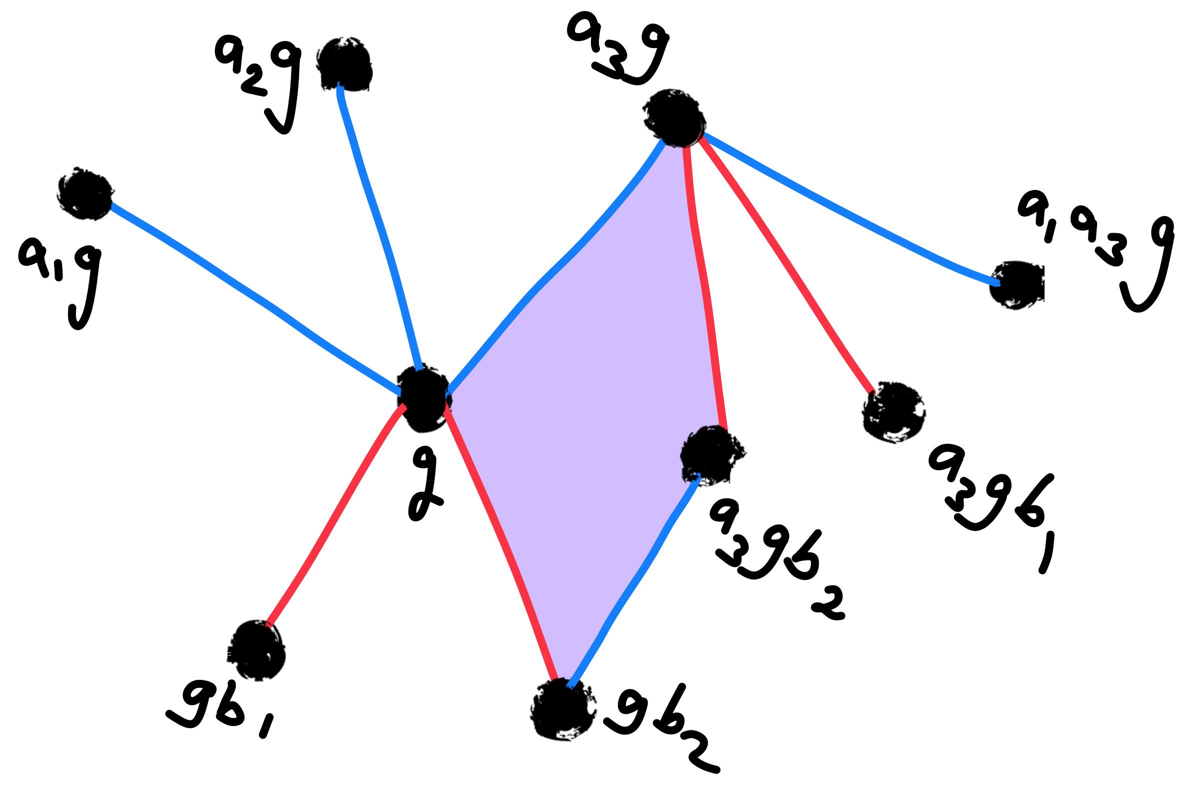
"a graph with squares"

Let G be a finite group,

Let $A, B \subset G$ be closed under taking inverses

Cay(G,A) is a graph with vertices G, and edges $E_A = \{\{g, ag\} : g \in G, a \in A\}$ (left *)

Cay(G,B) is a graph with vertices G, and edges $E_B = \{\{g, gb\} : g \in G, b \in B\}$ (right *)



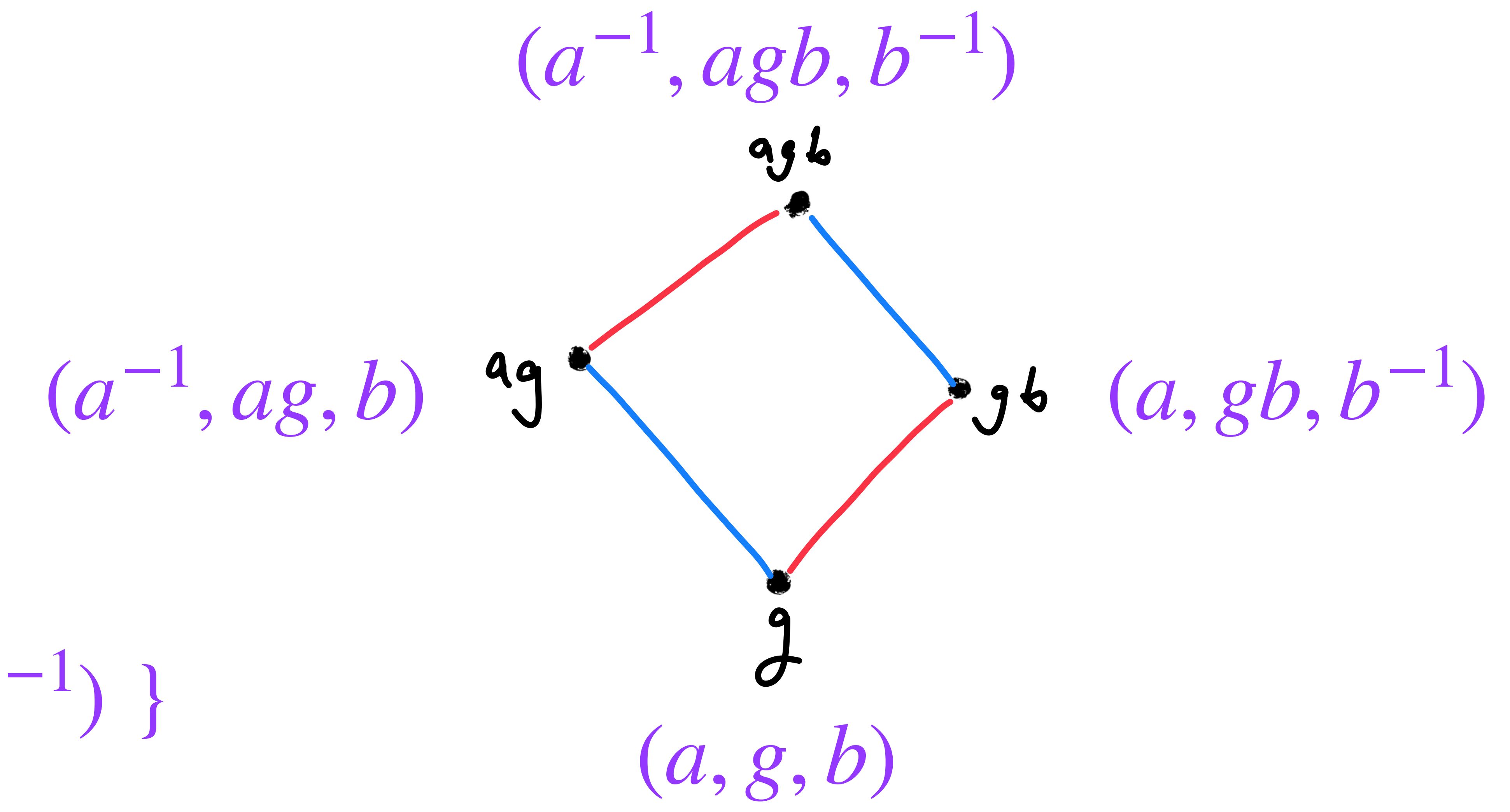
Left-right Cayley Complex

"a graph with squares"

Each triple $a \in A, g \in G, b \in B$ define a rooted square (a, g, b)

Each square can have 4 roots,

$[a, g, b] = \{\ (a, g, b), \quad (a^{-1}, ag, b), \quad (a^{-1}, agb, b^{-1}), \quad (a, gb, b^{-1})\ \}$



This square naturally contains

- The edges {g,ag}, {g,gb}, {gb,agb}, {ag,agb},
- The vertices g,ag,gb,agb

The set of squares is $X(2) = \{[a, g, b] : g \in G, a \in A, b \in B\} \ = \ A \times G \times B / \sim$

Left-right Cayley Complex Cay²(A,G,B)

Let G be a finite group, and let $A, B \subset G$ be closed under taking inverses.

The left-right Cayley complex Cay²(A,G,B) has

- Vertices G
- Edges $E_A \cup E_B$

$$E_A = \{\{g, ag\} : g \in G, a \in A\}, \quad E_B = \{\{g, gb\} : g \in G, b \in B\}$$

- Squares A x G x B / ~

We say that Cay²(A,G,B) is a λ-expander if Cay(G,A) and Cay(G,B) are λ-expanders.

Lemma: For every $\lambda > 0$ there are explicit infinite families of bounded-degree left-right Cayley complexes that are λ-expanders.

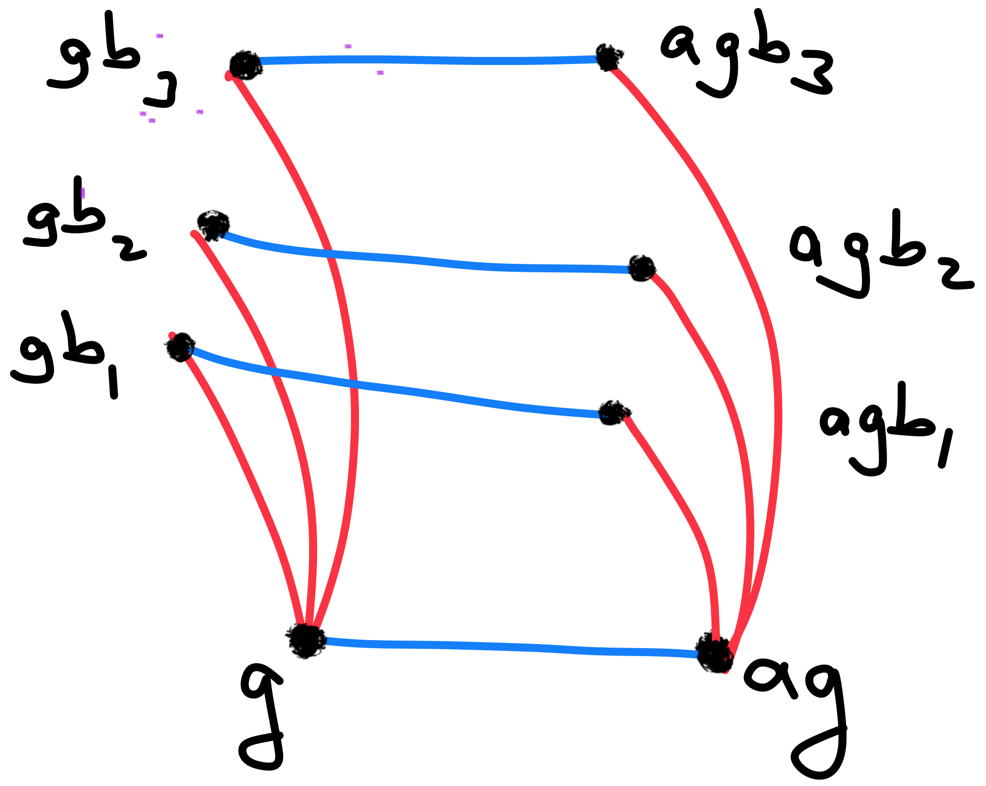
Left-right Cayley Complex

"a graph with squares"

Squares touching the edge {g,ag}

are naturally identified with B

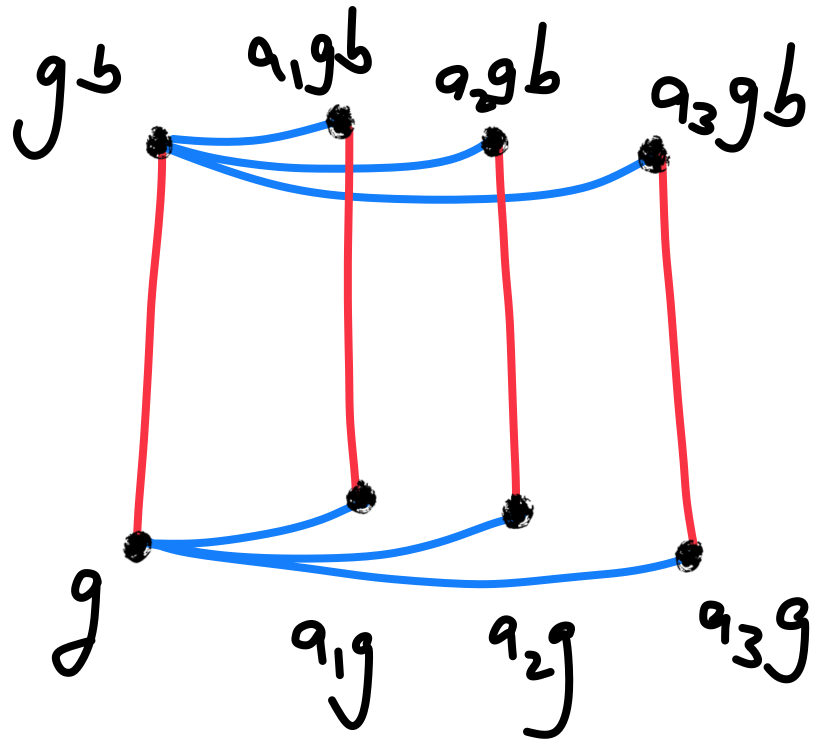
$$b \mapsto [a, g, b]$$



Squares touching the edge {g,gb}

are naturally identified with A

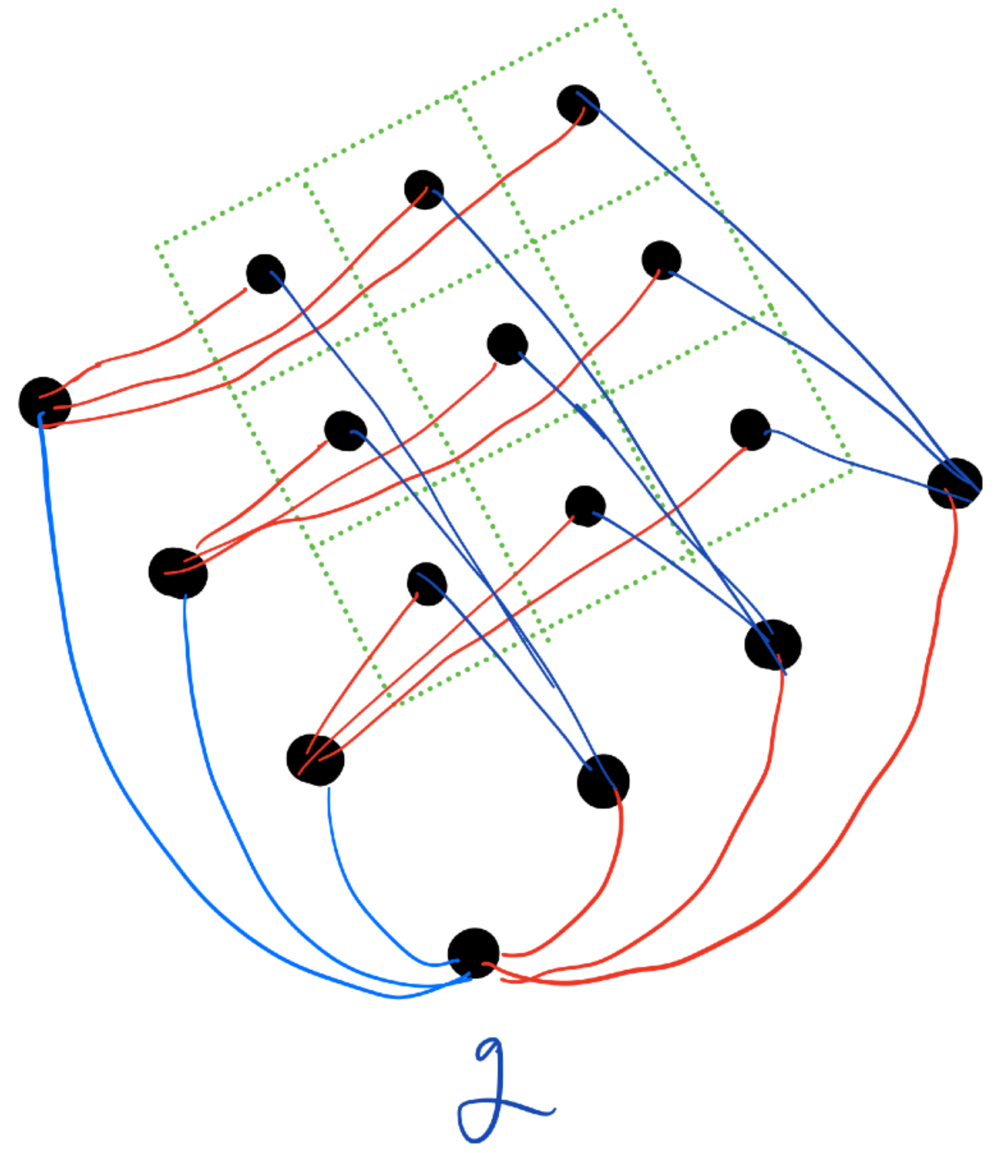
$$a \mapsto [a, g, b]$$



A vertex g has |A| + |B| neighbors

For each $a \in A, b \in B$ there is one square touching g,

so there is a natural bijection* $(a, b) \mapsto [a, g, b]$



* it is a bijection assuming $\forall a, b, g, \quad g^{-1}ag \neq b$

Left-right Cayley Complex

"a graph with squares"

Squares touching the edge {g,ag}

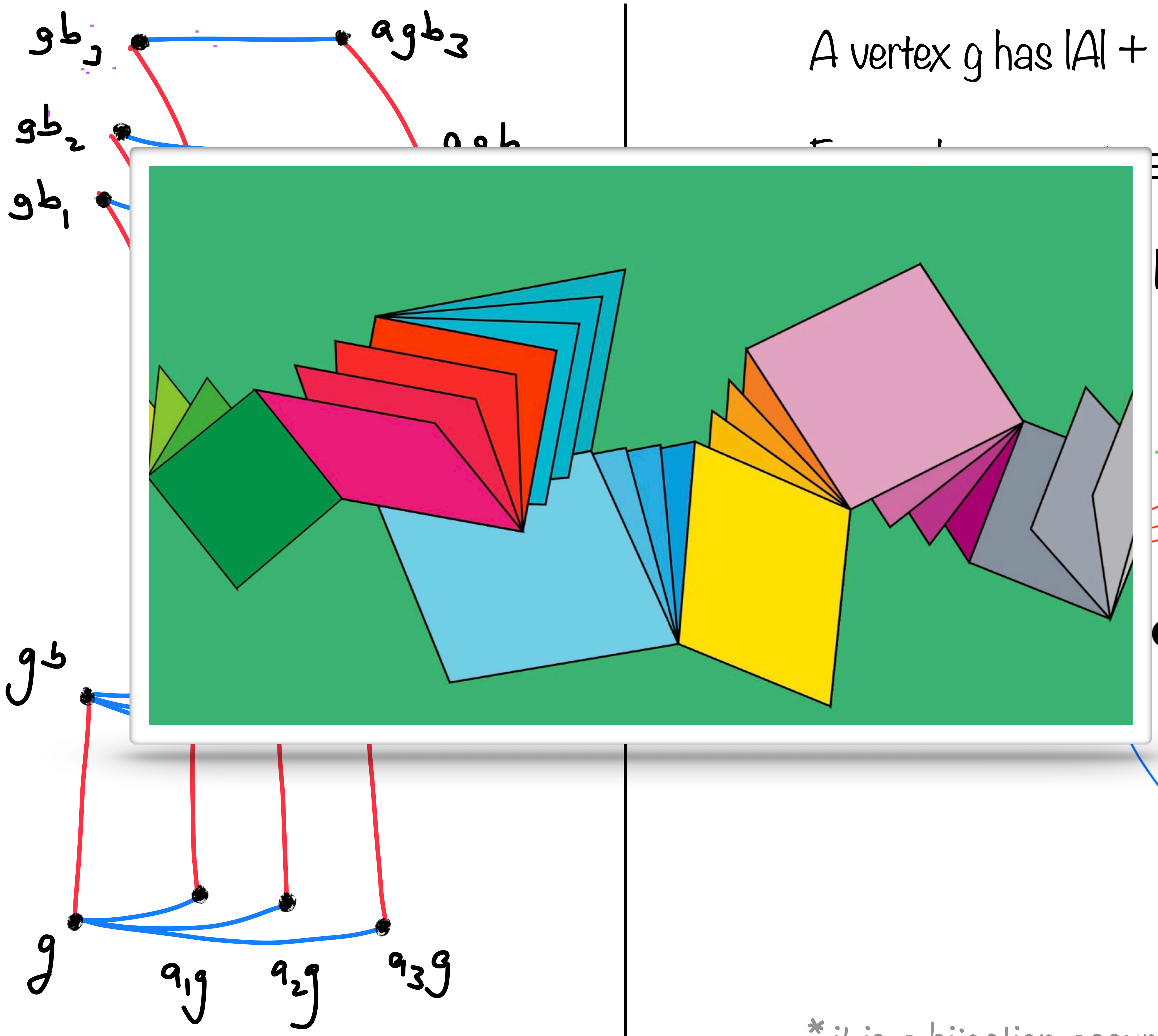
are naturally identified with B

$b \mapsto [a, g, b]$

Squares touching the edge {g,gb}

are naturally identified with A

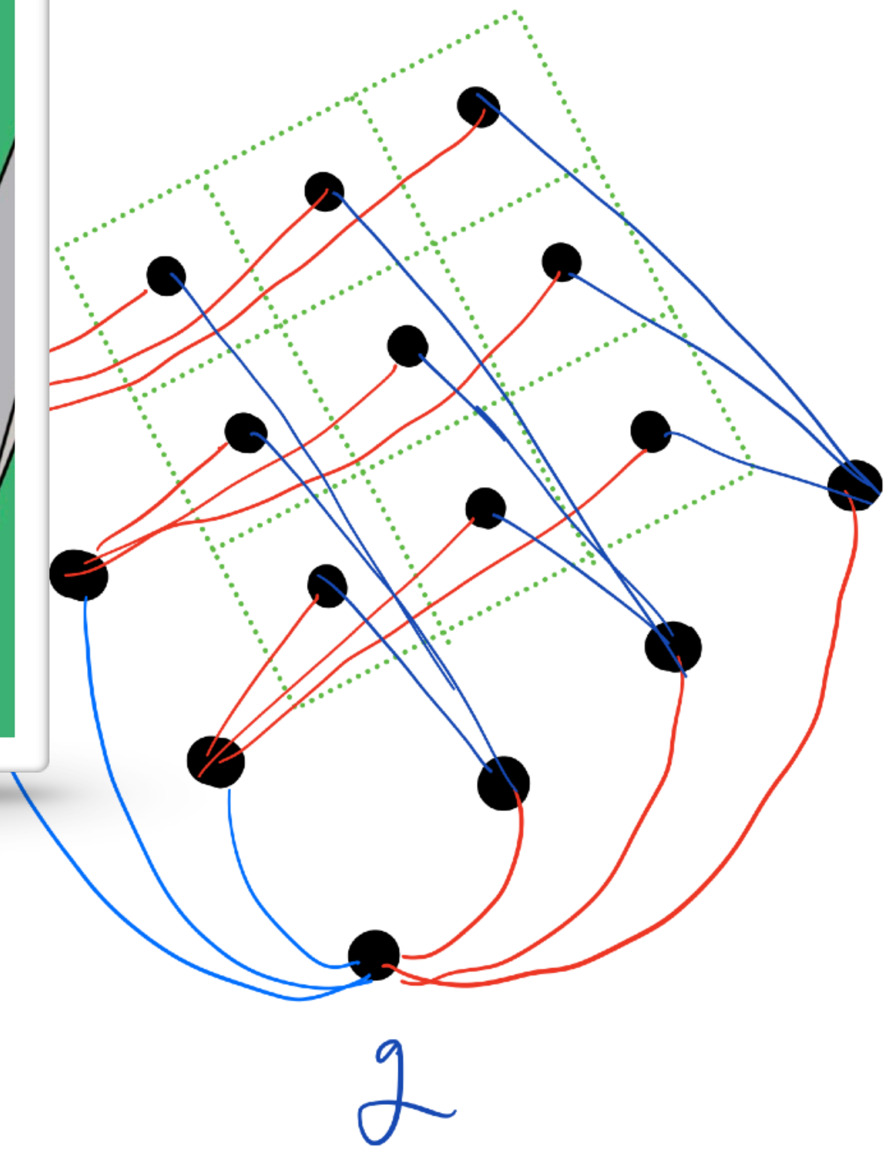
$a \mapsto [a, g, b]$



A vertex g has |A| + |B| neighbors

F… B there is one square touching g,

bijection* $(a, b) \mapsto [a, g, b]$



* it is a bijection assuming $\forall a, b, g, \quad g^{-1}ag \neq b$

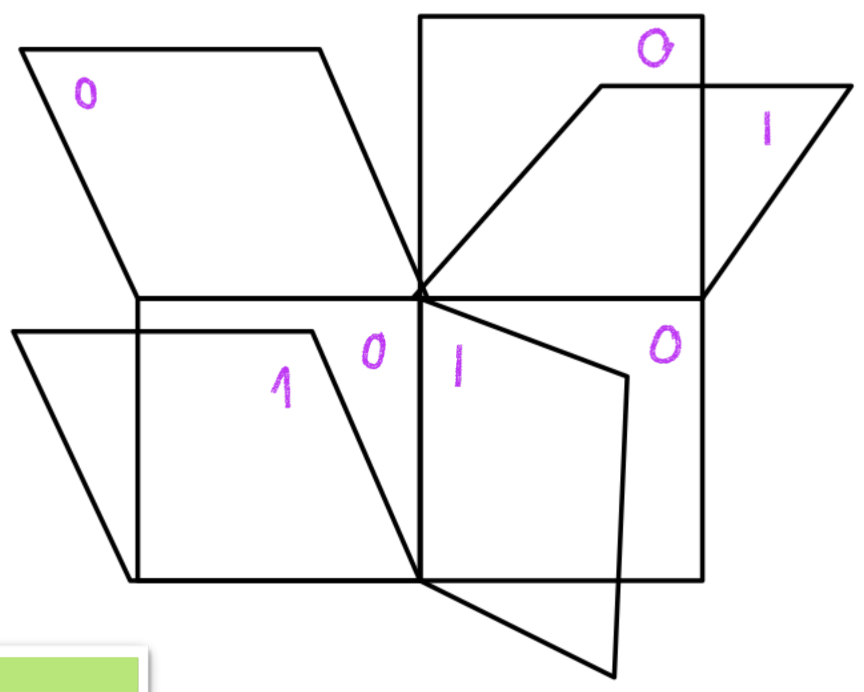
The Code

Let Cay^2(A,G,B) be a left-right Cayley complex.

Fix base codes $C_A \subseteq \{0,1\}^A, C_B \subseteq \{0,1\}^B$ (assuming $|A| = |B| = d$ we can take one base code $C_0 \subseteq \{0,1\}^d$ and let $C_A, C_B \simeq C_0$)

Define a code CODE = $C[G, A, B, C_A, C_B]$:

- The codeword bits are placed on the squares
- Each edge requires that the bits on the squares around it are in the base code



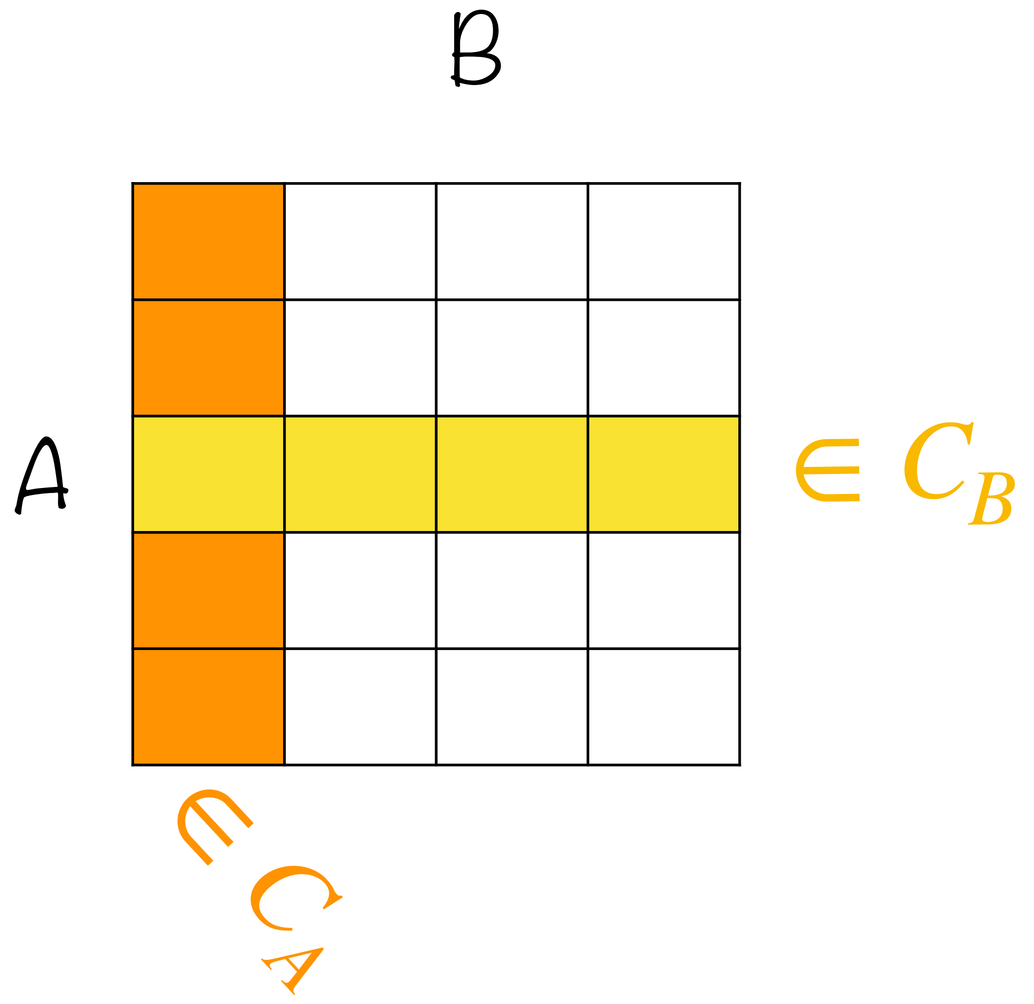
CODE = $\{f : Squares \to \{0,1\} : \forall a, g, b, \quad f([\cdot, g, b]) \in C_A, f([a, g, \cdot]) \in C_B\}$

Rate: $\geq 4r_0 - 3$ [calc: #squares - #constraints]

Distance: $\geq \delta_0^2(\delta_0 - \lambda)$ [easy propagation argument]

Local views are tensor codes

<u>Claim:</u> Fix f∈CODE. For each $g \in G$, $f([\cdot, g, \cdot]) \in C_A \otimes C_B$



<u>Theorem:</u> Assume Cay^2(A,G,B) is a λ-expander, and $C_A \otimes C_B$ is ρ-robustly testable. If $\lambda < \delta_0 \rho / 5$, then $C[G, A, B, C_A, C_B]$ is locally testable.

The tester is as follows:

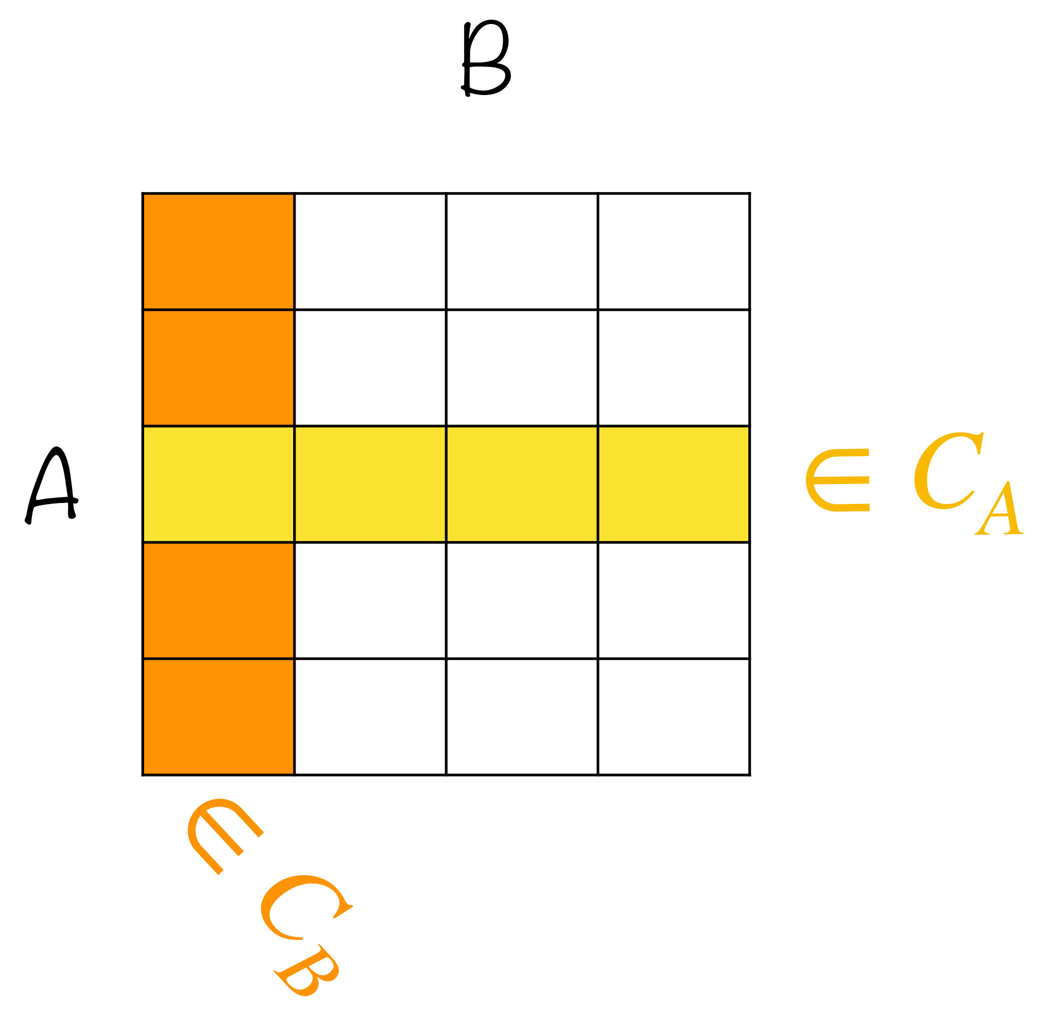
1. Select a vertex g uniformly,
2. Read f on all $|A| \cdot |B|$ squares touching g, namely $f([\cdot, g, \cdot])$.
3. Accept iff this belongs to $C_A \otimes C_B$

Then $\Pr_{g \in G}[f([\cdot, g, \cdot]) \notin C_A \otimes C_B) \geq const \cdot dist(f, C[G, A, B, C_A, C_B])$

CODE = $\{f : Squares \to \{0,1\} : \forall a, g, b, \quad f([\cdot, g, b]) \in C_A, f([a, g, \cdot]) \in C_B\}$

Robustly-testable tensor codes

<u>Definition</u> [Ben-Sasson-Sudan'05]: $C_A \otimes C_B$ is ρ-robustly testable if for all $w : A \times B \to \{0,1\}$, $\rho \cdot dist(w, C_A \otimes C_B) \leq$ row-distance + column-distance



Row-distance : average distance of each row to C_A

Column-distance : average distance of each column to C_B

<u>Lemma [Ben-Sasson-Sudan'05, Dinur-Sudan-Wigderson2006, Ben-Sasson-Viderman2009]:</u>

For every r>0 there exist base codes with rate r and constant distance whose tensors are robustly-testable. (Random LDPC codes, LTCs)

Proof of local-testability

Start with $f : Squares \to \{0,1\}$ and find $f' \in C,\ \ dist(f, f') \cdot const \leq$ rej(f)

ALG "self-correct":

1. Init: Each $g \in G$ finds $T_g \in C_A \otimes C_B$ closest to $f([\,\cdot\,, g, \cdot\,])$

   [define a progress measure Φ = # dispute edges]

2. Loop: If g can change T_g and reduce Φ then do it

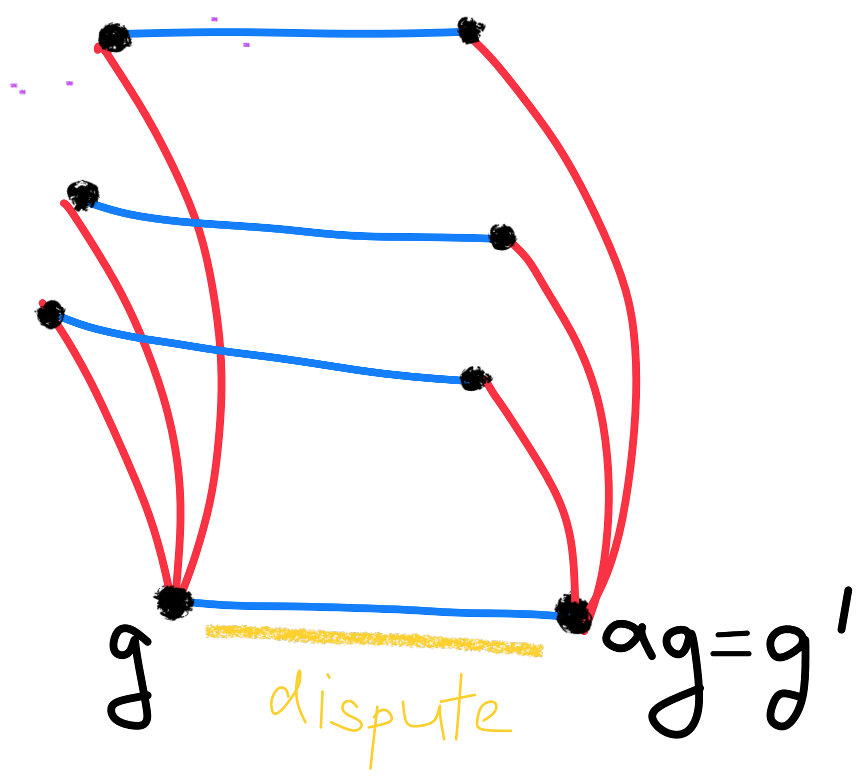
3. End: If $\Phi = 0$ let $f'([a,g,b]) = T_g(a,b)$ and output f', otherwise output "stuck"

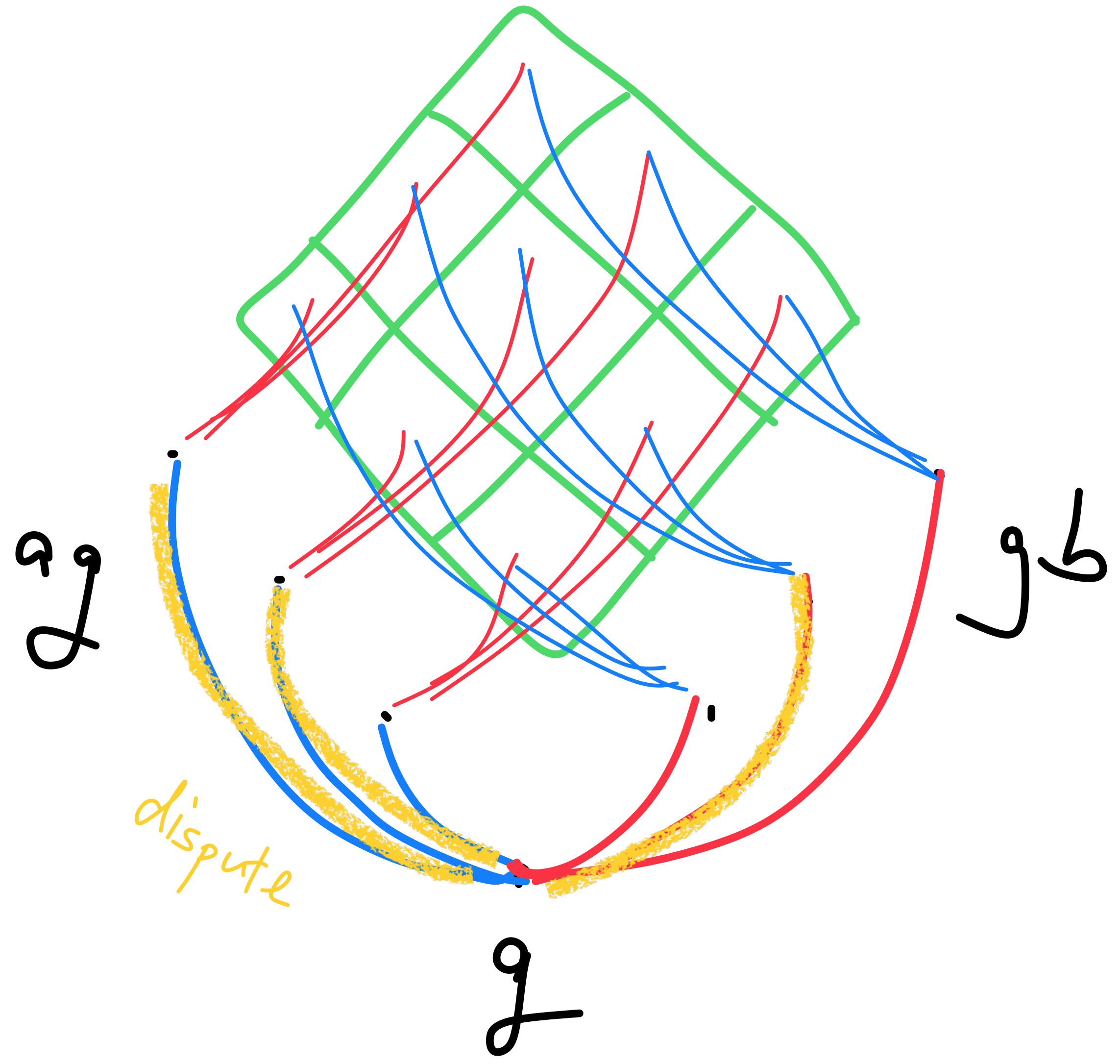
- steps $\leq \Phi\ \approx$ rej(f)
- If output f' then $dist(f, f') \cdot const \leq rej(f)$)
- If get stuck—> rej(f) > 0.1 so $dist(f, f') \cdot 0.1 \leq rej(f)$

Proof of local-testability

If ALG "self-correct" is stuck then rej (f) > 0.1

- If g,g' are in dispute, there must be many squares on {g,g'} with further dispute edges
- Can try to propagate, but, they all might be clumped around g
- But then g's neighbors all agree, so there must have been a better choice for Tg (using the LTCness of tensor codes)
- Random walk on the edges + expansion ==> dispute set is large





Main Result

Theorem: There exist $r, \delta > 0$ and $q \in \mathbb{N}$ and an explicit construction of an infinite family of error-correcting codes $\{C_n\}_n$ with rate $\geq r$, distance $\geq \delta$ and locally testable with q queries.

Proof: Take

1. Family of base codes $\{C_d\}_d$ with rate > ¾ and constant robustness ρ and distance δ
2. Set λ small enough wrt δ and ρ
3. Choose a family $\{Cay^2(A_n, G_n, B_n)\}_n$ of λ expanding left-right Cayley complexes, with $d = |A_n| = |B_n| = O(1/\lambda^2)$
4. Output $\{C[G_n, A_n, B_n, C_d, C_d]\}_n$

High dimensional expansion

The idea of using a higher-dimensional complex instead of a graph for LTCs has been circulating a number of years.

HDXs exhibit local-to-global features: prove something locally and then use expansion to globablize

[Garland 1973, Kaufman-Kazhdan-Lubotzky2014, Evra-Kaufman2016, Oppenheim2017, D.-Kaufman2017, D.-Harsha-Kaufman-LivniNavon-TaShma2018, Anari-Liu-OveisGharan-Vinzant2019]

Dikstein-D.-Harsha-RonZewi2019 proved that if one defines a code on a HDX using a base code that itself is an LTC, (and if there is an agreement-test), then the entire code is an LTC.

Recently also Kaufman-Oppenheim2021 proved a similar "schema".

How to"instantiate" this? ...we worked on the Lubotzky-Samuels-Vishne complexes (quotients of BT buildings), and have conjectured base codes, but no proof of local LTCness

Some questions

- Can one consrtuct LTCs on other HDX's such as LSV simplical complexes?
- Can one construct higher dimensional cubical complexes similarly?
- Can these LTCs be used for constructing PCPs?