Title: Injectivity radius bounds on the minimum distance of quantum LDPC codes

Date: Jul 15, 2014 10:30 AM

URL: http://pirsa.org/14070007

Abstract: Only a rare number of constructions of quantum LDPC codes are equipped with an unbounded minimum distance. Most of them are inspired by Kitaev toric codes constructed from the a tiling of the torus such as, color codes which are based on 3-colored tilings of surfaces, hyperbolic codes which are defined from hyperbolic tilings, or codes based on higher dimensional manifolds. These constructions are based on tilings of surfaces or manifolds and their parameters depend on the homology of the tiling.

In the first part of this talk, we recall homological bounds on the parameters of these quantum LDPC codes. In particular, the injectivity radius of the tiling provides a general lower bound on the minimum distance of these quantum LDPC codes.

Then, we extend the injectivity radius method to bound the minimum distance of a family of quantum LDPC codes based on Cayley graphs.
Finally, we improve these results by studying a notion of expansion of these Cayley graphs.

This talk is based on a joint work with Alain Couvreur and Gilles ZÃ©mor, and a joint work with Zhentao Li and Stephan TommassÃ©.

Injectivity radius bounds on the minimum distance of quantum LDPC codes

Nicolas Delfosse
joint work with Alain Couvreur and Gilles Zémor
joint work with Zhentao Li and Stéphan Thomassé

Université de Sherbrooke

July 15, 2014 - Perimeter Institute


INSTITUTE FOR THEORETICAL P


CAUTION

Injectivity radius bounds on the minimum distance of quantum LDPC codes

Nicolas Delfosse
joint work with Alain Couvreur and Gilles Zémor
joint work with Zhentao Li and Stéphan Thomassé

Université de Sherbrooke

July 15, 2014 - Perimeter Institute

Motivation

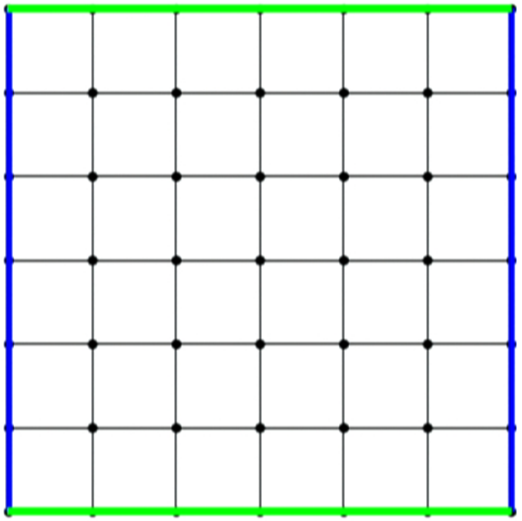
- A beautiful combinatorial problem! Connected to fascinating questions in topology and graph theory.
- Stricking difference with the classical setting:
  - Classical LDPC codes: $d = \Omega(n)$.
  - Quantum LDPC codes
    from classical constructions: $d = O(1)$
    from Kitaev idea: $d = O(\sqrt{n})$
- Key ingredient: degeneracy.

Outline

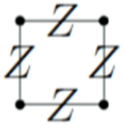
- Topological Codes
  - Injectivity radius bounds for toric codes
  - Hyperbolic codes
  - Higher dimensional codes
- Cayley Graphs Codes
  - Injectivity radius bound
  - Homological expansion

Kitaev's toric codes (Kitaev - 1997)

- Place a qubit (state of $\mathcal{H} = \mathbb{C}^2$) on each edge of a torus.
- This gives a global state $|\psi\rangle \in \mathcal{H}^{\otimes n}$ with $n = |E|$.



Site operator $X_v =$ 

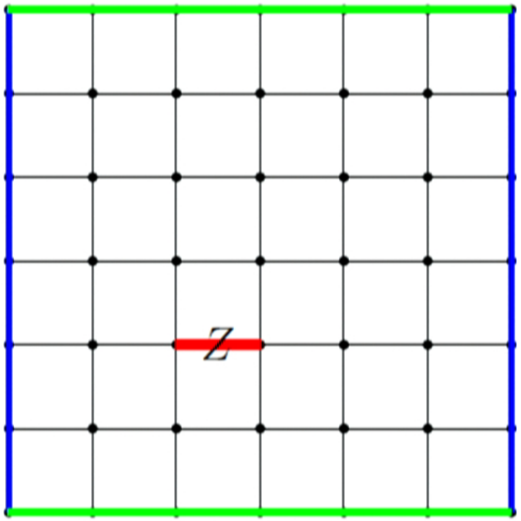
Face operator $Z_f =$ 

- The X_v and Z_f commute.

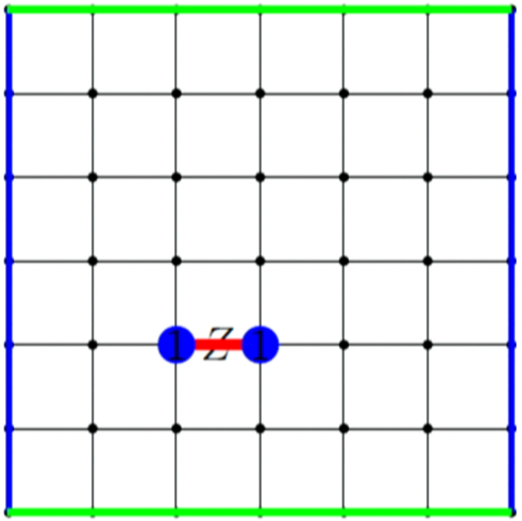
The toric code is the set of states $|\psi\rangle \in \mathcal{H}^{\otimes n}$ such that:

$$X_v|\psi\rangle = |\psi\rangle \text{ and } Z_f|\psi\rangle = |\psi\rangle \quad \forall v, \forall f.$$

Minimum distance fo the toric code

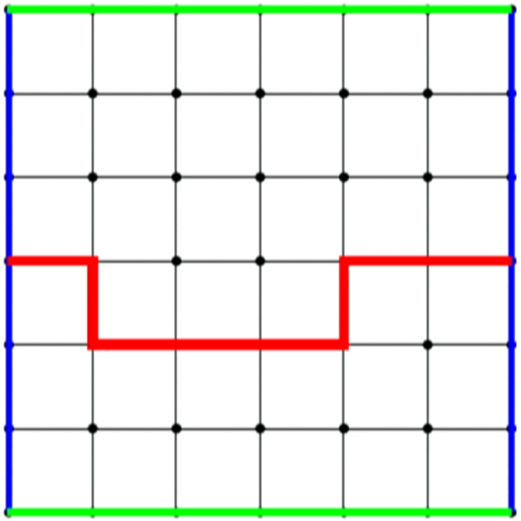


Minimum distance fo the toric code



- We detect the end-points of the error chains.

Minimum distance fo the toric code



- We detect the end-points of the error chains.
- Undetectable errors = cycles.
- Degeneracy: sum of faces have no effect.

Injectivity radius of the torus

Question: Why do we have $d = \Omega(n^{1/2})$?

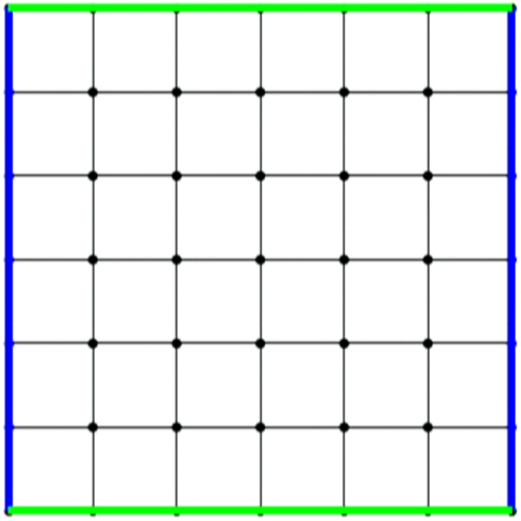


Figure : A ball in the square tiling of the torus

Injectivity radius of the torus

Question: Why do we have $d = \Omega(n^{1/2})$?

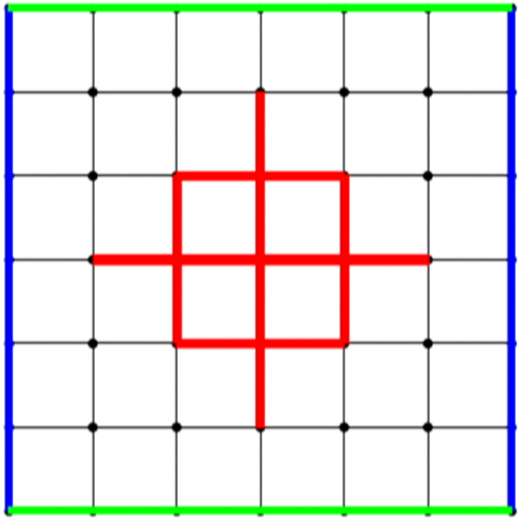


Figure : A ball in the square tiling of the torus

In the $m \times m$ tiling:

- No identification till the radius $(m-1)/2$.
- It is the same thing around each vertex.

Injectivity radius of the torus

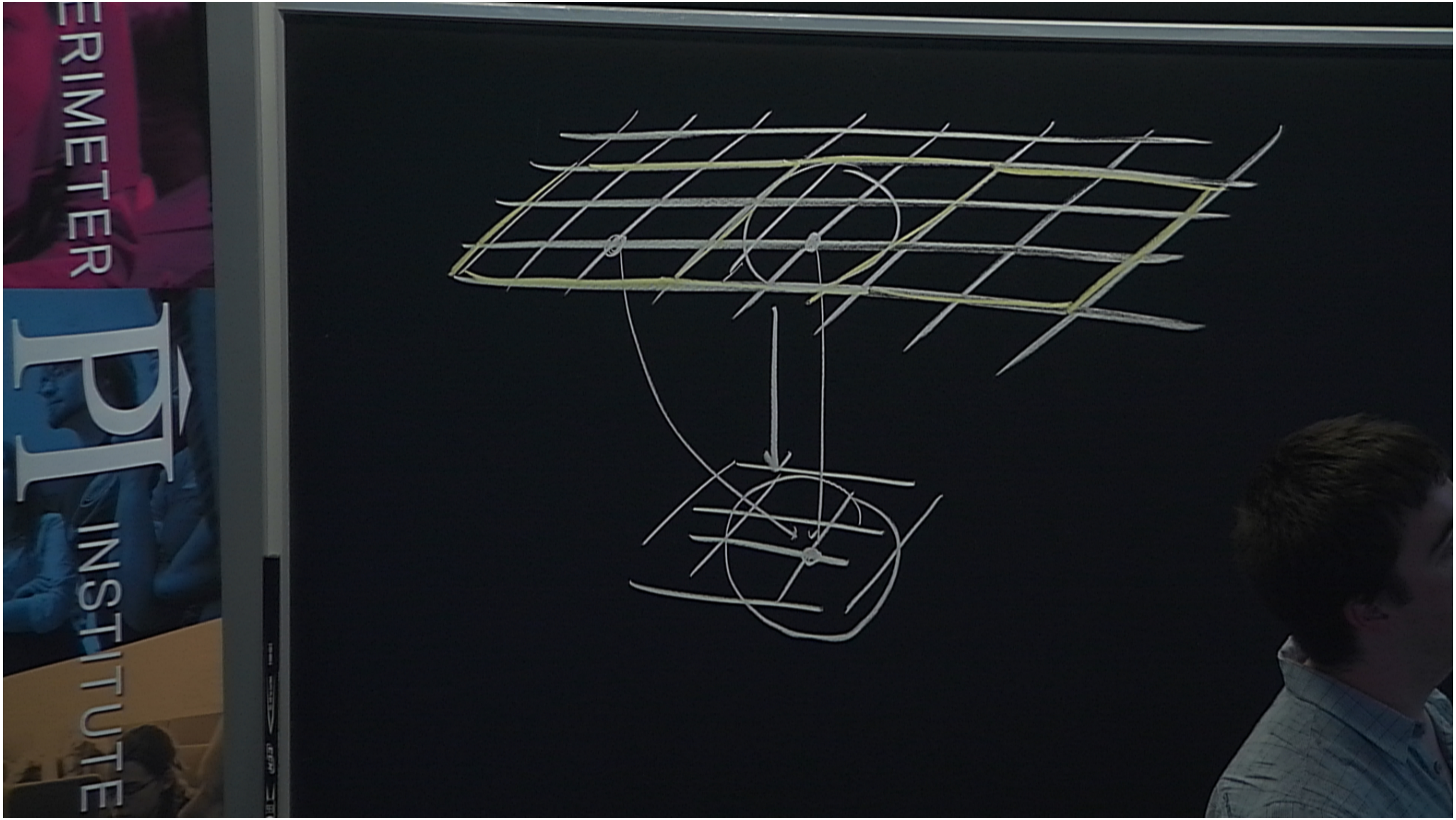
The torus is locally isomorphic to $\mathbb{Z}^2$:

$$B_{T_m}\left(x, \frac{m-1}{2}\right) \simeq B_{\mathbb{Z}^2}\left(0, \frac{m-1}{2}\right)$$

The injectivity radius is $(m-1)/2$.

Injectivity radius bound:
If a cycle is in a small ball of the torus
$\Rightarrow$ it is a cycle in $\mathbb{Z}^2$
$\Rightarrow$ it is a sum of faces
$\Rightarrow$ it doesn't appear in the computation of d

Conclusion : $d \geq m$. This proves that $d = \Omega(\sqrt{n})$


ERIMETER
PI
INSTITUTE

Bravyi-Poulin-Terhal bound

A number of constructions based on a square tiling have been proposed: with boundaries (Bravyi, Kitaev '98), with holes (Denis, Kitaev, Landahl, Preskill - '02), color toric codes (Bombin, Martin-Delgado - '06), ...

All these codes are subjected to the tradeoff:

Theorem (Bravyi, Poulin, Tehral - 2009)

The parameters $[[n, k, d]]$ of a local CSS code defined in a square lattice satisfy:

$$kd^2 \leq Cn.$$

Consequence:

- $R = k/n$ constant with growing d is impossible
- $d = O(\sqrt{n})$

Codes beating Bravyi-Poulin-Terhal bound

2 directions to go beyond Bravyi-Poulin-Terhal bound:

- Leave Euclidean geometry
- Go to higher dimension

Surface

Surface (orientable) = g torus stuck together.
The number of holes g is called the genus.

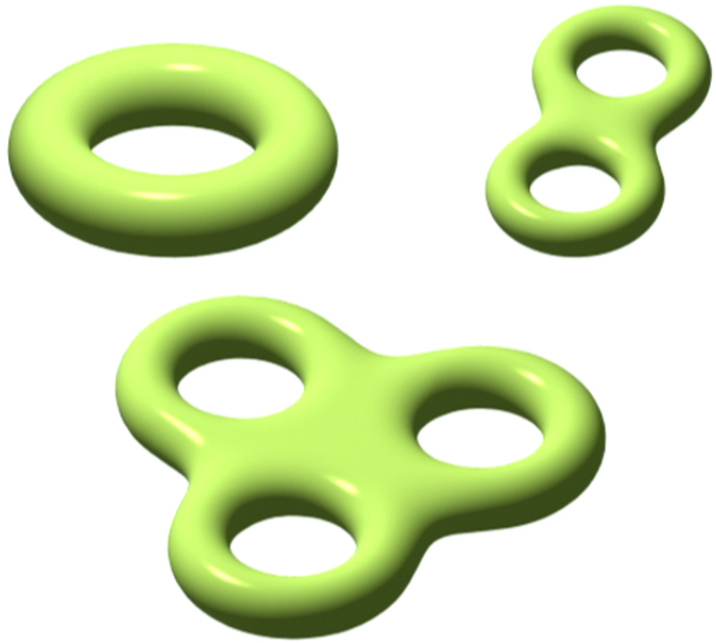


Figure : Surfaces of genus $g = 1$, 2 and 3.

Surface codes

Every finite tiling of surface G defines a surface code by:

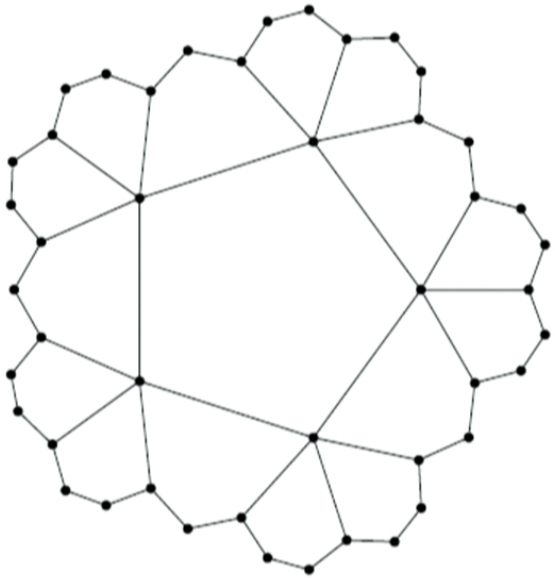
- X_v = site operators
- Z_f = face operators

Then undetectable errors are cycles and sum of faces have no effect

- $n = |E|$
- $k = 2g$
- d = shortest length of a cycle which is not a sum of faces

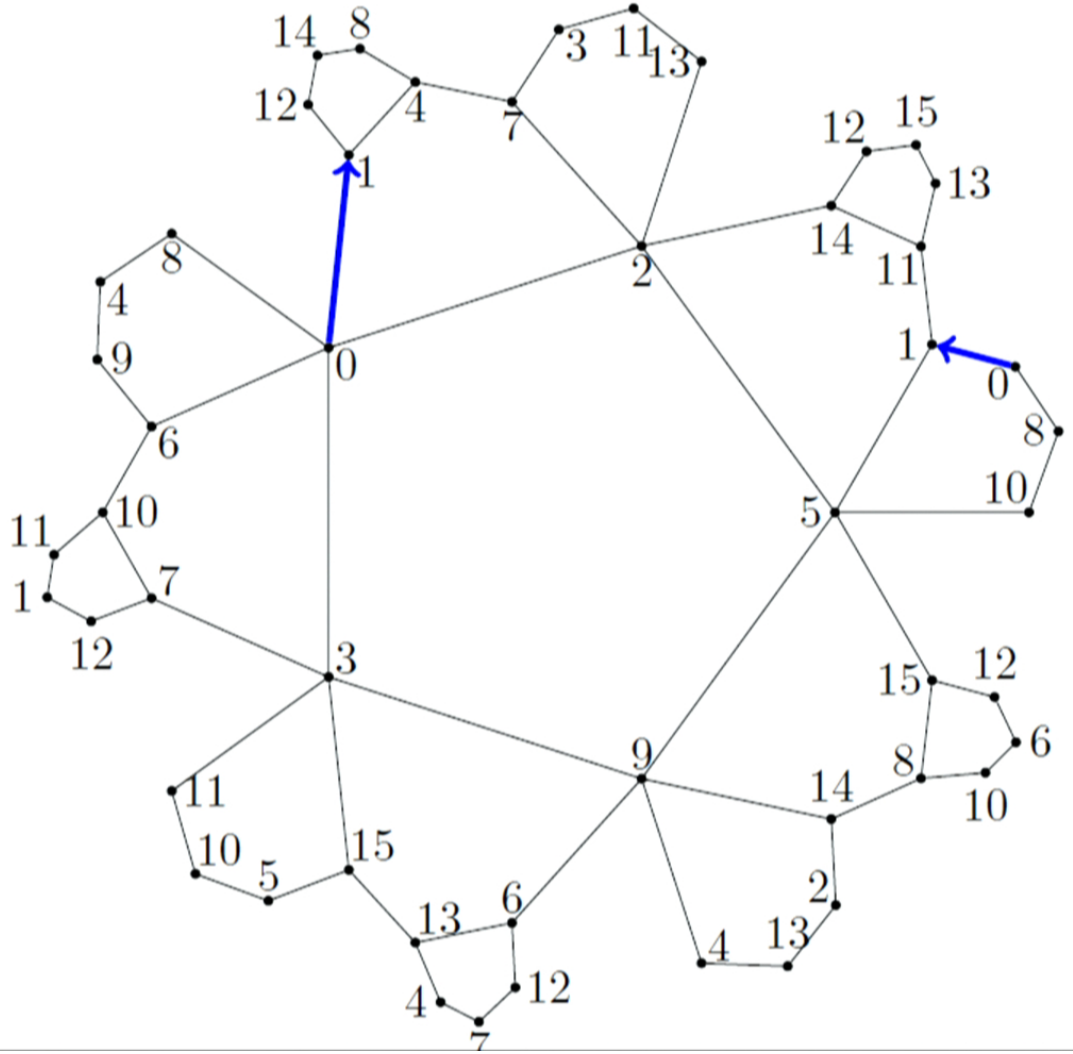
We want a non-Euclidean tiling.

infinite hyperbolic lattices

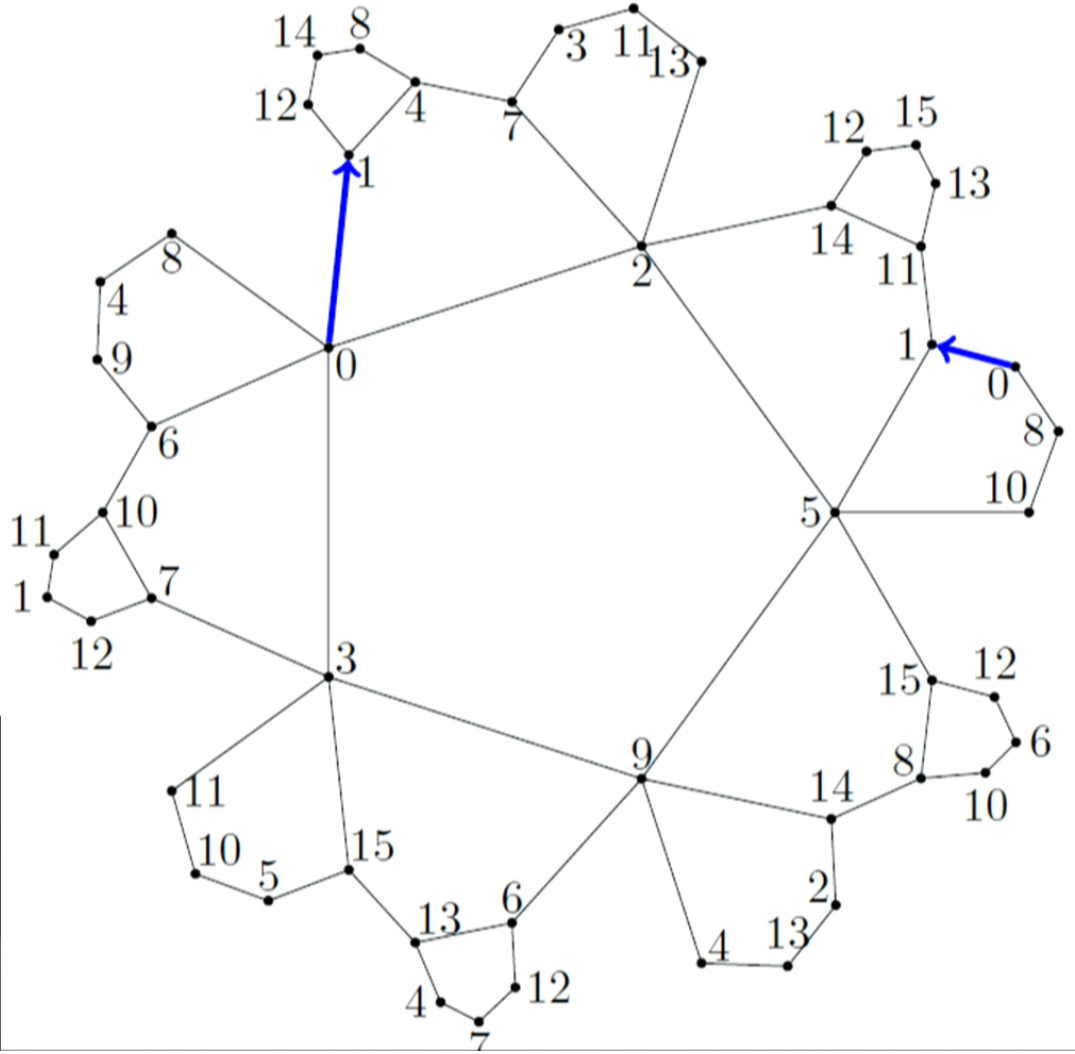


A 5-regular infinite hyperbolic lattice. To construct a surface code, take a finite quotient of this graph.

A regular tiling of genus $g = 5$



A regular tiling of genus $g = 5$



Parameters of hyperbolic codes

Hyperbolic surface codes beat than BPT tradeoff:

- constant rate $R = k/n$
- distance $d = \Omega(\log n)$

(Freedman, Meyer, Luo, - 2001, Zémor - 2009)

Hyperbolic color codes with the same parameters (D - 2013).

Questions:

- Can we have hyperbolic codes with a better distance?
- Is there a general tradeoff that encompass these codes!

Systole of a Riemannian manifold

$\mathcal{V}$ a closed, connected surface of genus $g \geq 2$, endowed with a Riemannian metric.

Definition

syst := length of the shortest cycle that is not a boundary.

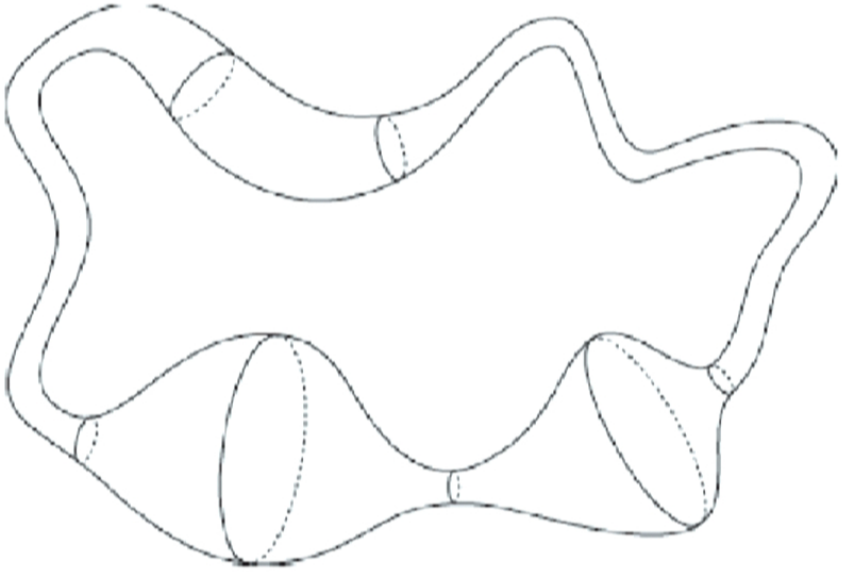


Figure : Where is the systole of this torus?

Systole of a Riemannian manifold

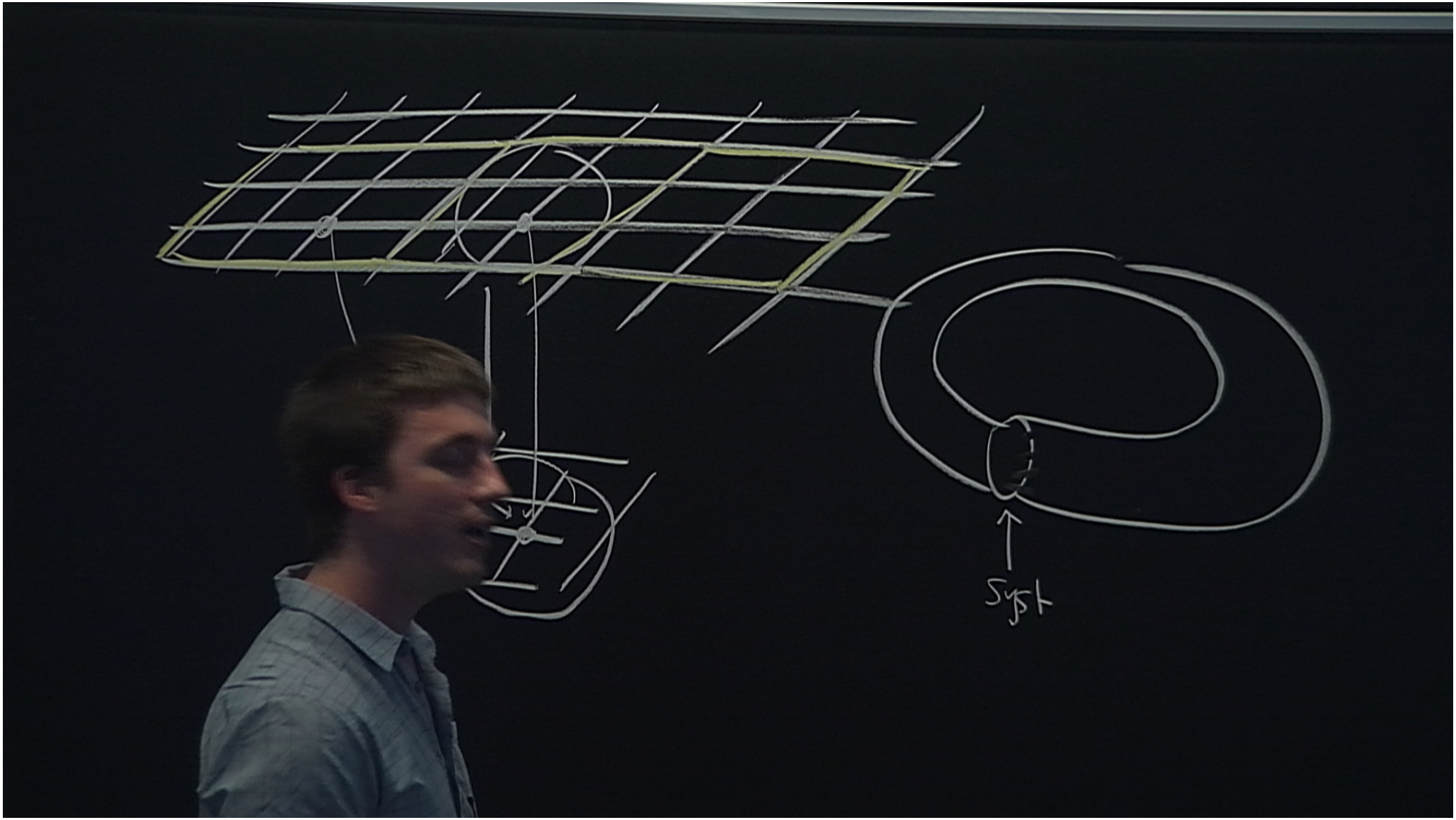
Two Remarks:

- When we fixe the systole, the area can not be too small.

Question: What is the smallest area of a surface, given its systole?

- If we add holes, the volume can be larger.

When g is large the area of the surface can be larger.


Syst

Systole of a Riemannian manifold

Theorem (Gromov - 1992)

$$(\text{syst})^2 \leq C \frac{(\log g)^2}{g} \text{Area}(\mathcal{V}).$$

To apply this result to surface codes, construct a metric s.t.:

- Area is proportional to the number of faces
- syst corresponds to the distance d
- g is proportional to the dimension k

Systole of a Riemannian manifold

Theorem (Gromov - 1992)

$$(\text{syst})^2 \leq C \frac{(\log g)^2}{g} \text{Area}(\mathcal{V}).$$

To apply this result to surface codes, construct a metric s.t.:

- Area is proportional to the number of faces
- syst corresponds to the distance d
- g is proportional to the dimension k

Topological codes in dimension D

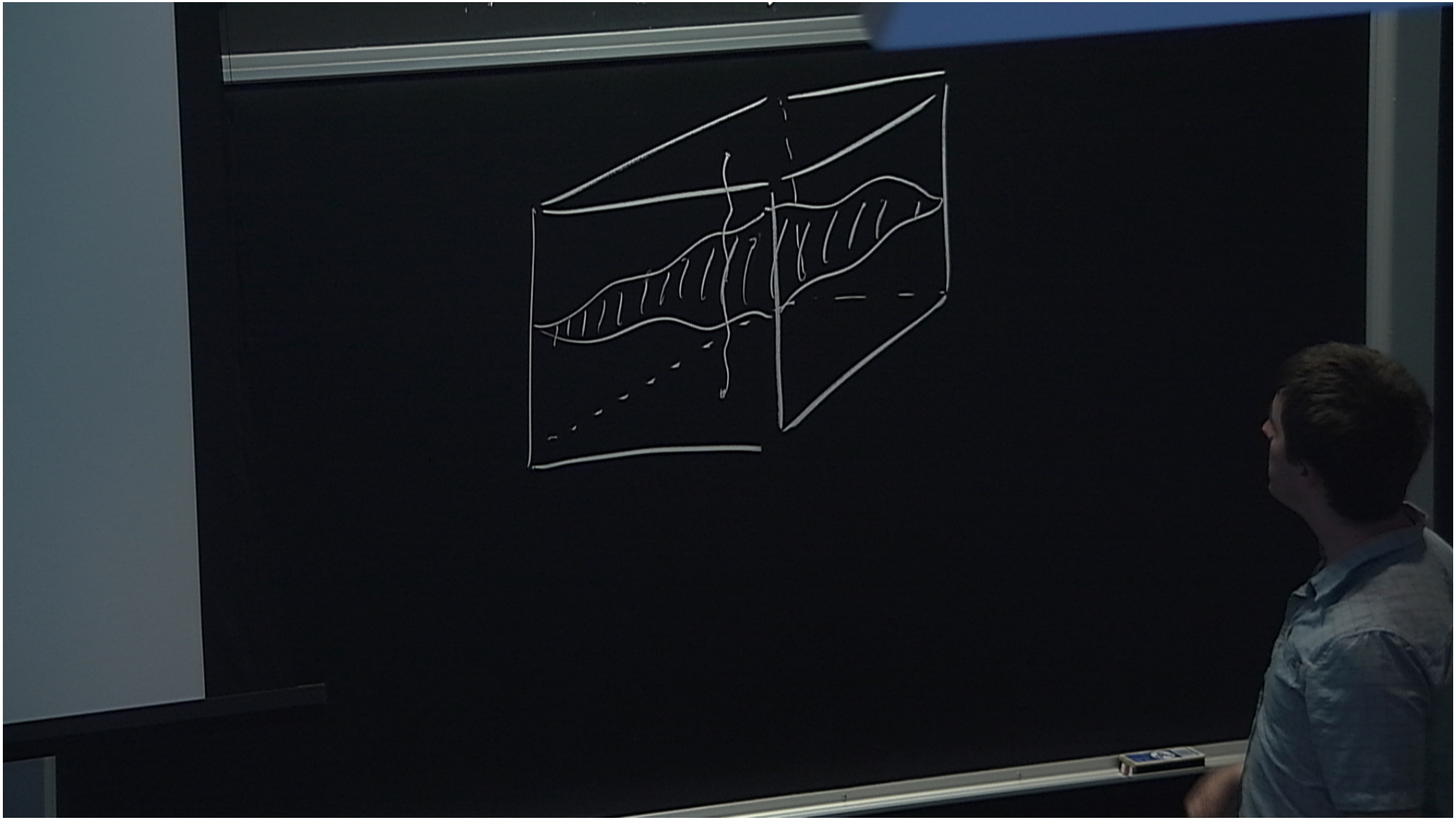
Every finite tiling of a D-manifold defines homological codes:

- place qubits on the t-cells, X_v on the $t-1$-cells, Z_f on the $t+1$-cells.
- $X_v = t$-cells incident to v (site operators)
- $Z_f = t$-cells included in f (face operators)

Then

- Undetectable Z-errors are t-cycles of the tiling
- Undetectable X-errors are $(D-t)$-cycle of the dual tiling
- $d =$ shortest length of a t-cycle of the tiling or a $(D-t)$-cycle of its dual which is not a boundary.

Question: Tradeoff between the t-systole and the $(D-t)$-systole of a D-manifold?



Systolic freedom

- t-syst = minimum volume of a t-cycle which is not a boundary.

By examining the D-dimensional toric code, we could imagine that

$$(t - \text{syst}) \times ((D - t) - \text{syst}) = O(Vol(\mathcal{M}_D))$$

But we can beat this bound using 3-manifolds. This leads to a distance $d = \Omega(\sqrt{n \log n})$.
(Freedman, Meyer and Luo - 2002).

Systolic freedom

- t-syst = minimum volume of a t-cycle which is not a boundary.

By examining the D-dimensional toric code, we could imagine that

$$(t - \text{syst}) \times ((D - t) - \text{syst}) = O(Vol(\mathcal{M}_D))$$

But we can beat this bound using 3-manifolds. This leads to a distance $d = \Omega(\sqrt{n \log n})$.
(Freedman, Meyer and Luo - 2002).

Quantum LDPC codes based on Cayley graphs

The Cayley graph

$H \in M_{r,n}(\mathbb{F}_2)$ of rank r with n even.
G the Cayley graph of $\mathbb{F}_2^r$ modulo the columns c_i of H.
A the adjacency matrix of G.

Proposition (MacKay, Mitchison, Shokrollahi - 07)

The matrix A defines a stabilizer code of length $N = 2^r$.

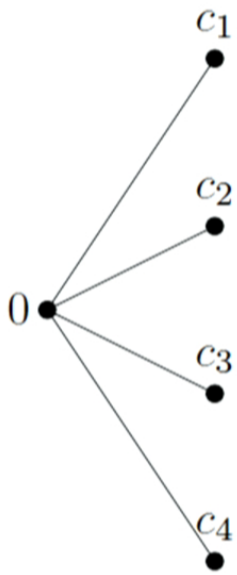
The weight of the stabilizer generators is n.

The Cayley graph

We can associate a stabilizer code to this graph:

- Stabilizers are generated by the X-spheres and the Z-spheres
- Undetectable errors = commute with the spheres

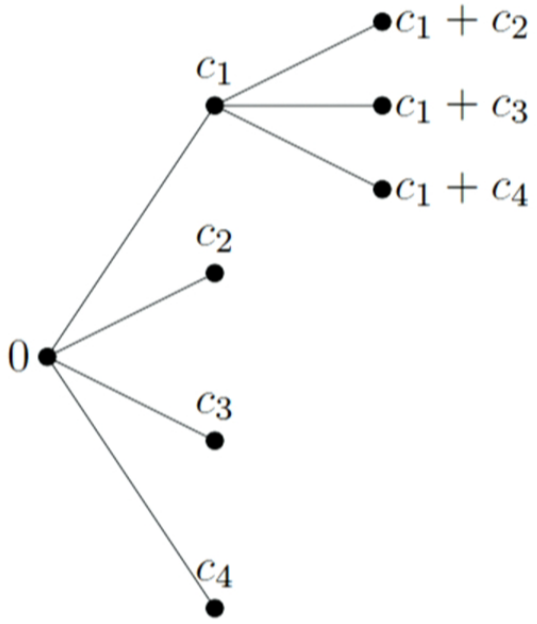
The Cayley graph



We can associate a stabilizer code to this graph:

- Stabilizers are generated by the X-spheres and the Z-spheres
- Undetectable errors = commute with the spheres

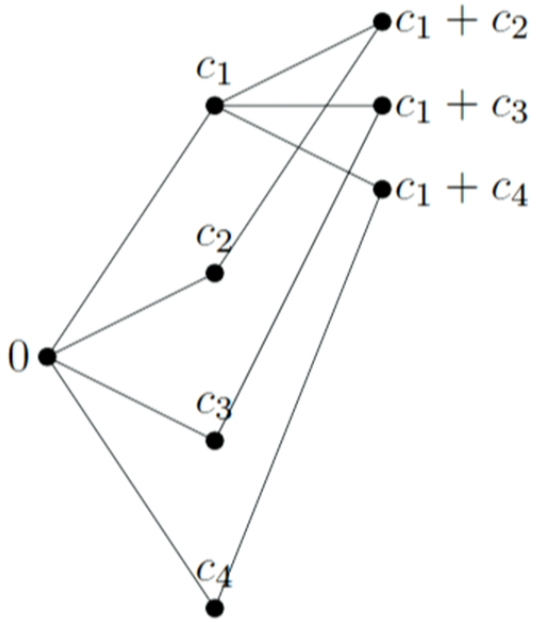
The Cayley graph



We can associate a stabilizer code to this graph:

- Stabilizers are generated by the X-spheres and the Z-spheres
- Undetectable errors = commute with the spheres

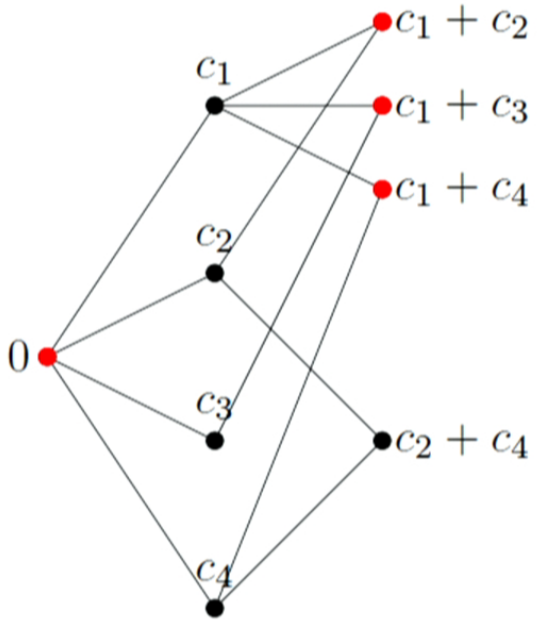
The Cayley graph



We can associate a stabilizer code to this graph:

- Stabilizers are generated by the X-spheres and the Z-spheres
- Undetectable errors = commute with the spheres

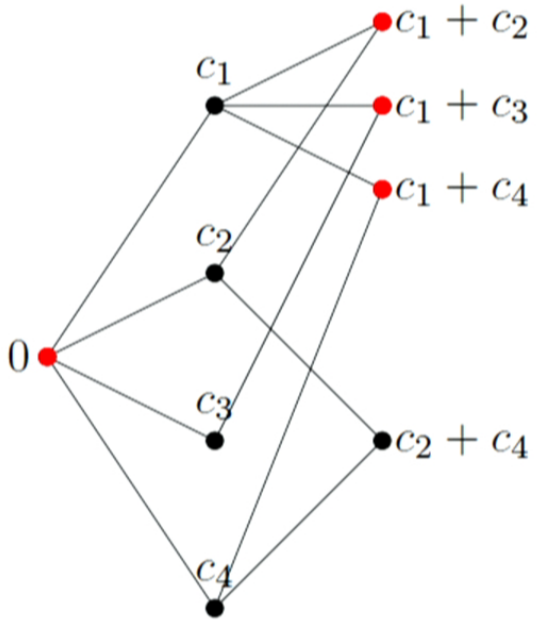
The Cayley graph



We can associate a stabilizer code to this graph:

- Stabilizers are generated by the X-spheres and the Z-spheres
- Undetectable errors = commute with the spheres

The Cayley graph



We can associate a stabilizer code to this graph:

- Stabilizers are generated by the X-spheres and the Z-spheres
- Undetectable errors = commute with the spheres

The quantum code associated with I_n

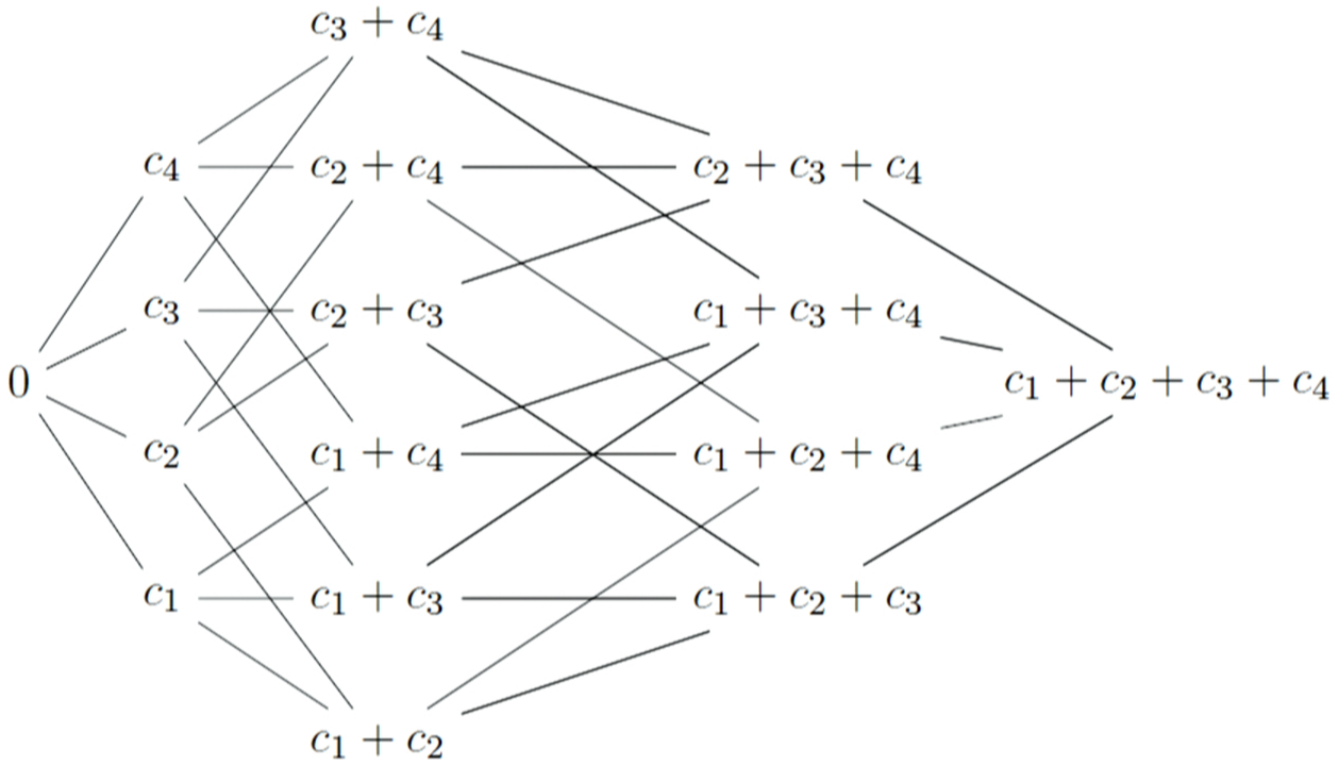


Figure : The cayley graph $G(I_4)$.

The quantum code associated with I_n

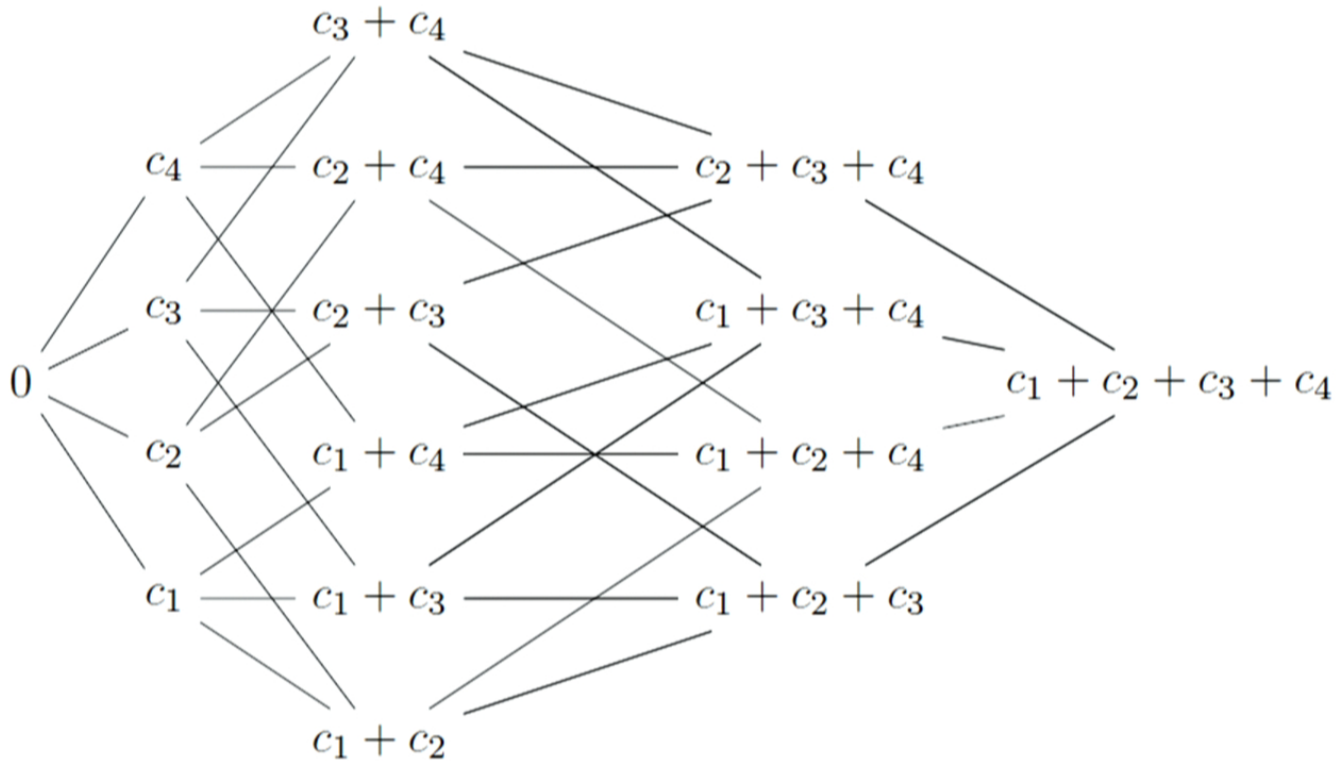


Figure : The cayley graph $G(I_4)$.

The quantum code associated with I_n

When $H = I_n$, we recognize the hypercube $\mathbb{F}_2^n$ of dimension n.

Parameters of the corresponding quantum code:

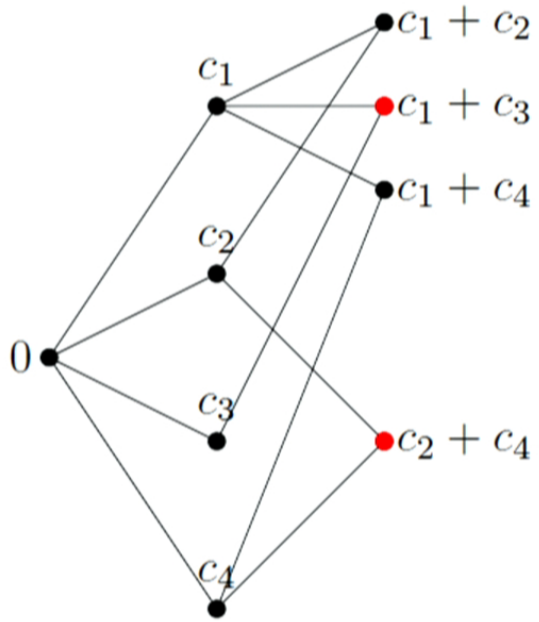
- We find $K = 0$, *i.e.* the quantum code is trivial.
- Then, every undetectable error is a stabilizer.

Minimum distance of the quantum code

- Then length $N = |V|$
- The minimum distance $D =$ cardinality of the smallest set of vertices which has an even intersection with the spheres but which is not a sum of spheres.

To apply the injectivity radius method look at the local structure of the graph.

Injectivity radius of the graph



A relation between the column $c_1 + c_2 + c_3 + c_4 = 0$, implies an identification of vertices: $c_1 + c_3 = c_2 + c_4$ and $c_1 = c_2 + c_3 + c_4 \ldots$

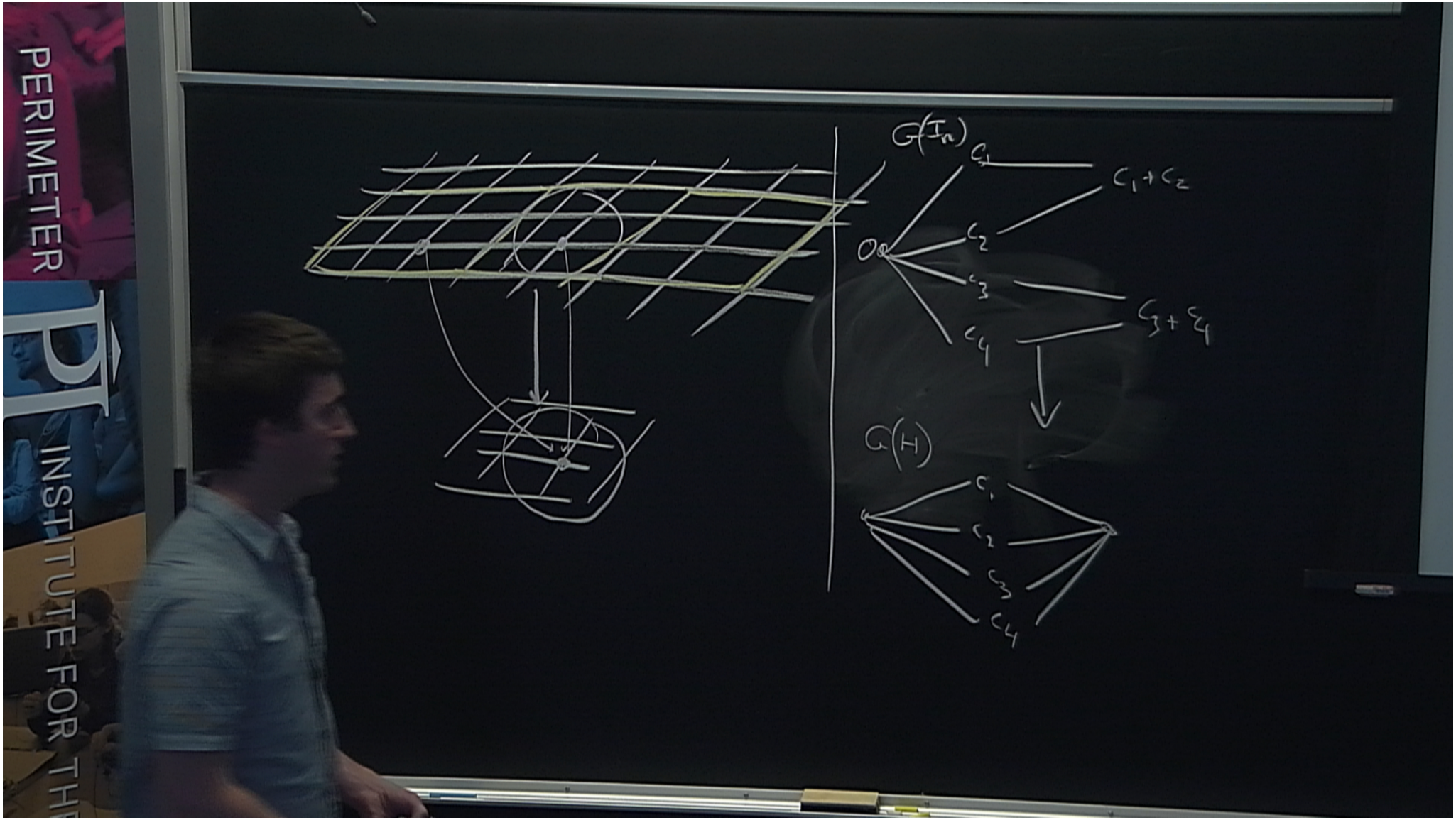
Injectivity radius of the graph

If there is no relation of weight $< d$ between the columns of H
Then $G(H)$ is locally isomorphic to the hypercube $G(I_n)$:

$$B_{I_n}\left(0, \frac{d-1}{2}\right) \simeq B_H\left(y, \frac{d-1}{2}\right)$$

(Couvreur, D, Zémor - 2013)

Injectivity radius method: If E_Z is an undetectable error in a small ball of $G(H)$.
$\Rightarrow$ it is an undetectable error in $G(I_n)$
$\Rightarrow$ it is a stabilizer
$\Rightarrow$ it doesn't appear in the computation of D


PERIMETER
INSTITUTE FOR THE
G(Γ_n)
C_1
C_1 + C_2
C_2
C_3
C_3 + C_4
C_4
G(H)
C_1
C_2
C_3
C_4

Injectivity radius of the graph

If there is no relation of weight $< d$ between the columns of H
Then $G(H)$ is locally isomorphic to the hypercube $G(I_n)$:

$$B_{I_n}\left(0, \frac{d-1}{2}\right) \simeq B_H\left(y, \frac{d-1}{2}\right)$$

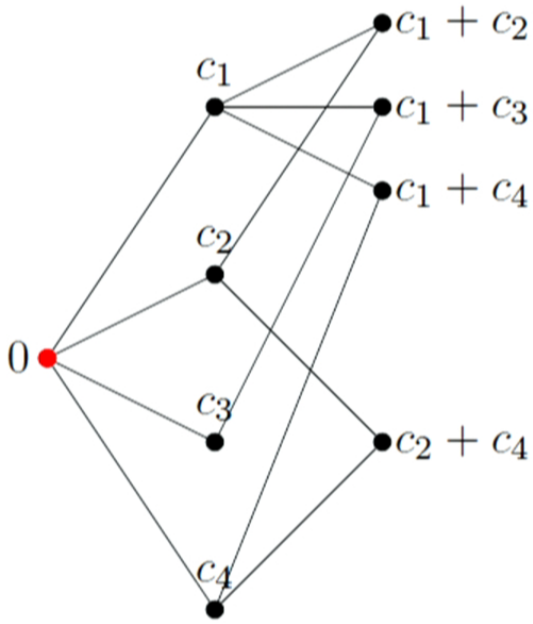
(Couvreur, D, Zémor - 2013)

Injectivity radius method: If E_Z is an undetectable error in a small ball of $G(H)$.
$\Rightarrow$ it is an undetectable error in $G(I_n)$
$\Rightarrow$ it is a stabilizer
$\Rightarrow$ it doesn't appear in the computation of D

Injectivity radius of the graph

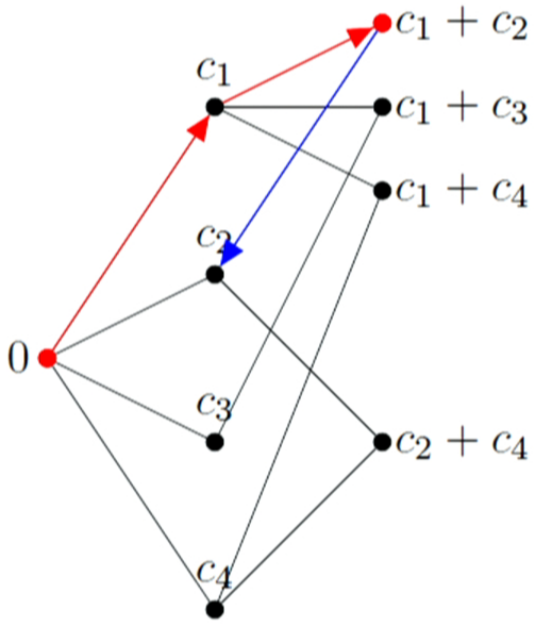
a non trivial undetectable error E_Z must leave the balls of radius $(d-1)/2$.
$\longrightarrow$ E contains at least $O(dn^2)$ vertices:

- assume $0 \in E_Z$,



Injectivity radius of the graph

a non trivial undetectable error E_Z must leave the balls of radius $(d-1)/2$.
$\longrightarrow$ E contains at least $O(dn^2)$ vertices:



- assume $0 \in E_Z$,
- spheres contain an even number of vertices of E_Z,
- spheres $S(c_i)$ contain another vertex of E_Z,
- at least $n/2$ new vertices.

ball of radius $2 \rightarrow O(n)$
ball of radius $4 \rightarrow O(n^2)$
radius 6? $\rightarrow O(n^{radius/2})$?
at least $(d-1)/8$ balls $\rightarrow$ $O(dn^2)$.

Injectivity radius of the graph

With this argument, we obtain

Theorem (Couvreur, D, Zémor - 2013)

If the classical code of parity–check matrix $H \in M_{r,n}(\mathbb{F}_2)$ has minimum distance d then:

$$D \geq an^2 d.$$

for some constant $a > 0$.

This bound is not tight.

We also found a family with parameters $[[2^n, 2^{n/2}, 2^{n/2-1}]]$. (Beyond BPT)

An homological expansion argument

- E_t the error restricited the qubits at distance t from 0.
- s_{t+1} the syndrome of E_t at distace $t+1$ from 0.

Adapting a method of Gromov we proved that

Lemma

- $|E_t| \geq |s_{t-1}|/(t-1)$
- $|s_{t+1}| \geq \frac{n-(t-1)t}{t+1}|E_t|$

Expansion: What is the size of s_{t+1} as a function of the size of E_t?
Homological Expansion: What is the size of s_{t+1} as a function of the minimum size of E_t up to a stabiizer?

An homological expansion argument

- E_t the error restricited the qubits at distance t from 0.
- s_{t+1} the syndrome of E_t at distace $t+1$ from 0.

Adapting a method of Gromov we proved that

Lemma

- $|E_t| \geq |s_{t-1}|/(t-1)$
- $|s_{t+1}| \geq \frac{n-(t-1)t}{t+1}|E_t|$

Expansion: What is the size of s_{t+1} as a function of the size of E_t?
Homological Expansion: What is the size of s_{t+1} as a function of the minimum size of E_t up to a stabiizer?

An homological expansion argument

which leads to

Theorem (D, Li, Thomassé - 2014)

$$D \geq \sum_{i=0}^{i \leq M} \frac{(n/2)^{i/2}}{i!},$$

where $M = \min\{(d-3)/2, \sqrt{n/2}\}$.

This gives $D \geq \Omega(2^{\sqrt{n}})$, when $d \geq \sqrt{n/2}$

Not tight: till radius $\sqrt{n}$.

Conclusion

- One of the first task is to extend our catalog of constructions.
- These Cayley graphs codes are clearly different from Kitaev's idea.
- What is the dimension K of these codes?
- High reduncancy in the stabilizers $\Rightarrow$ improve the decoding? fault-tolerance?
- Remark: Tillich-Zémor construction and its generalization by Pryadko-Kovalev give constant rate and $d = O(\sqrt{n})$.

Thank you for your attention!

An homological expansion argument

which leads to

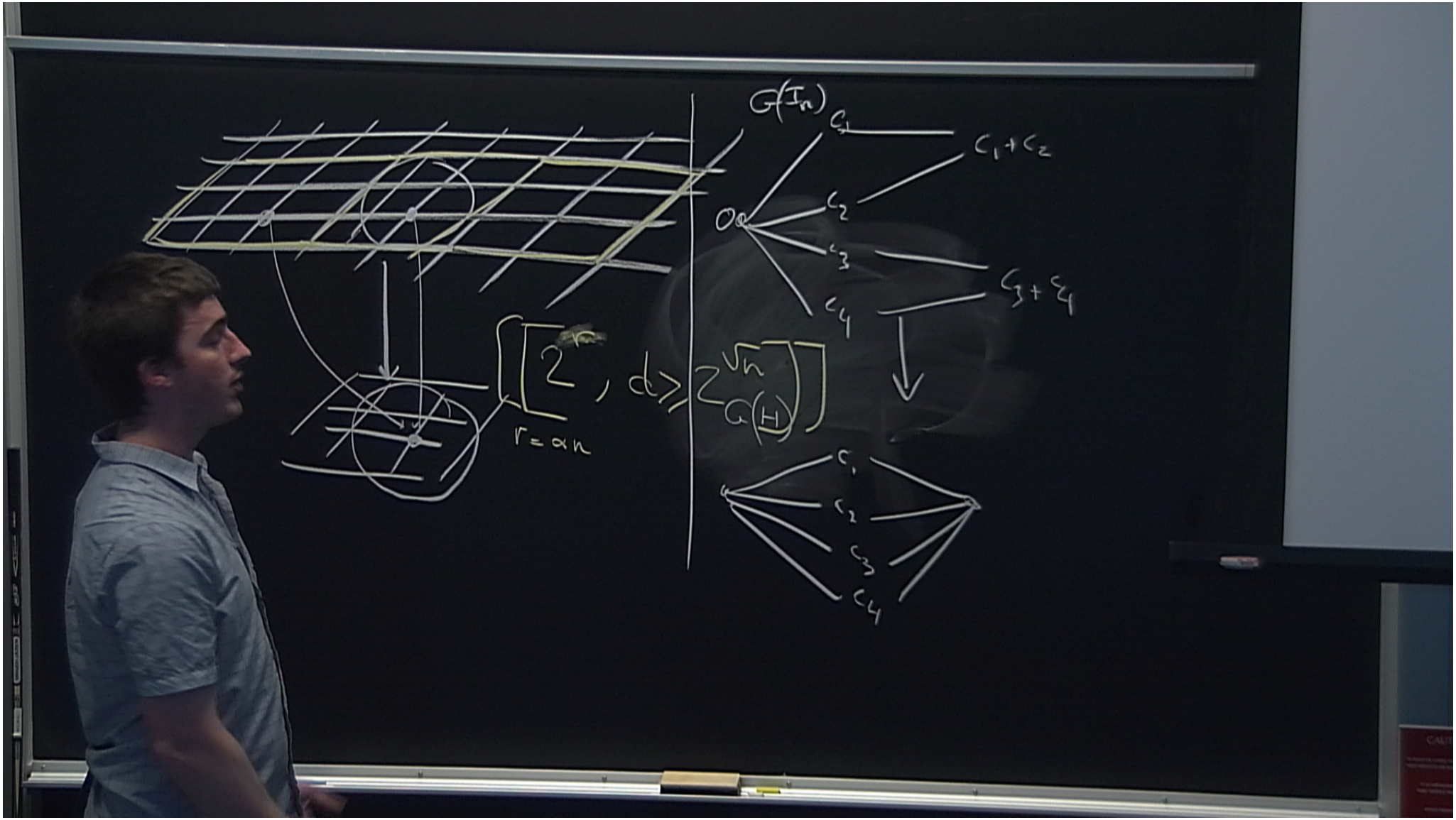
Theorem (D, Li, Thomassé - 2014)

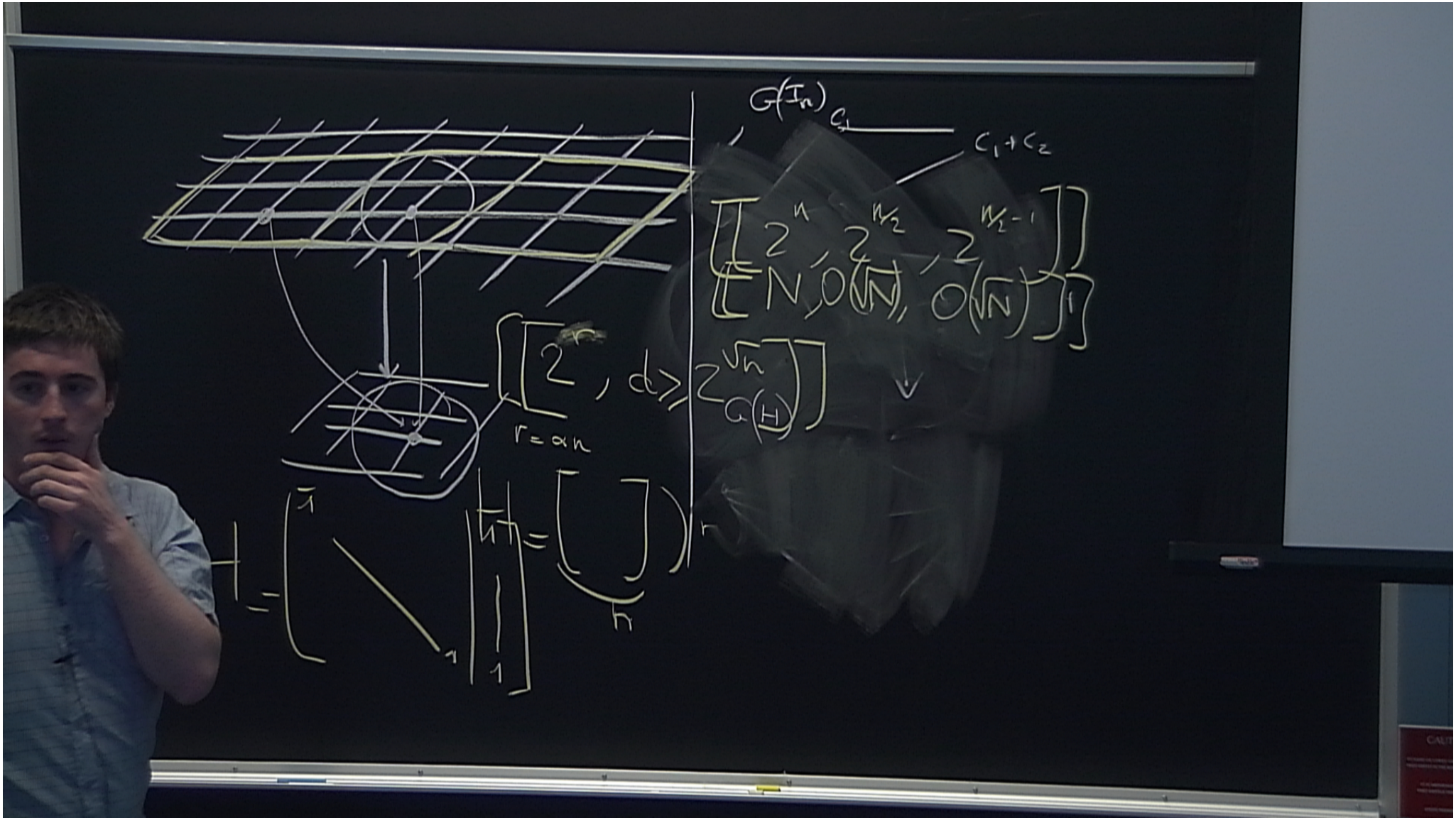
$$D \geq \sum_{i=0}^{i \leq M} \frac{(n/2)^{i/2}}{i!},$$

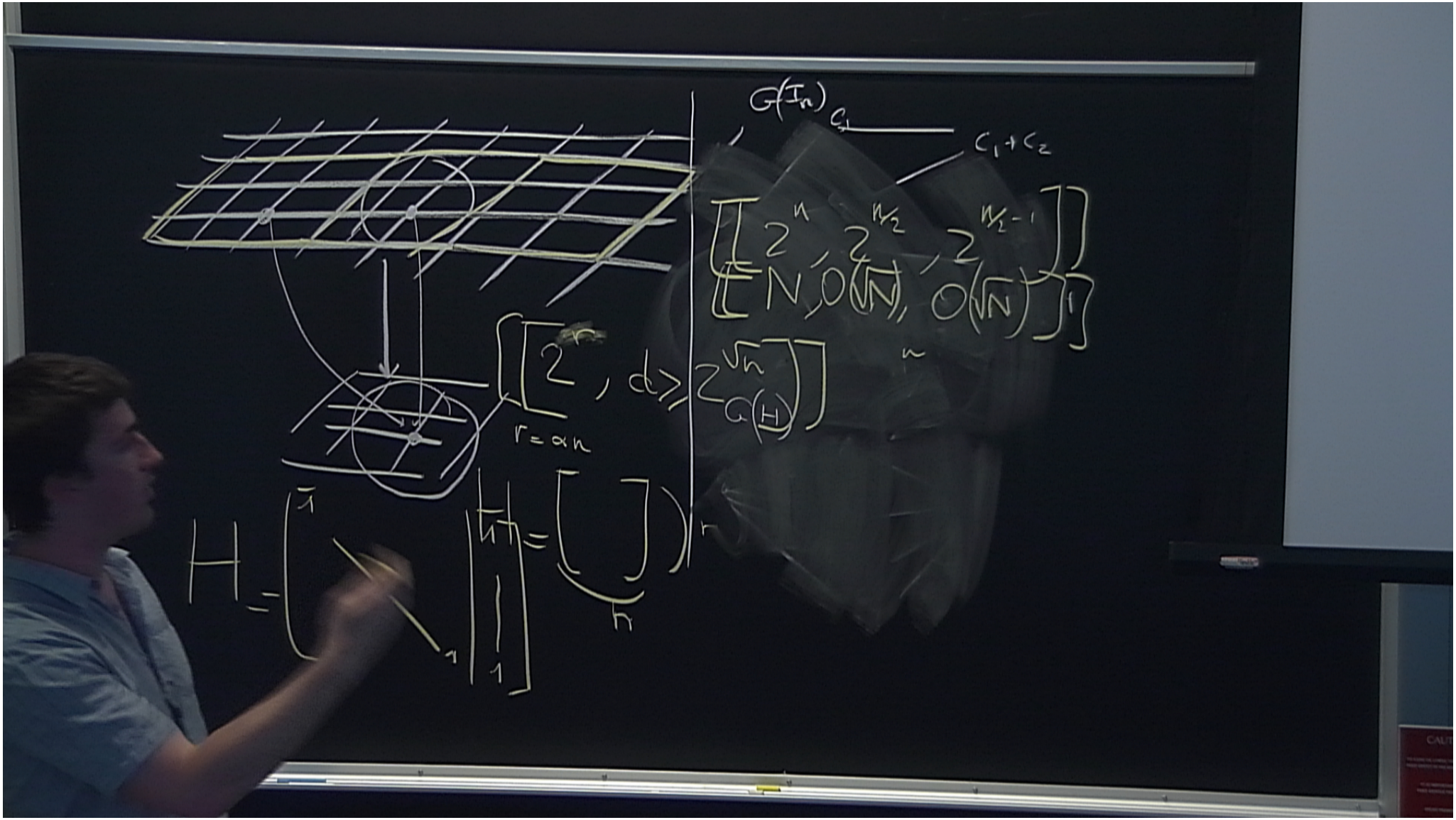
where $M = \min\{(d-3)/2, \sqrt{n/2}\}$.

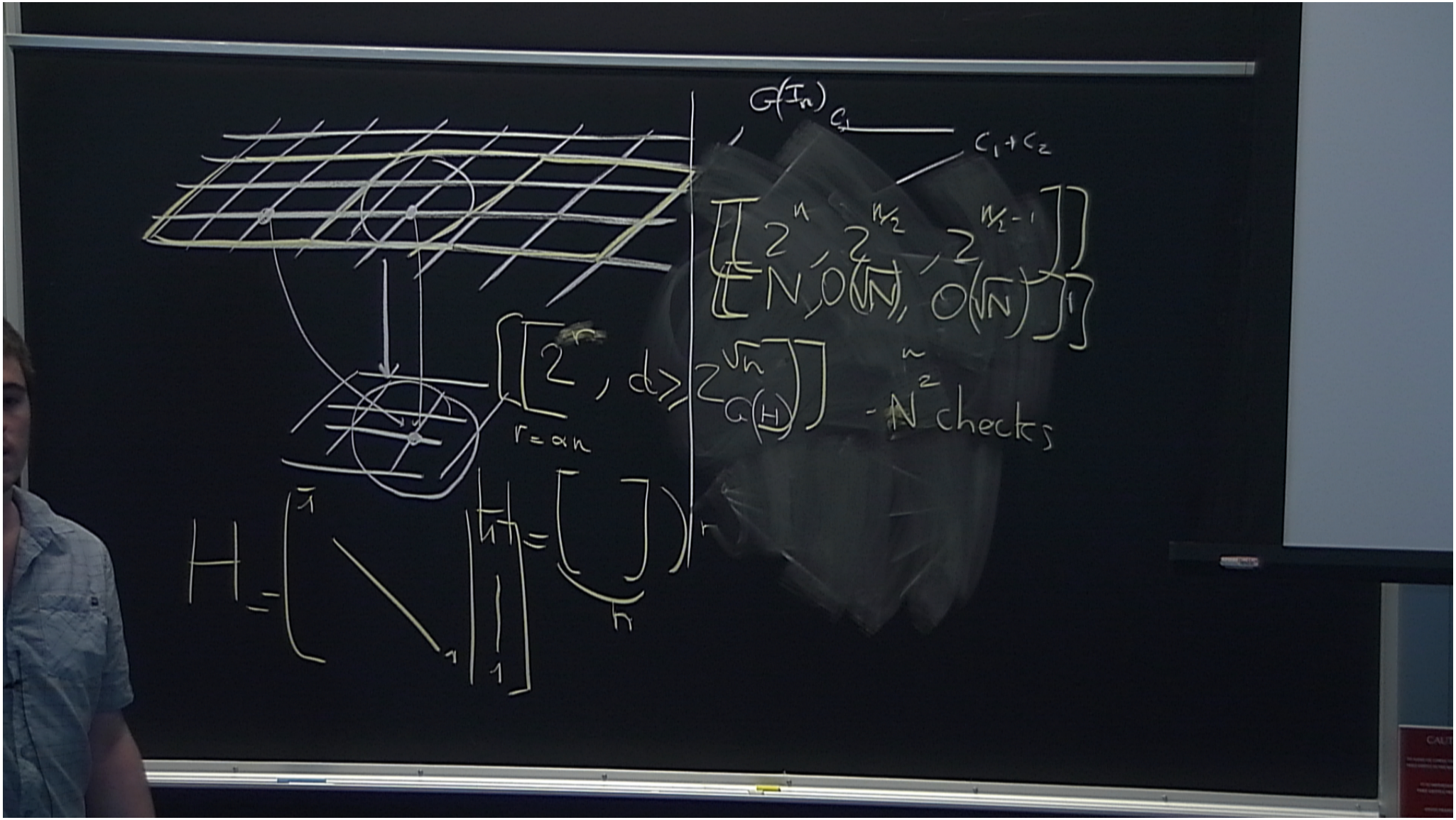
This gives $D \geq \Omega(2^{\sqrt{n}})$, when $d \geq \sqrt{n/2}$

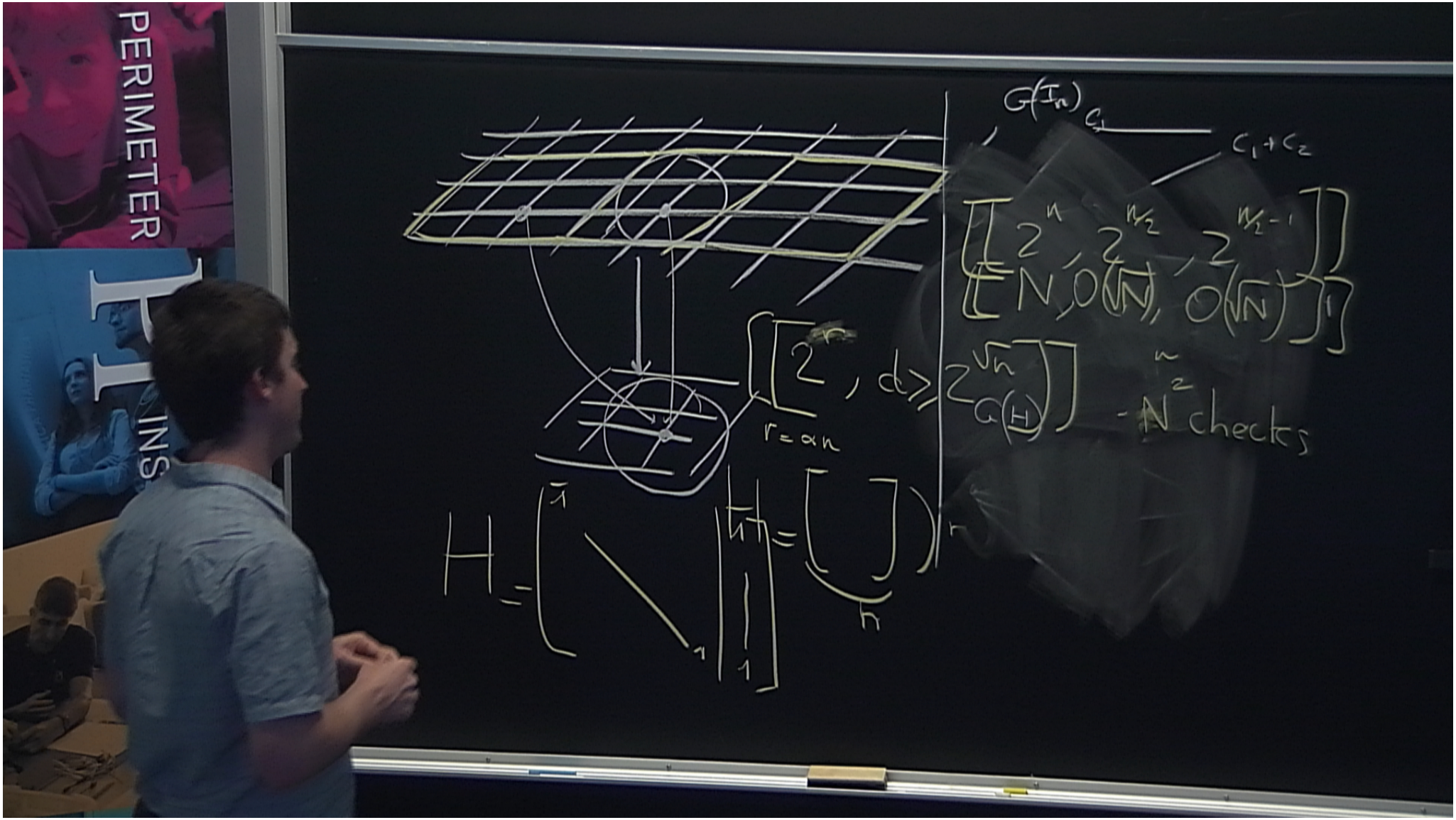
Not tight: till radius $\sqrt{n}$.


G(I_n)
C_1
C_1 + C_2
C_2
C_3
C_3 + C_4
C_4
r = αn
C_1
C_2
C_3
C_4


G(I_n)
C_1
C_1+C_2
r=αn


G(I_n)
C_1
C_1+C_2
r=αn


G(I_n)
C_1
C_1+C_2
r=αn
checks


PERIMETER
INS
$G(I_n)$
C_1
C_1+C_2
$r=\alpha n$
N^2 checks