Title: Single-Shot-Decoding with High Thresholds in LDPC Quantum Codes with Constant Encoding Rate

Speakers: Nikolas Breuckmann

Series: Perimeter Institute Quantum Discussions

Date: March 18, 2020 - 4:00 PM

URL: http://pirsa.org/20030026

Abstract: It is believed that active quantum error correction will be an essential ingredient to build a scalable quantum computer. The currently favored scheme is the surface code due to its high decoding threshold and efficient decoding algorithm. However, it suffers from large overheads which are even more severe when parity check measurements are subject to errors and have to be repeated. Furthermore, the number of encoded qubits in the surface code does not grow with system size, leading to a sub-optimal use of the physical qubits.

Finally, the decoding algorithm, while efficient, has non-trivial complexity and it is not clear whether it can be implemented in hardware that can keep up with the classical processing.

We present a class of low-density-parity check (LDPC) quantum codes which fix all three of the concerns mentioned above. They were first proposed in [1] and called 4D hyperbolic codes, as their definition is based on four-dimensional, curved geometries. They have the remarkable property that the number of encoded qubits grows linearly with system size, while their distance grows polynomially with system size, i.e. d~n a with 0.1 < a < 0.3. This is remarkable since it was previously conjectured that such codes could not exist [1]. Their structure allows for decoders which can deal with erroneous syndrome measurements, a property called single-shot error correction [2] as well as local decoding schemes [3].

Although [1] analyzed the encoding rate and distance of this code family abstractly, it is a non-trivial task to actually construct them. There is no known efficient deterministic procedure for obtaining small examples. Only single examples of reasonable size had been obtained previously [4]. These previous examples were part of different code families, so that it was not possible to determine a threshold. We succeeded to construct several small examples by utilizing a combination of randomized search and algebraic tools. We analyze the performance of these codes under several different local decoding procedures via Monte Carlo simulations. The decoders all share the property that they can be executed in parallel in O(1) time. Under the phenomenological noise model and including syndrome errors we obtain a threshold of ~5% which to our knowledge is the highest threshold among all local decoding schemes.

[1] A. Lubotzky, A. Guth, Journal Of Mathematical Physics 55, 082202 (2014).
[2] H. Bombin, Physical Review X 5 (3), 031043 (2015).
[3] M. Hastings, QIC 14, 1187 (2014).
[4] V. Londe, A. Leverrier, arXiv:1712.08578 (2017).

Zoom Link: https://pitp.zoom.us/j/417863219

Single-Shot Decoding of Linear Rate LDPC Quantum Codes with High Performance

Nikolas P. Breuckmann
UCLQ Fellow
University College London

2020-03-18
Perimeter Institute

arXiv:2001.03568

Background:

- What are LDPC & topological quantum codes
- How can we exploit geometry to construct codes?

4D Hyperbolic Codes:

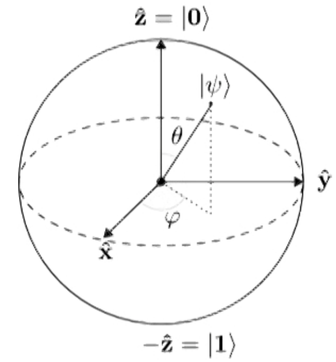
- Construction
- Decoding via belief propagation

Preliminary results:

- Method to reduce check-weights in LDPC codes

How can we perform quantum computation in the presence of noise?

- Arbitrary shifts of the state of a quantum computer
- Observation: Measurements discretise continuous errors
- [Shor '95]: Possible to correct errors in quantum computer



quantum error correcting codes

Threshold theorem [Aharonov - Ben-Or '96]:

There exists a threshold p_t such that,

if the error rate per gate and time step is $p < p_t$

then arbitrarily long quantum computations are possible.

Quantum Codes: Toy Example

- Consider the +1 - eigenstates of Z_1Z_2 and Z_2Z_3: |000> and |111> *(logical states)*
- Error: Pauli-X on the first qubit X_1 ⇒ |100> and |011>
- -1 - eigenstates of Z_1Z_2 and +1 - eigenstates of Z_2Z_3 *(parity checks / stabilizers)*

(Z_1Z_2, Z_2Z_3)	Type of X-error
$(1,1)$	no error
$(-1,1)$	error on the first qubit
$(-1,-1)$	error on the second qubit
$(1,-1)$	error on the third qubit

Quantum Codes

[Shor '95]: Extend example to protect a single qubit against an arbitrary error

[Gottesman '97]: Framework to construct codes (Stabilizer Formalism)

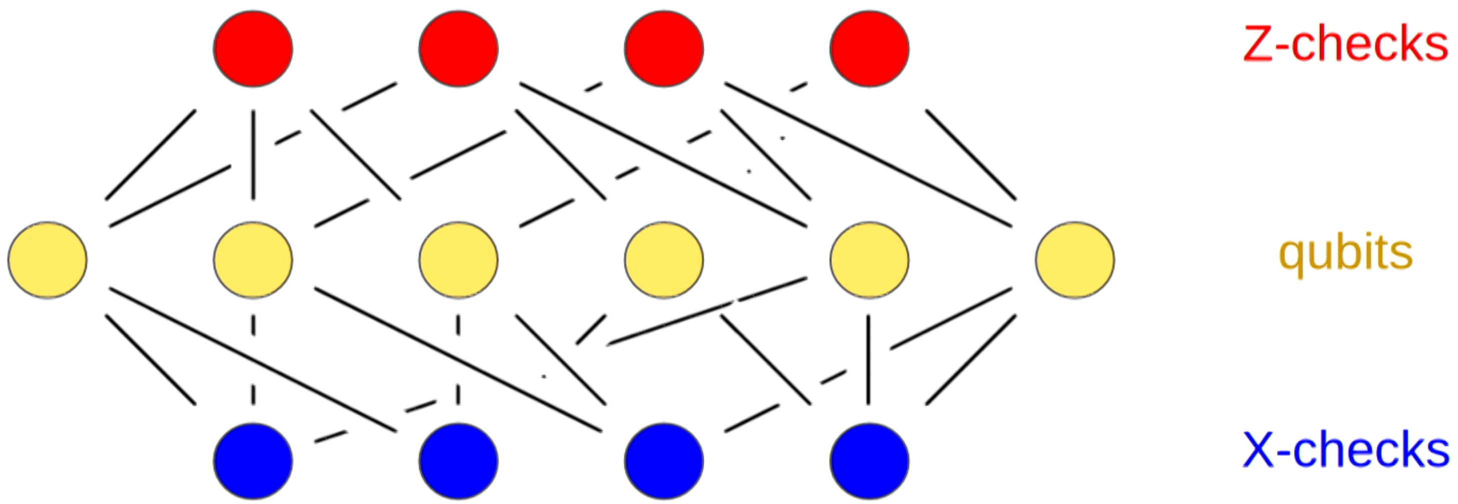
Two important facts:

- Check measurements need to <u>commute</u> for well-defined outcome
- # encoded qubits = # physical qubits - # independent checks

CSS Quantum Codes

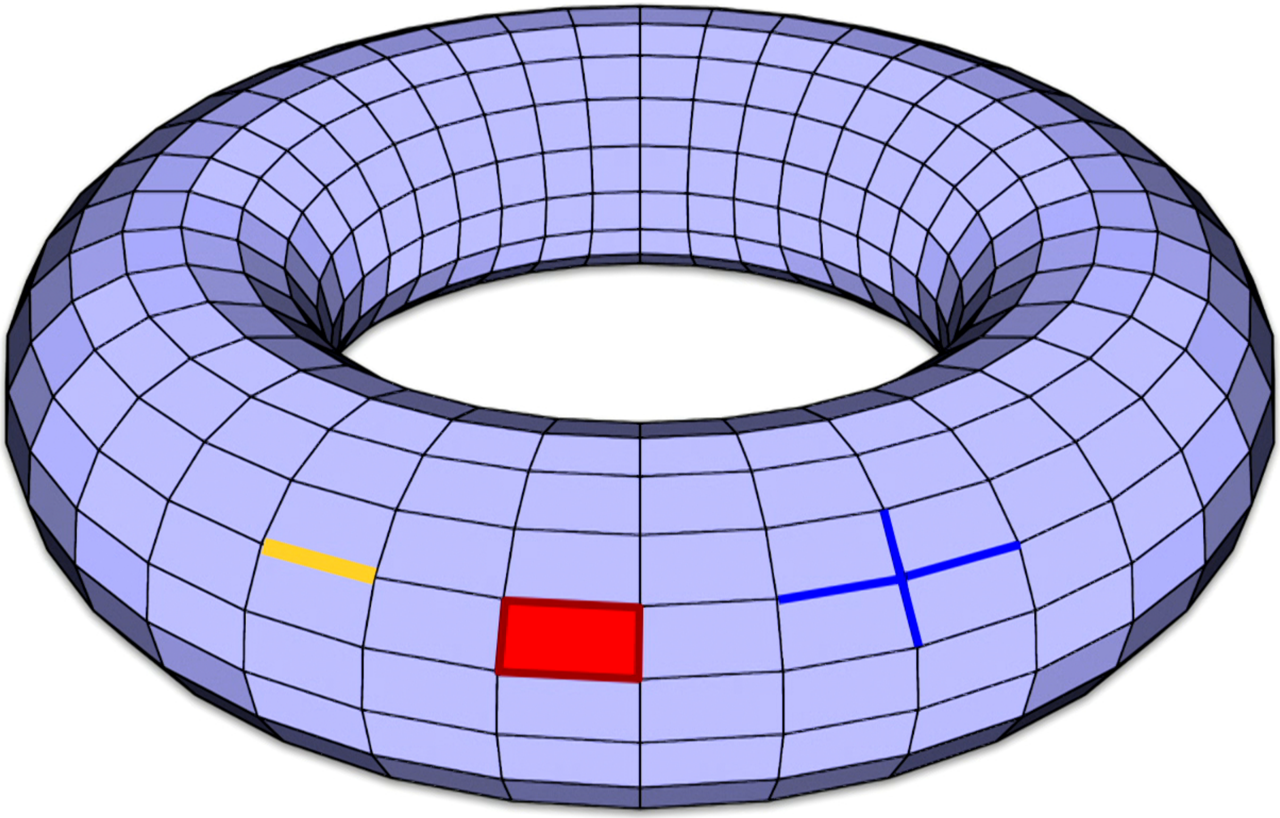
Important special* case: All checks either X-type or Z-type

Quantum code is given by a 3-level graph:

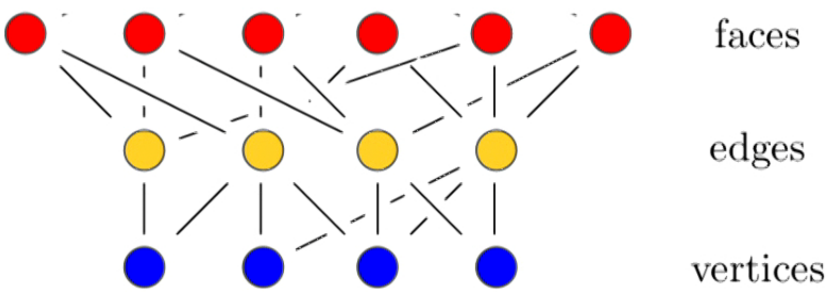


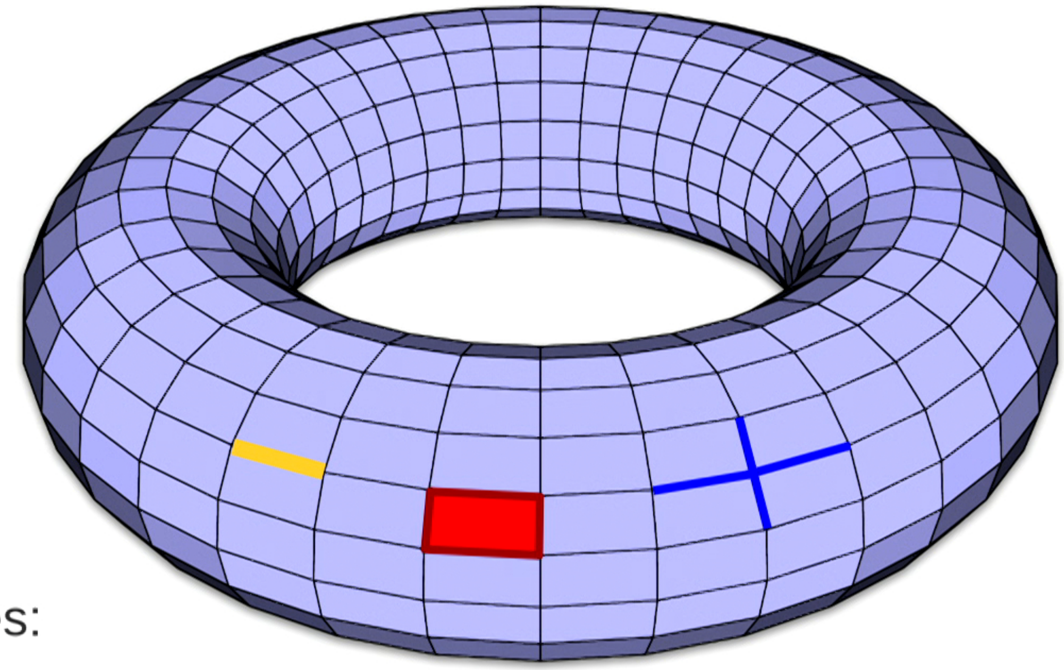
*Not that special: any stabilizer code can be mapped onto a CSS code, preserving most of its properties.

Example: Kitaev's Toric Code



Example: 2D Toric Code





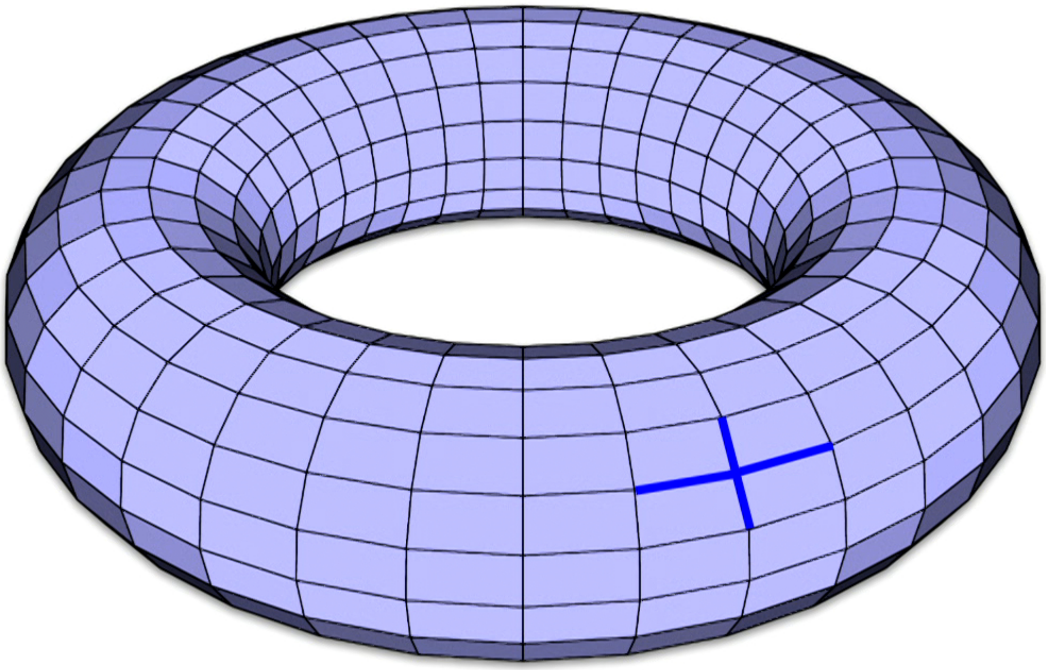
Any face and vertex share 0 or 2 edges:

This is a quantum code!

Example: 2D Toric Code

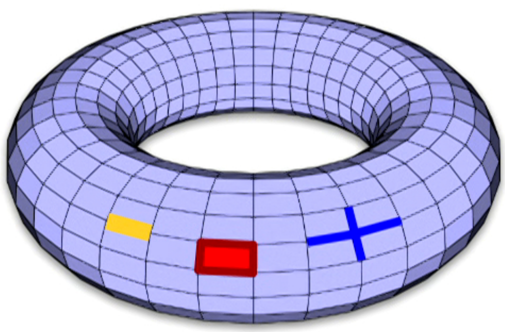
Logical degrees of freedom

- Must commute with all X-checks
- Hence: can not have end-points
- Contractible loop: product of Z-checks
- *Logicals are non-contractible loops* (k = 2)



Low-Density Parity Check Codes

1. The size of the support of each check is bounded
2. Each qubit is included in a bounded number of checks



Checks local in some geometry:
LDPC

Other qualities to judge a quantum code by

- Encoding rate k/n
- Distance d
- Efficient decoding (classical processing of syndrome)
- Threshold p_c
- Number of qubits in each check
- Logical gates

LDPC Quantum Codes

	Encoding k	Distance d
2D Euclidean codes (surface code, color code)	constant	$\sqrt{n}$
3D Euclidean codes (3D gauge color codes)	constant	$\sqrt[3]{n}$
2D Hyperbolic codes	linear	log(n)
Hypergraph product codes	linear	$\sqrt{n}$
4D Hyperbolic codes	linear	poly(n)

Linear rate codes are interesting:

[Gottesman '13]: LDPC codes with

- linear rate
- 'good' error correction capabilities
- efficient decoder

⇒ can do quantum fault-tolerance with *constant* overhead

4D Hyperbolic Codes

QUANTUM ERROR CORRECTING CODES
AND 4-DIMENSIONAL ARITHMETIC HYPERBOLIC
MANIFOLDS

LARRY GUTH AND ALEXANDER LUBOTZKY

2014

ABSTRACT. Using 4-dimensional arithmetic hyperbolic manifolds, we construct some new homological quantum error correcting codes. They are LDPC codes with linear rate and distance n^{ϵ}. Their rate is evaluated via Euler characteristic arguments and their distance using $\mathbb{Z}_2$-systolic geometry. This construction answers a queston

Motivation: disprove conjectured bound on parameters of homological codes
[Delfosse ‘13: holds for 2D]

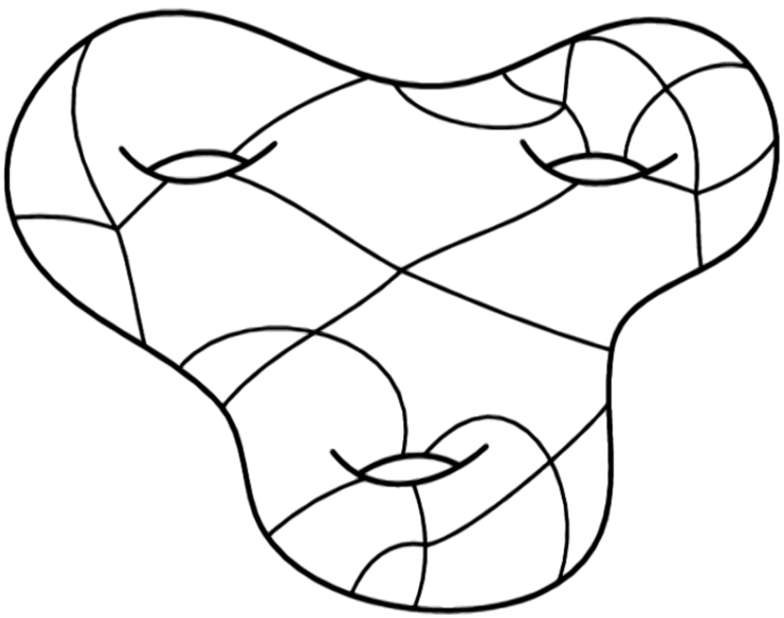
$$k\, d^2 \in O\left(n^{1+o(1)}\right)$$

show that 4D hyperbolic codes have parameters

$$[[n, k \in O(n), d \in O(n^{\epsilon})]]$$

Homological codes

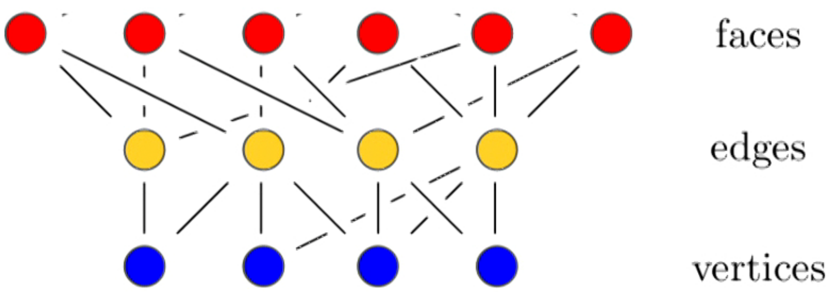
There is a general principle for constructing quantum codes:
Homology

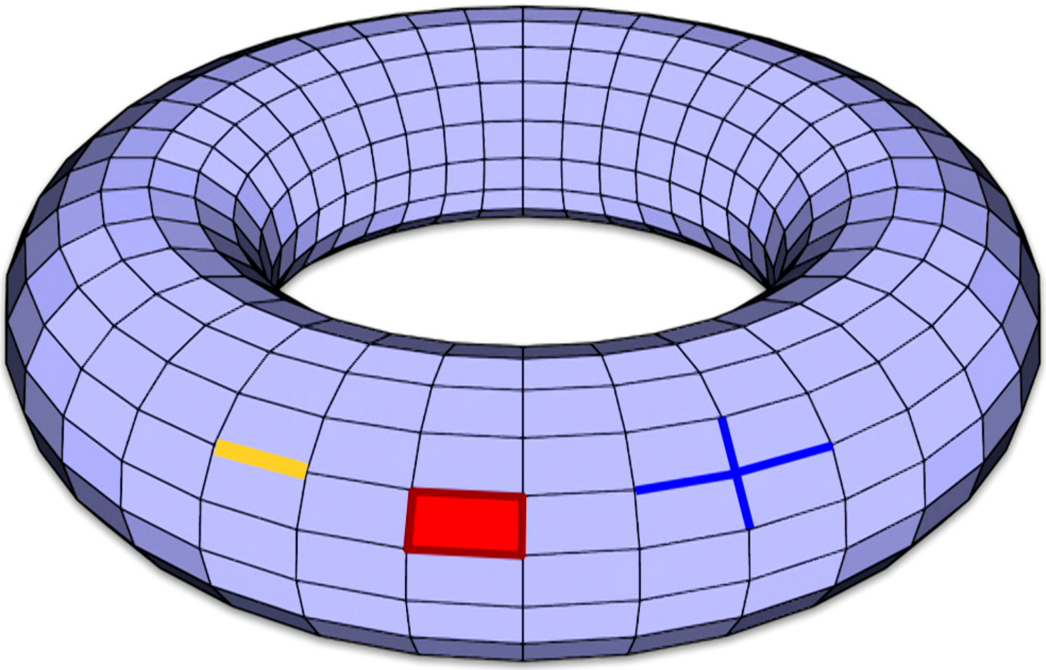


Recipe

1. Take tessellated D-manifold
2. Pick dimension $0 < i < D$
3. Identify:
   a. i-cells with qubits
   b. i-1-cells with X-checks
   c. i+1-cells with Z-checks

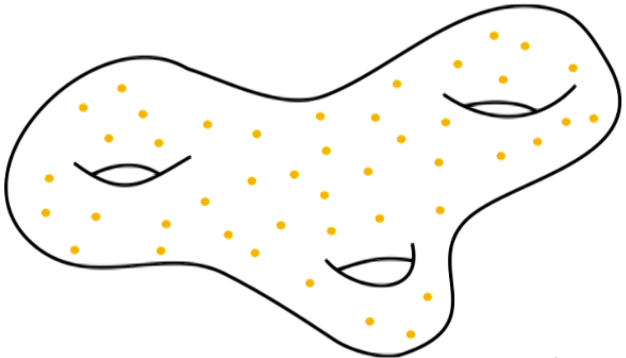
Example: 2D Toric Code





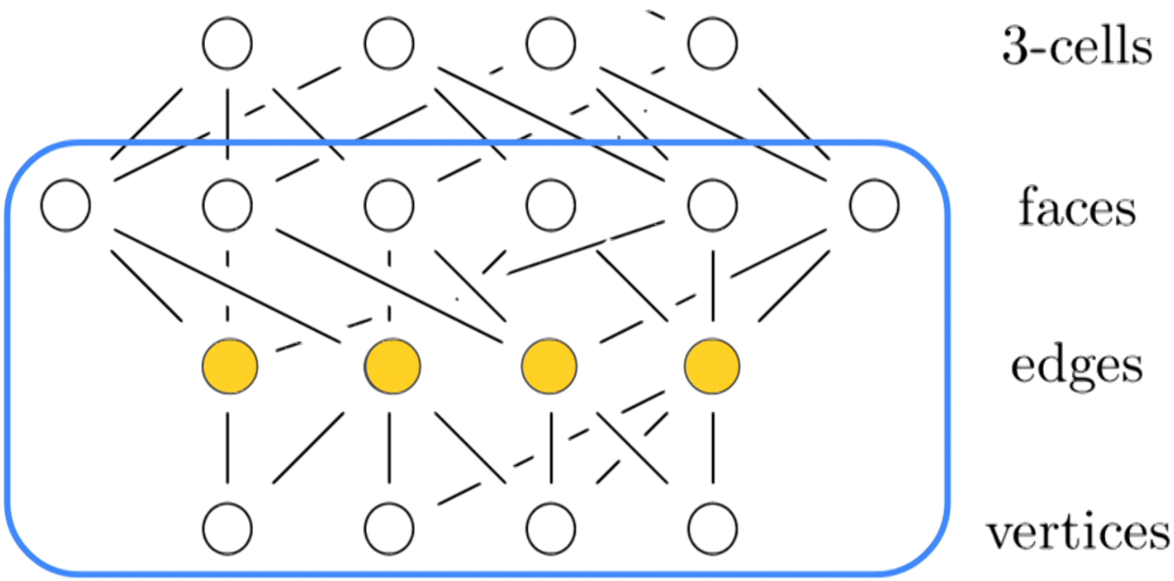
Homological codes

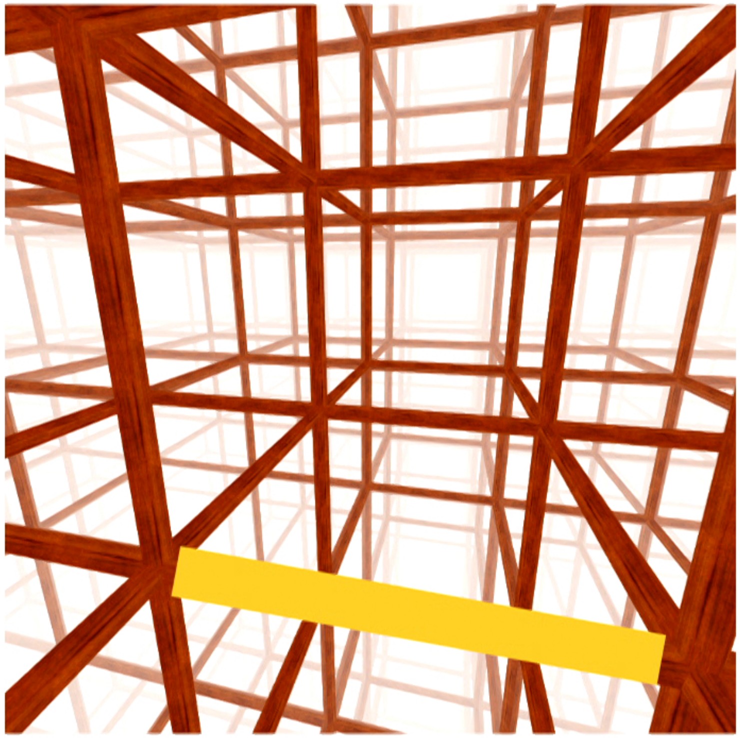
Use connection between code properties and geometry



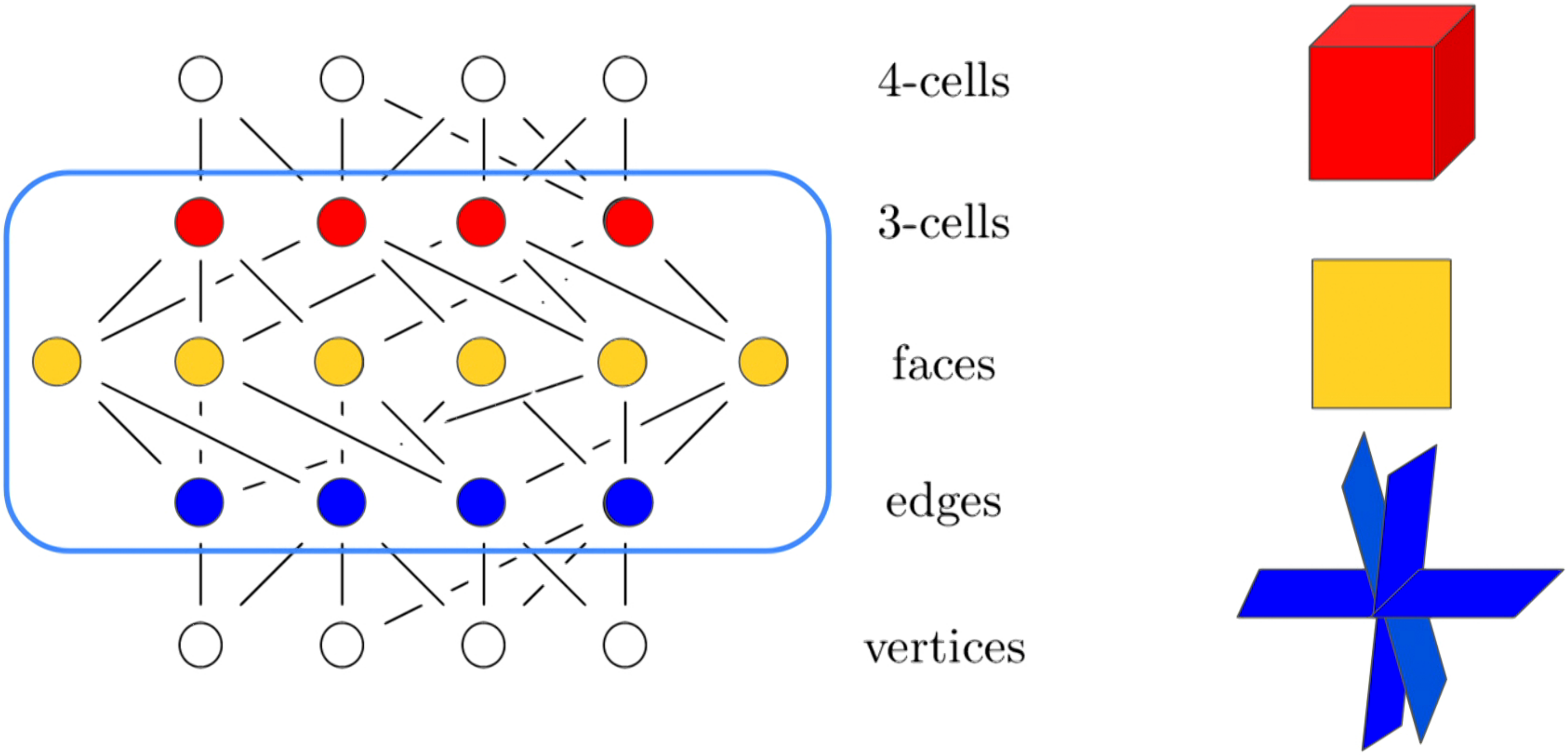
$$n \sim \mathrm{vol}_D(M) \qquad k \sim \dim H_i$$

Homological Codes: 3D Toric Code

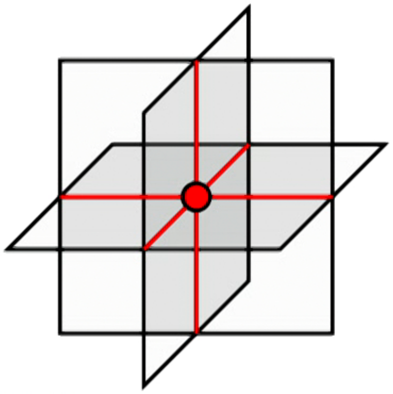




Homological Codes: 4D

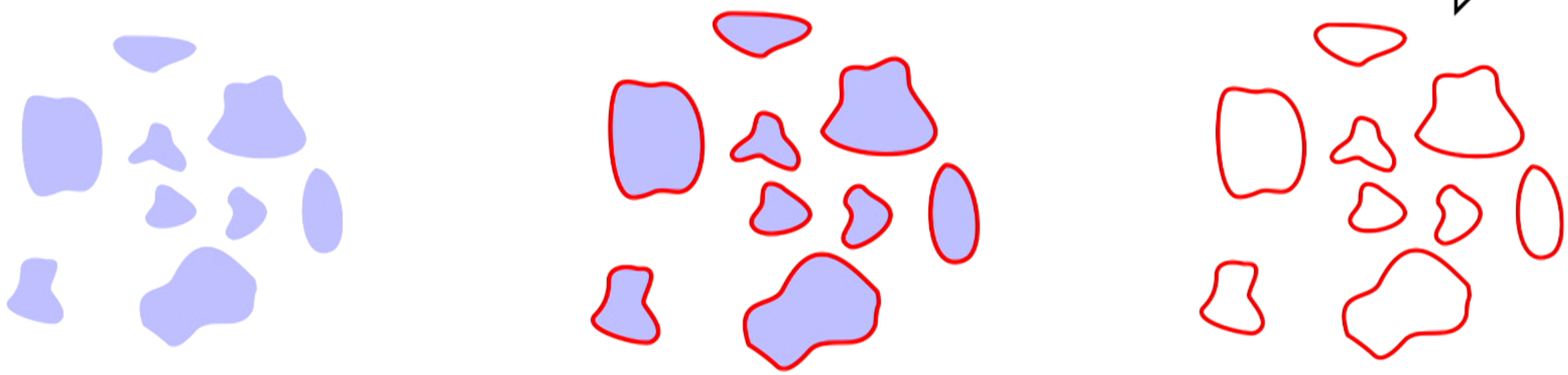


Why study 4D codes?



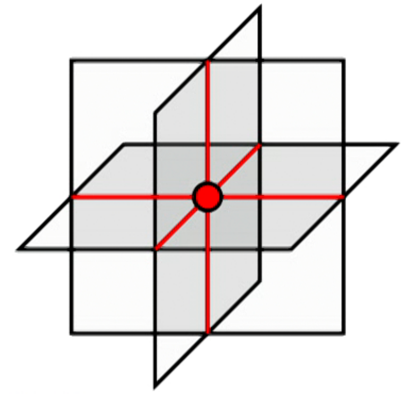
Parity checks satisfy local constraints:

- Simple decoding schemes based on local information



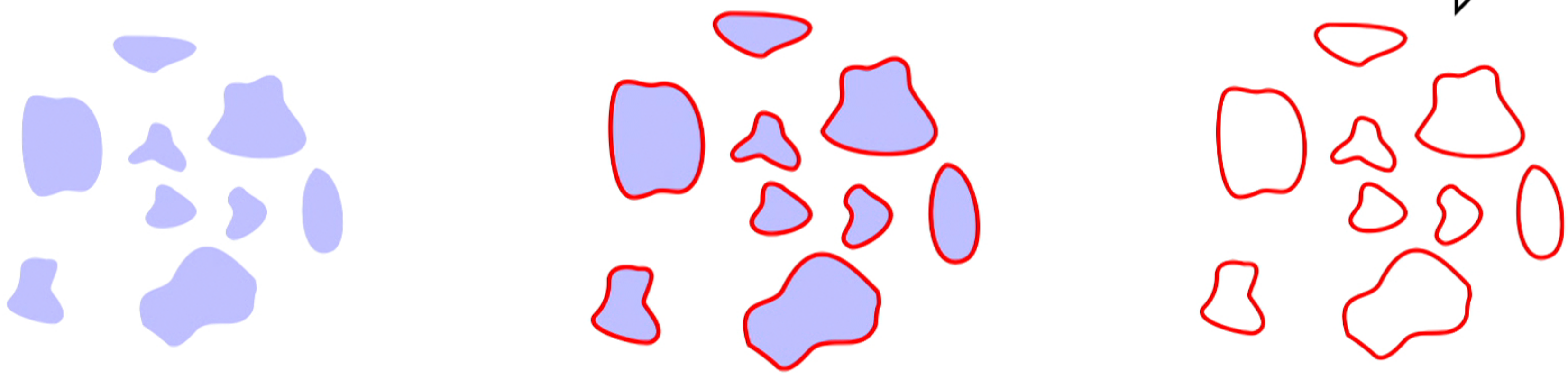
[Dennis et.al. ‘01, Pastawski et.al. ‘13, Hastings ‘13, Breuckmann et.al. ‘16, Kubicka et.al. ‘19]

Why study 4D codes?



Parity checks satisfy local constraints:

- Simple decoding schemes based on local information

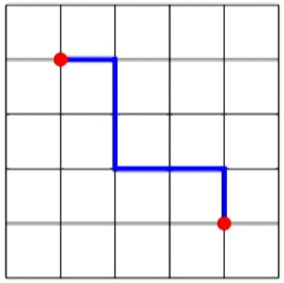


[Dennis et.al. ‘01, Pastawski et.al. ‘13, Hastings ‘13, Breuckmann et.al. ‘16, Kubicka et.al. ‘19]

[Hastings ‘13]: In combination with curvature allows for simple, effective decoding

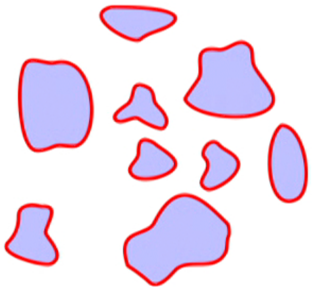
Single-Shot Decoding

In 2D topological codes:



- Check measurements give information about points
- Measurement errors may flip outcome
- need to repeat measurements to build confidence

In 4D topological codes:

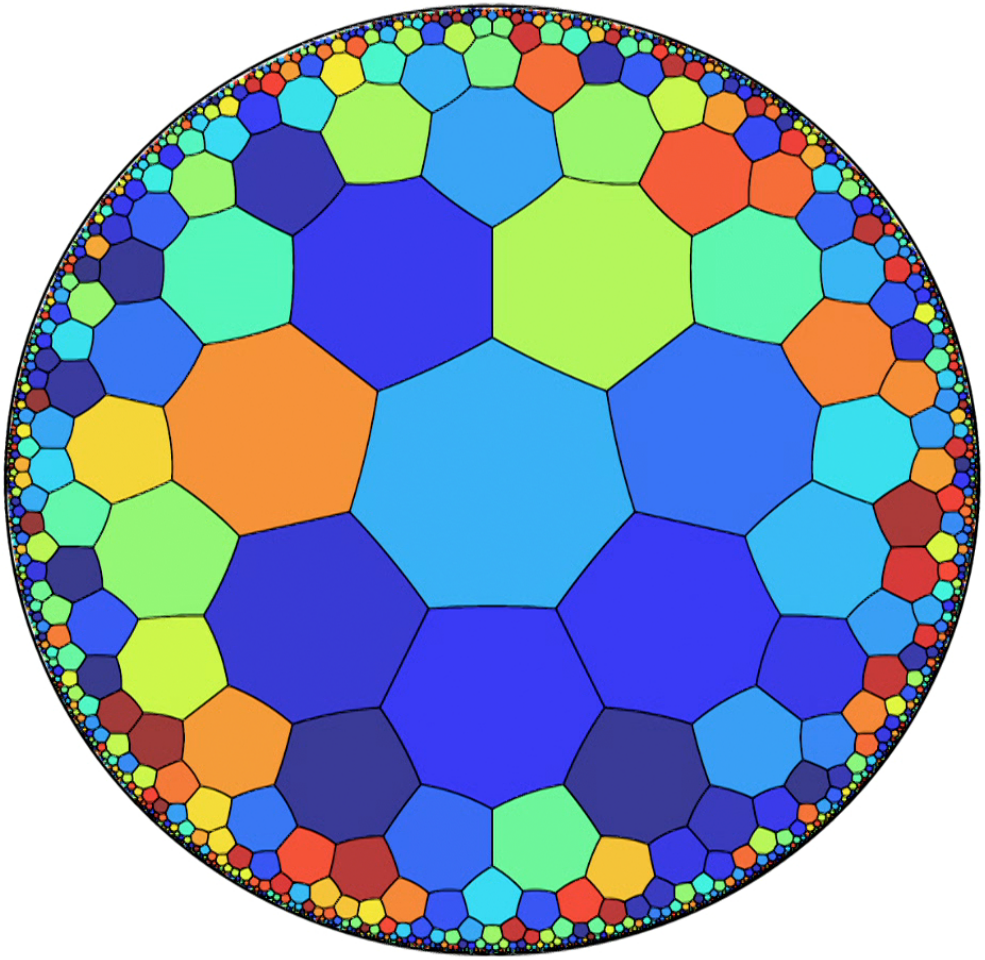


- Check measurements obey local linear dependence
- Measurement result can be ‘decoded’
- Need to measure only once

[Bombin ‘13]

Hyperbolic Codes in 2D

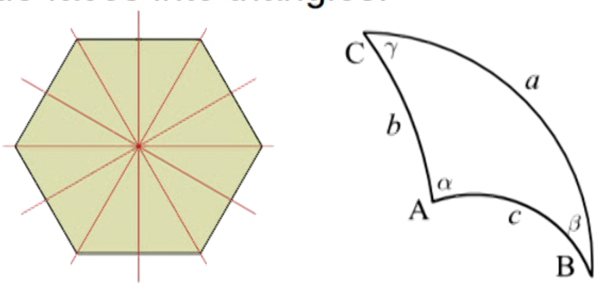
- Defined on negatively curved surfaces of increasing area
- Surfaces have large genus: many encoded qubits
- Parity check weight comparable to surface code



Regular tessellations in curved geometries

r = number of sides of a tile & s = number of tiles around a vertex

Subdivide faces into triangles:

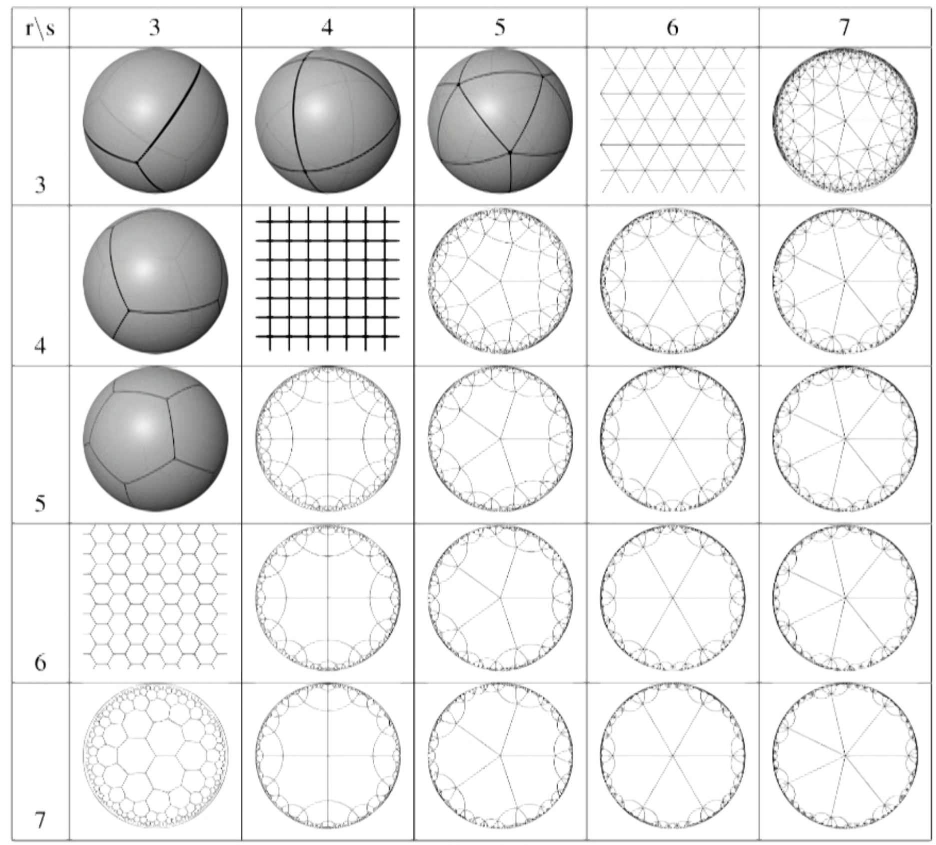


Curvature κ: condition on internal angles

$$\alpha+\beta+\gamma\begin{cases} >\pi & if\ \kappa>0 \\ =\pi & if\ \kappa=0 \\ <\pi & if\ \kappa<0. \end{cases}$$

Euclidean space: condition on r & s

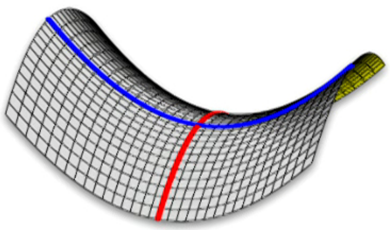
$$\pi/2+\pi/r+\pi/s=\pi$$

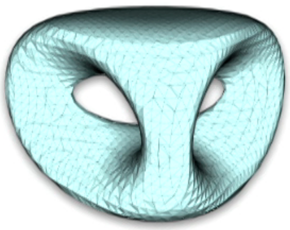


Hyperbolic codes: encoding rate k/n

Gauss-Bonnet Theorem:

$$\int \kappa \, dA = 2 - 2g$$





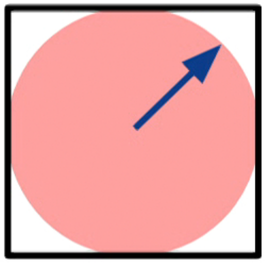
$$\dim H_1 = \frac{\text{area}(M)}{2\pi} + 2$$

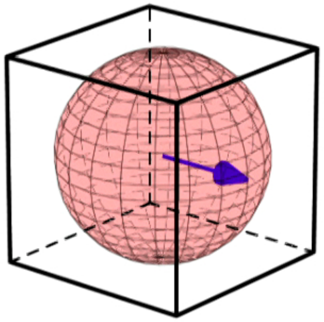
$$\Downarrow$$

$$k = \left(1 - \frac{2}{r} - \frac{2}{s}\right) n + 2$$

Hyperbolic codes: distance d

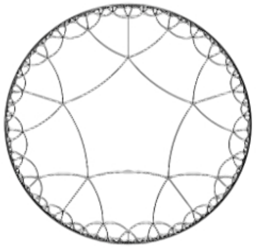
Definition: *Injectivity Radius **R*** -- largest radius of a **ball** that can be embedded without self-intersections





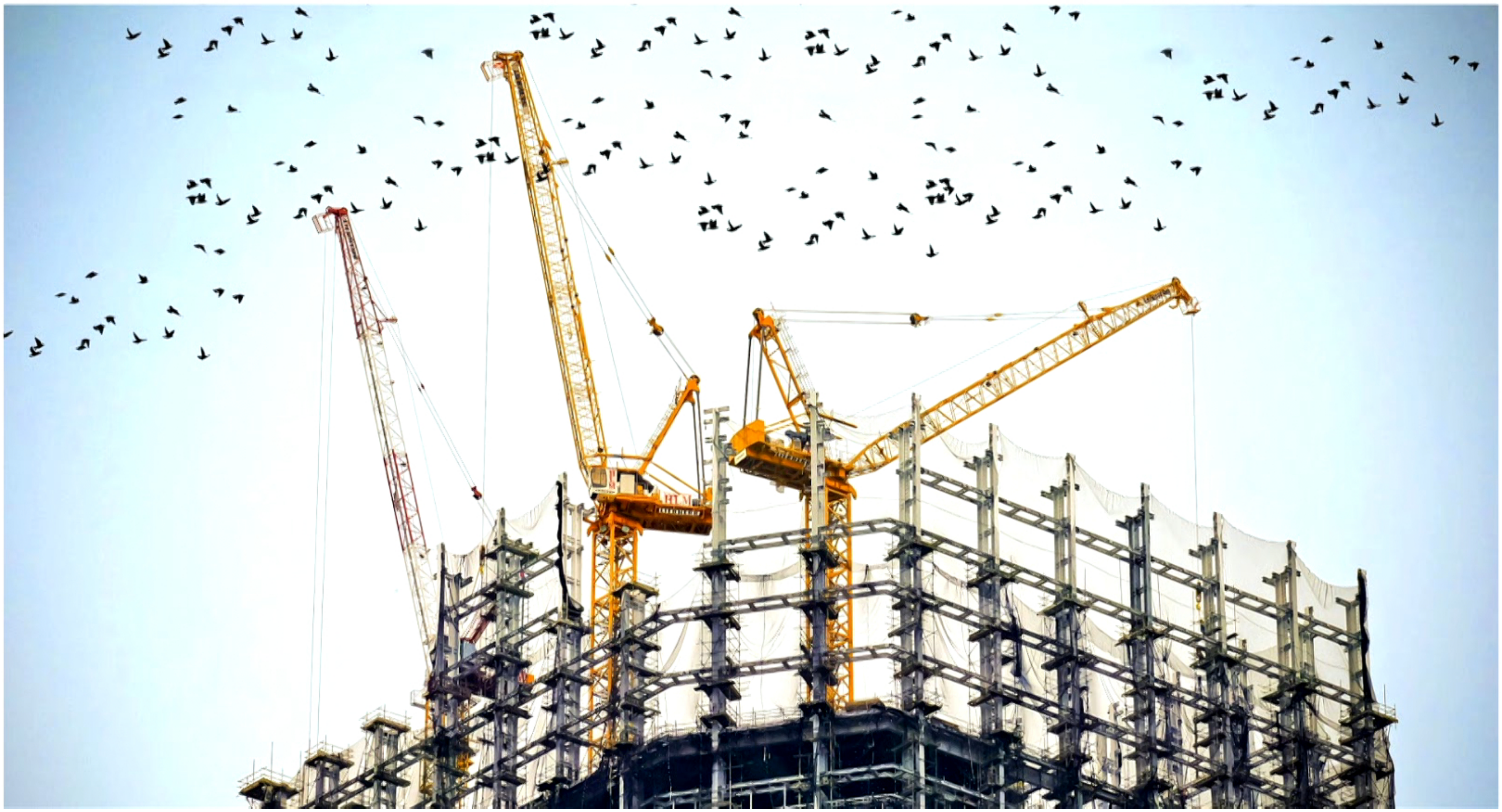
In hyperbolic space:

$$R \geq const. \times \log \mathrm{vol}_D(M)$$

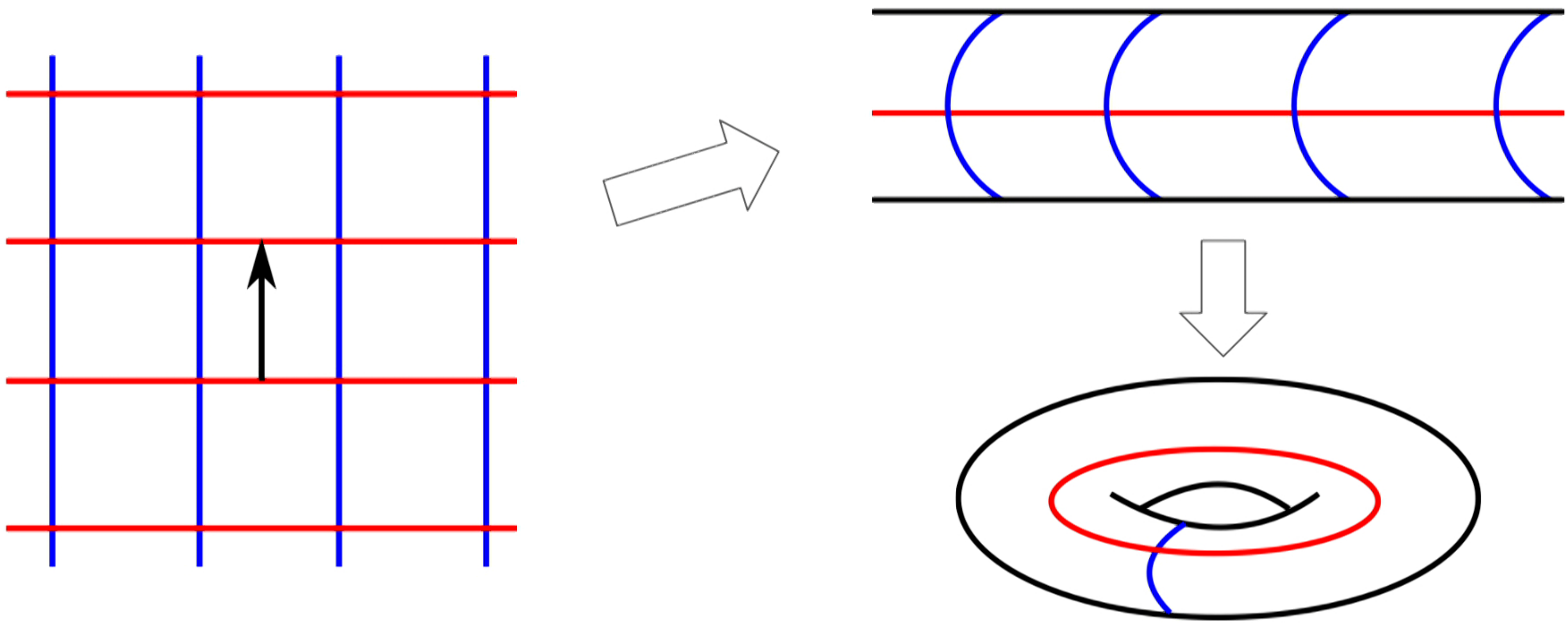


$$c \times \log(n) \leq d \leq c' \times \log(n)$$

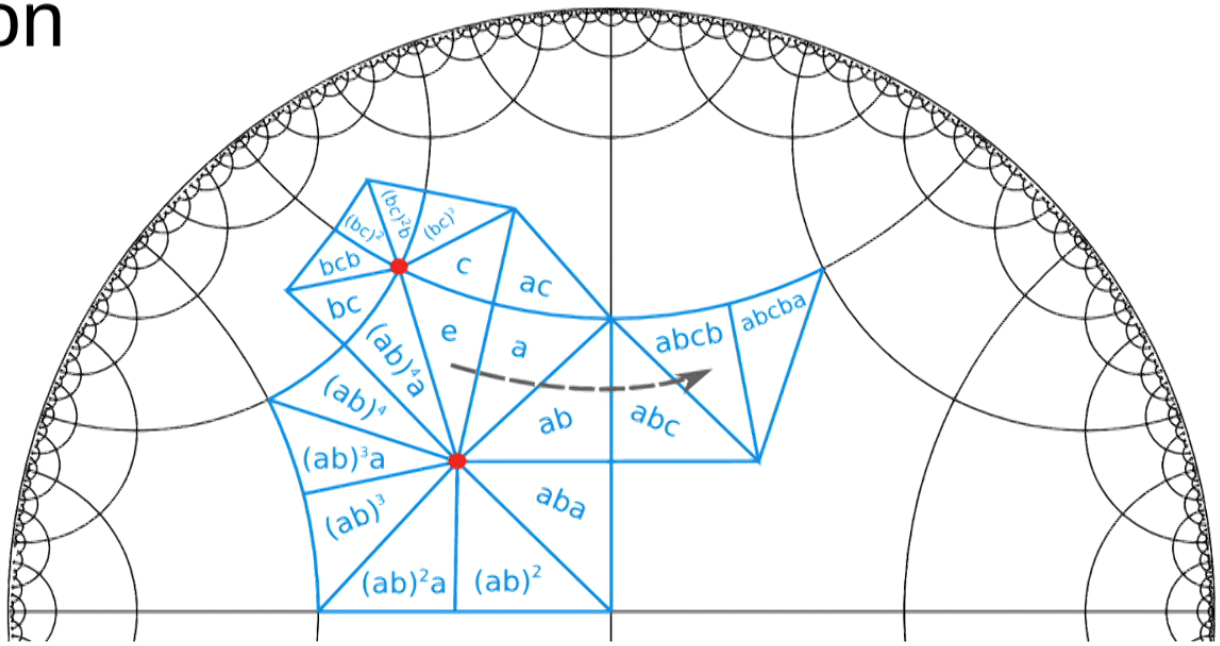
How can these codes be constructed?



Construction

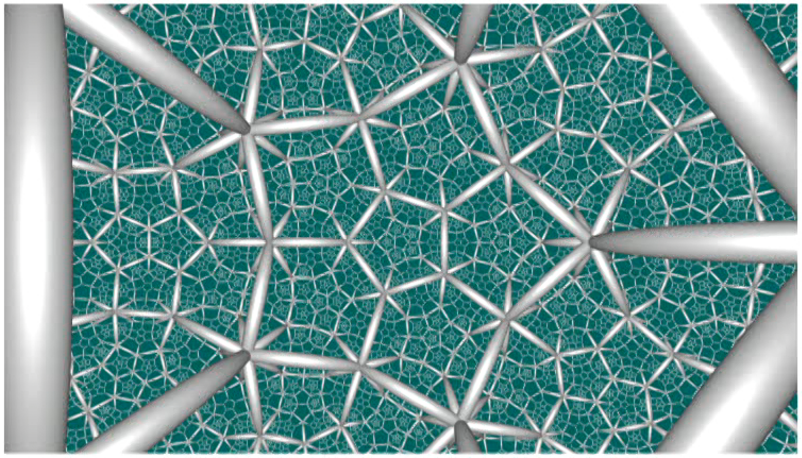


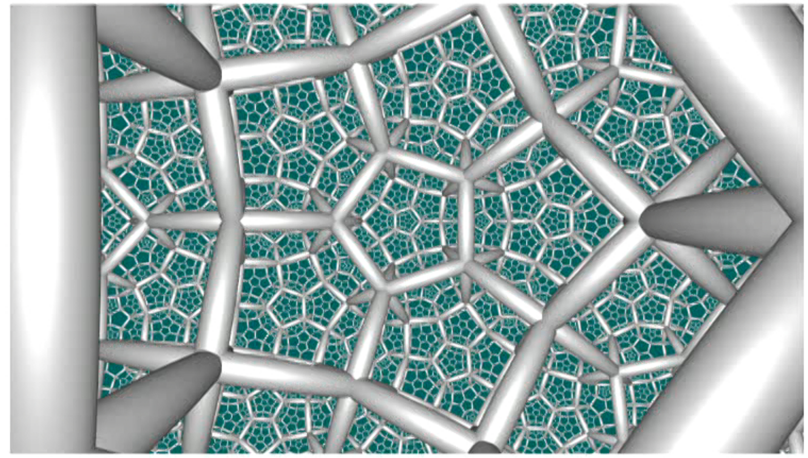
Construction

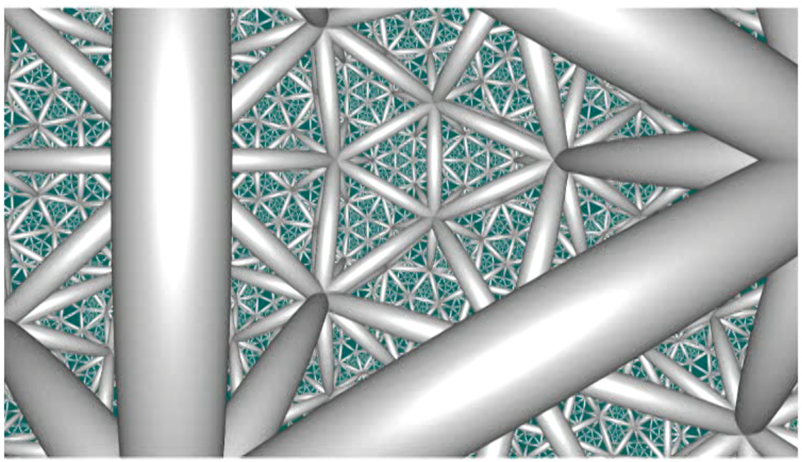


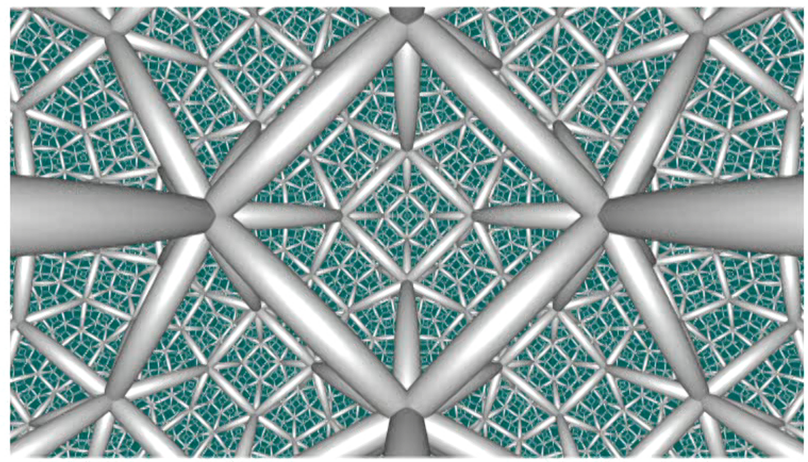
- Consider symmetry group of tessellation
- Group elements serve as (non-commutative) coordinates
- Identify fundamental triangles with group elements
- Procedure similar to “modding out translations” gives finite examples

Regular tessellations in 3D



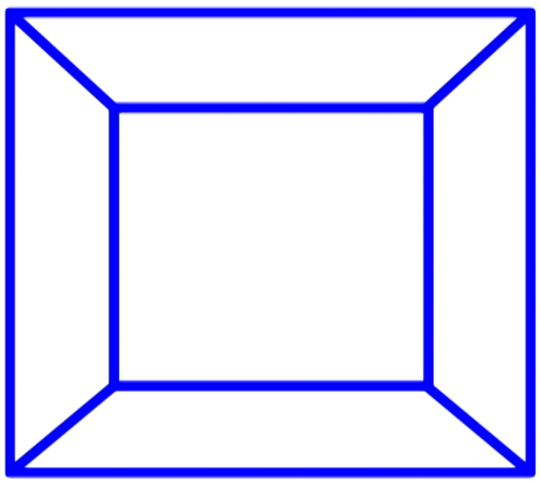


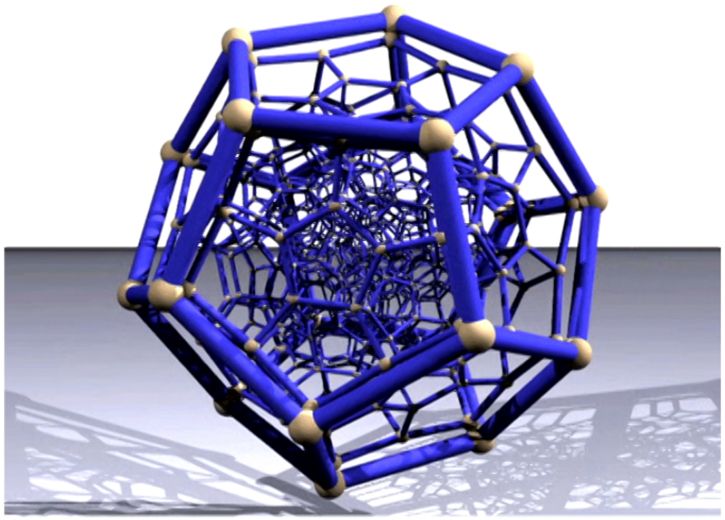




Tessellation of $\mathbb{H}^4$

- 5 regular tessellations
- Focus on {5,3,3,5} tessellation
- Self-dual tessellation by 120-cells
- 4D polytope with 120 dodecahedra at boundary





Hyperbolic codes: encoding rate k/n

Chern-Gauss-Bonnet Theorem:

$$\sum_{i=0}^{D}(-1)^i \dim H_i(M) = \frac{1}{(2\pi)^{\frac{D}{2}}}\int_M \mathrm{Pf}(\Omega)$$

4D

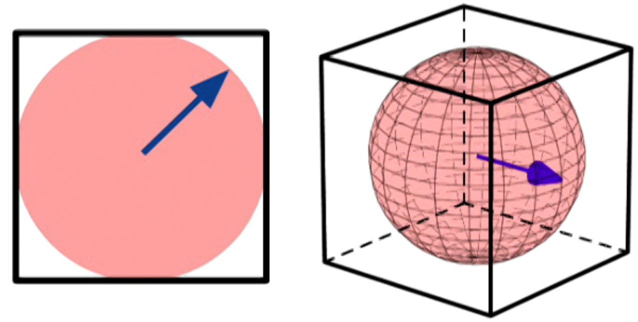
$$\dim H_2 \geq 2\frac{\mathrm{vol}(M)}{\mathrm{vol}(S^4)} - 2$$

$$k \geq const. \times n$$

Show that the constant is 13/72 for {5,3,3,5}

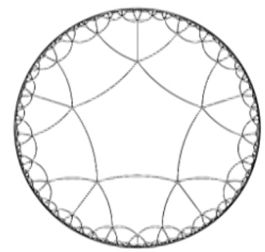
Hyperbolic codes: distance d

Definition: *Injectivity Radius* ***R*** -- largest radius of a **ball** that can be embedded without self-intersections



In hyperbolic space:

$$R \geq const. \times \log \mathrm{vol}_D(M)$$

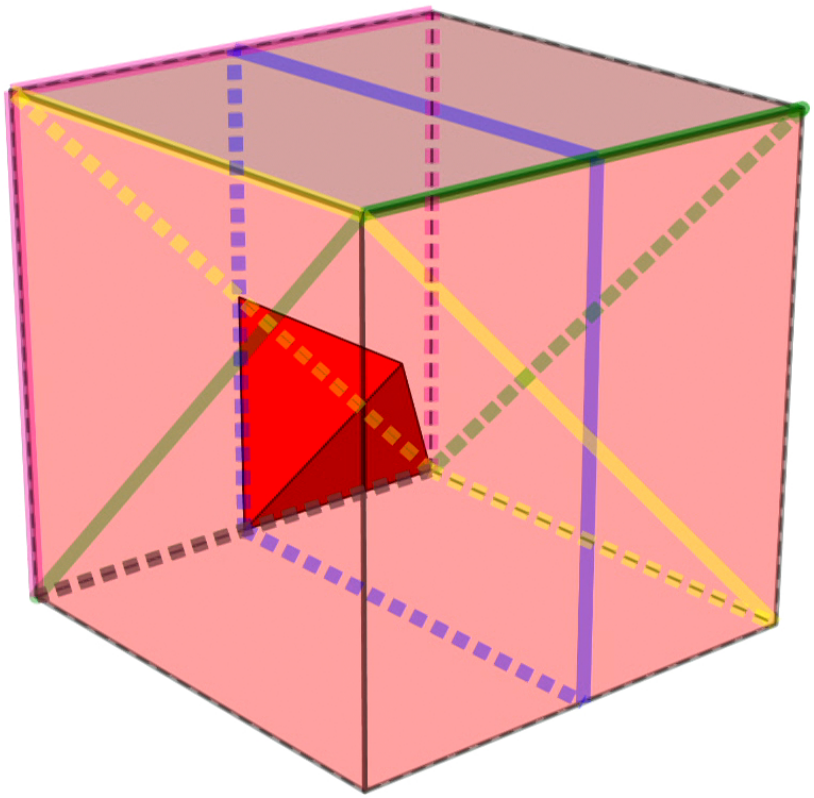


Anderson's Theorem: Volume of non-contractible i-cycle γ is lower bounded by volume of i-dimensional ball with radius being the injectivity radius R.

$$\mathrm{vol}_i(\gamma) \geq \mathrm{vol}_i(B_R) \geq const. \times \exp\left((i-1)R\right)$$

Guth-Lubotzky (2014): $d \geq const. \times n^{\epsilon} \quad \epsilon \in [0.1, 0.3]$

Same construction as in 2D



Subdivide tessellation into simplices (higher-dim. triangles)

For example, the translation

ababacbdedcbabacedcbaedced

gives [[144,72]] code

- Exhaustive search (computationally expensive)
- Randomized search

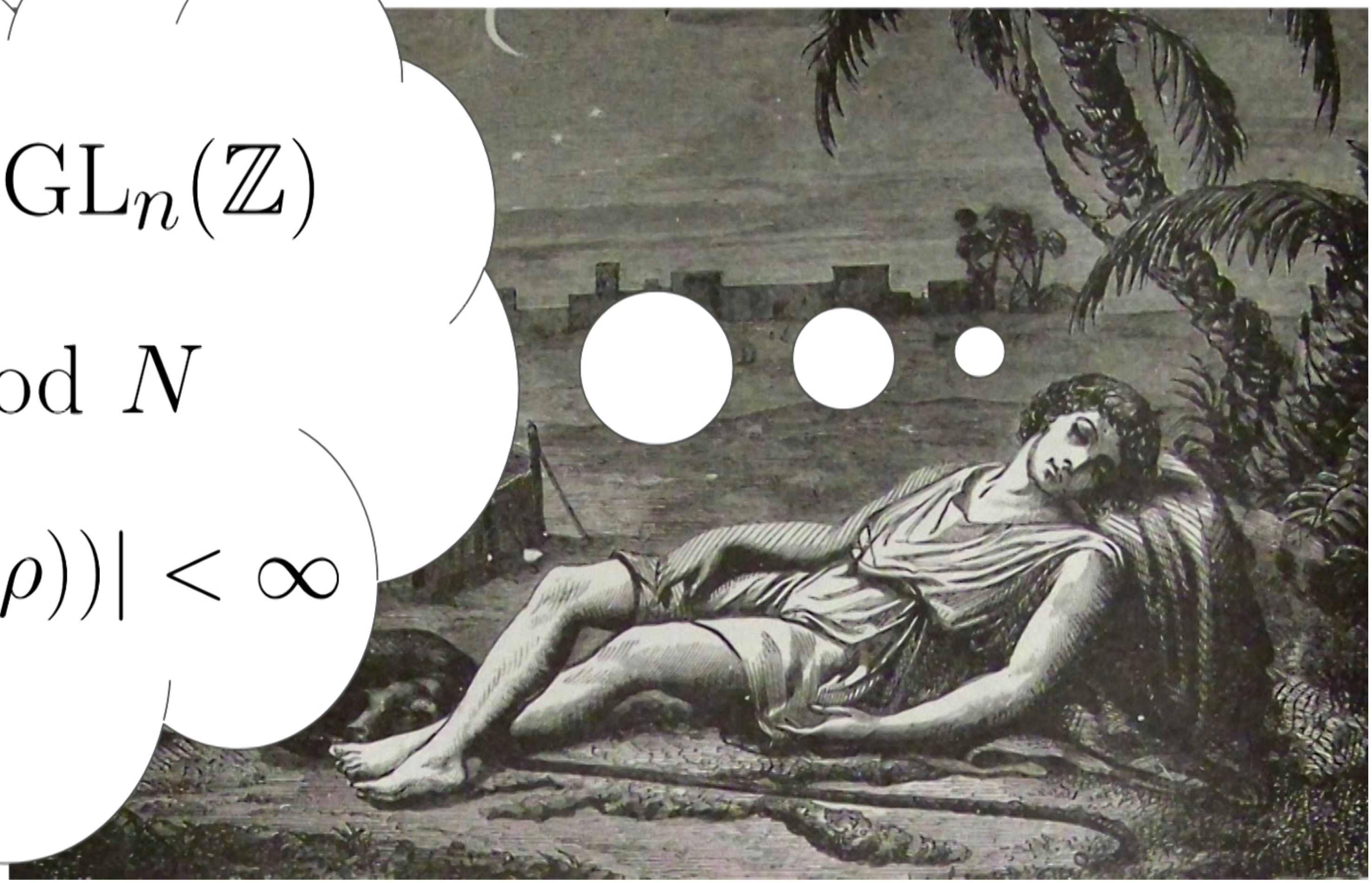
This method is not scalable

Construction via Linear Representation: Dream

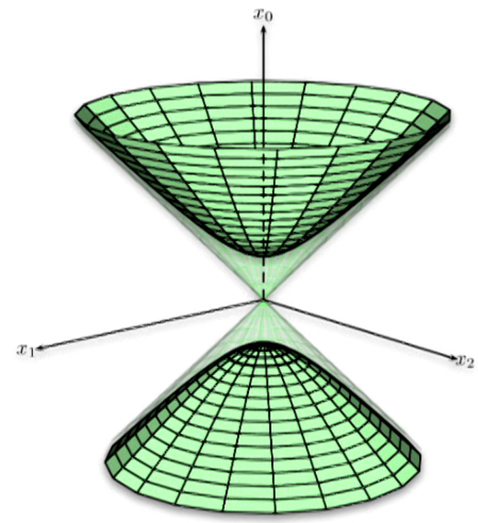
$$\rho : G \to \mathrm{GL}_n(\mathbb{Z})$$

$$A \mod N$$

$$|\mathrm{im}(\mathrm{mod} \circ \rho))| < \infty$$



Construction via Linear Representation



Can embed hyperbolic space into Minkowski space

$$\mathbb{H}^D = \left\{ x \in \mathbb{R}^{1,D} \,\middle|\, x \circ x = -x_0^2 + \sum_{i=1}^{D} x_i^2 = -1,\ x_0 > 0 \right\}$$

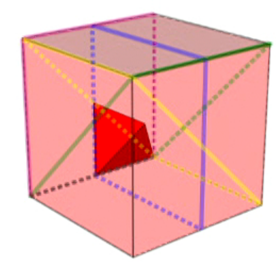
Symmetry group is orthochronous, homogeneous Lorentz group (generated by rotations and boosts)

$$O^+(1, D)$$

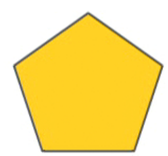
Change Gram-matrix of inner product to respect tessellation

$$g = \begin{bmatrix} 2 & \phi & 0 & 0 & 0 \\ \phi & 2 & -1 & 0 & 0 \\ 0 & -1 & 2 & -1 & 0 \\ 0 & 0 & -1 & 2 & \phi \\ 0 & 0 & 0 & \phi & 2 \end{bmatrix}$$

$$\rho(a_i) \cdot e_j = e_j - 2\,\frac{g_{i,j}}{g_{i,i}}\,e_i$$



$$\phi = \frac{1+\sqrt{5}}{2}$$



$$\rho : G \to \mathrm{GL}_5(\mathbb{Z}[\phi])$$

Construction via Linear Representation

Instead of factoring out number N we factor out maximal ideal I

$$I \subset \mathbb{Z}[\phi] \qquad \mathbb{Z}[\phi]/I \simeq \mathbb{F}_q$$

Work with polynomials

$$\mathbb{Z}[\phi] \simeq \mathbb{Z}[x]/\langle h \rangle \qquad h = x^2 - x - 1$$

Ideals come in two flavours

$$I = \langle p \rangle, \quad p \in \mathbb{P}$$

$$I = \langle p, g \rangle, \quad p \in \mathbb{P},\ g|h \text{ in } \mathbb{F}_p$$

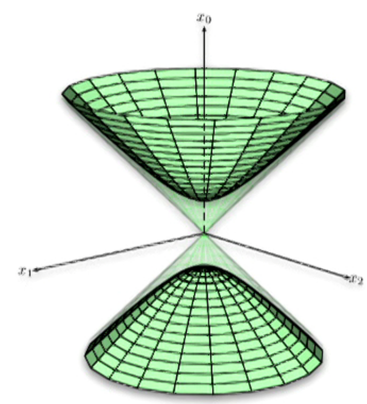
Construction via Linear Representation

Image of the full homogeneous Lorentz group O(1,D) under mod if I = <p>:

$$\mathrm{im}(\rho \circ \pi_I) \simeq \mathrm{GO}_5(q)$$

$GO_5(q)$ is group of 5x5 matrices which leave bilinear forms over F_q invariant

For characteristic > 2 it decomposes into simple groups as:



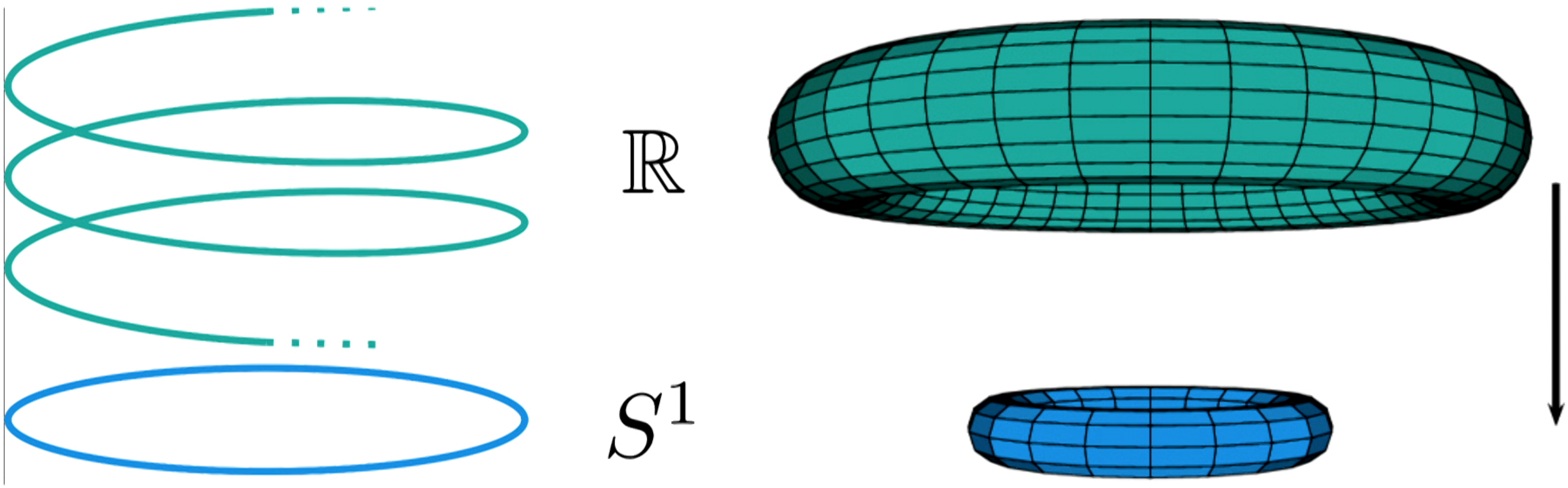
$$\mathrm{GO}_5(q) \simeq \Omega_5(q) \rtimes (C_2 \times C_2)$$

$$\mathrm{O}(1,3,\mathbb{R}) \simeq \mathrm{SO}^+(1,3,\mathbb{R}) \rtimes (C_2 \times C_2)$$

Standard counting argument gives order of $\Omega_5(q)$:

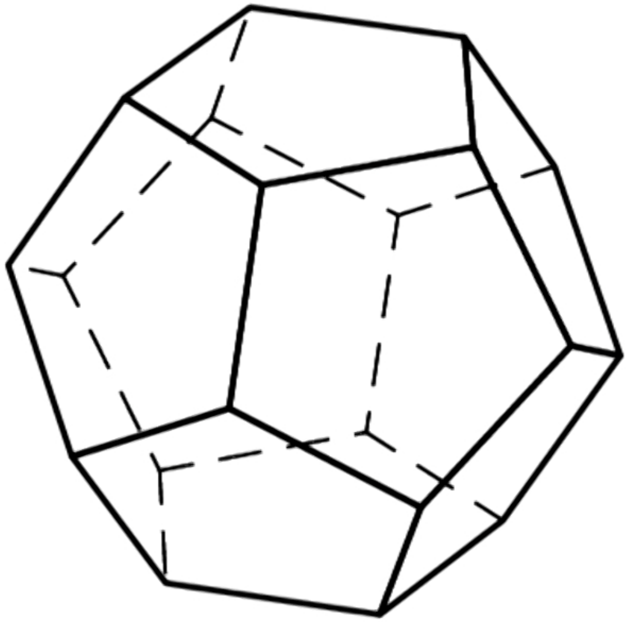
$$|\Omega_5(q) \rtimes C_2| = q^{10} - q^8 - q^6 + q^4$$

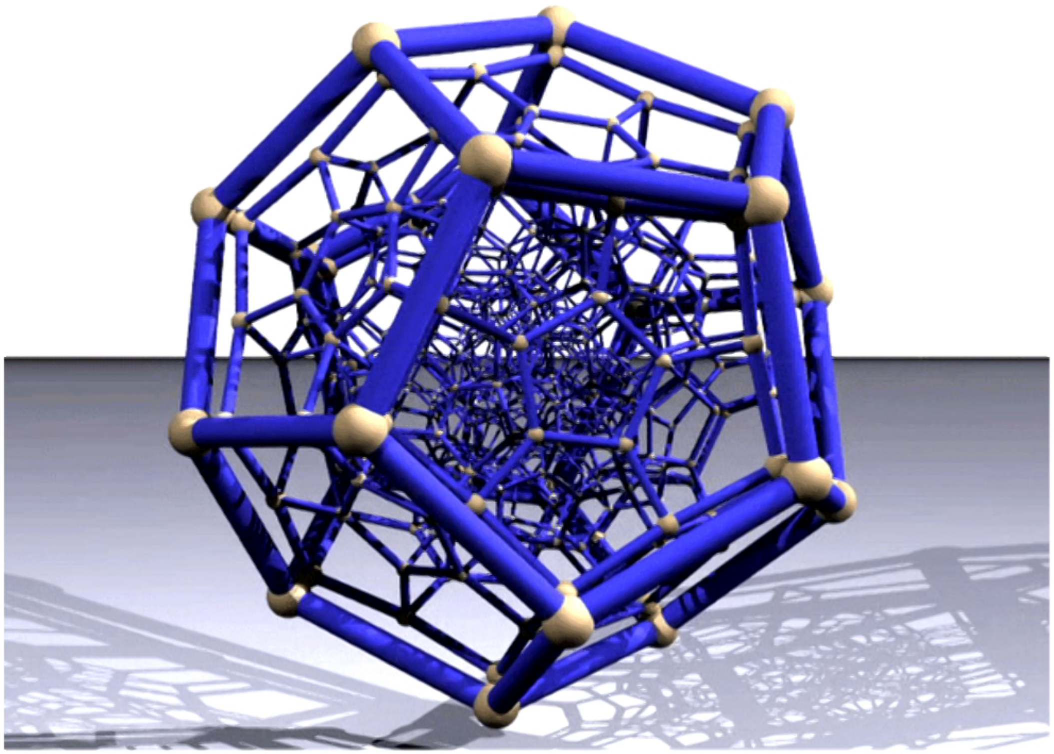
Obtain less symmetric examples:
Construction via Topological Coverings



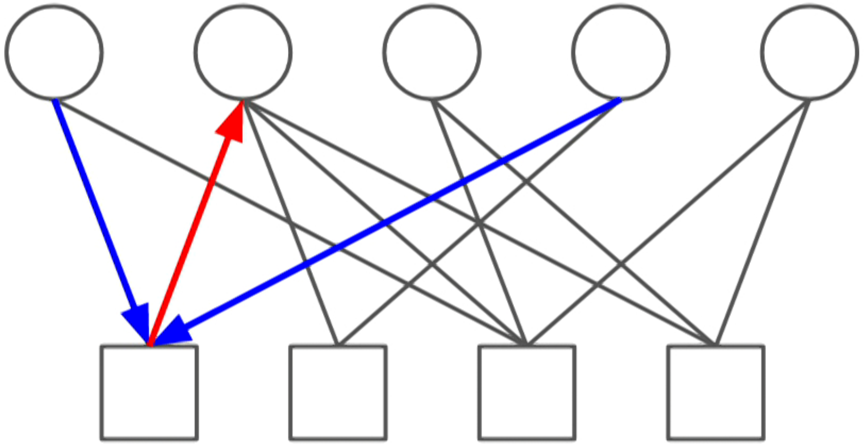
#	n	k	ideal	structure	Euler characteristic χ
1	144	72	–	$(\mathrm{SL}_2(5) \rtimes \mathrm{A}_5) \rtimes \mathbb{Z}_2$	26
2	720	184	–	125-fold covered by 10, $\mathbb{Z}_5 \times \mathbb{Z}_5 \times \mathbb{Z}_5$	130
3	3,264	744	–	3-fold covered by 6, $\mathbb{Z}_3$	636
4	3,600	736	–	25-fold covered by 10, $\mathbb{Z}_5 \times \mathbb{Z}_5$	650
5	4,896	1,124	–	2-fold covered by 6, $\mathbb{Z}_2$	968
6	9,792	2,200	$\langle 2 \rangle$	$\Omega_5(4)$	1,904
7	18,000	3,624	–	5-fold covered by 10, $\mathbb{Z}_5$	3,250
8	18,432	4,232	–	$\mathbb{Z}_2^{\times 8} \rtimes [(\mathrm{A}_5 \rtimes \mathrm{A}_5) \rtimes \mathbb{Z}_2]$	3,584
9	19,584	4,324	–	$\Omega_5(4) \rtimes \mathbb{Z}_2$	3,808
10	90,000	18,024	$\langle \sqrt{5} \rangle$	$\left[\left(\mathbb{Z}_5^{\times 4} \rtimes \mathrm{SL}_2(5)\right) \rtimes \mathrm{A}_5\right] \rtimes \mathbb{Z}_2$	16,250
11	34,432,128	?	$\langle 3 \rangle$	$\Omega_5(9) \rtimes \mathbb{Z}_2$	6,216,912
12	257,213,088	?	$\langle 11 \rangle$	$\Omega_5(11) \rtimes \mathbb{Z}_2$	46,441,252
13	61,140,357,792	?	$\langle 19 \rangle$	$\Omega_5(19) \rtimes \mathbb{Z}_2$	11,039,231,268

Smallest example: Davis manifold

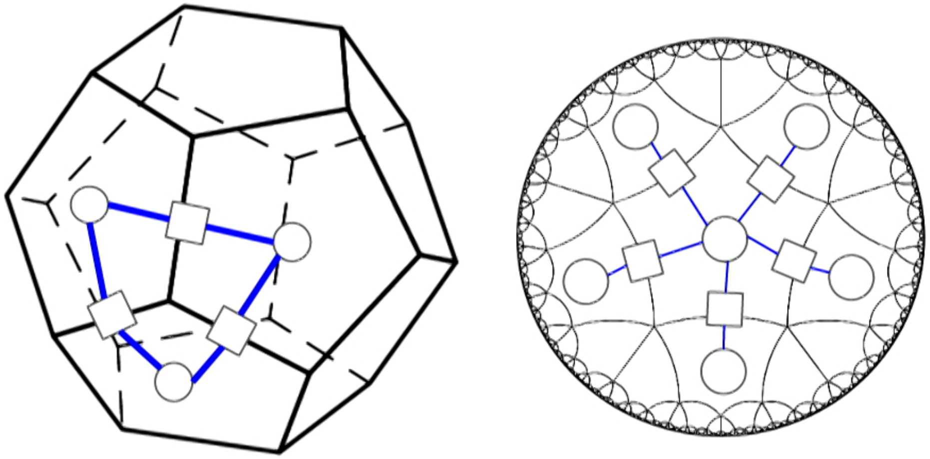




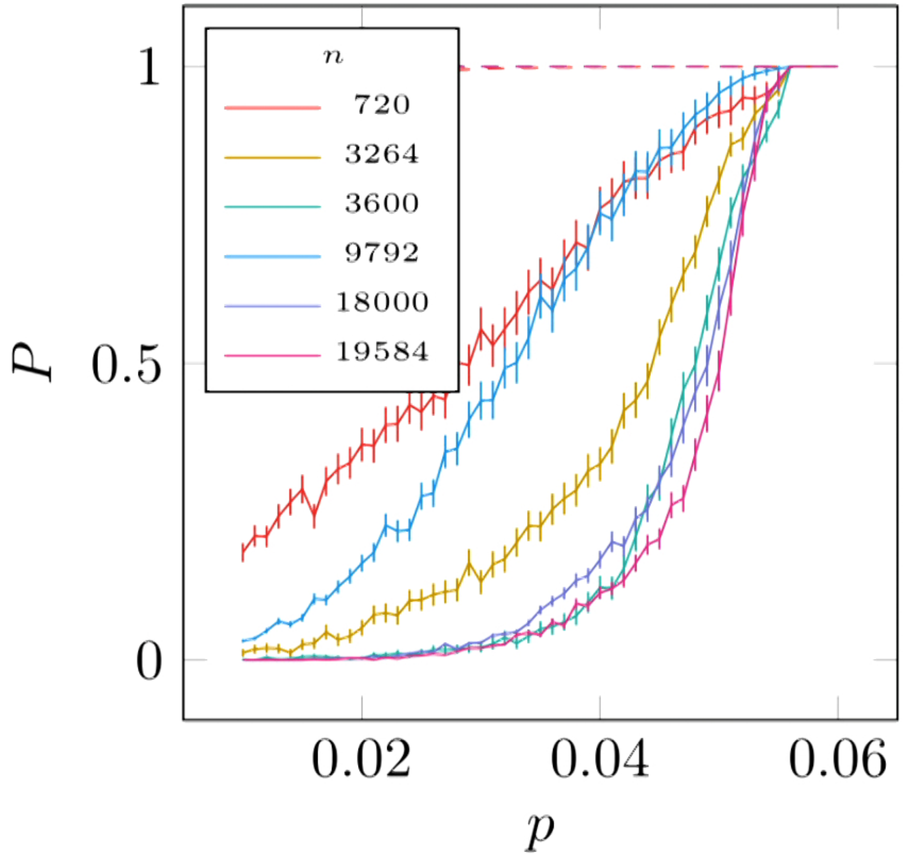
Belief Propagation



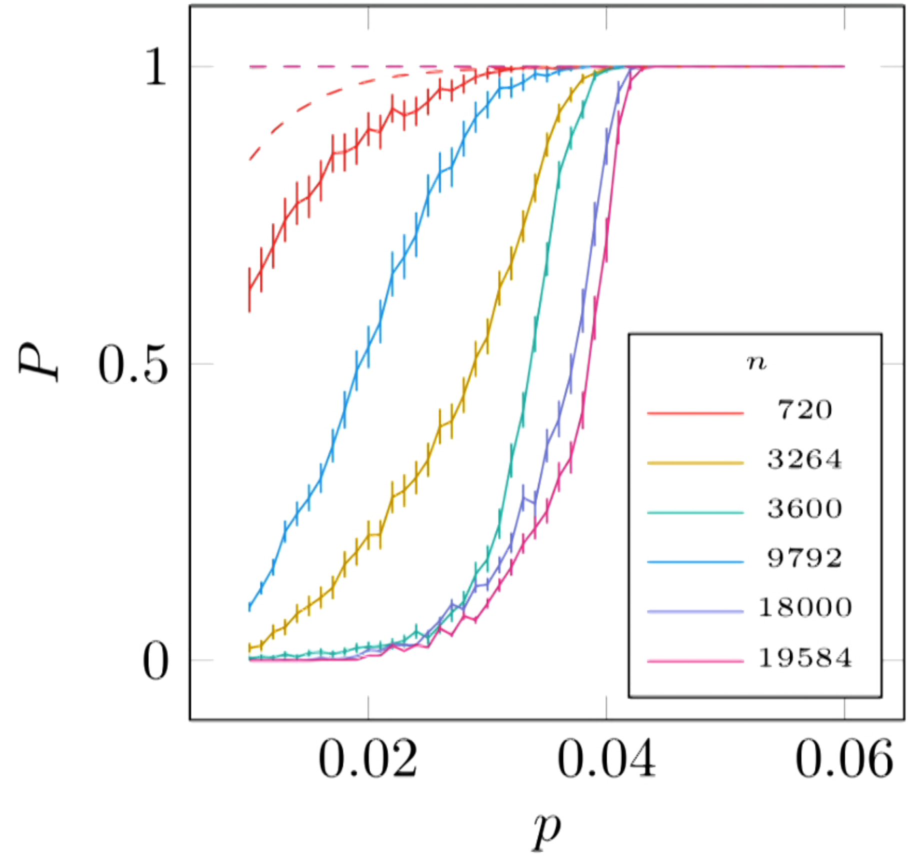
- Decoder for classical LDPC codes
- Very low computational complexity
- Operates iteratively via message passing



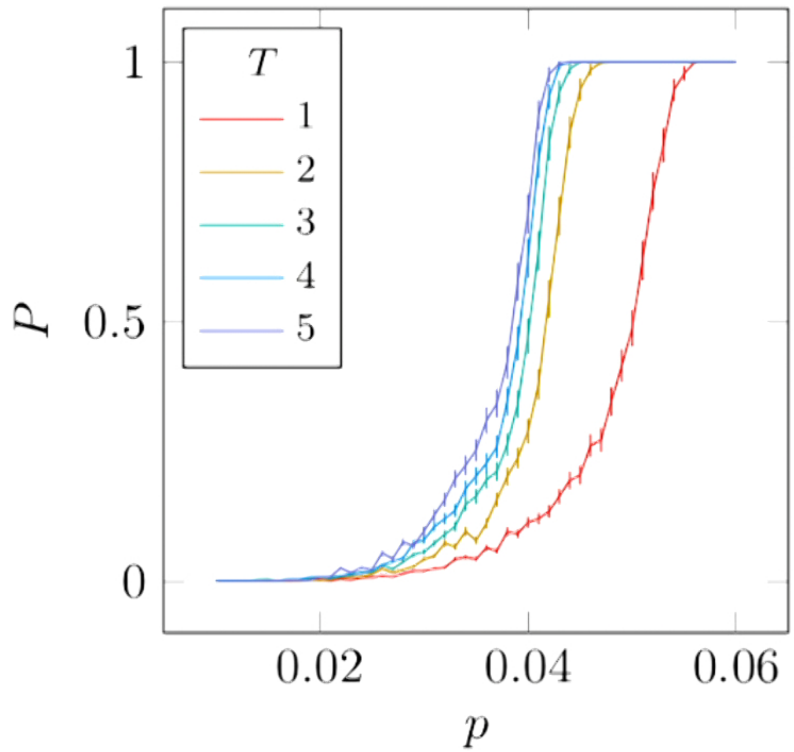
- Expect to work well because
  - girth is 6
  - is an expander
  - qubit degree is 5



Perfect Measurements



Noisy Measurements



Increasing number of rounds for fixed system size

Work in Progress

Two open issues:

- We use a ‘vanilla’ version of BP: very likely that the result can be improved
- High stabilizer weight

Weight reduction

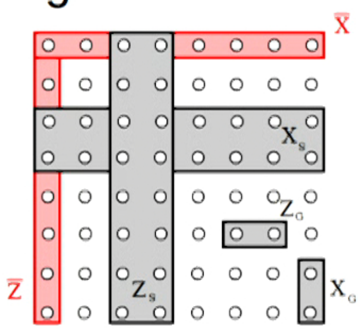
General method to reduce stabilizer weights by Hastings [arXiv:1611.03790]:

- Associate a 2D cell complex with code and perform local operations
- Can be used to turn non-LDPC codes LDPC
- Checks turn out to be constant size but large

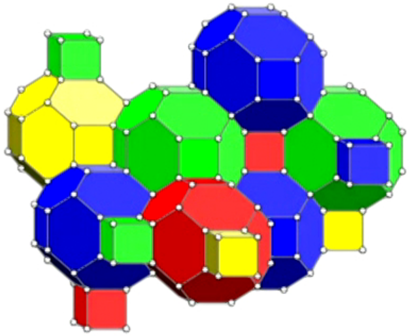
Weight reduction

Alternative strategy: **Subsystem codes**

- Break up stabilizer checks into smaller pieces (gauge operators)
- Gauge operators do not commute
- Measuring them gives random outcomes
- Their product gives outcome of stabilizer measurement



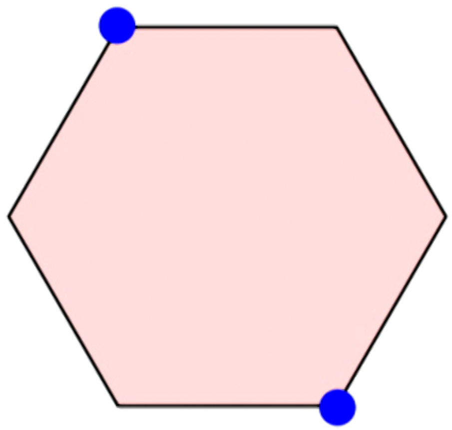
Bacon-Shor Code



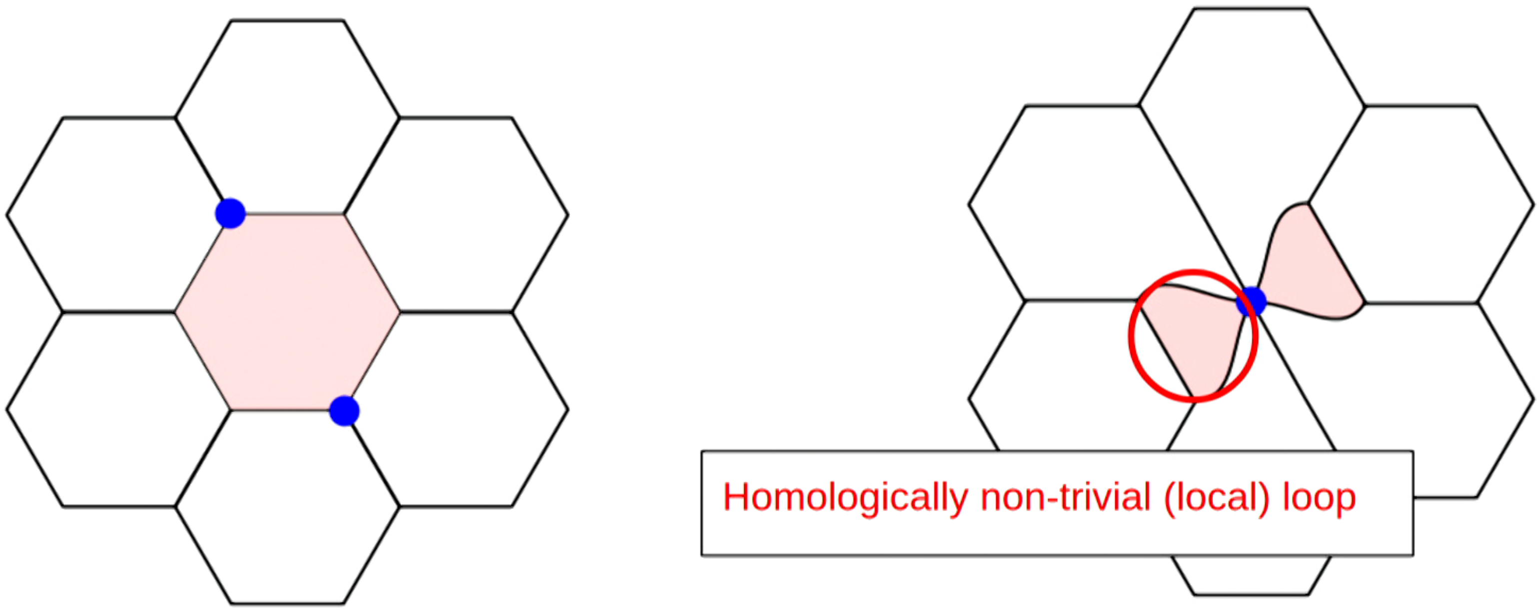
3D Gauge Color Code

Our work: general method to turn a CSS LDPC code into a subsystem code.

LDPC Subsystem Construction



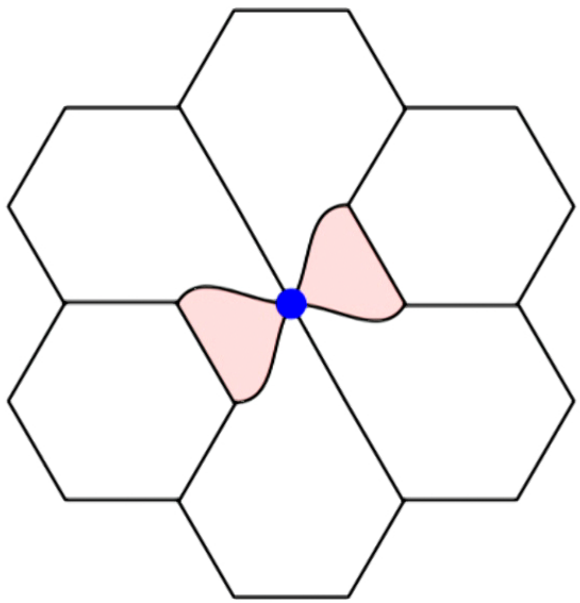
LDPC Subsystem Construction

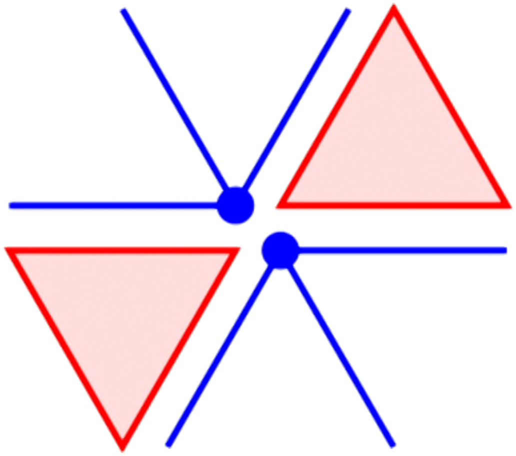


All stabilizers still commute!

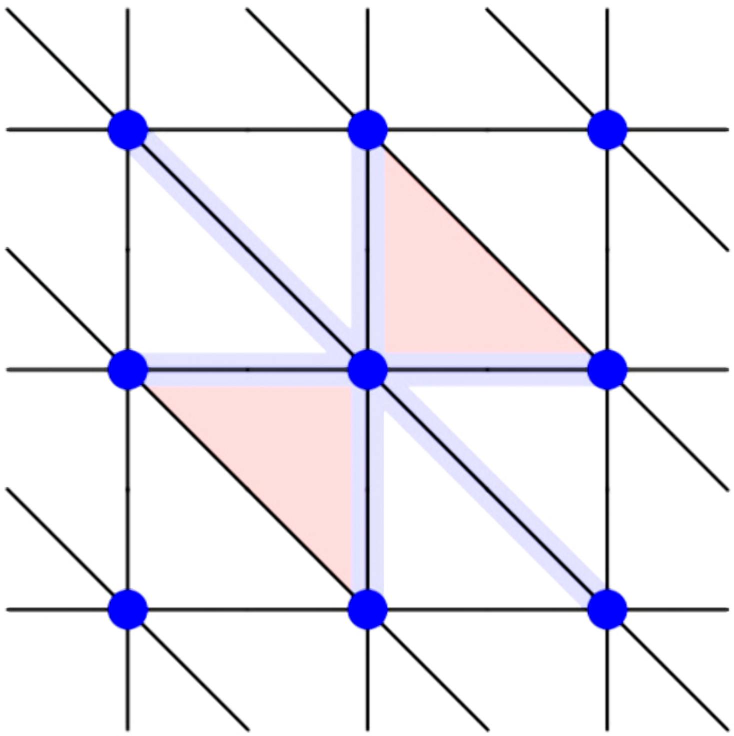
encoded qubits = # physical qubits - # independent checks

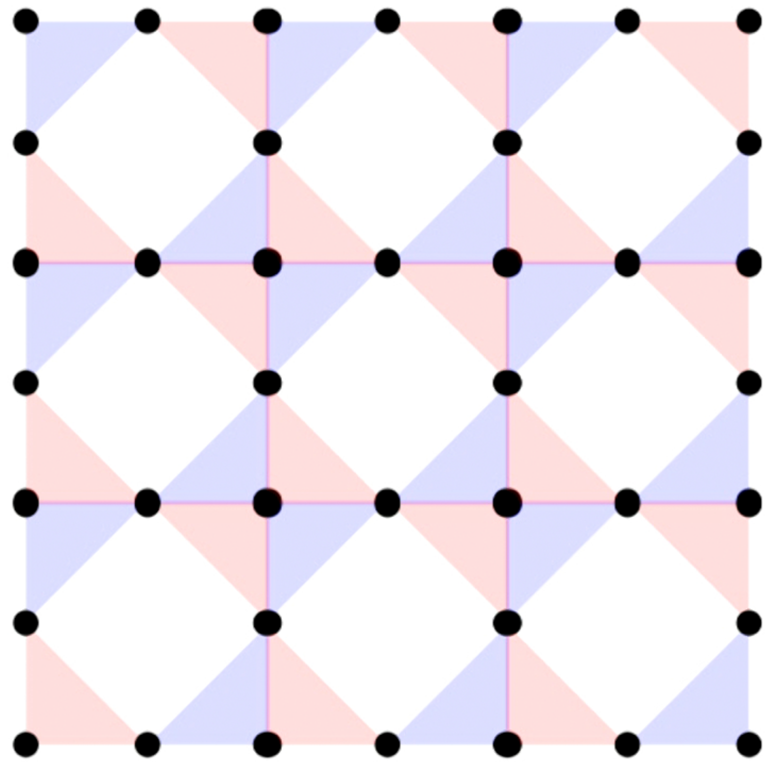
LDPC Subsystem Construction





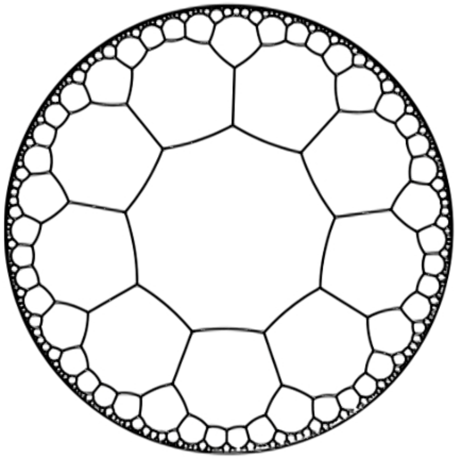
LDPC Subsystem Construction



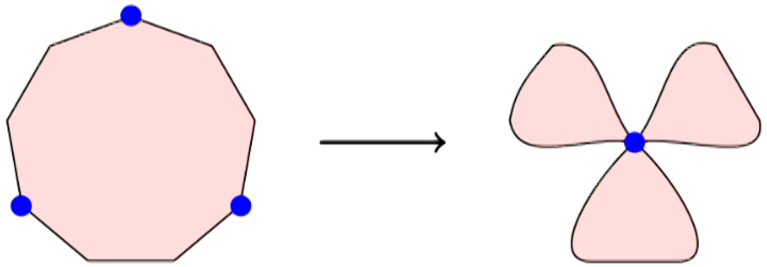


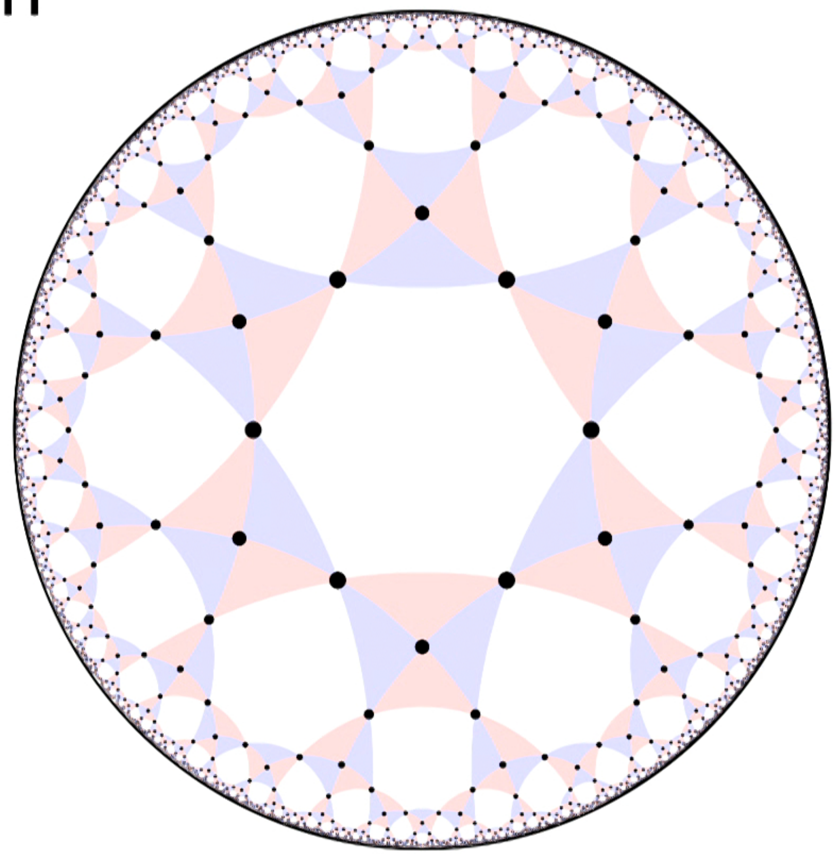
Turned weight-6 and weigh-3 checks into weight-3 gauge checks. Bravyi et.al. ‘13

LDPC Subsystem Construction



Merge several X-checks

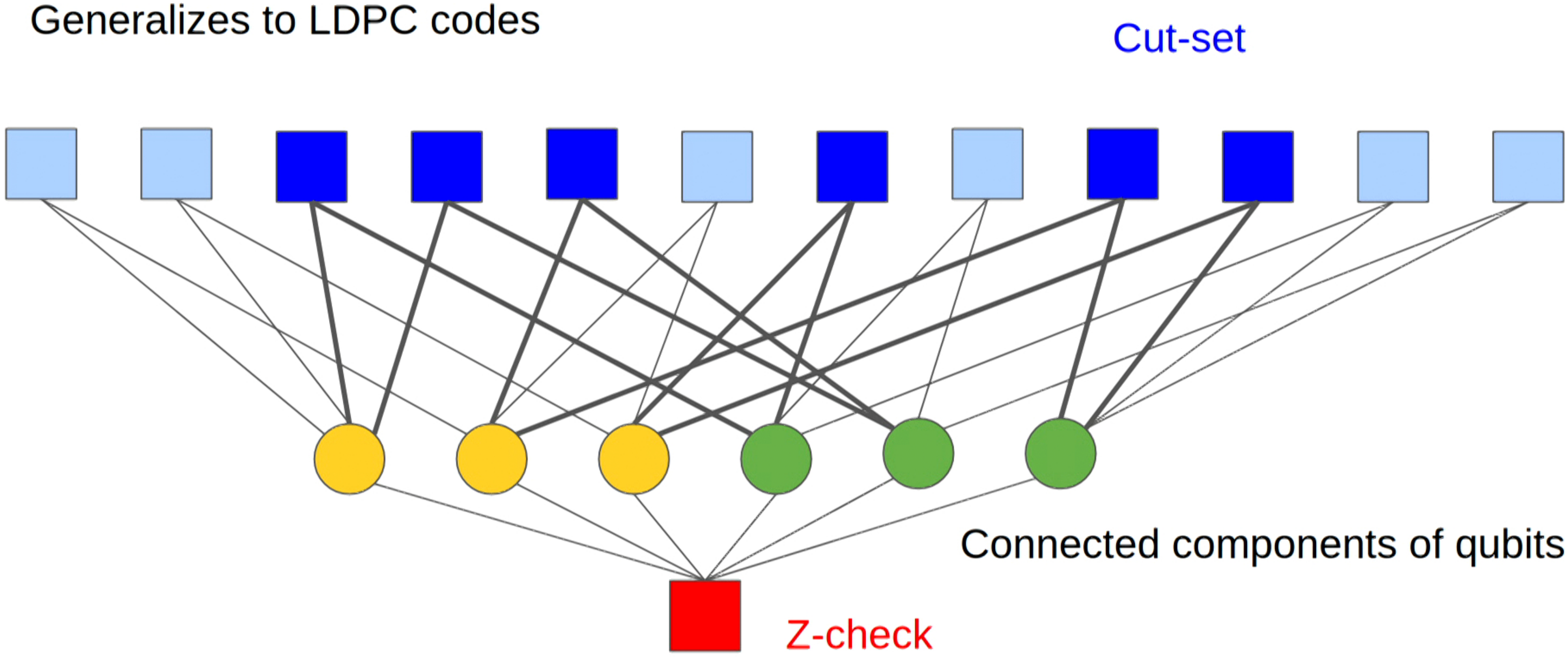




Obtain code with k = n/9 and weight-3 checks

LDPC Subsystem Construction

Generalizes to LDPC codes



LDPC Subsystem Construction

Advantages:

- Low check weight makes measurements much simpler to facilitate
- Errors on gauge operators
- Support of logical operators unaffected
- Support of logical + gauge reduced (by a factor depending on check-weight)

But: Still needs to be combined to a higher-weight stabilizer

$\Rightarrow$ Do not expect improvement in threshold

LDPC Subsystem Construction

Threshold can be improved when noise is biased ($p_Z > p_X$):

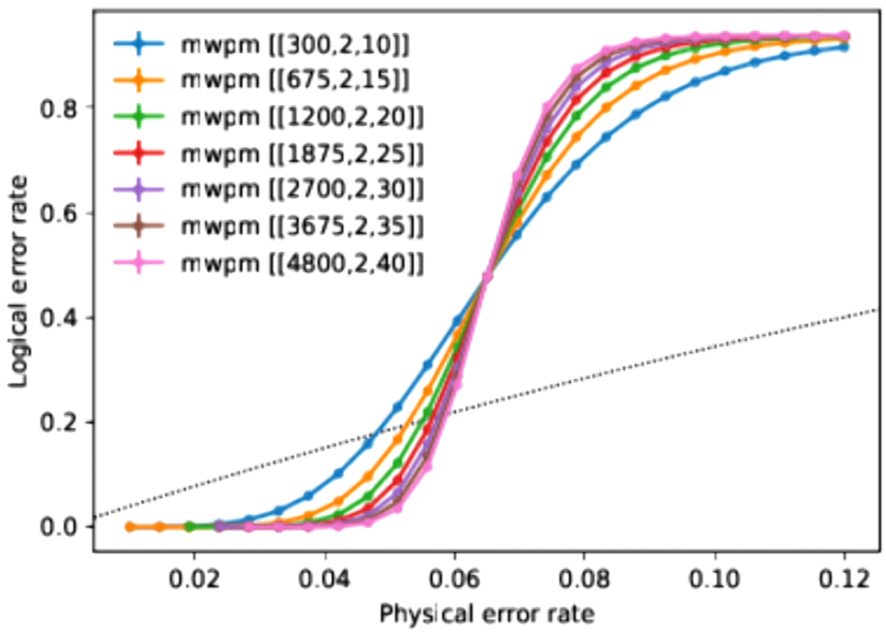
Gauge-switching

'Change our mind' about what constitutes a stabilizer:

Add commutative set of (low-weight) gauge operators to stabilizer group

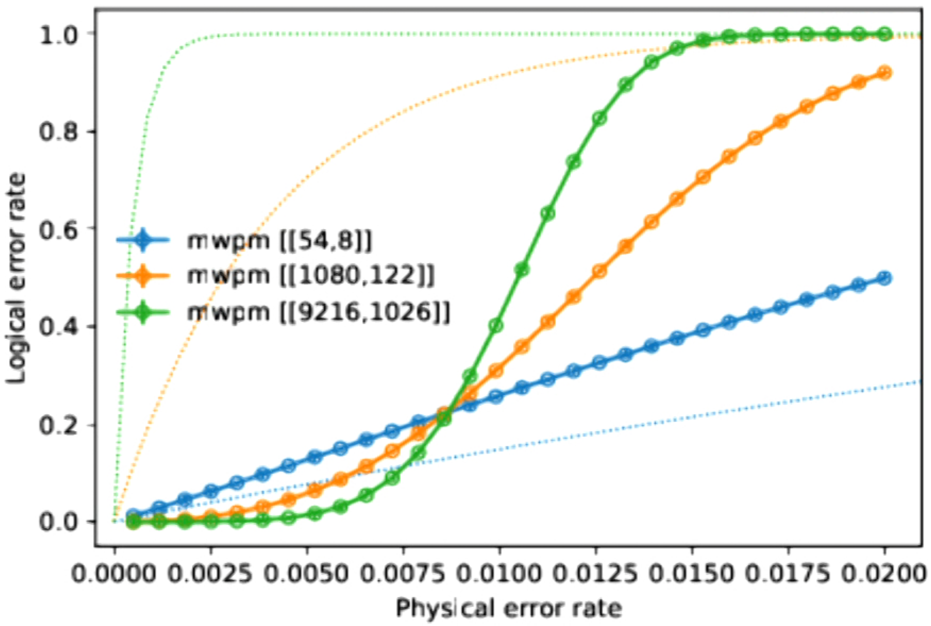
Recent work by Tuckett et.al. (2019) using different approach

Toric Code Gauge Switching

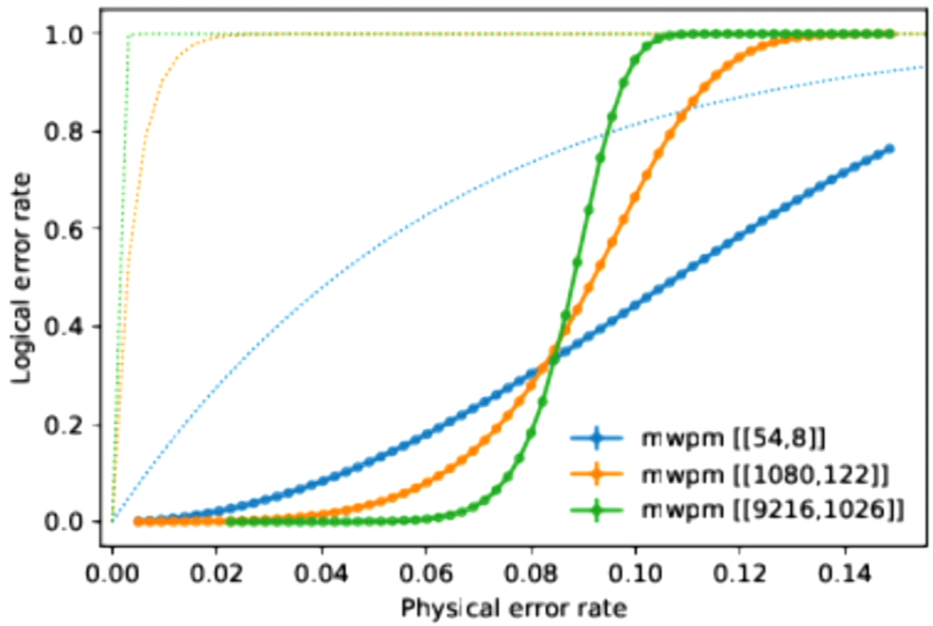


Unbiased noise (indep. X/Z)

Hyperbolic Codes Gauge Switching

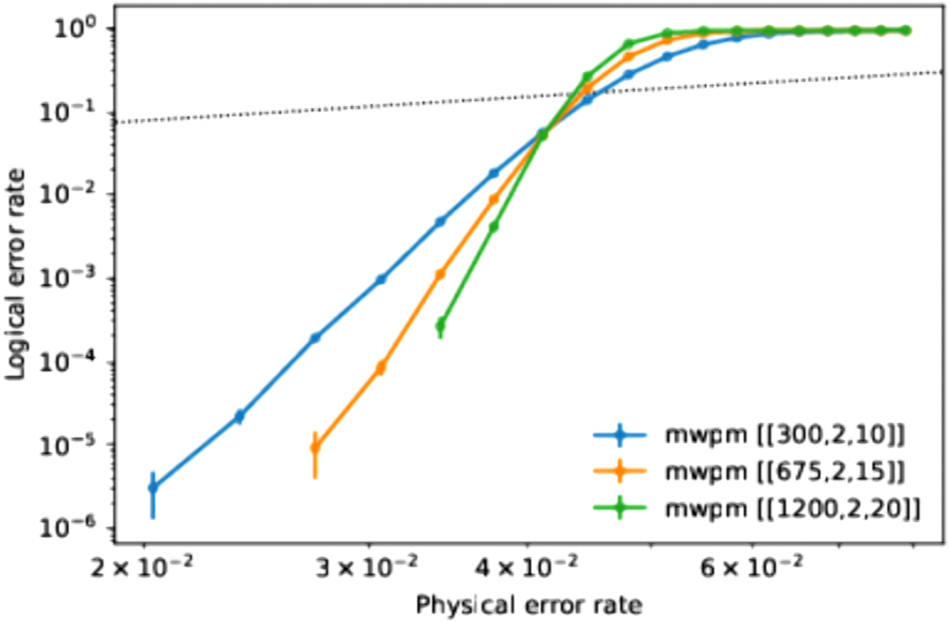


Unbiased noise (indep. X/Z)

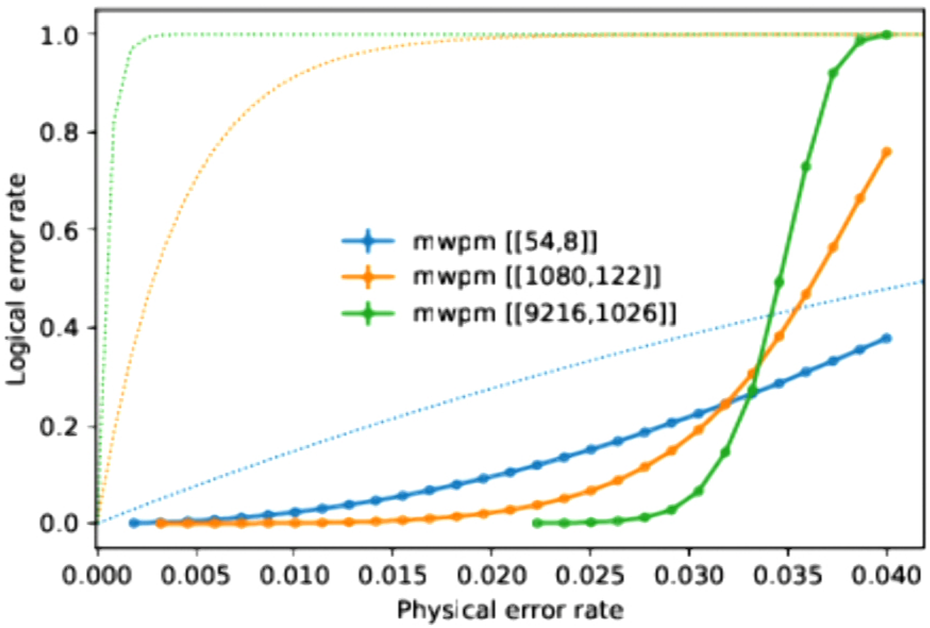


Biased noise ($p_z >> p_x$)

Noisy Measurements



Toric Code



Hyperbolic Code

Summary

4D hyperbolic codes:

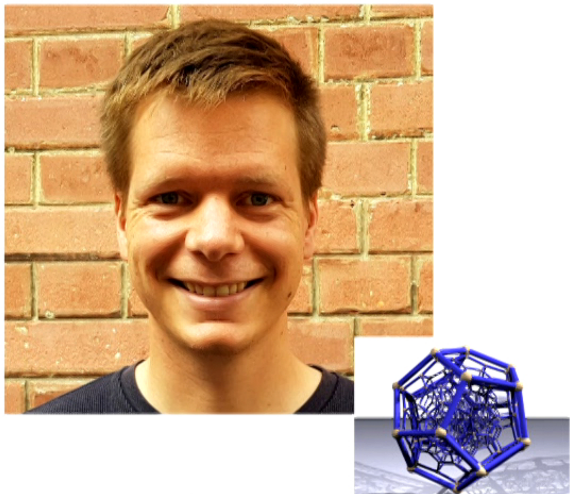
- Gave construction of this code family
- several 4D hyperbolic manifolds
- Code family has ~20% encoding rate
- BP decoding with noisy syndrome (p=q): results consistent with p_c~4%

Preliminary results on LDPC subsystem code construction:

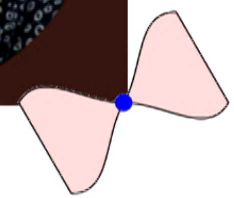
- Can locally merge and break checks into gauge operators
- ‘Balancing’ check weights

Thank you for your attention!

Questions?

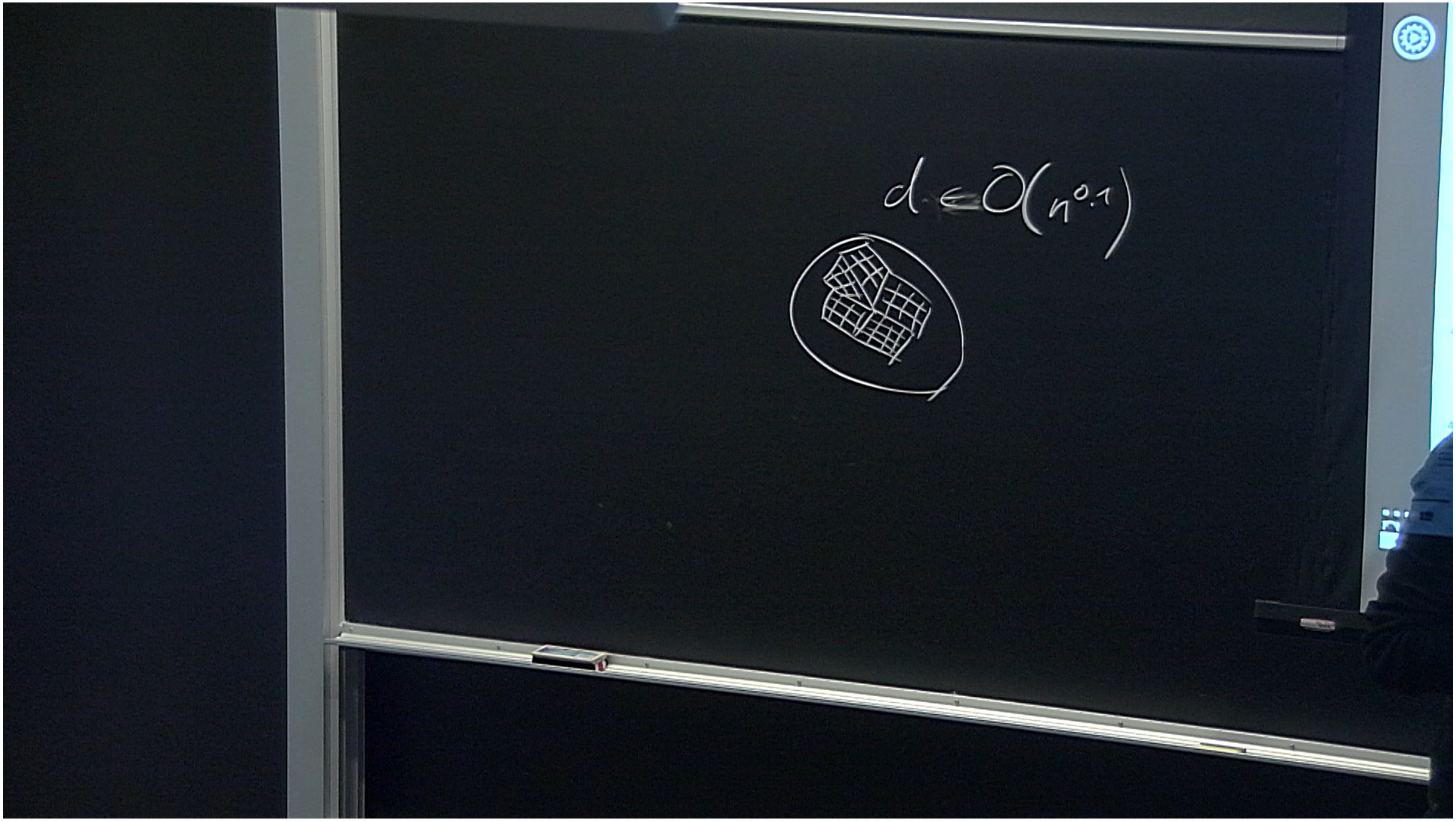


Vivien Londe



Oscar Higgott

arXiv:2001.03568


$d \in O(n^{0.1})$