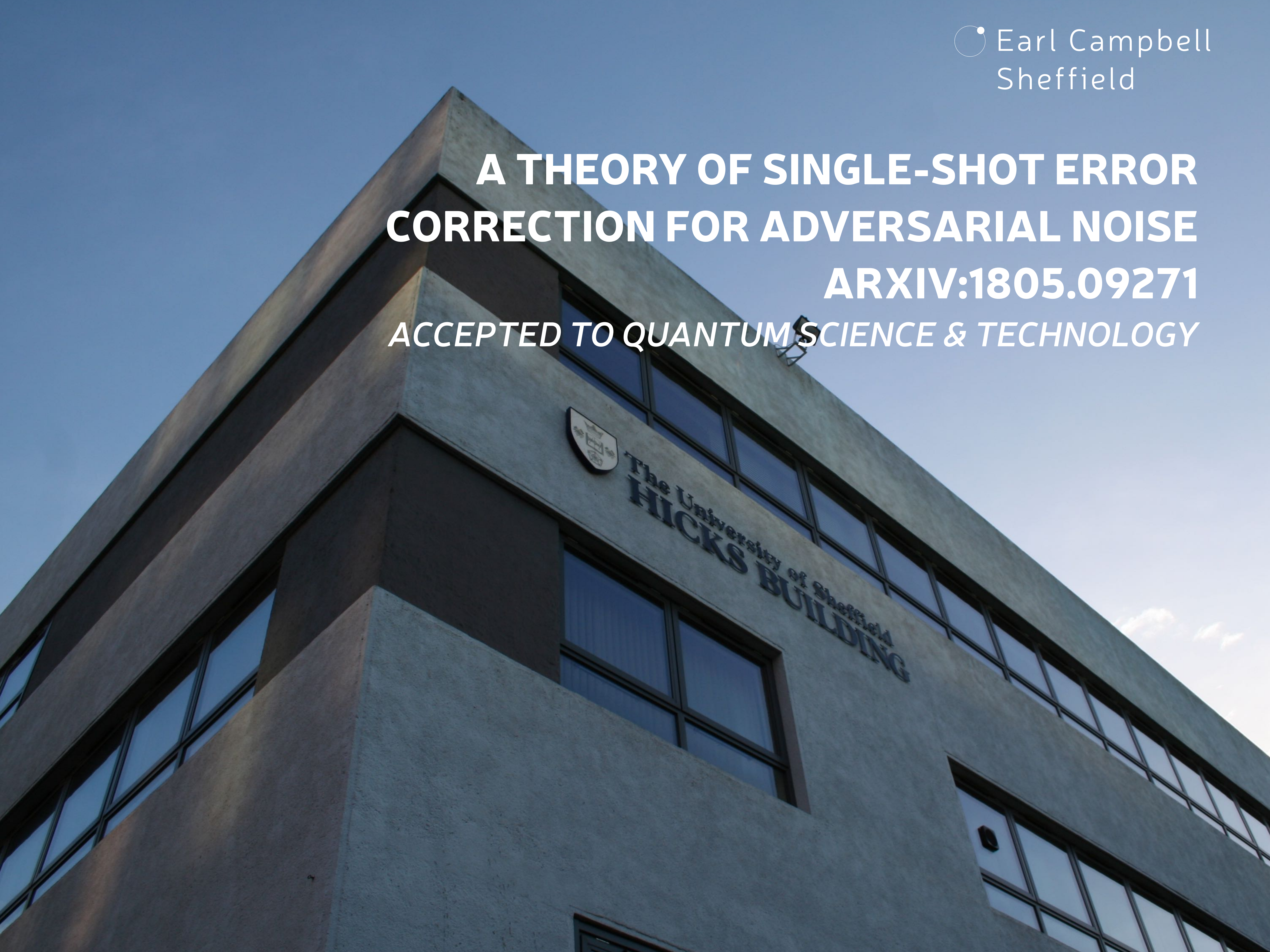
Earl Campbell
Sheffield

A THEORY OF SINGLE-SHOT ERROR CORRECTION FOR ADVERSARIAL NOISE

ARXIV:1805.09271

ACCEPTED TO QUANTUM SCIENCE & TECHNOLOGY



Sheffield

my group works on:

Quantum error correction

Magic state distillation

Circuit compilation

Resource estimation

Classical simulation methods

Magic theory

“Old” South Wales

my place of birth!

what?

Deal with **noisy measurements** without measurement repetition.

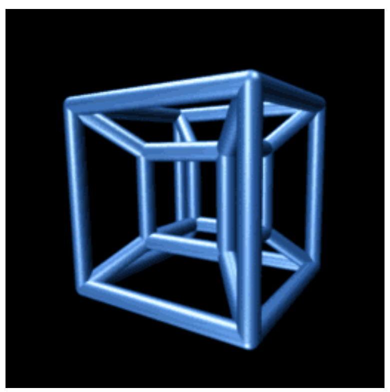
Fault tolerance in a single shot
Bombin Phys. Rev. X 5, 031043 2015 / QIP2015

why?

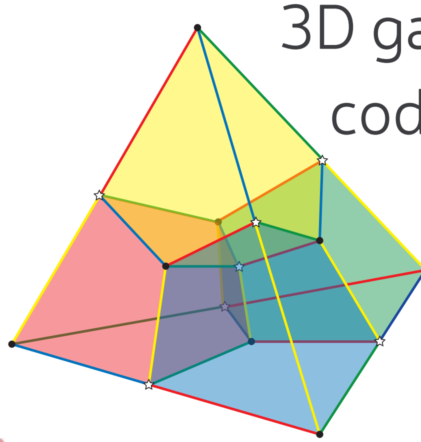
faster: no need for **d** repeated measurements

more reliable: handles time correlated noise / fabrication faults
Bombin Phys. Rev. X 6, 041034 (2016) / QIP2017

Topological single shot codes



4D topological codes



3D gauge codes

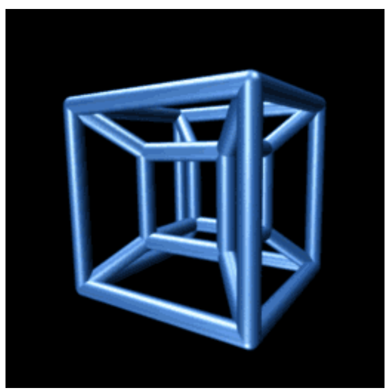
Trade off bounds

Bravyi-Poulin-Terhal PRL (2010)

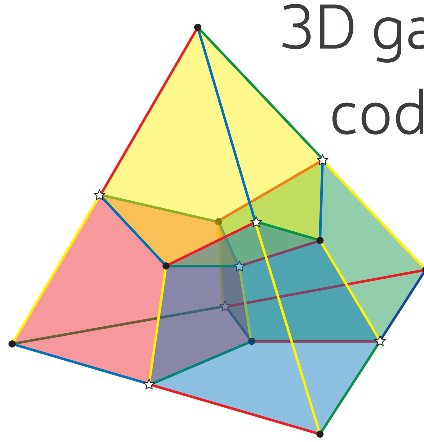
e.g. in 2D constrained by $kd^2 = O(n)$

All single shot codes

Topological single shot codes



4D topological codes



3D gauge codes

?????

Codes with better [[n,k,d]] parameters

????

Key results

Given any classical code
use homological product
to construct quantum "*single shot*" code

classical LDPC -> quantum LDPC

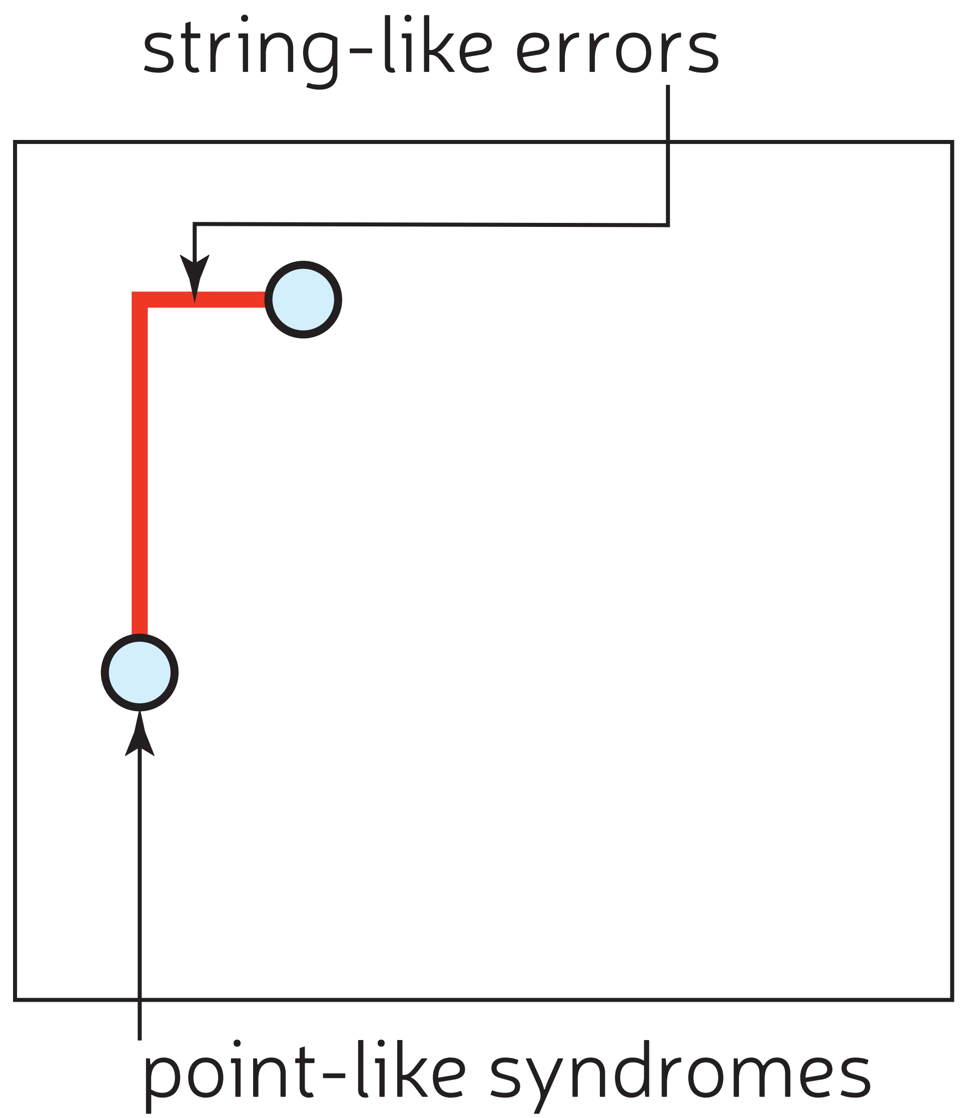
+ 4 mini-results on
foundations of single-shot error correction

1. Review single-shot
2. 3 mini-results
3. The homological product codes

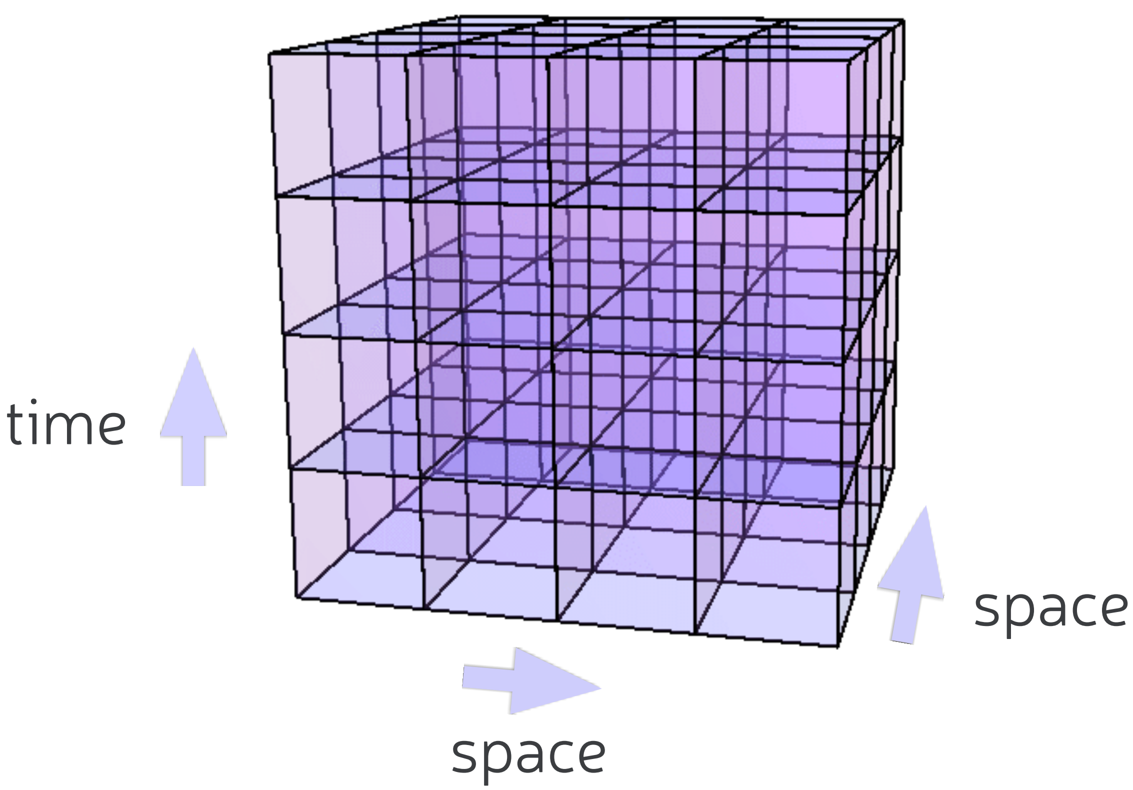
Noisy measurement problem in Toric code problem:

two measurement errors

looks same as long qubit error

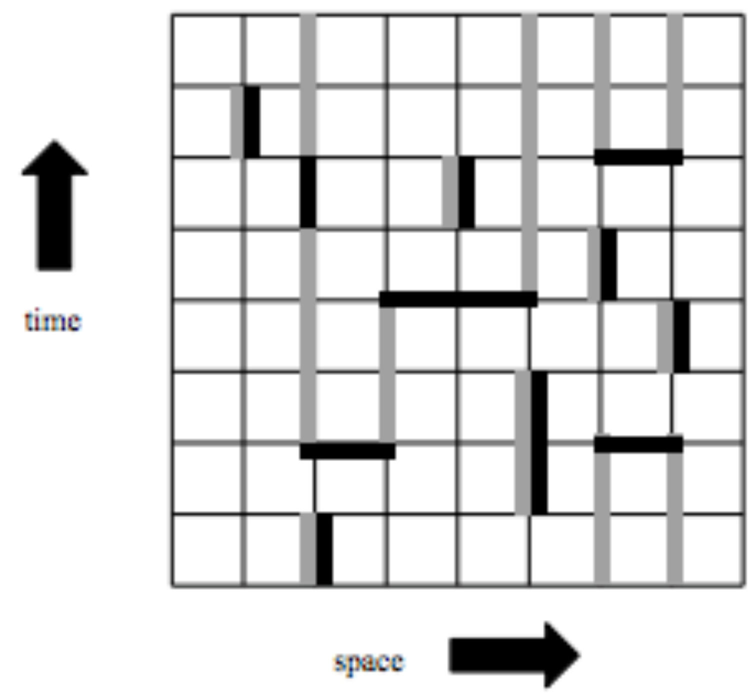


Solution for toric code: repeat measurements



2D Toric code: with history of measurement date leads to 3D space-time.

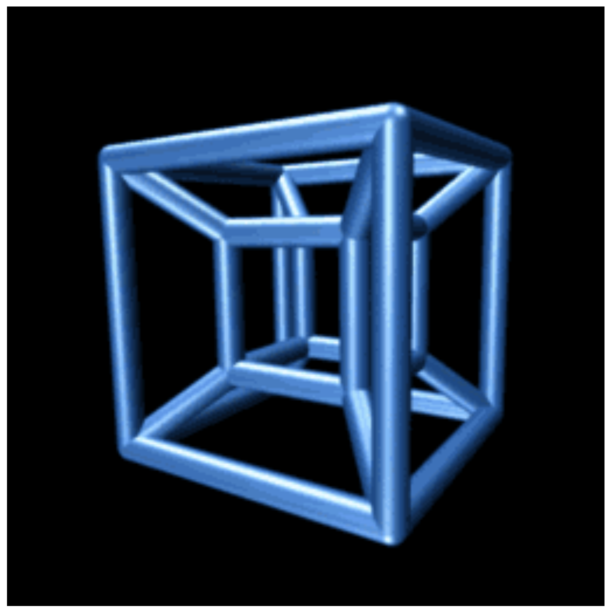
Perform minimum weight decoding in space-time picture.

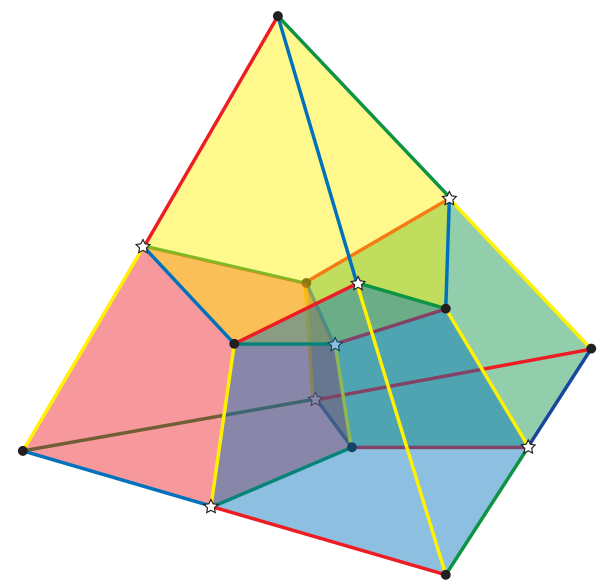


2D cross section from [Dennis Kitaev Preskill '01]

Single shot: the basic idea

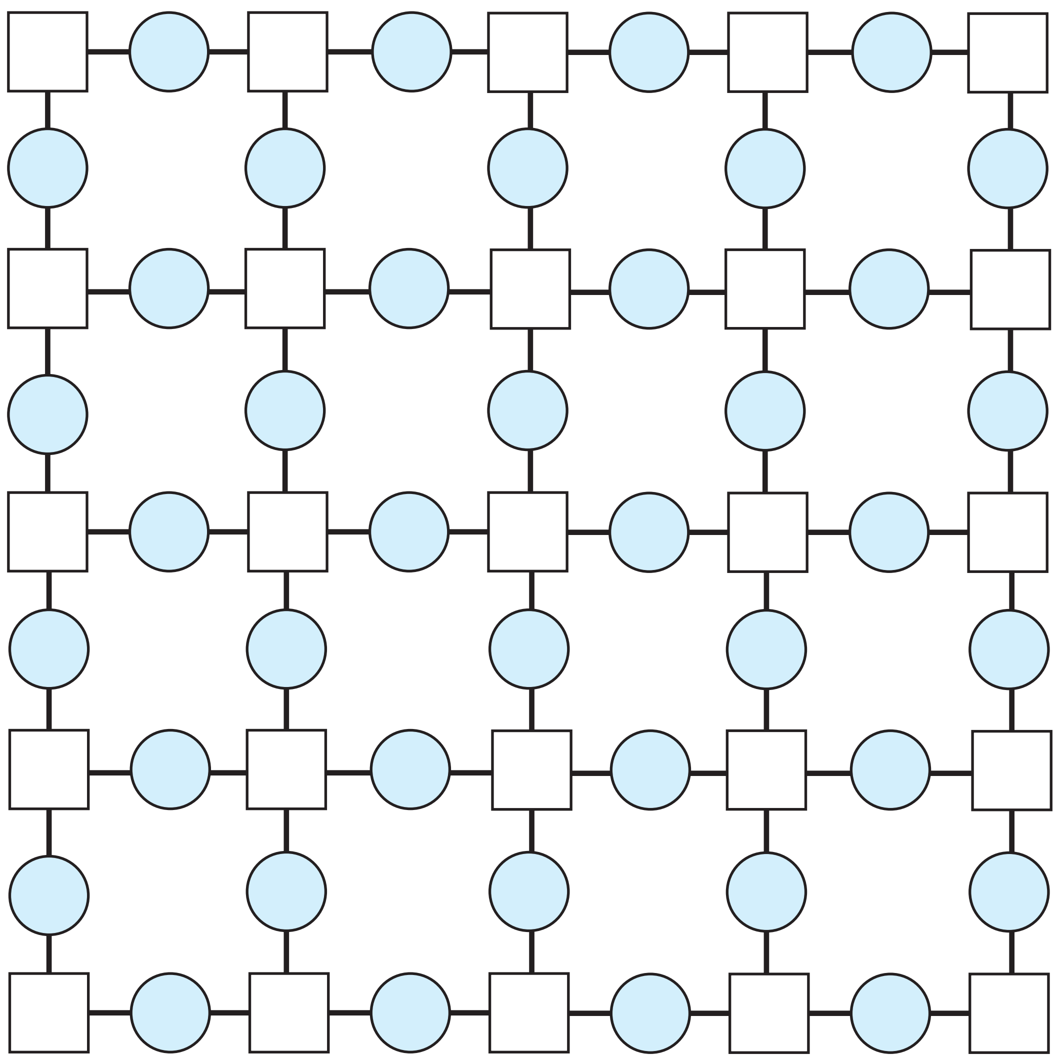
Measure code stabilisers once and try to infer error,
but measurement outcomes are noisy!

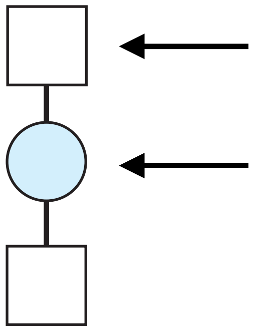




Possible for 3D gauge colour code
or 4D topological code (e.g. 4D toric code)

See e.g. [Kubica, Preskill arXiv:1809.10145]
[Breuckmann PhD thesis '18]
[Breuckmann, Duivenvoorden, Michels, Terhal QIC '17]
[Brown, Nickerson, Browne, Nat Comms '16]
[Pastawski, Clemente, Circa PRA '11]
[Dennis Kitaev Preskill J. Math. Phys. '01]





A bit

Parity check

measure parity of connected bits

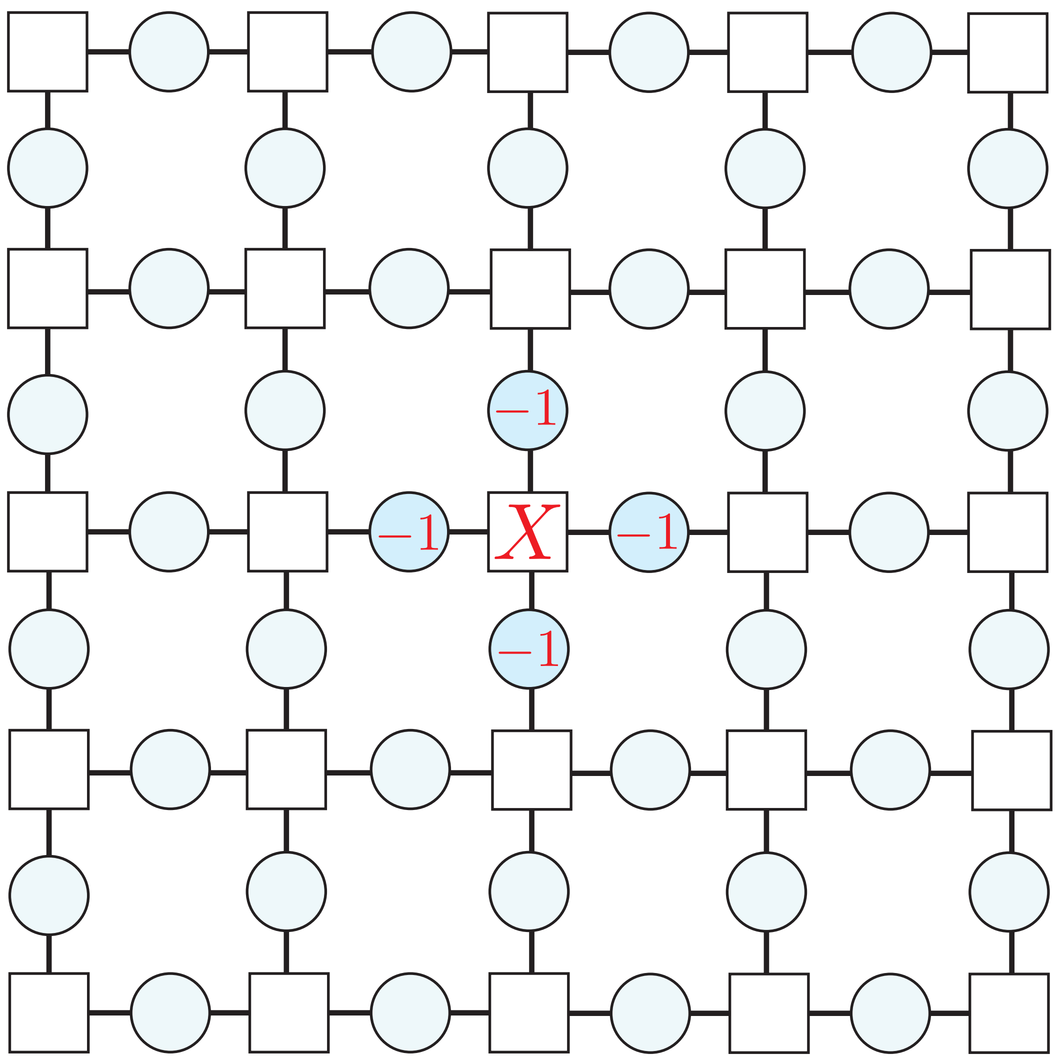
e.g. ZZ

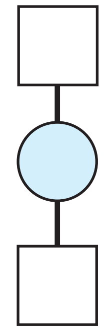
Classical single-shot: possible in 2D!

warm up example

ISING MODEL: CLASSICAL WARM UP

Earl Campbell





A bit

Parity check

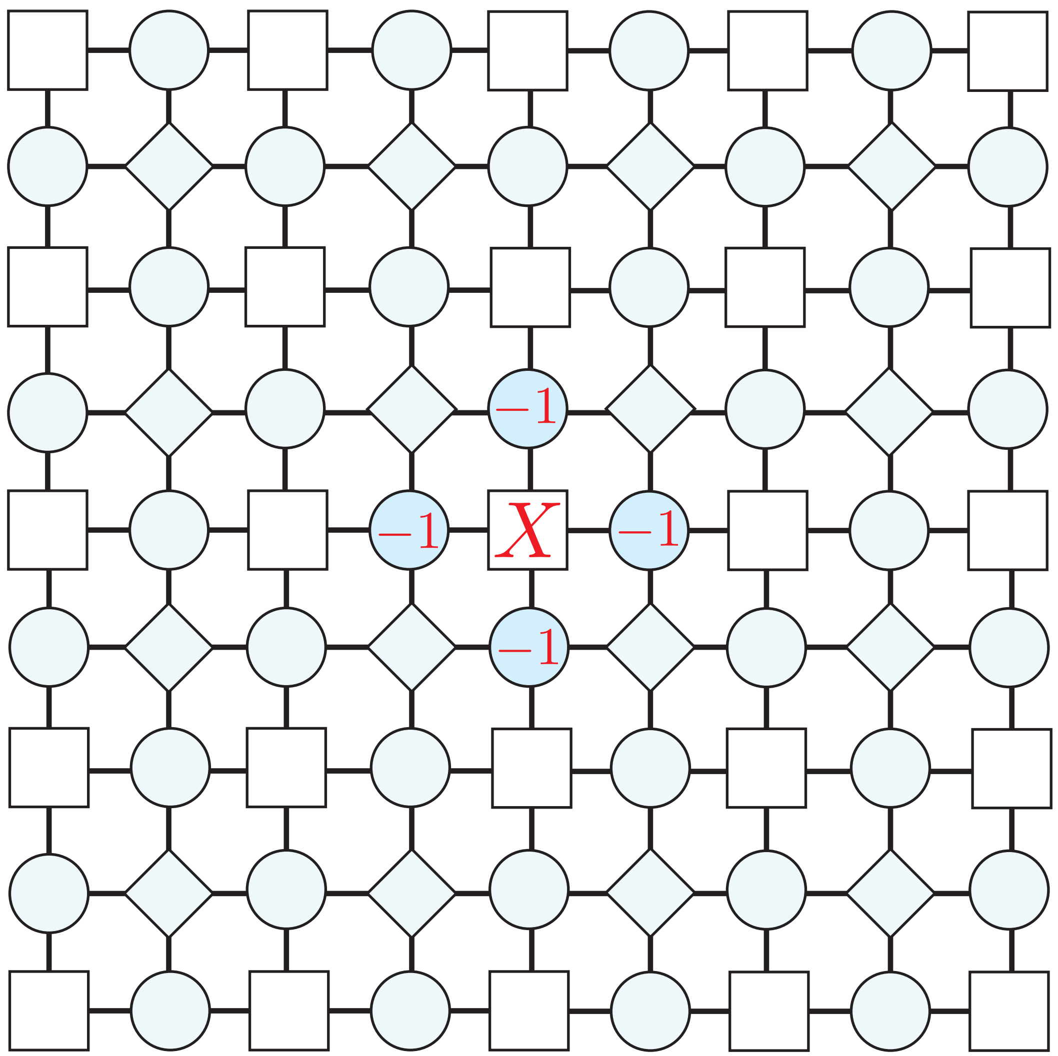
measure parity of connected bits

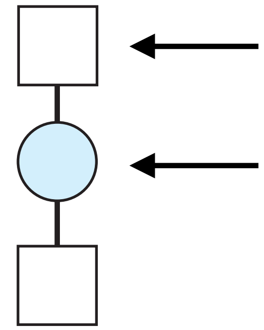
e.g. ZZ

X **A physical error**

-1 **“-1” measurement result**

ISING MODEL: CLASSICAL WARM UP



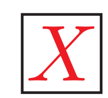


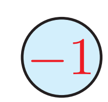
A bit

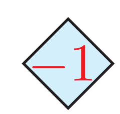
Parity check

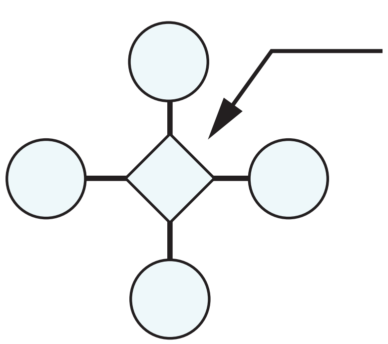
measure parity of connected bits

e.g. ZZ

 **A physical error**

 **"-1" measurement result**

 **"-1" meta-check result**

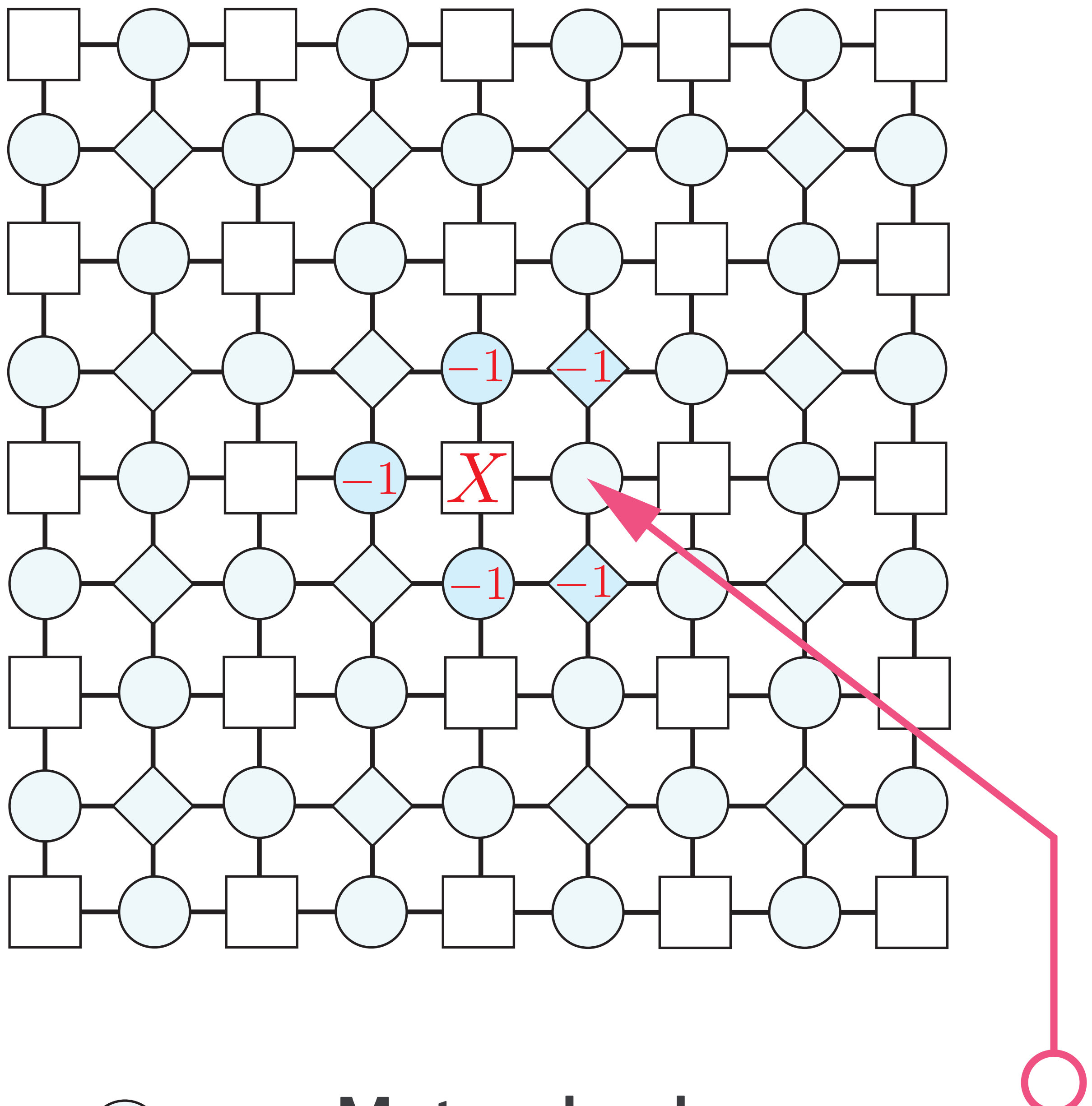


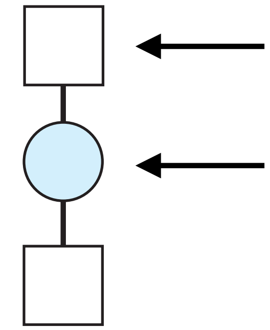
Meta-check:

"a check on checks"

calculates parity of all connected checks

Earl Campbell



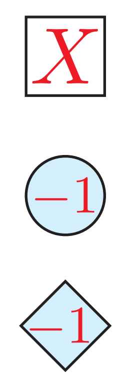


A bit

Parity check

measure parity of connected bits

e.g. ZZ



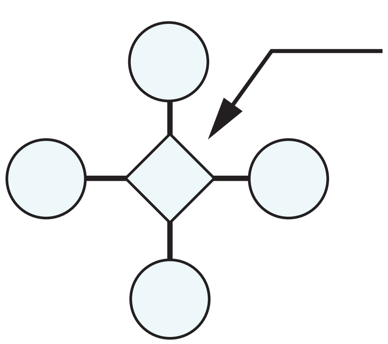
A physical error

"-1" measurement result

"-1" meta-check result

Measurement error!!!

should be "-1" but experiment reports "+1"



Meta-check:

"a check on checks"

calculates parity of all connected checks

Formal definition: Redundancy & metacheck:

Consider a set of Pauli checks that stabiliser codespace:

$$\mathcal{M} = \{M_1, M_2, \ldots\}$$

allow $\mathcal{M}$ to be overcomplete

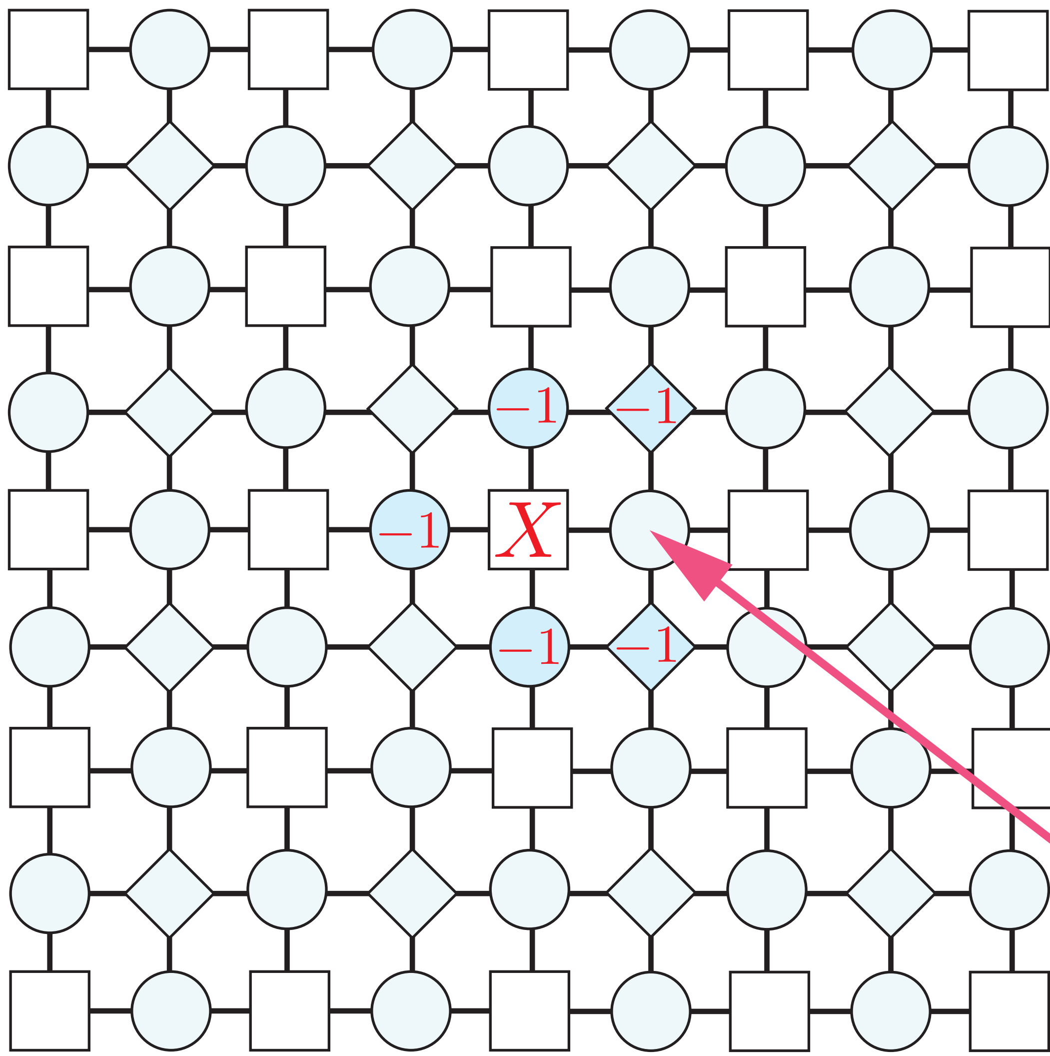
A redundancy is a sets of check multiplying to identity

e.g. $M_1 M_2 M_3 = \mathbb{I}$

Leads to consistency condition on parity checks.

Metacheck are a subset of redundancies that we choose to enforce.

Earl Campbell



Two stage decoder

Stage 1: Correct measurement error

Look at metachecks, find low weight measurement correction.

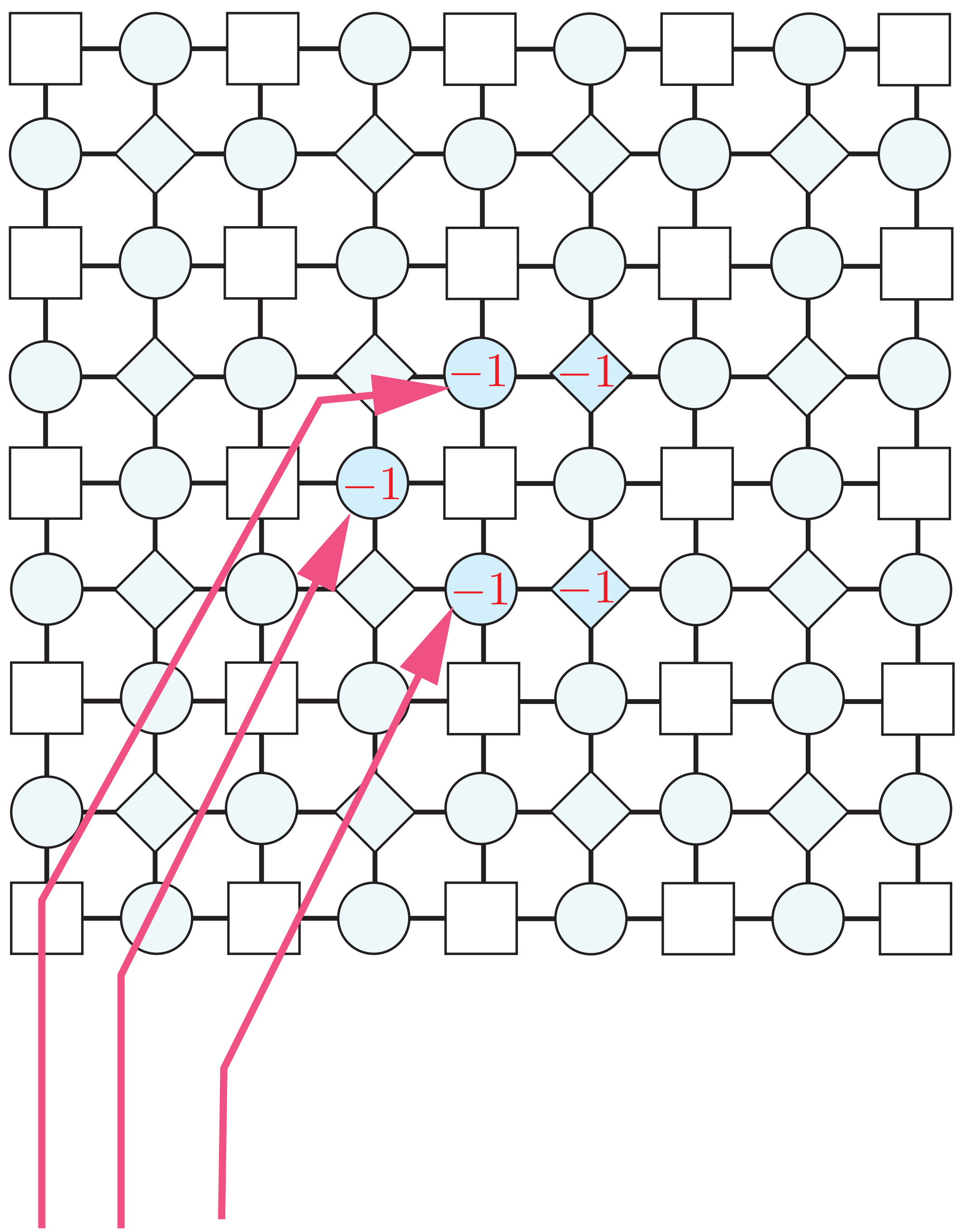
Stage 2: Correct physical bits

Look at repaired checks find low weight physical correction.

Measurement error!!!

should be "-1" but experiment reports "+1"

Earl Campbell



Two stage decoder

Stage 1: Correct measurement error

Look at metachecks, find low weight measurement correction.

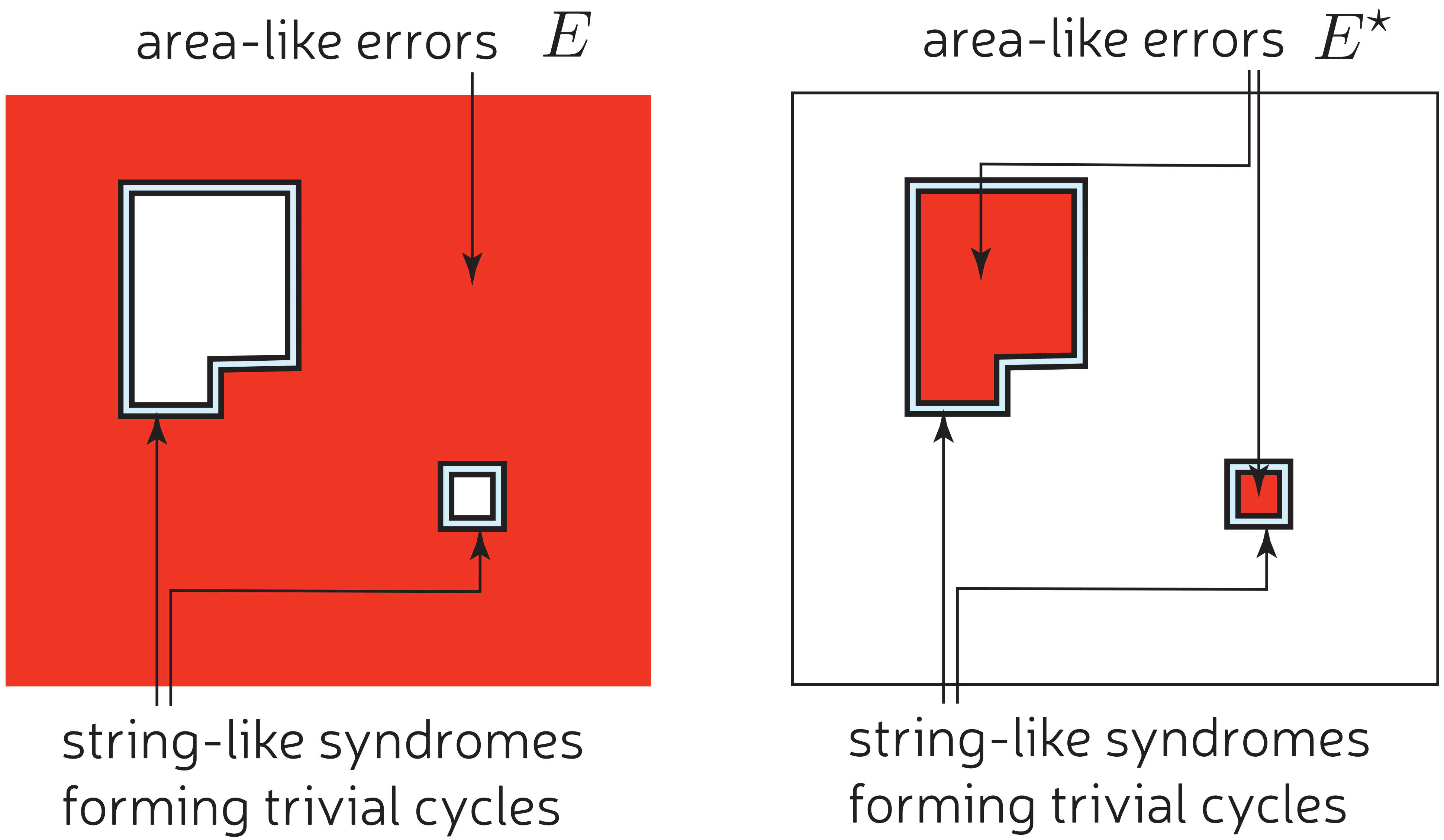
Stage 2: Correct physical bits

Look at repaired checks find low weight physical correction.

Same signature caused by **triple measurement error** and **no physical error**

Correction leads to a **residual error**

Area-law / soundness property



boundary size = syndrome weight $= x$

then $\mathrm{wt}[E^\star] \leq f(x) = x^2/2$

Adversarial quantum error correction

Error model

x = num. of of measurement errors

y= num. of single-qubit Pauli errors

Standard QEC

if **x=0** and **y < d/2**
then
can correct perfectly
Residual error weight **= 0**

Single-shot QEC

if **x, y <** some upperbound
then
there is a decoder such that
Residual error weight **<= f(x)**

where **f** is some function
s.t. **f(0)=0**

Adversarial quantum error correction

Error model

x = num. of of measurement errors

y= num. of single-qubit Pauli errors

Good family of SS codes

a family of **n**-qubit codes has good single shot QEC if

1) **x,y** bounds grow $\Omega(n^a)$

2) $f \in \mathrm{poly}(x)$

Single-shot QEC

if **x, y <** some upperbound then there is a decoder such that Residual error weight **<= f(x)**

where **f** is some function s.t. **f(0)=0**

Area-law / soundness property

A code & check set is (t, f) sound if

Given any consistent syndrome of weight $= x \leq t$ some constant

There exists an Pauli correction of weight $\leq f(x) \in \mathrm{poly}(x)$

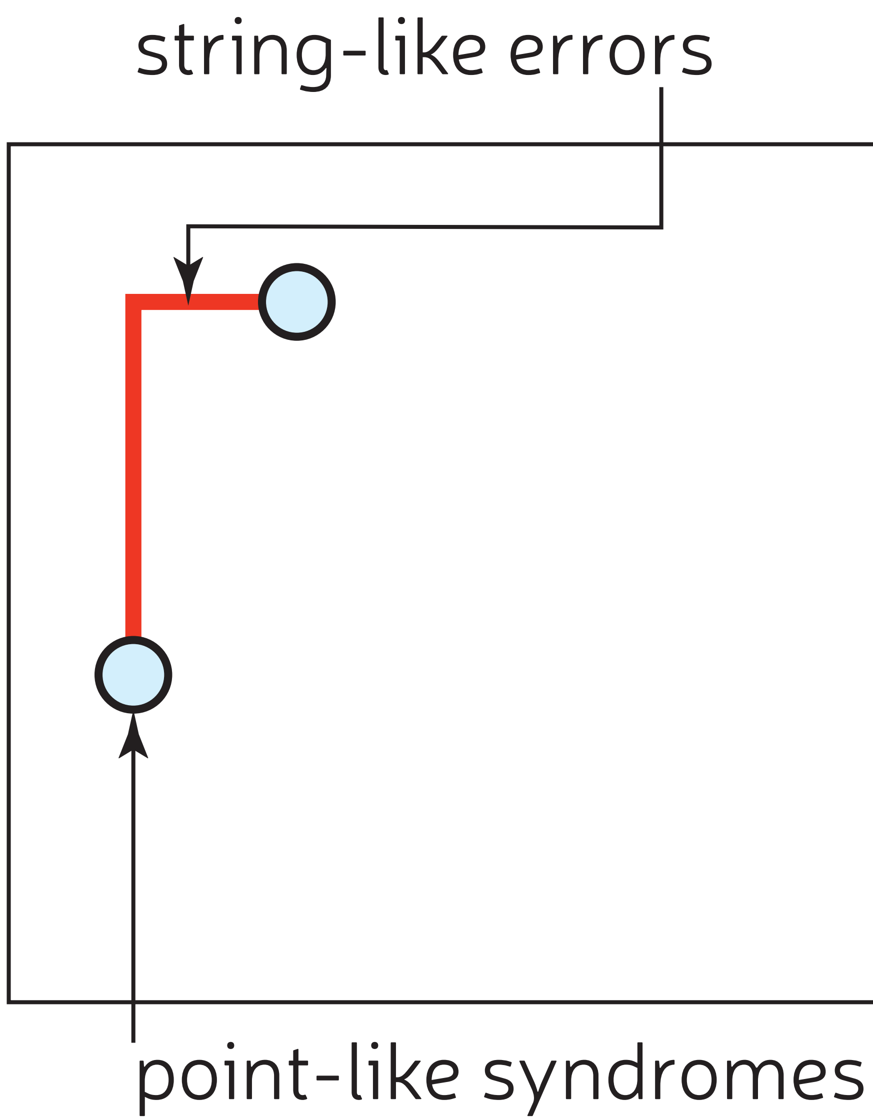
A code & check family has good soundness if

All members are (t_n, f) where t_n grows as $\Omega(n^a)$

Mini result 1: Good soundness $\longrightarrow$ good single-shot EC

proof uses two-stage decoder

Toric code problem: has poor soundness



syndrome weight $= 2$

then $\mathrm{wt}[E] \leq f(2) = ?\mathrm{unbounded}?$

soundness vs. energy barrier

Is soundness just the same thing as a large energy barrier?

Energy barrier

for one check set

Consider walks from one logical state to an orthogonal logical state,

- A walk is made of small steps $|\psi_{j+1}\rangle = P_j|\psi_j\rangle$

ψ_0 ψ_5

$|0_L$

a check family of n-qubit codes has a

Macroscopic Energy barrier

if the **energy barrier** grows as $\Omega(n^c)$

The energy of a state is the number of violated stabiliser checks.

The **energy penalty** of a walk is the "peak" energy during the walk.

The **energy barrier** of a check set is the min energy penalty over all walks.

LDPC + good soundness → **macroscopic energy barrier**

Theorem 2 *Any LDPC check family with good soundness and code distance d_Q growing as $\Omega(n^c)$ for some constant $0 < c$ will also have a macroscopic energy barrier.*

????

LDPC + macroscopic energy barrier → **good soundness**

Theorem 2 *Any LDPC check family with good soundness and code distance d_Q growing as $\Omega(n^c)$ for some constant $0 < c$ will also have a macroscopic energy barrier.*

No 2D topological code can have
a macroscopic energy barrier, [Bravyi, Terhal *NJP '09*]

Corollary 1 *Any 2D topological check family with code distance d_Q growing as $\Omega(n^c)$ for some constant $0 < c$ will not have good soundness.*

Choice of check set

Recall we:

Consider a set of Pauli checks that stabilise the codespace:

$$\mathcal{M} = \{M_1, M_2, \ldots\}$$

Soundness is a property of the set of stabiliser checks.

sooo….

We can ask:

“Given a code family does these exist a check-family with good soundness?”

Thm: for all codes $\exists$ checks w/ good soundness!

Proof sketch.

For every code we can find stabiliser generators that upto local Cliffords are of "**diagonalised**" form

$$
\begin{array}{lllllll}
S_1 = & X_1 & Z_2 & \mathbb{I}_3 & Z_4 & \dots \\
S_2 = & Z_1 & X_2 & \mathbb{I}_3 & Z_4 & \dots \\
S_3 = & Z_1 & \mathbb{I}_2 & X_3 & Z_4 & \dots
\end{array}
$$

Then every 1-bit syndrome can be corrected by a weight 1 error

$$Z_j S_j Z_j = -S_j$$

So residual error is less than syndrome, so $f(x) = x$

Mini result 1: Good soundness $\longrightarrow$ good single-shot EC

Mini result 2*: Good soundness + LDPC + distance $\Omega(n^a)$
$\longrightarrow$ macroscopic energy barrier

Mini result 3:** 2D topological code + distance $\Omega(n^a)$
$\longrightarrow$ bad soundness

Mini result 4: for all codes $\exists$ checks w/ good soundness!

** corollary following from
S. Bravyi and B. Terhal,

* similar result (w/ stronger soundness def) is used in study of PCP the
D. Aharonov and L. Eldar, *SIAM Journal on Computing* **44**, 1230 (2015).

Moral:

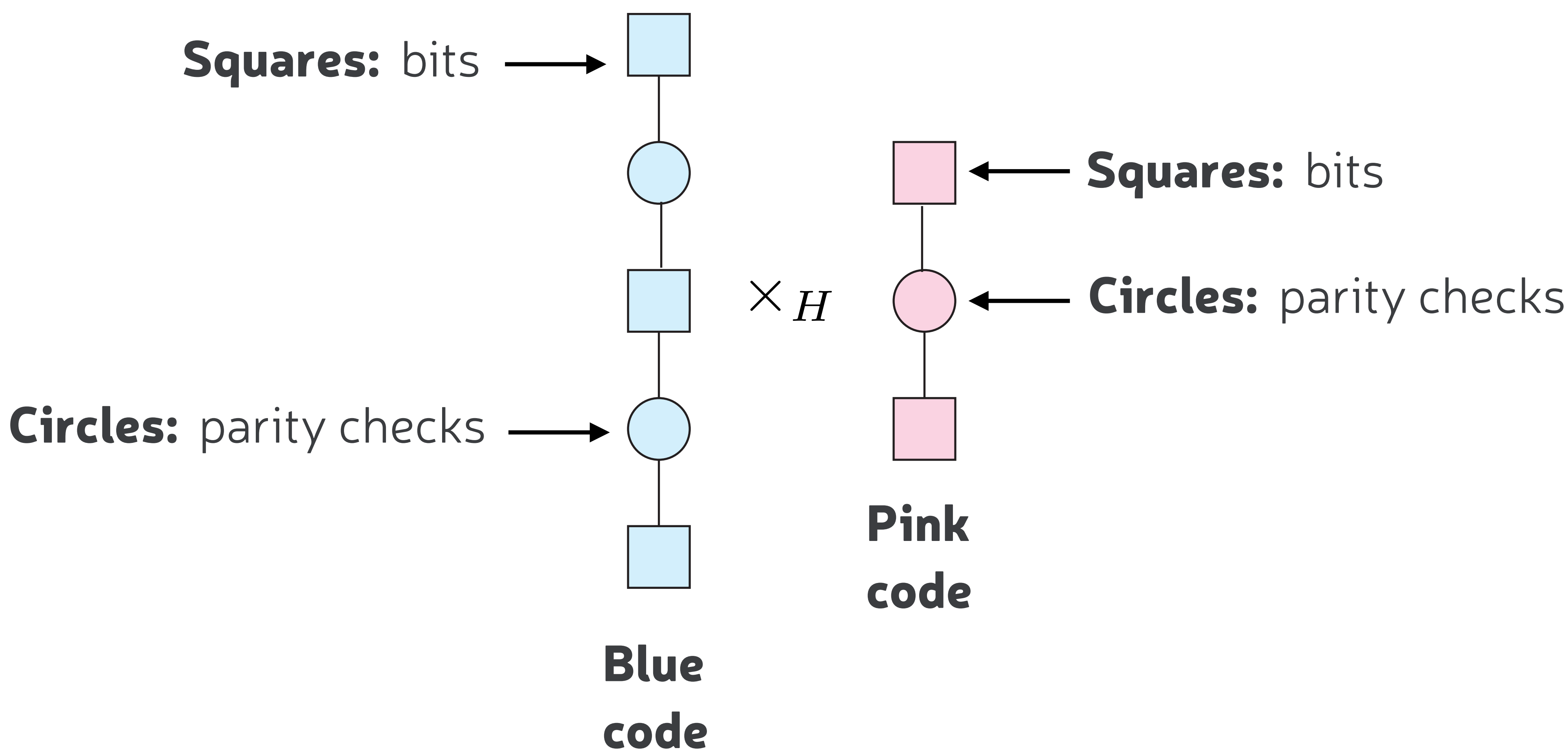
Easy to find codes/checks with good soundness

Tricky to find LDPC codes/checks with good soundness

1 big result: homological product constructions

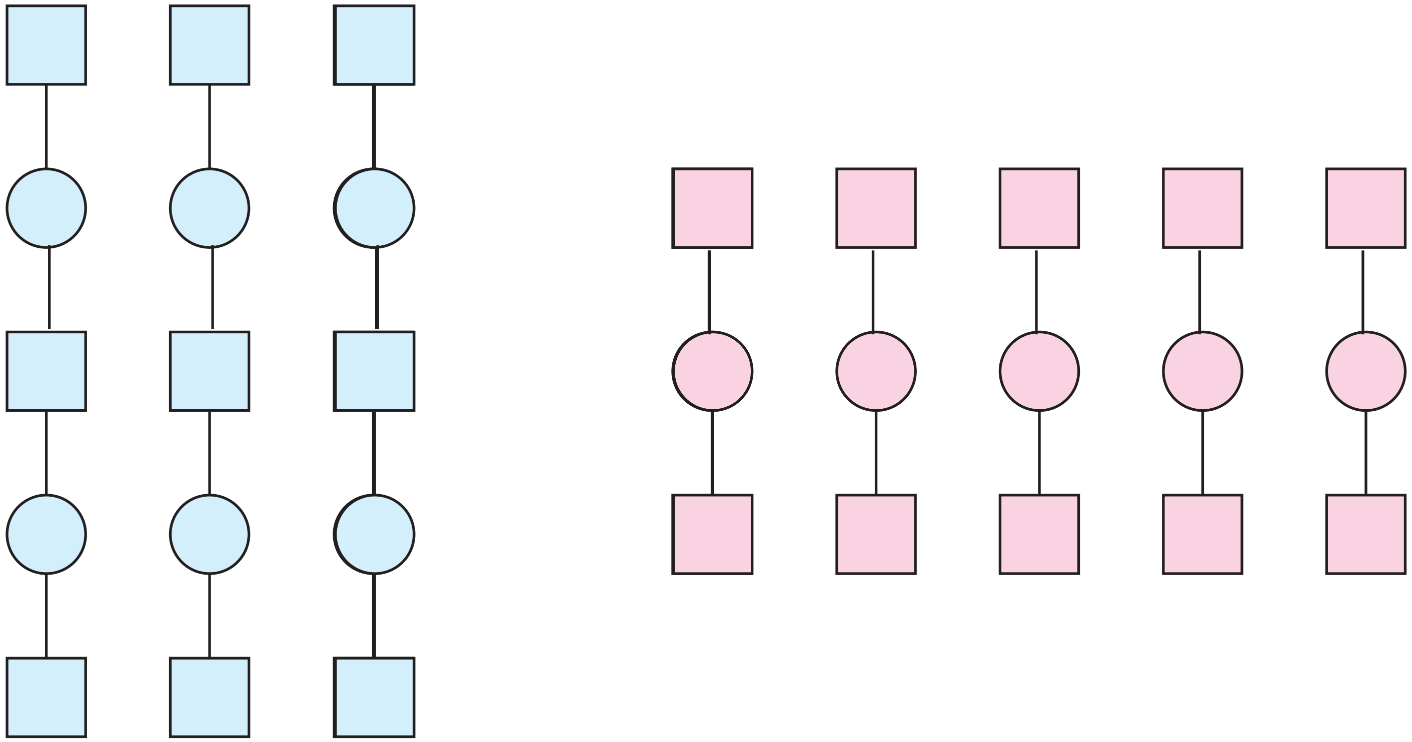
Warmup: Revise hyper graph product

Take two Tanner graphs representing classical code

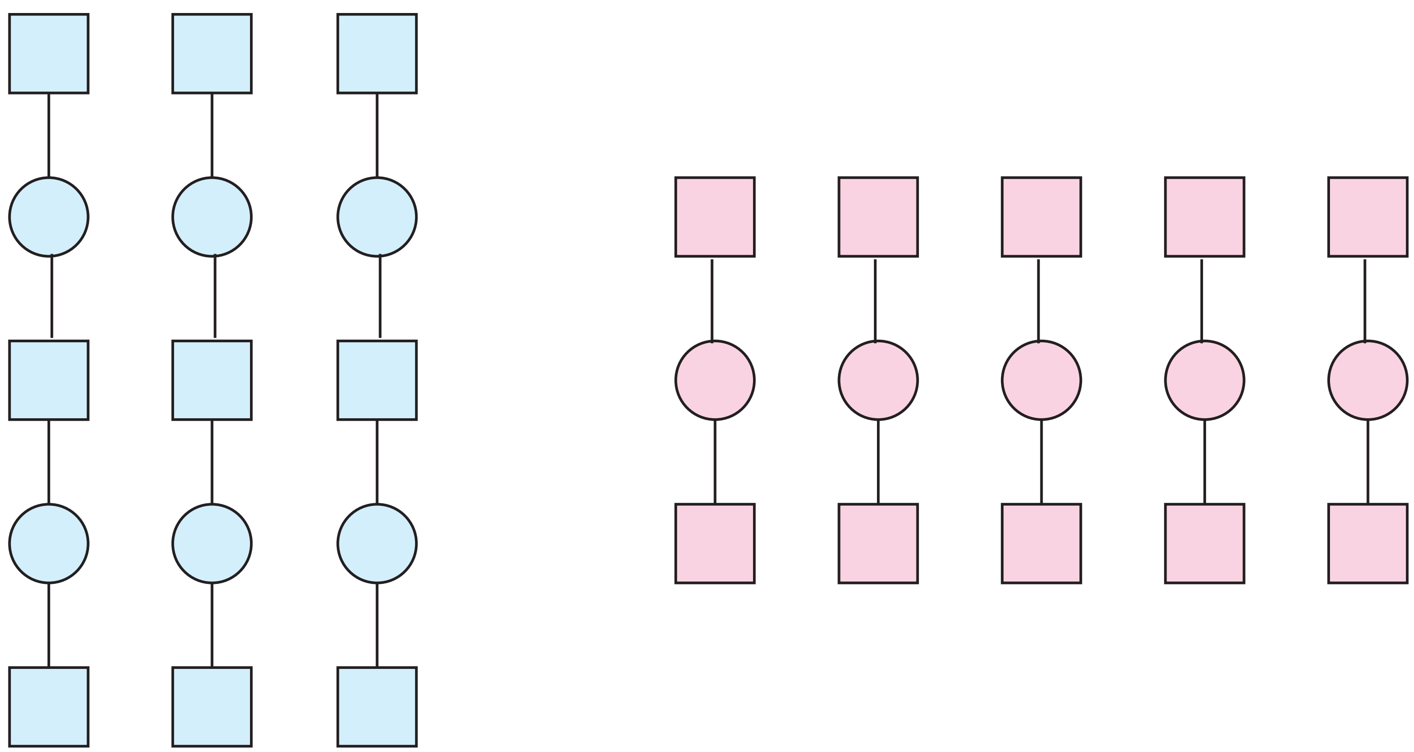


Essentially same as hyper graph product: [Tillich & Zemor IEEE '09]

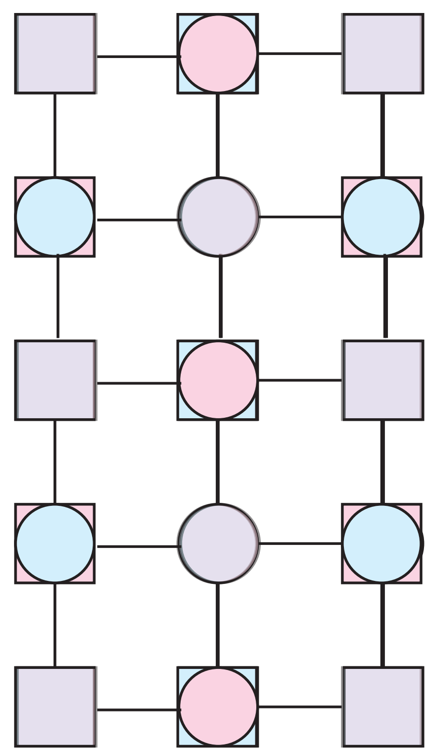
Clone the codes



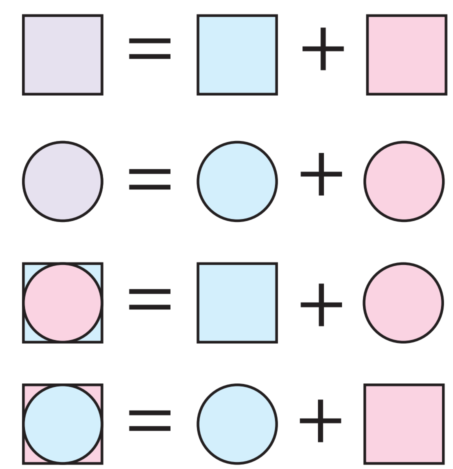
Superimpose codes



Superimpose codes



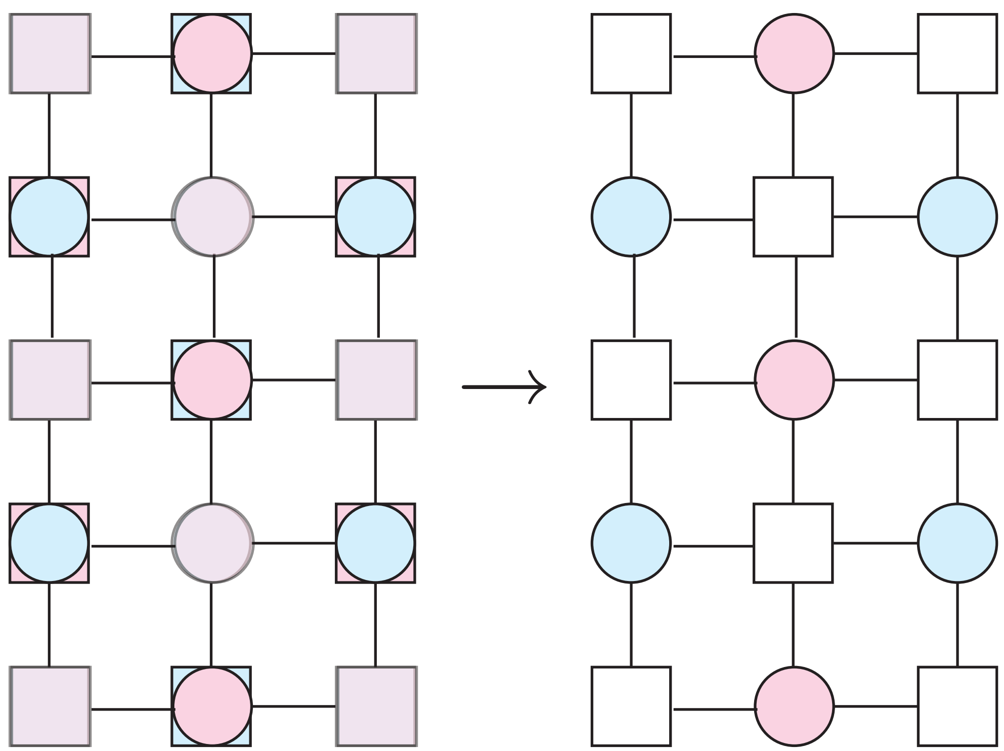
where



THE HYPER GRAPH / HOMOLOGICAL PRODUCT

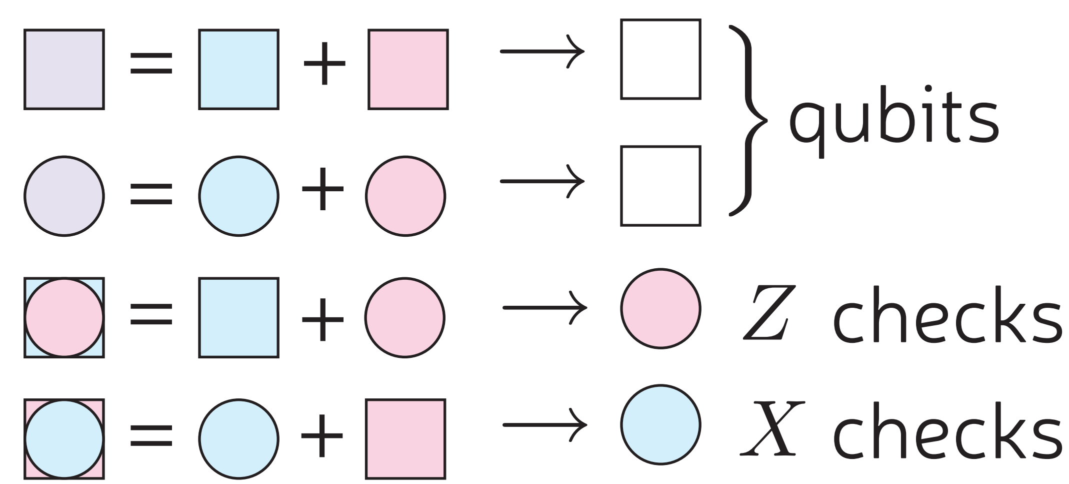
Earl Campbell

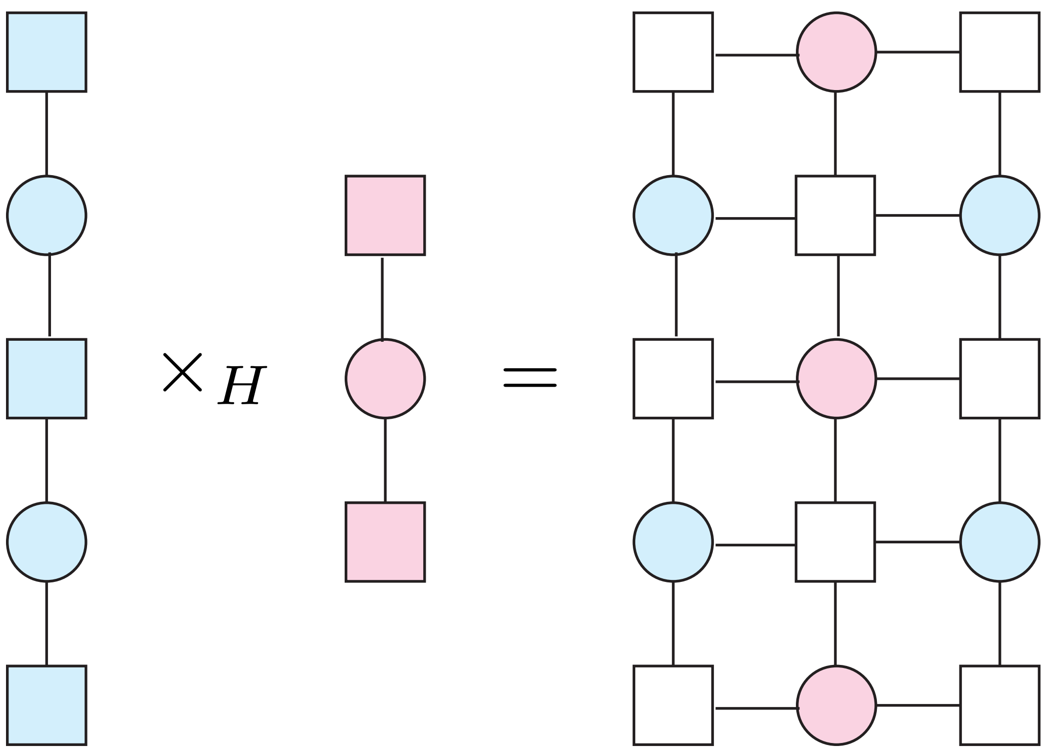
Relabel vertices



Finished!
A quantum code

where

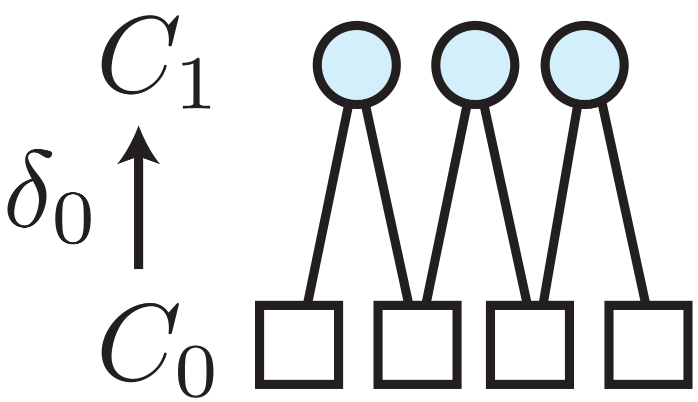




Always yields valid quantum code
for any pair of initial classical codes

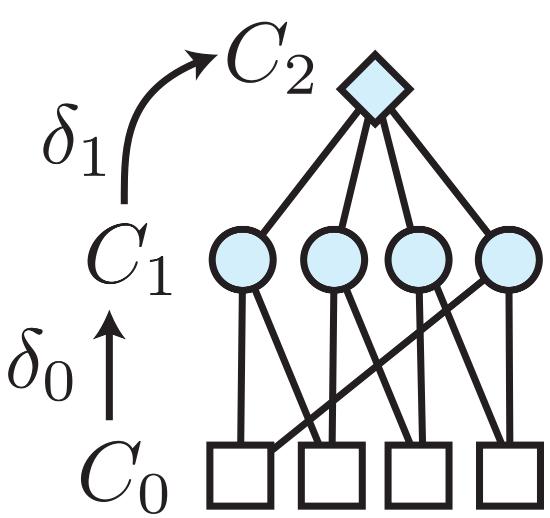
Unlike CCS construction where duality is required.

Why valid quantum code: because a chain complex!



Bipartite graph

$$[\delta_0]_{i,j} = \begin{cases} 1 & \text{if vertex } i \text{ in } C_0 \text{ is adjacent to vertex } j \text{ in } C_1 \\ 0 & \text{otherwise.} \end{cases}$$



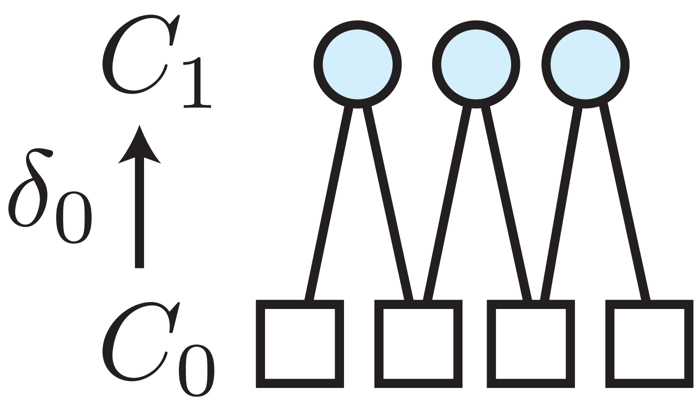
Tripartite graph

$$[\delta_0]_{i,j} = \begin{cases} 1 & \text{if vertex } i \text{ in } C_0 \text{ is adjacent to vertex } j \text{ in } C_1 \\ 0 & \text{otherwise.} \end{cases}$$

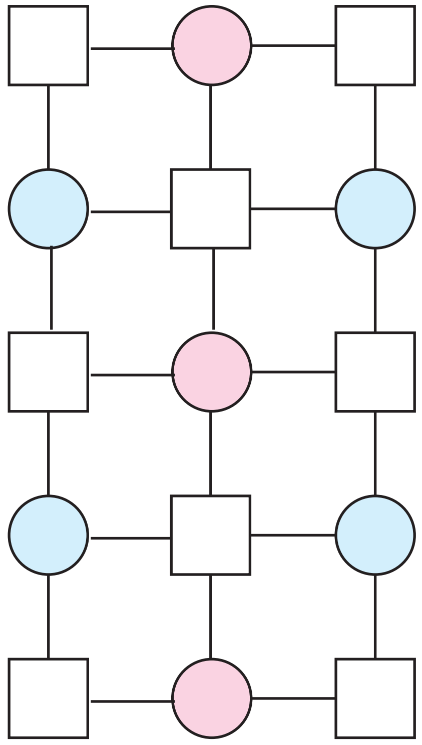
$$[\delta_1]_{i,j} = \begin{cases} 1 & \text{if vertex } i \text{ in } C_1 \text{ is adjacent to vertex } j \text{ in } C_2 \\ 0 & \text{otherwise.} \end{cases}$$

We say such a graph forms a **chain complex** if and only if

$$\delta_i \delta_{i-1} = 0 \quad \textbf{for all} \quad i$$



hypergraph product



$$\tilde{\delta}_0 = \begin{pmatrix} \mathbb{I} \otimes \delta_0^T \\ \delta_0 \otimes \mathbb{I} \end{pmatrix}$$

$$\tilde{\delta}_1 = \begin{pmatrix} \delta_0 \otimes \mathbb{I} & \mathbb{I} \otimes \delta_0^T \end{pmatrix}$$

since

$$\tilde{\delta}_1 \tilde{\delta}_0 = 2\delta_0 \otimes \delta_0^T = 0$$

the new object is indeed a chain complex!

We say such a graph forms a **chain complex** if and only if

$$\delta_i \delta_{i-1} = 0 \quad \textbf{for all} \quad i$$

If the graph has **3** or more parts then we can define a quantum code

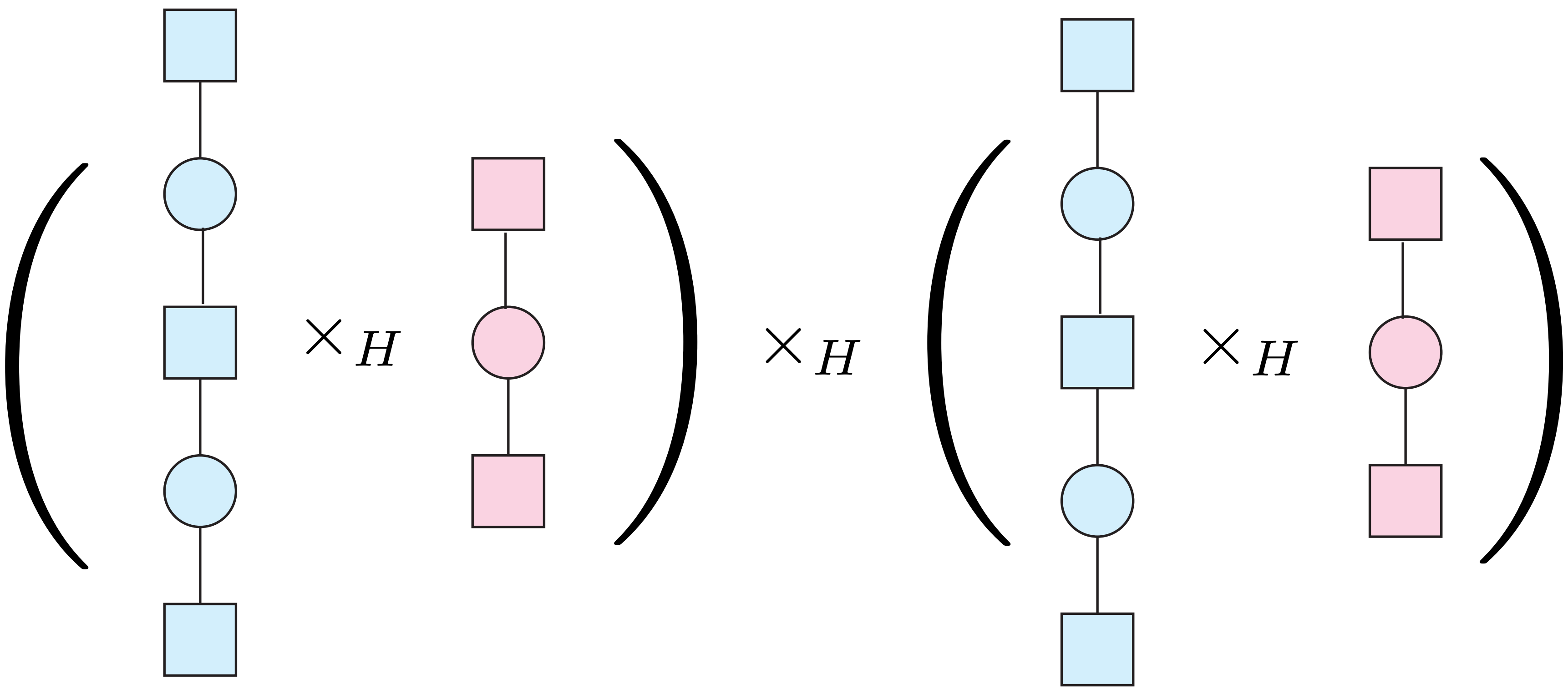
$C_{j+1} =$ the X checks $\longrightarrow$ $H_X = \delta_j$

$C_j =$ the qubits

$C_{j-1} =$ the Z checks $\longrightarrow$ $H_Z = \delta_{j-1}^T$

commutative $H_X H_Z^T = \delta_j (\delta_{j-1}^T)^T = \delta_j \delta_{j-1} = 0$

Double homological product



= chain complex graph with 5 levels of structure!

$$\breve{\delta}_1 \breve{\delta}_0 = 0$$
$$\breve{\delta}_2 \breve{\delta}_1 = 0$$
$$\cdots$$

give a quantum code with metachecks!

classical LDPC -> quantum LDPC

We say such a graph forms a **chain complex** if and only if

$$\delta_i \delta_{i-1} = 0 \quad \textbf{for all} \quad i$$

If the graph has **5** or more parts then we can define a quantum code

$C_{j+2} =$ the X metachecks $\rightarrow \delta_{j+1}$

$C_{j+1} =$ the X checks $\rightarrow H_X = \delta_j$

$C_j =$ the qubits

$C_{j-1} =$ the Z checks $\rightarrow H_Z = \delta_{j-1}^T$

$C_{j-2} =$ the Z metachecks $\rightarrow \delta_{j-2}^T$

$$\delta_i \delta_{i-1} = 0$$ entails that valid metacheck codes!

Given ***any*** classical code with

$n =$ no. physical bits
$k =$ no. logical bits
$d =$ distance

Double homological product

A quantum code

$n_Q =$ no. physical qubits
$k_Q =$ no. logical bits
$d_Q =$ distance

where...

$$n_Q = n^4 + 4n^2(n-k)^2 + (n-k)^4 \sim O(n^4)$$
$$k_Q = k^4$$
$$d_Q = d^2$$

Distance recently improved from $d_Q \geq d$ bound, by *Zeng and Pryadko arXiv:1810.01519*

Given ***any*** classical code with

$n =$ no. physical bits
$k =$ no. logical bits
$d =$ distance

Double homological product

A quantum code

$n_Q =$ no. physical qubits
$k_Q =$ no. logical bits
$d_Q =$ distance

where...

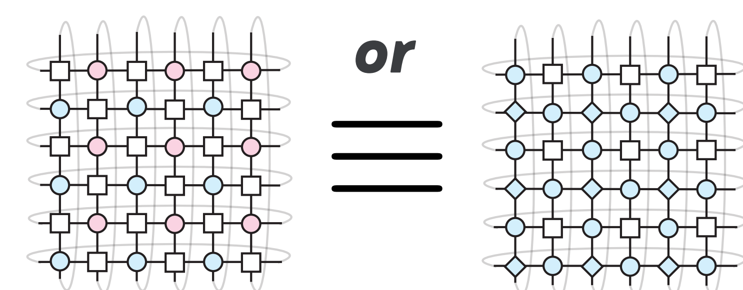
$$n_Q = n^4 + 4n^2(n-k)^2 + (n-k)^4 \sim O(n^4)$$
$$k_Q = k^4$$
$$d_Q = d^2$$

Theorem: Furthermore, the above code is always *(d-1, f)* sound with $f(x) = x^3/4$ or better!

Any classical code

Step one:
First homological product

A quantum code without metachecks ***or*** a <u>classical code</u> with metachecks



Step two:
Second homological product

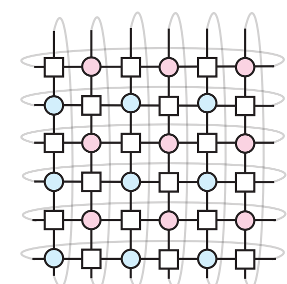
A quantum code

with meta checks & good soundness

Any classical code

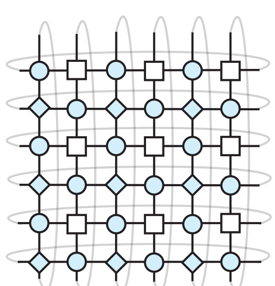
Step one:
First homological product

A quantum code without metachecks ***or*** a <u>classical code</u> with metachecks



or

$\equiv$

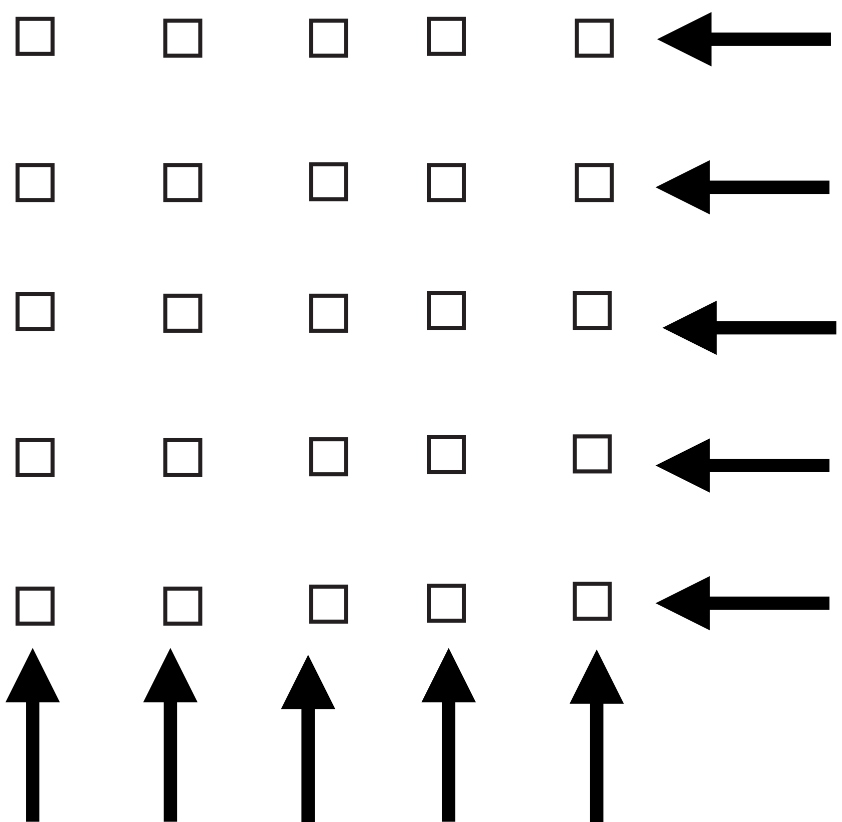


Lemma: Furthermore, the new <u>classical code</u> is always *(d, f)* sound with $f(x) = x^2/4$ or better!

Proof Sketch. *by explicit decoder design*

Initial code $[n, k, d]$ with parity check matrix H

Hypergraph classical codes with bits arranged in 2D:



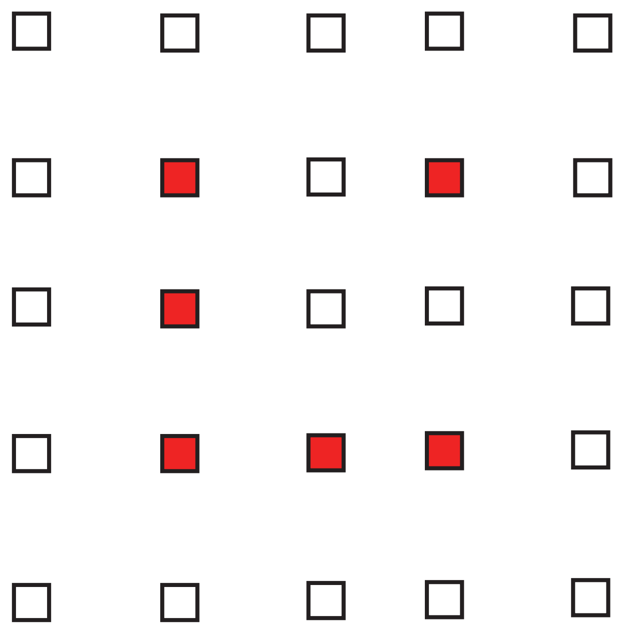
checks of H applied to every row

checks of H^T applied to every column

Lemma: Furthermore, the new <u>classical code</u> is always *(d, f)* sound with $f(x) = x^2/4$ or better!

Proof Sketch. *by explicit decoder design*

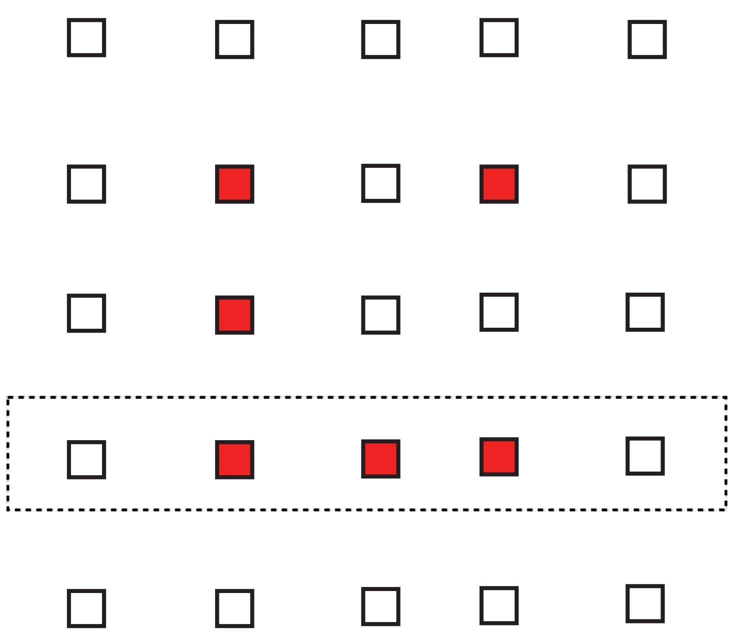
Consider some error pattern: *which we then minimise weight of!*



Lemma: Furthermore, the new classical code is always *(d, f)* sound with $f(x) = x^2/4$ or better!

Proof Sketch. *by explicit decoder design*

Look for codewords for original code in rows/columns

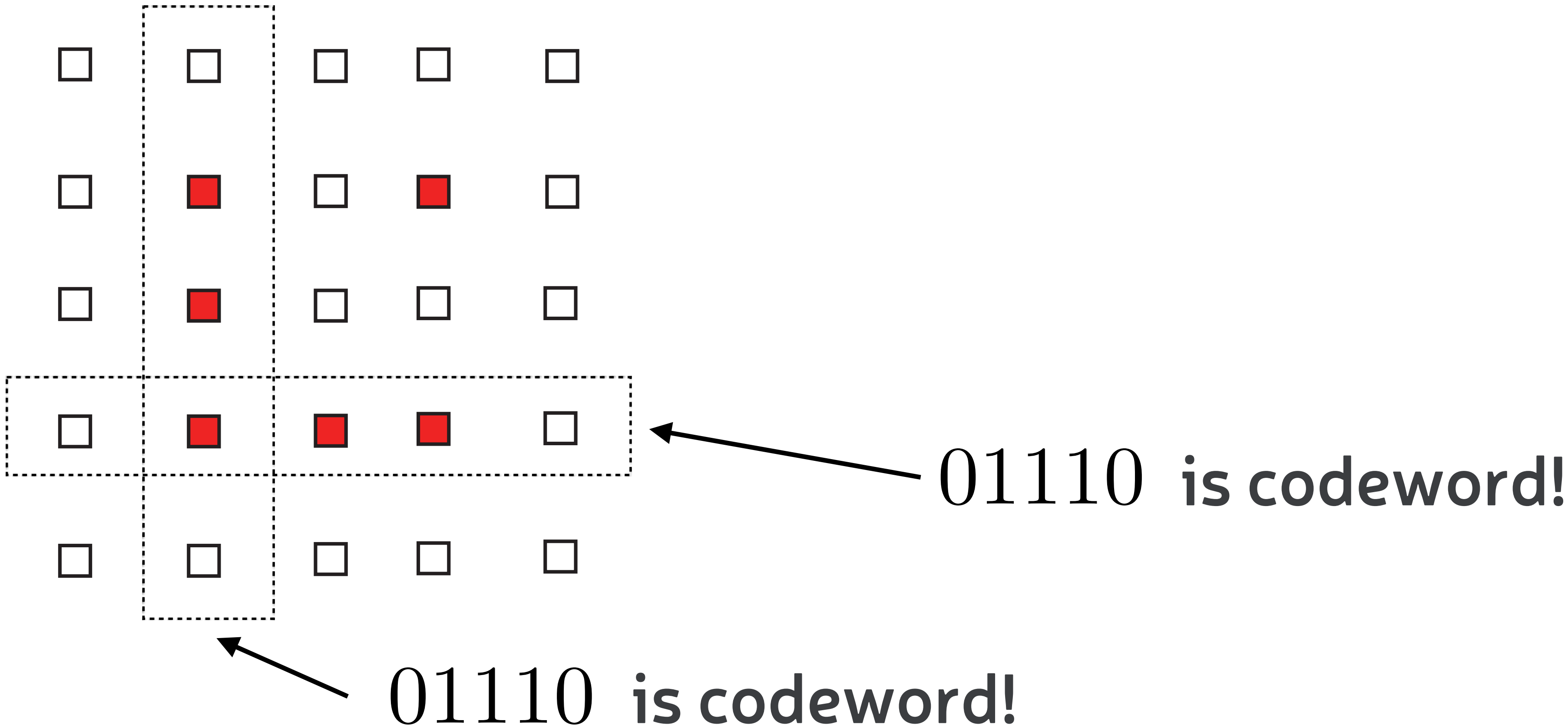


01110 **is codeword!**

Lemma: Furthermore, the new classical code is always *(d, f)* sound with $f(x) = x^2/4$ or better!

Proof Sketch. *by explicit decoder design*

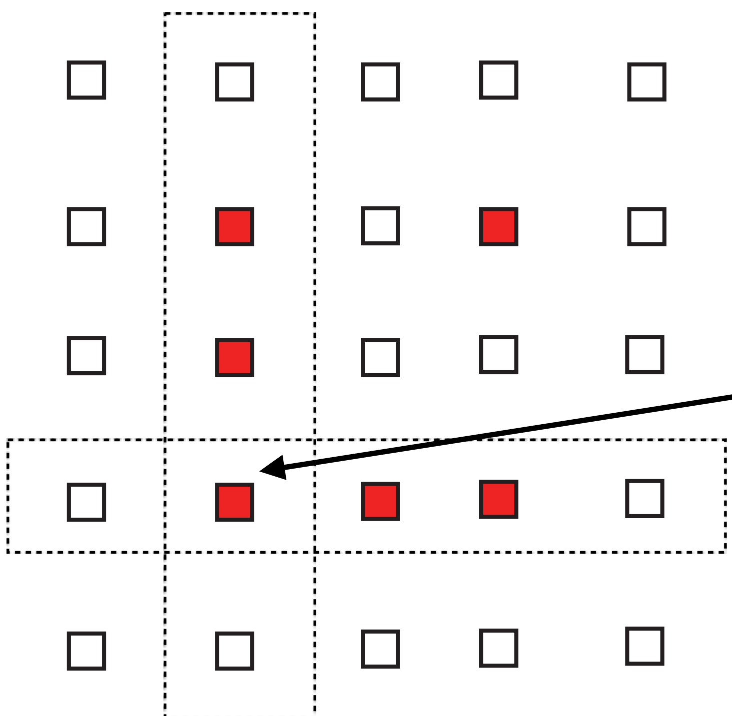
Look for codewords for original code in rows/columns



Lemma: Furthermore, the new <u>classical code</u> is always *(d, f)* sound with $f(x) = x^2/4$ or better!

Proof Sketch. *by explicit decoder design*

Look for codewords for original code in rows/columns



confirm **intersection** is red

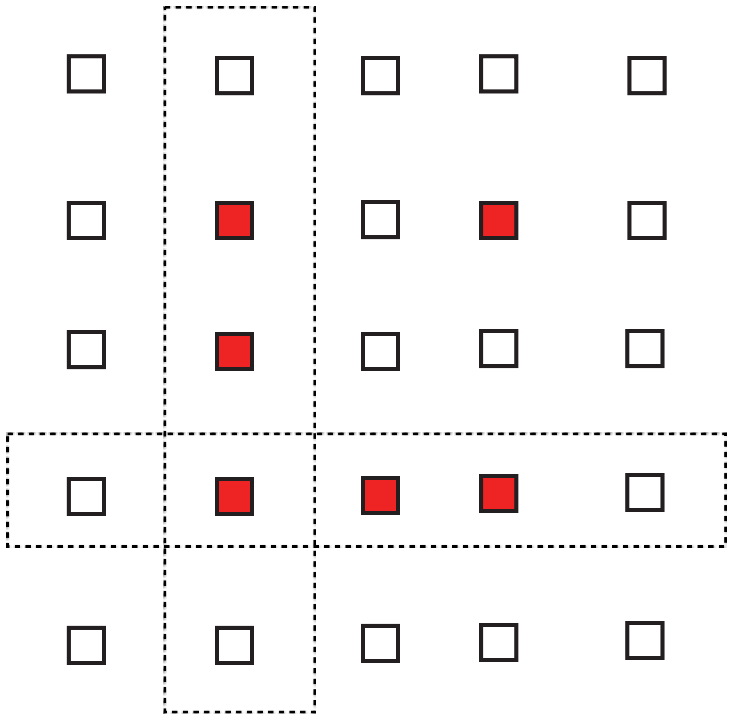
01110 **is codeword!**

01110 **is codeword!**

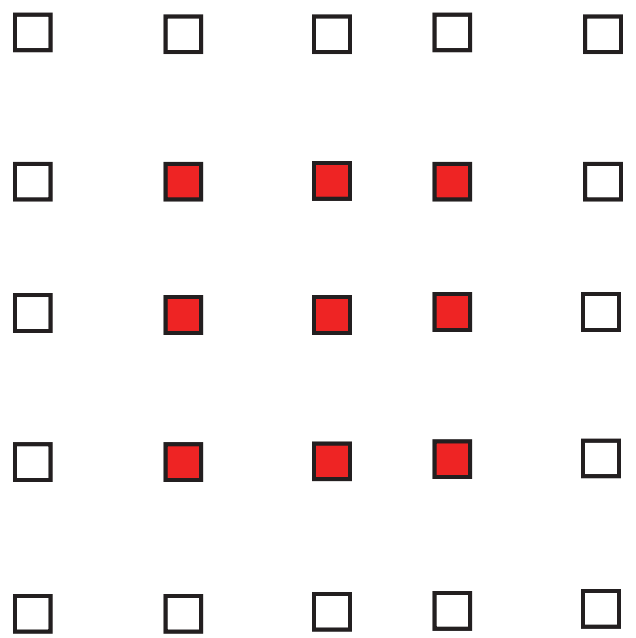
Lemma: Furthermore, the new classical code is always *(d, f)* sound with $f(x) = x^2/4$ or better!

Proof Sketch. *by explicit decoder design*

Form "product of code words"



$$01110 \times 01110$$



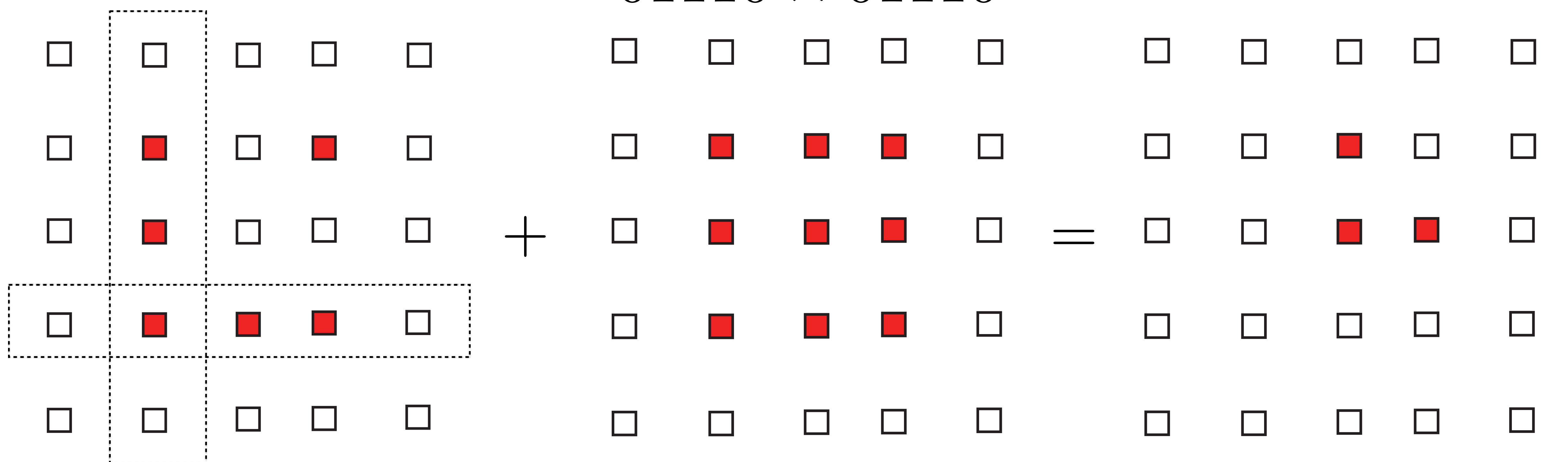
has trivial syndrome

Lemma: Furthermore, the new classical code is always *(d, f)* sound with $f(x) = x^2/4$ or better!

Proof Sketch. *by explicit decoder design*

Add “product of code words”

$$01110 \times 01110$$

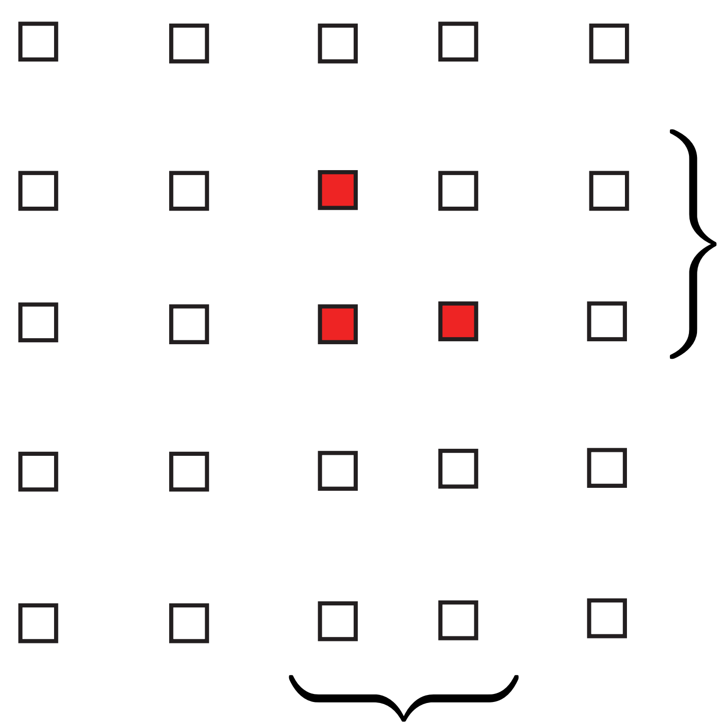


reduced weight with same syndrome

Lemma: Furthermore, the new classical code is always *(d, f)* sound with $f(x) = x^2/4$ or better!

Proof Sketch. *by explicit decoder design*

Repeat until



Not codewords

r = no. of rows

Not codewords

c = no. of columns

Every row/column

that is **not a codeword**

leads to violated **check**

Therefore,

syndrome weight $x \geq c + r$

but $\mathrm{wt}(E) \leq cr$

combined $\mathrm{wt}(E) \leq x^2/4$

Lemma: Furthermore, the new <u>classical code</u> is always *(d, f)* sound with $f(x) = x^2/4$ or better!

Redundancy, overheads & talking heads

Quantify redundancy

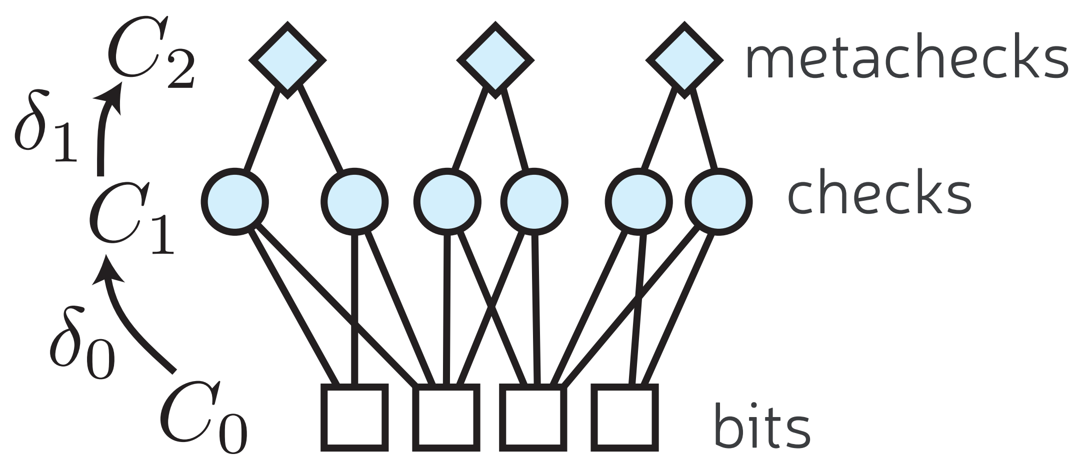
$$\nu = \frac{\text{number of checks measurements}}{\text{num. stabiliser generators}}$$

so $\nu = 1 \longleftrightarrow$ **no redundancy**

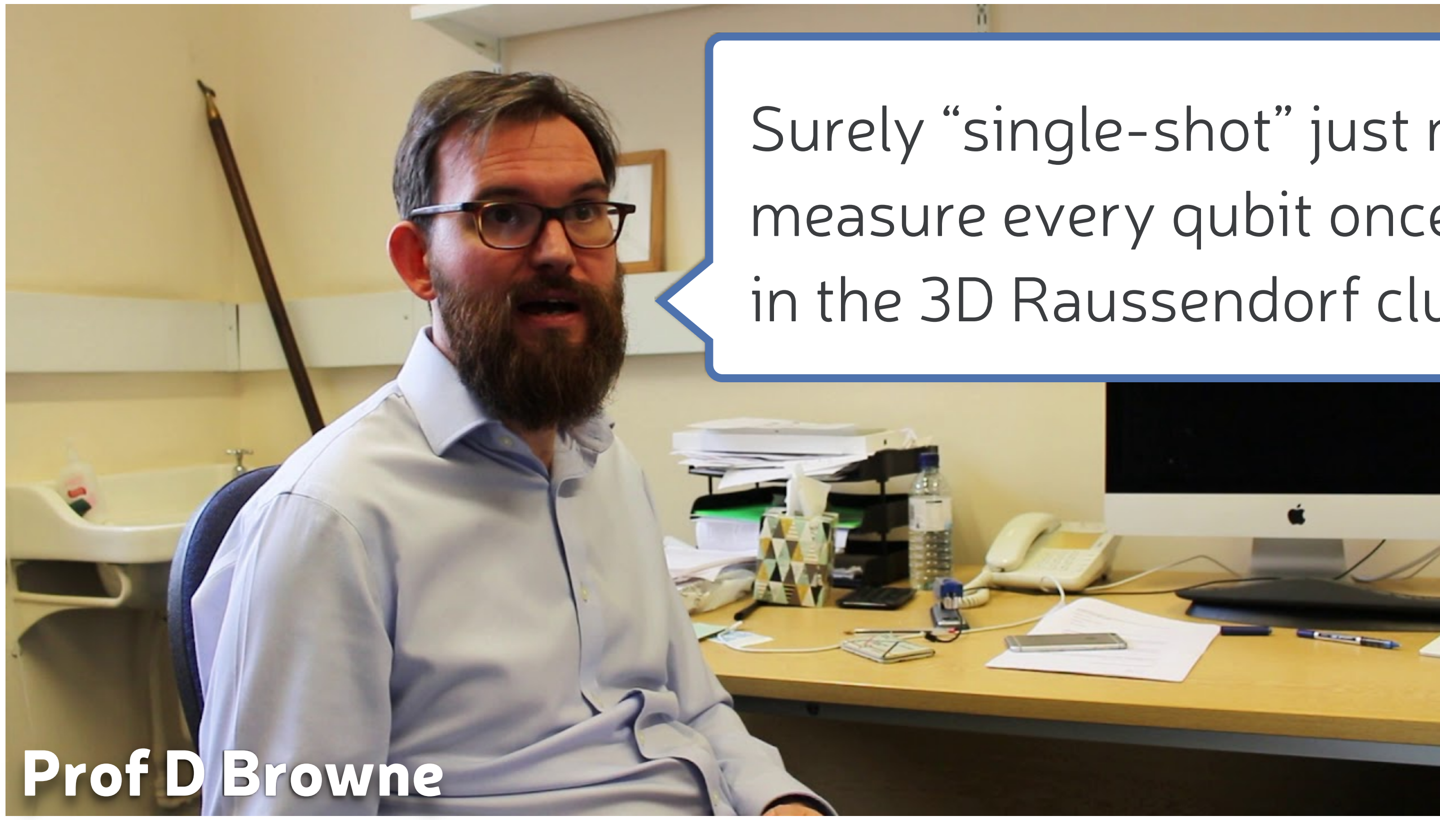
"**Interesting**" examples of single-shot have : $\nu \leq$ some constant

Formalism allows "trivial/uninteresting" single shot achieved using repeated measurements, but then $\nu \sim d$

trivial example



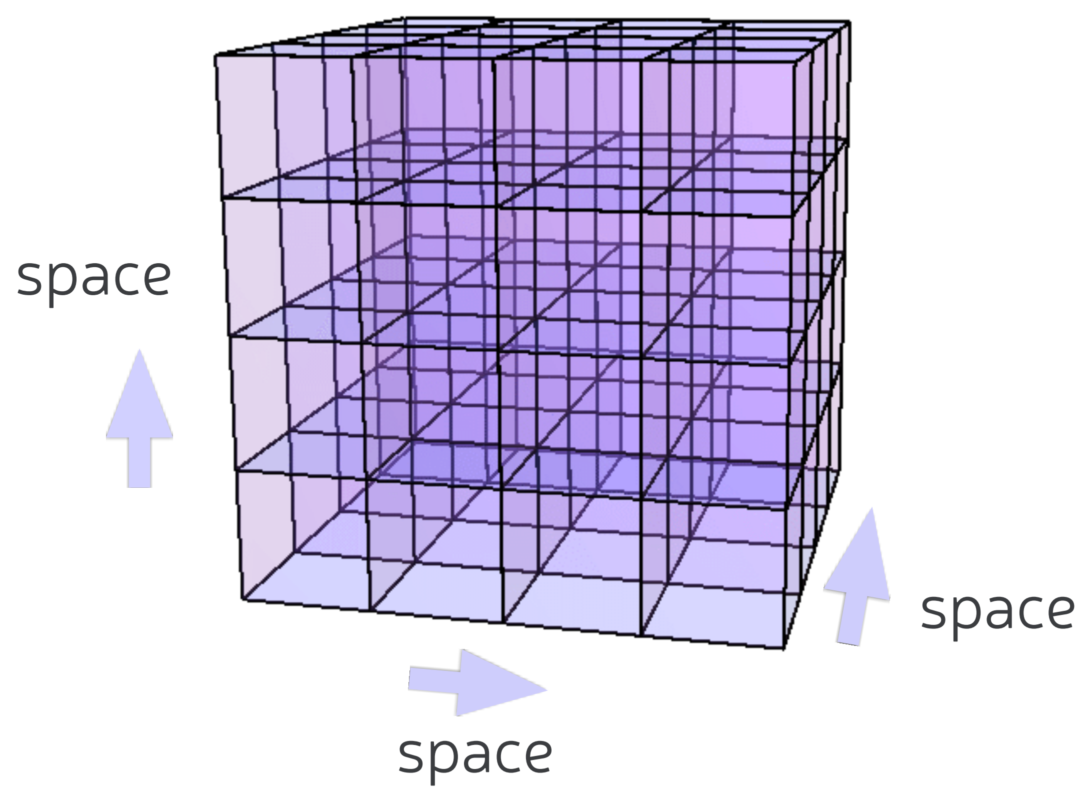
Analysis of double homological product shows.... $\nu < 2$



Surely “single-shot” just means you measure every qubit once. And you do this in the 3D Raussendorf cluster state model

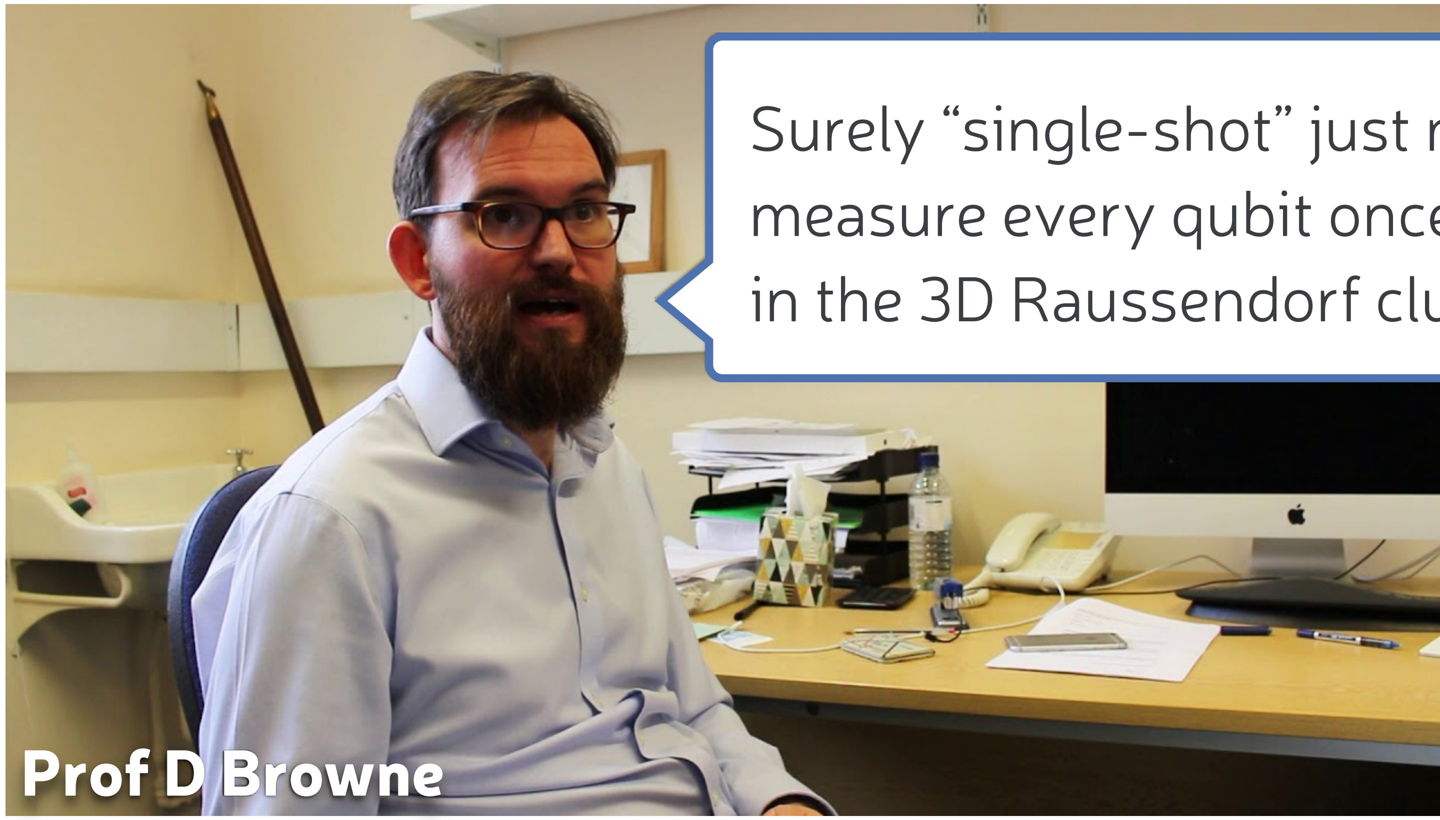
Raussendorf 3D cluster state
e.g. [Raussendorf, et al NJP ’07]

Like 2D toric code,
but 3 “space” dimensions.



Fiolated codes: extends idea to other CCS codes
[Bolt, Duclos-Cianci, Poulin, Stace, PRL ’16]

Basically repeated teleportation



Surely “single-shot” just means you measure every qubit once. And you do this in the 3D Raussendorf cluster state model

Hmmm…. maybe, maybe not…

But you have to pay an extra factor ***d*** in space cost in lieu of a factor ***d*** in measurement redundancy.

So if permitted, surely they would be **uninteresting** examples

Prof D Gottesman (at QIP2018)

But, in the **Steane model** of error correction
you don't need repeated measurements,
so isn't that single shot!

Refresher on Steane (a.k.a oold skool) EC:
Don't measure checks individually,
instead teleport through an ancilla $|+_L\rangle$
which you prepare offline to very high fidelity

Prof D Gottesman (at QIP2018)

But, in the **Steane model** of error correction you don't need repeated measurements, so isn't that single shot!

Hmmm…. this sounds a lot like foliated codes again.

This offline state preparation doesn't this normally use a factor **d** of extra resource.

Surely this is **"uninteresting"** again

What matters is resource cost

$$n\nu$$

number of qubits
including ancilla used
(e.g. foliation / Steane EC cost)

redundancy in measurements

but we also want lots of logical qubits.... so $$\frac{n\nu}{k}$$

number of logical qubits

How does this scale with the code distance

for 2D Toric code:

$$\frac{n\nu}{k} = O(d^3)$$

$$k = O(1), n = O(d^2), \nu = O(d)$$

for 4D Toric code:

$$\frac{n\nu}{k} = O(d^2)$$

$$k = O(1), n = O(d^2), \nu = O(1)$$

for double homological product codes

$$\frac{n\nu}{k} \sim \frac{n_c^4}{k_c^4}$$

where $[n_c, k_c, d_c]$ are initial classical parameters

there are classical codes where $\frac{n_c}{k_c} = O(1)$

so possible to achieve

$$\frac{n\nu}{k} = O(1)$$

constant overhead

Future work

Closing remarks

Soundness is sufficient condition for single-shot error correction

Constant overhead quantum fault-tolerance with quantum expander codes
Authors: Omar Fawzi, Antoine Grospellier, Anthony Leverrier

Uses single-shot codes with bad soundness!

Need to revisit problem to include also these examples of single-shot.

The University Of Sheffield.

reference more papers,
give examples of single shot codes/decoders,
discuss redundancy,

THANK YOU!

QUANTERA

EPSRC
Engineering and Physical Sciences Research Council