Stabilizer codes and a self-correcting quantum memory

Sergey Bravyi
Barbara Terhal

IBM Watson Research Center

Santa Fe, QIP 2009

What is the problem?

The goal is to design a realistic (2D or 3D) spin Hamiltonian whose ground state is an error correcting code. Relaxation times T_1, T_2 for a qubit encoded into the ground state must be macroscopic (grow with the system size).

Kitaev 97: Mimick classical self-correction in magnetic storage devices using systems with TQO. The toric code model.

Dennis et al 01: Self-correction is possible in the 4D toric code model

Bacon 01: 3D Quantum Compass Model (Bacon-Shor code)

Alicki et al 08: More rigorous analysis of the 4D toric code. Negative result for the 2D toric code.

Condensed matter physics	How a real device could look like? Decoherence mechanisms. Ground state properties
Coding theory	Study quantum error-correcting codes with local stabilizers. Find more examples beyond the toric code and Bacon-Shor code
Mathematical physics	Rigorous definition of self-correction. Is it possible in principle for realistic noise models?

2D stabilizer codes are not as good as we hoped

(a) Stabilizer codes with local generators

(b) Geometry of logical operators

(c) No-go theorem for 2D self-correcting q. memory

(d) Subsystem stabilizer codes with local generators

2D classical codes are better than we hoped

(a) Constructing quantum codes from classical codes

(b) 2D classical codes based on 1D cellular automatons

(c) Self-similarity under rescaling and fractal geometry

(d) Lower bounds on the distance

Stabilizer codes

Use n physical qubits to encode k logical qubits

Code-space: $\mathcal{L} \subseteq (\mathbb{C}^2)^{\otimes n}, \quad \dim(\mathcal{L}) = 2^k$

Stabilizer codes: code-space is spanned by states invariant under action of a stabilizer group $\mathcal{S}$

$$\mathcal{L} = \{|\psi\rangle \in (\mathbb{C}^2)^{\otimes n} \,:\, P\,|\psi\rangle = |\psi\rangle \quad \text{for all } P \in \mathcal{S}\}$$

$\mathcal{S}$ must be a subgroup of the Pauli group

$$\mathcal{P}(n) = \langle iI, X_1, Z_1, \ldots, X_n, Z_n \rangle$$

$\mathcal{S}$ must be abelian

$-I \notin \mathcal{S}$

Stabilizer codes

Use n physical qubits to encode k logical qubits

Code-space: $\mathcal{L} \subseteq (\mathbb{C}^2)^{\otimes n}, \quad \dim(\mathcal{L}) = 2^k$

Stabilizer codes: code-space is spanned by states invariant under action of a stabilizer group $\mathcal{S}$

$$\mathcal{L} = \{|\psi\rangle \in (\mathbb{C}^2)^{\otimes n} \, : \, P\,|\psi\rangle = |\psi\rangle \quad \text{for all } P \in \mathcal{S}\}$$

Logical operator: a Pauli operator that commutes with any element of $\mathcal{S}$ but does not belong to $\mathcal{S}$.

Stabilizer codes with local generators

Qubits are located at vertices of a D-dimensional lattice

$$\Lambda = \{1, \ldots, L\}^D$$

$n = L^D$ physical qubits; open/periodic boundary conditions

Definition: A Pauli operator P is r-local iff its support can be covered by a hypercube with r^D vertices.

We are interested in stabilizer codes for which the stabilizer group has r-local generators for some small constant r.

$$\mathcal{S} = \langle S_1, \ldots, S_m \rangle \quad \rightarrow \quad H = -\sum_{a=1}^{m} S_a$$

Such codes can be 'implemented' by a Hamiltonian with local interactions.

Main result: geometry of logical operators

Theorem: Any stabilizer code with r-local generators on a lattice $\Lambda = \{1, \ldots, L\}^D$ has at least one logical operator whose support can be covered by a D-dimensional box of size $r \times L \times \cdots \times L$.

$D = 1$: at least one logical operator has constant size; very bad codes even if active error correction is possible

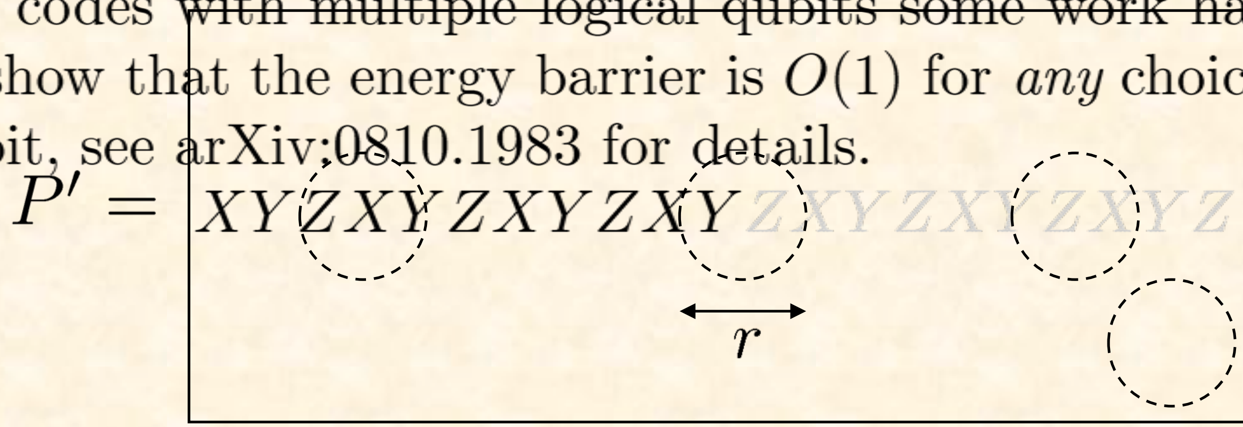
$D = 2$: at least one logical operator has string-like geometry; its support can be covered by $r \times L$ rectangle. This is a no-go result for self-correcting quantum memory: a partially implemented string costs at most $O(1)$ energy independent on the length of the string. No energy barrier that could prevent local errors from accumulating.

$$\mathcal{S} = \langle S_1, \ldots, S_m \rangle \quad \rightarrow \quad H = -\sum_{a=1}^{m} S_a$$

If a logical operator P has string-like geometry, the environment can map an encoded state $|\psi\rangle \in \mathcal{L}$ to $P|\psi\rangle$ by a sequence of single-qubit Pauli errors paying only constant energy penalty:

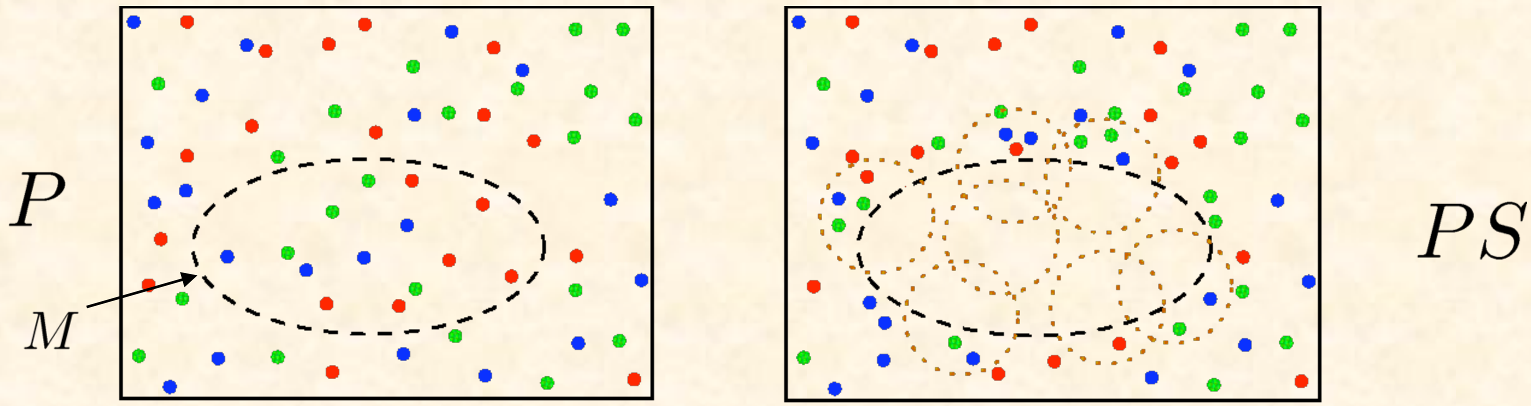
For codes with multiple logical qubits some work has to be done to show that the energy barrier is $O(1)$ for *any* choice of a logical qubit, see arXiv:0810.1983 for details.

Let P' be a partial implementation of P



$P'|\psi\rangle$ is a ground state for all generators S_a except for those located near the boundary of the string (within distance r). The number of such generators is at most $O(1)$.

Technical tools: cleaning lemma



Let P be a logical operator. Support of P is shown by the colored dots (representing X, Y, and Z).

Let $M \subseteq \Lambda$ be any subset of qubits (shown by the dashed ellipse). One of the following is true:

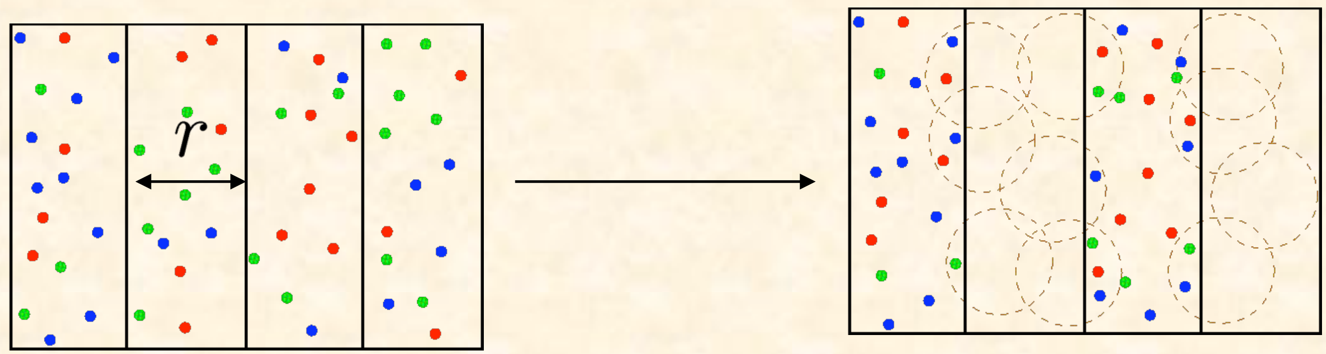
(a) There exists a logical operator supported on M

(b) There exists a stabilizer $S \in \mathcal{S}$ such that PS acts trivially on M. The stabilizer S includes only those generators whose support overlaps with M.

2D stabilizer codes have string-like logical operators:

1. Choose any logical operator P. Partition the lattice into vertical strips of size $r \times L$.

P



$Q = Q_1 Q_3$

2. If some strip supports a logical operator, we are done.

3. Otherwise clean out every even strip: $P \rightarrow Q = PS$.

4. Q is not a stabilizer $\Rightarrow$ some Q_j is not a stabilizer, say Q_1

5. Any generator of the stabilizer group overlaps with at most one uncleaned strip and thus Q_1 commutes with stabilizers. Thus Q_1 is a logical operator.

Subsystem codes

Use n physical qubits to encode k logical qubits

$$\text{Code-space:} \quad \mathcal{L} \subseteq (\mathbb{C}^2)^{\otimes n}$$

$$\mathcal{L} = \mathcal{L}_{logical} \otimes \mathcal{L}_{gauge}, \quad \dim\left(\mathcal{L}_{logical}\right) = 2^k$$

Logical subsystem

Gauge subsystem

Stabilizer codes: define $\mathcal{L}_{logical}$ and $\mathcal{L}_{gauge}$ in terms of groups of operators acting on these subspaces [Poulin 2005]

Gauge group $\mathcal{G}$	preserve the code-space $\mathcal{L}$ and act only on the gauge subsystem $\mathcal{L}_{gauge}$	Arbitrary (non-abelian) subgroup of the Pauli group $\mathcal{P}(n)$
Stabilizer group $\mathcal{S} \subseteq \mathcal{G}$	preserve the code-space $\mathcal{L}$ and act trivially on both subsystems	The center of $\mathcal{G}$
Logical operators	preserve the code-space $\mathcal{L}$ and act non-trivially on the logical subsystem $\mathcal{L}_{logical}$	Pauli operators that commute with any element of $\mathcal{S}$ but do not belong to $\mathcal{G}$

We are interested in subystem codes for which the gauge group has r-local generators. Such codes can be "implemented" by local Hamiltonians.

Example : 2D Bacon-Shor code

$$\mathcal{G} = \left\langle \begin{array}{cccc} \boxed{\begin{matrix} X & X & \\ & & \\ & & \end{matrix}} & \boxed{\begin{matrix} & X & X \\ & & \\ & & \end{matrix}} & \boxed{\begin{matrix} & & \\ & & \\ X & X & \end{matrix}} & \boxed{\begin{matrix} & & \\ & & \\ & X & X \end{matrix}} \\ \boxed{\begin{matrix} Z & & \\ Z & & \\ & & \end{matrix}} & \boxed{\begin{matrix} & & \\ Z & & \\ Z & & \end{matrix}} & \boxed{\begin{matrix} & & Z \\ & & Z \\ & & \end{matrix}} & \boxed{\begin{matrix} & & \\ & & Z \\ & & Z \end{matrix}} \end{array} \right\rangle$$

$$\mathcal{S} = \left\langle \boxed{\begin{matrix} X & X & \\ X & X & \\ X & X & \end{matrix}} \quad \boxed{\begin{matrix} & X & X \\ & X & X \\ & X & X \end{matrix}} \quad \boxed{\begin{matrix} Z & Z & Z \\ Z & Z & Z \\ & & \end{matrix}} \quad \boxed{\begin{matrix} & & \\ Z & Z & Z \\ Z & Z & Z \end{matrix}} \right\rangle$$

Logical operators: single columns of X and single rows of Z

The Hamiltonian = 2D Quantum Compass Model

Main Result: geometry of logical operators

Theorem 2: Suppose subsystem stabilizer code on a lattice $\Lambda = \{1, \ldots, L\}^D$ has a gauge group with r-local generators. Then there is at least one logical operator whose support can be covered by a D-dimensional box of size $3r \times L \times \cdots \times L$.

(for the proof see arXiv:0810.1983)

$D = 1$: at least one logical operator has constant size; very bad codes even if active error correction is possible

$D = 2$: at least one logical operator has string-like geometry. This doesn't imply a no-go theorem for self-correction, because logical operators may create excitations and a string may have constant energy cost per unit of length.

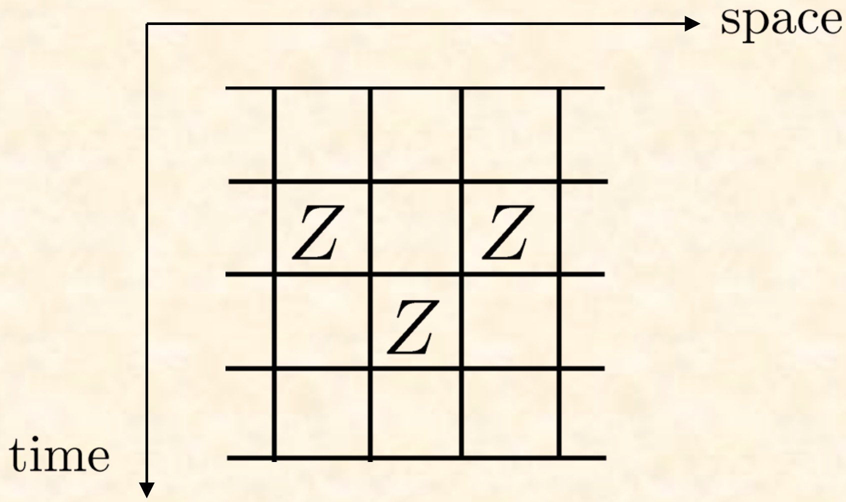
2D classical linear codes

Motivation: there is a systematic way of constructing stabilizer subsystem codes from classical linear codes
Bacon & Casaccino 2006

Classical	Quantum
$C_1 = [n_1, k_1, d_1]$ $C_2 = [n_2, k_2, d_2]$	$Q = [[n_1 n_2, k_1 k_2, \min(d_1, d_2)]]$
Spatial dimensions $D_1,\ D_2$	Spatial dimension $D_1 + D_2$
r-local parity checks	r-local generators of the gauge group

The code CA(1)

Define a classical linear 2D code CA(1) whose stabilizer group (parity checks) is generated by translations of

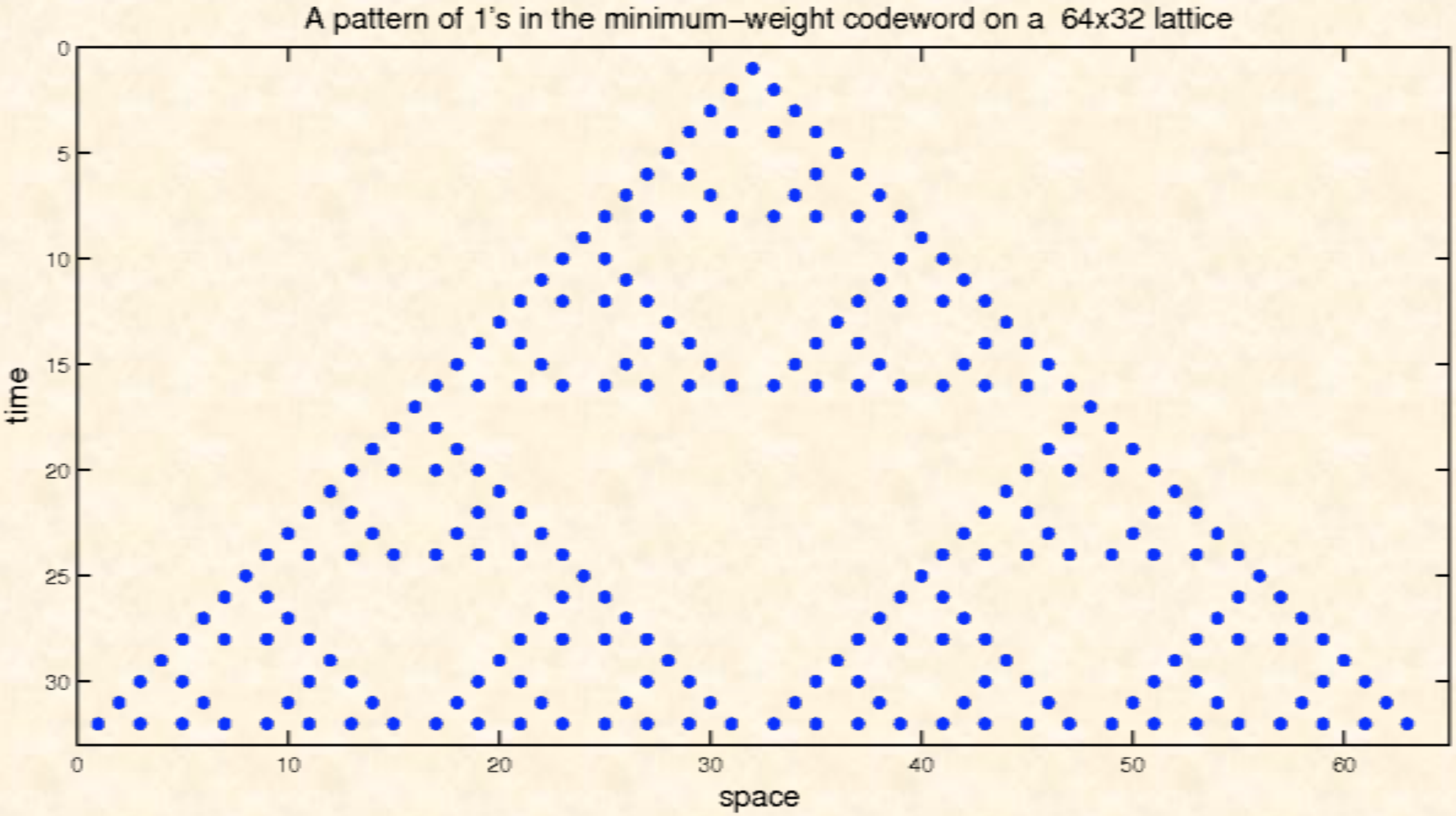


Any code-word of CA(1) represents "computational history" of 1D cellular automaton with transition rules

$$x_i^{t+1} = x_{i-1}^t \oplus x_{i+1}^t .$$

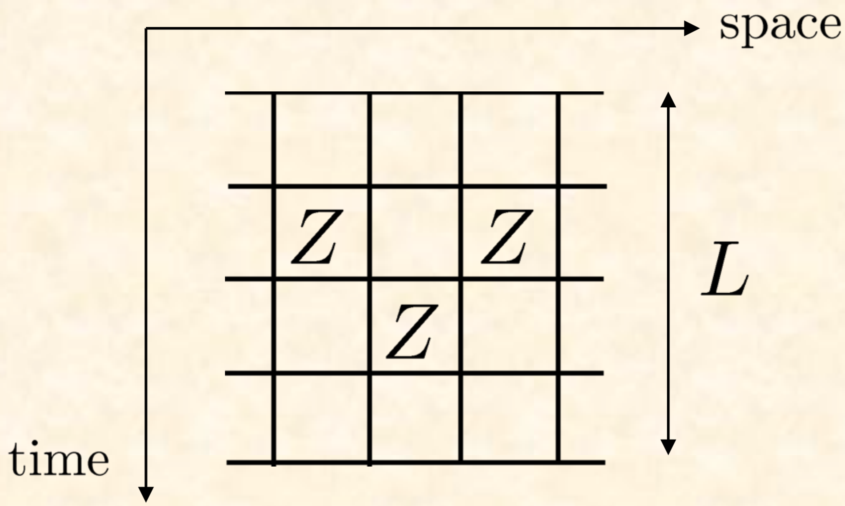
The idea of CA-based codes: Roychowdhury et al 1991

Example of a codeword: a pyramid



Any codeword of CA(1) is uniquely determined by initial conditions at $t = 0$. Any initial condition is admissible. Thus CA(1) has 1 logical bit per unit of length in the horizontal direction.

Rigorous analysis is possible for $\Lambda = \mathbb{Z} \times \{0, 1, \ldots, L-1\}$



Theorem: Suppose L is a power of 2. Then CA(1) has distance $d = L^{\log_2 3} \approx L^{1.6}$. Pyramids are the minimum-weight codewords.

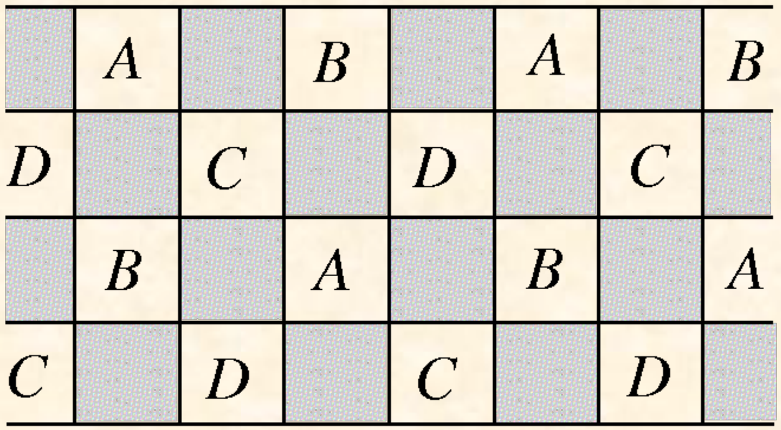
Numerical simulation: the same scaling holds for $L \times L$

It suggests that CA(1)=$[L^2, L, L^{\log_2 3}]$

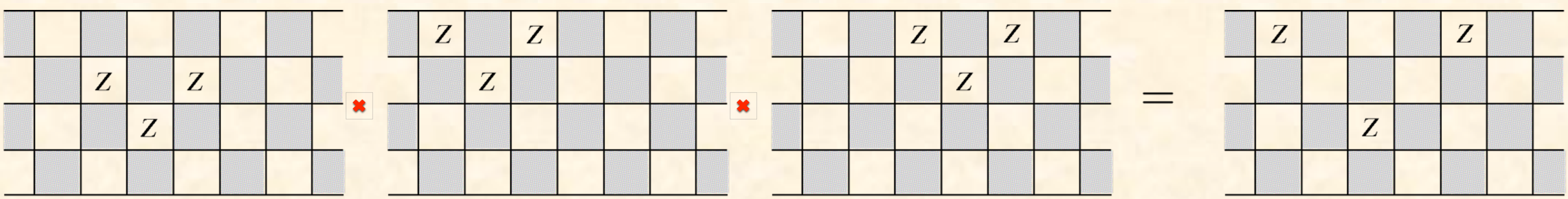
Bacon & Casaccino $\rightarrow$ $[[L^4, L^2, L^{\log_2 3}]]$ 4D subsystem code

Self-similarity of CA(1)

Consider 4 sublattices A, B, C, D defined below



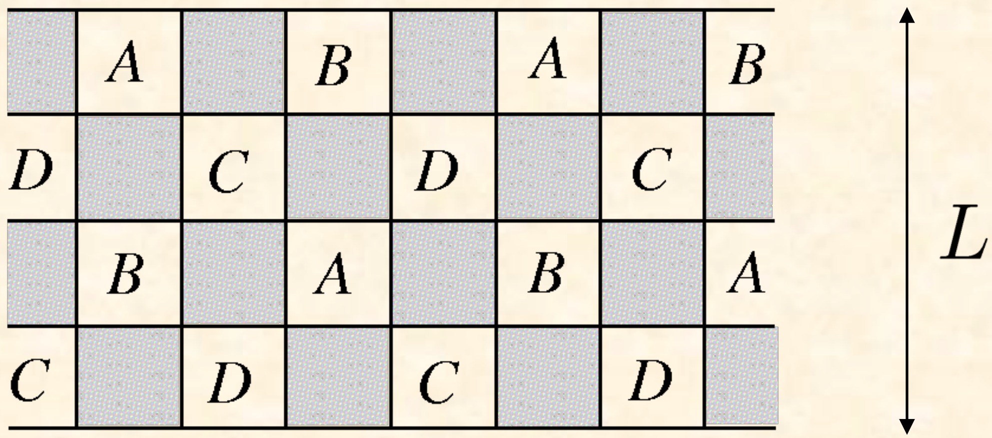
The code CA(1) reproduces itself on each of the sublattices A, B, C, D



Each sublattice A, B, C, D is obtained from the white sub-lattice by a change of scale $L \to L/2$

Self-similarity of CA(1)

Consider 4 sublattices A, B, C, D defined below



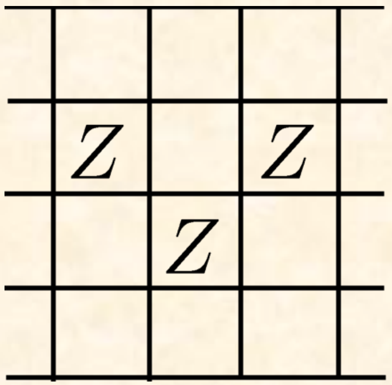
The code CA(1) reproduces itself on each of the sublattices A, B, C, D

$$d(L) \geq \Gamma \cdot d(L/2)$$

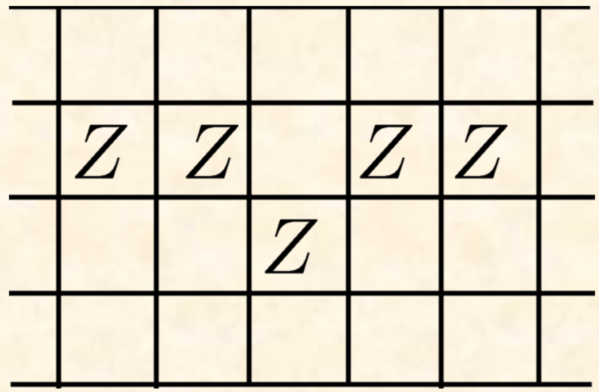
Γ is the minimum number of sublattices that can be occupied by a non-zero codeword.

Prove that $\Gamma = 3$. It yields $d \geq 3^{\log_2 L} = L^{\log_2 3}$.

The family of codes $\{\mathrm{CA}(r)\}$



CA(1)



CA(2)

e.t.c.

Any code $\mathrm{CA}(r)$ has self-similarity property. For any integer q the code reproduces itself on a sublattice with period 2^q.

Theorem: The distance of CA(2) satisfies $d \geq L^{\log_4(10)} \approx L^{1.7}$.

Numerical simulation: $d \sim L^{1.8}$

Numerical simulation of CA(r) for larger values of r yields

$$d \sim L^{\theta(r)}$$

r	$\theta(r)$
1	1.585
2	1.80
3	1.80
4	1.84
5	1.9

Conjecture: For any $\epsilon > 0$ one can make the distance $d \geq L^{2-\epsilon}$ by choosing sufficiently large r.

It would yield codes $[L^2, L, L^{2-\epsilon}]$

Compare it with the 2D repetition code $[L^2, 1, L^2]$

Bacon & Casaccino $\rightarrow$ $[[L^4, L^2, L^{2-\epsilon}]]$ 4D subsystem code

Open problems/conjectures

1. Prove that 3D stabilizer codes have string-like logical operators. It would imply no-go theorem for SCQM based on 3D stabilizer Hamiltonians.

2. Possibility of QSCM based on 2D subsystem stabilizer codes.

3. Tradeoff between k and d. For 2D classical codes we can prove $k\sqrt{d} = O(n)$. The code CA(1) satisfies $k\sqrt{d} \sim n^{0.9}$. Is this bound tight? What about quantum 2D codes?