Lectures on Fault-Tolerant Quantum Computation

B.M. Terhal, IBM Research

I. Descriptions of Noise and Quantum States

II. Quantum Coding and Error-Correction

III. Fault-Tolerant Error-Correction. Surface Codes. Some Results on Noise Thresholds.

Some Background Reading

Textbook by Michael Nielsen & Isaac Chuang
Lectures notes of John Preskill

PhD Thesis of Dan Gottesman
PhD Thesis by Ben Reichardt

Arxiv: quant-ph/0110143 by Dennis, Landahl, Kitaev,Preskill on use of surface codes
Arxiv: quant-ph/0610063 by Aliferis, Cross on Bacon-Shor Codes
Arxiv: 0711.1556 by Cross, DiVincenzo, Terhal with threshold studies

The 5 DiVincenzo Criteria

1. Architecture needs to be scalable with well-defined qubits.

2. Ability to initialize qubits to |00...0> state

3. Qubits should undergo little decoherence

4. Ability to enact a discrete set of logical gates. For example:

2-qubit gate: CNOT (C-X) or CPHASE (C-Z)

1-qubit gates: Pauli X, Z, Y, Hadamard, Phase gate, T gate

5. Ability to measure single qubits in the computational (0,1) basis.

Some Quantum Formalism

Density matrices ρ:

1. $\rho = \rho^\dagger$.
2. $\rho \geq 0$, non-negative eigenvalues
3. $Tr(\rho) = 1$.

Von Neumann projective measurement:

Rank 1 projectors $\{\Pi_i\}, \sum_i \Pi_i = I$

$p(i) = \mathrm{Tr}\Pi_i \rho$

POVM measurement:

$\{E_i\}$, $E_i^\dagger = E_i \geq 0$, $\sum_i E_i = I$.

$p(i) = \mathrm{Tr} E_i \rho$

Superoperators

$\mathcal{S}(\rho) = \sum_i A_i \rho A_i^\dagger$, Kraus operators A_i.

$\sum_i A_i^\dagger A_i = I$.

-Superoperators, TCP maps, map density matrices onto density matrices.

-Can always be viewed as a unitary interacting with system and environment

-Number of Kraus operators $\{A_i\}$ at most d^2. Kraus operators are non-unique.

-$I \otimes \mathcal{S}$ also TCP, compare with matrix transposition.

Examples

1. Depolarizing Channel :

$\mathcal{S}(\rho) = (1-p)\rho + p(X\rho X + Y\rho Y + Z\rho Z)/3$

2. Amplitude Damping Channel:

$|0\rangle \rightarrow |0\rangle$

$|1\rangle$ decays with rate γ to $|0\rangle$.

3. Over/Under-Rotation Channel:

Gaussian distribution around $U = e^{i\theta Z}$ with, say, $\theta = \pi/8$.

What is a discrete set of Kraus operators?

Superoperator Noise Model

Each location in a quantum circuit is represented by its own superoperator which ideally is close to the ideal operation.

(Simplest) Noise Model considered in Fault-Tolerance Theory

In what situations is this model sufficient….

(In)Sufficiency of Superoperator Noise Picture

Cross-talk between neighboring qubits (addressing the wrong qubits with the control fields)
Couplings we cannot turn off…

Some noise is best modeled as a system interacting with a quantum environment. Correlations in time and space, non-markovian environment.

Some noise can be clearly approximated by classical fluctuations of control parameters, correlations in time and space of these parameters.

Error Rates

Error rate of a superoperator?

$$\mathcal{S}(\rho) = U\rho U^\dagger + \mathcal{E}(\rho).$$

U is ideal gate.

$||\mathcal{E}||?$ should be $||I \otimes \mathcal{E}||$.

Diamond norm with useful norm properties

$$|||\mathcal{E}||_\diamond = \max_{||X||_{tr}=1} ||(I \otimes \mathcal{E})(X)||_{tr}$$

$$||X||_{tr} = Tr\sqrt{X^\dagger X}.$$

Error-Correction

Classical error-correction is fairly common:

Satellite communication & deep-space communication
Soft (radiation errors) in dynamical RAM in satellites
Compact discs (Reed Solomon codes) and hard discs.
Hard-wired coding of bits as ferromagnetic domains ->
2D repetition code

Noise levels of quantum operations are high

Quantum error-correction will be crucial in any robust implementation of quantum computation.

Passive EC (e.g. topological quantum computation) or active

Error-Correction

Classical error-correction is fairly common:

Satellite communication & deep-space communication
Soft (radiation errors) in dynamical RAM in satellites
Compact discs (Reed Solomon codes) and hard discs.
Hard-wired coding of bits as ferromagnetic domains ->
2D repetition code

Noise levels of quantum operations are high

Quantum error-correction will be crucial in any robust implementation of quantum computation.

Passive EC (e.g. topological quantum computation) or active

Classical Repetition Code

$|0\rangle \rightarrow |00...0\rangle \equiv |\bar{0}\rangle$, n (odd) bits
$|1\rangle \rightarrow |11...1\rangle \equiv |\bar{1}\rangle$

-Hamming distance d between codewords is n.

-Code can correct $t = (n-1)/2$ errors
where $d = 2t + 1$ by taking majority of bits.

-Logical bit flip is $\overline{X} = X_1 X_2 .... X_n$

Classical Repetition Code

Can we do error-correction without finding out whether the state is $|\bar{0}\rangle$ or $|\bar{1}\rangle$?

Yes, 'measure' $Z_i Z_{i+1}$ for adjacent bits and match the places where a -1 error syndrome for $Z_i Z_{i+1}$ is found.

Note: CNOT and Toffoli can be performed block-wise or transversal on encoded qubits.

Quantizing Repetition Code

First quantum code:
Shor's 9 qubit code, [[n=9,k=1,d=3]].

First, preserving 1 qubit against bitflip errors (X)

-Stabilizer S of a code, abelian subgroup of the Pauli group. S is here generated by $Z_1 Z_2$ and $Z_2 Z_3$.

-k=# encoded qubits=n-(# generators of S), here $3-2=1$.

Error Correction

Measure generators of stabilizer.
Syndrome determines error.
EC for this code: Single errors get corrected.

Two errors $X_1 X_2$, say, become logical $(\overline{X})$ errors.

How to measure a Pauli or product of Paulis....
nondestructively?
How linear combinations of errors get corrected
i.e. superoperator noise....

Phase flip errors on $\{|000\rangle, |111\rangle\}$ code: logical Z, $\overline{Z} = Z_i$.

Stabilizer picture:
-Logical operators commute with S.
Normalizer group N(S): all operators in Pauli group which commute with S.
Lowest weight element in N(S)-S is distance of code.

-Detectable errors anticommute with some elements in S.

[[9,1,3]] Shor code

Correct for Z errors with C_{phase}

$|0\rangle \rightarrow |+++\rangle$, $|1\rangle \rightarrow |---\rangle$.

Use concatenation, encode with C_{bit}

$|+\rangle \rightarrow (|000\rangle + |111\rangle)/\sqrt{2}$,

$|-\rangle \rightarrow (|000\rangle - |111\rangle)/\sqrt{2}$.

$\overline{X}$ and $\overline{Z}$ are weight 3 Pauli operators, d=3.

2+6=8 stabilizer generators.

Other Quantum Codes

More efficient quantum code than [[9,1,3]]: [[5,1,3]] but this code has a non-transversal CNOT

Steane code [[7,1,3]]:
-transversal CNOT, most studied code for FT.
-is CSS code, stabilizers are X or Z-stabilizers, never mix.

Bacon-Shor Code Family....

Other Quantum Codes

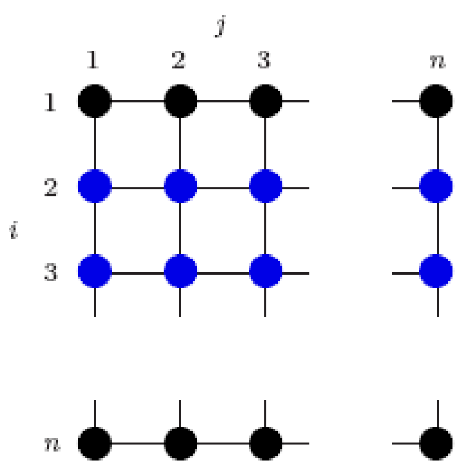
More efficient quantum code than [[9,1,3]]: [[5,1,3]]
but this code has a non-transversal CNOT

Steane code [[7,1,3]]:
-transversal CNOT, most studied code for FT.
-is CSS code, stabilizers are X or Z-stabilizers,
never mix.

Bacon-Shor Code Family....

Bacon-Shor Codes

Lattice of 3 x 3 qubits (or 5 x 5 or 7 x 7 etc.)
X-stabilizers are 2 adjacent horizontal lines of Xs.
Z-stabilizers (linear combinations of [[9,1,3]] stabilizers) are adjacent vertical lines of Zs.
9-4=5 encoded qubits…(in general n^2-2(n-1) qubits).



Elements in N(S)-S:
Horizontal $Z_j Z_{j+1}$.
Vertical $X_i X_{i+1}$.
Z along 1st vertical line
X along 1st horizontal line.

Bacon-Shor Codes

Elements in N(S)-S of weight 2, no protection against those errors...?

Elements in N(S)-S:

$Z_1 Z_2$, $X_2 X_5$: Logical ops. of gauge qubit 1

$Z_4 Z_5$, $X_5 X_8$: gauge qubit 2

$Z_2 Z_3$, $X_3 X_6$, gauge qubit 3

$Z_5 Z_6$, $X_6 X_9$, gauge qubit 4

$Z_1 Z_4 Z_7$, $X_7 X_8 X_9$ logical qubit!

Can correct 1 error on logical qubit.

Bacon-Shor Codes

Elements in N(S)-S of weight 2, no protection against those errors...?

Elements in N(S)-S:

$Z_1 Z_2$, $X_2 X_5$: Logical ops. of gauge qubit 1

$Z_4 Z_5$, $X_5 X_8$: gauge qubit 2

$Z_2 Z_3$, $X_3 X_6$, gauge qubit 3

$Z_5 Z_6$, $X_6 X_9$, gauge qubit 4

$Z_1 Z_4 Z_7$, $X_7 X_8 X_9$ logical qubit!

Can correct 1 error on logical qubit.

Measuring Stabilizers

Measure $Z_1Z_2Z_4Z_5Z_7Z_8$ row by row, i.e. measure Z_1Z_2, and Z_4Z_5 and Z_7Z_8.

Each of these commutes with S and $\overline{X}$ and $\overline{Z}$ of logical qubit.

Same for horizontal lines of Xs.
Advantage: simple (local) circuits for measuring stabilizer!
"Symmetrized, quantized, repetition code"

Surface Code Family

Qubits live on edges.
Stabilizer generated by:
-plaquette operators: ZZZZ around plaquette
-star operators: XXXX on edges touching vertex
13 qubits - 12 stabilizers=1 encoded qubit.

Elements in N(S)-S:
ZZ....Z from rough boundary to other rough boundary.
XX...X on "dual lattice" from smooth boundary to other smooth boundary.

Distance of this code is 3: [[13, 1, 3]] code

Surface Code Family

More general: $L \times L$ lattice of vertical links
$L(L-1)$ plaquettes, $L(L-1)$ stars, so
$L^2 + (L-1)^2 - 2L(L-1) = 1$ encoded qubit.

Distance is L. $[[L^2 + (L-1)^2, 1, L]]$ code
(Bacon-Shor codes $[[n^2, 1, n]]$)

Trivial operations on code space can be made from composing plaquette and star operators. These are loops of ZZ...Z on lattice and loops of XX..X on 'dual lattice'.

Errors on Surface Codes

Measure plaquette stabilizer. Note that this can be done locally. If outcome is -1, put a defect in the plaquette.

Defects appear in pairs (except at boundary), like in classical repetition code.

Error-Correction: match up defects pair-wise (or with ghost defects at boundary), so that the length of the strings connecting defects is small.

Code can correct many errors of weight more than L!
$\Rightarrow$ Topological Protection

Passive Noise Protection

Hamiltonian, sum of stabilizer generators
$H = -\sum_i S_i$.
2-dimensional ground-space is surface code space.
H has a gap. But is there topological protection
at nonzero temperature T?

Pairs of defects created, string can grow
without energy penalty to become a logical error!

Topological order destroyed at $T > 0$: needed:
1. fancier Hamiltonian? (e.g. 4-dim surface code..)
2. active EC.

Noise Threshold

Encoded operation: encoded gate followed by EC.
Assume code can correct a single error.
Every location in encoded gate and error-correction has an error probabability p.
Assume no single error can cause two errors on an encoded block! (idea of fault-tolerance).

p_1=Prob(incorrectable error) $=Np^2$ where N is number of pairs of locations leading to 2 or more errors in the block.

If $p_1 < p$, coding helps, below threshold $p_c = 1/N$
If $p_1 > p$, coding makes things worse.

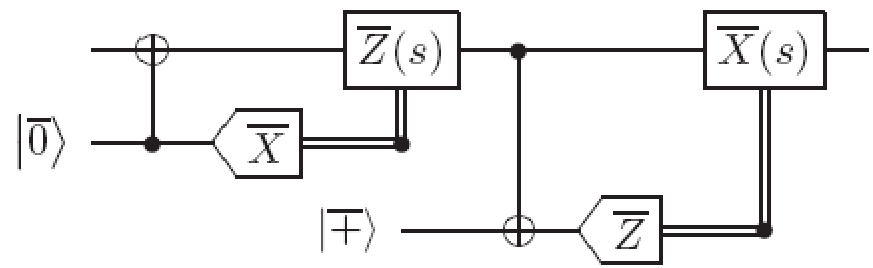
How can 1 error become 2 errors on data during EC?

Low-weight stabilizers are good!

Tricks for making EC fault-tolerant:

-Shor EC, instead of $|+\rangle$ use cat-state

$|\bar{+}\rangle \propto |00..0\rangle + |11..1\rangle$



-Steane EC

Copy X errors onto an ancilla prepared in logical state.

Read off X errors on ancillas.

Similar for Z errors.

Advantage: get info for all Z stabilizers in one go.

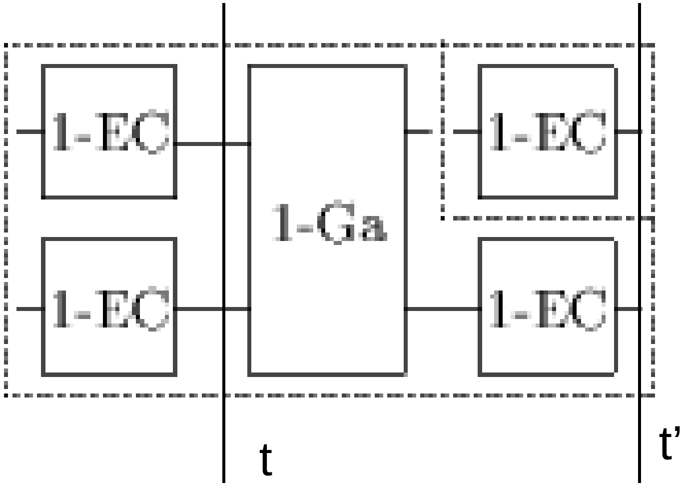
Bad overhead of preparing verified ancilla.

Threshold Studies

Parameters	Notes
[[5, 1, 3]]	non-CSS five qubit code [24]
[[7, 1, 3]]	Steane's 7-qubit code (doubly-even dual-containing) [25]
[[9, 1, 3]], [[25, 1, 5]], [[49, 1, 7]], [[81, 1, 9]]	Bacon-Shor codes [14]
[[15, 1, 3]]	Quantum Reed-Muller code [19, 20]
[[13, 1, 3]], [[41, 1, 5]], [[85, 1, 7]]	Surface codes [17, 18]
[[21, 3, 5]]	Dual-containing polynomial code on $GF(2^3)$ [26]
[[23, 1, 7]]	Doubly-even dual-containing Golay code (cyclic) [27]
[[47, 1, 11]]	Doubly-even dual-containing quadratic-residue code (cyclic) [21]
[[49, 1, 9]]	Concatenated [[7, 1, 3]] Hamming code [22]
[[60, 4, 10]]	Dual-containing polynomial code on $GF(2^4)$ [26]
[[79, 1, 15]], [[89, 1, 17]], [[103, 1, 19]], [[127, 1, 19]]	BCH codes, not analyzed [21]

Cross, DiVincenzo, Terhal, 2007

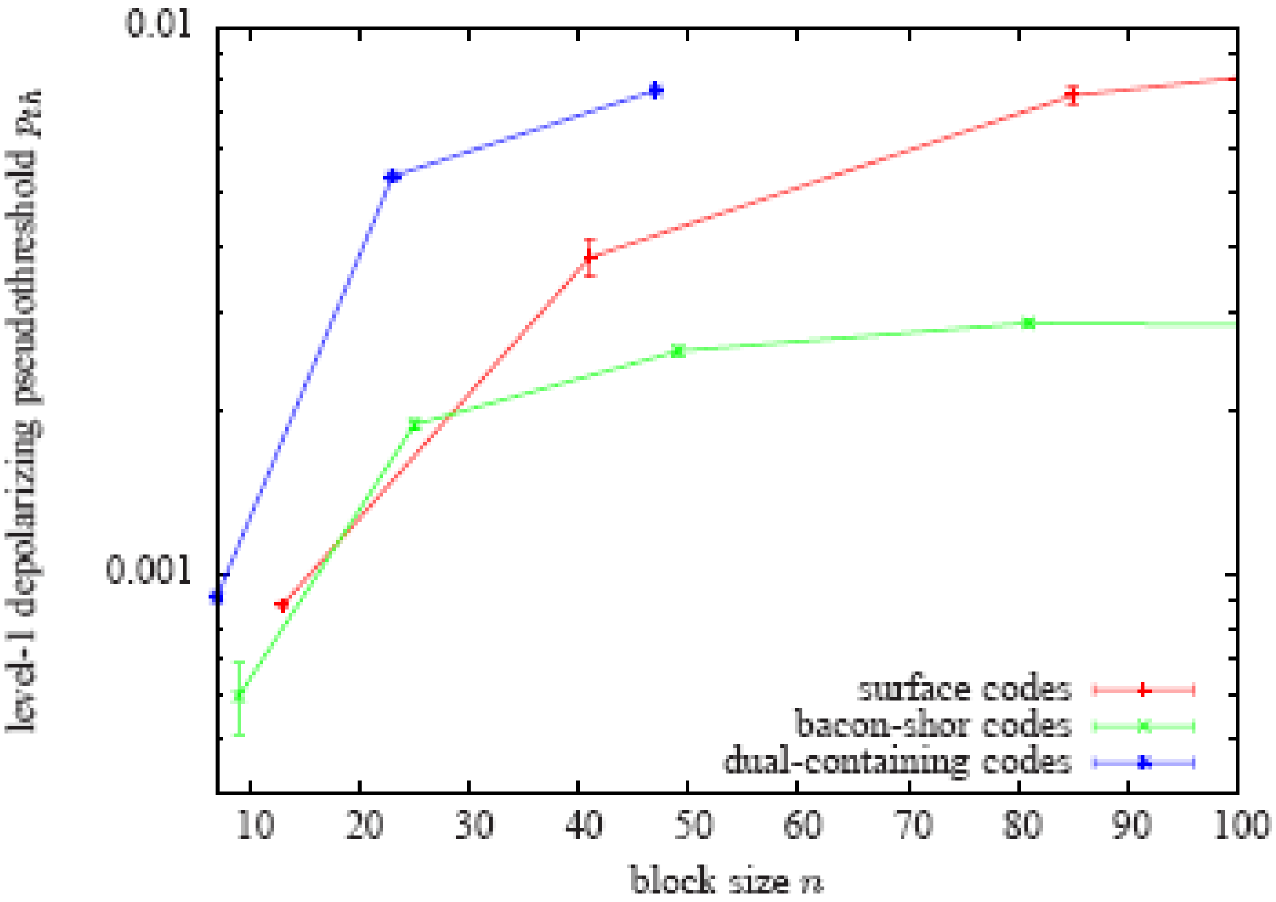
What we study



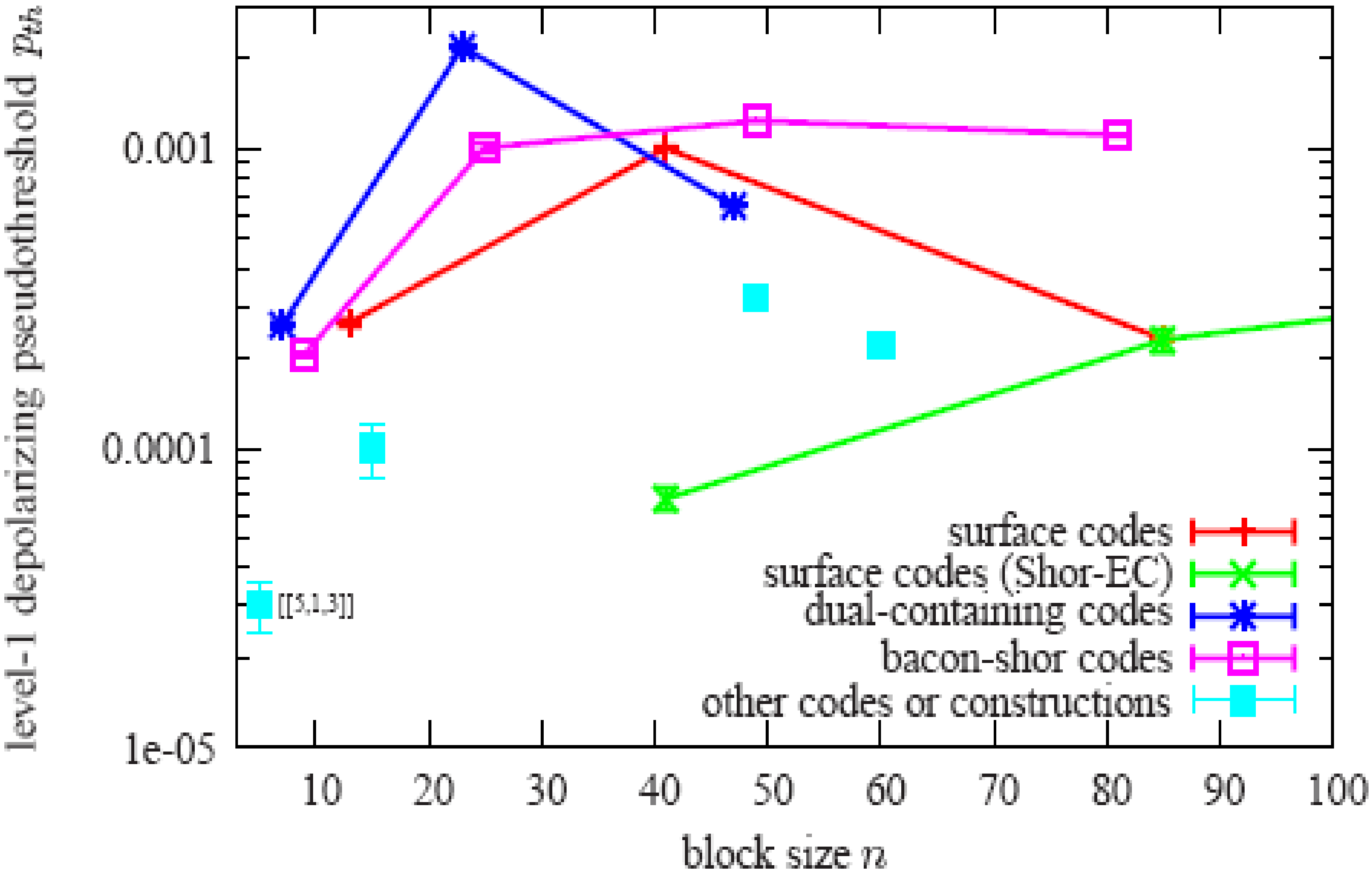
Extended-rectangle.
Here 1-Ga taken as transversal CNOT.
Steane EC.
Generate random X,Y,Z errors with probability p on all locations.
Follow errors through gates in the rectangle. If errors add up to logical error between state at t and state at t', call it a failure.

Estimate probability for failure p_1 as function of p.
Threshold: p_1=p.

Perfect Ancillas for Steane EC



Thresholds



level-1 depolarizing pseudothreshold p_{th}
0.001
0.0001
1e-05
10
20
30
40
50
60
70
80
90
100
block size n
[[5,1,3]]
surface codes
surface codes (Shor-EC)
dual-containing codes
bacon-shor codes
other codes or constructions

Surface Code

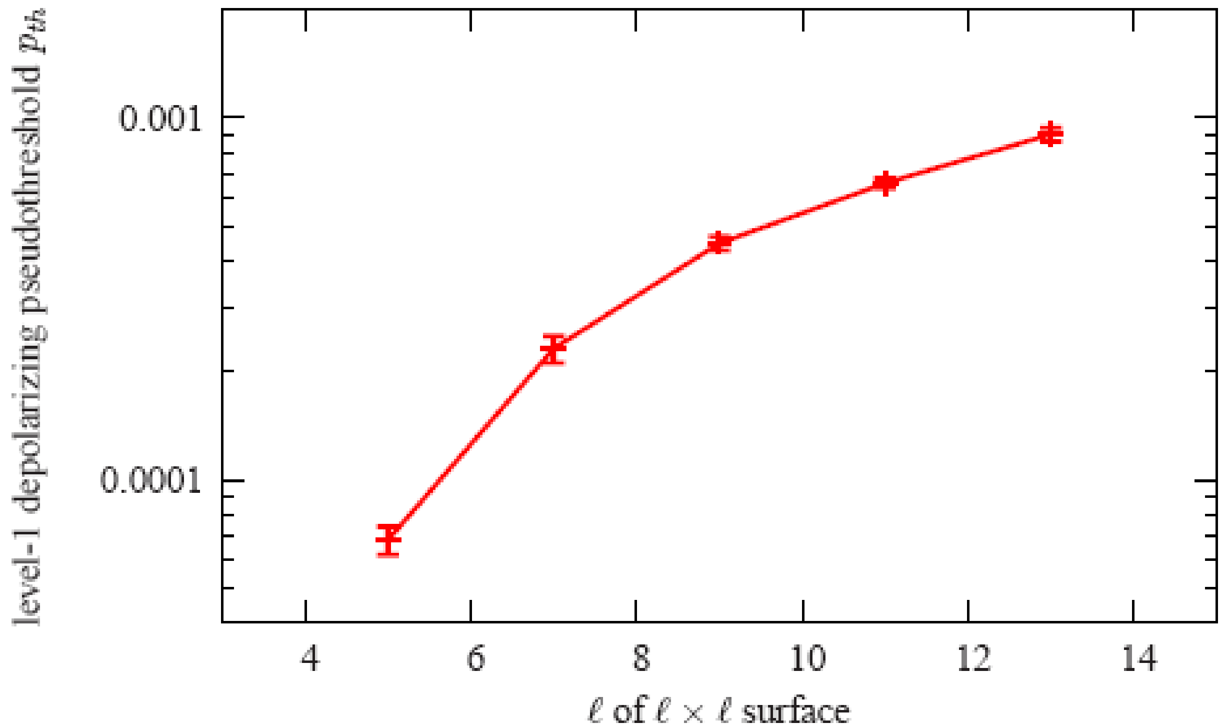


Figure 11: Surface code level-1 depolarizing pseudo-threshold versus ℓ for $\ell \times \ell$ surface code (the block-size $n = \ell^2 + (\ell - 1)^2$). The ex-Rec is a transversal CNOT gate with ℓ sequential Shor-EC steps per EC. The pseudo-threshold increases with ℓ and is expected to approach a constant value in the limit of large ℓ, unlike the other codes in this study.

We find for L ♎ 🕓, p_c goes to 3.5×10^{-3}

Overhead versus logical error-rate