History of quantum error correction

B.M. Terhal, QuTech,

and Dept. of Applied Math., TU Delft

QuTech

Theory of quantum error correction and fault-tolerance emerged quickly, in the years 1995-1997

Is decoherence fundamental?

Andrew Steane (Proc. Roy. Soc. Lond. A452 (1996) 2551) wrote:

"However, it can be argued that the possibility of decoherence is itself just as fundamental a feature of quantum mechanics as the interference and entanglement of which a quantum computer takes advantage.

Such decoherence must be considered, for example, in any discussion of the "Schroedinger's cat" paradox.

The cat in Schroedinger's thought-experiment corresponds here to the quantum computer itself.

Hence, *the idealisation in which decoherence is taken to be negligible is not merely a limit on the practical application of the theory of quantum computation*, it is in fact an "idealisation too far", since it involves neglecting a basic aspect of quantum theory, as has been emphasized by Landauer 1995".

The first quantum error correcting codes by Shor and Steane in 1995 and 1996.

Shor: one *can* reverse decoherence

Phys. Rev. A 52, R2493, 1995, Received May 1995:

"To preserve the state of superposition of the encoded qubit, what we do in effect is to measure the decoherence without measuring the state of the qubits."

One qubit is replaced by nine qubits and code can correct any single qubit error.

Superpositions of errors allowed! E.g. error on a single qubit $E = aI + bX + cY + dZ$, with $a, b, c, d \in \mathbb{C}$, and Pauli $X, Y, Z, Y \propto XZ$.

New key insights:

- we can learn about which error occurred without learning about the logical state.
- generalizes classical codes, but not by copying quantum information (no-cloning).
- one needs to correct both X (bit flip) and Z (phase flip) errors and this suffices: project errors by measurement onto a discrete set of errors.

Steane: fundamentals and 7 qubit code

Phys. Rev. Lett. 77, 1996, Received Oct. 1995:

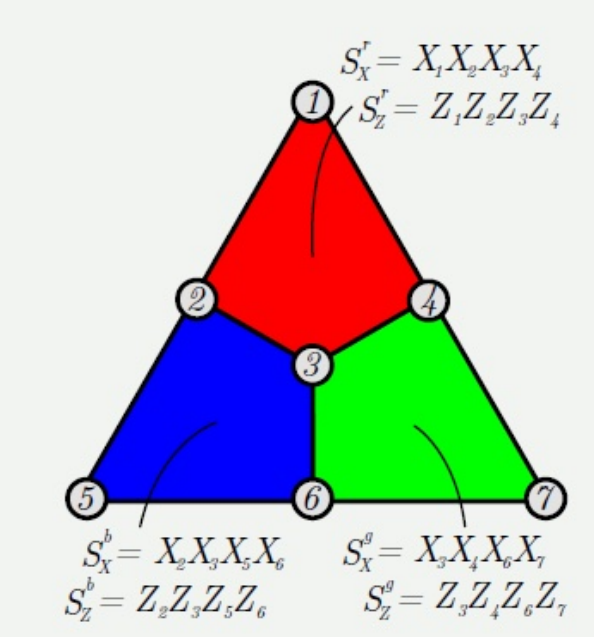
"…It is shown that a pair of states which are, in a certain sense, "macroscopically different," can form a superposition in which the *interference phase between the two parts is measurable*. This provides a highly stabilized "Schrödinger cat" state…"

$$|\overline{0}\rangle \propto |0000000\rangle + |1010101\rangle + |0110011\rangle + |1100110\rangle + |0001111\rangle + |1011010\rangle + |0111100\rangle + |1101001\rangle .$$
$$|\overline{1}\rangle \propto X_1X_2X_3X_4X_5X_6X_7|\overline{0}\rangle.$$

The phase in $|\overline{0}\rangle + |\overline{1}\rangle$ versus $|\overline{0}\rangle - |\overline{1}\rangle$ is robust or measurable, as the logical distance between these codewords is also 3, allowing to correct a phase flip error on any qubit.

$|\overline{0}\rangle = |\text{alive cat}\rangle, |\overline{1}\rangle = |\text{dead cat}\rangle$

Steane code and its parity checks (small two-dimensional color code, Bombin/Martin-Delgado, 2006)



Background: classical error correction

To protects bits and a classical computation from errors one can use a classical error-correcting code such as as the repetition code.

For example, the 3-bit repetition code (distance 3)

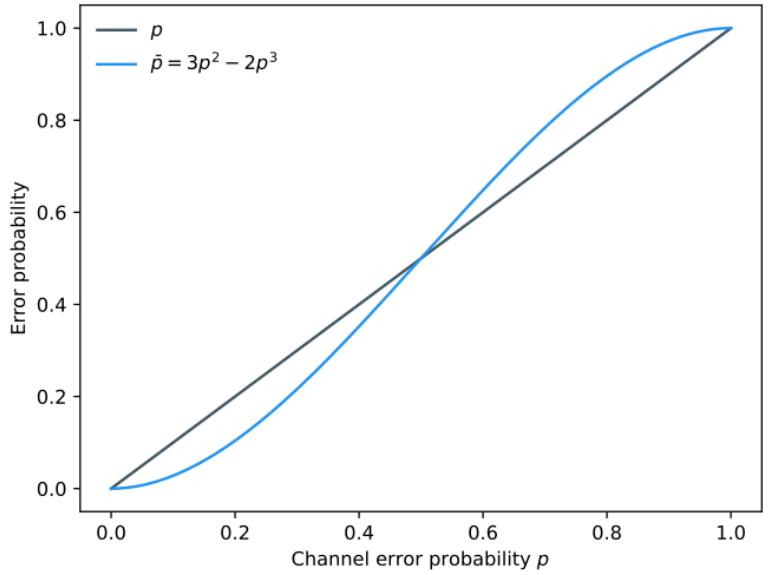
$$|0\rangle \to |000\rangle \equiv |\bar{0}\rangle \equiv |0\rangle_L, |1\rangle \to |111\rangle \equiv |\bar{1}\rangle \equiv |1\rangle_L.$$

One of the 3 bits flip, but taking majority of the bits one can still learn the logical bit.

Bit flip represented as Pauli X: $X|0\rangle = |1\rangle, X|1\rangle = |0\rangle$.

Computation on logical bits easy: just execute the computation three times in parallel and take a majority vote.

Logical failure occurs when 2 bit flips happen, with probability $O(p^2)$, given independent bit flip probability p.



classical error correction

Question 1: Taking a majority vote requires reading the bits: what if this is also inaccurate.

Von Neumann: "*Probabilistic logics and the synthesis of reliable organisms from unreliable components*" (1956):
recursively apply construction (``concatenation").
Below a value of the error probability ("threshold"),
logical error probability [$p_{i+1} = f(p_i) = O(p_i^2)$]
flows to 0.

Computation O with 4 input bits and 2 output bits, copied three times (O^1, O^2, O^3).
m is a majority function.

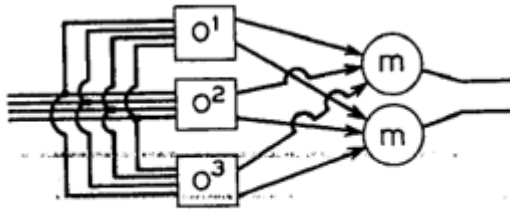


FIGURE 26

Question 2: What if we use this code for quantum information, i.e.

$$|\psi\rangle = \alpha|0\rangle + \beta|\,\rangle \rightarrow |\overline{\psi}\rangle = \alpha|000\rangle + \beta|111\rangle.$$

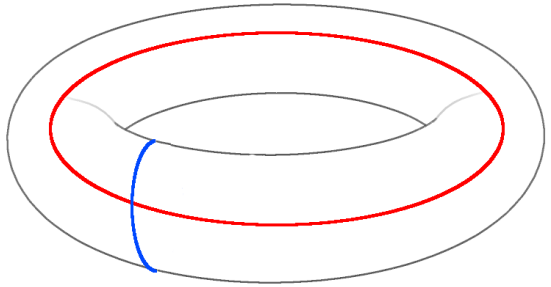
How do we then take a majority vote: measuring disturbs the quantum information.

Why not just measure M1: whether first two bits are the same, or not, but *not what they are*,
M2: whether last two bits are the same, or not, but *not what they are*.
Two bits of info, pointing uniquely to no error (I), error on qubit 1 (X_1), error on qubit 2 (X_2), error on qubit 3 (X_3).
Mathematically, using Pauli Z acting as $Z|0\rangle = |0\rangle, Z|1\rangle = -|1\rangle$, measurement M1 is determining the eigenvalue of $Z_1 Z_2$.

Kitaev: local check code

In Proc. of 3rd Int. Conf. on Quantum Comm. & Meas, Sept. 1996.

``…The most dangerous is the first step, the measurement. First of all, a single error in the syndrome can make it impossible to determine the error in the qubits. What is even worse, one error during a measurement can spoil all the qubits involved in this measurement. That is why local check codes are especially useful for fault-tolerant error correction. For a local check code, all the measurements can be organized into a quantum circuit of bounded depth…"



Introduced the toric code

Logical Z_L operators of the 2 logical qubits are the two nontrivial loops around the torus. The finer the tiling, the higher the distance.

Later: Bravyi/Kitaev & Freedman/Meyer (1998): lattice with a boundary → surface code

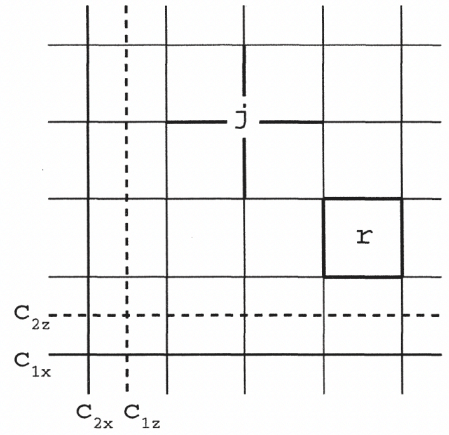
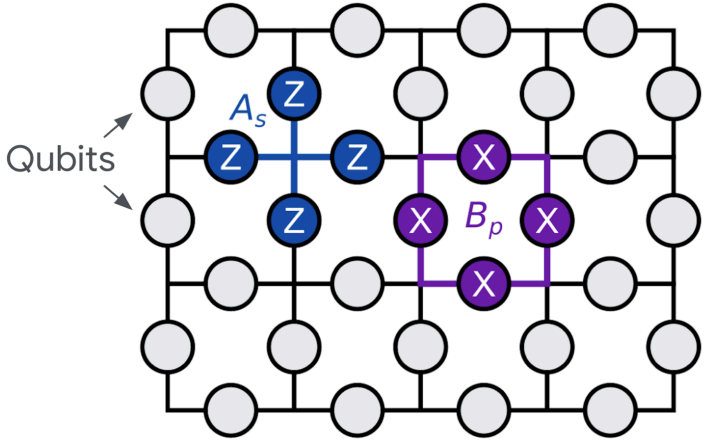


Figure 1. The toric code TOR(5).

Qubits on the edges of a lattice, tiling a torus.

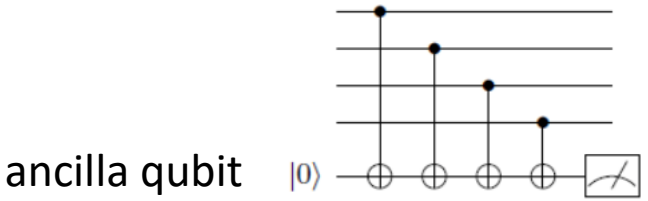
In code space, parity checks A_s, B_p for all vertices s and faces p, have eigenvalue 1 (all parity checks commute).

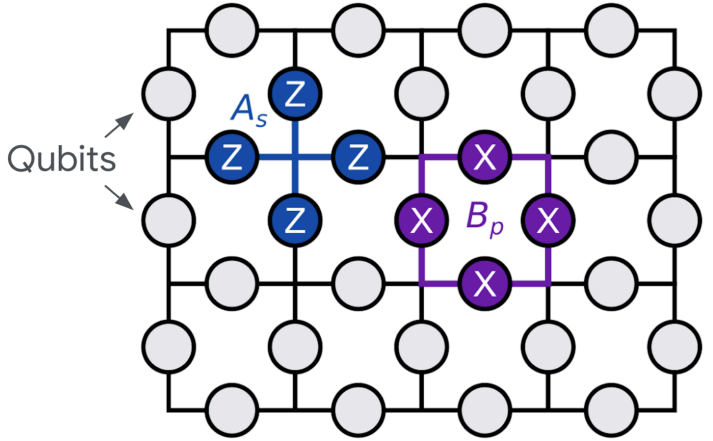


Kitaev: local check code

``…For a local check code, all the measurements can be organized into a quantum circuit of bounded depth…"

Here is such a circuit measuring some $A_s = ZZZZ$ using an extra "measure" or "ancilla" qubit:





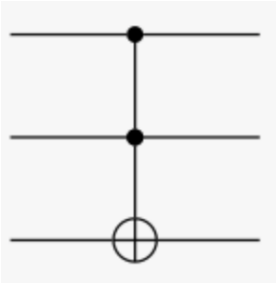
Ancilla qubits can be placed locally nearby on 2D lattice.

Gates and measurement in the circuit are subject to errors at experimental rates ($0.01\% - 5\,\%$).

In the same paper, Kitaev also introduced symplectic codes (stabilizer codes), and suggested using a `cascaded' (concatenated) toric code to reduce the logical error rate to arbitrary low-levels (fault-tolerant quantum memory) given that physical error probabilities are sufficiently low, below threshold.

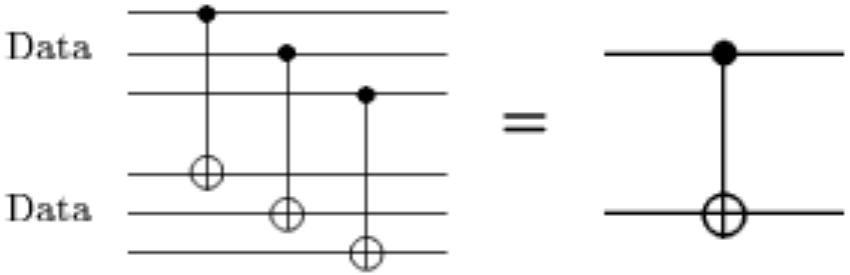
One more key idea: how to compute

Shor (``Fault-tolerant quantum computation", FOCS 1996) showed how to do universal logical computation (no concatenation).
For this he needed to show how to do a Toffoli gate fault-tolerantly!



Toffoli or CCX gate

Not all logical gates needed for quantum computation can be done transversally.



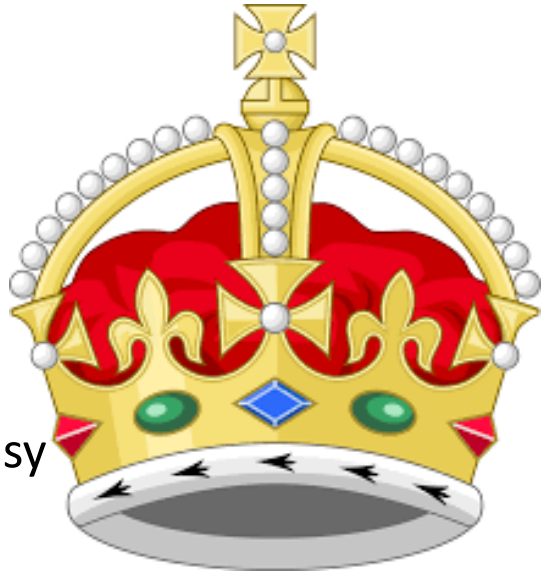
Transversal CNOT on
2 logical qubits each
represented by 3 physical
qubits.

Transversal is nice: fast and with little noise spread (fault-tolerant).

Fault-tolerant threshold theorem

After Shor in FOCS 1996

Knill/Laflamme/Zurek, Aharonov/Ben-Or & Kitaev (1996-1997) proved the fault-tolerant threshold theorem for quantum computation using code concatenation*.



*don't try proving this on a spare afternoon.

Theorem says: to simulate an (almost) perfect quantum circuit of size N, one can use a noisy quantum circuit of size $N \times \mathrm{poly}(\log N)$, if the noise is sufficiently weak and local (Aliferis, Gottesman, Preskill, 2005).

- uses frequent mid-circuit measurements (learning about errors, removal of entropy).
- assuming fast classical processing of error information (no backlog).
- assuming one can reduce leakage and loss errors to qubit errors.

Favourite surface code architecture: noise has to be below a threshold of $0.75\,\%$ per elementary operation.

Google AI & Collaborators (Nature 2024): first team below surface code threshold for a quantum memory

Jumping over 28 years of history….

…during which Dennis, Kitaev, Landahl & Preskill (2001) studied many details of the favourable toric code, and
…Raussendorf, Harrington & Goyal (RHG, 2005) showed how to a CNOT in the 2D surface code using hole moving

…Bravyi and Kitaev (2004) introduced magic state distillation

…Bombin and Delgado (2006) introduced color codes

…Fowler popularised the surface code architecture with Mariantoni, Martinis and Cleland (2012) as a concrete scheme to pursue, and
…Horsman et al. (2012) presented lattice surgery

…and we kept dreaming and thinking about how to engineer quantum error correction

…and many, many more people contributed…

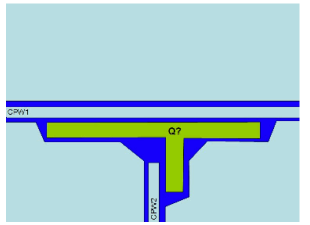


Fig. 9. A concept for a basic structure with one qubit coupled to two resonators. Dark blue is bare dielectric substrate, light blue is metal film constituting a "tee" structure of two coplanar waveguides (CPW), and green is a qubit of unspecified character (transmon, phase, flux, or other qubits could be made the embody the implied couplings). Many other elements (flux bias lines, measuring transmission lines) are not shown but could be made in a planar fashion.

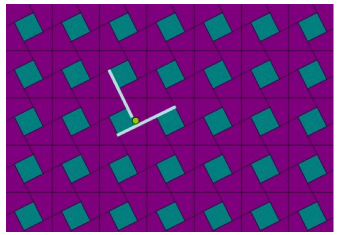


Fig. 10. A skew-square tiling on which the T structure of Fig. 9 could be repetitively placed to obtain a lattice that would be suitable for surface-code quantum computing.

DiVincenzo (2009): ``Fault tolerant architectures for superconducting qubits

Back to 1995

Workshop at ISI in Torino in 1995
(first installment in 1994)

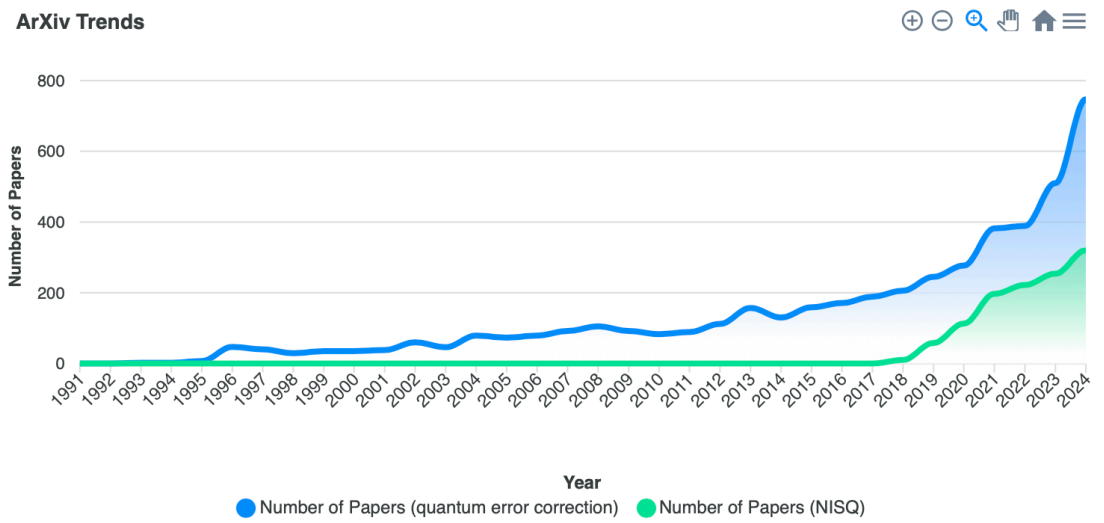
A lot of people thinking about
quantum error correction,
so I better think about something else*.

*Something else: Ising spin glasses and whether one determine ground-state energy via using annealing with a transverse field (“quantum annealing”).

Currently, quantum error correction fast growing subfield due to both experimental and theoretical progress (20% of the field?)

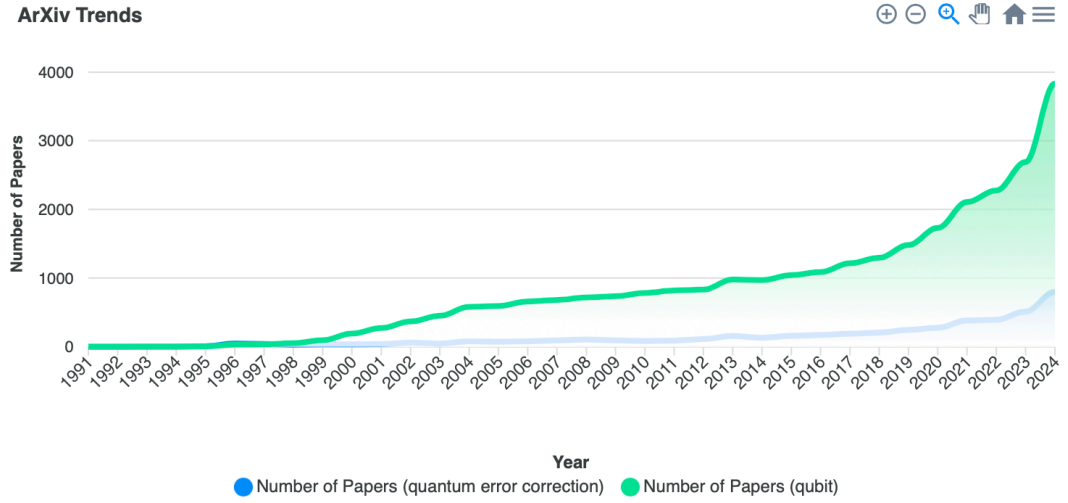
arXiv trends: discover research patterns by searching for keywords' presence in arXiv papers over time.

quantum error correction | Search | NISQ | Compare



arXiv trends: discover research patterns by searching for keywords' presence in arXiv papers over time.

quantum error correction | Search | qubit | Compare



Comments: overhead & challenges

- Right code architecture (use of concatenation, use of quantum LDPC codes which encode many logical qubits, use of biased noise/bosonic qubits) is an open question: it depends on qubit platform and noise characteristics. E.g. modular architectures (beyond 1000 or 10.000 qubits) may require use of slower or noisier components between modules.

- Qubit mobility and beyond nearest-neighbour qubit connectivity on chip can allow for more logical gates to be done transversally and/or more efficient LDPC (low density parity check) encodings (IBM group 2024/2025).

- Clock-speed of logical quantum processor is set by duration of QEC cycle (affected by measurement and/or moving time), but also by transversal or slower non-transversal constructions.

Gidney (Google AI) 2025: factoring a RSA 2048 bit number in less than a week using 1 million physical qubits, using surface codes concatenated with an error detection code (down from 20 million!).

Estimates: need at least $10^4 - 10^6$ physical qubits for a quantum advantage, leading to $10^2 - 10^3$ logical qubits using quantum error correction.

Quantum error correction
has moved from theory to experiment
and will become the digital foundation of
quantum information processing