Quantum error correction (QEC)

Mermin: Miracle of quantum error correction

Surprise, since the only way to detect errors is to make a measurement, while we are not allowed to learn information about qubit state

QEC: 1995 Peter Shor, independently Andrew Steane

QEC is necessary in a QC (makes QC less impossible), otherwise the whole computation should be within decoherence time, that is hard for long algorithms.

Classical computer: arbitrary long algorithms are OK using error correction.

Classical error correction

Simplest error correction: 3-bit repetitive code (think about memory)

Encoding $0 \to 000$
$1 \to 111$

Errors: bit flips

Decoding: all bits measured, majority, then encoding again (if need to maintain)

General approach to classical error correction:
1) detection of errors via error syndromes
2) correction: flip the wrong (flipped) bits

In 3-bit repetitive code, error syndrome is given by: parity of bits 1&2 and 2&3
(parity is sum modulo 2)

4 possible results: OK, flip bit 1, flip bit 2, flip bit 3

Protects against 1 bit flip

Probability of error: $p \to 3p^2(1-p) + p^3$ Works well if $p \ll 1$
Threshold: $p = 1/2$ (always helps)

Concatenation (layering): arbitrary small probability of error is possible

5-bit repetitive code protects against 2 errors, etc.

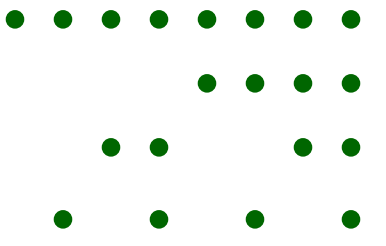
Classical error correction (cont.)

There are smarter ways for encoding (less redundancy needed), but the general idea is the same: use redundancy and parity checks

Error is evidenced by particular combination of wrong parity checks (error syndrome), then can be corrected. Usually works well for low probability of error p, though possible even for $p \to 1/2$.

(Simplified) idea of Hamming code

$b_0 b_1 b_2 b_3 b_4 b_5 b_6 b_7$



$$b_0 \oplus b_1 \oplus b_2 \oplus b_3 \oplus b_4 \oplus b_5 \oplus b_6 \oplus b_7 = c_0$$

$$b_4 \oplus b_5 \oplus b_6 \oplus b_7 = c_1$$

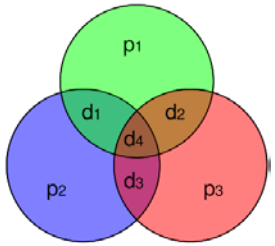
$$b_2 \oplus b_3 \oplus b_6 \oplus b_7 = c_2$$

$$b_1 \oplus b_3 \oplus b_5 \oplus b_7 = c_3$$

Using parity check bits $c_0 c_1 c_2 c_3$, we can easily find location (and therefore correct) one error in the bit string $b_0 b_1 b_2 b_3 b_4 b_5 b_6 b_7$

(in reality a little different, parity check bits are within the bit string, which correspondingly has less data bits)

Only logarithmic overhead



Quantum vs classical error correction

- Quantum error correction is really necessary (classical computer can work without error correction, usually used for memory and communication; for nanoscale computers can be needed for logic as well)
- Only indirect checking for errors is allowed (correcting without decoding!)
- Bit flip is not the only type of errors (also phase flips (*Z*) and bit-phase flips (*Y*))
- Errors grow continuously, not really flips. Two ways to think:

  1) gradual stochastic change of $|\psi\rangle$ (not quite correct, but OK)

  2) gradual entanglement with environment

We will first discuss idea of indirect checking for errors,
then discuss a code protecting from 3 types of errors (X, Y, Z),
and then discuss why this is sufficient for continuous errors

Idea of indirect checking for errors

3-qubit code, protecting from one bit flip

We cannot clone, but still can do encoding:

$$\alpha|0\rangle + \beta|1\rangle \;\rightarrow\; \alpha|000\rangle + \beta|111\rangle$$

(somewhat similar to repetitive code)

(operation $(\alpha|0\rangle + \beta|1\rangle)|00\rangle \rightarrow \alpha|000\rangle + \beta|111\rangle$ is unitary)

Idea: measurement of parities (sum modulo 2) without measurement of qubits

In this way we do not learn anything about α and β

Correction is also without decoding: just flip the flipped qubit

We need to measure operators Z_1Z_0 and Z_2Z_1 (numbering $q_2q_1q_0$)

Any Hermitian operator corresponds to an observable, with measurement results being the eigenvalues of this operator.

Operators Z_1Z_0 and Z_2Z_1 are Hermitian (since Z is Hermitian)

Consider Z_1Z_0: $(Z_1Z_0)^2 = \hat{1}$, so the eigenvalues are ± 1.

$+1$: even parity, the same qubit states (either $|00\rangle$ or $|11\rangle$ or their superposition)

-1: odd parity, different qubit states (superposition of $|01\rangle$ and $|10\rangle$)

The same for the operator Z_2Z_1

3-qubit code

The operation is similar to the classical 3-bit repetitive code

$|\psi\rangle = \alpha|000\rangle + \beta|111\rangle$ correct (uncorrupted) state (codeword)

After flip of qubit 0 it becomes $X_0|\psi\rangle = \alpha|001\rangle + \beta|110\rangle$

Similarly, $X_1|\psi\rangle = \alpha|010\rangle + \beta|101\rangle$, $X_2|\psi\rangle = \alpha|100\rangle + \beta|011\rangle$

	X_0	X_1	X_2	$\hat{1}$
Z_2Z_1	+	−	−	+
Z_1Z_0	−	−	+	+

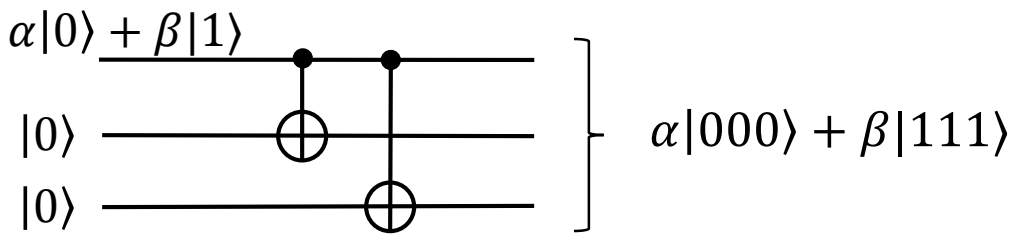
"+" means parity 0 (even)

"−" means parity 1 (odd)

From these results (error syndrome) we know if one qubit flipped or not, and which one flipped. Then we can correct by flipping that qubit back.

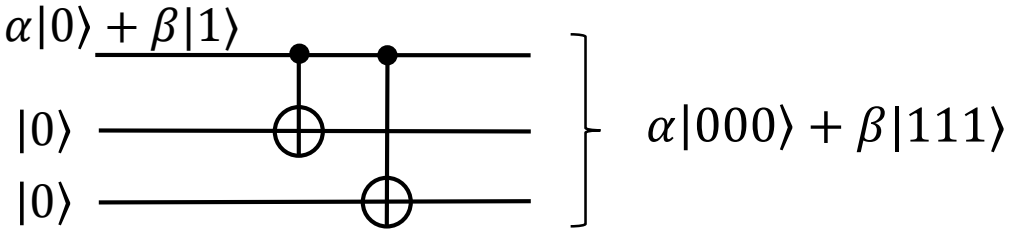
Now circuits

Encoding

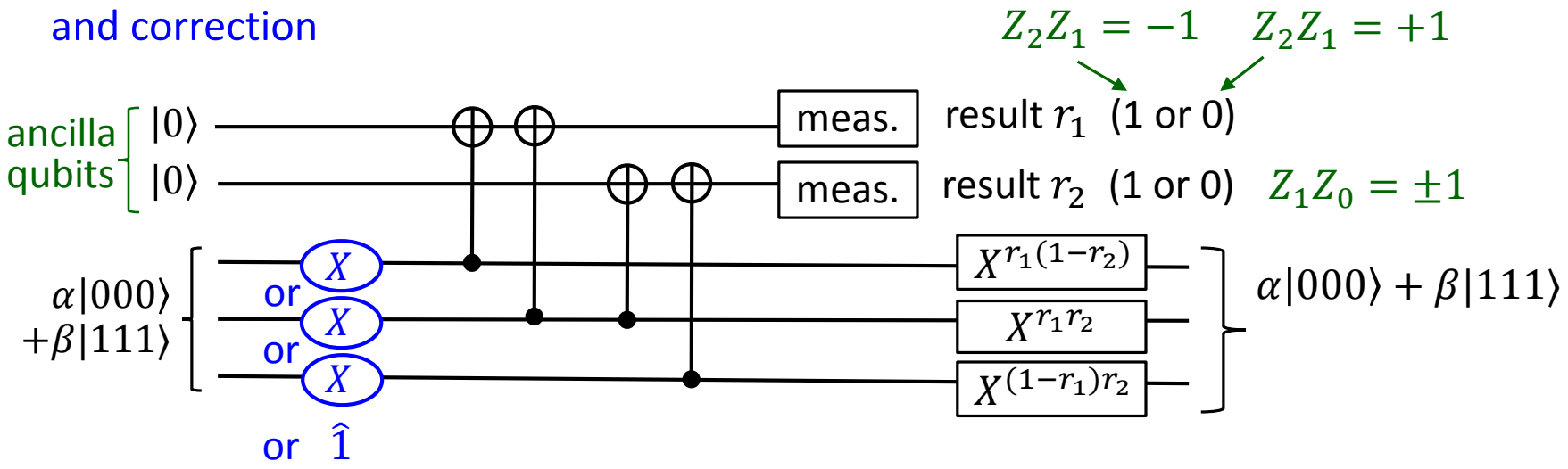


3-qubit code (cont.)

Encoding



Error detection and correction

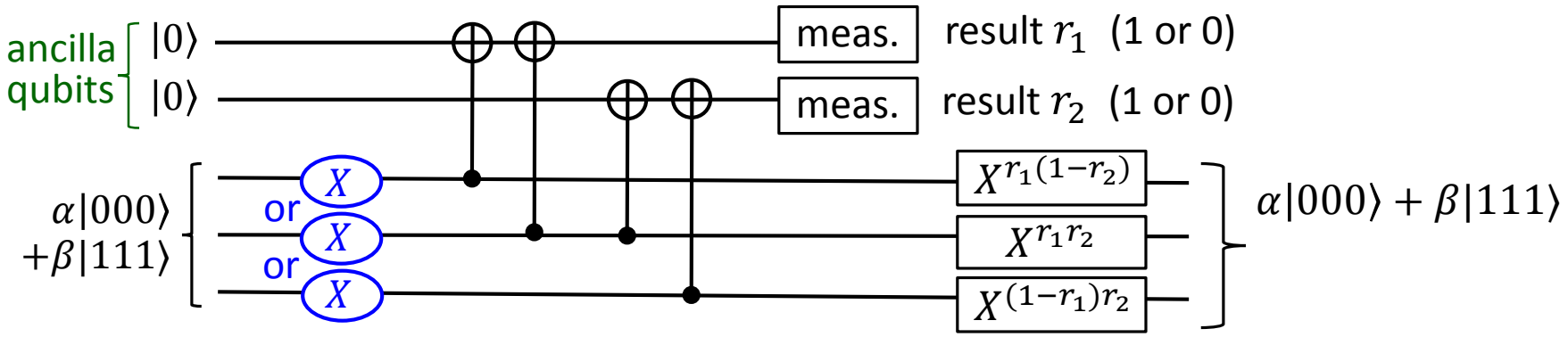


Check that works properly: error in upper qubit ⇒ upper ancilla 1 ⇒ upper qubit corrected
error in middle qubit ⇒ both ancillas 1 ⇒ middle qubit corrected
error in lower qubit ⇒ lower ancillas 1 ⇒ lower qubit corrected, no error ⇒ no correction

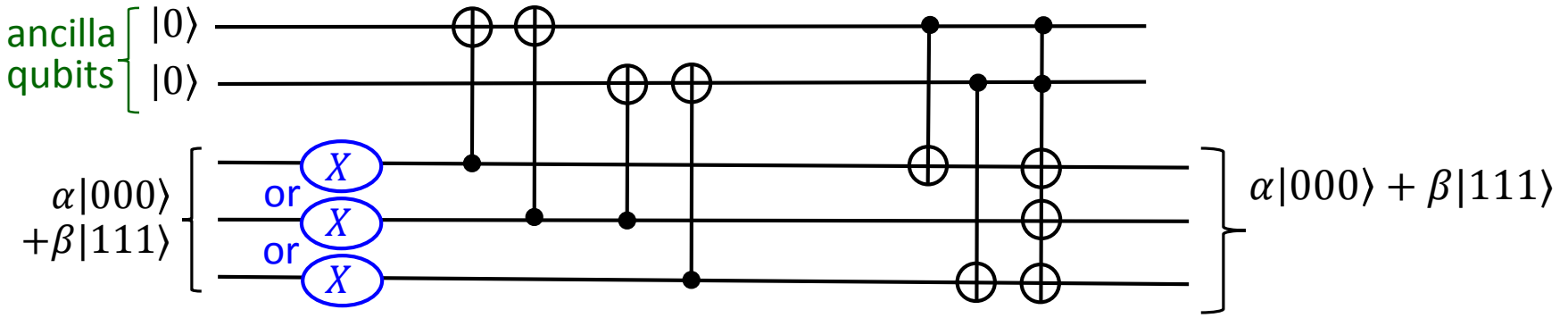
The same operation if entangled with other qubits: $\alpha|000\rangle|\phi_0\rangle + \beta|111\rangle|\phi_1\rangle$

3-qubit code: automated version

Standard procedure



Automated version: replace measurement with controlled operation



Check: if 00, then nothing, if 11, then middle qubit corrected,
if 01 or 10, then only one CNOT works, again OK

To reuse ancillas, we usually need to measure them (then the automated version is not quite useful); however, it is possible to rely on dissipation to “dump entropy”

QEC for continuous errors

A hint why QEC works for continuous errors (not a rigorous analysis)

Suppose the middle qubit does not flip, but rotates about X-axis

$$\alpha|000\rangle + \beta|111\rangle \rightarrow \cos\frac{\theta}{2}\,(\alpha|000\rangle + \beta|111\rangle) - i\sin\frac{\theta}{2}(\alpha|010\rangle + \beta|101\rangle)$$

When we measure parity (say, qubits 1 and 2), the system should "make a decision", then the state is either collapsed to the correct state (then no error syndrome) or it choses the second term (then error syndrome 11), which we will correct.

Measurement transforms continuous errors into discrete errors (flips)

QEC should protect against rotations about any axis. As we will see later, for that it is sufficient to protect against X, Y, and Z flips.

Analysis of space dimensions for QEC

3-qubit code

Valid (uncorrupted) codewords live in a 2D subspace of 8D Hilbert space
(here we discuss dimensions in complex spaces, not number of real parameters)

After corruption due to X_0, the state moves to a different (orthogonal) 2D subspace

Similarly the state moves to different subspaces after corruption due to X_1 and X_2

So, there will be 4 orthogonal 2D subspaces (correct and 3 with errors), which all fit well into 8D Hilbert space. This is why we can distinguish errors and correct them.

In general, an n-qubit code, protecting against single-qubit bit-flips requires

$$2^n \geq \underbrace{2(1+n)}_{(1+n)\text{ 2D subspaces for } n \text{ possible errors}}$$

Hilbert space

This is why $n \geq 3$ is needed for bit-flips

For general errors (3 kinds, will consider later)

$$2^n \geq 2(1+3n) \qquad \text{Therefore, } n \geq 5$$

Such 5-qubit code really exists (will consider later)

3-qubit code protecting from one phase flip (Z)

For bit-flip it was $|0\rangle_L \to |000\rangle$, $|1\rangle_L \to |111\rangle$, so that $\alpha|0\rangle_L + \beta|1\rangle_L \to \alpha|000\rangle + \beta|111\rangle$

logical

Now similar:

logical

$$|0\rangle_L \to \frac{1}{\sqrt{8}}(|0\rangle + |1\rangle)(|0\rangle + |1\rangle)\,(|0\rangle + |1\rangle)$$

$$|1\rangle_L \to \frac{1}{\sqrt{8}}(|0\rangle - 1\rangle)(|0\rangle - |1\rangle)\,(|0\rangle - |1\rangle)$$

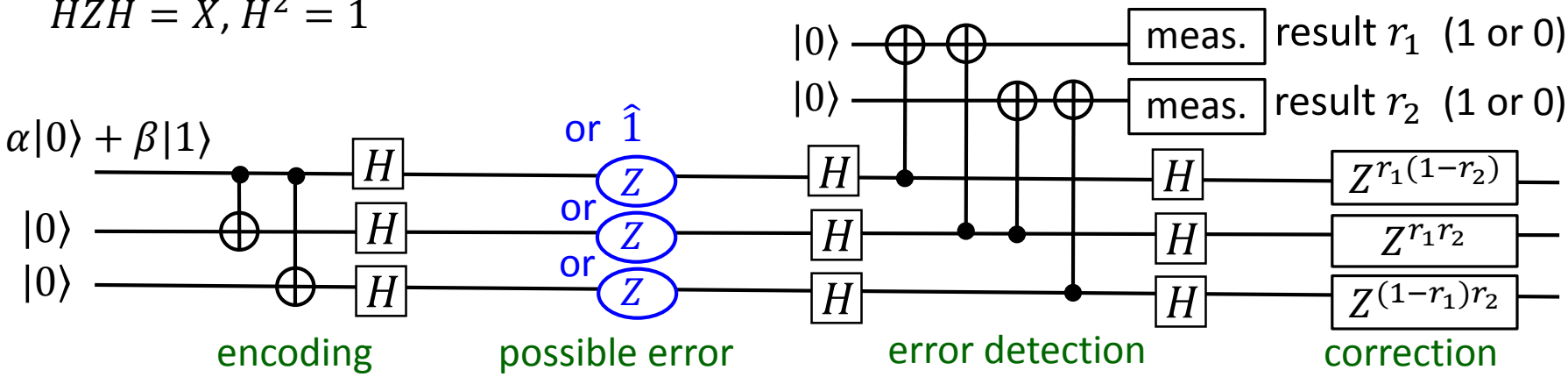
3 physical qubits

$$\alpha|0\rangle_L + \beta|1\rangle_L \to \frac{1}{\sqrt{8}}[\alpha\,(|0\rangle + |1\rangle)^{\otimes 3} + \beta(|0\rangle - |1\rangle)^{\otimes 3}]$$

If one qubit flips the phase, $(|0\rangle + |1\rangle) \leftrightarrow (|0\rangle - |1\rangle)$, it is possible to find which one, and then correct it back (by applying Z-gate)

Equivalent to fit-flip code,
$HZH = X$, $H^2 = \hat{1}$

To detect a Z-error, we need to measure X_1X_0 and X_2X_1



9-qubit Shor's code

Is it possible to protect from bit flips (X), phase flips (Z), and bit&phase flips (Y) at the same time?

Yes! 9-qubit Shor's code protects from one of such errors in any qubit

Idea: just concatenation of two previous codes (layering of codes)

$$|0\rangle_L \to \frac{1}{\sqrt{8}}(|000\rangle + |111\rangle)(|000\rangle + |111\rangle)\,(|000\rangle + |111\rangle)$$

$$|1\rangle_L \to \frac{1}{\sqrt{8}}(|000\rangle - |111\rangle)(|000\rangle - |111\rangle)\,(|000\rangle - |111\rangle)$$

One encoding deals with X-errors, the other one with Z-errors, while Y-errors are taken care of automatically, since $Y = -iZX$

In error correction, usually $Y \equiv ZX$ (e.g., Mermin's book)

If a qubit suffers from bit flip (X), then this changes parities within 3-qubit block

$$(|010\rangle + |101\rangle)(|000\rangle + |111\rangle)\,(|000\rangle + |111\rangle)/\sqrt{8}$$

$$(|010\rangle - |101\rangle)(|000\rangle - |111\rangle)\,(|000\rangle - |111\rangle)/\sqrt{8}$$

If a phase-flip of a qubit (Z), then changes sign ($+ \leftrightarrow -$) in the block

$$(|000\rangle - |111\rangle)(|000\rangle + |111\rangle)\,(|000\rangle + |111\rangle)/\sqrt{8}$$

$$(|000\rangle + |111\rangle)(|000\rangle - |111\rangle)\,(|000\rangle - |111\rangle)/\sqrt{8}$$

If Y-flip, then both

9-qubit Shor's code (cont.)

Encoding

$$\alpha|0\rangle_L + \beta|1\rangle_L \rightarrow \alpha\,(|000\rangle + |111\rangle)(|000\rangle + |111\rangle)\,(|000\rangle + |111\rangle)/\sqrt{8}$$
$$+\beta\,(|000\rangle - |111\rangle)(|000\rangle - |111\rangle)\,(|000\rangle - |111\rangle)/\sqrt{8}$$

Error detection and correction

1) Measure parities with 3-qubit blocks: $Z_0Z_1, Z_1Z_2,\ \ Z_3Z_4, Z_4Z_5,\ \ Z_6Z_7, Z_7Z_8$

If X-error is detected in ith qubit, correct by gate X_i

(if bit-flips in different 3-qubit blocks, they all can be corrected)

2) Measure parities of phases of 3-qubit blocks: $X_0X_1X_2X_3X_4X_5,\ X_3X_4X_5X_6X_7X_8$

($X_0X_1X_2$ changes sign of wavefunction if $000 - 111$ and does nothing if $000 + 111$, so these products compare signs)

If Z-error is detected in jth 3-qubit block, correct by gate Z applied to <u>any</u> qubit in this block

In Mermin's book a little different procedure: first detect errors, then correct.
Equivalent because step 2) is insensitive to bit flips:

For example, $X_0X_1X_2(|001\rangle - |110\rangle) = |110\rangle - |001\rangle = -(|001\rangle - |110\rangle)$

Shor's code: is it optimal?

$$\alpha|0\rangle_L + \beta|1\rangle_L \rightarrow \alpha\,(|000\rangle + |111\rangle)(|000\rangle + |111\rangle)\,(|000\rangle + |111\rangle)/\sqrt{8}$$
$$+\beta\,(|000\rangle - |111\rangle)(|000\rangle - |111\rangle)\,(|000\rangle - |111\rangle)/\sqrt{8}$$

8 measured operators: $Z_0Z_1, Z_1Z_2,\ \ Z_3Z_4, Z_4Z_5,\ \ Z_6Z_7, Z_7Z_8$

$X_0X_1X_2X_3X_4X_5,\ X_3X_4X_5X_6X_7X_8$

Therefore, $2^8 = 256$ possible results

Also, 9-qubit Hilbert space (512 dimensions) can hold 256 copies of a qubit space

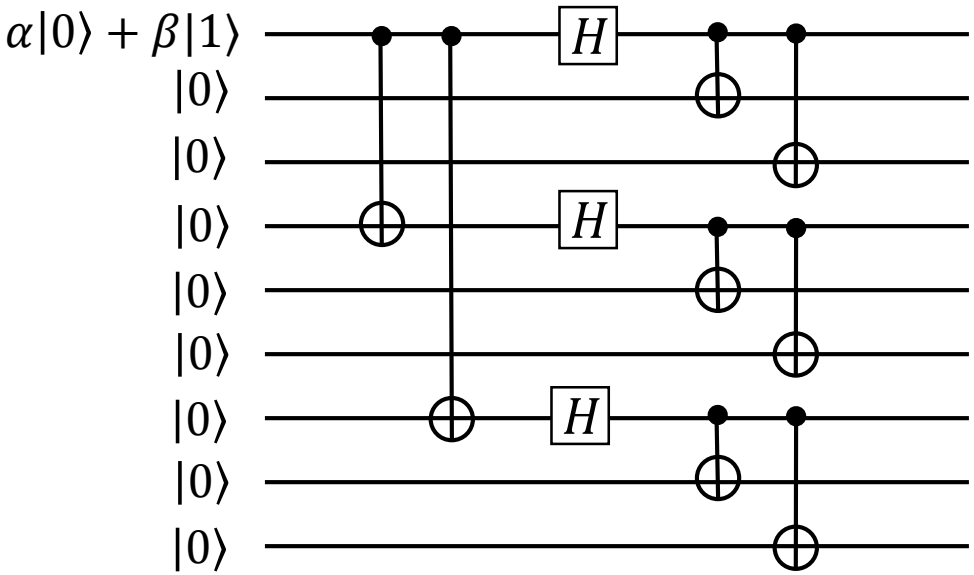
However, we need only $1 + 3 \times 9 = 28$ distinguishable results

(even less: $28 - 6 = 22$, because Z-errors may lead to the same result)
(degenerate quantum code)

$\Rightarrow$ 9-qubit Shor's code is not optimal

Shor's code: encoding

$$\alpha|0\rangle_L + \beta|1\rangle_L \rightarrow \alpha\,(|000\rangle + |111\rangle)(|000\rangle + |111\rangle)\,(|000\rangle + |111\rangle)/\sqrt{8}$$
$$+\beta\,(|000\rangle - |111\rangle)(|000\rangle - |111\rangle)\,(|000\rangle - |111\rangle)/\sqrt{8}$$



$$|0\rangle_L \rightarrow |000000000\rangle \rightarrow \frac{0+1}{\sqrt{2}}00\frac{0+1}{\sqrt{2}}00\frac{0+1}{\sqrt{2}}00 \rightarrow \frac{000+111}{\sqrt{2}}\frac{000+111}{\sqrt{2}}\frac{000+111}{\sqrt{2}}$$

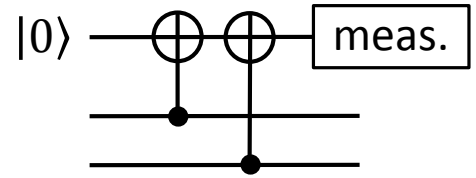
$$|1\rangle_L \rightarrow |100100100\rangle \rightarrow \frac{0-1}{\sqrt{2}}00\frac{0-1}{\sqrt{2}}00\frac{0-1}{\sqrt{2}}00 \rightarrow \frac{000-111}{\sqrt{2}}\frac{000-111}{\sqrt{2}}\frac{000-111}{\sqrt{2}}$$

Shor's code: syndrome extraction

8 measured operators: $Z_0Z_1, Z_1Z_2,\ \ Z_3Z_4, Z_4Z_5,\ \ Z_6Z_7, Z_7Z_8$

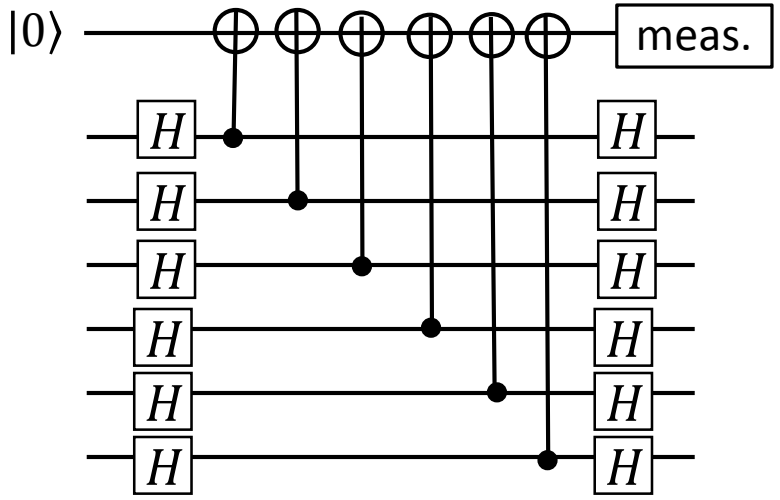
$X_0X_1X_2X_3X_4X_5,\ X_3X_4X_5X_6X_7X_8$

Z_0Z_1: as discussed before



Similarly for other Z_iZ_j (need 6 ancilla qubits for 6 operators Z_iZ_j)

realization of $X_0X_1X_2X_3X_4X_5$:



as always, operator eigenvalue $+1$ corresponds to measurement result 0, eigenvalue -1 corresponds to result 1

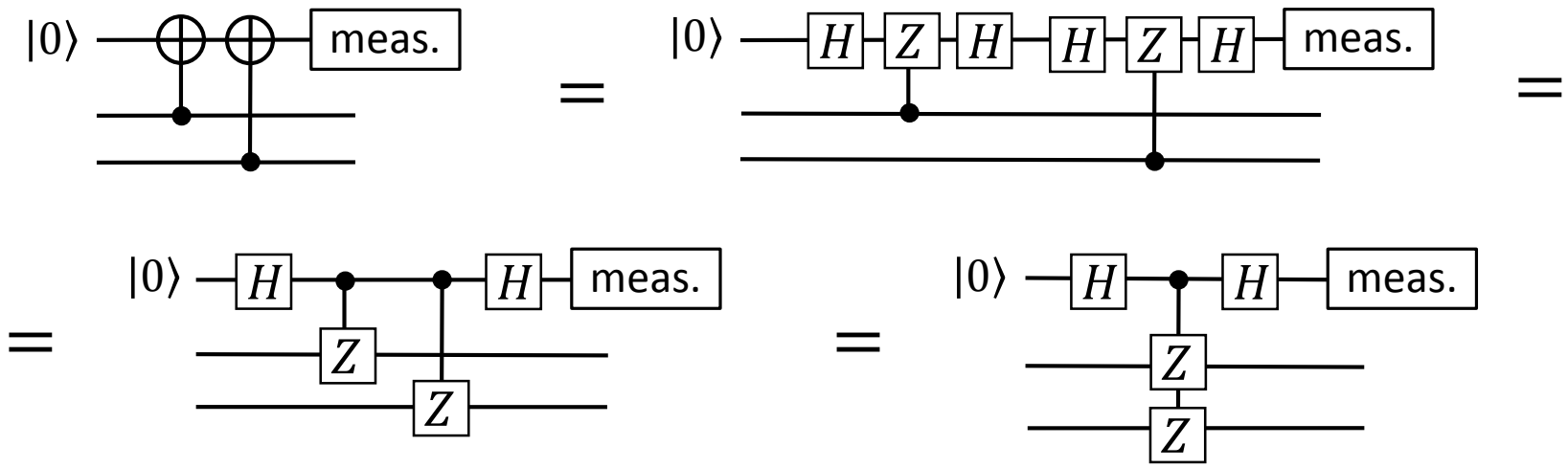
Easier to think that qubits are either $(|0\rangle + |1\rangle)/\sqrt{2}$ or $(|0\rangle - |1\rangle)/\sqrt{2}$ (i.e., eigenstates of X)

Overall need $6 + 2 = 8$ ancillas

Syndrome extraction: a different way

There is a different but equivalent way of measuring syndromes

Z_0Z_1

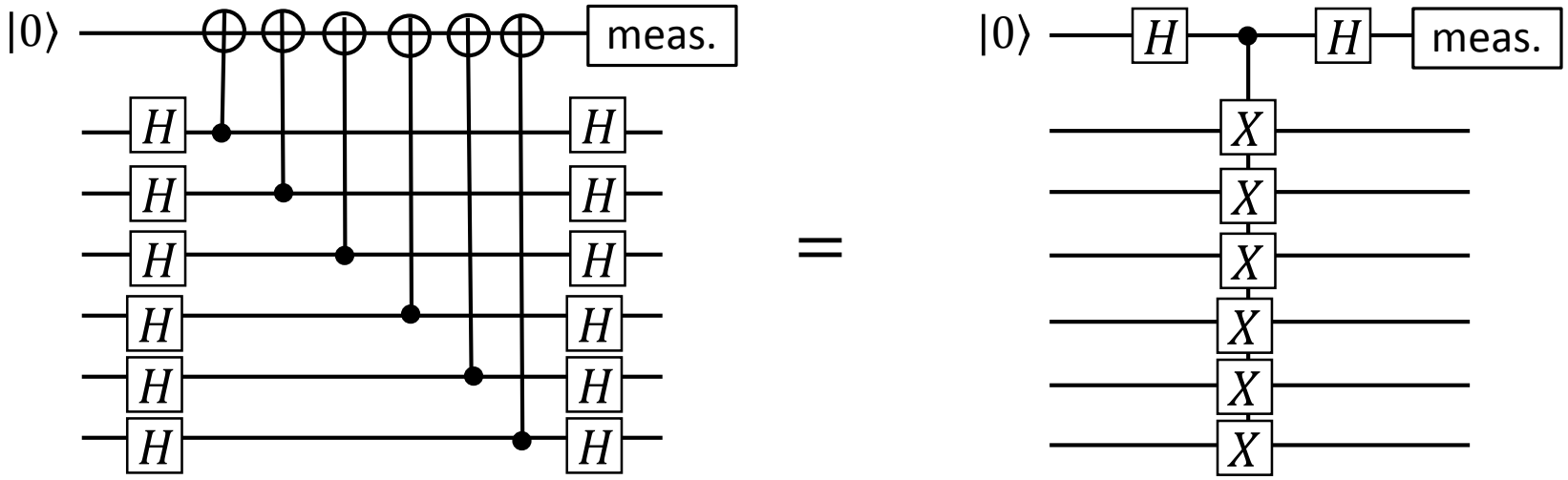


just a change of notation

In this way it is clear which operator is measured

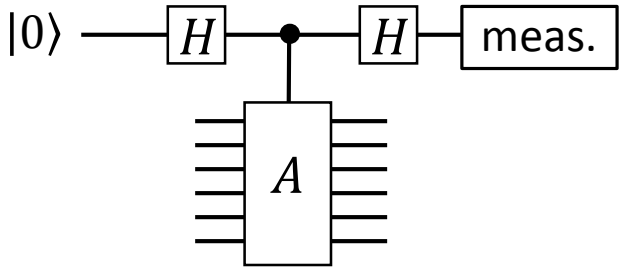
Syndrome extraction: general way

Similarly, for $X_0X_1X_2X_3X_4X_5$:



This is a general way, showing directly which operator we measure

If a multi-qubit operator A has eigenvalues ± 1, then it can always be measured as

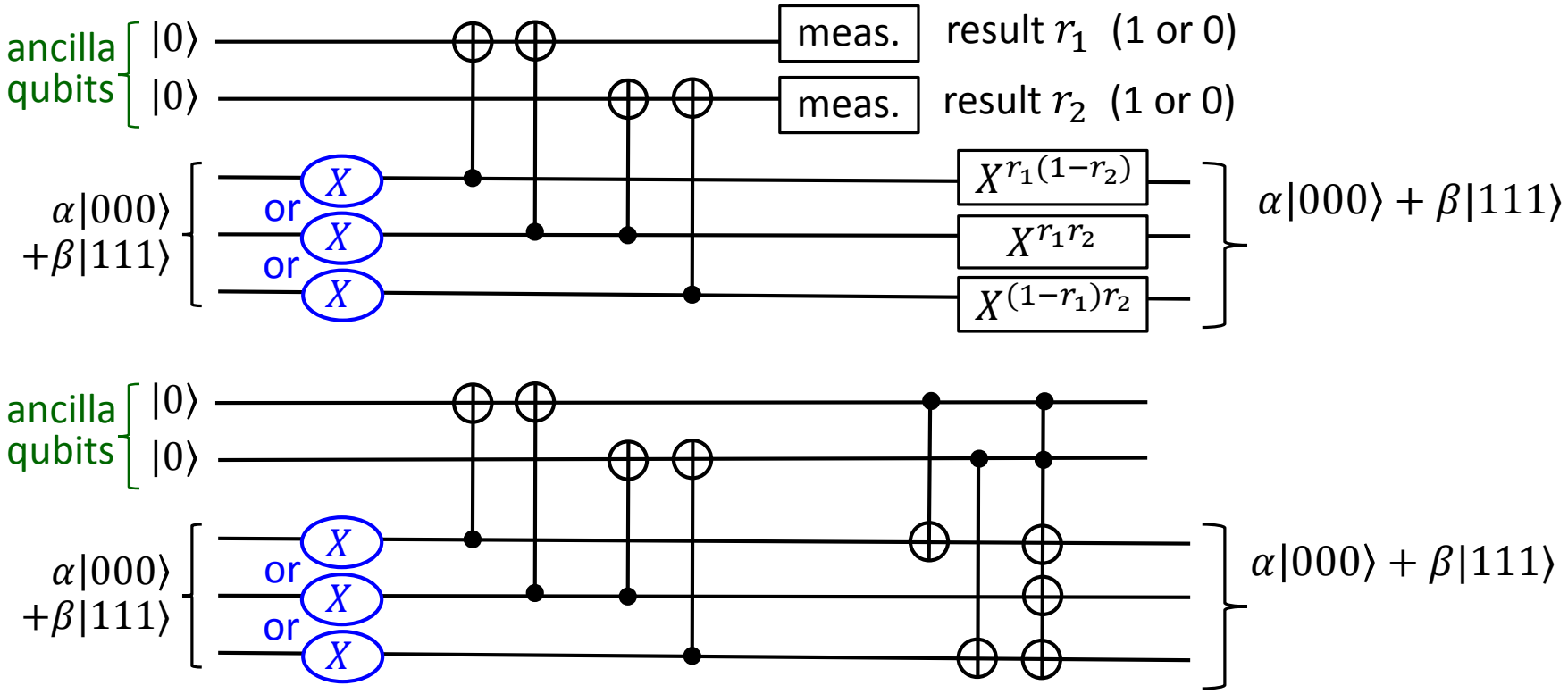


$$\rightarrow \quad |0\rangle \rightarrow \frac{|0\rangle + |1\rangle}{\sqrt{2}} \rightarrow \begin{cases} \frac{|0\rangle+|1\rangle}{\sqrt{2}} & \text{if eigenvalue of } A \text{ is } +1 \\ \frac{|0\rangle-|1\rangle}{\sqrt{2}} & \text{if eigenvalue of } A \text{ is } -1 \end{cases} \rightarrow \begin{cases} |0\rangle \\ |1\rangle \end{cases}$$

Automated version of quantum error correction

Conditional gates can always be replaced by controlled gates
(then no measurement is needed)

Previous example (for 3-qubit code)



Obviously the same if we measure ancilla qubits. However, no need to measure, then coherent superposition of scenarios, but correction works for each term (unentangled with ancilla qubits). Anyway, need to dump entropy (possibly resetting by switching on/off energy dissipation).

Error generation

Why protecting from only 3 errors (X, Y, Z) is sufficient?

We discussed a hint: for a small unwanted unitary evolution, measurement converts small continuous errors into rare big errors (X, Y, Z), otherwise restores initial state.

Now more general discussion based on interaction and entanglement with environment

1 qubit $|e\rangle|0\rangle \rightarrow |e_0\rangle|0\rangle + |e_1\rangle|1\rangle$

$|e\rangle|1\rangle \rightarrow |e_2\rangle|0\rangle + |e_3\rangle|1\rangle$

$|e_0\rangle \approx |e_3\rangle,\ \|e_{0,3}\| \approx 1,\ \|e_{1,2}\| \ll 1$

unitary interaction with environment

$|e\rangle$ is initial state of environment

$|e_i\rangle$ are not normalized (sums are normalized)

gradual process, $|e_1\rangle$ and $|e_2\rangle$ grow gradually

Then from linearity

$$|e\rangle|\psi\rangle \rightarrow (|e_0\rangle\,\hat{1} + |e_1\rangle\,X)\,\underbrace{|0\rangle\langle 0|}_{\frac{1+Z}{2}=\begin{pmatrix}1&0\\0&0\end{pmatrix}}\,|\psi\rangle + (|e_2\rangle\,X + |e_3\rangle\,\hat{1})\,\underbrace{|1\rangle\langle 1|}_{\frac{1-Z}{2}=\begin{pmatrix}0&0\\0&1\end{pmatrix}}\,|\psi\rangle =$$

projector operators

$$= \underbrace{\frac{|e_0\rangle + |e_3\rangle}{2}}_{\text{denote } |d\rangle}\,\hat{1}\,|\psi\rangle + \underbrace{\frac{|e_1\rangle + |e_2\rangle}{2}}_{|a\rangle \text{ (small)}}\,X|\psi\rangle + \underbrace{\frac{|e_0\rangle - |e_3\rangle}{2}}_{|b\rangle \text{ (small)}}\,Z|\psi\rangle + \underbrace{\frac{|e_1\rangle - |e_2\rangle}{2}}_{|c\rangle \text{ (small)}}\,XZ|\psi\rangle$$

Error generation (cont.)

1 qubit $|e\rangle|0\rangle \rightarrow |e_0\rangle|0\rangle + |e_1\rangle|1\rangle$ $|e\rangle|1\rangle \rightarrow |e_2\rangle|0\rangle + |e_3\rangle|1\rangle$

Then

$$|e\rangle|\psi\rangle \rightarrow (|d\rangle\,\hat{1} + |a\rangle\,X + |b\rangle\,Y + |c\rangle\,Z)\,|\psi\rangle$$

(here $Y \equiv XZ$ for brevity)

Small $|a\rangle$, $|b\rangle$, $|c\rangle$, while $\| |d\rangle\| \approx 1$,

During quantum error correction procedure, these terms are distinguished $\Rightarrow$ projected $\Rightarrow$ only one term remains $\Rightarrow$ can correct back to $|\psi\rangle$ (we do not care about environment)

(From Schrödinger equation, $|a\rangle$, $|b\rangle$, $|c\rangle$ should grow linearly in time, then probabilities grow as t^2. Then measurement helps even without correction (quantum Zeno effect). Unfortunately, errors usually grow linearly (not quadratically) in time, so need to correct.)

Error generation: several qubits

This idea can be generalized to several qubits

$$|e\rangle|\Psi\rangle_n \rightarrow \sum_{\mu_1=0}^{3}\sum_{\mu_2=0}^{3}\cdots\sum_{\mu_n=1}^{3}|e_{\mu_1\mu_2\ldots\mu_n}\rangle\ U_{\mu_1}^{(1)}U_{\mu_2}^{(2)}\ldots U_{\mu_n}^{(n)}\ |\Psi\rangle_n$$

where $U_0^{(k)}=\hat{1}_k, U_1^{(k)}=X_k,\ U_2^{(k)}=Y_k,\ U_3^{(k)}=Z_k$, acting on kth qubit

This formula is exact. If errors are small and independent for each qubit, then the terms with more than 1 error are small

$$|e\rangle|\Psi\rangle_n \rightarrow \approx \left(|d\rangle\,\hat{1}+\sum_{i=1}^{n}|a_i\rangle\,X_i+|b_i\rangle\,Y_i+|c_i\rangle\,Z_i\right)|\Psi\rangle_n$$

This is why protection against 3 types of one-qubit errors is sufficient.

(Obviously, not always the case. For example, if two qubits couple to the same environment, then errors are correlated. But this is a much harder case, so people usually consider independent errors.)

The next group of terms: two errors (in two qubits), then three errors, etc.

If a code can correct for 2 or more errors, then correlation problem can be solved, and we can also afford to do the procedure less often.

Stabilizer codes

General idea:

Single-qubit errors X_i, Y_i, Z_i move encoded states into different orthogonal subspaces. Making certain measurements, we distinguish these subspaces, and therefore find which error has occurred. Then we correct by applying X_i, Y_i, or Z_i.

Then for a code encoding one logical qubit into n physical qubits and protecting from any one-qubit error, we need

$$2^n \geq 2\,(1+3n) \qquad \Rightarrow\ n \geq 5$$

dimension of Hilbert space

each subspace

# of scenarios

More general, for a code encoding k logical qubits into n physical qubits, and correcting up to t errors, we need

$$2^n \geq 2^k \sum_{j=0}^{t} \binom{n}{j} 3^j$$

Quantum Hamming bound

(Actually, this bound can be violated in degenerate codes, when different errors lead to the same state)

Stabilizer codes are similar to classical linear codes (also Calderbank-Shor-Steane codes)

Stabilizer codes: syndrome measurement

To distinguish subspaces, we measure a set of commuting operators A_i. They are constructed as direct products of Pauli operators, and for each of them $A_i^2 = \hat{1}$; therefore eigenvalues are ± 1.

Examples: Z_0Z_1, Z_1Z_2, $X_0X_1X_2X_3X_4X_5$, etc.

Since A_i are commuting, we can measure them simultaneously or in any sequence. Subspaces corresponding to different measurement results are orthogonal.

Art of design: measured operators (and corresponding subspaces) should be able to diagnose errors in qubits

Measurement of any such operator A projects a state in the Hilbert space into one of two subspaces, corresponding to eigenvalues $\lambda = +1$ and $\lambda = -1$

$\lambda = +1$ (usually measurement result 0) $\leftrightarrow$ projector $\mathrm{P}_0^A = (\hat{1} + A)/2$

$\lambda = -1$ (usually measurement result 1) $\leftrightarrow$ projector $\mathrm{P}_1^A = (\hat{1} - A)/2$

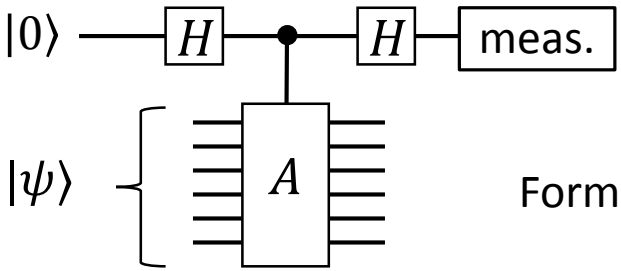
Check: $\left(\mathrm{P}_0^A\right)^2 = \left(\hat{1} + A\right)^2/4 = (\hat{1} + \hat{1} + 2A)/4 = \left(\hat{1} + A\right)/2 = \mathrm{P}_0^A$, similar for P_1^A

If $A|\psi\rangle = +1|\psi\rangle$, then $\frac{\hat{1}+A}{2}\,|\psi\rangle = |\psi\rangle$, while $\frac{\hat{1}-A}{2}\,|\psi\rangle = 0$.

Similarly, if $A|\psi\rangle = -1|\psi\rangle$, then $\frac{\hat{1}-A}{2}\,|\psi\rangle = |\psi\rangle$, while $\frac{\hat{1}+A}{2}\,|\psi\rangle = 0$

Measurement of operators A_i

We already discussed this previously.



$$|0\rangle \rightarrow \frac{|0\rangle + |1\rangle}{\sqrt{2}} \rightarrow \begin{cases} \frac{|0\rangle+|1\rangle}{\sqrt{2}} \text{ if } \lambda = +1 \\ \frac{|0\rangle-|1\rangle}{\sqrt{2}} \text{ if } \lambda - 1 \end{cases} \rightarrow \begin{cases} |0\rangle \\ |1\rangle \end{cases}$$

Formally $\frac{|0\rangle + |1\rangle}{\sqrt{2}} |\psi\rangle \rightarrow \frac{|0\rangle|\psi\rangle + |1\rangle(A|\psi\rangle)}{\sqrt{2}} \rightarrow$

$$\rightarrow \frac{(|0\rangle + |1\rangle)\,|\psi\rangle + (|0\rangle - |1\rangle)(A\,|\psi\rangle)}{2} = |0\rangle \underbrace{\frac{\hat{1} + A}{2}}_{\mathrm{P}_0^A} |\psi\rangle + |1\rangle \underbrace{\frac{\hat{1} - A}{2}}_{\mathrm{P}_1^A} |\psi\rangle$$

measurement selects one of two terms

5-qubit code

$2^5 = 32$ dimensions in Hilbert space

$3 \times 5 = 15$ possible errors

$2 \times (1 + 15) = 32$: all dimensions should be used

Need to distinguish 16 scenarios $\Rightarrow$ 4 operators A_i (they are usually called M_i)

$$M_0 = Z_1 X_2 X_3 Z_4$$
$$M_1 = Z_2 X_3 X_4 Z_0$$
$$M_2 = Z_3 X_4 X_0 Z_1$$
$$M_3 = Z_4 X_0 X_1 Z_2$$

qubit numbering: $k = 0, 1, 2, 3, 4$

There is no $M_4 = Z_0 X_1 X_2 Z_3$
because $M_4 = M_0 M_1 M_2 M_3$

$M_i^2 = \hat{1}$ for all of them because $X_k^2 = Z_k^2 = \hat{1}$

$M_i M_j = M_j M_i$ (commute) because $X_k Z_k = -Z_k X_k$,
and exactly two pairs of anticommuting operators

Encoding:

$$|0\rangle_L = \frac{1}{4}\left(\hat{1} + M_0\right)\left(\hat{1} + M_1\right)\left(\hat{1} + M_2\right)\left(\hat{1} + M_3\right)|00000\rangle$$
$$|1\rangle_L = \frac{1}{4}\left(\hat{1} + M_0\right)\left(\hat{1} + M_1\right)\left(\hat{1} + M_2\right)\left(\hat{1} + M_3\right)|11111\rangle$$

States $|0\rangle_L$ and $|1\rangle_L$ are orthogonal to each other because $|0\rangle_L$ is a superposition of terms with odd number of 0s and even number of 1s, while for $|1\rangle_L$ it is even number of 0s and odd number of 1s (each M_i flips 2 qubits). Possible to check that $|0\rangle_L$, $|1\rangle_L$ are normalized.

5-qubit code (cont.)

$$M_0 = Z_1X_2X_3Z_4$$
$$M_1 = Z_2X_3X_4Z_0$$
$$M_2 = Z_3X_4X_0Z_1$$
$$M_3 = Z_4X_0X_1Z_2$$

$$|0\rangle_L = \frac{1}{4}(\hat{1} + M_0)(\hat{1} + M_1)(\hat{1} + M_2)(\hat{1} + M_3)\,|00000\rangle$$

$$|1\rangle_L = \frac{1}{4}(\hat{1} + M_0)(\hat{1} + M_1)(\hat{1} + M_2)(\hat{1} + M_3)\,|11111\rangle$$

$|0\rangle_L$ and $|1\rangle_L$ are eigenstates of all M_i with eigenvalue $+1$; this is because all M_i commute and $M_i(\hat{1} + M_i) = \hat{1} + M_i$.

Therefore, measurement of M_i does not disturb superposition $|\psi\rangle = \alpha|0\rangle_L + \beta|1\rangle_L$ (it is also an eigenvector with eigenvalue $+1$).

It is possible to check that if we apply X_k (or Y_k or Z_k) to one qubit, then $X_k|\psi\rangle$, $Y_k|\psi\rangle$, and $Z_k|\psi\rangle$ are also eigenvectors of all M_i, but with different sets of eigenstates.

	M_0	M_1	M_2	M_3
$\|\psi\rangle$	+	+	+	+
$X_0\|\psi\rangle$	+	−	+	+
$Y_0\|\psi\rangle$	+	−	−	−

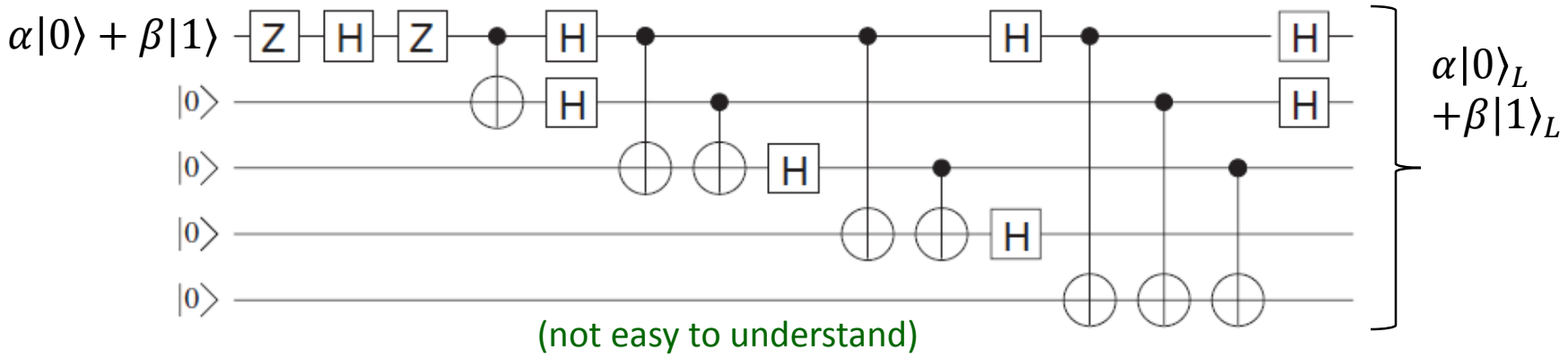
(and all other cases)

Full table:

	$X_0Y_0Z_0$	$X_1Y_1Z_1$	$X_2Y_2Z_2$	$X_3Y_3Z_3$	$X_4Y_4Z_4$	1
$M_0 = Z_1X_2X_3Z_4$	+	+	+	−	−	+	−	−	+	+
$M_1 = Z_2X_3X_4Z_0$	−	−	+	+	+	+	−	−	+	+	−	−	+
$M_2 = Z_3X_4X_0Z_1$	+	−	−	−	−	+	+	+	+	−	−	+	+
$M_3 = Z_4X_0X_1Z_2$	+	−	−	+	−	−	+	+	+	+	+	+	+

5-qubit code: circuits

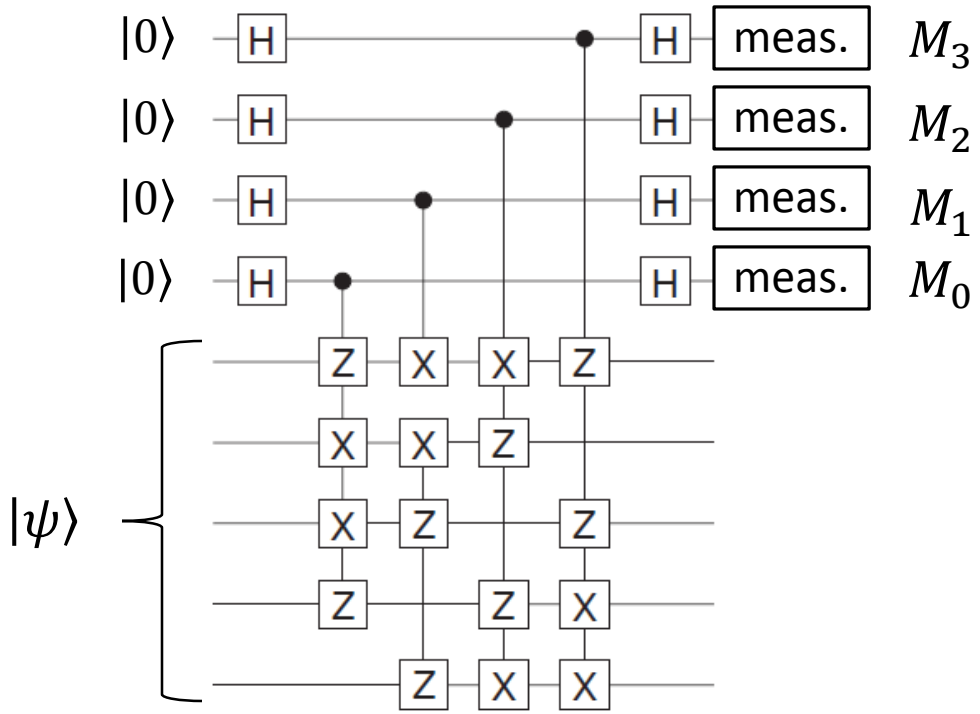
Encoding



(not easy to understand)

Measurement of error syndrome

$$M_0 = Z_1X_2X_3Z_4$$
$$M_1 = Z_2X_3X_4Z_0$$
$$M_2 = Z_3X_4X_0Z_1$$
$$M_3 = Z_4X_0X_1Z_2$$



7-qubit code (Steane)

Why do we need it? 5-qubit code is shorter!

(9-qubit code is not useful
though easy to understand)

7-qubit code is quite popular because it is good for "fault-tolerant" QC:
Several important logic operations can be done <u>without decoding</u>
(so far we considered only "memory", it is also good for "logic")

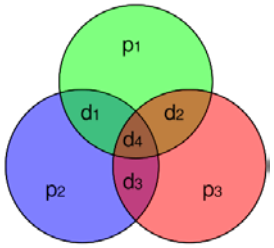
7 qubits $\Rightarrow$ $1 + 3 \times 7 = 22$ scenarios $\Rightarrow$ need at least 5 operators A_i ($2^5 = 32$)

However, this code uses 6 operators for error syndrome:

$$M_0 = X_0X_4X_5X_6 \qquad N_0 = Z_0Z_4Z_5Z_6$$
$$M_1 = X_1X_3X_5X_6 \qquad N_1 = Z_1Z_3Z_5Z_6$$
$$M_2 = X_2X_3X_4X_6 \qquad N_2 = Z_2Z_3Z_4Z_6$$

Up to renumbering, this is
the classical Hamming code

(different notation in N-C book)



6	5	4	3	2	1	0
X	X	X				X
X	X		X		X	
X		X	X	X		

The same combinations for M_i and N_i, only $X \leftrightarrow Z$

For all of them $M_i^2 = N_i^2 = \hat{1}$, so eigenvalues ± 1

All of them commute with each other
($[M_i, M_j] = 0$ trivially, $[N_i, N_j] = 0$ trivially,
$[M_i, N_j] = 0$ because even number of anticommuting pairs)

Since all of them commute, they divide 2^7-dim. Hilbert space into $2^6 = 64$ 2D subspaces

7-qubit code (cont.)

$M_0 = X_0X_4X_5X_6 \quad N_0 = Z_0Z_4Z_5Z_6$

$M_1 = X_1X_3X_5X_6 \quad N_1 = Z_1Z_3Z_5Z_6$

$M_2 = X_2X_3X_4X_6 \quad N_2 = Z_2Z_3Z_4Z_6$

6	5	4	3	2	1	0
X	X	X				X
X	X		X		X	
X		X	X	X		

Encoding

$$|0\rangle_L = \frac{1}{\sqrt{8}}\left(\hat{1} + M_0\right)\left(\hat{1} + M_1\right)\left(\hat{1} + M_2\right)|0000000\rangle$$

$$|1\rangle_L = \frac{1}{\sqrt{8}}\left(\hat{1} + M_0\right)\left(\hat{1} + M_1\right)\left(\hat{1} + M_2\right)|1111111\rangle$$

Orthogonal because $|0\rangle_L$ contains terms with odd number of 0s , while even for $|1\rangle_L$

$|\psi\rangle = \alpha|0\rangle_L + \beta|1\rangle_L$ is an eigenvector of all M_i and N_i with eigenvalues $+1$

(because $M_i\left(\hat{1} + M_i\right) = \hat{1} + M_i$, also N_i commute with $(\hat{1} + M_j)$,
and $|0\rangle_7$ and $|1\rangle_7$ are eigenstates of N_i with eigenvalue $+1$)

All 21 errors and correct codeword are distinguishable (states after errors are still eigenstates of M_i and N_i because X_k, Y_k, Z_k either commute or anticommute with M_i and N_i)

If X_k error occurs, then all M_i are still $+1$ (because commute with X_k), while one or two or three N_i become -1 (easy to see). From "pattern", we find qubit k affected by error.

Similarly, if Z_k error occurs, then N_i are still $+1$, but some M_i change to -1

If $Y_k = Z_kX_k$ error occurs, then both M_i and N_i change (the same pattern)

After detecting the error, we correct it by applying X_k, Y_k, Z_k (or nothing)

7-qubit code (cont.)

$M_0 = X_0X_4X_5X_6 \quad N_0 = Z_0Z_4Z_5Z_6$

$M_1 = X_1X_3X_5X_6 \quad N_1 = Z_1Z_3Z_5Z_6$

$M_2 = X_2X_3X_4X_6 \quad N_2 = Z_2Z_3Z_4Z_6$

6	5	4	3	2	1	0
X	X	X				X
X	X		X		X	
X		X	X	X		

Encoding

$$|0\rangle_L = \frac{1}{\sqrt{8}}(1+M_0)(1+M_1)(1+M_2)\,|0000000\rangle$$

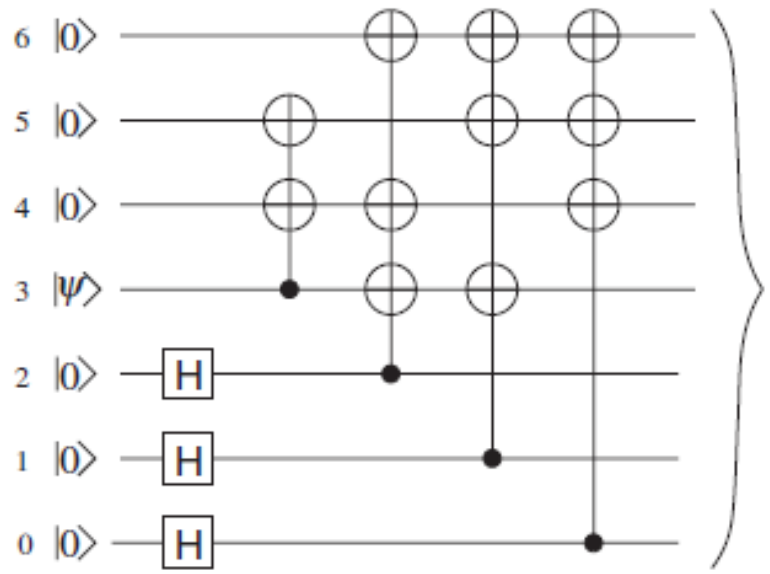
$$|1\rangle_L = \frac{1}{\sqrt{8}}(1+M_0)(1+M_1)(1+M_2)\,|1111111\rangle$$

Not all $2^6 = 64$ combinations of the error syndrome are used (only $1 + 3 \times 7 = 22$).
Remaining 42 combinations correspond to two-qubit errors X_iZ_j ($7 \times 6 = 42$);
this is useful, but not quite, because errors Z_iZ_j, X_iX_j, etc. are not dealt with.

7-qubit code: encoding circuit

Encoding

$\alpha|0\rangle + \beta|1\rangle$



$\alpha|0\rangle_L + \beta|1\rangle_L$

$$|0\rangle_L = \frac{1}{\sqrt{8}}(1 + M_0)(1 + M_1)(1 + M_2)\,|0000000\rangle$$

$$|1\rangle_L = \frac{1}{\sqrt{8}}(1 + M_0)(1 + M_1)(1 + M_2)\,|1111111\rangle$$

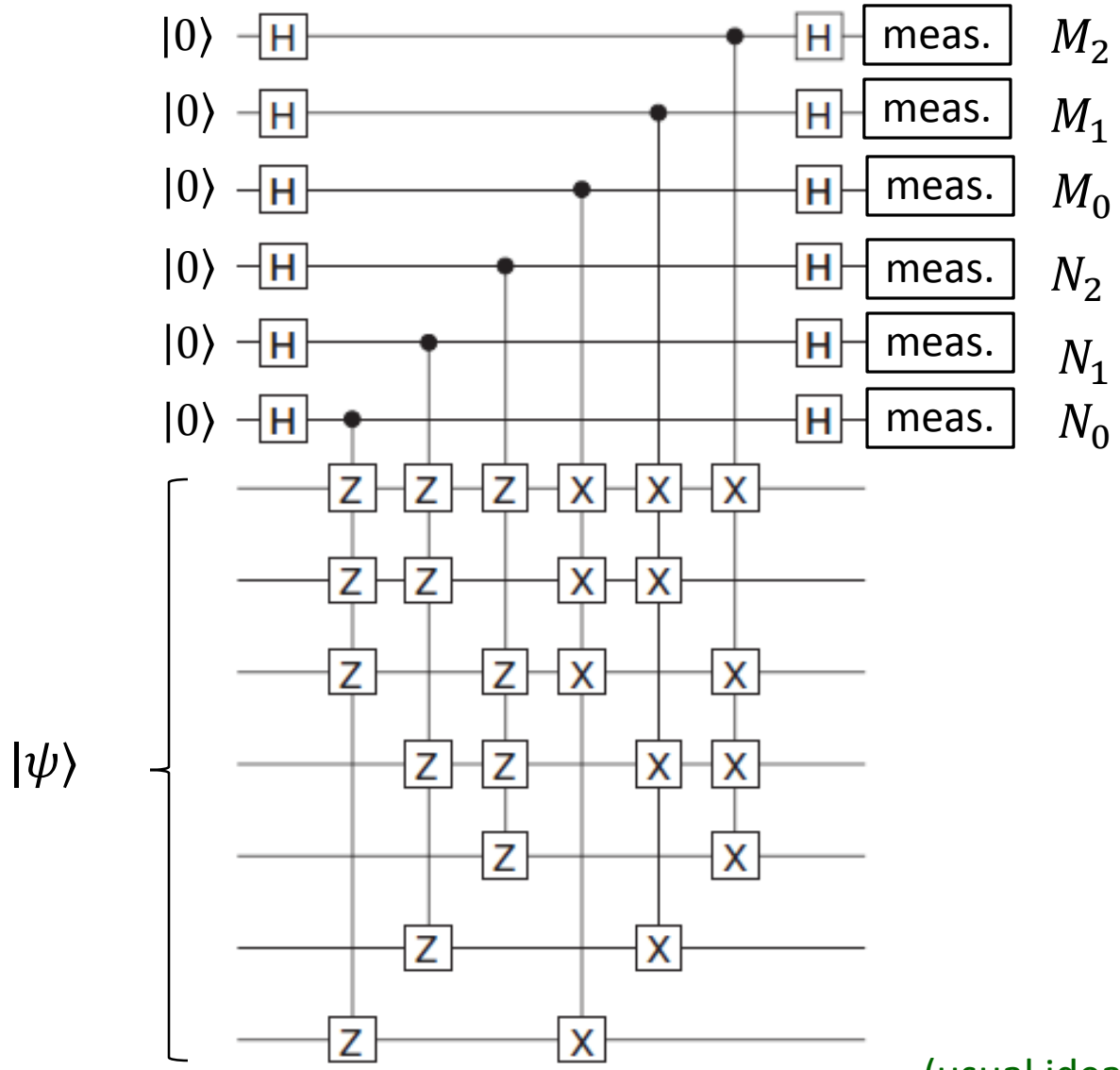
(not very easy to understand, but not very difficult either)

7-qubit code: circuit for error syndrome

Measurement of error syndrome

$$M_0 = X_0X_4X_5X_6$$
$$M_1 = X_1X_3X_5X_6$$
$$M_2 = X_2X_3X_4X_6$$

$$N_0 = Z_0Z_4Z_5Z_6$$
$$N_1 = Z_1Z_3Z_5Z_6$$
$$N_2 = Z_2Z_3Z_4Z_6$$



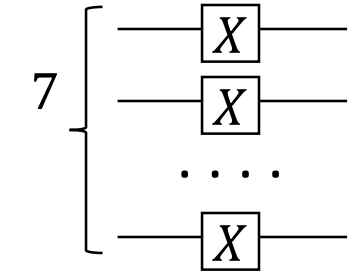
(usual idea)

7-qubit code: direct operations on 7-qubit codewords

Now discuss why 7-qubit code is so popular: it allows some logic operations to be done directly on the encoded 7-qubit state (without decoding)

Several important gates on logic qubits are realized as tensor products of gates on physical qubits ("transversal gates", "bitwise")

1. X-operation on logic qubit $\leftrightarrow$ $X^{\otimes 7}$ on physical qubits



Easy to see that $X^{\otimes 7}|0\rangle_L = |1\rangle_L,\ X^{\otimes 7}|1\rangle_L = |0\rangle_L$ (because all X_i commute and construction of $|0\rangle_L$ and $|1\rangle_L$ uses only X_i)

$$|0\rangle_L = \frac{1}{\sqrt{8}}\left(\hat{1} + M_0\right)\left(\hat{1} + M_1\right)\left(\hat{1} + M_2\right)|0000000\rangle$$

$$|1\rangle_L = \frac{1}{\sqrt{8}}\left(\hat{1} + M_0\right)\left(\hat{1} + M_1\right)\left(\hat{1} + M_2\right)|1111111\rangle$$

$$M_0 = X_0X_4X_5X_6$$
$$M_1 = X_1X_3X_5X_6$$
$$M_2 = X_2X_3X_4X_6$$

2. Similarly, Z-operation on logic qubit $\leftrightarrow$ $Z^{\otimes 7}$ on physical qubits

To prove, we need to show that $Z^{\otimes 7}|0\rangle_L = |0\rangle_L$ and $Z^{\otimes 7}|1\rangle_L = -|1\rangle_L$ (then linearity)

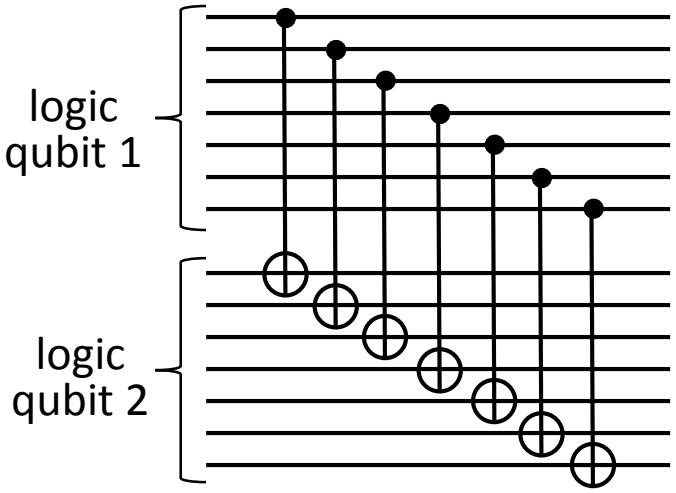
This is because $Z^{\otimes 7}$ commutes with M_i (4 anticommuting pairs), while $Z^{\otimes 7}|0000000\rangle = |0000000\rangle$ and $Z^{\otimes 7}|1111111\rangle = -|1111111\rangle$

7-qubit code: transversal gates

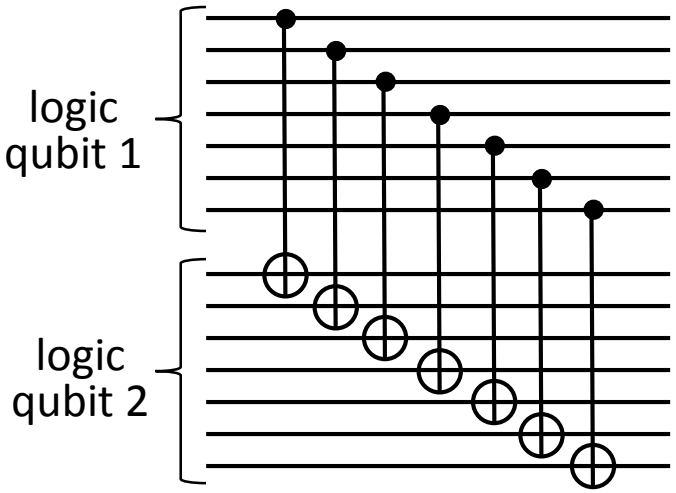
1. X-operation on logic qubit $\leftrightarrow$ $X^{\otimes 7}$ on physical qubits, $X_L = X^{\otimes 7}$
2. Z-operation on logic qubit $\leftrightarrow$ $Z^{\otimes 7}$ on physical qubits, $Z_L = Z^{\otimes 7}$
3. The same for Y-operation since $Y = ZX$ (composition), $Y_L = Y^{\otimes 7}$

   (Actually, the same for 5-qubit code: logic X, Y, and Z are easy to implement)
4. The same for Hadamard: $H_L = H^{\otimes 7}$ (not possible in 5-qubit code)

   (Proof is not very short, will not discuss).
5. Most importantly, CNOT can also be implemented qubit-by-qubit



7-qubit code: transversal CNOT



$$|0\rangle_L = \frac{1}{\sqrt{8}}\left(\hat{1} + M_0\right)\left(\hat{1} + M_1\right)\left(\hat{1} + M_2\right)|0000000\rangle$$

$$|1\rangle_L = \frac{1}{\sqrt{8}}\left(\hat{1} + M_0\right)\left(\hat{1} + M_1\right)\left(\hat{1} + M_2\right)|1111111\rangle$$

$$M_0 = X_0X_4X_5X_6$$

$$M_1 = X_1X_3X_5X_6$$

$$M_2 = X_2X_3X_4X_6$$

Not too hard to see why it works:

$|0\rangle_L$ and $|1\rangle_L$ (and their superpositions) are not changed by operators M_i (eigenvalue 1).

Therefore, if control is $|0\rangle_L = \frac{1}{\sqrt{8}}\left(\hat{1} + M_0 + M_1 + M_2 + M_0M_1 + M_0M_2 + M_1M_2 + \right.$

Now, if control is $|1\rangle_L = X^{\otimes 7}|0\rangle_L$, then extra flip of each target qubit;
since any X_i commutes with any M_j, this is equivalent to the flip $|0\rangle_L \leftrightarrow |1\rangle_L$ for target.

Fault-tolerant QC

So, we can do logical operations without decoding, and error correction can be used at each step. We can correct faulty gates as well (if only one works incorrectly); this works for one-qubit gates and also for CNOT (then errors are in two blocks and can both be corrected).

Again, 1) do logic without decoding, 2) correct faulty gates, single-qubit errors do not become multi-qubit errors.

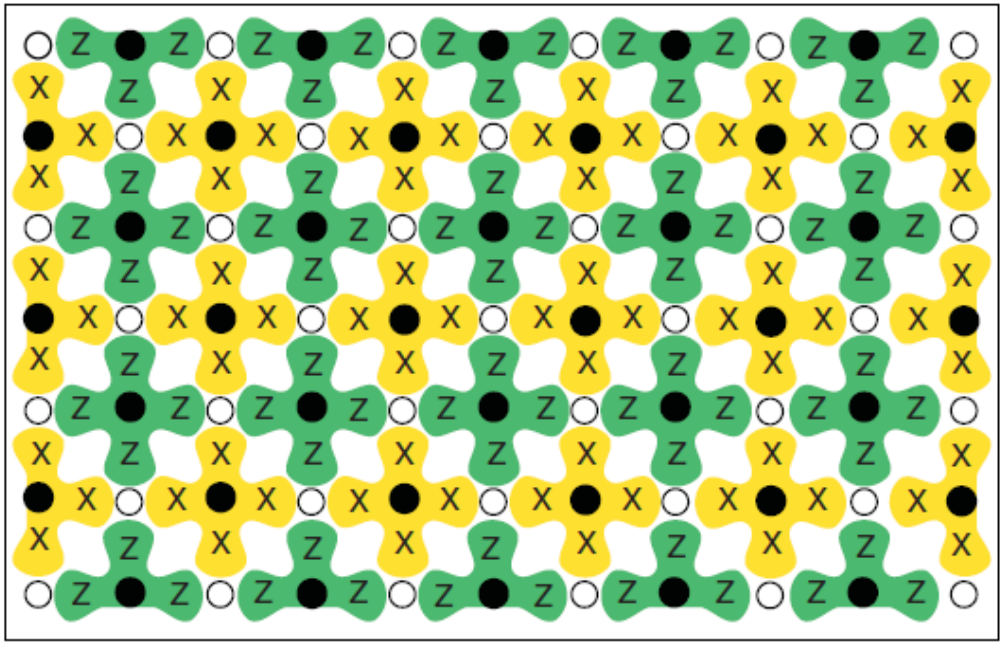
These are main requirements of a “fault-tolerant” QC

Fault tolerance: failure of a component leads to at most one error in each encoded block

Many tricks to make each step of a QC operation fault-tolerant, including production of ancillas, measurement, gates, “wires”, etc.

Recently much attention to topological codes: toric code (Kitaev), surface codes, color codes, etc.

Example: Surface code for superconducting qubits



A.G. Fowler, M. Mariantoni, J.M. Martinis, and A.N. Cleland, PRA 86, 032324 (2012)

4-qubit operators measured
Data qubits and ancilla qubits
Only nearest neighbors involved

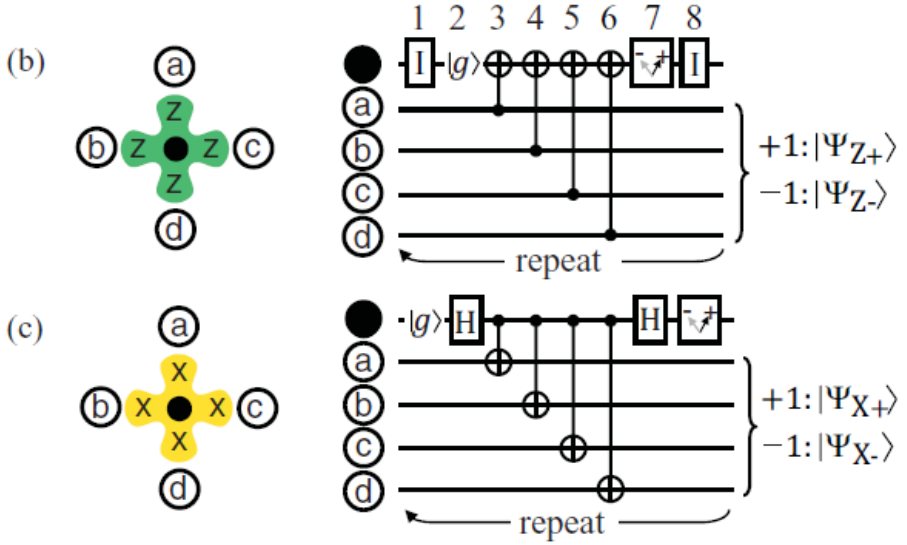


FIG. 1. (Color online) (a) A two-dimensional array implementation of the surface code. Data qubits are open circles (○), measurement qubits are solid circles (●), with measure-Z qubits colored green (dark) and measure-X qubits colored orange (light). Away from the boundaries, each data qubit contacts four measure qubits, and each measure qubit contacts four data qubits; the measure qubits perform four-terminal measurements. On the boundaries, the measure qubits contact only three data qubits and perform three-terminal measurements, and the data qubits contact either two or three measure qubits. The solid line surrounding the array indicates the array boundary. (b) Geometric sequence of operations (left), and quantum circuit (right) for one surface code cycle for a measure-Z qubit, which stabilizes $\hat{Z}_a\hat{Z}_b\hat{Z}_c\hat{Z}_d$. (c) Geometry and quantum circuit for a measure-X qubit, which stabilizes $\hat{X}_a\hat{X}_b\hat{X}_c\hat{X}_d$. The two identity $\hat{I}$ operators for the measure-Z process, which are performed by simply waiting, ensure that the timing on the measure-X qubit matches that of the measure-Z qubit, the former undergoing two Hadamard $\hat{H}$ operations. The identity operators come at the beginning and end of the sequence, reducing the impact of any errors during these steps.

Threshold theorem

Threshold theorem: If error correction lowers error probability and everything is fault-tolerant, then concatenation makes error probability arbitrarily small.

More quantitatively, if $p < p_{th}$ (p is failure probability for a component, p_{th} is a threshold), then an ideal circuit with $M(n)$ gates can be realized with error probability $< \varepsilon$ by a circuit with $O[poly\left(\log \frac{M(n)p_{th}}{\varepsilon}\right) M(n)]$ gates. (A big overhead is possible, but it is not exponential.)

polynomial of a fixed degree

Problem: the threshold p_{th} is usually low, because we need many qubits for error correction, and this increases the error probability

Currently $p_{th} \sim 10^{-6} - 10^{-2}$ for different codes (surface codes claim $p_{th} \sim 10^{-2}$)

Often people crudely say $p_{th} \sim 10^{-4}$

This is what makes QC potentially possible