Introduction to Quantum Information Processing

QIC 710 / CS 768 / PH 767 / CO 681 / AM 871

Lecture 14 (2017)

Jon Yard
QNC 3126
jyard@uwaterloo.ca
http://math.uwaterloo.ca/~jyard/qic710

Classical error correcting codes

Binary symmetric channel

Each bit that goes through it has probability ε of being flipped

3-bit repetition code:

- Encode each bit b as bbb
- Decode each received message $b_1 b_2 b_3$ as $\text{majority}(b_1, b_2, b_3)$

Reduces the effective error probability per data bit to $3\varepsilon^2 - 2\varepsilon^3$ at a cost of tripling the message length ("rate" is $1/3$).

Is this useful?

- If $\varepsilon = 0.1$ and this is applied to k-bit messages then around 3% of the k bits will be in error, rather than 10%
- If $\varepsilon = .01$ and this is applied to k-bit messages then around $.03\%$ of the k bits will be in error, rather than 1%

Can one do better?

A rough "big picture" view I

"Good" codes (for classical information):

Message: 0100110101110101 (some k-bit string)

Encoding: 011001101010010111110101011101 0 (n bits) ***constant expansion***

Errors: 010011101010110110110111011 0110

Decoding: 0100110101110101   ***no errors with probability*** $\rightarrow \mathbf{1}$ ***as*** $\boldsymbol{n} \rightarrow \infty$

k/n is the ***rate*** of the code (= reciprocal of message expansion)

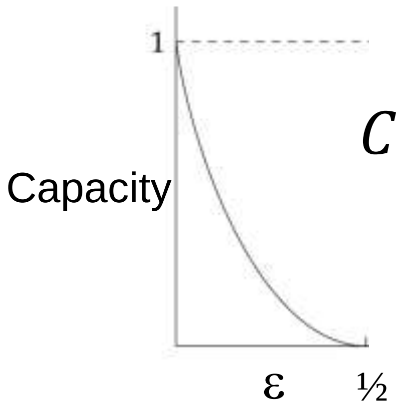
Theorem (good codes exist):

For all $\varepsilon < 1/2$, there exist encoding and decoding functions $E\colon\{0,1\}^k \rightarrow \{0,1\}^n$ and $D\colon\{0,1\}^n \rightarrow \{0,1\}^k$ such that k/n is ***constant*** and the probability of ***any*** errors $\rightarrow 0$ as $k \rightarrow \infty$.

A rough "big picture" view II

Rate as a function of noise level:

Each bit going through channel flips with probability ε



$$C(\varepsilon) = 1 - H(\varepsilon, 1-\varepsilon)$$
$$= 1 - (-\varepsilon \log(\varepsilon) - (1-\varepsilon)\log(1-\varepsilon))$$

The **rate** $R = \frac{k}{n}$ of a code is the reciprocal of message expansion. For every rate $R < \mathrm{C}(\varepsilon)$ (less than the **capacity**), there exist "good" codes for large n.

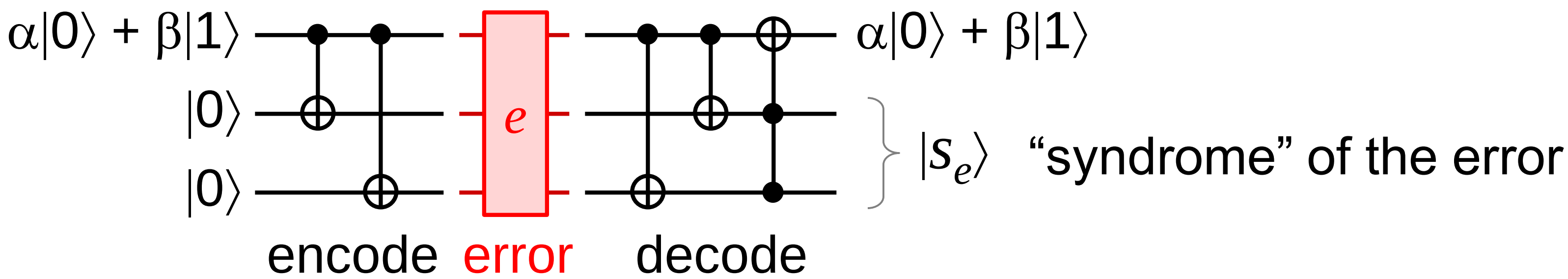
Informally, "good" codes with block length n have this property: probability of ***any*** errors occurring in block → 0 as $n \to \infty$.

What about ***quantum*** error correcting codes?

Shor’s 9-qubit code

3-qubit code for one X-error

The following 3-qubit quantum code protects against up to one error, ***if*** the error can only be a quantum bit-flip (an X operation)



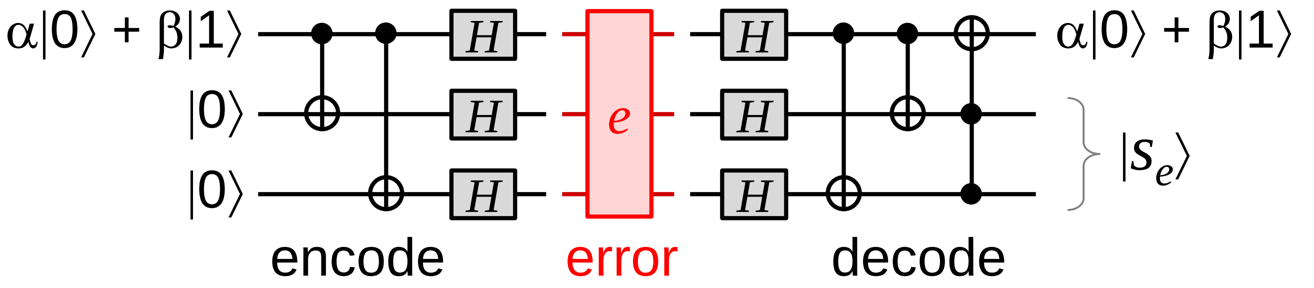
Error can be any one of:	$I\otimes I\otimes I$	$X\otimes I\otimes I$	$I\otimes X\otimes I$	$I\otimes I\otimes X$
Corresponding syndrome:	$\vert 00\rangle$	$\vert 11\rangle$	$\vert 10\rangle$	$\vert 01\rangle$

The essential property is that, in each case, the data $\alpha|0\rangle + \beta|1\rangle$ is shielded from (i.e. unaffected by) the error

What about Z errors? This code leaves them intact…

3-qubit code for one Z-error

Using the fact that $HZH = X$, one can adapt the previous code to protect against Z-errors instead of X-errors

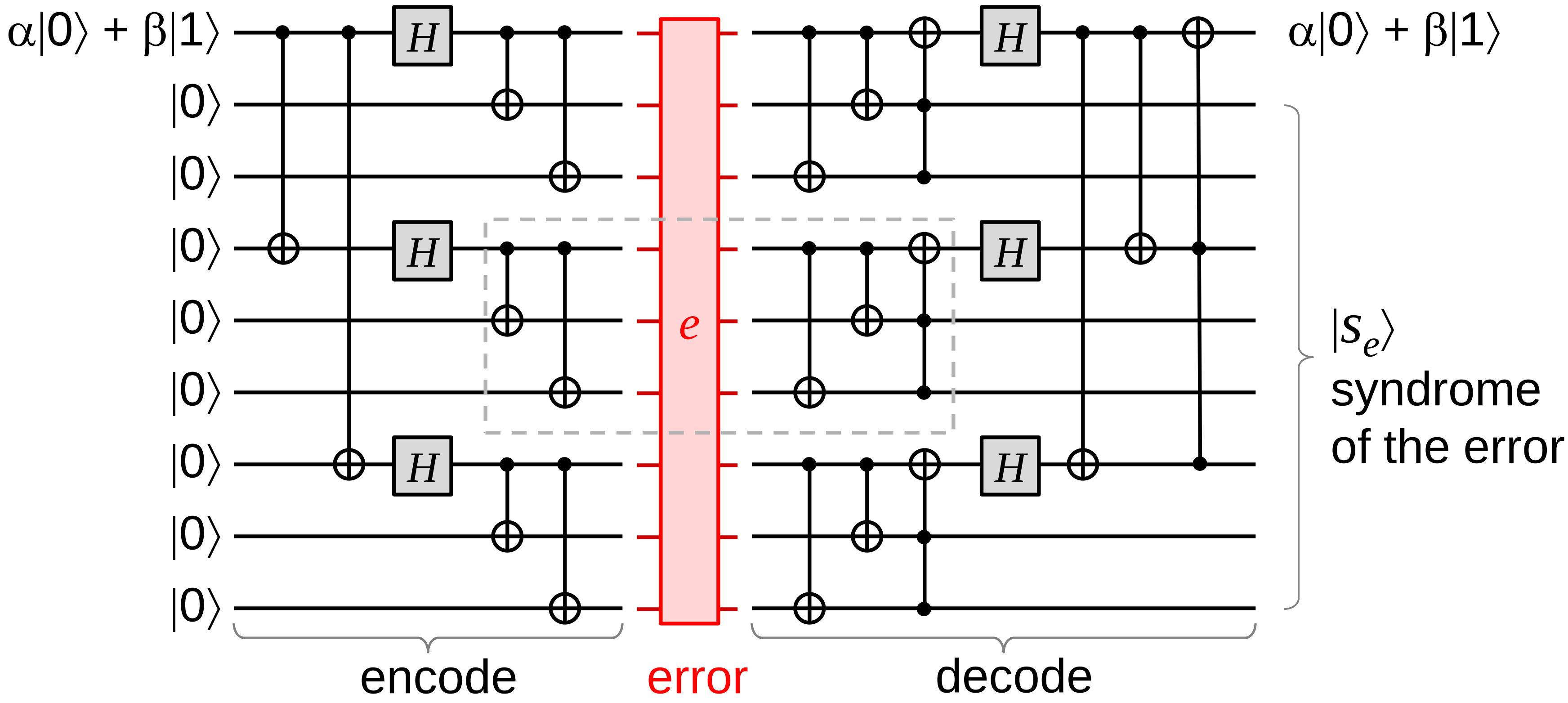


Error can be any one of: $I \otimes I \otimes I$ $Z \otimes I \otimes I$ $I \otimes Z \otimes I$ $I \otimes I \otimes Z$

This code leaves X-errors intact

Is there a code that protects against errors that are arbitrary one-qubit unitaries?

Shor's 9-qubit quantum code



The "inner" part corrects any single-qubit X-error

The "outer" part corrects any single-qubit Z-error

Since $Y = iXZ$, single-qubit Y-errors are also corrected

Arbitrary one-qubit errors

Suppose that the error is some arbitrary one-qubit unitary operation U

Since there exist scalars $\lambda_1, \lambda_2, \lambda_3$ and λ_4 such that

$$U \ = \lambda_1 I + \lambda_2 X + \lambda_3 Y + \lambda_4 Z$$

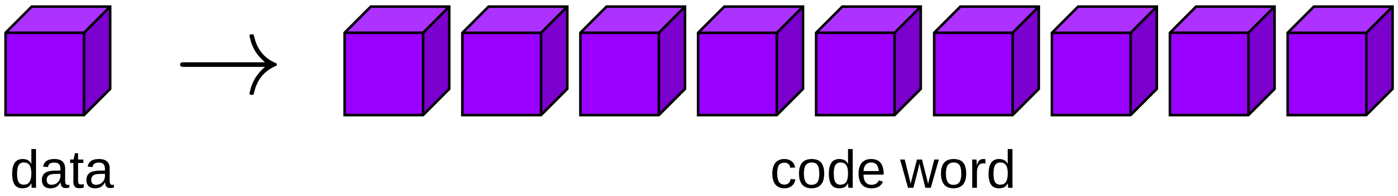
a straightforward calculation shows that, when a U-error occurs on the k^{th} qubit, the output of the decoding circuit is

$$(\alpha|0\rangle \ + \ \beta|1\rangle)(\lambda_1|s_{e_1}\rangle + \lambda_2|s_{e_2}\rangle + \lambda_3|s_{e_3}\rangle + \lambda_4|s_{e_4}\rangle)$$

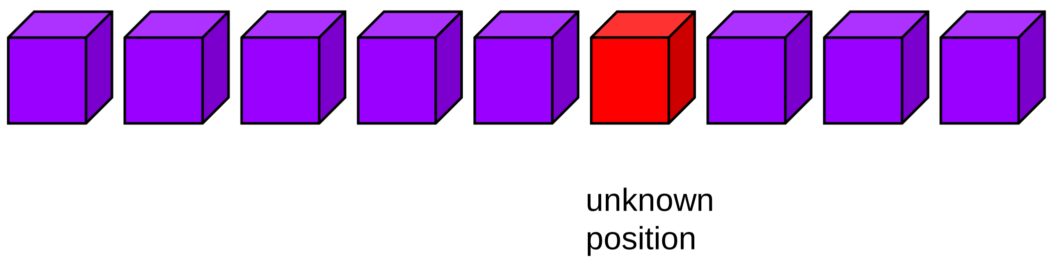
Where $s_{e_1}, s_{e_2}, s_{e_3}$ and s_{e_4} are the syndromes associated with the four errors (I, X, Y and Z) on the k^{th} qubit.

Hence the code actually protects against ***any*** unitary one-qubit error (in fact the error can be any one-qubit quantum operation)

Summary of 9-qubit code



Can recover data from ***any*** 1 qubit error:



It turns out the data can also be recovered data from ***any*** 2 qubit ***erasure*** error: