How good is the Shor Code?

Remark: If one qubit is affected by both a phase and a bit flip then the error gets also corrected by the previous method.

$\Rightarrow$ Shor code allows to recover from X_i, Z_i and $Y_i = X_i Z_i$.Can we do better?

Assume the noise is modelled by a quantum operation:

$$\mathcal{E}(|\psi_L\rangle\langle\psi_L|) = \sum_i E_i|\psi_L\rangle\langle\psi_L|E_i^\dagger.$$

Remember: Such a quantum operation *replaces* $|\psi_L\rangle\langle\psi_L|$ by $E_i|\psi_L\rangle\langle\psi_L|E_i^\dagger$ with probability $\mathrm{Tr}(E_i|\psi_L\rangle\langle\psi_L|E_i^\dagger)$.

Assume: E_i acts only upon the first qubit of $|\psi_L\rangle$. It is easy to verify that $X_1, Y_1 = X_1 Z_1$ and Z_1 form a basis for all operator acting upon the first qubit:

$$E_i = e_{i,0}\mathbb{I} + e_{i,1}X_1 + e_{i,2}Z_1 + e_{i,3}Y_1$$

for some complex numbers $e_{i,j}$ s.t. $\sum_j \mid e_{i,j} \mid^2 \leq 1$.

BRICS

Shor code is a $[9, 1, 3]$-QECC

Assume w.l.g that E_i happened to be the operation performed by the environment. The resulting un-normalized state $E_i|\psi_L\rangle$ can be written:

$$\begin{aligned} E_i|\psi_L\rangle &= (e_{i,0}\mathbb{I} + e_{i,1}X_1 + e_{i,2}Z_1 + e_{i,3}Y_1)|\psi_L\rangle \\ &= e_{i,0}|\psi_L\rangle + e_{i,1}X_1|\psi_L\rangle + e_{i,2}Z_1|\psi_L\rangle + e_{i,3}X_1Z_1|\psi_L\rangle. \end{aligned}$$

Therefore, measuring the syndrome results in:

- Fixing the error to be either X_1, Y_1, Z_1 or $\mathbb{I}$,
- Since we know wich one occured (property of the syndrome measurement) we can fix the error!

⇒ Any error acting upon anyone qubit can be fixed
⇒ Shor code is a $[9, 1, 3]$-QECC!

BRICS

An Error-Correcting Condition

Theorem: *Suppose C is a quantum error-correcting code and R is an operation allowing to recover from noise process $\mathcal{E} = \{E_i\}_i$. Suppose $\mathcal{F} = \{F_j\}_j$ is another noise process that satisfies for all i, j:*

$$F_j = \sum_i m_{i,j} E_i$$

for complex numbers $m_{i,j}$. Then R also allows to recover from $\mathcal{F}$.

$\Rightarrow$ If a code C recovers from errors through the depolarizing channel:

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

provided no more than t qubits were disturbed then C recovers from any noise operation acting upon t qubits!

CSS codes

We now find codes allowing to correct *many errors*. Let:

C_1: be a $[n, k_1]$-linear error-correcting code,

C_2: be a $[n, k_2]$-linear error-correcting code,

such that

$$C_2 \subset C_1 \text{ and } C_1, C_2^{\perp} \text{ correct both } t \text{ errors.}$$

For $x \in C_1$, we define the quantum codeword:

$$|x + C_2\rangle = \frac{1}{\sqrt{|\ C_2\ |}} \sum_{y \in C_2} |x \oplus y\rangle.$$

- Each codeword corresponds to a coset in C_1/C_2,
- $(\forall x \neq x')[\langle x + C_2 | x' + C_2 \rangle \in \{0, 1\}]$,
- The number of different codewords is $2^{k_1 - k_2} = |\ C_1/C_2\ | = \frac{|C_1|}{|C_2|}$.

BRICS

Encoding Information in CSS codes

Let C_1 be a $[n, k_1]$-code and C_2 a $[n, k_2]$-code s.t. $C_2 \subset C_1$. Remember that $C_1/C_2 = \{c + C_2 : c \in C_1\}$.

- Observe that if $c \oplus c' \in C_2$ then

  $$|c + C_2\rangle = |c' + C_2\rangle$$

  since $c + C_2 = c + ((c \oplus c') + C_2) = c' + C_2$.

- Cosets are either disjoint or coincide: Let $d \in (c + C_2) \cap (c' + C_2)$. It follows that $d = c \oplus c_2 = c' \oplus c_2'$ for some $c_2, c_2' \in C_2$. This means that $c \oplus c' = c_2 \oplus c_2' \in C_2$ which we have seen imply that $c + C_2 = c' + C_2$.

- Each $c \in C_1$ is in some coset in C_1/C_2 and since each pair of cosets is either disjoint or coincide it follows:

  $$\#C_1 = \#(\text{different cosets}) \cdot \#(\text{any coset}) \Rightarrow \#(\text{different cosets}) = 2^{k_1 - k_2}.$$

- All these cosets can be numbered in binary and the basis state $|x\rangle$ for $x \in \{0, 1\}^{k_1 - k_2}$ can be encoded with the coset labelled with x.

Noisy CSS Codewords

H_1: parity check matrix for C_1,

H_2: parity check matrix for $C_2^{\perp}$,

$e_1 \in \{0,1\}^n$: the blit-flip error pattern,

$e_2 \in \{0,1\}^n$: the phase-flip error pattern.

$$|x + C_2\rangle \overset{\text{noise}}{\mapsto} \frac{1}{\sqrt{|\, C_2 \,|}} \sum_{y \in C_2} (-1)^{(x \oplus y) \cdot e_2} |x + y + e_1\rangle.$$

Given H_1 there exists a unitary transform that maps

$$|x + y + e_1\rangle \otimes |0\rangle \mapsto |x + y + e_1\rangle \otimes |H_1(x + y + e_1)\rangle = |x + y + e_1\rangle \otimes |H_1 e_1\rangle.$$

Applied to a codeword,

$$\sum_{y \in C_2} (-1)^{(x \oplus y) e_2} |x + y + e_1\rangle \otimes |0\rangle \overset{H_1}{\mapsto} \sum_{y \in C_2} (-1)^{(x \oplus y) e_2} |x + y + e_1\rangle \otimes |H_1 e_1\rangle.$$

BRICS

Correcting Bit-Flips

After measuring the bit-flip error-syndrome $s_X = H_1 e_1$, we can use the error-correcting capability of C_1 to recover given $w(e_1) \leq t$:

Error Locations: s_X allows to find for what positions i, $(e_1)_i = 1$.

Error-Correction: Applying X in positions where $(e_1)_i = 1$ allows to recover from bit-flips.

The resulting state is:

$$\frac{1}{\sqrt{|\, C_2 \,|}} \sum_{y \in C_2} (-1)^{(x \oplus y) \cdot e_2} |x + y\rangle.$$

It remains to recover from phase-flips.

$\Rightarrow$ We do that using the error-correction capability of $C_2^{\perp}$.

BRICS

Correcting Phase-Flips

As for the the Shor code, we shall correct phase-flips after *rotating* in the Hadamard basis:

$$\frac{1}{\sqrt{|\, C_2 \,|}} \sum_{y \in C_2} (-1)^{(x \oplus y) \cdot e_2} |x + y\rangle \overset{H^{\otimes n}}{\mapsto} \frac{1}{\sqrt{2^n \,|\, C_2 \,|}} \sum_{z} \sum_{y \in C_2} (-1)^{(x \oplus y) \cdot (e_2 \oplus z)} |z\rangle.$$

Setting $z' = z \oplus e_2$, we get:

$$\sum_{z'} \sum_{y \in C_2} (-1)^{(x \oplus y) \cdot z'} \left| z' \oplus e_2 \right\rangle = \sum_{z'} (-1)^{x z'} \sum_{y \in C_2} (-1)^{y z'} \left| z' + e_2 \right\rangle.$$

Since $\sum_{y \in C_2} (-1)^{y z'} = |\, C_2 \,|$ if $z' \in C_2^{\perp}$ and 0 otherwise. We get:

$$\frac{|\, C_2 \,|}{\sqrt{2^n \,|\, C_2 \,|}} \sum_{z' \in C_2^{\perp}} (-1)^{x z'} \left| z' + e_2 \right\rangle.$$

The phase-flips have now been converted to bit-flips!

BRICS

Correcting Phase-Flips (II)

We have,

$$\sqrt{\frac{|\,C_2\,|}{2^n}} \sum_{z' \in C_2^{\perp}} (-1)^{xz'} |z' + e_2\rangle \overset{H_2}{\mapsto} \sqrt{\frac{|\,C_2\,|}{2^n}} \sum_{z' \in C_2^{\perp}} (-1)^{xz'} |z' + e_2\rangle |H_2 e_2\rangle$$

$$\overset{\text{correction}}{\mapsto} \sqrt{\frac{|\,C_2\,|}{2^n}} \sum_{z' \in C_2^{\perp}} (-1)^{xz'} |z'\rangle$$

$$\overset{H^{\otimes n}}{\mapsto} \frac{1}{\sqrt{|\,C_2\,|}} \sum_{y \in C_2} |x + y\rangle,$$

since,

- $H_2(z' + e_2) = H_2 e_2$ by definition of H_2,
- Since $H^{\otimes n}$ is it self-inverse and

$$H^{\otimes n} \frac{1}{\sqrt{|\,C_2\,|}} \sum_{y \in C_2} |x + y\rangle = \sqrt{\frac{|\,C_2\,|}{2^n}} \sum_{z' \in C_2^{\perp}} (-1)^{xz'} |z'\rangle.$$

BRICS

A $[7,1,3]$-QECC

Consider the $[7,4,3]$-Hamming code defined by:

$$H = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix} \text{ and } G = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}.$$

Let C_1 be the $[7,4,3]$-Hamming code and let $C_2 = C_1^{\perp}$ be its dual:

$\Rightarrow$ G is the parity check matrix for C_2,

$\Rightarrow$ C_2 is a $[7,3]$-code,

$\Rightarrow$ $C_2 \subset C_1$ since $C_2 = \text{RowSpace}(H) \subset \text{RowSpace}(G) = C_1$,

$\Rightarrow$ $C_2^{\perp} = (C_1^{\perp})^{\perp} = C_1$ corrects 1 error,

$\Rightarrow$ The $\text{CSS}(C_1, C_2)$ is a $[7,1,3]$-QECC!

BRICS

A Class of CSS codes

Consider the following CSS code indexed by parameters u and v,

$$|x + C_2\rangle \equiv \frac{1}{\sqrt{|\ C_2\ |}} \sum_{y \in C_2} (-1)^{u \cdot y} |x \oplus y \oplus v\rangle$$

This is as good as a normal CSS code. Let e_1 and e_2 be the bit-flip and phase-flip error patterns respectively.

$$|x + C_2\rangle \overset{\text{noise}}{\mapsto} \frac{1}{\sqrt{|\ C_2\ |}} \sum_{y \in C_2} (-1)^{(x \oplus y \oplus v) \cdot e_2 \oplus u \cdot y} |x \oplus y \oplus v \oplus e_1\rangle.$$

This CSS code is denoted by $\mathrm{CSS}_{u,v}$. We now proceed the same way as for the CSS code in order to correct bit- and phase-flips.

BRICS

Recovering from Bit-Flips

The bit-flip error syndrom is computed and measured.

$$|x + C_2\rangle \overset{\text{noise}}{\mapsto} \frac{1}{\sqrt{|\,C_2\,|}} \sum_{y \in C_2} (-1)^{(x \oplus y \oplus v)\cdot e_2 \oplus u \cdot y} |x \oplus y \oplus v \oplus e_1\rangle.$$

It follows that

$$s_X = H_1(x \oplus y \oplus v \oplus e_1) = H_1(v \oplus e_1).$$

Since v is known so is $s_v = H_1 v$:

$$s_X \oplus s_v = H_1 e_1,$$

which we know how to correct for.

BRICS

Recovering from Phase-Flips

We have,

$$|\varphi_{pf}\rangle \overset{\text{phase-error}}{:=} \frac{1}{\sqrt{|C_2|}} \sum_{y\in C_2} (-1)^{(x\oplus y\oplus v)\cdot e_2 \oplus u\cdot y} |x \oplus y \oplus v\rangle.$$

We now apply $H^{\otimes n}$ upon $|\varphi_{pf}\rangle$:

$$H^{\otimes n}|\varphi_{pf}\rangle = \frac{2^{-n/2}}{\sqrt{|C_2|}} \sum_{z} \sum_{y\in C_2} (-1)^{(x\oplus y\oplus v)(z\oplus e_2)\oplus u\cdot y} |z\rangle$$

We now make the change of variable $z' := z \oplus e_2 \oplus u$:

$$\frac{2^{-n/2}}{\sqrt{|C_2|}} \sum_{z'} \sum_{y\in C_2} (-1)^{(x\oplus y\oplus v)(z'\oplus u)\oplus u\cdot y} |z' \oplus u \oplus e_2\rangle$$

$$= \frac{2^{-n/2}}{\sqrt{|C_2|}} \sum_{z'} (-1)^{(x\oplus v)(u\oplus z')} \sum_{y\in C_2} (-1)^{z'y} |z' \oplus u \oplus e_2\rangle$$

BRICS

Recovering from Phase-Flips (II)

$$\frac{2^{-n/2}}{\sqrt{|\, C_2 \,|}} \sum_{z'} (-1)^{(x \oplus v)(u \oplus z')} \sum_{y \in C_2} (-1)^{y \cdot z'} |z' \oplus u \oplus e_2\rangle.$$

Since $\sum_{y \in C_2} (-1)^{yz'} = |\, C_2 \,|$ when $z' \in C_2^{\perp}$ and 0 otherwise, we get

$$\frac{\sqrt{|\, C_2 \,|}}{2^{-n/2}} \sum_{z' \in C_2^{\perp}} (-1)^{(x \oplus v)(u \oplus z')} |z' \oplus u \oplus e_2\rangle.$$

It follows that

$$s_Z = H_2(z' \oplus u \oplus e_2) = H_2(u \oplus e_2).$$

Since u is known so is $s_u = H_1 u$:

$$s_Z \oplus s_u = H_2 e_2,$$

which we know how to correct for.

Properties of $\mathrm{CSS}_{u,v}$ codes

We now look at which paramers u and v correspond to different $\mathrm{CSS}_{u,v}$ codes:

- $\mathrm{CSS}_{u,v}$ generates the same code as $\mathrm{CSS}_{u',v'}$ if
  - $H_1 v = H_1 v'$, and
  - $H_2 u = H_2 u'$.
  - In other words, If v and v' belong to the same coset of C_1 and u and u' belong to the same coset of $C_2^\perp$ then $\mathrm{CSS}_{u,v}$=$\mathrm{CSS}_{u',v'}$.
- Moreover, if $H_1 v \neq H_1 v'$ or $H_2 u \neq H_2 u'$ then

$$\mathrm{CSS}_{u,v} \perp \mathrm{CSS}_{u',v'}.$$

BRICS

Noisy EPR-pairs

1. Suppose Alice prepares:

$$2^{-n/2} \sum_{x \in \{0,1\}^n} |x\rangle^A \otimes |x\rangle^B$$

2. Alice now sends the B-register to Bob,

3. Unfortunately some bit flips $e_1 \in \{0,1\}^n$ and phase-flips $e_2 \in \{0,1\}^n$ occurred. The state is now

$$2^{-n/2} \sum_{x \in \{0,1\}^n} (-1)^{x \cdot e_2} |x\rangle \otimes |x \oplus e_1\rangle.$$

How can Alice and Bob correct for e_1 and e_2 using only classical communication assuming $w(e_1) \leq t$ and $w(e_2) \leq t$?

$\mathbf{CSS}_{u,v}$ Codes Against Noisy EPR-pairs

Since for $H_1 v \neq H_1 v'$ or $H_2 u \neq H_2 u'$:

$$\mathrm{CSS}_{u,v} \perp \mathrm{CSS}_{u',v'},$$

and

- Each codes has dimension $2^{k_1-k_2}$,
- There are 2^{n-k_1} different syndroms in H_1 and 2^{k_2} different syndroms in H_2 (remember H_2 is the parity check matrix of $C_2^{\perp}$),
- The dimension spans by all these $\mathrm{CSS}_{u,v}$ codes is therefore the whole space of n qubits:

$$2^{k_1-k_2} 2^{n-k_1} 2^{k_2} = 2^n!$$

BRICS

EPR-pairs in the $\{\text{CSS}_{u,v}\}_{u,v}$ basis

Let

$$|\xi_{v_k,u,v}\rangle = \frac{1}{\sqrt{C_2}} \sum_{y \in C_2} (-1)^{u \cdot y} |v_k \oplus y \oplus v\rangle$$

It can be shown that,

$$2^{-n/2} \sum_{x \in \{0,1\}^n} |x\rangle \otimes |x\rangle = 2^{-n/2} \sum_{v_k,u,v} |\xi_{v_k,u,v}\rangle \otimes |\xi_{v_k,u,v}\rangle.$$

- n EPR pairs can be expressed as a superposition of pairs of identical orthonormal CSS codewords taken from all codes in $\{\text{CSS}_{u,v}\}_{u,v}$!
- Alice could measure syndroms u and v and announce them to Bob.
- Bob then know he received a codeword in $\text{CSS}_{u,v}$ *before* the noise occured....

BRICS

Fixing Noisy EPR-pairs

1. Alice prepares:
   $2^{-n/2}\sum_{x\in\{0,1\}^n}|x\rangle^A \otimes |x\rangle^B = 2^{-n/2}\sum_{v_k,u,v}|\xi_{v_k,u,v}\rangle^A \otimes |\xi_{v_k,u,v}\rangle^B,$
2. Alice now sends the B-register to Bob:
   $$2^{-n/2}\sum_{v_k,u,v}|\xi_{v_k,u,v}\rangle^A \otimes \left|\tilde{\xi}_{v_k,u,v}\right\rangle^B,$$
3. Alice measures syndroms u and v and announces them to Bob,
4. Bob knowing $\mathrm{CSS}_{u,v}$ can fix the errors:
   $$2^{(k_2-k_1)/2}\sum_{v_k}|\xi_{v_k,u,v}\rangle^A \otimes |\xi_{v_k,u,v}\rangle^B,$$
5. If Alice and Bob perform decoding they finally obtain:
   $$2^{(k_2-k_1)/2}\sum_{x\in\{0,1\}^{k_1-k_2}}|x\rangle^A \otimes |x\rangle^B.$$

BRICS