A Short Introduction to Stabilizer Codes

Andreas Klappenecker

Department of Computer Science

Texas A&M University

Repetition Codes

Classical Codes

$$0 \mapsto 000$$
$$1 \mapsto 111$$

Quantum Codes

$$|0\rangle \mapsto |000\rangle$$
$$|1\rangle \mapsto |111\rangle$$

What kind of errors can be corrected?

Repetition Codes

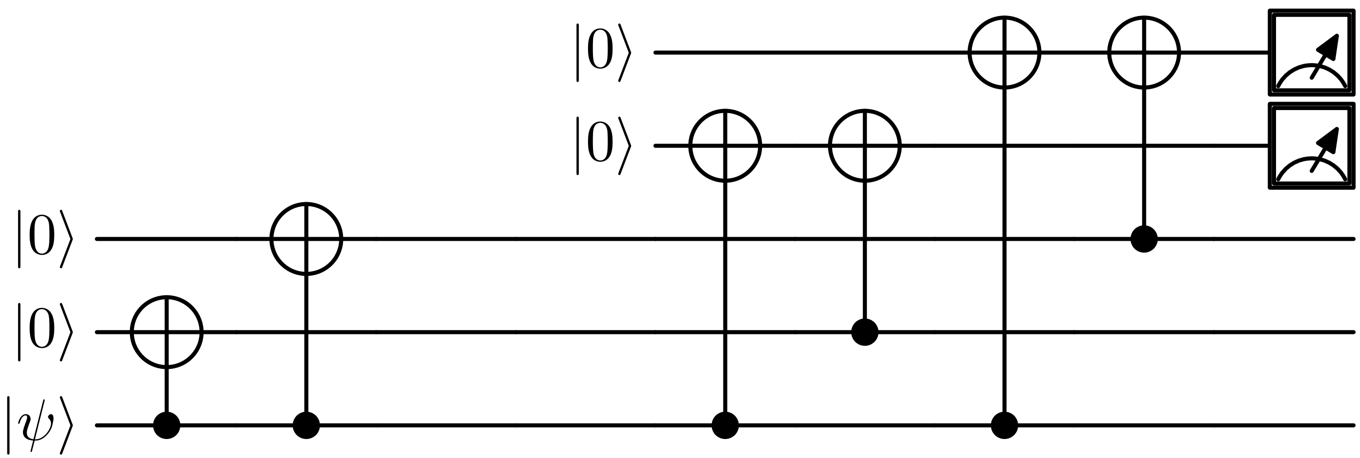
The classical code is able to correct a single bit flip.

The quantum code is able to correct single bit flips,

$$X \otimes I \otimes I, \quad I \otimes X \otimes I, \quad I \otimes I \otimes X,$$

and more!

Syndrome Calculation



Error	$X \otimes I \otimes I$	syndrome	10
Error	$I \otimes X \otimes I$	syndrome	01
Error	$I \otimes I \otimes X$	syndrome	11

Linearity of Syndrome Calculation

Error	$X \otimes I \otimes I$	syndrome	10
Error	$I \otimes X \otimes I$	syndrome	01

$$\boxed{E = \frac{1}{\sqrt{2}} X \otimes I \otimes I + \frac{1}{\sqrt{2}} I \otimes X \otimes I}$$

$$\frac{1}{\sqrt{2}} |10\rangle \otimes \left(X \otimes I \otimes I \left|\overline{\psi}\right\rangle\right) + \frac{1}{\sqrt{2}} |01\rangle \otimes \left(I \otimes X \otimes I \left|\overline{\psi}\right\rangle\right)$$

Discretization of Errors

Consider errors $E = E_n \otimes \cdots \otimes E_1$ $\qquad E_i \in \{I, X, Y, Z\}$

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \ Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \ Y = XZ = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}.$$

The weight of E is the number of $E_i \neq I$.

If a code Q corrects errors E of weight t or less, then Q can correct arbitrary errors affecting $\leq t$ qubits.

The Goal of the Game

A quantum error control code Q is a K-dimensional subspace of $\mathbf{C}^{2^n}$.

The goal is to find a quantum error control code which is able to correct (or detect) errors of weight t or less, where t is as large as possible.

The Stabilizer of a Code

Let $\mathcal{E}_n^{+} = \{E_n \otimes \cdots \otimes E_1 \mid E_i = I, X, Y, Z\}$.

Let $Q \leq \mathbf{C}^{2^n}$ be a quantum error control code.

The stabilizer of Q is defined to be the set

$$S = \{M \in \mathcal{E}_n^{+} \mid Mv = v \text{ for all } v \in Q\}.$$

S is a group, necessarily abelian if $Q \neq \{0\}$.

The Stabilizer of the Repetition Code

$Q \leq \mathbf{C}^{2^3}$ is the 2-dimensional code spanned by

$$|\overline{0}\rangle = |000\rangle$$

$$|\overline{1}\rangle = |111\rangle$$

The stabilizer of Q is given by

$$S = \{I \otimes I \otimes I,\ Z \otimes Z \otimes I,\ I \otimes Z \otimes Z,\ Z \otimes I \otimes Z\}$$

Stabilizer Codes

Let Q be a quantum error correcting code.

Let S be the stabilizer of Q.

The code Q is called a stabilizer code if and only if the condition $Mv = v$ for all $M \in S$ implies that $v \in Q$.

Q is the joint +1-eigenspace of the operators in S.

Is it a Stabilizer Code?

The repetition code is a stabilizer code. Why?

The code spanned by

$$\begin{aligned}|\overline{0}\rangle &= \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle) \\ |\overline{1}\rangle &= |11\rangle\end{aligned}$$

is not a stabilizer code. Why?

Projections and Dimensions

Let $Q \leq \mathbf{C}^{2^n}$ be a stabilizer code with stabilizer S.

$$P_Q = \frac{1}{|S|} \sum_{M \in S} M$$

is an orthogonal projection onto Q.

Indeed, check that $P_Q^2 = P_Q$ and $P_Q = P_Q^\dagger$ hold.

$$\dim Q = \mathrm{tr} P_Q = 2^n/|S|$$

Stabilizer Trivia

The repetition code is a stabilizer code.

Stabilizer S contains four elements,

$$S = \{I \otimes I \otimes I,\ Z \otimes Z \otimes I,\ I \otimes Z \otimes Z,\ Z \otimes I \otimes Z\}$$

Therefore, the projection operation P_Q associated with S gives

$$\dim Q = 2^3/|S| = 2$$

Stabilizer versus Non-Stabilizer Codes

If Q is not a stabilizer code, and S is the stabilizer of Q, then

$$\frac{1}{|S|} \sum_{M \in S} M$$

will project onto a space properly containing Q.

The Gretchen Question

How can we constuct good stabilizer codes?

What Next?

We discuss some constructions of stabilizer codes.

- We will have a closer look at errors.

- Symplectic geometry associated with stabilizer codes.

- Algebraic and combinatorial constructions.

Detectable Errors

An error E is detectable by a quantum code Q iff

$$P_Q E P_Q = c_E P_Q, \qquad c_E \in \mathbf{C}.$$

Distinguishable states $v, w \in Q$, $\langle v|w\rangle = 0$, remain distinguishable $\langle v|E|w\rangle = 0$.

Detection of the error does not reveal anything about the encoded state $\langle v|E|v\rangle = \langle v'|E|v'\rangle$.

Correctable Errors

A set $\mathcal{E} \subseteq \mathcal{E}_n^+$ of errors is correctable by a quantum code Q iff all errors in

$$\{E^\dagger F \mid E, F \in \mathcal{E}\}$$

are detectable.

No confusion principle: $v \perp w$ implies $Ev \perp Fw$. Syndrome measurement does not reveal the encoded state.

Errors in Stabilizer Codes

$$XZ = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = -ZX$$

Error operators in $\mathcal{E}_n^+$ (tensor products of I, X, Y, Z) either

- commute $EF = FE$
- or anticommute $EF = -FE$.

Errors in Stabilizer Codes

Let S be the stabilizer of a quantum code Q.

If an error E anticommutes with some $M \in S$, then E is detectable by Q.

Indeed,

$$P_Q E P_Q = P_Q E M P_Q = -P_Q M E P_Q = -P_Q E P_Q.$$

hence $P_Q E P_Q = 0$.

Errors: the Good, the Bad, and the Ugly

Let S be the stabilizer of a stabilizer code Q.

An error E is good if it does not affect the encoded information, e.g. $E \in S$.

An error E is bad if it is detectable, e.g. anticommutes with some $M \in S$.

An error E is ugly if it cannot be detected.

Examples of the Good, the Bad, and the Ugly

Let Q be the repetition code.

Good	$Z \otimes Z \otimes I$	$Z \otimes Z \otimes I\,\vert 111\rangle = \vert 111\rangle$
Bad	$X \otimes I \otimes I$	
Ugly	$X \otimes X \otimes X$	$X \otimes X \otimes X\,\vert 111\rangle = \vert 000\rangle$

Error Correction Capabilities

Let Q be a stabilizer code with stabilizer S.
Let $C(S)$ the commutator of S in $\mathcal{E}_n^+$.

All errors outside $C(S) - \langle \pm S \rangle$ can be detected.

If $C(S) - \langle \pm S \rangle$ does not contain errors of weight $\leq 2t$, then Q can correct errors of weight $\leq t$. Why?

Error Correction Capabilities

Suppose that $\mathcal{E}$ contains all errors of weight $\leq t$.

Then $E^\dagger F$ has weight $\leq 2t$. Show: $E^\dagger F$ is detectable

If $E^\dagger F \notin C(S)$, then $E^\dagger F$ anticommutes with some $M \in S$, hence is detectable.

If $E^\dagger F \in \langle \pm S \rangle$, then $E^\dagger F$ is good, hence detectable.

Short Summary

Any M_1, M_2 in the stabilizer S commute.

Detectable errors anticommute with some M in S or are elements in S (up to a sign).

Task: Find a short description of these properties.

Notation

Denote by X_a, $a = (a_n, \ldots, a_1) \in \mathbf{F}_2$, the operator

$$X_a = X^{a_n} \otimes \ldots \otimes X^{a_1}.$$

For instance, $X_{110} = X^1 \otimes X^1 \otimes X^0 = X \otimes X \otimes I$.

Operators in $\mathcal{E}_n^+$ are of the form $\pm X_a Z_b$.

Symplectic Geometry

Consider

$$M_1 = X_a Z_b \qquad M_2 = X_c Z_d$$

When do M_1 and M_2 commute?

$$M_1 M_2 \;=\; X_a Z_b X_c Z_d = (-1)^{b \cdot c} X_{a+b} Z_{b+d}$$

$$M_2 M_1 \;=\; X_c Z_d X_a Z_b = (-1)^{a \cdot d} X_{a+b} Z_{b+d}$$

M_1, M_2 commute iff $a \cdot d + b \cdot c = 0$ mod 2.

Short Description of a Stabilizer

Suppose that S is the stabilizer of a 2^k-dimensional stabilizer code. Then $|S| = 2^{n-k}$.

S can be generated by $n - k$ operators $X_a Z_b$.

Let $H = (H_x | H_z)$ be an $(n-k) \times 2n$ matrix over $\mathbf{F}_2$.

The rows of H contain the vectors $(a|b)$.

Short Description of a Stabilizer

Let

$$S = \{I \otimes I \otimes I,\ Z \otimes Z \otimes I,\ I \otimes Z \otimes Z,\ Z \otimes I \otimes Z\}$$

S is generated by $Z \otimes Z \otimes I$ and $Z \otimes I \otimes Z$.

$$H = \left(\begin{array}{c|c} 000 & 110 \\ 000 & 101 \end{array} \right)$$

$(a|b) = (000|110)$ and $(c|d) = (000|101)$

$$a \cdot d + b \cdot c = 000 \cdot 101 + 110 \cdot 000 = 0$$

The New Language

The commutator $C(S)$ contains all the ugly errors.

Modulo a sign, each operator in $C(S)$ is of the form

$$M = X_a Z_b$$

with $a \cdot d + b \cdot c = 0$ for all $X_c Z_d \in S$. Hence

$$(a|b) \perp (c|d)$$

w.r.t. the symplectic inner product.

The New Language

If $|S| = 2^{n-k}$, then $|C(S)| = 2 \cdot 2^{n+k}$.

[2^{n+k} because of the symplectic duality, twice because of the signs $\pm$]

Adding $2k$ rows to H gives a new matrix G describing the commutator $C(S)$. Recall that ugly errors are contained in $C(S) - \langle \pm S \rangle$.

The Repetition Code Revisited

$$G = \left(\begin{array}{c|c} 000 & 110 \\ 000 & 101 \\ \hline 111 & 000 \\ 000 & 111 \end{array}\right)$$

G is the generator matrix of a code.

Minimum distance is 2. The minimum distance needs to be ≥ 3 to correct an arbitrary error.

The Repetition Code Revisited II

M_1	000	110
M_2	000	101
$\overline{X}_1$	111	000
$\overline{Z}_1$	000	111

M_1, M_2 generate the stabilizer S

k operators $\overline{X}_k$ mapping to X_a's

k operators $\overline{Z}_k$ mapping to Z_b's

Codewords $\quad |c_1\rangle = \overline{X}_1^{c_1} \sum_{M \in S} M \, |000\rangle$

A Comparison of Notations

Stabilizer S	matrix H
Commutator $C(S)$	matrix G
Ugly errors $\subseteq C(S) - \langle \pm S \rangle$	$\langle G \rangle - \langle H \rangle$
Correct t errors	$\mathrm{MinDist}(\langle G \rangle - \langle H \rangle) \geq 2t + 1.$

The [[5,1,3]] Code

$$G = \left(\begin{array}{c|c} 10010 & 01100 \\ 01001 & 00110 \\ 10100 & 00011 \\ 01010 & 10001 \\ \hline 11111 & 00000 \\ 00000 & 11111 \end{array}\right)$$

One can check that all linear combinations of rows of G have at least weight 3.

$$\text{weight}((a|b)) = |\{i\,|a_i = 1 \text{ or } b_i = 1\}|$$

The [[5,1,3]] Code

Codewords

$$
\begin{aligned}
|\overline{0}\rangle &= \sum_{M \in S} M\,|00000\rangle \\
|\overline{1}\rangle &= \overline{X}\,|\overline{0}\rangle
\end{aligned}
$$

Shor's [[9,1,3]] Code

M_1	000	000	000	110	000	000
M_2	000	000	000	101	000	000
M_3	000	000	000	000	110	000
M_4	000	000	000	000	101	000
M_5	000	000	000	000	000	110
M_6	000	000	000	000	000	101
M_7	111	111	000	000	000	000
M_8	111	000	111	000	000	000
$\overline{X}$	111	111	111	000	000	000
$\overline{Z}$	000	000	000	111	111	111

Conclusions and Outlook

- Symplectic binary code allow simple design.
- Connections with codes over $\mathbf{F}_4$.
- Good quantum codes exist.
- Resilient Quantum Computers