Quantum Error Correction / CO639

lecture: 2004-02-24

Prepared by Annika Niehage

Edited by Daniel Gottesman

Guest Lecturer: Martin Rötteler

April 28, 2004

1 Codes over fields of arbitrary prime order

Plan:

- higher-dimensional quantum codes
- generalize error basis (*Pauli matrices*), *Clifford group*

Motivation:

- sometimes binary is too restrictive,
  e.g. $[[3,1,2]]_2$ does not exist
  for alphabet size 3 this exists
  e.g. $[[9,5,3]]_2$ does not exist
  for alphabet size 3 this guy exists
- beautiful constructions for higher-dimensional codes (e.g. *Reed Solomon codes*)

Literature:

[1] D. Gottesman: "*Fault-tolerant quantum computation with higher-dimensional systems*," QCQC '98, quant-ph/9802007

[2] A. Ashikhmin, M. Knill: "*Nonbinary quantum stabilizer codes*," quant-ph/0005008

[3] M. Grassl, M. Rötteler, Th. Beth: "*Efficient quantum circuits for non-qubit QECC*," quant-ph/0211014

Example: $[[3,1,2]]_2$ does not exist ($\rightarrow$ assignment 3)

Let's construct a $[[3,1,2]]_d$ for **any** odd $d \in \mathbb{N}$. Let

$$G := \left(\begin{array}{ccc|ccc} 1 & 1 & 1 & 1 & 1 & 0 \\ 2 & 0 & 0 & 0 & 1 & 1 \end{array}\right) \in \mathbb{Z}^{2\times 6}$$

and let C be the stabilizer code given by G.

Define the **symplectic inner product** as

$$(x,y) * (a,b) = ya - xb$$

Then

$$\left(\begin{array}{ccccccc} 1 & 1 & 1 & | & 1 & 1 & 0 \end{array}\right) * \left(\begin{array}{ccccccc} 2 & 0 & 0 & | & 0 & 1 & 1 \end{array}\right) = 2 - 2 = 0$$

Show that this detects any error E of wt 1.

- One way would be to find an element $M \in S$ s.t. $[M,E] \neq 0$.
- **Here**: We can assume that

$$E = \begin{array}{l} \left(\begin{array}{ccccccc} u & 0 & 0 & | & v & 0 & 0 \end{array}\right) \\ \left(\begin{array}{ccccccc} 0 & u & 0 & | & 0 & v & 0 \end{array}\right) \\ \left(\begin{array}{ccccccc} 0 & 0 & u & | & 0 & 0 & v \end{array}\right) \end{array}, u,v \in \mathbb{Z},\ (u,v) \neq (0,0)$$

$\Rightarrow$ Compute

$$A_1 := G * \left(\begin{array}{ccccccc} u & 0 & 0 & | & v & 0 & 0 \end{array}\right) = \begin{pmatrix} u-v \\ -2v \end{pmatrix} = \underbrace{\begin{pmatrix} 1 & 1 \\ 2 & 0 \end{pmatrix}}_{\det=-2} \cdot \begin{pmatrix} -v \\ u \end{pmatrix}$$

$$A_2 := G * \left(\begin{array}{ccccccc} 0 & u & 0 & | & 0 & v & 0 \end{array}\right) = \begin{pmatrix} u-v \\ u \end{pmatrix} = \underbrace{\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}}_{\det=1} \cdot \begin{pmatrix} -v \\ u \end{pmatrix}$$

$$A_3 := G * \left(\begin{array}{ccccccc} 0 & 0 & u & | & 0 & 0 & v \end{array}\right) = \begin{pmatrix} -v \\ u \end{pmatrix} = \underbrace{\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}}_{\det=1} \cdot \begin{pmatrix} -v \\ u \end{pmatrix}$$

$\Rightarrow$ can detect all wt 1 errors

$$\begin{aligned} &\Leftrightarrow \quad A_1,\ A_2,\ A_3 \text{ are invertible if we compute } mod\ d \\ &\Leftrightarrow \quad \det A_i \text{ is invertible} \\ &\qquad \Leftrightarrow\ 2 \text{ is invertible in } \mathbb{Z}/p\mathbb{Z} \\ &\qquad \Leftrightarrow\ d \text{ is odd} \end{aligned}$$

Result: for any odd $d \in \mathbb{N}$ there exists a $[[3,1,2]]_d$ stabilizer code.

Recall: $GF(p)$ is the set $\{0, \dots, p-1\}$ equipped with usual "+", "·" $mod\ p$, p prime.

Definition: (**Error bases**)

Let p be a prime. Then define

$$\begin{aligned} X_\alpha &:= \sum_{x=0}^{p-1} |x+\alpha\rangle\langle x| \ \text{ for } \alpha \in\ GF(p) \\ Z_\beta &:= \sum_{z=0}^{p-1} \omega_p^{\beta\cdot z} |z\rangle\langle z| \ \text{ for } \beta \in\ GF(p) \\ &\quad \text{where } \omega_p = \exp\left(\frac{2\pi i}{p}\right) \end{aligned}$$

These operators are also called "**Weyl operators**".

(for $GF(q)$, $q = p^r$:

$$\begin{aligned} X_\alpha &:= \sum_{x \in GF(q)} |x+\alpha\rangle\langle x| \ \text{ for } \alpha \in\ GF(q) \\ Z_\beta &:= \sum_{z \in GF(q)} \omega_p^{tr(\beta\cdot z)} |z\rangle\langle z| \ \text{ for } \beta \in\ GF(p) \end{aligned}$$

)

Theorem: Let p be a prime.

(i) $\forall \alpha,\, \beta:\ X_\alpha \cdot Z_\beta = \omega_p^{-\alpha\beta} Z_\beta \cdot X_\alpha$

(ii) $\forall \alpha,\, \alpha',\, \beta,\, \beta' : (X_\alpha \cdot Z_\beta)\cdot(X_{\alpha'} \cdot Z_{\beta'}) = \omega_p^{\alpha'\beta - \alpha\beta'} (X_{\alpha'} \cdot Z_{\beta'})\cdot(X_\alpha \cdot Z_\beta)$

(iii) The set $\{X_\alpha Z_\beta :\ \alpha, \beta \in GF(p)\}$ is an orthonormal basis for $\mathbb{C}^{p\times p}$ with respect to the inner product

$$\langle A, B\rangle := \frac{1}{p} tr(A^\dagger B)$$

Proof:

(i) We have to compute

$$\begin{aligned}
X_\alpha Z_\beta X_\alpha^{-1} &= (\sum_x |x+\alpha\rangle\langle x|)(\sum_z \omega_p^{\beta\cdot z}|z\rangle\langle z|)(\sum_{x'}|x'\rangle\langle x'+\alpha|) \\
&= \sum_x \omega_p^{\beta\cdot x}|x+\alpha\rangle\langle x+\alpha| \\
&= \sum_x \omega_p^{\beta\cdot(x-\alpha)}|x\rangle\langle x| \\
&= \sum_x \omega_p^{-\alpha\beta}\omega_p^{\beta\cdot x}|x\rangle\langle x| \\
&= \omega_p^{-\alpha\beta}\sum_x \omega_p^{\beta\cdot x}|x\rangle\langle x| \\
&= \omega_p^{-\alpha\beta} Z_\beta
\end{aligned}$$

(ii) direct consequence of (i)

(iii) To show:

(a) if $(\alpha,\beta)\neq(\alpha',\beta')$, then $tr((X_\alpha Z_\beta)^\dagger(X_{\alpha'}Z_{\beta'}))\neq 0$.

(b) This will follow if we can show that $tr(X_\alpha Z_\beta)\neq 0$ iff $(\alpha,\beta)\neq(0,0)$

We compute

$$\begin{aligned}
\frac{1}{p}tr(X_\alpha Z_\beta) &= \frac{1}{p}tr\left[(\sum_x |x+\alpha\rangle\langle x|)(\sum_z \omega_p^{\beta\cdot z}|z\rangle\langle z|)\right] \\
&= \frac{1}{p}tr(\sum_x \omega_p^{\beta\cdot x}|x+\alpha\rangle\langle x|) \\
&= \frac{1}{p}\sum_{x=0}^{p-1}\omega_p^{\beta\cdot x}\underbrace{\langle x+\alpha|x\rangle}_{\delta_{\alpha,0}} \\
&= \delta_{\alpha,0}\,\delta_{\beta,0}
\end{aligned}$$

□

Definition: Let p be a prime, X_α, Z_β as above.
For $\vec{\alpha},\ \vec{\beta}\in GF(p)^n$ define

$$\begin{aligned}
X_{\vec{\alpha}} &:= X_{\alpha_1}\otimes\cdots\otimes X_{\alpha_n} \\
Z_{\vec{\beta}} &:= Z_{\beta_1}\otimes\cdots\otimes Z_{\beta_n}
\end{aligned}$$

Remark: "Everything holds for the $X_{\vec{\alpha}},\ Z_{\vec{\beta}}$ as well."

This means

(i) $(X_{\vec{\alpha}} \cdot Z_{\vec{\beta}}) \cdot (X_{\vec{\alpha}'} \cdot Z_{\vec{\beta}'}) = \omega_p^{\sum_{i=1}^n \alpha'_i\beta_i - \alpha_i\beta'_i}(X_{\vec{\alpha}'} \cdot Z_{\vec{\beta}'}) \cdot (X_{\vec{\alpha}} \cdot Z_{\vec{\beta}})$

(ii) similarly

(iii) The set $\{X_{\vec{\alpha}}Z_{\vec{\beta}} \ :\ \vec{\alpha},\ \vec{\beta} \in GF(p)^n\}$ is an ONB for $\mathbb{C}^{p^n \times p^n}$.

Definition: (**Pauli group**, **Clifford group**)

$$\begin{aligned}
\mathcal{P}_{n,p} &:= \langle X_{\vec{\alpha}}Z_{\vec{\beta}} \ :\ \vec{\alpha},\ \vec{\beta} \in GF(p)^n \rangle \\
\mathcal{C}_{n,p} &:= N_{U(p^n)}(\mathcal{P}_{n,p})
\end{aligned}$$

Definition/Theorem: (**famous elements of $\mathcal{C}_{n,p}$**)

(i) $DFT := \frac{1}{\sqrt{p}} \sum_{x,z} \omega_p^{xz} |z\rangle\langle x|$

(ii) $P := \sum_z \omega_p^{\frac{z(z-1)}{2}} |z\rangle\langle z|$

(iii) $ADD^{(1,2)} := \sum_{x,y} |x\rangle_1 |x+y\rangle_2 \langle x|_1 \langle y|_2$

(iv) $M_\gamma := \sum_{y=0}^{p-1} |\gamma y\rangle\langle y|$ for $\gamma \in GF(p)$

Proof:

(i) We have to show that $DFT^\dagger\, E\, DFT$ is again a Pauli matrix (for all $E \in \mathcal{P}_{1,p}$)

$$\begin{aligned}
DFT^\dagger\, Z_\beta\, DFT &= \Big(\frac{1}{\sqrt{p}} \sum_{i,j} \omega_p^{-ij} |i\rangle\langle j|\Big)\Big(\sum_z \omega_p^{\beta z} |z\rangle\langle z|\Big)\Big(\frac{1}{\sqrt{p}} \sum_{k,l} \omega_p^{kl} |k\rangle\langle l|\Big) \\
&= \frac{1}{p} \sum_{i,l,z} \omega_p^{(-iz+\beta z+zl)} |i\rangle\langle l| \\
&= \frac{1}{p} \sum_{i,l} \Big(\underbrace{\sum_z \omega_p^{(-i+\beta+l)z}}_{=\begin{cases} 0 & \text{if} \quad -i+\beta+l \neq 0 \\ p & \text{if} \quad -i+\beta+l=0 \Leftrightarrow i=\beta+l \end{cases}} \Big) |i\rangle\langle l| \\
&= \sum_l |l+\beta\rangle\langle l| \\
&= X_\beta
\end{aligned}$$

Similarly, we can show: $DFT^\dagger \, X_\alpha \, DFT = Z_\alpha^{-1} \Rightarrow DFT$ acts on $(\alpha|\beta) \in GF(p)^2$ as the matrix

$$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$

Or the other way round with conjugation $U \mapsto UEU^\dagger$

$$\begin{array}{ccc} X & \stackrel{DFT}{\mapsto} & Z \\ Z & \mapsto & X^{-1} \end{array}$$

(Exercise): Show that

(ii) P acts like $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, $\begin{array}{ccc} X & \mapsto & XZ \\ Z & \mapsto & Z \end{array}$

(iii) M_γ acts like $\begin{pmatrix} \gamma^{-1} & 0 \\ 0 & \gamma \end{pmatrix}$

(iv) $ADD^{(1,2)}$ acts on $(\alpha_1|\beta_1)$, $(\alpha_2|\beta_2)$ as the matrix

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 \\ -1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} \alpha_1 \\ \beta_1 \\ \alpha_2 \\ \beta_2 \end{pmatrix} = \begin{pmatrix} \alpha_1 \\ \beta_1 + \beta_2 \\ -\alpha_1 + \alpha_2 \\ \beta_2 \end{pmatrix}$$

$\square$