

2012 KIAS International Conference on Coding Theory and Applications 15–17 November 2012

Quantum Codes from Classical Codes: An overview

Markus Grassl

16 November 2012



Centre for Quantum Technologies

Markus.Grassl@nus.edu.sg www.codetables.de

Quantum Information (I)

Quantum-bit (qubit)

basis states:

"0"
$$\hat{=} |0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \in \mathbb{C}^2,$$
 "1" $\hat{=} |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \in \mathbb{C}^2$

general state:

$$|q\rangle = \alpha |0\rangle + \beta |1\rangle \qquad \text{where } \alpha, \beta \in \mathbb{C} \text{, } |\alpha|^2 + |\beta|^2 = 1$$

measurement:

- result "0" with probability $|\alpha|^2$, projection $P_0 = |0\rangle\langle 0|$
- result "1" with probability $|\beta|^2$, projection $P_1 = |1\rangle\langle 1|$

Quantum Information (II)

Quantum register

basis states:

$$|b_1\rangle \otimes \ldots \otimes |b_n\rangle =: |b_1 \ldots b_n\rangle = |\mathbf{b}\rangle$$
 where $b_i \in \{0, 1\}$

general state:

$$|\psi\rangle = \sum_{\boldsymbol{x} \in \{0,1\}^n} c_{\boldsymbol{x}} |x\rangle \qquad \text{where } \sum_{\boldsymbol{x} \in \{0,1\}^n} |c_{\boldsymbol{x}}|^2 = 1$$

 \longrightarrow normalized vector in $(\mathbb{C}^2)^{\otimes n} \cong \mathbb{C}^{2^n}$ basis vectors are labelled by bitstrings x

partial measurement of first qubit, e.g., result "0":

$$|\psi'\rangle = \alpha(|0\rangle\langle 0|\otimes I_2\otimes\cdots\otimes I_2)|\psi\rangle = \alpha \sum_{\boldsymbol{y}\in\{0,1\}^{n-1}} c_{0\boldsymbol{y}}|0\boldsymbol{y}\rangle$$

Quantum Information (III)

Quantum operations

- unitary transformations (solution of Schrödinger equation for closed systems)
- measurements: orthogonal projection operators P_i

Elementary operations

- local unitary operations $U^{(i)} = I \otimes \ldots \otimes I \otimes U \otimes I \otimes \ldots \otimes I$ where $U \in SU(2)$
- "controlled NOT operation"

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} = \underbrace{\hat{-}}_{-} \hat{-} |x\rangle |y\rangle \mapsto |x\rangle |x+y\rangle$$

Quantum Information (IV)

Mixed States

- ensemble of quantum states $|\psi_i\rangle$ with probabilities p_i
- modelled by *density matrix*

$$\rho = \sum_{i} p_i |\psi_i\rangle \langle \psi_i|$$

where $|\psi_i\rangle\langle\psi_i|$ is the projector onto the state $|\psi_i\rangle$

• example:

measurement of $|\psi\rangle=\alpha|0\rangle+\beta|1\rangle$ in standard basis $\{|0\rangle,|1\rangle\}$

$$\rho = \begin{pmatrix} |\alpha|^2 & 0\\ 0 & |\beta|^2 \end{pmatrix}$$

Interaction System/Environment



"Channel"

$$Q: \rho_{in} := |\phi\rangle\langle\phi| \longmapsto \rho_{out} := Q(|\phi\rangle\langle\phi|) := \sum_{i} E_{i}\rho_{in}E_{i}^{\dagger}$$

with Kraus operators (error operators) E_i

Local/low correlated errors

- product channel $Q^{\otimes n}$ where Q is "close" to identity
- Q can be expressed (approximated) with error operators \tilde{E}_i such that each E_i acts on few subsystems, e.g. quantum gates

Quantum Error-Correcting Codes

- subspace C of a complex vector space $\mathcal{H} \cong \mathbb{C}^N$ usually: $\mathcal{H} \cong \mathbb{C}^m \otimes \mathbb{C}^m \otimes \ldots \otimes \mathbb{C}^m =: (\mathbb{C}^m)^{\otimes n}$ "*n* qudits"
- errors: described by linear transformations acting on
 - some of the subsystems (local errors)
 - many subsystems in the same way (correlated errors)
- notation: $C = [n, k, d]_q = ((n, q^k, d))_q$ q^k -dimensional subspace C of $(\mathbb{C}^q)^{\otimes n}$
- minimum distance d:
 - detection of errors acting on d-1 subsystems
 - correction of errors acting on $\lfloor (d-1)/2 \rfloor$ subsystems
 - correction of erasures acting on $d-1\ {\rm known}\ {\rm subsystems}$

Basic Ideas

partitioning of all words

- (linear) algebra





orthogonal decomposition

- codewords
- • bounded weight errors
- other errors

$$(\mathbb{C}^q)^{\otimes n} = \mathcal{H}_{\mathcal{C}} \oplus \mathcal{H}_{\mathcal{E}_1} \oplus \ldots \oplus \mathcal{H}_{\mathcal{E}_i} \oplus \ldots$$

– combinatorics

Characterization of QECCs

QECC Characterization

[Knill & Laflamme, Phyical Review A 55, 900–911 (1997)]

A subspace C of H with orthonormal basis $\{|c_1\rangle, \ldots, |c_K\rangle\}$ is an error-correcting code for the error operators $\mathcal{E} = \{E_1, E_2, \ldots\}$, if there exists constants $\alpha_{k,l} \in \mathbb{C}$ such that for all $|c_i\rangle$, $|c_j\rangle$ and for all $E_k, E_l \in \mathcal{E}$:

$$\langle c_i | E_k^{\dagger} E_l | c_j \rangle = \delta_{i,j} \alpha_{k,l}. \tag{1}$$

It is sufficient that (1) holds for a vector space basis of \mathcal{E} .

 \implies only a finite set of errors

Quantum Errors

Bit-flip error:

• Interchanges $|0\rangle$ and $|1\rangle$. Corresponds to "classical" bit error.

• Given by NOT gate
$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

Phase-flip error:

• Inverts the *relative* phase of $|0\rangle$ and $|1\rangle$. Has no classical analogue!

• Given by the matrix
$$Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

Combination:

• Combining bit-flip and phase-flip gives
$$Y = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = XZ.$$

Pauli and Hadamard Matrices

"Pauli" matrices:

$$I, \ X = \left(\begin{array}{cc} 0 & 1 \\ 1 & 0 \end{array}\right), \ Z = \left(\begin{array}{cc} 1 & 0 \\ 0 & -1 \end{array}\right), \ Y = XZ = \left(\begin{array}{cc} 0 & -1 \\ 1 & 0 \end{array}\right)$$

Hadamard matrix:
$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

Important properties:

• $H^{\dagger}XH = Z$, "*H* changes bit-flips to phase-flips"

•
$$ZX = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = -Y = -XZ$$
, "X and Z anticommute"

• All errors either commute or anticommute!

Repetition Code

classical:

sender: repeats the information,

```
e.g. 0 \mapsto 000, 1 \mapsto 111
```

receiver: compares received bits and makes majority decision

quantum mechanical "solution":

sender: copies the information, e.g. $|\psi\rangle = \alpha |0\rangle + \beta |1\rangle \mapsto |\psi\rangle |\psi\rangle |\psi\rangle$ receiver: compares and makes majority decision

but: unknown quantum states can neither be copied nor can they be disturbance-free compared

The No-Cloning Theorem

Theorem: Unknown quantum states cannot be copied.

Proof: The copier would map $|0\rangle|\psi_{\text{blank}}\rangle \mapsto |0\rangle|0\rangle$, $|1\rangle|\psi_{\text{blank}}\rangle \mapsto |1\rangle|1\rangle$, and hence

$$\begin{aligned} (\alpha|0\rangle + \beta|1\rangle)|\psi_{\mathsf{blank}}\rangle &\mapsto \alpha|0\rangle|0\rangle + \beta|1\rangle|1\rangle \\ &\neq (\alpha|0\rangle + \beta|1\rangle) \otimes (\alpha|0\rangle + \beta|1\rangle) \\ &= \alpha^2|0\rangle|0\rangle + \beta^2|1\rangle|1\rangle + \alpha\beta(|0\rangle|1\rangle + |1\rangle|0\rangle) \end{aligned}$$



Contradiction to the linearity of quantum mechanics!

Simple Quantum Error-Correcting Code

Repetition code: $|0\rangle \mapsto |000\rangle$, $|1\rangle \mapsto |111\rangle$

Encoding of one qubit:

 $\alpha |0\rangle + \beta |1\rangle \mapsto \alpha |000\rangle + \beta |111\rangle.$

This defines a two-dimensional subspace $\mathcal{H}_{\mathcal{C}} \leq \mathcal{H}_2 \otimes \mathcal{H}_2 \otimes \mathcal{H}_2$

bit-flip	quantum state	subspace			
no error	$\alpha 000\rangle + \beta 111\rangle$	$(\mathbb{1}\otimes\mathbb{1}\otimes\mathbb{1})\mathcal{H}_{\mathcal{C}}$			
$1^{\rm st}$ position	$\alpha 100 angle + \beta 011 angle$	$(X\otimes \mathbb{1}\otimes \mathbb{1})\mathcal{H}_{\mathcal{C}}$			
$2^{\rm nd}$ position	$\alpha 010\rangle+\beta 101\rangle$	$(\mathbb{1}\otimes X\otimes \mathbb{1})\mathcal{H}_{\mathcal{C}}$			
$3^{\rm rd}$ position	$\alpha 001\rangle + \beta 110\rangle$	$(\mathbb{1}\otimes\mathbb{1}\otimes X)\mathcal{H}_{\mathcal{C}}$			

Hence we have an orthogonal decomposition of $\mathcal{H}_2\otimes\mathcal{H}_2\otimes\mathcal{H}_2$

Simple Quantum Error-Correcting Code

Problem: What about phase-errors?

Phase-flip $Z: |0\rangle \mapsto |0\rangle$ and $|1\rangle \mapsto -|1\rangle$.

In the Hadamard basis $|+\rangle, |-\rangle$ given by

$$\begin{array}{ll} |+\rangle & = & \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \\ |-\rangle & = & \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \end{array}$$

the phase-flip operates like the bit-flip $Z|+\rangle = |-\rangle$, $Z|-\rangle = |+\rangle$.

To correct phase errors we use repetition code and Hadamard basis:

$$\begin{array}{rcl} 0\rangle & \mapsto & (H\otimes H\otimes H)\frac{1}{\sqrt{2}}(|000\rangle + |111\rangle) = \frac{1}{2}(|000\rangle + |011\rangle + |101\rangle + |110\rangle) \\ 1\rangle & \mapsto & (H\otimes H\otimes H)\frac{1}{\sqrt{2}}(|000\rangle - |111\rangle) = \frac{1}{2}(|001\rangle + |010\rangle + |100\rangle + |111\rangle) \end{array}$$

Simple Quantum Error-Correcting Code

phase-flip	quantum state	subspace
no error	$\frac{\alpha}{2}(000\rangle + 011\rangle + 101\rangle + 110\rangle)$	$(\mathbb{1}\otimes\mathbb{1}\otimes\mathbb{1})\mathcal{H}_{\mathcal{C}}$
	$+\frac{\beta}{2}(001\rangle + 010\rangle + 100\rangle + 111\rangle)$	
$1^{\rm st}$ position	$\frac{\alpha}{2}(000\rangle + 011\rangle - 101\rangle - 110\rangle)$	$(Z\otimes 1\!\!\!1\otimes 1\!\!\!1)\mathcal{H}_{\mathcal{C}}$
	$+ \frac{\beta}{2} (001\rangle + 010\rangle - 100\rangle - 111\rangle)$	
$2^{\rm nd}$ position	$\frac{\alpha}{2}(000\rangle - 011\rangle + 101\rangle - 110\rangle)$	$(\mathbb{1}\otimes Z\otimes\mathbb{1})\mathcal{H}_{\mathcal{C}}$
	$+\tfrac{\beta}{2}(001\rangle- 010\rangle+ 100\rangle- 111\rangle)$	
$3^{\rm rd}$ position	$\frac{\alpha}{2}(000\rangle - 011\rangle - 101\rangle + 110\rangle)$	$(1\!\!1\otimes 1\!\!1\otimes Z)\mathcal{H}_{\mathcal{C}}$
	$-\frac{\beta}{2}(001\rangle + 010\rangle + 100\rangle - 111\rangle)$	

We again obtain an orthogonal decomposition of $\mathcal{H}_2\otimes\mathcal{H}_2\otimes\mathcal{H}_2$

Shor's Nine-Qubit Code $\llbracket 9, 1, 3 \rrbracket_2$

Bit-flip code: $|0\rangle \mapsto |000\rangle$, $|1\rangle \mapsto |111\rangle$ Phase-flip code: $|0\rangle \mapsto |+++\rangle$, $|1\rangle \mapsto |---\rangle$

Effect of single-qubit errors on the bit-flip code:

- $\bullet~X\mbox{-errors}$ change the basis states, but can be corrected
- Z-errors at any of the three positions:

- \implies bit-flip code & error correction convert the channel into a phase-error channel
- \implies Concatenation of bit-flip code and phase-flip code yields $[\![9, 1, 3]\!]_2$

Bit-flips and Phase-flips

Let $C \leq \mathbb{F}_2^n$ be a linear code. Then the image of the state

$$rac{1}{\sqrt{|C|}}\sum_{oldsymbol{c}\in C}|oldsymbol{c}
angle$$

under a bit-flip $m{x}\in\mathbb{F}_2^n$ and a phase-flip $m{z}\in\mathbb{F}_2^n$ is given by

$$\frac{1}{\sqrt{|C|}} \sum_{\boldsymbol{c} \in C} (-1)^{\boldsymbol{z} \cdot \boldsymbol{c}} |\boldsymbol{c} + \boldsymbol{x}\rangle.$$

Hadamard transform $H\otimes\ldots\otimes H$ maps this to

$$\frac{(-1)^{\boldsymbol{x}\boldsymbol{z}}}{\sqrt{|C^{\perp}|}} \sum_{\boldsymbol{c}\in C^{\perp}} (-1)^{\boldsymbol{x}\cdot\boldsymbol{c}} |\boldsymbol{c}+\boldsymbol{z}\rangle$$

CSS Codes

Introduced by R. Calderbank, P. Shor, and A. Steane [Calderbank & Shor, Physical Review A, **54**, 1098–1105, 1996] [Steane, Physical Review Letters **77**, 793–797, 1996]

Construction: Let $C_1 = [n, k_1, d_1]$ and $C_2 = [n, k_2, d_2]$ be classical linear codes with $C_2^{\perp} \leq C_1$. Let $\{\boldsymbol{x}_1, \ldots, \boldsymbol{x}_K\}$ be representatives for the cosets C_1/C_2^{\perp} . Define quantum states

$$|\boldsymbol{x}_{\boldsymbol{i}} + C_2^{\perp}\rangle := \frac{1}{\sqrt{|C_2^{\perp}|}} \sum_{\boldsymbol{y} \in C_2^{\perp}} |\boldsymbol{x}_{\boldsymbol{i}} + \boldsymbol{y}\rangle$$

Theorem: The vector space C spanned by these states is a quantum code with parameters $[\![n, k_1 + k_2 - n, d]\!]$ where $d \ge \min(d_1, d_2)$.

CSS Codes — how they work

Basis states:

$$|\boldsymbol{x}_i + C_2^{\perp}\rangle = rac{1}{\sqrt{|C_2^{\perp}|}} \sum_{\boldsymbol{y} \in C_2^{\perp}} |\boldsymbol{x}_i + \boldsymbol{y}
angle$$

Suppose a bit-flip error **b** happens to $|\boldsymbol{x}_i + C_2^{\perp}\rangle$:

$$rac{1}{\sqrt{|C_2^{\perp}|}}\sum_{oldsymbol{y}\in C_2^{\perp}} |oldsymbol{x}_i+oldsymbol{y}+oldsymbol{b}
angle$$

Now, we introduce an ancilla register initialized in $|0\rangle$ and compute the syndrome.

CSS Codes — how they work

Let H_1 be the parity check matrix of C_1 , i.e., $\boldsymbol{x}H_1^t = 0$ for all $\boldsymbol{x} \in C_1$.

$$\frac{1}{\sqrt{|C_2^{\perp}|}} \sum_{\boldsymbol{y} \in C_2^{\perp}} |\boldsymbol{x}_i + \boldsymbol{y} + \boldsymbol{b}\rangle | (\boldsymbol{x}_i + \boldsymbol{y} + \boldsymbol{b}) H_1^t \rangle = \frac{1}{\sqrt{|C_2^{\perp}|}} \sum_{\boldsymbol{y} \in C_2^{\perp}} |\underbrace{\boldsymbol{x}_i + \boldsymbol{y}}_{\in C_1} + \boldsymbol{b}\rangle |\boldsymbol{b} H_1^t \rangle$$

Then measure the ancilla to obtain $s = bH_1^t$. Use this to correct the error by a conditional operation which flips the bits in **b**.

Phase-flips: Suppose we have the state

$$\frac{1}{\sqrt{|C_2^{\perp}|}} \sum_{\boldsymbol{y} \in C_2^{\perp}} (-1)^{(\boldsymbol{x}_i + \boldsymbol{y}) \cdot \boldsymbol{z}} |\boldsymbol{x}_i + \boldsymbol{y}\rangle$$

Then $H^{\otimes n}$ yields a superposition over a coset of C_2 which has a bit-flip. Correct it as before (with a parity check matrix for C_2).

Example: Steane's Seven Qubit Code $[\![7, 1, 3]\!]_2$

Given the dual of a binary Hamming code C with generator matrix

then C is a [7,3,4] and $C \leq C^{\perp}$. The dual code C^{\perp} is a [7,4,3] and has generator matrix

$$G' = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix}$$



CSS Codes: Summary

- uses a pair of nested classical codes $C_2 \leq C_1$ over \mathbb{F}_q
- basis states of the CSS code correspond to cosets $C_2 + t_i \subset C_1$ \implies dimension of the code is $|C_1|/|C_2|$
- X-errors are corrected using $C_1 = [n, k_1, d_1]_q$
- Z-errors are corrected using the Euclidean dual $C_2^{\perp} = [n, n k_2, d_2^{\perp}]_q$

$$\implies \mathcal{C} = \llbracket n, k_1 - k_2, \ge \min(d_1, d_2^{\perp}) \rrbracket_q$$

- we can do (slightly) better if
 wgt(C₁ \ C₂) > wgt(C₁) or wgt(C₂[⊥] \ C₁[⊥]) > wgt(C₂[⊥])
- we may compute the dual distance using other inner products

Quantum Stabilizer Codes

[Gottesman, PRA 54 (1996); Calderbank, Rains, Shor, & Sloane, IEEE-IT 44 (1998)]

Basic Idea

Decomposition of the complex vector space into eigenspaces of operators.

Error Basis for Qudits

[A. Ashikhmin & E. Knill, Nonbinary quantum stabilizer codes, IEEE-IT 47 (2001)]

$$\mathcal{E} = \{ X^{\alpha} Z^{\beta} \colon \alpha, \beta \in \mathbb{F}_q \},\$$

where (you may think of $\mathbb{C}^q\cong\mathbb{C}[\mathbb{F}_q]$)

$$\begin{array}{lll} X^{\alpha} & := & \displaystyle\sum_{x \in \mathbb{F}_{q}} |x + \alpha \rangle \langle x| & \text{ for } \alpha \in \mathbb{F}_{q} \\ \\ \text{and} & Z^{\beta} & := & \displaystyle\sum_{z \in \mathbb{F}_{q}} \omega^{\operatorname{tr}(\beta z)} |z \rangle \langle z| & \text{ for } \beta \in \mathbb{F}_{q} \ (\omega := \omega_{p} = \exp(2\pi i/p)) \end{array}$$

Stabilizer Codes

common eigenspace of an Abelian subgroup S of the group \mathcal{G}_n with elements

$$\omega^{\gamma}(X^{\alpha_1}Z^{\beta_1}) \otimes (X^{\alpha_2}Z^{\beta_2}) \otimes \ldots \otimes (X^{\alpha_n}Z^{\beta_n}) =: \omega^{\gamma}X^{\alpha}Z^{\beta},$$

where $oldsymbol{lpha},oldsymbol{eta}\in\mathbb{F}_q^n$, $\gamma\in\mathbb{F}_p.$

quotient group:

$$\overline{\mathcal{G}}_n := \mathcal{G}_n / \langle \omega I \rangle \cong (\mathbb{F}_q \times \mathbb{F}_q)^n \cong \mathbb{F}_q^n \times \mathbb{F}_q^n \quad \text{as additive group}$$

 \mathcal{S} Abelian subgroup

$$\iff (\boldsymbol{\alpha}, \boldsymbol{\beta}) \star (\boldsymbol{\alpha}', \boldsymbol{\beta}') = 0 \text{ for all } \omega^{\gamma}(x^{\boldsymbol{\alpha}}Z^{\boldsymbol{\beta}}), \ \omega^{\gamma'}(x^{\boldsymbol{\alpha}'}Z^{\boldsymbol{\beta}'}) \in \mathcal{S},$$

where \star is a symplectic inner product on $\mathbb{F}_q^n \times \mathbb{F}_q^n$

Stabilizer codes correspond to symplectic codes over $\mathbb{F}_q^n \times \mathbb{F}_q^n$.

Symplectic Codes

most general:

additive codes $C \subset \mathbb{F}_q^n \times \mathbb{F}_q^n$ that are self-orthogonal with respect to

$$(\boldsymbol{v}, \boldsymbol{w}) \star (\boldsymbol{v}', \boldsymbol{w}') := \operatorname{tr}(\boldsymbol{v} \cdot \boldsymbol{w}' - \boldsymbol{v}' \cdot \boldsymbol{w}) = \operatorname{tr}(\sum_{i=1}^{n} v_i w_i' - v_i' w_i)$$

most studied:

 \mathbb{F}_q -linear codes $C \subset \mathbb{F}_q^n \times \mathbb{F}_q^n$ that are self-orthogonal with respect to

$$(\boldsymbol{v}, \boldsymbol{w}) \star (\boldsymbol{v}', \boldsymbol{w}') := \boldsymbol{v} \cdot \boldsymbol{w}' - \boldsymbol{v}' \cdot \boldsymbol{w} = \sum_{i=1}^{n} v_i w_i' - v_i' w_i$$

 \mathbb{F}_{q^2} -linear Hermitian codes $C \subset \mathbb{F}_{q^2}^n$ that are self-orthogonal with respect to

$$\boldsymbol{x} \star \boldsymbol{y} := \sum_{i=1}^n x_i^q y_i$$

Symplectic Codes & Stabilizer Codes

Theorem: (Ashikhmin & Knill) Let C be a symplectic code over $\mathbb{F}_q \times \mathbb{F}_q$ of size q^{n-k} and let $d := \min\{ \operatorname{wgt}(\boldsymbol{c}) \colon \boldsymbol{c} \in C^* \setminus C \}.$ Then there is a stabilizer code $\mathcal{C} = [\![n, k, d]\!]_q$.

Special cases:

- C = C₁[⊥] × C₂[⊥] with linear codes C₁, C₂ over 𝔽_q, C₂[⊥] ⊂ C₁, d = min{wgt(C₁ \ C₂[⊥]), wgt(C₂ \ C₁[⊥])}
 Calderbank-Shor-Steane (CSS) codes
- $C = C_1 \times C_1$ with a self-orthogonal linear code $C_1 \subset C_1^{\perp}$ over \mathbb{F}_q
- C = {(v, w): v + γw ∈ C₁} where C₁ is a Hermitian self-orthogonal linear code over 𝔽_{q²} (with some particular γ ∈ 𝔽_{q²} \ 𝔽_q)

Quantum Singleton Bound

[E. Rains, Nonbinary Quantum Codes, IEEE-IT **45**, pp. 1827–1832 (1999)] general bound on the minimum distance of $C = [n, k, d]_q$:

$$2d \le n - k + 2 \tag{2}$$

Quantum MDS codes:

quantum codes with equality in (2)

Minimum distance of a stabilizer code:

$$d_{\min}(\mathcal{C}) := \min\{ \operatorname{wgt}(\boldsymbol{c}) \colon \boldsymbol{c} \in C^* \setminus C \} \ge d_{\min}(C^*), \tag{3}$$

where C is the symplectic code corresponding to $\ensuremath{\mathcal{C}}$

Note: for QMDS codes we get equality in (3)

Stabilizer Codes & Classical Codes

• up to a global phase, any element of the n-qubit Pauli group \mathcal{P}_n can be written as

$$g = X^{\boldsymbol{a_1}} Z^{\boldsymbol{b_1}} \otimes \ldots \otimes X^{\boldsymbol{a_n}} Z^{\boldsymbol{b_n}} \qquad (\boldsymbol{a_j}, \boldsymbol{b_j} \in \{0, 1\})$$

- g corresponds to a binary vector (a|b) of length 2n or a vector v = a + ωb of length n over GF(4) = {0, 1, ω, ω²}
- the product of two elements g and h given by $v = a + \omega b$ and $w = c + \omega d$ corresponds to $v + w = (a + c) + \omega (b + d)$
- two elements g and h given by $v = a + \omega b$ and $w = c + \omega d$ commute iff

$$\boldsymbol{a} \cdot \boldsymbol{d} - \boldsymbol{b} \cdot \boldsymbol{c} = 0$$
 or equivalently $\boldsymbol{v} * \boldsymbol{w} = \operatorname{tr}(\boldsymbol{v} \cdot \boldsymbol{w}^2) = 0$

• the weight of g equals the Hamming weight of \boldsymbol{v}

Stabilizer Codes & Classical Codes

- a stabilizer code C = [n, k, d] is the joint +1-eigenspace of the stabilizer group $S = \langle S_1, \dots, S_{n-k} \rangle$
- the normalizer \mathcal{N} is generated by \mathcal{S} and logical operators $\overline{X}_1, \ldots, \overline{X}_k$, $\overline{Z}_1, \ldots, \overline{Z}_k$,
- the stabilizer ${\mathcal S}$ corresponds to a self-orthogonal additive code $C=(n,2^{n-k})$ over GF(4)
- the normalizer ${\mathcal N}$ corresponds to the symplectic dual code $C^\star = (n, 2^{n+k})$
- the minimum distance d of \mathcal{C} is given by

$$d = \min\{ \operatorname{wgt}(\boldsymbol{v}) : \boldsymbol{v} \in C^* \setminus C \}$$



stabilizer state



stabilizer

Canonical Basis

- fix logical operators \overline{X}_j and \overline{Z}_j
- the stabilizer S and the logical operators \overline{Z}_j mutually commute
- the logical state $|\overline{00...0}\rangle$ fixed by \mathcal{S} and all \overline{Z}_j is a stabilizer state
- define the (logical) basis states as

$$\left|\overline{i_{1}i_{2}\ldots i_{k}}\right\rangle = \overline{X}_{1}^{i_{1}}\cdots \overline{X}_{k}^{i_{k}}\left|\overline{00\ldots 0}\right\rangle$$

Canonical Basis

- fix logical operators \overline{X}_j and \overline{Z}_j
- the stabilizer S and the logical operators \overline{Z}_j mutually commute
- the logical state $|\overline{00\dots 0}\rangle$ fixed by ${\cal S}$ and all \overline{Z}_j is a stabilizer state
- define the (logical) basis states as

$$\left|\overline{i_{1}i_{2}\ldots i_{k}}\right\rangle = \overline{X}_{1}^{i_{1}}\cdots \overline{X}_{k}^{i_{k}}\left|\overline{00\ldots 0}\right\rangle$$

generalization: union stabilizer codes

• take the vector space sum of several subspaces from the decomposition

$$|\overline{j};\overline{i_1i_2\ldots i_k}\rangle = t_j\overline{X}_1^{i_1}\cdots\overline{X}_k^{i_k}|\overline{00\ldots 0}\rangle$$

• corresponds to the union of cosets $C^{\star} + t_j$ of the normalizer code C^{\star}



Example: Five Qubit Code $\llbracket 5, 1, 3 \rrbracket$

$$\begin{pmatrix} X & X & Z & I & Z \\ Z & X & X & Z & I \\ I & Z & X & X & Z \\ Z & I & Z & X & X \\ \hline I & I & Z & Y & Z \\ \hline I & I & Z & X & X \end{pmatrix} \hat{=} \begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 \\ \hline 0 & 0 & 0 & 1 & 1 \\ \hline 0 & 0 & 0 & 1 & 0 & 1 \\ \hline 0 & 0 & 0 & 1 & 0 & 1 \\ \hline 0 & 0 & 0 & 1 & 0 & 1 \\ \hline 0 & 0 & 0 & 1 & 0 & 1 \\ \hline 0 & 0 & 0 & 1 & 0 & 0 \\ \hline 0 & 0 & 0 & 1 & 0 & 0 \\ \hline 0 & 0 & 0 & 1 & 0 & 0 \\ \hline 0 & \omega & 1 & 1 & \omega & 0 \\ \hline 0 & \omega & 1 & 1 & \omega & 0 \\ \hline 0 & \omega & 0 & \omega & 1 & 1 \\ \hline 0 & 0 & 0 & 0 & 1 & 0 \\ \hline 0 & 0 & 0 & 1 & 0 \\ \hline 0 & 0 & 0 & 0 & 1 & 0 \\ \hline \end{pmatrix}$$

Graphical Quantum Codes

[D. Schlingemann & R. F. Werner: QECC associated with graphs, PRA **65** (2002), quant-ph/0012111] [Grassl, Klappenecker & Rötteler: Graphs, Quadratic Forms, & QECC, ISIT 2002, quant-ph/0703112]

Basic idea

- given $C \leq C^{\star}$, we can find D with $C \leq D = D^{*} \leq C^{\star}$
- D is a classical symplectic self-dual code defining a single quantum state $C_0 = [\![n, 0, d]\!]_q$
- the standard form of the stabilizer matrix is (I|A)
- self-duality implies that A is symmetric
- A can be considered as adjacency matrix of a graph with n vertices
- logical X-operators give rise to more quantum states in the code $\mathcal{C} = [\![n,k,d']\!]_q$
- use additionally k input vectices

Graphical Representation of $\llbracket 6, 2, 3 \rrbracket_3$

(1	0	0	0	0	0	0	0	0	1	0	2
	0	1	0	0	0	0	0	0	1	2	2	2
	0	0	1	0	0	0	0	1	0	2	0	1
	0	0	0	1	0	0	1	2	2	0	0	0
	0	0	0	0	1	0	0	2	0	0	0	2
	0	0	0	0	0	1	2	2	1	0	2	0
	0	0	0	0	0	0	1	0	1	1	0	0
	0	0	0	0	0	0	1	0	0	0	2	$1 \int$

stabilizer & logical X-operators



graphical representation

Encoder based on Graphical Representation

[M. Grassl, Variations on Encoding Circuits for Stabilizer Quantum Codes, LNCS 6639, pp. 142–158, 2011]



The Graphical Representation is not Unique

There are four non-isomorphic graphs which yield graphical quantum codes that are equivalent to Steane's CSS code $[7, 1, 3]_2$:



The graphs are related by *local complementation*.

CSS-like Codes from Non-linear Codes

recall: CSS codes

basis states

$$|\boldsymbol{x}_i + C_2^{\perp}\rangle := rac{1}{\sqrt{|C_2^{\perp}|}} \sum_{\boldsymbol{y} \in C_2^{\perp}} |\boldsymbol{x}_i + \boldsymbol{y}\rangle,$$

where $oldsymbol{x}_i$ are representatives of C_1/C_2^\perp

generalization:

basis states

$$|S_i\rangle := \frac{1}{\sqrt{|S_i|}} \sum_{\boldsymbol{c} \in S} |\boldsymbol{c}\rangle,$$

where S_i are some disjoint sets of codewords

Lemma

$$\min_{i \neq j} \operatorname{dist}(S_i, S_j) \ge d \Longrightarrow \text{distance } d \text{ with respect to } X \text{-errors}$$

CSS-like Codes: Phase Errors

• phase errors correspond to measurements:

 $I = P_0 + P_1 = |0\rangle\langle 0| + |1\rangle\langle 1| \quad Z = P_0 - P_1 = |0\rangle\langle 0| - |1\rangle\langle 1|$

- distance d with respect to Z-errors if measuring d-1 positions does not reveal information about the quantum state
- probability of measurement result $x = x_{i_1} \dots x_{i_{d-1}}$ is proportional to the number of words in S_j with x at the corresponding positions
- measurement result is completely random if all possible strings x appear equally often

Lemma (see also [Feng, Ling & Xing, IEEE-IT **52** (2006)]) each S_j is an OA of strength $d - 1 \Longrightarrow$ distance d with respect to Z-errors

Example: \mathbb{Z}_4 -linear Quantum Codes

[Ling & Solé, "Nonadditive Quantum Codes from \mathbb{Z}_4 -Codes", preprint hal-00338309, (2008)]

Theorem Suppose $C \subset C'$ are two linear \mathbb{Z}_4 -codes of length n with $|C| = 4^{k_1} 2^{k_2}$ and $|C'| = 4^{k'_1} 2^{k'_2}$.

Then there exists a quantum code $((2n, K, d))_2$ with $K = 2^{2k_1+k_2-2k'_1-k'_2}$ and $d \ge \min\{d_{\mathsf{Lee}}(C' \setminus C), d_{\mathsf{Lee}}(C^{\perp})\}.$

Examples:

- $((64, 2^{10}, 12))_2$ from the Calderbank-McGuire code $C' = (32, 2^{37}, 12)_{\mathbb{Z}_4}$ and a subcode $C = (32, 2^{27})_{\mathbb{Z}_4}$ with dual distance $d_{\text{Lee}}(C^{\perp}) = 12$
- CSS-like codes from Goethals/Preparata codes, but better codes can be obtained using union stabilizer codes ([Grassl & Rötteler, ISIT 2008])

An Improved Family of Non-Additive Codes

[Grassl & Rötteler, ISIT 2008]

- Steane's enlargement construction applied to C[⊥]_G ⊂ C_G ⊂ C_P, where C_G and C_P are linear subcodes of the Goethals and Preparata codes, yields
 C₀ = [[2^m, 2^m 7m + 3, 8]]
- using the translations $\mathcal{T}_0 = \{(t^{(1)}|t^{(2)}): t^{(1)}, t^{(2)} \in \mathcal{T}\}$ we obtain a union stabilizer code $\mathcal{C} = ((2^m, 2^{2^m 5m + 1}, 8))$
- the best stabilizer code known to us has parameters $[\![2^m,2^m-5m-2,8]\!]$

Reed-Muller	Goethals	BCH	Goethals-Preparata
$[\![64, 20, 8]\!]$	$((64, 2^{30}, 8))$	$[\![64, 32, 8]\!]$	$(\!(64, 2^{35}, 8)\!)$
$[\![256, 182, 8]\!]$	$(\!(256,2^{210},8)\!)$	$[\![256, 214, 8]\!]$	$(\!(256,2^{217},8)\!)$
$[\![1024,912,8]\!]$	$((1024, 2^{966}, 8))$	$[\![1024, 972, 8]\!]$	$(\!(1024,2^{975},8)\!)$