## 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


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

## Quantum Information (I)

## Quantum-bit (qubit)

basis states:

$$
" 0 " \hat{=}|0\rangle=\binom{1}{0} \in \mathbb{C}^{2}, \quad " 1 " \hat{=}|1\rangle=\binom{0}{1} \in \mathbb{C}^{2}
$$

general state:

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

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:

$$
\left|b_{1}\right\rangle \otimes \ldots \otimes\left|b_{n}\right\rangle=:\left|b_{1} \ldots b_{n}\right\rangle=|\boldsymbol{b}\rangle \quad \text { where } b_{i} \in\{0,1\}
$$

general state:

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

$\longrightarrow$ normalized vector in $\left(\mathbb{C}^{2}\right)^{\otimes n} \cong \mathbb{C}^{2^{n}}$
basis vectors are labelled by bitstrings $x$
partial measurement of first qubit, e.g., result " 0 ":

$$
\left|\psi^{\prime}\right\rangle=\alpha\left(|0\rangle\langle 0| \otimes I_{2} \otimes \cdots \otimes I_{2}\right)|\psi\rangle=\alpha \sum_{\boldsymbol{y} \in\{0,1\}^{n-1}} c_{0 \boldsymbol{y}}|0 y\rangle
$$

## 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 $U \in S U(2)$
- "controlled NOT operation"

$$
\left(\begin{array}{llll}
1 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 \\
0 & 0 & 0 & 1 \\
0 & 0 & 1 & 0
\end{array}\right) \hat{=} \hat{=}|x\rangle|y\rangle \mapsto|x\rangle|x+y\rangle
$$

## Quantum Information (IV)

## Mixed States

- ensemble of quantum states $\left|\psi_{i}\right\rangle$ with probabilities $p_{i}$
- modelled by density matrix

$$
\rho=\sum_{i} p_{i}\left|\psi_{i}\right\rangle\left\langle\psi_{i}\right|
$$

where $\left|\psi_{i}\right\rangle\left\langle\psi_{i}\right|$ is the projector onto the state $\left|\psi_{i}\right\rangle$

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

$$
\rho=\left(\begin{array}{cc}
|\alpha|^{2} & 0 \\
0 & |\beta|^{2}
\end{array}\right)
$$

## Interaction System/Environment

## "Closed" System


"Channel"

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

$$
\text { with Kraus operators (error operators) } E_{i}
$$

## Local/low correlated errors

- product channel $\mathrm{Q}^{\otimes n}$ 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 $\mathcal{C}$ of a complex vector space $\mathcal{H} \cong \mathbb{C}^{N}$ usually: $\mathcal{H} \cong \mathbb{C}^{m} \otimes \mathbb{C}^{m} \otimes \ldots \otimes \mathbb{C}^{m}=:\left(\mathbb{C}^{m}\right)^{\otimes n} \quad$ " $n$ qudits"
- errors: described by linear transformations acting on
- some of the subsystems (local errors)
- many subsystems in the same way (correlated errors)
- notation: $\mathcal{C}=\llbracket n, k, d \rrbracket_{q}=\left(\left(n, q^{k}, d\right)\right)_{q}$ $q^{k}$-dimensional subspace $\mathcal{C}$ of $\left(\mathbb{C}^{q}\right)^{\otimes n}$
- 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 $d-1$ known subsystems


## Basic Ideas

## partitioning of all words

## orthogonal decomposition

- combinatorics
- (linear) algebra

- codewords
-     - bounded weight errors
- other errors

$$
\left(\mathbb{C}^{q}\right)^{\otimes n}=\mathcal{H}_{\mathcal{C}} \oplus \mathcal{H}_{\mathcal{E}_{1}} \oplus \ldots \oplus \mathcal{H}_{\mathcal{E}_{i}} \oplus \ldots
$$

## Characterization of QECCs

## QECC Characterization

[Knill \& Laflamme, Phyical Review A 55, 900-911 (1997)]
A subspace $\mathcal{C}$ of $\mathcal{H}$ with orthonormal basis $\left\{\left|c_{1}\right\rangle, \ldots,\left|c_{K}\right\rangle\right\}$ is an error-correcting code for the error operators $\mathcal{E}=\left\{E_{1}, E_{2}, \ldots\right\}$, if there exists constants $\alpha_{k, l} \in \mathbb{C}$ such that for all $\left|c_{i}\right\rangle,\left|c_{j}\right\rangle$ and for all $E_{k}, E_{l} \in \mathcal{E}$ :

$$
\begin{equation*}
\left\langle c_{i}\right| E_{k}^{\dagger} E_{l}\left|c_{j}\right\rangle=\delta_{i, j} \alpha_{k, l} . \tag{1}
\end{equation*}
$$

It is sufficient that (1) holds for a vector space basis of $\mathcal{E}$.
$\Longrightarrow$ 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 $X=\left(\begin{array}{ll}0 & 1 \\ 1 & 0\end{array}\right)$

Phase-flip error:

- Inverts the relative phase of $|0\rangle$ and $|1\rangle$. Has no classical analogue!
- Given by the matrix $Z=\left(\begin{array}{rr}1 & 0 \\ 0 & -1\end{array}\right)$


## Combination:

- Combining bit-flip and phase-flip gives $Y=\left(\begin{array}{rr}0 & -1 \\ 1 & 0\end{array}\right)=X Z$.


## Pauli and Hadamard Matrices

"Pauli" matrices:

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

Hadamard matrix: $H=\frac{1}{\sqrt{2}}\left(\begin{array}{rr}1 & 1 \\ 1 & -1\end{array}\right)$

Important properties:

- $H^{\dagger} X H=Z, \quad$ " $H$ changes bit-flips to phase-flips"
- $Z X=\left(\begin{array}{rr}0 & 1 \\ -1 & 0\end{array}\right)=-Y=-X Z, \quad " X$ 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,

$$
\text { e.g. }|\psi\rangle=\alpha|0\rangle+\beta|1\rangle \mapsto|\psi\rangle|\psi\rangle|\psi\rangle
$$

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 $|0\rangle\left|\psi_{\text {blank }}\right\rangle \mapsto|0\rangle|0\rangle,|1\rangle\left|\psi_{\text {blank }}\right\rangle \mapsto|1\rangle|1\rangle$, and hence

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



Contradiction to the linearity of quantum mechanics!

## Simple Quantum Error-Correcting Code

Repetition code: $\quad|0\rangle \mapsto|000\rangle,|1\rangle \mapsto|111\rangle$
Encoding of one qubit:

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

This defines a two-dimensional subspace $\mathcal{H}_{C} \leq \mathcal{H}_{2} \otimes \mathcal{H}_{2} \otimes \mathcal{H}_{2}$

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

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
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:

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

## Simple Quantum Error-Correcting Code

| phase-flip | quantum state | subspace |
| :---: | :---: | :---: |
| no error | $\begin{array}{r} \frac{\alpha}{2}(\|000\rangle+\|011\rangle+\|101\rangle+\|110\rangle) \\ +\frac{\beta}{2}(\|001\rangle+\|010\rangle+\|100\rangle+\|111\rangle) \end{array}$ | $(\mathbb{1} \otimes \mathbb{1} \otimes \mathbb{1}) \mathcal{H}_{\mathcal{C}}$ |
| $1^{\text {st }}$ position | $\begin{array}{r} \frac{\alpha}{2}(\|000\rangle+\|011\rangle-\|101\rangle-\|110\rangle) \\ +\frac{\beta}{2}(\|001\rangle+\|010\rangle-\|100\rangle-\|111\rangle) \end{array}$ | $(Z \otimes \mathbb{1} \otimes \mathbb{1}) \mathcal{H}_{\mathcal{C}}$ |
| $2^{\text {nd }}$ position | $\begin{array}{r} \frac{\alpha}{2}(\|000\rangle-\|011\rangle+\|101\rangle-\|110\rangle) \\ +\frac{\beta}{2}(\|001\rangle-\|010\rangle+\|100\rangle-\|111\rangle) \end{array}$ | $(\mathbb{1} \otimes Z \otimes \mathbb{1}) \mathcal{H}_{\mathcal{C}}$ |
| $3^{\text {rd }}$ position | $\begin{gathered} \frac{\alpha}{2}(\|000\rangle-\|011\rangle-\|101\rangle+\|110\rangle) \\ -\frac{\beta}{2}(\|001\rangle+\|010\rangle+\|100\rangle-\|111\rangle) \end{gathered}$ | $(\mathbb{1} \otimes \mathbb{1} \otimes Z) \mathcal{H}_{\mathcal{C}}$ |

We again obtain an orthogonal decomposition of $\mathcal{H}_{2} \otimes \mathcal{H}_{2} \otimes \mathcal{H}_{2}$

## Shor's Nine-Qubit Code $\left[9,1,3 \rrbracket_{2}\right.$

Bit-flip code: $\quad|0\rangle \mapsto|000\rangle, \quad|1\rangle \mapsto|111\rangle$
Phase-flip code: $\quad|0\rangle \mapsto|+++\rangle, \quad|1\rangle \mapsto|---\rangle$
Effect of single-qubit errors on the bit-flip code:

- $X$-errors change the basis states, but can be corrected
- Z-errors at any of the three positions:

$$
\left.\begin{array}{rlr}
Z|000\rangle & = & |000\rangle \\
Z|111\rangle & = & -|111\rangle
\end{array}\right\} \text { "encoded" } Z \text {-operator }
$$

$\Longrightarrow$ bit-flip code \& error correction convert the channel into a phase-error channel
$\Longrightarrow$ Concatenation of bit-flip code and phase-flip code yields $\llbracket 9,1,3 \rrbracket_{2}$

## Bit-flips and Phase-flips

Let $C \leq \mathbb{F}_{2}^{n}$ be a linear code. Then the image of the state

$$
\frac{1}{\sqrt{|C|}} \sum_{c \in C}|c\rangle
$$

under a bit-flip $\boldsymbol{x} \in \mathbb{F}_{2}^{n}$ and a phase-flip $\boldsymbol{z} \in \mathbb{F}_{2}^{n}$ is given by

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

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

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

## 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 $C_{1}=\left[n, k_{1}, d_{1}\right]$ and $C_{2}=\left[n, k_{2}, d_{2}\right]$ be classical linear codes with $C_{2}^{\perp} \leq C_{1}$. Let $\left\{x_{1}, \ldots, x_{K}\right\}$ be representatives for the cosets $C_{1} / C_{2}^{\perp}$. Define quantum states

$$
\left|x_{i}+C_{2}^{\perp}\right\rangle:=\frac{1}{\sqrt{\left|C_{2}^{\perp}\right|}} \sum_{\boldsymbol{y} \in C_{2}^{\perp}}\left|x_{i}+\boldsymbol{y}\right\rangle
$$

Theorem: The vector space $\mathcal{C}$ spanned by these states is a quantum code with parameters $\llbracket n, k_{1}+k_{2}-n, d \rrbracket$ where $d \geq \min \left(d_{1}, d_{2}\right)$.

## CSS Codes - how they work

Basis states:

$$
\left|\boldsymbol{x}_{i}+C_{2}^{\perp}\right\rangle=\frac{1}{\sqrt{\left|C_{2}^{\perp}\right|}} \sum_{\boldsymbol{y} \in C_{2}^{\perp}}\left|\boldsymbol{x}_{i}+\boldsymbol{y}\right\rangle
$$

Suppose a bit-flip error $\boldsymbol{b}$ happens to $\left|\boldsymbol{x}_{i}+C_{2}^{\perp}\right\rangle$ :

$$
\frac{1}{\sqrt{\left|C_{2}^{\perp}\right|}} \sum_{\boldsymbol{y} \in C_{2}^{\perp}}\left|\boldsymbol{x}_{i}+\boldsymbol{y}+\boldsymbol{b}\right\rangle
$$

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 $\boldsymbol{x} \in C_{1}$.

$$
\frac{1}{\sqrt{\left|C_{2}^{\perp}\right|}} \sum_{\boldsymbol{y} \in C_{2}^{\perp}}\left|\boldsymbol{x}_{i}+\boldsymbol{y}+\boldsymbol{b}\right\rangle\left|\left(\boldsymbol{x}_{i}+\boldsymbol{y}+\boldsymbol{b}\right) H_{1}^{t}\right\rangle=\frac{1}{\sqrt{\left|C_{2}^{\perp}\right|}} \sum_{\boldsymbol{y} \in C_{2}^{\perp}}|\underbrace{\boldsymbol{x}_{i}+\boldsymbol{y}}_{\in C_{1}}+\boldsymbol{b}\rangle\left|\boldsymbol{b} H_{1}^{t}\right\rangle
$$

Then measure the ancilla to obtain $s=\boldsymbol{b} H_{1}^{t}$. Use this to correct the error by a conditional operation which flips the bits in $\boldsymbol{b}$.

Phase-flips: Suppose we have the state

$$
\frac{1}{\sqrt{\left|C_{2}^{\perp}\right|}} \sum_{\boldsymbol{y} \in C_{2}^{\perp}}(-1)^{\left(\boldsymbol{x}_{i}+\boldsymbol{y}\right) \cdot \boldsymbol{z}}\left|\boldsymbol{x}_{i}+\boldsymbol{y}\right\rangle
$$

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 $\llbracket 7,1,3 \rrbracket_{2}$

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

$$
G=\left(\begin{array}{lllllll}
0 & 0 & 1 & 0 & 1 & 1 & 1 \\
0 & 1 & 0 & 1 & 1 & 1 & 0 \\
1 & 0 & 0 & 1 & 0 & 1 & 1
\end{array}\right)
$$

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

$$
G^{\prime}=\left(\begin{array}{lllllll}
0 & 0 & 0 & 1 & 1 & 0 & 1 \\
\hline 0 & 0 & 1 & 0 & 1 & 1 & 1 \\
0 & 1 & 0 & 1 & 1 & 1 & 0 \\
1 & 0 & 0 & 1 & 0 & 1 & 1
\end{array}\right)
$$



## 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 $C_{2}+\boldsymbol{t}_{i} \subset C_{1}$ $\Longrightarrow$ dimension of the code is $\left|C_{1}\right| /\left|C_{2}\right|$
- $X$-errors are corrected using $C_{1}=\left[n, k_{1}, d_{1}\right]_{q}$
- $Z$-errors are corrected using the Euclidean dual $C_{2}^{\perp}=\left[n, n-k_{2}, d_{2}^{\perp}\right]_{q}$
$\Longrightarrow \mathcal{C}=\llbracket n, k_{1}-k_{2}, \geq \min \left(d_{1}, d_{2}^{\perp}\right) \rrbracket_{q}$
- we can do (slightly) better if $\operatorname{wgt}\left(C_{1} \backslash C_{2}\right)>\operatorname{wgt}\left(C_{1}\right)$ or $\operatorname{wgt}\left(C_{2}^{\perp} \backslash C_{1}^{\perp}\right)>\operatorname{wgt}\left(C_{2}^{\perp}\right)$
- 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)]

$$
\mathcal{E}=\left\{X^{\alpha} Z^{\beta}: \alpha, \beta \in \mathbb{F}_{q}\right\}
$$

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

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

## Stabilizer Codes

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

$$
\omega^{\gamma}\left(X^{\alpha_{1}} Z^{\beta_{1}}\right) \otimes\left(X^{\alpha_{2}} Z^{\beta_{2}}\right) \otimes \ldots \otimes\left(X^{\alpha_{n}} Z^{\beta_{n}}\right)=: \omega^{\gamma} X^{\alpha} Z^{\beta}
$$

where $\boldsymbol{\alpha}, \boldsymbol{\beta} \in \mathbb{F}_{q}^{n}, \gamma \in \mathbb{F}_{p}$.

## quotient group:

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

$\mathcal{S}$ Abelian subgroup

$$
\begin{array}{r}
\Longleftrightarrow(\boldsymbol{\alpha}, \boldsymbol{\beta}) \star\left(\boldsymbol{\alpha}^{\prime}, \boldsymbol{\beta}^{\prime}\right)=0 \text { for all } \omega^{\gamma}\left(x^{\boldsymbol{\alpha}} Z^{\boldsymbol{\beta}}\right), \omega^{\gamma^{\prime}}\left(x^{\boldsymbol{\alpha}^{\prime}} Z^{\boldsymbol{\beta}^{\prime}}\right) \in \mathcal{S} \\
\text { where } \star \text { is a symplectic inner product on } \mathbb{F}_{q}^{n} \times \mathbb{F}_{q}^{n} .
\end{array}
$$

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

$$
(\boldsymbol{v}, \boldsymbol{w}) \star\left(\boldsymbol{v}^{\prime}, \boldsymbol{w}^{\prime}\right):=\operatorname{tr}\left(\boldsymbol{v} \cdot \boldsymbol{w}^{\prime}-\boldsymbol{v}^{\prime} \cdot \boldsymbol{w}\right)=\operatorname{tr}\left(\sum_{i=1}^{n} v_{i} w_{i}^{\prime}-v_{i}^{\prime} w_{i}\right)
$$

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

$$
(\boldsymbol{v}, \boldsymbol{w}) \star\left(\boldsymbol{v}^{\prime}, \boldsymbol{w}^{\prime}\right):=\boldsymbol{v} \cdot \boldsymbol{w}^{\prime}-\boldsymbol{v}^{\prime} \cdot \boldsymbol{w}=\sum_{i=1}^{n} v_{i} w_{i}^{\prime}-v_{i}^{\prime} w_{i}
$$

$\mathbb{F}_{q^{2}}$-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 $d:=\min \left\{\operatorname{wgt}(\boldsymbol{c}): \boldsymbol{c} \in C^{\star} \backslash C\right\}$.
Then there is a stabilizer code $\mathcal{C}=\llbracket n, k, d \rrbracket_{q}$.

## Special cases:

- $C=C_{1}^{\perp} \times C_{2}^{\perp}$ with linear codes $C_{1}, C_{2}$ over $\mathbb{F}_{q}, C_{2}^{\perp} \subset C_{1}$, $d=\min \left\{\operatorname{wgt}\left(C_{1} \backslash C_{2}^{\perp}\right), \operatorname{wgt}\left(C_{2} \backslash C_{1}^{\perp}\right)\right\}$
Calderbank-Shor-Steane (CSS) codes
- $C=C_{1} \times C_{1}$ with a self-orthogonal linear code $C_{1} \subset C_{1}^{\perp}$ over $\mathbb{F}_{q}$
- $C=\left\{(\boldsymbol{v}, \boldsymbol{w}): \boldsymbol{v}+\gamma \boldsymbol{w} \in C_{1}\right\}$ where $C_{1}$ is a Hermitian self-orthogonal linear code over $\mathbb{F}_{q^{2}}$ (with some particular $\gamma \in \mathbb{F}_{q^{2}} \backslash \mathbb{F}_{q}$ )


## Quantum Singleton Bound

[E. Rains, Nonbinary Quantum Codes, IEEE-IT 45, pp. 1827-1832 (1999)]
general bound on the minimum distance of $\mathcal{C}=\llbracket n, k, d \rrbracket_{q}$ :

$$
\begin{equation*}
2 d \leq n-k+2 \tag{2}
\end{equation*}
$$

## Quantum MDS codes:

quantum codes with equality in (2)
Minimum distance of a stabilizer code:

$$
\begin{equation*}
\mathrm{d}_{\min }(\mathcal{C}):=\min \left\{\operatorname{wgt}(\boldsymbol{c}): \boldsymbol{c} \in C^{\star} \backslash C\right\} \geq \mathrm{d}_{\min }\left(C^{\star}\right) \tag{3}
\end{equation*}
$$

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

$$
g=X^{a_{1}} Z^{b_{1}} \otimes \ldots \otimes X^{a_{n}} Z^{b_{n}} \quad\left(a_{j}, b_{j} \in\{0,1\}\right)
$$

- $g$ corresponds to a binary vector $(\boldsymbol{a} \mid \boldsymbol{b})$ of length $2 n$ or a vector $\boldsymbol{v}=\boldsymbol{a}+\omega \boldsymbol{b}$ of length $n$ over $G F(4)=\left\{0,1, \omega, \omega^{2}\right\}$
- the product of two elements $g$ and $h$ given by $\boldsymbol{v}=\boldsymbol{a}+\boldsymbol{\omega} \boldsymbol{b}$ and $\boldsymbol{w}=\boldsymbol{c}+\omega \boldsymbol{d}$ corresponds to $\boldsymbol{v}+\boldsymbol{w}=(\boldsymbol{a}+\boldsymbol{c})+\omega(\boldsymbol{b}+\boldsymbol{d})$
- two elements $g$ and $h$ given by $\boldsymbol{v}=\boldsymbol{a}+\omega \boldsymbol{b}$ and $\boldsymbol{w}=\boldsymbol{c}+\omega \boldsymbol{d}$ commute iff

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

- the weight of $g$ equals the Hamming weight of $v$


## Stabilizer Codes \& Classical Codes

- a stabilizer code $\mathcal{C}=\llbracket n, k, d \rrbracket$ is the joint +1 -eigenspace of the stabilizer group $\mathcal{S}=\left\langle S_{1}, \ldots, S_{n-k}\right\rangle$
- the normalizer $\mathcal{N}$ is generated by $\mathcal{S}$ and logical operators $\bar{X}_{1}, \ldots, \bar{X}_{k}$, $\bar{Z}_{1}, \ldots, \bar{Z}_{k}$,
- the stabilizer $\mathcal{S}$ corresponds to a self-orthogonal additive code $C=\left(n, 2^{n-k}\right)$ over $G F(4)$
- the normalizer $\mathcal{N}$ corresponds to the symplectic dual code $C^{\star}=\left(n, 2^{n+k}\right)$
- the minimum distance $d$ of $\mathcal{C}$ is given by

$$
d=\min \left\{\operatorname{wgt}(\boldsymbol{v}): \boldsymbol{v} \in C^{\star} \backslash C\right\}
$$

## Stabilizer and Normalizer

 stabilizer state $\left\{\left(\begin{array}{c|c}S_{1}^{X} & S_{1}^{Z} \\ \vdots & \vdots \\ S_{n-k}^{X} & S_{n-k}^{Z} \\ \hline \bar{Z}_{1}^{X} & \bar{Z}_{1}^{Z} \\ \vdots & \vdots \\ \bar{Z}_{k}^{X} & \bar{Z}_{k}^{Z} \\ ----- & ----- \\ \bar{X}_{1}^{X} & \bar{X}_{1}^{Z} \\ \vdots & \vdots \\ \bar{X}_{k}^{X} & \bar{X}_{k}^{Z}\end{array}\right)\right.$ stabilizer
## Canonical Basis

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

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

## Canonical Basis

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

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

## generalization: union stabilizer codes

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

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

- corresponds to the union of cosets $C^{\star}+\boldsymbol{t}_{j}$ of the normalizer code $C^{\star}$


## Stabilizer, Normalizer \& Translations



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

$$
\begin{aligned}
& \hat{=}\left(\begin{array}{ccccc}
1 & 1 & \omega & 0 & \omega \\
\omega & 1 & 1 & \omega & 0 \\
0 & \omega & 1 & 1 & \omega \\
\omega & 0 & \omega & 1 & 1 \\
\hline \frac{0}{0}-\frac{0}{0} & -\frac{\omega}{1} & -\frac{\omega^{2}}{\omega}-\frac{\omega}{1}
\end{array}\right)
\end{aligned}
$$

## 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 $\mathcal{C}_{0}=\llbracket n, 0, d \rrbracket_{q}$
- the standard form of the stabilizer matrix is $(I \mid A)$
- 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 $\mathcal{C}=\llbracket n, k, d^{\prime} \rrbracket_{q}$
- use additionally $k$ input vectices


## Graphical Representation of $\llbracket 6,2,3 \rrbracket_{3}$

$$
\left(\begin{array}{llllll|lllll}
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0
\end{array}\right)
$$

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 $\llbracket 7,1,3 \rrbracket_{2}$ :



The graphs are related by local complementation.

## CSS-like Codes from Non-linear Codes

recall: CSS codes
basis states

$$
\left|\boldsymbol{x}_{i}+C_{2}^{\perp}\right\rangle:=\frac{1}{\sqrt{\left|C_{2}^{\perp}\right|}} \sum_{\boldsymbol{y} \in C_{2}^{\perp}}\left|\boldsymbol{x}_{i}+\boldsymbol{y}\right\rangle
$$

where $\boldsymbol{x}_{i}$ are representatives of $C_{1} / C_{2}^{\perp}$

## generalization:

basis states

$$
\left|S_{i}\right\rangle:=\frac{1}{\sqrt{\left|S_{i}\right|}} \sum_{c \in S}|\boldsymbol{c}\rangle
$$

where $S_{i}$ are some disjoint sets of codewords
Lemma

$$
\min _{i \neq j} \operatorname{dist}\left(S_{i}, S_{j}\right) \geq d \Longrightarrow \text { distance } d \text { with respect to } X \text {-errors }
$$

## 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 $\boldsymbol{x}=x_{i_{1}} \ldots x_{i_{d-1}}$ is proportional to the number of words in $S_{j}$ with $\boldsymbol{x}$ at the corresponding positions
- measurement result is completely random if all possible strings $\boldsymbol{x}$ 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 $C \subset C^{\prime}$ are two linear $\mathbb{Z}_{4}$-codes of length $n$ with $|C|=4^{k_{1}} 2^{k_{2}}$ and $\left|C^{\prime}\right|=4^{k_{1}^{\prime}} 2^{k_{2}^{\prime}}$.
Then there exists a quantum code $((2 n, K, d))_{2}$ with $K=2^{2 k_{1}+k_{2}-2 k_{1}^{\prime}-k_{2}^{\prime}}$ and $d \geq \min \left\{d_{\text {Lee }}\left(C^{\prime} \backslash C\right), d_{\text {Lee }}\left(C^{\perp}\right)\right\}$.

## Examples:

- $\left(\left(64,2^{10}, 12\right)\right)_{2}$ from the Calderbank-McGuire code $C^{\prime}=\left(32,2^{37}, 12\right)_{\mathbb{Z}_{4}}$ and a subcode $C=\left(32,2^{27}\right)_{\mathbb{Z}_{4}}$ with dual distance $d_{\text {Lee }}\left(C^{\perp}\right)=12$
- 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 $C_{\mathcal{G}}^{\perp} \subset C_{\mathcal{G}} \subset C_{\mathcal{P}}$, where $C_{\mathcal{G}}$ and $C_{\mathcal{P}}$ are linear subcodes of the Goethals and Preparata codes, yields $\mathcal{C}_{0}=\llbracket 2^{m}, 2^{m}-7 m+3,8 \rrbracket$
- using the translations $\mathcal{T}_{0}=\left\{\left(t^{(1)} \mid t^{(2)}\right): t^{(1)}, t^{(2)} \in \mathcal{T}\right\}$ we obtain a union stabilizer code $\mathcal{C}=\left(\left(2^{m}, 2^{2^{m}-5 m+1}, 8\right)\right)$
- the best stabilizer code known to us has parameters $\llbracket 2^{m}, 2^{m}-5 m-2,8 \rrbracket$

| Reed-Muller | Goethals | BCH | Goethals-Preparata |
| :---: | :---: | :---: | :---: |
| $\llbracket 64,20,8 \rrbracket$ | $\left(\left(64,2^{30}, 8\right)\right)$ | $\llbracket 64,32,8 \rrbracket$ | $\left(\left(64,2^{35}, 8\right)\right)$ |
| $\llbracket 256,182,8 \rrbracket$ | $\left(\left(256,2^{210}, 8\right)\right)$ | $\llbracket 256,214,8 \rrbracket$ | $\left(\left(256,2^{217}, 8\right)\right)$ |
| $\llbracket 1024,912,8 \rrbracket$ | $\left(\left(1024,2^{966}, 8\right)\right)$ | $\llbracket 1024,972,8 \rrbracket$ | $\left(\left(1024,2^{975}, 8\right)\right)$ |

