DIMACS

Center for Discrete Mathematics and Theoretical Computer Science

A National Science Foundation Science and Technology Center

Workshop on Codes and Association Schemes

November 9–12, 1999

An ensemble of properties of classical codes useful for quantum codes

Markus Grassl

Arbeitsgruppe *Quantum Computing*

Prof. Thomas Beth

Institut für Algorithmen und Kognitive Systeme

Universität Karlsruhe, Germany

Overview

1. A combinatorial identity
   - quantum error-correcting codes
   - quantum jumps
   - Theorem 1
2. Doubly-even codes
   - fault tolerant quantum computation
   - Theorem 2
3. Weakly self-dual codes
   - self-dual bases
   - subfield expansion
   - Theorem 3
   - quantum Reed-Solomon codes

CSS Codes

(Calderbank & Shor/Steane)

Definition:

Let $C = [n, k, d]$ be a weakly self-dual linear binary code, i. e., $C \leq C^\perp$, where $C^\perp = [n, n-k, d^\perp]$.

For coset representatives $\boldsymbol{w} \in C^\perp/C$, define

$$|\psi_{\boldsymbol{w}}\rangle := \frac{1}{\sqrt{|C|}} \sum_{\boldsymbol{c} \in C} |\boldsymbol{c} + \boldsymbol{w}\rangle$$

or equivalently (Hadamard transformation)

$$|\widehat{\psi}_{\boldsymbol{w}}\rangle := \frac{1}{\sqrt{|C^\perp|}} \sum_{\boldsymbol{c} \in C^\perp} (-1)^{\boldsymbol{c}\cdot\boldsymbol{w}} |\boldsymbol{c}\rangle$$

$\Longrightarrow$ quantum error-correcting code

$$\mathcal{C} = [[n, n-2k, d' \geq d^\perp]]$$

Some Physics: Spontaneous Emission

Quantum jump

$$\begin{tikzcd} |1\rangle \arrow[r] \arrow[dr] & |1\rangle \\ |0\rangle \arrow[r] & |0\rangle \end{tikzcd}$$

(cf. “Z channel”)

Effective Hamiltonian (no jump)

$$H_{\mathsf{eff}} = \sum_{\nu=1}^{n} -i\hbar\,\Gamma\,|1\rangle_\nu\langle 1|_\nu$$

Effective time evolution

$$U_{\mathsf{eff}}(t) = \exp\left(-iH_{\mathsf{eff}}\,t/\hbar\right) = \prod_{\nu=1}^{n} \exp\left(-t\,\Gamma\,|1\rangle_\nu\langle 1|_\nu\right)$$

Effect on CSS Codes (I)

$$
\begin{aligned}
E_{\boldsymbol{w},\boldsymbol{w}'}(t) := \langle\widehat{\psi}_{\boldsymbol{w}'}|U_{\mathsf{eff}(t)}|\widehat{\psi}_{\boldsymbol{w}}\rangle &= \sum_{\boldsymbol{c}\in C^\perp}(-1)^{\boldsymbol{c}\cdot(\boldsymbol{w}+\boldsymbol{w}')}e^{-t\,\Gamma\,\mathrm{wgt}\,\boldsymbol{c}}\\
&= \sum_{j=0}^{\infty}\frac{(-\Gamma)^j}{j!}t^j\underbrace{\sum_{\boldsymbol{c}\in C^\perp}(-1)^{\boldsymbol{c}\cdot(\boldsymbol{w}+\boldsymbol{w}')}(\mathrm{wgt}\,\boldsymbol{c})^j}_{(*)}
\end{aligned}
$$

$E_{\boldsymbol{w},\boldsymbol{w}'}(t)$ should be proportional to identity (up to some high order in t).

diagonal terms: $\boldsymbol{w}=\boldsymbol{w}' \Longrightarrow (*)$ independent of $\boldsymbol{w}$

off-diagonal terms: When does $\sum_{\boldsymbol{c}\in C^\perp}(-1)^{\boldsymbol{c}\cdot\widetilde{\boldsymbol{w}}}(\mathrm{wgt}\,\boldsymbol{c})^j$ vanish, i. e.,
of which order (in t) are the errors?

Weight "Moments" and Coset Distance

Theorem 1:

Let $C = [n,k]$ be a linear binary code and let $\boldsymbol{w} \in \mathbb{F}_2^n$.

Then

$$\forall k \le j\colon \sum_{\boldsymbol{c} \in C^\perp} (-1)^{\boldsymbol{c}\cdot\boldsymbol{w}}\,\mathrm{wgt}(\boldsymbol{c})^k = 0 \quad\Longrightarrow\quad \mathrm{d}_H(C, C+\boldsymbol{w}) > j \tag{1}$$

and

$$\sum_{\boldsymbol{c} \in C^\perp} (-1)^{\boldsymbol{c}\cdot\boldsymbol{w}}\,\mathrm{wgt}(\boldsymbol{c})^j \neq 0 \quad\Longrightarrow\quad \mathrm{d}_H(C, C+\boldsymbol{w}) \le j \tag{2}$$

Proof of Theorem 1 (I)

in characteristic zero:

$$\begin{aligned}\mathrm{wgt}(\boldsymbol{c})^j = (c_1 + \ldots + c_n)^j &= \sum_{\nu_1+\ldots+\nu_n=j} c_1^{\nu_1} \cdot \ldots \cdot c_n^{\nu_n} \\ &= \sum_{k=1}^{j} \sum_{\substack{\{i_1,\ldots,i_k\} \\ \subseteq\{1,\ldots,n\}}} \alpha_{i_1\ldots i_k} (c_{i_1} \cdot \ldots \cdot c_{i_k})\end{aligned}$$

where $\alpha_{i_1\ldots i_k} \geq 0$

$$(*) = \sum_{\boldsymbol{c}\in C^\perp} (-1)^{\boldsymbol{c}\cdot\widetilde{\boldsymbol{w}}} (\mathrm{wgt}\,\boldsymbol{c})^j = \sum_{k=1}^{j} \sum_{\substack{\{i_1,\ldots,i_k\} \\ \subseteq\{1,\ldots,n\}}} \alpha_{i_1\ldots i_k} \underbrace{\sum_{\boldsymbol{c}\in C^\perp} (-1)^{\boldsymbol{c}\cdot\widetilde{\boldsymbol{w}}} (c_{i_1} \cdot \ldots \cdot c_{i_k})}_{(**)}$$

Proof of Theorem 1 (II)

Theorem 1 follows using

Lemma 2:

Let $\mathrm{d}_H(C, C + \boldsymbol{w}) = d$ and $\mathcal{I} = \{i_1, \ldots, i_k\} \subseteq \{1, \ldots n\}$ where $|\mathcal{I}| = k$.

Then for

$$\sum_{\boldsymbol{c} \in C^\perp} (-1)^{\boldsymbol{c} \cdot \widetilde{\boldsymbol{w}}} (c_{i_1} \cdot \ldots \cdot c_{i_k}) \qquad (**)$$

1. $(**)$ vanishes for $|\mathcal{I}| = k < d$.
2. $(**)$ does not vanish for some $\mathcal{I}$ with $|\mathcal{I}| = d$.
3. If $(**)$ does not vanish, then its sign is $(-1)^d$.

Proof: omitted (quite technical)

Effect on CSS Codes (II)

Recall:

$$E_{\boldsymbol{w},\boldsymbol{w}'}(t) = \sum_{j=0}^{\infty} \frac{(-\Gamma)^j}{j!} t^j \underbrace{\sum_{\boldsymbol{c}\in C^\perp} (-1)^{\boldsymbol{c}\cdot(\boldsymbol{w}+\boldsymbol{w}')} (\operatorname{wgt} \boldsymbol{c})^j}_{(*)}$$

Apply Theorem 1 for $\boldsymbol{w}+\boldsymbol{w}' =: \widetilde{\boldsymbol{w}} \in C^\perp$

$\Longrightarrow \mathrm{d}_H(C, C+\widetilde{\boldsymbol{w}}) \geq d_{\min}(C^\perp) =: d_{\min}$

$\Longrightarrow$ $(*)$ vanishes for exactly $j < d_{\min}$

$\Longrightarrow$ errors are of order $t^{d_{\min}}$

Fault Tolerant Quantum Computation

Which operations $U_1 \otimes \ldots \otimes U_n$ with $U_\nu \in \mathcal{U}(2)$ operate on the code space?

CSS codes: $|\psi_{\boldsymbol{w}}\rangle := \frac{1}{\sqrt{|C|}} \sum_{\boldsymbol{c} \in C} |\boldsymbol{c} + \boldsymbol{w}\rangle$

C is even, i. e., $(1, \ldots, 1) \in C^\perp$:

$$G_{\text{even}} \geq \left\langle \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}^{\otimes n}, \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}^{\otimes n}, \frac{1}{\sqrt{2^n}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}^{\otimes n} \right\rangle$$

If, additionally, C is doubly even:

$$G_{\text{doubly even}} \geq \left\langle G_{\text{even}}, \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}^{\otimes n} \right\rangle$$

Doubly Even Cyclic Codes

Theorem 2:
Any weakly self-dual cyclic linear binary code $C = [n, k]$ of odd length is doubly even.

Proof:
We show that the generator polynomial $\boldsymbol{g}(X)$ of C has doubly even weight.

$C^\perp$ is generated by $\boldsymbol{h}^{\mathsf{rev}}(X) := X^{\deg \boldsymbol{h}}\boldsymbol{h}(1/X)$ where $X^n - 1 = \boldsymbol{g}(X)\boldsymbol{h}(X)$.

$$
\begin{array}{ll}
C \le C^\perp & \Longrightarrow \boldsymbol{h}^{\mathsf{rev}}(X) | \boldsymbol{g}(X) \\
 & \Longrightarrow \boldsymbol{f}(X) := \boldsymbol{g}(X)\boldsymbol{g}^{\mathsf{rev}}(X) = \boldsymbol{a}(X)(X^n - 1) \\
(X-1)|\boldsymbol{a}(X) & \Longrightarrow \boldsymbol{a}(X) \text{ has } 2m \text{ terms} \\
\deg \boldsymbol{a} < n & \Longrightarrow \boldsymbol{f}(X) \text{ has } 4m \text{ terms}
\end{array}
$$

Proof of Theorem 2 (continued)

$$\boldsymbol{g}(X) = \sum_{i=1}^{w} X^{d_i} \quad \text{where } d_1 = 0 < d_2 < \ldots < d_w < n$$

$(X-1)|\boldsymbol{g}(X) \Longrightarrow w$ is even

$$\boldsymbol{f}(X) = \sum_{i=1}^{w} X^{d_i} \left(X^{d_w} \sum_{j=1}^{w} X^{-d_j} \right) = X^{d_w} \sum_{i,j=1}^{w} X^{d_i - d_j}$$

Terms $X^{d_i-d_j}$ and $X^{d_k-d_l}$ cancel each other if

- $i = j$: w cases, w even
- $i \neq j$: $X^{d_i-d_j} = X^{d_k-d_l} \Longrightarrow X^{d_j-d_i} = X^{d_l-d_k}$

  $\Longrightarrow$ four terms are cancelled

$$\left.\begin{array}{l} \Longrightarrow \boldsymbol{f}(X) \text{ has } w^2 - w - 4\ell = w(w-1) - 4\ell \text{ terms} \\ \text{Recall: } \boldsymbol{f}(X) \text{ has } 4m \text{ terms and } w \text{ is even.} \end{array}\right\} \Longrightarrow w \text{ is divisible by } 4$$

Weakly Self-Dual Codes (I)

Dual basis:

For a basis $\mathcal{B} = (b_1, \ldots, b_\ell)$ of $\mathbb{F}_{2^\ell} | \mathbb{F}_2$ let $\mathcal{B}^\perp = (b'_1, \ldots, b'_\ell)$ denote the *dual basis* with

$$\operatorname{tr}(b_i \cdot b'_j) = \delta_{ij}.$$

Subfield expansion:

For $C = [n, k, d] \leq \mathbb{F}_{2^\ell}^n$, define

$$\mathcal{B}(C) := \Big\{ (c_{11}, \ldots, c_{1\ell}, \ldots, c_{n1}, \ldots, c_{n\ell}) : \\ \boldsymbol{c} = (c_1, \ldots, c_n) \in C,\ c_i = \textstyle\sum_{j=1}^{\ell} c_{ij} b_j \Big\}$$

$\Longrightarrow \mathcal{B}(C) = [\ell n, \ell k, d' \geq d] \leq \mathbb{F}_2^{\ell n}$

Weakly Self-Dual Codes (II)

Theorem 3:

The following diagram commutes:

$$\begin{array}{ccc}
C & \longrightarrow & C^\perp \\
\text{basis } \mathcal{B} \Big\downarrow & & \Big\downarrow \text{ dual basis } \mathcal{B}^\perp \\
\mathcal{B}(C) & \longrightarrow & \mathcal{B}^\perp(C^\perp) = \big(\mathcal{B}(C)\big)^\perp
\end{array}$$

Proof: (main idea)

$\boldsymbol{c} \in C$, $\boldsymbol{d} \in C^\perp$ arbitrary:

$$0 = \sum_{i=1}^{n} c_i d_i = \sum_{i=1}^{n} \left(\sum_{j=1}^{\ell} c_{ij} b_j\right) \left(\sum_{l=1}^{\ell} d_{il} b'_l\right)$$

taking trace:

$$0 = \sum_{i=1}^{n} \sum_{j,l=1}^{\ell} c_{ij} d_{il} \underbrace{\operatorname{tr}(b_j b'_l)}_{=\delta_{j,l}} = \sum_{i=1}^{n} \sum_{j=1}^{\ell} c_{ij} d_{ij}$$

$\Longrightarrow \mathcal{B}^\perp(\boldsymbol{d}) \in \mathcal{B}(C)^\perp$

Weakly Self-Dual Codes (III)

Corollary 4:
Let $C = [n,k] \leq \mathbb{F}_{2^\ell}$ be a weakly self-dual code, i. e., $C \leq C^\perp$, and let $\mathcal{B}$ be a self-dual basis of $\mathbb{F}_{2^\ell}|\mathbb{F}_2$.

Then $\mathcal{B}(C) \leq \mathcal{B}(C^\perp)$.

Remark:
For $\mathbb{F}_{2^\ell}$ there exists always a self-dual basis over $\mathbb{F}_2$. (D. Jungnickel, *Finite Fields*, Proposition 4.3.1, p. 124f).

Idea:

- start with a weakly self-dual code C over $\mathbb{F}_{2^\ell}$ and a self-dual basis $\mathcal{B}$
- obtain a weakly self-dual binary code $\mathcal{B}(C)$
- obtain a CSS code

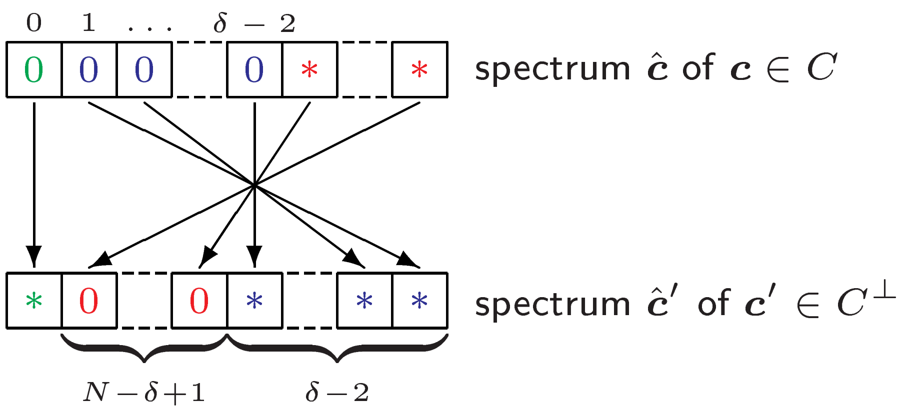
Quantum Reed-Solomon Codes

RS codes over $\mathbb{F}_{2^\ell}$ of length $n = 2^\ell - 1$ with generator polynomial

$$\boldsymbol{g}(X) = (X-1)(X-\alpha)\ldots(X-\alpha^{\delta-2})$$

are weakly self-dual iff $\delta > n/2 + 1$:

$$\begin{aligned} \boldsymbol{g}^\perp(X) &= (X-\alpha^{-(\delta-1)})(X-\alpha^{-\delta})\ldots(X-\alpha^{-(n-1)}) \\ &= (X-\alpha^1)(X-\alpha^2)\ldots(X-\alpha^{n-\delta+1}) \end{aligned}$$



$$C = [2^\ell - 1, 2^\ell - \delta, \delta] = [n, k, n-k+1]$$

$$\Longrightarrow \mathcal{B}(C) = [\ell(2^\ell-1), \ell(2^\ell-\delta), \delta' \geq \delta]$$

$$\Longrightarrow \text{QECC } \mathcal{C} = [[\ell(2^\ell-1), \ell(n-2k), d \geq k+1]]$$