First International Conference on Quantum Error Correction
University of Southern California, Los Angeles, USA December, 17-20, 2007

A Framework for Non-Additive Quantum Codes

Markus Grassl

joint work with

Martin Rötteler
NEC Laboratories America, Inc.

Institute for Quantum Optics and Quantum Information
Austrian Academy of Sciences
Innsbruck, Austria

Overview

- Review of the stabilizer formalism
- Union stabilizer codes
- The search graph
- Encoding circuits
- CSS-like non-additive codes
- New families of non-additive codes
- Summary & outlook

Motivation

Non-stabilizer codes $((n, K, d))$ can have a higher dimension compared to stabilizer codes $[[n, k, d]] = ((n, 2^k, d))$.

- $((5, 6, 2))$: found via numerical iteration
  [Rains, Hardin, Shor & Sloane, PRL **79**:953–954 (1997)]
  later explained as union of codes $[[5, 0, 3]]$
  [Grassl & Beth, quant-ph/9703016]
- $((9, 12, 3))$: derived from a graph state
  [Yu, Chen, Lai & Oh, arXiv.0704.2122]
- $((10, 20, 3))$: formalism for the construction of codes from graph states
  (see Bei Zeng's talk/poster)
  [Cross, Smith, Smolin & Zeng, arXiv:0708.1021v4]
- $((10, 24, 3))$: also using graph states
  [Yu, Chen & Oh, arXiv.0709.1780]

Stabilizer Codes & Classical Codes

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

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

- g corresponds to a binary vector $(\boldsymbol{a}|\boldsymbol{b})$ of length $2n$ or a vector $\boldsymbol{v} = \boldsymbol{a} + \omega \boldsymbol{b}$ of length n over $GF(4) = \{0, 1, \omega, \omega^2\}$

- the product of two elements g and h given by $\boldsymbol{v} = \boldsymbol{a} + \omega \boldsymbol{b}$ 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

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

- the weight of g equals the Hamming weight of $\boldsymbol{v}$

Stabilizer Codes & Classical Codes

- a stabilizer code $\mathcal{C} = [[n,k,d]]$ is the joint $+1$-eigenspace of the stabilizer group $\mathcal{S} = \langle S_1, \ldots, S_{n-k} \rangle$
- 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 $C^* = (n, 2^{n+k})$
- the minimum distance d of $\mathcal{C}$ is given by

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

Stabilizer and Normalizer

$$\left(\begin{array}{c|c}
S_1^X & S_1^Z \\
\vdots & \vdots \\
S_{n-k}^X & S_{n-k}^Z \\
\hline
\overline{Z}_1^X & \overline{Z}_1^Z \\
\vdots & \vdots \\
\overline{Z}_k^X & \overline{Z}_k^Z \\
\hdashline
\overline{X}_1^X & \overline{X}_1^Z \\
\vdots & \vdots \\
\overline{X}_k^X & \overline{X}_k^Z
\end{array}\right)$$

Example: Five Qubit Code $[\![5,1,3]\!]$

$$
\left(\begin{array}{ccccc}
X & X & Z & I & Z \\
Z & X & X & Z & I \\
I & Z & X & X & Z \\
Z & I & Z & X & X \\
\hline
I & I & Z & Y & Z \\
\hdashline
I & I & X & Z & X
\end{array}\right)
\mathrel{\hat{=}}
\left(\begin{array}{ccccc|ccccc}
1 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\
0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\
0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 1 \\
0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 \\
\hline
0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\
\hdashline
0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0
\end{array}\right)
$$

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

Canonical Basis

- fix logical operators $\overline{X}_j$ and $\overline{X}_j$
- the stabilizer S and the logical operators $\overline{Z}_j$ mutually commute
- the logical state $\left|\overline{00\ldots0}\right\rangle$ is a stabilizer state
- define the (logical) basis states as

$$\left|\overline{i_1 i_2 \ldots i_k}\right\rangle = \overline{X}_1^{i_1} \cdots \overline{X}_k^{i_k} \left|\overline{00\ldots0}\right\rangle$$

Orthogonal Decomposition

- the code $\mathcal{C}$ is the joint $+1$ eigenspace of the stabilizer $\mathcal{S}$
- for a Pauli operator t, define the character χ_t

$$\chi_t(S_i) := \begin{cases} +1 & \text{if } t \text{ and } S_i \text{ commute,} \\ -1 & \text{if } t \text{ and } S_i \text{ anti-commute} \end{cases}$$

- the spaces $t_1\mathcal{C}$ and $t_2\mathcal{C}$ are $\begin{cases} \text{orthogonal for } \chi_{t_1} \neq \chi_{t_2}, \\ \text{identical for } \chi_{t_1} = \chi_{t_2} \end{cases}$
- equivalently, $t_1\mathcal{C} = t_2\mathcal{C}$ iff $t_1^{-1}t_2 \in \mathcal{N}$
- orthogonal decomposition

$$(\mathbb{C}^2)^{\otimes n} = \bigoplus_{t \in \mathcal{T}} t\,\mathcal{C} \qquad \mathcal{T} \text{ is a set of coset representatives } \mathcal{P}_n/\mathcal{N}$$

Pauli Distance

- *operational* distance between pure states

$$\operatorname{dist}(|\psi\rangle, |\phi\rangle) = \min\{\operatorname{wgt}(p) : p \in \mathcal{P}_n \mid \langle\phi| p |\psi\rangle \neq 0\}$$

- for subspaces $\mathcal{V}_1$ and $\mathcal{V}_2$ with projection operators Π_1 and Π_2

$$\operatorname{dist}(\mathcal{V}_1, \mathcal{V}_2) = \min\{\operatorname{wgt}(p) : p \in \mathcal{P}_n \mid \operatorname{tr}(\Pi_1 p \Pi_2 p^\dagger) \neq 0\}$$

- for translates $t_1\mathcal{C}$ and $t_2\mathcal{C}$ of a stabilizer code $\mathcal{C}$

$$\operatorname{dist}(t_1\mathcal{C}, t_2\mathcal{C}) = \min\{\operatorname{wgt}(p) : p \in \mathcal{P}_n \mid p\, t_1\mathcal{C} = t_2\mathcal{C}\}$$

  for Pauli operators t_1, t_2, clearly

$$\operatorname{dist}(t_1\mathcal{C}, t_2\mathcal{C}) = \operatorname{dist}(\mathcal{C}, t_1^{-1}t_2\mathcal{C})$$

Computing the Pauli Distance

Theorem:

The distance of the spaces $t_1\mathcal{C}$ and $t_2\mathcal{C}$ equals the distance of the cosets $C^* + t_1$ and $C^* + t_2$ which is given by the minimum weight in the coset $C^* + t_1 - t_2$. Here t_i denotes both an n-qubit Pauli operator and the corresponding vector over $GF(4)$.

Proof:

$$\begin{aligned}
\operatorname{dist}(t_1\mathcal{C}, t_2\mathcal{C}) &= \min\{\operatorname{wgt}(p) : p \in \mathcal{P}_n \mid p\, t_1\mathcal{C} = t_2\mathcal{C}\} \\
&= \operatorname{dist}(C^* + t_1, C^* + t_2) \\
&= \operatorname{dist}(C^* + (t_1 - t_2), C^*) \\
&= \min\{\operatorname{wgt}(c + t_1 - t_2) : c \in C^*\} \\
&= \min\{\operatorname{wgt}(v) : v \in C^* + t_1 - t_2\}.
\end{aligned}$$

Union Stabilizer Code

(see also [Grassl & Beth 97], [Arvind, Kurur & Parthasarathy, QIC **4**:411–436 (2004)])

Let $\mathcal{C}_0 = [[n, k, d_0]]$ be a stabilizer code and let $\mathcal{T}_0 = \{t_1, \ldots, t_K\}$ be a subset of the coset representatives of the normalizer $\mathcal{N}_0$ of the code $\mathcal{C}_0$ in $\mathcal{P}_n$. Then the *union stabilizer code* is defined as

$$\mathcal{C} = \bigoplus_{t \in \mathcal{T}_0} t\,\mathcal{C}_0.$$

If C_0 and C_0^* with $C \subseteq C^*$ denote the classical codes corresponding to the stabilizer $\mathcal{S}_0$ and the normalizer $\mathcal{N}_0$ of $\mathcal{C}_0$, then the (in general non-additive) *union normalizer code* is given by

$$C^* = \bigcup_{t \in \mathcal{T}_0} C_0^* + t = \{c + t_i : c \in C_0^*, i = 1, \ldots, K\}.$$

The minimum distance of $\mathcal{C}$ is at least $d = \min(d_0, d_{\min}(C^*))$.

Stabilizer, Normalizer & Translations

$$
\left(\begin{array}{c|c}
S_1^X & S_1^Z \\
\vdots & \vdots \\
S_{n-k}^X & S_{n-k}^Z \\
\hline
\overline{Z}_1^X & \overline{Z}_1^Z \\
\vdots & \vdots \\
\overline{Z}_k^X & \overline{Z}_k^Z \\
\hdashline
\overline{X}_1^X & \overline{X}_1^Z \\
\vdots & \vdots \\
\overline{X}_k^X & \overline{X}_k^Z
\end{array}\right)
$$
$$
\left\{\begin{array}{c|c}
t_1^X & t_1^Z \\
\vdots & \vdots \\
t_K^X & t_K^Z
\end{array}\right\}
$$

Canonical Basis

- fix logical operators $\overline{X}_j$ and $\overline{X}_j$
- the stabilizer S and the logical operators $\overline{Z}_j$ mutually commute
- the logical state $\left|\overline{00\ldots0}\right\rangle$ is a stabilizer state
- define the (logical) basis states as

$$\left|\overline{j}; \overline{i_1 i_2 \ldots i_k}\right\rangle = t_j \left(\overline{X}_1^{i_1} \cdots \overline{X}_k^{i_k}\right) \left|\overline{00\ldots0}\right\rangle$$

The Search Graph

goal: find a good set $\mathcal{T}_0$ of coset representatives

- the cosets of $\mathcal{N}$ in $\mathcal{P}_n$ correspond to cosets of $C_0^* = (n, 2^{n+k}, d_0)$ in the full space
- define a *search graph*
  - the vertices are all 2^{n-k} coset representatives
  - coset representatives t_1, t_2 are connected iff $\mathrm{wgt}_{\min}(C_0^* + (t_1 - t_2)) \geq d$
- define a *reduced search graph*
  - choose w. l. o. g. $t_1 = id \in \mathcal{T}_0$
  - keep only vertices that are connected to t_1
- search a maximal/large clique of size K in this graph

$\Longrightarrow$ union stabilizer code of dimension $K \times 2^k$ and distance at least $\min(d, d_0)$

Example: $((10, 20, 3))$ and $((10, 10 \times 2^1, 3))$

Approach I

- start with a graph state $[[10, 0, 4]]$
- reduced search graph with 668 vertices and 142 233 edges (density 63.85%)
- approx. 1030 s to find a maximal clique of size 20 (using cliquer)

Approach II

- start with a stabilizer code $[[10, 1, 3]]$
- reduced search graph with 214 vertices and 8 706 edges (density 38.20 %)
- less than 1 s to find a maximal clique of size 10 (using cliquer)

Approach II does not yield an optimal code $((10, 24, 3))$

(Inverse) Encoding Circuits

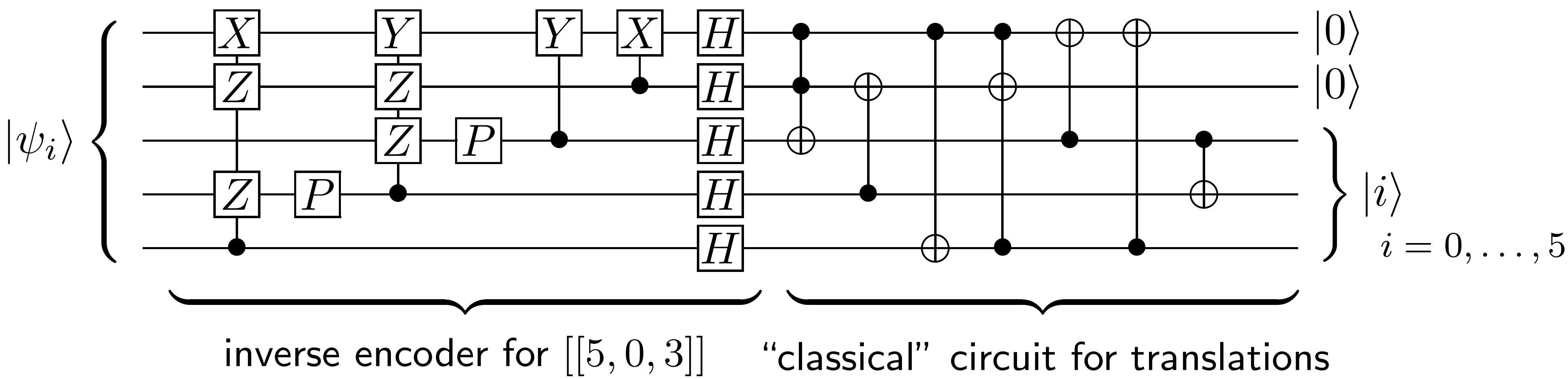
(see [Grassl, Rötteler & Beth, quant-ph/0211014])

- encoding of stabilizer codes requires only (non-local) Clifford operations
- use Clifford operations to transform the stabilizer $\mathcal{S}$ into a trivial stabilizer $\mathcal{S}_0 = \langle Z^{(1)}, \ldots, Z^{(n-k)} \rangle$
- corresponding trivial code is given by $|\phi\rangle \mapsto |00\ldots0\rangle\,|\phi\rangle$
- the resulting circuit U_C transforms also the logical operators into trivial logical operators
- "trivial" transformed translation operators $\tilde{t}_i$ can be choosen as X-only Pauli operators
- "classical" circuit that maps $\tilde{t}_i\,|0\rangle \mapsto |i\rangle$

Encoding Circuits: Transformed Translations

$$
\left\{\begin{array}{c|c}
\left(\begin{array}{c|c}
S_1^X & S_1^Z \\
\vdots & \vdots \\
S_{n-k}^X & S_{n-k}^Z \\
\hline
\overline{Z}_1^X & \overline{Z}_1^Z \\
\vdots & \vdots \\
\overline{Z}_k^X & \overline{Z}_k^Z \\
\hdashline
\overline{X}_1^X & \overline{X}_1^Z \\
\vdots & \vdots \\
\overline{X}_k^X & \overline{X}_k^Z
\end{array}\right) \\
\hline
t_1^X & t_1^Z \\
\vdots & \vdots \\
t_K^X & t_K^Z
\end{array}\right\}
\xrightarrow{U_C}
\left\{\begin{array}{c|c}
\left(\begin{array}{c|c}
 & \begin{matrix} 1 & & 0\cdots 0 \\ & \ddots & \vdots \quad \vdots \\ & & 1\ 0\cdots 0 \end{matrix} \\
\hline
 & \begin{matrix} 0\cdots 0 & 1 & \\ \vdots \quad \vdots & & \ddots \\ 0\cdots 0 & & 1 \end{matrix} \\
\hdashline
\begin{matrix} 0\cdots 0 & 1 & \\ \vdots \quad \vdots & & \ddots \\ 0\cdots 0 & & 1 \end{matrix} &
\end{array}\right) \\
\hline
\tilde{t}_1^X & \tilde{t}_1^Z \\
\vdots & \vdots \\
\tilde{t}_K^X & \tilde{t}_K^Z
\end{array}\right\}
$$

Inverse Encoding Circuit $((5,6,2))$



CSS-Like Union Stabilizer Codes

- given $C_1 = [n, k_1, d_1]$ and $C_2 = [n, k_2, d_2]$ with $C_2^\perp \subset C_1$, we obtain a CSS code $\mathcal{C}_0 = [[n, k_1 + k_2 - n, d_0]]$ with $d_0 \geq \min(d_1, d_2)$
- replace C_i by unions of cosets of C_i

$$\widetilde{C}_i = \bigcup_{t^{(i)} \in \mathcal{T}_i} C_i + t^{(i)}$$

  such that $d_{\min}(\widetilde{C}_i) \geq \widetilde{d} \leq d_0$

- using $\mathcal{C}_0$ and the translations $\mathcal{T}_0 = \{(t^{(1)}|t^{(2)}) : t^{(1)} \in \mathcal{T}_1, t^{(2)} \in \mathcal{T}_2\}$ we obtain a union stabilizer code of dimension $|\mathcal{T}_1| \cdot |\mathcal{T}_2| \cdot 2^{k_1+k_2-n}$ and minimum distance at least $\widetilde{d}$

Goethals & Preparata Codes

- non-linear binary codes of length 2^m for m even
- both the Goethals code $\mathcal{G}(m)$ and the Preparata code $\mathcal{P}(m)$ are unions of cosets of the Reed-Muller code $\mathcal{R}(m) := \mathrm{RM}(m-3,m)$
- nested subcodes of $\mathrm{RM}(m-2,m)$, i. e.,

$$\mathrm{RM}(m-3,m) \subset \mathcal{G}(m) \subset \mathcal{P}(m) \subset \mathrm{RM}(m-2,m).$$

- parameters

$$\begin{aligned}
\mathrm{RM}(m-3,m) = \mathcal{R}(m) &= [2^m, 2^m - \tbinom{m}{2} - m - 1, 8] \\
\mathcal{G}(m) &= (2^m, 2^{2^m-3m+1}, 8) \\
\mathcal{P}(m) &= (2^m, 2^{2^m-2m}, 6) \\
\mathrm{RM}(m-2,m) &= [2^m, 2^m - m - 1, 4]
\end{aligned}$$

New Families of Non-Additive Codes

- CSS construction applied to $\mathrm{RM}(2,m) \subset \mathrm{RM}(m-3,m)$ yields $\mathcal{C}_0 = [[2^m, 2^m - 2\binom{m}{2} - 2m - 2, 8]]$
- Steane's enlargement construction yields "quantum Reed-Muller codes" $\mathcal{C}_{\mathrm{RM}} = [[2^m, 2^m - \binom{m}{2} - 2m - 2, 6]]$
- CSS-like union stabilizer codes with $\mathrm{RM}(m-3,m) \subset \mathcal{G}(m)$ yields $\mathcal{C}_{\mathcal{G}} = ((2^m, 2^{2^m-6m+2}, 8))$
- CSS-like union stabilizer codes with $\mathrm{RM}(m-3,m) \subset \mathcal{P}(m)$ yields $\mathcal{C}_{\mathcal{P}} = ((2^m, 2^{2^m-4m}, 6))$
- Steane's enlargement construction applied to BCH codes yields stabilizer codes $[[2^m, 2^m - 5m - 2, 8]]$ and $[[2^m, 2^m - 3m - 2, 6]]$

New Families of Non-Additive Codes

distance $d = 6$

enlarged Reed-Muller	Preparata	enlarged BCH
$[[64, 35, 6]]$	$((64, 2^{40}, 6))$	$[[64, 44, 6]]$
$[[256, 210, 6]]$	$((256, 2^{224}, 6))$	$[[256, 230, 6]]$
$[[1024, 957, 6]]$	$((1024, 2^{984}, 6))$	$[[1024, 992, 6]]$

distance $d = 8$

CSS Reed-Muller	Goethals	enlarged BCH
$[[64, 20, 8]]$	$((64, 2^{30}, 8))$	$[[64, 32, 8]]$
$[[256, 182, 8]]$	$((256, 2^{210}, 8))$	$[[256, 214, 8]]$
$[[1024, 912, 8]]$	$((1024, 2^{966}, 8))$	$[[1024, 972, 8]]$

A Closer Look at Goethals & Preparata Codes

$\mathcal{G}(m)$ and $\mathcal{P}(m)$ are cosets of nested *linear* codes $C_{\mathcal{G}}$ and $C_{\mathcal{P}}$, respectively, using the *very same coset* representatives $t_i \in \mathcal{T}$

$$
\begin{tikzcd}[arrows=dash]
 & \mathrm{RM}(m-2,m) = [2^m, 2^m - m - 1, 4] \arrow[d] \\
{[2^m, 2^m - 3m + 1, 6]} = C_{\mathcal{P}} \arrow[r] \arrow[d] & \mathcal{P}(m) = \bigcup_i C_{\mathcal{P}} + t_i \arrow[d] \\
{[2^m, 2^m - 4m + 2, 8]} = C_{\mathcal{G}} \arrow[r] \arrow[d] & \mathcal{G}(m) = \bigcup_i C_{\mathcal{G}} + t_i \\
\mathrm{RM}(m-3,m) &
\end{tikzcd}
$$

An Improved Family of Non-Additive Codes

- Steane's enlargement construction applied to $C_{\mathcal{G}}^{\perp} \subset C_{\mathcal{G}} \subset C_{\mathcal{P}}$ yields $\mathcal{C}_0 = [[2^m, 2^m - 7m + 3, 8]]$
- 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
$[[64, 20, 8]]$	$((64, 2^{30}, 8))$	$[[64, 32, 8]]$	$((64, 2^{35}, 8))$
$[[256, 182, 8]]$	$((256, 2^{210}, 8))$	$[[256, 214, 8]]$	$((256, 2^{217}, 8))$
$[[1024, 912, 8]]$	$((1024, 2^{966}, 8))$	$[[1024, 972, 8]]$	$((1024, 2^{975}, 8))$

Summary & Outlook

- non-additive codes as union of arbitrary stabilizer *codes*
- search graph of considerably smaller size
- extremal cases: stabilizer codes and codeword stabilized codes
- new families of non-additive codes
- improved family of non-additive with $d = 8$

future work

- circuits for "syndrome measurement"
- fault-tolerant operations
- more classes of new codes