Nonbinary Quantum Reed-Muller Codes

Pradeep Sarvepalli
pradeep@cs.tamu.edu

Department of Computer Science,
Texas A&M University

Joint work with Dr. Andreas Klappenecker
Outline

- Introduction
- Generalized Reed-Muller Codes
- Quantum Reed-Muller Codes
- Puncturing Quantum Codes
- Optimal Quantum Codes
- Conclusions
A $q$-ary quantum code $Q$, denoted by $[[n, k, d]]_q$, is a $q^k$ dimensional subspace of $\mathbb{C}^{q^n}$ and can correct all errors upto $\left\lfloor \frac{d-1}{2} \right\rfloor$.

Let $G = \{ E = E_1 \otimes E_2 \cdots \otimes E_n \}$ ($q^n \times q^n$ matrices)

$Q$ is the joint eigenspace of a commutative subgroup, $S \leq G$

$$E|v\rangle = |v\rangle, \ E \in S, \ \text{for all} \ |v\rangle \in Q$$
CSS Construction

- $S$ can be mapped to a self-orthogonal classical code

$$C \subseteq C^d$$

**Lemma 1** Let $C_1 = [n, k_1, d_1]_q$, $C_2 = [n, k_2, d_2]_q$ be linear codes over $\mathbb{F}_q$ with $C_1 \subseteq C_2$ and

$$d = \min \text{wt}\{(C_2 \setminus C_1) \cup (C_1^\perp \setminus C_2^\perp)\}.$$ Then there exists an $[[n, k_2 - k_1, d]]_q$ quantum code

- The construction of quantum codes reduces to constructing self-orthogonal classical codes
Generalized Reed-Muller Codes

GRM codes are defined by using two objects

- A vector space of functions,
  \[ L_m(\nu) = \{ f(x_1, \ldots, x_m) \mid \deg f \leq \nu \} \]
  Ex: \( L_2(2) = \langle 1, x, y, xy, x^2, y^2 \rangle \)

- All points in \( \mathbb{F}_q^m \); \( n = q^m \)
  Ex: \( \mathbb{F}_2^2 = \{(0, 0); (0, 1); (1, 0); (1, 1)\} \)

- \( R_q(\nu, m) = \{ f(P_1), \ldots f(P_n) \mid f \in L_m(\nu) \} \)

- Each codeword is obtained by evaluating a function on each of the \( n \) points
  Ex: \( x \in L_2(2) \) gives the codeword \((0, 0, 1, 1)\)
$\mathcal{R}_q(\nu, m)$ is an $[q^m, k(\nu), d(\nu)]_q$ code where

\[ k(\nu) = \sum_{j=0}^{m} (-1)^j \binom{m}{j} \left( m + \nu - jq \right), \]
\[ d(\nu) = (R + 1)q^Q, \]

where $m(q - 1) - \nu = (q - 1)Q + R$, such that $0 \leq R < q - 1$. 

**Properties of GRM Codes**
The codes are nested, i.e., if $\nu_1 \leq \nu_2$, then
\[ R_q(\nu_1, m) \subseteq R_q(\nu_2, m) \]

The dual of a GRM code is also a GRM code
\[ R_q(\nu, m)\perp = R_q(\nu\perp, m), \]
where $\nu\perp = m(q - 1) - \nu - 1$

GRM codes are a family of nested codes whose parameters including the dual distance are easily computed.
Recall that CSS construction makes use of nested codes

**Theorem 1** For $0 \leq \nu_1 \leq \nu_2 \leq m(q - 1) - 1$, there exists a quantum code with parameters

$$[[q^m, k(\nu_2) - k(\nu_1), \min\{d(\nu_1^\perp), d(\nu_2)\}]]_q$$

Self-orthogonal codes over $\mathbb{F}_{q^2}$ with respect to the Hermitian inner product also give quantum codes
The Hermitian inner product of two vectors $x, y \in \mathbb{F}_{q^2}^n$ is defined as

$$\langle x|y \rangle_h = (x_1, \ldots, x_n) \cdot (y_1^q, \ldots, y_n^q) = \langle x|y^q \rangle$$

**Lemma 2** Let $C$ be a linear $[n, k]_{q^2}$ contained in its Hermitian dual, $C^\perp_h$, such that $d = \min\{\text{wt}(C^\perp_h \setminus C)\}$. Then there exists an $[[n, n - 2k, d]]_q$ quantum code.

So when are the GRM codes self-orthogonal in this sense?
If two polynomials $f, g$ are Hermitian orthogonal then $q\nu_g \leq m(q^2 - 1) - \nu_f - 1$

**Lemma 3** Let $0 \leq \nu \leq m(q - 1) - 1$, then $R_{q^2}(\nu, m) \subseteq R_{q^2}(\nu, m)_{\perp h}$

**Theorem 2** For $0 \leq \nu \leq m(q - 1) - 1$, there exist quantum codes $[[q^{2m}, q^{2m} - 2k(\nu), d(\nu_{\perp})]]_q$

We now have two families of quantum codes constructed from GRM codes
Puncturing Quantum Codes

- Observe the lengths of codes we constructed

\[ [[q^m, k(\nu_2) - k(\nu_1), \min\{d(\nu_1^\perp), d(\nu_2)\}]]_q \]

- Lengths are \( q, q^2, \ldots \); We would like to have codes of other lengths, hence the need for puncturing

- Classical puncturing is very easy

- It is not always possible to puncture quantum codes, because the punctured code may not be self-orthogonal
How do we puncture it so that the code is still self-orthogonal?

The answer lies in the puncture code $P_h(C)$

$$
P_h(C) = \left\{ \text{tr}_{q^2/q}(a_i b_i^q)^n_{i=1} \mid a, b \in C \right\}^\perp
$$

If there exists a vector of nonzero weight $r$ in $P_h(C)$, then an $[[n, k, d]]_q$ quantum code can be punctured to $[[r, \geq k - (n - r), \geq d]]_q$
However

- $P_h(C')$ is not always easy to compute
- The weight distribution is difficult to compute

We simplify the problem by computing a “nice” subcode and its minimum distance

**Theorem 3** Let $C = \mathcal{R}_{q^2}(\nu, m)$ with

\[
0 \leq \nu \leq m(q - 1) - 1 \quad \text{and} \quad (q + 1)\nu \leq \mu \leq m(q^2 - 1) - 1.
\]

Then $P_h(C') \supseteq \mathcal{R}_{q^2}(\mu, m)^\perp \mid_{\mathbb{F}_q}$. 
Quantum MDS Codes

- Quantum Singleton Bound $2d \leq n - k + 2$, for quantum MDS codes $2d = n - k + 2$

- Grassl, Rötteler and Beth constructed many quantum MDS codes with lengths $n \leq q$ and $n = q^2, q^2 \pm 1$

- Despite a lot of numerical evidence that there exist quantum MDS codes of lengths between $q$ and $q^2 - 1$ analytical proofs were missing

- Our next goal is to construct some of these missing quantum MDS codes
If \( m = 1 \), then the quantum GRM codes are MDS

We know that \( P_h(C) \supseteq \mathcal{R}_{q^2}(\mu, 1)^\perp|_{F_q} \)

We find \( q \)-ary subcodes in \( \mathcal{R}_{q^2}(\mu, 1)^\perp \)

We can show that

\[
P_h(C) \supseteq \mathcal{R}_{q^2}(\mu, 1)^\perp|_{F_q} \\
\supseteq \mathcal{R}_q(q - \nu - 1, 2) \supseteq \mathcal{R}_q(\alpha, 2),
\]

\[0 \leq \alpha \leq q - \nu - 1, \ 0 \leq \nu \leq q - 2\]
Lemma 4  Let $C = R_{q^2}(\nu, 1)$ with $0 \leq \nu \leq q - 2$, then the puncture code $P_h(C)$ has a vector of weight $(q - \alpha)q$, where $0 \leq \alpha \leq q - \nu - 1$.

Theorem 4  There exist quantum MDS codes with the parameters

$$[[ (q - \alpha)q, q^2 - q\alpha - 2\nu - 2, \nu + 2 ]]_q$$

for $0 \leq \nu \leq q - 2$ and $0 \leq \alpha \leq q - \nu - 1$.

This gives us quantum MDS codes of lengths $q, 2q, \ldots, q^2$. Analytical proofs for codes of other lengths in this range remain to be found.
Conclusions

- Constructed two families of quantum codes
- Showed how they can be punctured
- Proved the existence of a series of quantum MDS codes with lengths in the range $q$ and $q^2$

Acknowledgment: This research was supported by NSF, Texas A&M TITF Initiative and TEES Select Young Faculty Award