Remarkable Degenerate Quantum Stabilizer Codes from Duadic Codes

Pradeep Sarvepalli

Department of Computer Science
Texas A&M University

IEEE International Symposium on Information Theory, 2006

Coauthors: Dr. Andreas Klappenecker and Salah A. Aly

Motivation

- Much work has been done in quantum error correction in view of its importance for practical quantum computing
- Quantum codes have essential differences with respect to the classical codes
- The ‘quantum’ aspects of the quantum codes have been somewhat neglected in code construction

This talk focuses on one such aspect to derive quantum codes

Quantum Codes

A q-ary quantum code with parameters $[[n, k, d]]_q$

- q^k-dimensional subspace in $\mathcal{H} = \mathbb{C}^{q^n}$
- detects up to $d - 1$ errors

Assuming independent errors on each qubit we can write each error E as $E = E_1 \otimes E_2 \otimes \cdots \otimes E_n$

- $\mathrm{wt}(E) = |\{i | E_i \neq I\}|$

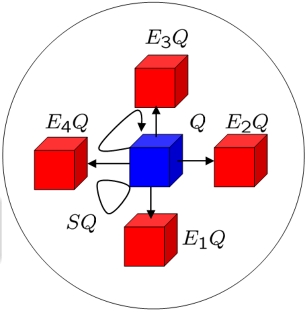
Quantum codes can be derived from self-orthogonal additive codes and their properties related to the distance and dual distance of the additive code

Errors - A Closer Look

Detectable errors

- Either take a code vector $|u\rangle$ outside the code space
- Or change the global phase

Errors which only change phase are called nice errors



Undetectable errors

- Takes a code vector to another code vector

An error E is detectable if and only if $\langle u|E|u\rangle = \langle v|E|v\rangle$ for any code vectors u, v

Degeneracy in Quantum Codes

Nondegenerate codes

All nice errors have weight $\geq d$

Degenerate codes

There exist some nice errors with weight $< d$

A quantum code for which $\langle u|E|v\rangle = q^{-n} \operatorname{Tr} E$ for all errors whose weight is $< d$ is called nondegenerate and degenerate otherwise

Depolarizing Channel can be thought of as a q^2-ary symmetric channel. With probability $1 - p$, there is no error and with probability $p/(q^2 - 1)$ there are $q^2 - 1$ different errors

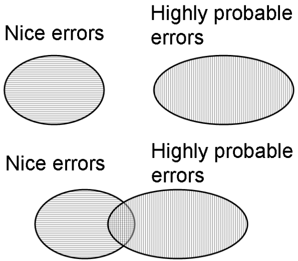
If we assume that the errors are independent, then the errors of low weight are more likely to occur.

The Relevance of Degeneracy

In quantum scenario error correction itself could faulty

Nice errors do not require active error correction

In a nondegenerate code all nice errors have weight $\geq d$ so we cannot take advantage of the fact that some errors do not require active error correction



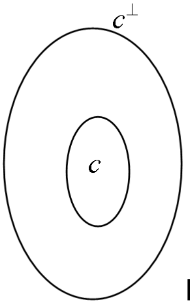
In degenerate codes, there are nice errors whose weight is less than d

Quantum Codes - Previous Work

Lemma (CSS Construction)

Let $C = [n, k, d']_q$, be a linear code over $\mathbb{F}_q$ with $C \subseteq C^\perp$ and $d = wt\{(C^\perp \setminus C)\}$. Then there exists an $[[n, n-2k, d]]_q$ quantum code pure to d'

A popular approach is to take self-orthogonal classical codes whose dual distance $\geq d$ forcing $d' \geq d$, and thus giving nondegenerate codes



However, choosing a poor code C such that $C^\perp \setminus C$ has large weight is difficult

Most of the known classical codes lead to nondegenerate codes

Background

Duadic codes require two sets S_0, S_1 and a permutation $\mu_a : i \mapsto ia \mod n$ such that

1. $S_0 \cap S_1 = \emptyset$
2. $S_0 \cup S_1 = \{1, \ldots, n-1\}$
3. $aS_0 \equiv S_1 \mod n$ and $aS_1 \equiv S_0 \mod n$

A duadic code is a cyclic code with defining set one of the sets $S_0, S_1, \{0\} \cup S_0, \{0\} \cup S_1$

Duadic codes exist if and only if $q \equiv \square \mod n$

Duadic Codes

Some preliminaries

- $c = (c_1, \ldots, c_n) \in \mathbb{F}_q^n$ is said to be even-like if $\sum_i c_i = 0$
- A code C is said to be even-like if every codeword in C is even-like and odd-like otherwise
- The map $\mu_a : i \mapsto ai$ mod n is a permutation of the set $\{0, 1, \ldots n-1\}$ if $\gcd(n, q) = 1$

Let α be a primitive nth root of unity and let

$$g_i(x) = \prod_{j \in S_i} (x - \alpha^j).$$

$D_i = \langle g_i(x) \rangle$ is an odd-like code with parameters $[n, (n+1)/2]_q$

$C_i = \langle (x-1) g_i(x) \rangle$ and has parameters $[n, (n-1)/2]_q$

Equivalent Codes

$$C_1 \xrightarrow{M} C \xrightarrow{\gamma} C_2$$

- Two codes C_1, C_2 are equivalent if there exists a monomial matrix M and automorphism γ of $\mathbb{F}_q$ such that $C_2 = C_1 M\gamma$. Equivalence is denoted by $\sim$

Equivalent codes have same weight distribution

- Given a cyclic code C with defining set T, the map μ_a induces an equivalent code $C\mu_a$ whose defining set is $a^{-1}T$

The duadic codes are equivalent i.e, $D_0 \sim D_1$ and $C_0 \sim C_1$

- If $a = -1$, then it follows that $C\mu_{-1}$ has defining set $-T$

Duals of Duadic Codes

The duals of duadic codes are equivalent to duadic codes, more precisely

$$C_i^\perp \sim D_i \quad \text{and} \quad D_i^\perp \sim C_i$$

Sketch of Proof

- The defining set of $C_0^\perp$ is $-(\{0\} \cup S_0 \cup S_1 \setminus S_0 \cup \{0\}) = -S_1$
- $-S_1$ is the defining set of $D_1\mu_{-1}$
- Therefore, it follows that $C_0^\perp \sim D_1 \sim D_0$

Odd-like distance of a duadic code D_i refers to $d_o = \text{wt}(D_i \setminus C_i)$. Further $d_o^2 \geq n$

$\text{wt}(C_i^\perp \setminus D_i^\perp) = \text{wt}(D_i \setminus C_i) = d_o$

Quantum Duadic Codes

A popular method for constructing quantum codes uses nested codes $C \subseteq D \subseteq \mathbb{F}_q^n$

Lemma (CSS Construction)

Let $C = [n, k, d]_q$, $D = [n, k', d']_q$ be linear codes over $\mathbb{F}_q$ with $C \subseteq D$ and $d = \min wt\{(D \setminus C) \cup (C^\perp \setminus D^\perp)\}$. Then there exists an $[[n, k' - k, d]]_q$ quantum code

- Since $C_i \subset D_i$, the duadic codes naturally lend themselves to CSS construction
- $\dim D_i - \dim C_i = (n+1)/2 - (n-1)/2 = 1$
- $\mathrm{wt}(D_i \setminus C_i) = \mathrm{wt}(C_i^\perp \setminus D_i^\perp) = d_o$

Quantum Duadic Codes

Theorem

If $q \equiv \square \mod n$*, then there exist quantum codes with parameters* $[[n, 1, d_o \geq \sqrt{n}]]_q$*. If* μ_{-1} *gives a splitting then we can sharpen* $d_o^2 \geq n^2 - n + 1$

Degenerate Duadic Codes

But we still have to show the existence of degenerate codes.

We will illustrate the idea by first considering when n is a prime power

Degenerate Quantum Duadic Codes

Lemma

Let $q \equiv \square \mod p$ *and* $t = \mathrm{ord}_p(q)$. *The minimum distance of duadic codes of length* $n = p^m$ *is upperbounded by* $d \leq p^z$, *where* $p^z | q^t - 1$ *and* $p^{z+1} \nmid q^t - 1$

Theorem

Let $q \equiv \square \mod p$, $t = \mathrm{ord}_p(q)$ *and* $p^z || q^t - 1$. *Then there exist degenerate quantum duadic codes with parameters* $[[p^m, 1, d_o]]_q$ *where* $m > 2z$.

- We already know that there exist duadic codes with parameters $[[p^m, 1, d_o]]_q$
- But the previous lemma states the distance is $\leq p^z < d_o$ if $m > 2z$. Hence the code must be degenerate

Degenerate Quantum Duadic Codes - Example

- $2 \equiv \square \mod 7$ as $2 \equiv 4^2 \mod 7$, hence duadic codes and quantum duadic codes $[[7^m, 1, \geq 7^{m/2}]]$ exist
- $\text{ord}_7(2) = 3$, and $7 | 2^3 - 1$ and $7^2 \not| 2^3 - 1$, therefore $z = 1$
- For all $m > 2$ the duadic codes $[[7^m, 1, 7^{m/2}]]$ are degenerate

These codes have nice errors of weight 4.

Degenerate Quantum Duadic Codes

Lemma

Let $q \equiv \Box \mod p_i$, $t_i = \text{ord}_p(q)$ *and* $p^{z_i} || q^{t_i} - 1$ *There exist duadic codes of length* $n = \prod p_i^m$ *whose minimum distance is upperbounded by* $d \leq \min p^{z_i}$.

Theorem

Let $q \equiv \Box \mod p_i$, $t_i = \text{ord}_p(q)$ *and* $p^{z_i} || q^{t_i} - 1$ *Let* $n = \prod p_i^m$*, then there exist degenerate quantum duadic codes with parameters* $[[n, 1, d_o]]_q$ *where* $m_i > 2z_i$.

- We already know that there exist duadic codes with parameters $[[n, 1, d_o]]_q$
- The previous lemma states the the distance $\leq \min p_i^{z_i} < d_o$ if $m_i > 2z_i$. Hence the code must be degenerate

Quantum Duadic Codes - Hermitian Case

- We can also construct q-ary quantum codes from codes over $\mathbb{F}_{q^2}$
- The hermitian inner product between $x, y \in \mathbb{F}_{q^2}^n$ is defined as $x^q \cdot y$

Lemma

If $C^{\perp_h} \subseteq C \subseteq \mathbb{F}_{q^2}^n$ is an $[n, k, d]_{q^2}$ code, then there exists a $[[n, 2k - n, \geq d]]_q$ quantum code

Are there any self-orthogonal duadic codes?

If μ_{-q} gives a splitting, then duadic codes are self-orthogonal

Quantum Duadic codes

Theorem

If $\operatorname{ord}_n(q)$ is odd, then there exist quantum duadic codes with parameters $[[n, 1, d_o]]_q$.

As in the Euclidean case we can find degenerate quantum codes

Theorem

Let $n = \prod p_i^{m_i}$ be an odd integer with $\operatorname{ord}_n(q)$ odd and every $p_i \equiv -1 \bmod 4$. Let $t_i = \operatorname{ord}_{p_i}(q^2)$, and $p_i^{z_i} \| q^{2t_i} - 1$. Then for $m_i > 2z_i$, there exist degenerate quantum codes with parameters $[[n, 1, d]]_q$ pure to $d' \leq \min\{p_i^{z_i}\} < d$ with $d^2 - d + 1 \geq n$.

Summary

- Constructed new families of quantum codes based on the duadic codes
- Showed the existence of degenerate quantum duadic codes with large distance
- These methods can probably be generalized to polyadic codes to get degenerate codes with higher rate