The spectrum of stabilizer quantum codes of distance 3

Jürgen Bierbrauer
Department of Mathematical Sciences
Michigan Technological University
Houghton, Michigan 49931 (USA)

February 6, 2009

Abstract

We determine the parameters of the stabilizer quantum codes of minimum distance $d = 3$.

The translation from quantum coding to geometric algebra was done in [3].

Definition 1. *An additive quaternary quantum stabilizer $[[n, k, d]]$-code C (short: quantum code) where $k > 0$ is an additive code of length n with alphabet $Z_2 \times Z_2$ of binary dimension $r = n - k$ satisfying the following conditions:*

- *$C \subset C^\perp$ where the dual is with respect to the symplectic form.*
- *Each word of weight $< d$ in $C^\perp$ is in C.*

The code is **pure** *if $C^\perp$ has minimum weight $\geq d$.*

An $[[n, 0, d]]$-code C is a self-dual quaternary quantum stabilizer code of minimum weight $\geq d$.

In the present paper we determine the spectrum of quantum codes $[[n, n - r, 3]]$.

Theorem 1. *Let*

$$n_{max}(r) = (2^r - 8)/3 \text{ for odd } r, \ n_{max}(r) = (2^r - 1)/3 \text{ for even } r.$$

For odd $r \geq 5$ the spectrum of lengths n such that $[[n, n-r, 3]]$ exists consists of all integers between r and $n_{max}(r)$ except for $n_{max}(r) - 1$.

For even $r \geq 6$ the spectrum of lengths n such that $[[n, n-r, 3]]$ exists consists of all integers between r and $n_{max}(r)$ except for $n_{max}(r) - \{1, 2, 3\}$.

There exist pure codes for all parameters with the exception of $[[6, 1, 3]]$ (in case $r = 5$) which is necessarily impure.

The remainder of the paper is dedicated to the proof of Theorem 1. It follows rather directly from the results of [1] and [5].

The non-existence part of the proof

Consider at first pure $[[n, n-r, 3]]$-codes. As the geometric description is in terms of n pairwise skew lines in $PG(r-1, 2)$ it follows $n \leq (2^r - 1)/3$. In [1] it is shown that that there is no pure such code of length $n = (2^r - 1 - y)/3$ where $0 < y \leq 10, y \neq 7, 8$. This shows $n \leq n_{max}(r)$. It also shows that pure codes of length $n_{max}(r) - 1$ for odd r or of length $n_{max}(r) - 1, n_{max}(r) - 2, n_{max}(r) - 3$ for even r cannot exist.

Consider impure codes now. The geometric description of a length n quantum code as given in [1] is based on a multiset of n codeobjects each of which is a line or a point in $PG(r-1, 2)$. In case $d = 3$ the code is pure if the codeobjects form a set of mutually skew lines. It has been shown in [1], Proposition 3.1 that a quantum code with parameters $[[n-1, n-r, 3]]$ or $[[n-2, n-r, 3]]$ can be constructed if either one of the codeobjects is not a line or if some codeline occurs twice. This shows that we can assume that the codeobjects form a set of lines. Assume they are not mutually skew. It has been shown in [1] that the codelines intersecting some other codelines come in bundles. Let $P_1, P_2, \ldots, P_k$ be the points of $PG(r-1, 2)$ which are on more than one codeline and let $u_i \geq 2$ be the number of codelines through P_i. It was shown in [1], Theorem 3.2 that

$$n \leq (\sum u_i) + (2^{r - \sum(u_i - 1)} - 1 - k)/3.$$

This shows that impure codes $[[n, n-r, 3]]$ do not exist when $n \in n_{max}(r) - \{1, 2, 3\}$ for even r or $n = n_{max}(r) - 1$ for odd r.

The constructive part of the proof

Proceed by induction on r. We have to show that codes $[[n, n-r, 3]]$ exist for all $r \leq n \leq n_{max}(r)$ with the exception of the gaps as given in Theorem 1. Here we use the following obvious fact:

Lemma 1. *The existence of a pure $[[n, n-(r-1), 3]]$-code for $r \leq n$ implies the existence of a pure $[[n, n-r, 3]]$-code.*

The data base [4] and the results of [1] show in fact that the claim is true up to $r = 9$. The existence for length $n_{max}(r)$ is particularly evident in the geometric language. Those codes correspond to a spread of lines in $PG(r, 2)$ if r is even, to a partial spread covering the complement of a plane when r is odd. The latter case arises from an iterated use of the Blokhuis-Brouwer construction ([2], see Section 4 of [1]).

Let $r = 2l \geq 6$. Because of the induction hypothesis it suffices to show the existence of $[[n, n-2l, 3]]$-codes for n between $n_{max}(2l-1)-1 = (2^{2l-1}-11)/3$ and $n_{max}(2l) - 4 = (2^{2l} - 13)/3$. For $r = 6$ this is the interval $7 \leq n \leq 17$ where existence follows from the data base. For $r \geq 8$ existence of those codes with redundancy r is shown in [5] with the exception of length $(2^{2l-1}-8)/3$. As this length equals $n_{max}(2l-1)$ existence follows from Lemma 1.

Let $r = 2l + 1 \geq 7$. Because of the induction hypothesis it suffices to show the existence of $[[n, n-(2l+1), 3]]$-codes for n between $n_{max}(2l) - 3 = (2^{2l} - 10)/3$ and $n_{max}(2l+1) - 2 = (2^{2l+1} - 14)/3$. The constructions of [5] together with Lemma 1 cover all those lengths except for $n = (2^{2l+1} - 14)/3$.

Use the following construction, Corollary 4.3 of [1], which is a recursive version of the Blokhuis-Brouwer construction:

Proposition 1. *If a pure $[[n, n-r, 3]]$-code exists then so does a pure $[[2^r + n, 2^r + n - (r+2), 3]]$-code.*

Recursive application to the pure $[[38, 31, 3]]$-code constructed in [1] shows that pure $[[(2^{2l+1}-14)/3, (2^{2l+1}-14)/3-(2l+1), 3]]$-codes exist for all $l \geq 3$. This completes the proof.

References

[1] J. Bierbrauer, G. Faina, M. Giulietti, S. Marcugini, F. Pambianco: *The geometry of quantum codes, Innovations in Incidence Geometry* **6** (2007), 289-307.

[2] A. Blokhuis and A. E. Brouwer, *Small additive quaternary codes* *European Journal of Combinatorics* **25** (2004), 161-167.

[3] A. R. Calderbank, E. M. Rains, P. M. Shor, N. J. A. Sloane: *Quantum error-correction via codes over* $GF(4)$, *IEEE Transactions on Information Theory* **44** (1998), 1369-1387.

[4] http://www.codetables.de/

[5] S. Yu, Y. Dong, Q. Chen, C.H. Oh: *All the optimal stabilizer codes of distance* 3, *arXiv:0901.1968v1 [quant-ph] 14 Jan 2009.*