Geometric constructions of quantum codes

Jürgen Bierbrauer, D. Bartoli, S. Marcugini, and F. Pambianco

Abstract. We give a geometric description of binary quantum stabilizer codes. In the case of distance $d = 4$ this leads to the notion of a quantum cap. We describe several recursive constructions for quantum caps and construct in particular quantum 36-and 38-caps in $PG(4, 4)$. This yields quantum codes with new parameters $[[36, 26, 4]]$ and $[[38, 28, 4]]$.

1. Introduction

It has been shown in [**6**] that certain additive quaternary codes give rise to quantum codes. We use the following definition:

Definition 1. *A quaternary quantum stabilizer code is an additive quaternary code C which is contained in its dual, where duality is with respect to the symplectic form.*

A **pure** $[[n, l, d]]$*-code is a quaternary quantum stabilizer code of binary dimension $n - l$ and dual distance $\geq d$.*

The spectrum of quantum stabilizer codes of distance 2 is easily determined. The complete determination of the parameter spectrum of additive quantum codes of distance 3 is given in [**3**]. The analogous problem for $d = 4$ is wide open. A recent result is the non-existence of a $[[13, 5, 4]]$ quantum code, see [**5**].

In [**4**] we formulate the problem in geometric terms. Here we concentrate on the special case when $d = 4$ and the code is quaternary linear. This leads to the following definition:

Definition 2. *A set of n points in $PG(m-1, 4)$ is* **pre-quantum** *if it satisfies the following equivalent conditions:*

- *The corresponding quaternary $[n, m]_4$ code has all weights even.*
- *Each hyperplane meets the set in the same parity as the cardinality of the set.*

It is a **quantum cap** *if moreover it is a cap and generates the entire ambient space.*

It is in fact easy to see that the conditions in Definition 2 are equivalent. The translation result is the following (see [**4**]):

Theorem 1. *The following are equivalent:*

- *A pure quantum code $[[n, n - 2m, 4]]$ which is linear over $\mathbb{F}_4$.*

- *A quantum n-cap in $PG(m-1,4)$.*

The relation between the two items of Theorem 1 is as follows: let C be the quaternary linear code describing the $[[n,n-2m,4]]$-quantum code and M a generator matrix of C. Then M is an (m,n)-matrix with entries from $\mathbb{F}_4$. A corresponding quantum cap is described by the projective points defined by the columns of M.

In this paper we concentrate on quantum caps in $PG(3,4)$ and in $PG(4,4)$. In the next section we review a known recursive construction. In the final section we construct quantum 36-and 38-caps in $PG(4,4)$. This yields positive answers to the existence questions of quantum codes $[[36,26,4]]$ and $[[38,28,4]]$ that remained open in the data base [**9**]. These quantum codes are best possible as $[[36,26,5]]$- and $[[38,28,5]]$-quantum codes cannot exist.

2. A recursive construction

The most obvious recursive construction is the following:

THEOREM 2. *Let K_1,K_2 be disjoint pre-quantum sets in $PG(m-1,4)$. Then $K_1\cup K_2$ is pre-quantum.*
Let $K_1\subset K_2$ be pre-quantum sets. Then also $K_2\setminus K_1$ is pre-quantum.

The proof is trivial. Theorem 2 leads to the question when a subset of a pre-quantum set is pre-quantum. This can be expressed in coding-theoretic terms.

DEFINITION 3. *Let M be a quaternary (m,n)-matrix whose columns generate different points, and K the corresponding n-set of points in $PG(m-1,4)$. The* **associated binary code** *A is the binary linear code of length n generated by the supports of the quaternary codewords of the code generated by M.*

Observe that by definition K is pre-quantum if and only if A is contained in the all-even code. This leads to the following characterization:

THEOREM 3. *Let $K\subset PG(m-1,4)$ be pre-quantum and $K_1\subseteq K$. Then K_1 (and its complement $K\setminus K_1$) is pre-quantum if and only if the characteristic vector of K_1 is contained in the dual $A^\perp$ of the binary code A associated to K.*

This is essentially Theorem 7 of [**6**]. It can be used in two ways. One is to start from a quantum cap K and construct (pre-)quantum caps $K_1\subset K$ contained in it. This is the point of view taken by Tonchev in [**11**]. In fact the maximum size of a cap in $PG(4,4)$ is 41, there are two such caps and one is quantum. Also, there is a uniquely determined 40-cap in $AG(4,4)$ and it is quantum (for these facts see [**7, 8**]). Tonchev starts from the quantum 41-cap and determines its quantum subcaps. This leads to quantum caps of sizes $n\in\{10,12,14-27,29,31,33,35\}$ in $PG(4,4)$. It is easy to see that the smallest pre-quantum cap in any dimension is the hyperoval in the plane. By Theorem 2 it follows that this method cannot produce quantum caps of sizes between 36 and 40 in $PG(4,4)$. Tonchev then applies the same method to the Glynn cap (a 126-cap in $PG(5,4)$) and also produces a linear $[[27,13,5]]$ quantum code.

We take a more geometric point of view. Here is a direct application of Theorem 2:

COROLLARY 1. *Assume there exist a quantum i-cap in $AG(m-1,4)$ and a pre-quantum j-cap in $AG(m-1,4)$. Then there is a quantum $(i+j)$-cap in $PG(m,4)$.*

PROOF. Let H_1, H_2 be different hyperplanes in $PG(m,4)$ and $S = H_1 \cap H_2$. Represent the i-cap on $H_1 \setminus S$ and the j-cap on $H_2 \setminus S$. The corresponding disjoint union clearly is a cap and it is pre-quantum. As the i-cap generates $PG(m-1,4)$ and the j-cap is not empty together the caps generate all of $PG(m,4)$. $\square$

As an example, the union of two hyperovals on different planes H_1, H_2 of $PG(3,4)$ is a quantum 12-cap provided $H_1 \cap H_2$ is an exterior line of both hyperovals. In the next section we briefly describe the quantum caps in $PG(3,4)$ as they are needed as ingredients for the recursive constructions.

3. Quantum caps in $PG(3,4)$

It can be shown that the sizes of quantum caps in $PG(3,4)$ are $8, 12, 14$ and 17 (see [**1**]). Theorem 1 shows that this can be expressed equivalently as follows: pure linear $[[n, n-8, 4]]$-quantum codes exist precisely for $n \in \{8, 12, 14, 17\}$. Here the 17-cap is the elliptic quadric, obviously quantum. The construction of a quantum 12-cap was described in the previous section. The quantum 8-cap A can be described as the set-theoretic difference of $PG(3,2)$ and a Fano subplane. It has the peculiarity not to contain a coordinate frame. Another description of A is based on hyperovals: choose hyperovals $\mathcal{O}_1, \mathcal{O}_2$ on two planes which share two points on the line of intersection. The symmetric sum $\mathcal{O}_1 + \mathcal{O}_2$ is then the quantum 8-cap.

The quantum 14-cap in $PG(3,4)$ is a highly interesting object. It is the uniquely determined complete 14-cap in $PG(3,4)$. Its group of automorphisms is the semidirect product of an elementary abelian group of order 8 and $GL(3,2)$ (see [**7**]). It contains 7 hyperovals. Here is a construction using only hyperovals: there is a configuration in $PG(3,4)$ consisting of three collinear planes and a hyperoval in each plane, where the line of intersection is a secant for all three hyperovals. The symmetric sum of two hyperovals is then our quantum 8-cap and the union of all three hyperovals is the quantum 14-cap. This shows also that we can think of the 14-cap as a disjoint union of a hyperoval and a quantum 8-cap. In Section 6 we will construct a quantum 38-cap in $PG(4,4)$ based on four copies of the quantum 14-cap on four hyperplanes. For that purpose we give a more detailed description.

DEFINITION 4. *Let $\mathcal{O}$ be a hyperoval and Π_0 a Fano plane of $PG(2,4)$. Then $\mathcal{O}$ and Π_0 are* **well-positioned** *if $\mathcal{O} \cap \Pi_0 = \emptyset$ and if the three lines of Π_0 containing the points of $\mathcal{O}$ are concurrent in a point $P \in \Pi_0$. Write then $\Pi_0 = \Pi(P, \mathcal{O})$.*

LEMMA 1. *Let $\mathcal{O}$ be a hyperoval in $PG(2,4)$. There are precisely 15 Fano planes in $PG(2,4)$ which are well-positioned with respect to $\mathcal{O}$.*

PROOF. This follows directly from the definition. Those 15 Fano planes are the $\Pi_0(P)$ where P varies over the points outside $\mathcal{O}$. Recall that $PG(2,4)$ and its hyperovals and Fano planes play a central role in the construction of the large Witt design as it is described for example in Hughes-Piper [**10**]. There are 360 Fano planes in $PG(2,4)$ and each is well-positioned with respect to 7 hyperovals, one for each bundle of lines through a point of the Fano plane. There are 168 hyperovals and so it is not surprising that each hyperoval is well-positioned with respect to 15 Fano planes. $\square$

LEMMA 2. *Let E be a plane in $PG(3,4)$ and $\mathcal{O} \subset E$ a hyperoval. Let $\Pi \subset PG(3,4)$ be a $PG(3,2)$ and $\Pi_0 = \Pi \cap E$ a Fano plane. Let $A = \Pi \setminus \Pi_0$. Then $A \cup \mathcal{O}$ is a cap if and only if $\mathcal{O}$ and Π_0 are well-positioned in E.*

PROOF. Let $P \in \Pi_0$ and $\mathcal{O}$ the union of the points $\notin \Pi_0$ on the union of the lines of Π_0 through P. The fact that Π_0 is a blocking set in E shows that $\mathcal{O}$ is a cap, hence a hyperoval. $\square$

Lemma 2 shows one way to describe the complete 14-caps in $PG(3,4)$: start from a subgeometry $\Pi = PG(3,2)$ and a Fano plane $\Pi_0 \subset \Pi$. Let $A = \Pi \setminus \Pi_0$ and E the subplane $PG(2,4)$ generated by Π_0. Pick $P \in \Pi_0$ and let $\mathcal{O}$ be the union of the points of $E \setminus \Pi_0$ on the lines of Π_0 through P. Then $A \cup \mathcal{O}$ is a complete (quantum) 14-cap. This is not a parametrization as each 14-cap can be written like that in 7 ways.

4. Applications of Theorem 2

Application of Corollary 1 to the quantum caps in $PG(3,4)$ (only the elliptic quadric is not affine) and to the pre-quantum 6-cap (the hyperoval in a plane) yields quantum caps in $PG(4,4)$ of sizes

$$14+6=20, 12+6=18, 8+6=14, 14+8=22, 14+12=26,$$

$$14+14=28, 12+8=20, 12+12=24, 8+8=16.$$

Corollary 1 can be slightly generalized so as to allow the use of the elliptic quadric K_1 on H_1. Let $\{P\} = K_1 \cap S$ and $K_2 \subset AG(3,4)$ a pre-quantum cap. Then $K_1 \cup K_2$ is a quantum cap provided $K_2 \cup \{P\}$ is a cap. This works for $j = 6, 8$ and thus yields quantum caps of sizes $17+6=23, 17+8=25$ in $PG(4,4)$. It does not work for $j = 12$ or $j = 14$ as those quantum caps in $AG(3,4)$ are complete in $PG(3,4)$ (see [**2**]). The union of two disjoint hyperovals on two planes which meet in a point yields a quantum 12-cap in $PG(4,4)$.

5. A more general recursive construction

THEOREM 4. *Let Π_1, Π_2 be different hyperplanes of $PG(m,4)$ and $K_i \subset \Pi_i$ be pre-quantum caps such that $K_1 \cap \Pi_1 \cap \Pi_2 = K_2 \cap \Pi_1 \cap \Pi_2$. Then the symmetric sum $K_1 + K_2 = (K_1 \setminus K_2) \cup (K_2 \setminus K_1)$ is a pre-quantum cap.*

PROOF. It is clear that $K_1 + K_2$ is a cap. Only the quantum condition needs to be verified. Let H be a hyperplane. If H contains $\Pi_1 \cap \Pi_2$ there is no problem. Assume this is not the case. Then H meets each of $\Pi_1, \Pi_2, \Pi_1 \cap \Pi_2$ in a hyperplane. By the pre-quantum condition applied to $K_i \subset \Pi_i$ it follows that the sets $(K_1 \cap K_2) \setminus H, K_1 \setminus (K_2 \cup H), K_2 \setminus (K_1 \cup H)$ all have the same parity. $\square$

If we apply Theorem 4 to an elliptic quadric on one of the hyperplanes then we must choose an elliptic quadric on the second hyperplane as well. This leads to quantum 24- and 32-caps. The other ingredients can be combined. Observe that all of them have planes with 0 or 2 or 4 intersection points and all but the 8-cap also contain a hyperoval. This leads to quantum caps of sizes

$$6+8=14, 8+8=16, 4+8=12, 4+10=14, 8+10=18, 10+10=20,$$

$$6+6=12, 6+10=16, 6+12=18, 10+12=22, 12+12=24, 8+8=16,$$

$$8+12=20, 8+14=22, 12+12=24, 12+14=26, 14+14=28.$$

6. New quantum caps in $PG(4,4)$.

Let $\mathbb{F}_4 = \{0, 1, \omega, \overline{\omega}\}$. In this section we will write for brevity $2 = \omega, 3 = \overline{\omega}$.

A quantum 36-cap in $PG(4,4)$. Fix a plane E and three different hyperplanes H_1, H_2, H_3 containing E. Let $V \cup \{N\}$ be an oval in E, let $K_3 \subset H_3$ be a quantum 12-cap (union of two hyperovals) such that $K_3 \cap E = V$ and let $K_i, i = 1, 2$ be elliptic quadrics in H_i such that $H_i \cap E = V \cup \{N\}$. Define

$$K = K_1 \cup K_2 \cup K_3 \setminus \{N\}.$$

Then $|K| = 4 + 12 + 12 + 8 = 36$. We claim that K is pre-quantum. Let H be a hyperplane. There is no problem if H contains E. Let $g = H \cap E$, a line. As K_3 is pre-quantum it generates no problems. It is obvious that H intersects $K_1 \setminus E$ and $K_2 \setminus E$ in the same cardinality. This proves the statement.

In order to obtain the promised quantum cap it remains to be shown that K can be chosen to be a cap. Here is one such quantum cap:

$$\left(\begin{array}{c|c|c|c|c}
0000 & 000000000000 & 111111111111 & 1111 & 1111 \\
0000 & 111111111111 & 000000000000 & 1111 & 1111 \\
0101 & 000111222333 & 000111222333 & 0123 & 0123 \\
1211 & 001223002022 & 223001022002 & 1133 & 0011 \\
1031 & 020311033212 & 022133112030 & 2031 & 0202
\end{array}\right)$$

A quantum 38-cap in $PG(4,4)$. Start from a subplane $E = PG(2,4)$ of $PG(4,4)$ defined by $x_1 = x_2 = 0$ and a hyperoval $\mathcal{O}$ of E which we choose as the union of $P_y = (0:0:1:y:y^2)$ for $y \in GF(4)$, $P_\infty = (0:0:0:0:1)$ and the nucleus $N = (0:0:0:1:0)$. Concretely

$$\mathcal{O} = \{00100, 00010, 00001, 00111, 00123, 00132\}.$$

Next choose a point $Q \in E \setminus \mathcal{O}$. Without restriction $Q = (0:0:1:1:0)$. Then Q is on two exterior lines with respect to $\mathcal{O}$. Those are $[1:1:2]$ and $[1:1:3]$. The points $\neq Q$ on $[1:1:2]$ are $R_1 = 013, R_2 = 103, R_3 = 122, R_4 = 131$ where we used an obvious notational convention. Consider the Fano planes $F_i = \Pi(R_i, \mathcal{O})$ (see Definition 4). By definition F_i is well-positioned with respect to $\mathcal{O}$.

Consider now the four hyperplanes H_1, H_2, H_3, H_4 containing E which are defined by $x_1 = 0, x_2 = 0, x_2 = 3x_1$ and $x_2 = 2x_1$, respectively. Representatives for points in $H_i \setminus E$ will always be written in the form $01*, 10*, 21*$ and $31*$, respectively. Let now G_i be a subspace $PG(3,2)$ of H_i which contains the Fano plane F_i and let $A_i = G_i \setminus F_i, i = 1,2,3,4$. Then A_i is a quantum 8-cap in H_i and $A_i \cup \mathcal{O}$ is a quantum 14-cap. Let $K = \mathcal{O} \cup A_1 \cup A_2 \cup A_3 \cup A_4$. Then K is a quantum set of 38 points. It is a quantum cap if and only if it is a cap. The question is if G_i can be chosen in a way such that this is the case. It seems to be advantageous to switch to vector space language. Then $F_1 = \langle 013, 022, 203 \rangle$ where $\langle\rangle$ denotes the three-dimensional space over $\mathbb{F}_2$ generated by those vectors. Likewise $F_2 = \langle 103, 202, 023 \rangle$ and $F_3 = \langle 122, 011, 301 \rangle, F_4 = \langle 131, 023, 303 \rangle$.

Lemma 3.

$$S_4 = F_1 + F_3 = \langle 002, 020, 033, 100, 303 \rangle, S_3 = F_1 + F_4 = \langle 001, 030, 013, 100, 310 \rangle,$$

$$S_2 = 3F_1 + F_4 = \langle 001, 010, 023, 320, 200 \rangle, S_1 = F_2 + F_3 = \langle 002, 030, 021, 200, 320 \rangle.$$

Furthermore $2F_2 \subset S_4, 3F_2 \subset S_3, 2F_3 \subset S_2, F_4 \subset S_1$.

This is easy to check. Let now

$$G_1 = 01a_1 + F_1, G_2 = 10a_2 + F_2, G_3 = 21a_3 + F_3, G_4 = 31a_4 + F_4.$$

The cap condition is then equivalent to the following four conditions being satisfied

- $b_4 = a_1 + 2a_2 + a_3 \notin S_4$.
- $b_3 = a_1 + 3a_2 + a_4 \notin S_3$.
- $b_2 = 3a_1 + 2a_3 + a_4 \notin S_2$.
- $b_1 = a_2 + a_3 + a_4 \notin S_1$.

Observe $b_1 = b_3 + b_4, b_2 = b_3 + 2b_4$. It follows that all we need to find are elements $b_3 \notin S_3, b_4 \notin S_4$ such that $b_3 + b_4 \notin S_1, b_3 + 2b_4 \notin S_2$. One possible choice is $b_3 = 011, b_4 = 001$ and $a_1 = 220, a_2 = 113, a_3 = 000, a_4 = 103$. Here is the cap:

$$\left(\begin{array}{c|c|c|c|c} 000000 & 00000000 & 11111111 & 22222222 & 33333333 \\ 000000 & 11111111 & 00000000 & 11111111 & 11111111 \\ 100111 & 22202000 & 10312032 & 01031232 & 10120323 \\ 010123 & 23021301 & 11131333 & 02103213 & 03201321 \\ 001132 & 03231012 & 30102321 & 02113302 & 32001132 \end{array}\right)$$

References

[1] D. Bartoli, S. Marcugini, F. Pambianco: *A computer based classification of caps in PG(3,4),* Rapporto Tecnico N. 8/2009 del Dipartimento di Matematica e Informatica, Università degli Studi di Perugia.

[2] D. Bartoli, J. Bierbrauer, S. Marcugini, F. Pambianco: *The structure of binary quantum caps,* in preparation.

[3] J. Bierbrauer: *The spectrum of stabilizer quantum codes of distance* 3, submitted for publication in *IEEE Transactions on Information Theory.*

[4] J. Bierbrauer, G. Faina, M. Giulietti, S. Marcugini, F. Pambianco: *The geometry of quantum codes, Innovations in Incidence Geometry* **6** (2009), 53-71.

[5] J. Bierbrauer, S. Marcugini, F. Pambianco: *The non-existence of a* $[[13, 5, 4]]$ *quantum stabilizer code,* ArXiv 0908.1348v1.

[6] 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.

[7] Y.Edel and J. Bierbrauer: 41 *is the largest size of a cap in* $PG(4, 4)$, *Designs, Codes and Cryptography* **16**(1999),151-160.

[8] Y.Edel and J. Bierbrauer: *The largest cap in* $AG(4, 4)$ *and its uniqueness, Designs, Codes and Cryptography* **29** (2003), 99-104.

[9] M. Grassl: http://www.codetables.de/

[10] D.R. Hughes and F.C. Piper: *Design Theory,* Cambridge University Press 1985.

[11] V. Tonchev: *Quantum codes from caps, Discrete Mathematics* **308** (2008), 6368-6372.

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

Dipartimento di Matematica e Informatica, Università degli Studi di Perugia, Perugia (Italy)

Dipartimento di Matematica e Informatica, Università degli Studi di Perugia, Perugia (Italy)

Dipartimento di Matematica e Informatica, Università degli Studi di Perugia, Perugia (Italy)