The structure of quaternary quantum caps

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

D. Bartoli, G. Faina, S. Marcugini and F. Pambianco
Dipartimento di Matematica e Informatica
Università degli Studi di Perugia
Perugia (Italy)

Yves Edel†
Department of Mathematics
Ghent University (Belgium)

March 6, 2013

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 quaternary quantum cap. We describe several recursive constructions for quantum caps, determine the quantum caps in $PG(3, 4)$ and the cardinalities of quantum caps in $PG(4, 4)$.

*research partially supported NSA grant H98230-10-1-0159

†The research of this author takes place within the project "Linear codes and cryptography" of the Research Foundation – Flanders (FWO) (Project nr. G.0317.06), and is supported by the Interuniversitary Attraction Poles Programme - Belgian State - Belgian Science Policy: project P6/26-Bcrypt.

Key words

quantum cap, quaternary code, quantum stabilizer code, symplectic geometry, projective space, trace, hyperoval, elliptic quadric.

MSC classification

11T71, 51E22, 81P70.

1 Introduction

One of the results of the seminal paper [6] is a description of a class of quantum codes, the quantum stabilizer codes, in terms of certain additive quaternary codes. Additive quaternary codes are defined over an alphabet of 4 letters and linear over the binary field $\mathbb{F}_2$. A generalization of this mechanism from base field $\mathbb{F}_2$ to base field $\mathbb{F}_q$ was first defined in [3], Definition 1. This results in a description of q-ary quantum stabilizer codes in terms of q^2-ary $\mathbb{F}_q$-linear codes. A theory of **cyclic** q-ary quantum stabilizer codes is developed in [3] as well. The definition of q^2-ary $\mathbb{F}_q$-linear quantum stabilizer codes $[[n,k,d]]_q$ has been rediscovered in various occasions in the meantime. In the classical quaternary case (observe that the ground field is $\mathbb{F}_2$) an equivalent geometric formulation in terms of sets of lines in binary projective spaces has been given in [5], see also [10]. In the present paper we concentrate on the special case of **linear** q-ary quantum codes where the q^2-ary codes are indeed $\mathbb{F}_{q^2}-$linear.

Definition 1. *A linear q^2-ary quantum stabilizer code is a subspace $\mathcal{C} \subset \mathbb{F}_{q^2}^n$ such that $\mathcal{C} \subseteq \mathcal{C}^\perp$ where duality is with respect to the Hermitian inner product.*

Here the Hermitian inner product of $x = (x_1, \ldots, x_n)$ and $y = (y_1, \ldots, y_n)$ is $\langle x, y\rangle = \sum_{i=1}^n x_i y_i^q$. The reason for this definition is that a linear q^2-ary quantum stabilizer code $\mathcal{C}$ of length n, dimension m and dual distance $\geq d$ (equivalently: of strength $> d$) allows the construction of a pure quantum stabilizer code $[[n, n-2m, d]]_q$ (see [3], Theorem 1). Consider the geometric description of the linear q^2-ary code $\mathcal{C}$: the columns of a generator matrix describe a set of n points in $PG(m-1, q^2)$ such that any $d-1$ of those points are in general position (they generate $PG(d-2, q^2)$). If this is satisfied, then

$\mathcal{C}$ from Definition 1 (of dimension m and strength $d-1$) defines a quantum code $[[n, n-2m, d]]_q$.

The paper is organized as follows: in Sections 2,3 we consider q-ary quantum stabilizer codes for an arbitrary prime-power q. In Section 2 we show that self-orthogonal linear q-ary codes allow the construction of q-ary quantum stabilizer codes (Theorem 1). Theorem 2 in Section 3 is a projection construction which generalizes Theorem 7 of [6] from the binary case to the case of an arbitrary prime-power q. From then on we restrict to the binary case $q = 2$ and abbreviate the parameters of binary quantum stabilizer codes $[[n, m, d]]_2$ by $[[n, m, d]]$. Recall that the equivalent coding-theoretic description is in terms of quaternary additive codes. We restrict to the special case that this quaternary code is in fact $\mathbb{F}_4$-linear.

In Section 4 the notion of a quantum cap is defined. This is the geometric expression for distance 4 $\mathbb{F}_4$-linear pure quantum codes (see Theorem 3). The remainder of the paper is a systematic study of quaternary quantum caps in low-dimensional projective spaces. Equivalence of caps in $PG(m-1, 4)$ is with respect to the group $P\Gamma L(m, 4)$. We start in Section 5 by showing that there are no quantum n-caps of cardinality $n < 6$ in any space $PG(m-1, 4)$, and there is precisely one quantum 6-cap, the hyperoval in $PG(2, 4)$. In Section 6 some elementary recursive constructions for quantum caps are discussed. Section 7 contains a complete census of the quantum caps in $PG(3, 4)$. They exist of cardinalities $8, 12, 14$ and 17. For each cardinality there is precisely one such cap. We determine also the automorphism groups and give various different constructions. One motivation is that those caps can be used as ingredients for the construction of quantum caps in higher-dimensional spaces via the recursive constructions. In Section 8 we study quantum caps in $PG(4, 4)$. One main result is the complete determination of all cardinalities n for which quantum caps exist in $PG(4, 4)$, see Theorem 10. We close in Section 9 with a construction for small quantum caps in spaces of arbitrary dimension.

2 Quantum subfield subcodes

Theorem 1. *Let G a generator matrix of a self-orthogonal linear q-ary code $\mathcal{D} \subseteq \mathcal{D}^{\perp}$ of parameters $[n, m, d]_q$ where duality is with respect to the Euclidean bilinear form (the dot product). Seen over $\mathbb{F}_{q^2}$, matrix G generates an $[n, m, d]_{q^2}$-code which is a quantum code. If the q^2-ary code has strength*

t, *then the quantum parameters are* $[[n, n-2m, t+1]]_q$.

Proof. The definition of the Hermitian inner product shows that the q^2-ary code $\mathcal{C}$ generated by G is Hermitian self-orthogonal. Code $\mathcal{C}$ is Galois closed (for the notion of a Galois closed linear code see Section 12.3 of [2]) and $\mathcal{D}$ is its subfield code. If $\mathcal{D}$ is an $[n, m, d]_q$-code, then $\mathcal{C}$ is an $[n, m, d]_{q^2}$-code (see [2], Theorem 12.17). It therefore defines a linear q^2-ary $[[n, n-2m, d]]_q$-quantum code. □

As an example consider the ternary Golay code, a self-dual $[12, 6, 6]_3$-code. By Theorem 1 it defines a 9-ary quantum code with the same parameters and therefore a $[[12, 0, 6]]_3$-quantum code. Another example is the extended binary Hamming code $[8, 4, 4]_2$ (geometrically: the points of $PG(3, 2) \setminus PG(2, 2)$) which defines a Hermitian self-dual $[8, 4, 4]_4$-code. Geometrically it is represented by a set of 8 points in $PG(3, 4)$. Any 3 of those points are in general position, meaning that they are not collinear. We will speak of a quantum 8-cap below, see Definition 4. In particular this defines a binary $[[8, 0, 4]]$ quantum code.

3 Quantum codes by projection

Definition 2. *Let* $N : \mathbb{F}_{q^2} \longrightarrow \mathbb{F}_q$ *the norm* ($N(x) = x^{q+1}$). *Let* $\mathcal{C}$ *be an* $\mathbb{F}_{q^2}$*-linear code of length* n. *The* **norm code** *of* $\mathcal{C}$ *is the code* $N(\mathcal{C}) \subseteq \mathbb{F}_q^n$ *spanned over* $\mathbb{F}_q$ *by the norms* $N(u) = (N(u_1), \ldots, N(u_n))$ *where* $u = (u_1, \ldots, u_n) \in \mathcal{C}$. *Denote by* $N(\mathcal{C})^\perp$ *its dual with respect to the Euclidean bilinear form.*

Lemma 1. *Let the Hermitian bilinear form be defined on* $\mathbb{F}_{q^2}^n$ *by* $\langle (x_1, \ldots, x_n), (y_1, \ldots, y_n) \rangle = \sum x_i y_i^q$. *Let* $\mathcal{C} \subset \mathbb{F}_{q^2}^n$ *a linear code. Then* $\mathcal{C}$ *is self-orthogonal with respect to the Hermitian form if and only if* $\langle u, u \rangle = 0$ *for all* $u \in \mathcal{C}$.

Proof. Assume $\langle u, u \rangle = 0$ for all $u \in \mathcal{C}$, let $u, v \in \mathcal{C}, \lambda \in \mathbb{F}_{q^2}$. Then

$$0 = \langle \lambda u + v, \lambda u + v \rangle = \langle \lambda u, v \rangle + \langle v, \lambda u \rangle = T(\lambda \langle u, v \rangle)$$

where $T(\alpha) = \alpha + \alpha^q$ is the trace : $\mathbb{F}_{q^2} \longrightarrow \mathbb{F}_q$. It follows that $\alpha = \langle u, v \rangle$ has the property $T(\lambda\alpha) = 0$ for all $\lambda \in \mathbb{F}_{q^2}$. This shows $\alpha = 0$. □

Theorem 2. *Let* $\mathcal{C} \subset \mathbb{F}_{q^2}^n$ *a linear code and* $u \in N(\mathcal{C})^\perp$. *Then the projection from* $\mathcal{C}$ *to the support of* u *is equivalent to a linear* q^2*-ary quantum stabilizer code in the sense of Definition 1.*

Proof. Assume the support of u consists of the first m coordinates. By code equivalence it can be assumed $u = (1, 1, \ldots, 1, 0, \ldots, 0)$. Let $u, v \in \mathcal{C}$ and π the projection to the first m coordinates. We have to show $\langle \pi(u), \pi(v) \rangle = 0$ for all $u, v \in \mathcal{C}$. By Lemma 1 it suffices to show $\langle \pi(u), \pi(u) \rangle = 0$ for all $u \in \mathcal{C}$, equivalently $\sum_{i=1}^{m} u_i u_i^q = \sum_{i=1}^{m} N(u_i) = 0$ which is satisfied by definition of the norm code. □

In particular $\mathcal{C}$ itself is a linear q^2-ary quantum stabilizer code if and only if $N(\mathcal{C})^\perp$ contains the all-1-word, and it is equivalent to such a quantum code if and only if $N(\mathcal{C})^\perp$ contains a word of full weight n. Theorem 7 of [6] is the special case of Theorem 2 when $q = 2$ and $\mathcal{C}$ itself is a linear quaternary quantum stabilizer code. Observe that in case $q = 2$ the self-orthogonality condition is independent of code equivalence. This follows from the fact that $\lambda^{q+1} = \lambda^3 = 1$ for all $0 \neq \lambda \in \mathbb{F}_4$. For $q > 2$ the self-orthogonality condition is not independent of the choice of generators of the projective points in the geometric description of $\mathcal{C}$. This is one motivation to restrict further to the linear quaternary case (case $q = 2$ of Definition 1) in the sequel.

4 Quaternary quantum caps

The spectrum of quaternary quantum codes of distances $d \leq 3$ is completely known, see [16]. We consider the first open case of distance $d = 4$. The points of $PG(m-1, 4)$ describing the columns of a generator matrix of $\mathcal{C}$ have the property that no three are on a line.

Definition 3. *A point set in $PG(k, q)$ is a* **cap** *if no three points are on a line.*

For a recent survey concerning caps in projective Galois spaces see [4]. Definition 3 leads to the following notion:

Definition 4. *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 its weights even.*
- *Each hyperplane meets the set in the same parity as the cardinality of the set.*

It is **quantum** *if in addition it is not contained in a hyperplane. It is a* **quantum cap** *if moreover it is a cap.*

It is in fact easy to see that the conditions in Definition 4 are equivalent. The translation from coding-theoretic to geometric language is given by the following (see [5]):

Theorem 3. *The following are equivalent:*

- *A pure quantum code* $[[n, n-2m, 4]]$ *which is linear over* $\mathbb{F}_4$.
- *A quantum* n*-cap in* $PG(m-1, 4)$.

5 The smallest quantum cap

It is an elementary and important fact that the hyperoval in $PG(2, 4)$ is the only quantum cap in projective dimension ≤ 2.

Proposition 1. *There is no quantum cap in the projective line. The only quantum cap in* $PG(2, 4)$ *is the hyperoval. This is the uniquely determined smallest quantum cap in any projective dimension.*

Proof. It is immediately clear that sets of one or two points in $PG(1, 4)$ are not quantum. All caps in $PG(2, 4)$ are contained in the hyperoval. For any proper subset K of the hyperoval there are lines avoiding the set as well as tangents. This shows that K is not quantum. Consider a quantum cap K of size $n \leq 6$ in $PG(m, 4), m \geq 3$. As the quantum cap has to generate the ambient space, we have $n \geq 4$. Observe that a contradiction is obtained if we can find hyperplanes intersecting K in different parities. This is the case in particular if K is in general position. Case $n = 4$ is therefore excluded. If $n = 5$ and K is not in general position, then $m = 3$ and either K is a coordinate frame or $K \subset PG(3, 4)$ has some 4 points on a plane. The latter case contradicts the definition of a quantum cap. In the former case it is easy to see that there are planes meeting K in 3 points and also there are planes meeting K in 2 points, contradiction. Let finally $n = 6$. If $m = 3$, then some 4 points are in a plane Π. Let $l \subset \Pi$ be a line meeting K in precisely one point. It follows that one of the 5 planes containing l must meet K in just one point. This contradicts the definition of a quantum cap. If $m = 5$, then K is in general position and a contradiction results. The last case is

$m = 4$. Let Π be a plane meeting K in precisely 3 points. Each of the 5 solids containing Π must pick up at least one additional point of K. This yields the contradiction $|K| \geq 3 + 5$. □

$\mathcal{K}(2,6)$	
100	111
010	132
001	123

The quantum code described by the hyperoval has parameters $[[6, 0, 4]]$.

6 Recursive constructions

The most obvious recursive construction is the following:

Theorem 4. *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 5. *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. As $K = K_1 + K_2$ does not meet $\Pi_1 \cap \Pi_2$, it is a cap. Only the quantum condition needs to be verified. The pre-quantum conditions of $K_1 \subset \Pi_1$ and $K_2 \subset \Pi_2$ imply that $|K|$ is even. Let H be a hyperplane. If H contains $\Pi_1 \cap \Pi_2$, then either H is different from Π_1, Π_2 and $H \cap K = \emptyset$ or $H = \Pi_i, i = 1, 2$ and $|H \cap K|$ is even because of the quantum condition satisfied by $K_i \subset \Pi_i$. Assume H does not contain $\Pi_1 \cap \Pi_2$. 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. □

Here are two applications of Theorem 5: Let $K_i \subset E_i$ be hyperovals in planes E_i of $PG(3, 4), i = 1, 2$. If $E_1 \cap E_2$ is an exterior line of both K_1 and K_2, then $K_1 \cup K_2$ is a quantum 12-cap in $PG(3, 4)$. If K_1 and K_2 meet in two points, then $K_1 + K_2$ is a quantum 8-cap.

Theorem 6. *Π_1, Π_2 be different hyperplanes of $PG(m,4), S = \Pi_1 \cap \Pi_2$. Let $K_1 \subset \Pi_1$ be a quantum cap in Π_1 and $K_2 \subset \Pi_2 \setminus S$ an (affine) pre-quantum cap. Assume $K_2 \cup (K_1 \cap S)$ is a cap. Then $K_1 \cup K_2$ is a quantum cap.*

Proof. $K_1 \cup K_2$ is pre-quantum by Theorem 4. It is a cap if and only if $K_2 \cup (K_1 \cap E)$ is a cap. Clearly it is not contained in a hyperplane. □

Theorem 6 applies in particular when $|K_1 \cap S| = 1$ and K_2 is a pre-quantum cap which can be extended to a cap by a point in the secundum S.

Theorem 7. *Let Π_1, Π_2 be different $(m-2)$-dimensional subspaces of $PG(m,4)$ which together generate $PG(m,4)$. Let $K_i \subset \Pi_i$ 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 $K_1 + K_2$ is a pre-quantum cap.*

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

Recall that equivalence is with respect to the action of the group $G = P\Gamma L(4,4)$ of order $g = 2^{13}(4^4-1)(4^3-1)(4^2-1) = 2^{13} \times 3^4 \times 5^2 \times 7 \times 17$.

Theorem 8. *The sizes of quantum caps in $PG(3,4)$ are $8, 12, 14$ and 17. For each of these cardinalities there is up to equivalence exactly one such quantum cap.*

The unique quantum cap in projective dimension 2, the hyperoval in $PG(2,4)$, will be denoted by $\mathcal{K}(2,6)$, see Section 5. The quantum caps in $PG(3,4)$ will be denoted $\mathcal{K}(3,8), \mathcal{K}(3,12), \mathcal{K}(3,14), \mathcal{K}(3,17)$. Let G_i be the automorphism group of $\mathcal{K}(3,i)$ (the stabilizer in G) and $g_i = |G_i|$. Denote by a_j the number of planes meeting K in cardinality j (the j-planes). In the remainder of this section we prove Theorem 8 and give various descriptions of those four quantum caps.

The elliptic quadric $\mathcal{K}(3,17)$.

The upper bound is obvious: it is known that the unique largest cap in $PG(3,4)$ is the elliptic quadric of 17 points, see [13]. As it meets each hyperplane in 1 or 5 points, it follows that the elliptic quadric in $PG(3,4)$ is indeed quantum. G_{17} has order $g_{17} = 16320 = 17 \times 16 \times 15 \times 4$ and contains

the simple group $SL(2,16)$ in its sharply triply transitive action on $\mathcal{K}(3,17)$. Clearly $a_1 = 17$ and $a_5 = 68$.

It is known that caps of size 15 or 16 are embedded in the elliptic quadric. It follows that such caps cannot be quantum (see Theorem 4). Because of Proposition 1 we are reduced to cardinalities between 7 and 14.

A standard counting method is **secundum counting:** in the case of $PG(3,4)$ a secundum is a line. We fix a secant line and study the distribution of points on the 5 planes through the secant. In the case of cardinality 13 this shows, because of the quantum condition (see Definition 4), that each secant is contained in precisely 3 planes meeting the cap in 5 points. The number of such planes is therefore $\binom{13}{2} \times 3/10$, contradiction. Cardinality 9 is excluded by the same argument. For cardinality 7 this argument shows that any 4 points are in general position. This defines a $[7,4]_4$-code whose dual has parameters $[7,3,5]_4$ contradicting the Griesmer bound. For cardinality 11, let $e_i, i = 1,3,5$ be the number of planes meeting K in i points. By secundum counting we obtain $e_5 = 11, e_3 = 55$. This implies $e_1 = 19$. On the other hand, let $P \in K$. Consider the pairs (g,E) where g is a secant, $P \in g, g \subset E$ and E a 5-plane. There are 10×2 such pairs. This shows that P is contained in five 5-planes. An analogous count shows that P is in fifteen 3-planes. This shows that P must be on one 1-plane which yields the contradiction $e_1 = 11 \neq 19$. On the non-existence side it remains to exclude cardinality 10.

Lemma 2. *There is no quantum* 10*-cap in* $PG(3,4)$.

Proof. Let K be such a quantum 10-cap. Observe that planes intersect K in $0, 2$ or 4 points. In fact, a hyperoval as intersection is excluded as otherwise the complement of the hyperoval in K would be a quantum 4-cap in $PG(3,4)$ or in $PG(2,4)$, which is not possible. The standard counting argument based on secant lines shows that each secant is in precisely four 4-planes. There are 30 such planes and they define a Steiner system $S(3,4,10)$. A generator matrix can be given the form

$$\left(\begin{array}{cccc|cccc|cc} 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & & & & \\ 0 & 0 & 1 & 0 & 1 & & 0 & & & \\ 0 & 0 & 0 & 1 & 1 & & & 0 & & \end{array}\right)$$

where the missing entries are nonzero. Let $c_i, i = 1, \ldots, 10$ be the columns of this matrix and $P_i \in PG(3,4)$ the corresponding points. Comparison

with the first row shows that in each of the remaining rows the four entries to be determined must be such that each entry occurs twice or not at all. Consider rows z_i, z_j where $i, j \geq 2$. Then $z_i + z_j$ shows that the triples of nonzero entries in cordinates $k \geq 6$ where both z_i and z_j have nonzero entries agree in precisely one coordinate. Further $z_i + \lambda z_j$ for $\lambda \neq 0, 1$ show that those triples satisfy the proportionality condition: if the triples are abc and ade, respectively, then $d/b = e/c$. As an example, let $z_2 = 010010uabc$, $z_3 = 00101v0ade$. Then $z_2 + z_3 = (01100vu0, b + d, c + e)$ and $z_2 + \omega z_3, z_2 + \overline{\omega} z_3$ yield the proportionality condition.

No two of the $c_i, i \geq 5$ can agree in more than 2 coordinates as otherwise those two points would be collinear with a $P_i, i \leq 4$.

Clearly we can choose the basis such that $z_1 + z_2$ has weight 6. This means that two of the remaining entries in z_2 are 1. By applying a field automorphism the two last entries can be chosen as ω. There are three non-equivalent possibilities how the entries 1 can be distributed. Assume at first

$$\left(\begin{array}{cccc|cccc|cc} 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & \omega & \omega \\ 0 & 0 & 1 & 0 & 1 & a & 0 & b & c & d \\ 0 & 0 & 0 & 1 & 1 & & & 0 & & \end{array}\right)$$

Then $c \neq d$. Case $b = 1$ is impossible as the proportionality condition is not satisfied. We can choose $c = \omega$. It follows $(a, b, c, d) = (\overline{\omega}, \omega, \omega, \overline{\omega})$. The entries in the last row are $efef$ and cannot be completed.

Next consider

$$\left(\begin{array}{cccc|cccc|cc} 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & \omega & \omega & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & a & 0 & b & c & d \\ 0 & 0 & 0 & 1 & 1 & & & 0 & & \end{array}\right)$$

Clearly $b = \omega$ and $a = 1$ are impossible. We have $b = 1$. By proportionality $a = \overline{\omega}$ and we have

$$\left(\begin{array}{cccc|cccc|cc} 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & \omega & \omega & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & \overline{\omega} & 0 & 1 & \overline{\omega} & 1 \\ 0 & 0 & 0 & 1 & 1 & & & 0 & & \end{array}\right)$$

and this cannot be completed. Finally consider the case

$$\left(\begin{array}{cccc|cccc|cc} 1&0&0&0&0&1&1&1&1&1\\ 0&1&0&0&1&0&1&\omega&1&\omega\\ 0&0&1&0&1&a&0&b&c&d\\ 0&0&0&1&1&&&0&& \end{array}\right)$$

$c = 1$ is impossible as then $b = d$. If $d = \omega$, then $c = b\overline{\omega}$. It follows $b = \overline{\omega}$ and this cannot be completed. This shows $b = \omega$ and $c = d\overline{\omega}$. It follows

$$\left(\begin{array}{cccc|cccc|cc} 1&0&0&0&0&1&1&1&1&1\\ 0&1&0&0&1&0&1&\omega&1&\omega\\ 0&0&1&0&1&\overline{\omega}&0&\omega&\omega&\overline{\omega}\\ 0&0&0&1&1&e&x&0&y&f \end{array}\right)$$

The assumption $x = e, y = f$ leads to a contradiction. We have $x = f, y = e$. The proportionality condition yields $e = \overline{\omega}, f = 1$. The matrix is

$$\left(\begin{array}{cccc|cccc|cc} 1&0&0&0&0&1&1&1&1&1\\ 0&1&0&0&1&0&1&\omega&1&\omega\\ 0&0&1&0&1&\overline{\omega}&0&\omega&\omega&\overline{\omega}\\ 0&0&0&1&1&\overline{\omega}&1&0&\overline{\omega}&1 \end{array}\right)$$

Here the first and the two last points are collinear, contradiction. □

The quantum 8-cap $\mathcal{K}(3, 8)$.

Clearly a quantum 8-cap K cannot contain a hyperoval. It follows that each secant is on 3 planes meeting K in cardinality 4. There are therefore 14 such planes and they define a Steiner system $S(3, 4, 8)$. Write a generator matrix in the form $(I|P)$. Then P has one entry zero in each column, and these occur in different rows. We have the form $\left(\begin{array}{cccc|cccc} 1&0&0&0&0&1&1&1\\ 0&1&0&0&1&0&a&b\\ 0&0&1&0&1&c&0&d\\ 0&0&0&1&1&e&f&0 \end{array}\right)$ (without restriction). Comparison of the first row with the others shows $a = b, c = d, e = f$. Comparison of the later rows shows $a = \cdots = f(\neq 0)$. A final obvious manipulation produces the standard generator matrix $(I|I + J)$ of the extended Hamming code. We see that K is uniquely determined as constructed in Section 2. We define $K = \mathcal{K}_8$ to consist of the vectors of odd weight in $\mathbb{F}_2^4$ when interpreted as points in $PG(3, 4)$. The automorphism

group G_8 has then the form $G_8 = E_8GL(3,2) \times Z_2$ of order $g_8 = 16 \times 168$, the direct product of its center (generated by the Frobenius automorphism) and the stabilizer of a plane (the plane $x_1 + x_2 + x_3 + x_4 = 0$) in $GL(4,2)$. In particular there are precisely $g/g_8 = 64 \times 27 \times 25 \times 17$ copies of $\mathcal{K}_8$ in $PG(3,4)$. The group G_8 is 3-transitive on the points of the cap.

Here is a different description of $\mathcal{K}_8$: choose hyperovals $\mathcal{O}_1, \mathcal{O}_2$ on two planes which share a common secant. The symmetric sum $\mathcal{O}_1 + \mathcal{O}_2$ is then a quantum cap. This is a special case of Theorem 5. It follows that we have a copy of $\mathcal{K}(3,8)$. Clearly $a_4 = 14, a_2 = 56, a_0 = 15$. Recall also Section 2 where $\mathcal{K}(3,8)$ was constructed as an application of Theorem 1. For future reference we think of $\mathcal{K}(3,8)$ as the set of points in $PG(3,4)$ represented by the vectors of weights 1 or 3 with entries in $\mathbb{F}_2$.

The quantum 14-cap $\mathcal{K}(3,14)$

A 14-cap contained in the elliptic quadric cannot be quantum as otherwise the complementary set of 3 points would have to be pre-quantum (see Theorem 4). It is known that there is only one 14-cap which is not embedded. This is the complete 14-cap and it is quantum. The complete 14-cap and its automorphism group were described in [7]. Here we want to describe it from scratch.

Proposition 2. *The complete* 14*-cap in* $PG(3,4)$ *is the disjoint union of* $\mathcal{K}(3,8)$ *and a hyperoval in a plane.*

Proof. Secundum counting shows that each secant of K must be contained in a plane which meets K in a hyperoval. In particular K contains hyperovals. It follows from Theorem 4 that its complement in K must be a quantum 8-cap and therefore a copy of $\mathcal{K}(3,8)$. □

Let X be the set of points in $PG(3,4)$ extending $\mathcal{K}(3,8)$ to a 9-cap. A moment's thought shows that X consists of the points generated by the vectors of weight 3 whose nonzero entries are pairwise different and by the weight 4 vectors whose entries sum to 0. It follows $|X| = 8 + 6 = 14$ and X is contained in the plane $H : x_1 + x_2 + x_3 + x_4 = 0$. In fact X consists of the points of H which are not in the Fano subplane of H consisting of its points with coordinates in $\mathbb{F}_2$. This shows the following:

Proposition 3. *Let* H *be the plane* $x_1 + x_2 + x_3 + x_4 = 0$ *and* E *its Fano subplane consisting of points with coordinates in* $\mathbb{F}_2$. *Then* $\mathcal{K}(3,8) \cup Y$ *is a cap*

in $PG(3,4)$ if and only if $Y \subset H, Y \cap E = \emptyset$ and Y is a cap, and $\mathcal{K}(3,8) \cup Y$ is a quantum cap if and only if moreover Y is a hyperoval.

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 [12]. There are 360 Fano planes and 168 hyperovals in $PG(2,4)$.

Proposition 4. *Each Fano plane $E \subset PG(2,4)$ is disjoint from 7 hyperovals. Here each point $P \in E$ determines a hyperoval disjoint from E which consists of the points off E in the union of the bundle of lines of E that concur in P.*

Proof. Each of the 7 lines of E contains two points $\notin E$. A hyperoval disjoint from E must be the union of three such pairs of points from three lines of E. The fact that E is a blocking set in $PG(2,4)$ shows that a hyperoval is obtained if and only if those three lines are concurrent. □

Theorem 9. *Each $\mathcal{K}(3,8)$ is contained in precisely seven $\mathcal{K}(3,14)$. Each $\mathcal{K}(3,14)$ contains precisely seven copies of $\mathcal{K}(3,8)$ and seven hyperovals. We have $g_{14} = g_8 = 2^7 \times 3 \times 7$. Each pair of hyperovals intersects in a secant, and this secant is in precisely three hyperovals.*

Proof. Propositions 3 and 4 show that $\mathcal{K}(3,8)$ is in precisely 7 copies of $\mathcal{K}(3,14)$. Fix $K = \mathcal{K}(3,14)$. Let a_j be the number of planes meeting K in cardinality j (the j-planes), where $j \in \{0,2,4,6\}$. Let l be a secant of K. If l is in j of the 6-planes, then it is in $6-2j$ of the 4-planes and in $j-1$ of the 2-planes. It follows $j \in \{1,2,3\}$. Let l_j be the corresponding number of secants. Then $l_1 + l_2 + l_3 = \binom{14}{2} = 91$ and the obvious equations expressing a_2, a_4, a_6 in terms of the l_i have a unique solution:

$$a_6 = 7, a_4 = 56, a_2 = 14, a_0 = 8.$$

Each pair of hyperovals contained in K must intersect in a secant. The symmetric sum of those two hyperoval is a copy of $\mathcal{K}(3,8)$. It follows that the secant is on a third hyperoval. In terms of the system of equations this implies $l_3 = 7, l_2 = 0, l_1 = 84$. □

This indicates also how to construct $\mathcal{K}(3,14)$ in terms of hyperovals: there is a configuration in $PG(3,4)$ consisting of three collinear planes and a hyperoval in each plane, where all hyperovals share the same two points on the line of intersection. The symmetric sum of two hyperovals is then $\mathcal{K}(3,8)$ and the union of all three hyperovals is $\mathcal{K}(3,14)$.

The quantum 12-cap $\mathcal{K}(3,12)$

Assume K does not contain a hyperoval. Then K intersects each plane in at most 4 points. This yields a $[12,4,8]_4$-code. Concatenation with a $[4,2,3]_2$-code yields a $[48,8,24]_2$-code. This contradicts the Griesmer bound. It follows that K contains a hyperoval $\mathcal{O}$. Proposition 1 shows that $K \setminus \mathcal{O}$ is a hyperoval as well, so K is the disjoint union of two hyperovals. Each hyperoval is in a plane and those planes intersect in a line avoiding K, see the construction in the previous section. It is easy to see that K is uniquely determined. The fact that each $PG(2,4)$ contains precisely 168 hyperovals and that each line in $PG(2,4)$ is disjoint from 48 hyperovals shows that the total number of $\mathcal{K}(3,12)$ in $PG(3,4)$ is $85 \times 168 \times 6 \times 4 \times 48/2 = g/240$. This shows $g_{12} = 240$. Obvious counting arguments show

$$a_6 = 2, a_4 = 45, a_2 = 30, a_0 = 8.$$

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

Let $\mathbb{F}_4 = \{0, 1, \omega, \overline{\omega}\}$. In this section we will write for brevity $2 = \omega, 3 = \overline{\omega}$. Let $G = P\Gamma L(5,4)$ of order $g = 2^{21} \times 3^5 \times 5^2 \times 7 \times 11 \times 17 \times 31$.

Theorem 10. *Quantum n-caps in $PG(4,4)$ exist precisely for $10 \leq n \leq 41$ such that $n \notin \{11, 37, 39\}$.*

The fact that $n \geq 10$ follows from the self-orthogonality of the corresponding code, see Definition 1. As an application of Theorem 7, choose two planes Π_1, Π_2 in $PG(4,4)$ which meet in a point X. Let $K_i \cup \{X\}$ be a hyperoval in Π_i, for $i = 1, 2$. Then the symmetric sum $K_1 \cup K_2$ is a quantum 10-cap in $PG(4,4)$. 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]). In particular the sizes of quantum caps in $PG(4,4)$ are in the interval $10 \leq n \leq 41$. Tonchev [15] starts from the quantum 41-cap and determines its quantum subcaps, using Theorem 7 of [6]. This leads to quantum caps of sizes $n \in \{10, 12, 14 - 27, 29, 31, 33, 35\}$ in $PG(4,4)$. This method has its limitations. In fact, it follows from Theorem 4 and the fact that the smallest pre-quantum cap has size 6 that this construction cannot yield caps of sizes between 36 and 40. Theorem 2 can be applied to the non-quantum 41-cap in $PG(4,4)$

as well. As the dual of its norm code has a word of weight 36, this yields a quantum 36-cap in $PG(4,4)$.

Our proof that cardinalities $11, 37, 39$ are excluded consists in an exhaustive computer searches.

We are however more interested in conceptual geometric constructions. In the present section we want to show that the theorems from Section 6 yield transparent constructions for many quantum caps in $PG(4,4)$. At first apply Theorem 5. If one of the ingredients is the elliptic quadric, we must choose an elliptic quadric on the second hyperplane as well. This leads to quantum 24- and 32-caps. Apply Theorem 5 to the remaining ingredients. They all possess planes with 0 or 2 or 4 intersection points and all but $\mathcal{K}(3,8)$ also contain a hyperoval. This leads to quantum caps of all even sizes between 12 and 28. Theorem 6 can be applied when $K_1 \subset \Pi_1$ is the elliptic quadric such that $E = \Pi_1 \cap \Pi_2$ is a tangent plane of K_1, $K_1 \cap E = \{P\}$ and $K_2 \subset \Pi_2 \setminus S$ a quantum cap in $AG(3,4)$ such that $K_2 \cup \{P\}$ is a cap. As $\mathcal{K}(2,6)$ and $\mathcal{K}(3,8)$ are affine (in $AG(3,4)$) and can be extended by a point of the plane at infinity, they may be used in the role of K_2. This yields quantum caps of sizes $17+6=23$ and $17+8=25$.

Description and classification

At the extremes of the interval the quantum caps tend to be almost uniquely determined. We start with some results concerning quantum caps of size ≤ 12.

Theorem 11. *There exist precisely two quantum* 10*-caps in* $PG(4,4)$.

Theorem 11 has been proved by an exhaustive search. We denote those two caps by $\mathcal{K}(4,10,1)$ and $\mathcal{K}(4,10,2)$, where $\mathcal{K}(4,10,1)$ is the cap derived from Theorem 7. Using the facts that $PG(4,4)$ has $341 = 11 \times 31$ points, that $PG(3,4)$ has $357 = 3 \times 7 \times 17$ lines and $2^7 \times 3 \times 7 \times 17$ pairs of skew lines and that each point of $PG(2,4)$ is in 48 hyperovals, we see that the orbit of $\mathcal{K}(4,10,1)$ has length $341 \times (2^7 \times 3 \times 7 \times 17) \times 48^2 = 2^{15} \times 3^3 \times 7 \times 11 \times 17 \times 31$. This shows that the automorphism group of $\mathcal{K}(4,10,1)$ has order $g_{4,10,1} = 2^6 \times 3^2 \times 5^2$. We can give a characterization of the second quantum 10-cap:

Theorem 12. *There is precisely one quantum* 10*-cap* $\mathcal{K}(4,10,2)$ *in* $PG(4,4)$ *which contains a basis such that each set of* 6 *cap points containing the basis is a frame. Its automorphism group is an extension of an elementary-abelian group of order* 32 *by the symmetric group* S_5.

$\mathcal{K}(4,10,2)$	
10000	11111
01000	13222
00100	12322
00010	12232
00001	12223

Proof. Let $\overline{x}$ denote the conjugate of $x \in \mathbb{F}_4$. A generator matrix has the form (I, P) where all entries of P are nonzero. Obviously the top row of P can be chosen with all entries $= 1$. The quantum condition shows that all other rows have one entry with frequency three, the remaining two nonzero symbols precisely once. We can choose notation such that the entry with frequency three is $= 1$. This yields without restriction $\begin{pmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 2 & 3 \end{pmatrix}$ as first rows. The rows r_i of P satisfy $\overline{r}_i \cdot r_j = \delta_{ij}$. The cap code is self-dual with respect to the Hermitian form. It follows that $(\overline{P}^t, I)$ also is a generator matrix. In particular the columns s_i of P satisfy $\overline{s}_i \cdot s_j = \delta_{ij}$ as well, and P is invertible.

Assume there is a row with the same location for the repeated letter: $\begin{pmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 2 & 3 \\ 1 & 1 & 1 & 3 & 2 \end{pmatrix}$.

We can arrange the first column to be constant 1. This forces the remaining entries in s_2, s_3 to be $2, 3$: $\begin{pmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 2 & 3 \\ 1 & 1 & 1 & 3 & 2 \\ 1 & 2 & 3 & c & c \\ 1 & 3 & 2 & c & c \end{pmatrix}$. Rows $3, 4$ yield a contradiction. Assume there are two rows such that the locations of the ones intersect in precisely one coordinate. Then the orthogonality condition cannot be satisfied. It follows that the locations of the triply repeated letter in two of the rows from r_2 to r_4 intersect in two coordinates. In particular the first three rows can be chosen as $\begin{pmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 2 & 3 \\ 2 & 1 & 1 & 1 & 3 \end{pmatrix}$.

It is impossible that the location of the repeated entry in row 4 contains the intersection of the locations from rows two and three as the orthogonality

condition is violated. The completion is now uniquely determined:

$$P = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 2 & 3 \\ 2 & 1 & 1 & 1 & 3 \\ 1 & 1 & 2 & 1 & 3 \\ 1 & 2 & 1 & 1 & 3 \end{pmatrix}.$$

It is easy to obtain the generator matrix in standard form given above. Consider the automorphism group. Let the points in $PG(4,4)$ defined by the columns of the generator matrix be $P_1, \ldots, P_5$ (of weight 1) and $Q_1, \ldots, Q_5$. Then $f = \begin{pmatrix} 0 & 0 & 0 & 0 & 1 \\ 3 & 0 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 & 0 \\ 0 & 0 & 2 & 0 & 0 \\ 0 & 0 & 0 & 2 & 0 \end{pmatrix}$ (in its action on columns from the left) maps $(P_1, P_2, P_3, P_4, P_5)(Q_1, Q_2, Q_3, Q_4, Q_5)$ and

$$v = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \end{pmatrix} \text{ maps } (P_2, P_3, P_4, P_5)(Q_2, Q_3, Q_4, Q_5).$$

There are 10 quadruples of points which are dependent and therefore in a plane. They are P_i, P_j, Q_i, Q_j where $1 \leq i < j \leq 5$. It follows that the columns come in pairs $\{P_i, Q_i\}$. The unions of two pairs are the dependent quadruples, the unions of three pairs generate the 10 hyperplanes with 6 points each. This defines sets of 10 special planes and of 10 special solids, where each special plane is on three special solids and also the other way around. The bases satisfying the conditions of our theorem are those 32 bases that contain no pair. Because of uniqueness, the automorphism group is transitive on those 32 bases. The kernel in the action on the five blocks is an elementary-abelian group V of order 32 and $G_{4,10,2}/V \cong S_5$. It is obvious that we really have a cap. □

Next we turn to quantum 12-caps. An exhaustive computer search showed that there are precisely 5 non-equivalent quantum 12-caps in $PG(4,4)$. We denote them by $\mathcal{K}(4,12,1), \ldots \mathcal{K}(4,12,5)$ and give synthetic descriptions. Here $\mathcal{K}(4,12,1) = \mathcal{O}_1 \cup \mathcal{O}_2$ where $\mathcal{O}_i$ is a hyperoval on plane E_i and $E_1 \cap E_2$ is a point not belonging to $\mathcal{O}_1$ or $\mathcal{O}_2$. Clearly there is only one such orbit.

A trivial counting argument shows that the total number of those caps in $PG(4,4)$ is $(11 \times 17 \times 31) \times 168 \times 15 \times 256 \times 120/2$. It follows that the order of the automorphism group is $g_{4,12,1} = 2^8 \times 9 = 2,304$.

The description of $\mathcal{K}(3,8) \subset PG(3,4)$ shows that each secant l to it is on precisely two planes meeting $\mathcal{K}(3,8)$ only in the points of l. It is therefore possible to choose two hyperplanes H_1, H_2 in $PG(4,4)$, two points A, B on the plane $E = H_1 \cap H_2$ and copies $K_i \subset H_1$ of $\mathcal{K}(3,8)$ such that $K_i \cap E = \{A, B\}$. The symmetric sum $K_1 + K_2$ is then a quantum 12-cap in $PG(4,4)$. This leads to the quantum caps $\mathcal{K}(4,12,2), \mathcal{K}(4,12,3), \mathcal{K}(4,12,4)$. The orders of their automorphism groups are $g_{4,12,2} = 12, g_{4,12,3} = 128, g_{4,12,4} = 768$.

In order to describe $\mathcal{K}(4,12,5)$ start from two planes $E_1, E_2 \subset PG(4,4)$ meeting in a point P. Let l_i be a line on E_i through P and $P_i \in l_i, P_i \neq P$. Let E_3 be the plane generated by l_1 and l_2. Let $\mathcal{O}_i$ be a hyperoval on E_i through P, P_i and $\mathcal{O}$ a hyperoval on $\mathcal{O}$ through P, P_1, P_2. Then $\mathcal{O}_1 + \mathcal{O}_2 + \mathcal{O}$ is a quantum set and a moment's thought shows that it is a cap. This describes $\mathcal{K}(4,12,5)$. The length of the orbit is $(11 \times 17 \times 31) \times 21 \times 256 \times 20 \times 20 \times 3 \times 12 \times 12/2$. The order of the automorphism group is therefore $g_{4,12,5} = 2^6 \times 3 = 192$.

Consider now large quantum caps in $PG(4,4)$. We saw in the proof of Theorem 10 that there is precisely one quantum 41-cap $\mathcal{K}(4,41)$. This cap had first been constructed by Tallini [14]. Its automorphism group is solvable of order 240 (see also [4]). There is precisely one complete 40-cap in $PG(4,4)$. It is affine, the unique largest cap in $AG(4,4)$ [8] and it is the unique quantum 40-cap $\mathcal{K}(4,40)$ in $PG(4,4)$. The automorphism group of $\mathcal{K}(4,40)$ is a semidirect product of the elementary-abelian group E_{16} and A_5. An exhaustive computer search showed that there is precisely one quantum 38-cap $\mathcal{K}(4,38)$. It is in the union of four hyperplanes $H_1, \ldots, H_4$ through a common plane E and it is defined as the union $A_1 \cup \cdots \cup A_4$ where $A_i \subset H_i$ is a copy of $\mathcal{K}(3,14)$ and such that all A_i meet E in the same hyperoval. This cap was constructed in [1]. In fact it can also be found inside the Glynn 126-cap in $PG(5,4)$ (see [9]. The $[126,6,88]_4$code generated by the Glynn cap has weight distribution $A_0 = 1, A_{88} = 945, A_{96} = 3087, A_{120} = 63$. Each of the 315 hyperplanes defined by codewords of minimum weight 88 intersects the Glynn cap in a cap with $126 - 88 = 38$ points. These are copies of $\mathcal{K}(4,38)$. The automorphism group of the Glynn cap has order $120,960$ and contains $PGL(3,4)$ as a subgroup of index 2. The automorphism group of $\mathcal{K}(4,38)$ has order $120,960/315 = 384 = 2^7 \times 3$ and therefore agrees with the stabilizer of $\mathcal{K}(4,38)$ in the automorphism group of the Glynn cap.

An exhaustive search showed that there are precisely two quantum 36-caps in $PG(4,4)$. Here $\mathcal{K}(4,38,1)$ is contained in a bundle of three hyperplanes H_1, H_2, H_3 which meet in a common plane E. Let $K_1 \subset H_1, K_2 \subset H_2$ be elliptic quadrics such that K_1 and K_2 meet E in the same set $\mathcal{O} = V \cup \{N\}$ of 5 points. Let K_3 be a copy of $\mathcal{K}(3,12)$ in H_3 such that $K_3 \cap E = V$. We have then $\mathcal{K}(4,38,1) = K_1 \cup K_2 \cup K_3 \setminus \{N\}$.

We do not have complete characterizations for the quantum caps of any size between 13 and 35. It seems that those of odd size are harder to construct. Theorems 5,6 need the elliptic quadric in a hyperplane as one of the two ingredients. We therefore searched for quantum caps in $PG(4,4)$ intersecting a hyperplane in an elliptic quadric. The cardinalities of the resulting quantum caps are the odd numbers between 23 and 35. There is precisely one quantum cap of $23 = 17+6$ points containing the elliptic quadric (union of the elliptic quadric and the hyperoval). This is an incomplete 23-cap. There is precisely one quantum cap of $27 = 17+10$ points containing the elliptic quadric. It is incomplete and uses the 10-cap $\mathcal{K}(4,10,2)$. There are precisely two quantum caps of $29 = 17+12$ points, one complete and one incomplete. Both use $\mathcal{K}(4,12,2)$ in the role of the affine 12-cap. There is precisely one quantum 35-cap containing an elliptic quadric in a hyperplane.

9 Quantum caps in higher-dimensional spaces

Obviously a lower bound on the size of a quantum cap in $PG(m,4)$ is $2(m+1)$ (corresponding to linear $[[2(m+1),0,4]]$ quantum codes). The quantum caps $\mathcal{K}(2,6)$ and $\mathcal{K}(4,10,2)$ belong to an infinite family which shows that quantum $2(m+1)$-caps exist in $PG(m,4)$ when m is odd.

Theorem 13. *$PG(m,4)$ for even m contains a quantum $2(m+1)$-cap possessing $m+1$ points in general position such that each additional point completes it to a frame.*

In fact, choose a generator matrix $(I|P)$ where $P = \begin{pmatrix} 1111\ldots \\ 1322\ldots \\ 1232\ldots \\ 1223\ldots \\ \ldots \end{pmatrix}$.

Then it is easy to see that this generates a cap and that any two rows are Hermitian orthogonal to one another.

Theorem 14. *$PG(m,4)$ for odd $m \geq 3$ contains a quantum $2(m+1)$-cap.*

In fact, use $(I|I+J)$ as generator matrix. The smallest member of the family is $\mathcal{K}(3,8)$ in $PG(3,4)$.

The largest known quantum caps in $PG(5,4), PG(7,4), PG(9,4)$ are also the largest known caps in those spaces. These are the Glynn 126-cap in $PG(5,4)$, a 756-cap in $PG(7,4)$ and a 5040-cap in $PG(9,4)$ (see [4]).

References

[1] D. Bartoli, J. Bierbrauer, S. Marcugini, F. Pambianco: *Geometric constructions of quantum codes, Error-Correcting Codes, Finite Geometries and Cryptography,* Contemporary Mathematics, vol 523, Amer. Math. Soc, Providence, RI, 2010, pp. 149-154.

[2] J. Bierbrauer: *Introduction to Coding Theory,* Chapman and Hall/ CRC Press 2004.

[3] J. Bierbrauer and Y. Edel: *Quantum twisted codes, Journal of Combinatorial Designs* **8** (2000), 174-188.

[4] J. Bierbrauer and Y. Edel: *Large caps in projective Galois spaces,* in: **Current research topics in Galois geometry,** J. de Beule and L. Storme (eds), Nova Science Publishers 2010, pp. 81-94.

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

[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] D.G. Glynn: *A 126-cap in $PG(5,4)$ and its corresponding $[126,6,88]$-code, Util. Math.* **55** (1999), 201-210.

[10] D.G. Glynn, T.A. Gulliver, J.G. Maks, M.K. Gupta: *The geometry of additive quantum codes,* manuscript, 2006.

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

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

[13] J. W. P. Hirschfeld: *Finite projective spaces in three dimensions,* Clarendon Press, Oxford 1985.

[14] G. Tallini: *Calotte complete di $S_{4,q}$ contenenti due quadriche ellittiche quali sezioni iperpiane, Rend. Mat. e Appl.* **23** (1964), 108-123.

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

[16] S. Yu, J. Bierbrauer, Y. Dong, Q. Chen, C.H. Oh: *All the stabilizer codes of distance* 3, *IEEE Transactions on Information Theory,* to appear.