Innovations in Incidence Geometry
Volume 6 (2007), Pages 289–307
ISSN 1781-6475

The geometry of quantum codes

Jürgen Bierbrauer Giorgio Faina Massimo Giulietti
Stefano Marcugini Fernanda Pambianco

Abstract

We give a geometric interpretation of additive quantum stabilizer codes in terms of sets of lines in binary symplectic space. It is used to obtain synthetic geometric constructions and non-existence results. In particular several open problems are removed from Grassl's database [13].

Keywords: quantum codes, symplectic geometry, Hermitian form, additive codes, Blokhuis-Brouwer construction, APN function, spread, quantum cap
MSC 2000: missing

1 Introduction

The most popular construction of quantum error-correcting codes was developed in [6]. It uses a special class of additive quaternary codes. Those codes are known as *quantum stabilizer codes*. We start in Section 2 by recalling basic facts concerning quaternary additive codes and their geometric representation as developed in [5, 3, 4]. Quantum stabilizer codes live in symplectic geometry. Starting point for our investigation is a geometric interpretation of quantum stabilizer codes in terms of systems of lines in symplectic geometry. It is one of the aims to obtain more transparent constructions and bounds using geometric terminology. The paper is mostly concerned with codes of distance $d \leq 4$. Our simplified approach allows us to derive more general constructions. In particular we resolve a number of existence questions (see Grassl's database [13]). Among the results are constructions of new pure codes

$$[[36, 29, 3]], [[37, 30, 3]], [[38, 31, 3]], [[81, 73, 3]], [[756, 740, 4]], [[5040, 5020, 4]]$$

and proofs of nonexistence for parameters $[[39, 32, 3]], [[82, 74, 3]], [[83, 75, 3]]$. For the geometric approach to linear codes see [1]. The general geometric description of quantum stabilizer codes is given in Section 2. Section 3 discusses

impure codes in the case of small distance. A construction in case $d = 3$ based on secunda is described in Section 4. This leads to a pure $[[37, 30, 3]]$-code. Section 5 contains a detailed study of the geometry of pure codes when $d = 3$. We construct a $[[81, 73, 3]]$-code and derive non-existence results. A link to almost perfectly nonlinear codes is described in Section 6. Most of our new pure $d = 3$ codes are constructed in Section 7. The final Section 8 is dedicated to case $d = 4$ and quantum caps. We wish to thank Gohar M. Kyureghyan for helpful discussions which led to Section 6.

2 Geometric description of quantum stabilizer codes

We use the notion of an *additive* code as the relaxation of the notion of a linear code, where the alphabet is not considered as a finite field but only as a vector space over some ground field. Here we consider only the quaternary case, where the ground field is $\mathbb{F}_2$.

Definition 2.1. Let k be such that $2k$ is a positive integer. An additive quaternary $[n, k]_4$-code $\mathcal{C}$ (length n, dimension k) is a $2k$-dimensional subspace of $\mathbb{F}_2^{2n}$, where the coordinates come in pairs of two. We view the codewords as n-tuples where the coordinate entries are elements of $\mathbb{F}_2^2$.

A *generator matrix* of $\mathcal{C}$ is a binary $(2k, 2n)$-matrix whose rows form a basis of the binary vector space $\mathcal{C}$.

In the case of quantum stabilizer codes we view the ambient space $\mathbb{F}_2^{2n}$ as a binary symplectic space, where each of the n parameter sections corresponds to a hyperbolic plane, equivalently a 2-dimensional symplectic space. Each codeword is therefore a vector in the $2n$-dimensional symplectic geometry over $\mathbb{F}_2$.

Definition 2.2. 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.

Describe C by a generator matrix M. Each of the n coordinate sections contains 2 columns which we view as points in binary projective space. The geometric description of the quantum code is in terms of the system of n lines (the codelines) generated by those n pairs of points. This terminology is not always fully justified. It is possible that 0-columns occur and that the two points in a coordinate section are identical. These degenerate cases are best described by the strength:

Definition 2.3. Let C be a quaternary additive code of length n, with generator matrix M. The *strength* of C is the largest number t such that any t codelines are in general position.

For example $t \geq 1$ means that each coordinate section does indeed generate a codeline, and $t \geq 2$ means that those n codelines are pairwise skew. The general definition of the parameters of a quantum stabilizer code is as follows.

Definition 2.4. An $[[n, m, d]]$-code C where $m > 0$ is a quaternary quantum stabilizer code of binary dimension $n-m$ satisfying the following: any codeword of $C^\perp$ having weight at most $d-1$ is in C.

The code is *pure* if $C^\perp$ does not contain codewords of weight $\leq d-1$, equivalently if C has strength $t \geq d-1$.

An $[[n, 0, d]]$-code C is a self-dual quaternary quantum stabilizer code of strength $t = d-1$.

In particular, whenever some $\leq d-1$ codelines are not in general position there is a hyperplane containing all the other codelines. We prefer working with pure quantum codes. The reason why in Definition 2.4 we did not distinguish between codelines and codepoints is that codepoints are easily disposed of.

Lemma 2.5. *Assume there is an $[[n, m, d]]$-code, $d \geq 2$, one of whose codeobjects is not a line but a point (equivalently, the code does not have strength ≥ 1). Then the remaining objects define an $[[n-1, m, d]]$-code. Conversely, if an $[[n-1, m, d]]$-code exists, then there is an $[[n, m, d]]$-code one of whose codeobjects is a point.*

Proof. Let a point $P = L_n$ be a codeobject of an $[[n, m, d]]$-code C. By the definition of the symplectic product there is a nonzero codeword in $C^\perp$ with entries 00 in all but the last coordinate section. By Definition 2.4 this codeword is in C. Write it as last row of a generator matrix. Consider the matrix obtained by removing the last row and $L_n = P$. This is again a self-dual code and it generates an $[[n-1, m, d]]$-quantum code.

If a generator matrix of an $[[n-1, m, d]]$-code is given we can add an extra coordinate consisting of a 0-column and a 1-column, and an extra row with all entries 00 except for the additional column. This defines an $[[n, m, d]]$-code whose n-th codeobject is a point. □

As $[[n-1, m, d]]$-code implies an $[[n, m, d]]$-code we can think of the basic problem as minimizing n when m, d are given. Lemma 2.5 shows that we can assume all codeobjects to be lines. The role of codepoints is restricted to the construction of an $[[n, m, d]]$-code from an $[[n-1, m, d]]$-code.

Consider a pure $[[n, m, d]]$-code. In our quaternary notation it is the dual of an additive $[n, (n+m)/2, d]_4$-code. Most important is the self-orthogonality condition. Imagine a generator matrix of C. The codewords are linear combinations of rows. Those factors describe a hyperplane in $\mathsf{PG}(n-m-1, 2)$. Consider two codewords of C and the hyperplanes H_1 and H_2 corresponding

to them. Consider the secundum $S = H_1 \cap H_2$. In the symplectic product of the codewords the codelines L that intersect S nontrivially give no contribution, the others do. It follows that the self-orthogonality condition is: the number of codelines skew to S must be even. In this perspective it is most natural to work with the redundancy $r = n - m$. This leads to the following description.

Theorem 2.6. *The following are equivalent:*

- *a pure* $[[n, n-r, t+1]]$ *quantum stabilizer code;*
- *a set of* n *lines, the* codelines*, in* $\mathsf{PG}(r-1,2)$ *any* t *of which are in general position and such that for every secundum* S *the number of codelines skew to* S *is even.*

Theorem 2.6 is the geometric description of pure quantum stabilizer codes. The secundum condition says that for any two codewords u, v we have that $wt(u+v)$ and $wt(u) + wt(v)$ have the same parity. This implies that the pure quantum codes come in two varieties: either all weights are even or the words of even weight form a subcode of codimension 1.

Consider the easiest case $t = 1$. Use all lines of $\mathsf{PG}(r-1,2)$. The number of lines is $n = g_r = (2^r - 1)(2^{r-1} - 1)/3$. Let S be a secundum. It contains g_{r-2} lines. There are $t_r = ((2^{r-2}-1)(2^r - 2^{r-2})/2 = 3 \times 2^{r-3}(2^{r-2}-1)$ lines meeting S in one point. The number of lines skew to S is therefore $g_r - g_{r-2} - t_r = 2^{2r-4}$, which is even for $r > 2$. It follows that, for $r > 2$, the family of all lines in $\mathsf{PG}(r-1,2)$ defines a quantum code

$$[[g_r, g_r - r, 2]]_4 = [[(2^r - 1)(2^{r-1} - 1)/3, (2^r - 1)(2^{r-1} - 1)/3 - r, 2]]_4 .$$

This solves the existence problem of *projective* distance 2 pure quaternary quantum codes. However, there is no need to limit ourselves to projective codes. In case $r = 2$, use the ambient space, itself a line, n times. When n is even this is an $[[n, n-2, 2]]$-code. For odd n we have to use $r = 3$ and construct $[[n, n-3, 2]]$-codes.

Authors, I added the word "pure" here to improve layout; is this okay?

Corollary 2.7. *There exist pure* $[[m+2, m, 2]]$*-codes when* m *is even and pure* $[[m+3, m, 2]]$*-codes when* m *is odd. These values of* n *are minimal among general quantum stabilizer codes.*

The linear quaternary case

We can use *linear* quaternary codes (over the alphabet $\mathbb{F}_4$) in order to construct (automatically pure) $[[n, n-2m, d]]$ quantum codes. Here is the translation theorem:

Theorem 2.8. *The following are equivalent:*

- *a pure quantum code* $[[n, n-2m, t+1]]$ *which is linear over* $\mathbb{F}_4$*;*
- *a set of* n *points in* $\mathsf{PG}(m-1,4)$ *all* t *of which are in general position and such that the intersection size with any hyperplane has the same parity as* n*;*
- *an* $[n,m]_4$ *code of strength* t *all of whose weights are even;*
- *an* $[n,m]_4$ *code of strength* t *which is self-orthogonal with respect to the Hermitian form.*

Proof. Consider the equivalence of the first two items, using Theorem 2.6. Observe that a hyperplane of $\mathsf{PG}(m-1,4)$ is a secundum of $\mathsf{PG}(2m-1,2)$. This shows that the first item implies the second. Assume now the condition of the second item is satisfied and consider a secundum S which is not an $\mathbb{F}_4$-hyperplane. Let $K = S \cap \omega S$ be the largest $\mathbb{F}_4$-subspace contained in S. Then K has binary codimension 4 in $V = \mathbb{F}_2^{2m}$. The quaternary hyperplanes containing K form a spread $\{S_1, \dots S_5\}$ in the factor space V/K and S/K is a line in this factor space $\mathsf{PG}(3,2)$. Let m be the number of codepoints (lines if considered binary) contained in K and a_i the number of codepoints in S_i but not in K. Then $n = m = \sum a_i$ is the number of codepoints, and the quaternary condition applied to S_i shows $\sum_{j \neq i} a_j$ even. It follows that all a_i have the same parity. The number of codepoints disjoint from S is the sum of two of those numbers and therefore even.

The equivalence with the third item is obvious. Finally, the Hermitian form is identically zero if and only if each vector is orthogonal to itself. In the quaternary case this is equivalent with the weights being even. □

3 The role of impurity

Proposition 3.1. *An* $[[n,m,d]]$ *of strength* 0 *is equivalent with an* $[[n-1,m,d]]$*. An* $[[n,m,d]]$ *with a double codeline is equivalent with an* $[[n-2,m,d]]$*.*

Proof. The first statement is a special case of Lemma 2.5. The same observation yields the second statement. □

Theorem 3.2. *Let* C *be an* $[[n, n-r, d]]$*-code of strength* ≥ 1 *without double codelines, where* $d \geq 3$*. Let* $P_1, \dots, P_k$ *be the points on more than one codeline, denote by* u_i *the valency of* P_i*. Then*

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

Proof. Let $L_1 = P_1Q_1$ and $L_2 = P_1Q_2$ be codelines. There is a hyperplane $H_{1,2}$ containing all remaining codelines and intersecting each of L_1, L_2 in P_1. In particular there is no triangle of codelines. Let $L_i = P_1Q_i$ be the codelines through P_1 and $H_{1,i}$ the hyperplane determined by L_1, L_i. Then $U_1 = \bigcap H_{1,i}$ where $i = 2, \dots u_1$, has codimension $u_1 - 1$. It contains all remaining codelines and meets each L_i precisely in P_1. The bundles of codelines through P_i do not intersect. The intersection U of the subspaces $U_i, i = 1, 2 \dots, k$ has codimension $\kappa = \sum(u_i - 1)$. The lines contained in U (if any) are pairwise different. As U also contains the $P_i, i = 1, \dots k$, the statement is obtained. □

4 A construction in case $d = 3$

In the pure case the n lines describing an $[[n, n - r, 3]]$ form a partial spread. The following construction is essentially from Blokhuis-Brouwer [5].

Theorem 4.1. *Let S be a secundum of $\mathsf{PG}(r, 2)$. There is a partial spread partitioning the points outside S.*

The space $\mathsf{PG}(r, 2)$ possesses a spread if r is odd. If r is even and $E \subset \mathsf{PG}(r, 2)$ is a plane, then the points outside E can be partitioned into a partial spread.

Proof. Use the argument from [5]. Consider $V_{k+2} = \mathbb{F}_2^{k+2}$ whose elements we write as (a, b, c) where $a \in F = \mathsf{GF}(2^k), b, c \in \mathbb{F}_2$. Let $\epsilon \in F \setminus \mathbb{F}_2$. For each $x \in F$ consider the line $L_x = \langle (x, 1, 0), (\epsilon x, 0, 1)\rangle$. These are pairwise disjoint and partition the points outside the secundum $b = c = 0$. This proves the first statement. The rest follows by induction. □

Corollary 4.2. *Let $g_{l,i} = \left(2^l - 2^{l-2i}\right)/3$. If $l - 2i = 0$ or $l - 2i \geq 3$ there is a pure $[[g_{l,i}, g_{l,i} - l, 3]]$ quantum code.*

Proof. The number $g_{l,i}$ is the number of lines partitioning the points of V_l outside V_{l-2i}. The corresponding partial spread defines the quantum code. The self-orthogonality condition of Theorem 2.6 is satisfied as a secundum has an odd number of points and intersects a V_{l-2i} with $l - 2i \geq 3$ in an odd number of points. □

This family contains the so-called Hamming codes and Gottesman codes; see [6, Theorems 10 and 11], and the quaternary special case of [2, Theorem 12]. Some small examples are

$$[[5, 1, 3]], [[8, 3, 3]], [[21, 15, 3]], [[40, 33, 3]] .$$

In fact we can use this method recursively:

Corollary 4.3. *Let $g_{l,i}$ as in Corollary 4.2 where $l-2i \geq 4$. If there is a pure $[[n, n-(l-2i), 3]]$ then there is a pure $[[g_{l,i}+n, g_{l,i}+n-l, 3]]$.*

Proof. Use the partial spread to partition the points outside the V_{l-2i} and the codelines of the $[[n, n-(l-2i), 3]]$ inside the V_{l-2i}. □

Application to $[[32, 25, 3]]$ and $[[5, 0, 3]]$ yield a $[[37, 30, 3]]$. This solves an existence problem left open in [13]. Observe the clarity of the construction: we work in V_7. The 32 lines of the first code partition the points outside a secundum V_5, the lines of the second code can be chosen to partition the points of a hyperplane of the V_5, or alternatively as a partition of the points of a parabolic quadric in V_5.

5 The geometric description in case $d = 3$

Theorem 2.8 describes linear quantum codes with $d = 3$ as sets of n different points meeting each hyperplane in the same parity as n. Equivalently this is a projective linear $[n, m]_4$-code all of whose weights are even. The complementary point set will then have the same property. We arrive at the following result.

Theorem 5.1. *The following are equivalent:*

- *a pure linear $[[n, n-2m, 3]]$-code;*
- *a set of n different points in $\mathsf{PG}(m-1, 4)$ meeting each hyperplane in the same parity as n;*
- *a projective linear $[n, m]_4$-code all of whose weights are even;*
- *a pure linear $[[(4^m-1)/3-n, (4^m-1)/3-n-2m, 3]]$-code.*

Observe that point sets of $\mathsf{PG}(m-1, 4)$ of even cardinality with the property from Theorem 5.1 form a binary linear code (they are closed under symmetric sums) and the symmetric sum of two lines (a *double line*) in $\mathsf{PG}(2, 4)$ belongs to the code. Its complement is a $[[13, 7, 3]]$-code. Also, the hyperoval in $\mathsf{PG}(2, 4)$ has this property. It yields a $[[6, 0, 3]]$ code. An appropriate symmetric sum with a double line produces a set of 10 points and therefore a $[[10, 4, 3]]$-code. Its complement in $\mathsf{PG}(2, 4)$ is a $[[11, 5, 3]]$-code. The union of two disjoint hyperovals yields a $[[12, 6, 3]]$-code. Its complement yields a second construction of a $[[9, 3, 3]]$-code. The complement of a Fano plane in $\mathsf{PG}(2, 4)$ is a $[[14, 8, 3]]$-code. A line yields a $[[5, 0, 3]]$-code and its complement is a $[[16, 10, 3]]$-code.

This yields satisfactory descriptions for many of the $d = 3$ codes.

A quadratic construction

Not all examples are of this form. For example, a pure $[[9,3,3]]$ can also be constructed via the elliptic quadric in $\mathsf{PG}(5,2)$. It has 27 points and there is a spread partitioning those 27 isotropic points. Each secundum meets it in odd cardinality.

More generally consider the hyperbolic and elliptic quadrics $Q^+(2m-1)$ and $Q^-(2m-1)$ in $\mathsf{PG}(2m-1,2)$. Their number of points $(2^m-1)(2^{m-1}+1)$ in the hyperbolic, $(2^m+1)(2^{m-1}-1)$ in the elliptic case. Let $m=2l$ be even in the hyperbolic case, $m=2l+1$ odd in the elliptic case. The quadrics can be partitioned into generators. Those generators, of projective dimension $2l-1$, can themselves be partitioned into lines. It follows that the quadrics can be partitioned into lines. As each quadric in binary projective space is either empty or has an odd number of isotropic points, it follows that the secundum condition is satisfied in those cases. We have proved the following result.

Theorem 5.2. *Let $n=(2^{2l-1}+1)(4^l-1)/3$ for $l\geq 2$. Then there is a pure*

$$[[n,n-4l,3]]\text{-code.}$$

Let $n=(2^{2l+1}+1)(4^l-1)/3$ for $l\geq 1$. Then there is a pure

$$[[n,n-4l-2,3]]\text{-code.}$$

Examples are parameters $[[9,3,3]]$, $[[45,37,3]]$, $[[155,145,3]]$.

Using the complement

When n is large it is natural to consider the set of points that are not contained in the union of the codelines.

Theorem 5.3. *Let n,r be given and $y=2^r-1-3n$. A pure $[[n,n-r,3]]$ quantum code is equivalently described by the following:*

- *a self-orthogonal projective code C of length y and dimension $\leq r$;*
- *a partial spread of n lines in $\mathsf{PG}(r-1,2)$ covering the points which are not columns of a generator matrix of C.*

Proof. Start from a pure quantum code, let Y be the set of y points in $\mathsf{PG}(r-1,2)$ not contained in a line of the corresponding partial spread and X its complement. Then y and n have different parities. Let S be a secundum. Then $S\cap X$ has the same parity as n, so $S\cap Y$ has the parity of y.

Let G be the (r, y)-matrix whose columns are the points of Y, and C the projective code generated by G. We saw that each secundum S meets Y in the parity of y. Let H be a hyperplane, $m = |H \cap Y|$. Then all weights of the corresponding code have the same parity. This is therefore even. It follows that m has the same parity as y and all words of C have even weight. Let $u, v \in C$ and denote by a, b, c, d the number of coordinates where the entries of u and v are $(0,0), (0,1), (1,0), (1,1)$, respectively. We saw that a has the parity of y whereas b, c are even. As $a + b + c + d = y$ this implies that d is even and $u \cdot v = 0$. We have that C is a self-orthogonal projective code. Clearly we have reached an equivalent description. □

In Theorem 5.3 it is impossible that y is 2 mod 3 (otherwise 2^r would have to be a multiple of 3), and y is a multiple of 3 if m is even, y is 1 mod 3 if m is odd. This description in terms of the complement Y is particularly useful when $y = 2^r - 1 - 3n$ is small.

Definition 5.4. Let $\mathcal{Y}$ be the family of point sets $Y \subseteq \mathsf{PG}(l, 2)$ with the property that the matrix with the elements of Y as columns generates a self-orthogonal code. Let $y = |Y|$ be the length and k the dimension of this code.

Observe that subspaces $\mathsf{PG}(k, 2)$ for $k \geq 2$ belong to $\mathcal{Y}$ and that $\mathcal{Y}$ is closed under symmetric sums.

Proposition 5.5. *Let $Y \in \mathcal{Y}$. If $y \leq 13$, then one of the following occurs.*

(1) $y = 7, k = 3$ *and Y a plane;*

(2) $y = 8, k = 4$ *and Y is the complement of a plane. The corresponding code is the $[8, 4, 4]_2$ extended Hamming code;*

(3) $y = 11, k = 5$ *and $Y = E_1 \oplus E_2 \oplus S$ is the symmetric sum of two planes E_1, E_2 meeting in a point and a solid containing E_2;*

(4) $y = 12, k = 5$ *and Y is the exclusive or $E_1 \oplus E_2$ of two planes meeting in a point;*

(5) $y = 12, k = 6$ *and Y is equivalent to the set of 6-tuples of weights 1 or 5;*

(6) $y = 13, k = 6$ *and $Y = E_1 \oplus E_2 \oplus S$ is the symmetric sum of two skew planes E_1, E_2 and a solid containing E_2.*

Proof. Obviously $y \leq 6$ is impossible, and Y is a plane if $y = 7$. If $y = 8$ then $k = 4$. We must have the complement of a plane. Considering complements cases $y = 9$ and $y = 10, k = 4$ are excluded.

Let now $y = 10, k = 5$ and write a generator matrix $(I|P)$. Then P is a quadratic matrix with rows of odd weight and even pairwise intersections. No

row of P can have weight 5. If there is a row of weight 1, then Y intersects a hyperplane H in 8 points and $Y \oplus H$ has 9 points, contradiction. It follows that all rows of P have weight 3. This is impossible.

Let $y = 11$. Necessarily $k = 5$. Assume P has a row of weight 1. The column containing this entry 1 contradicts projectivity. Let a be the number of rows of P that have weight 5. The remaining rows have weight 3. Case $a = 5$ leads to a solution, likewise $a = 2$ and $a = 1$. They are all equivalent.

Let $y = 12$. Considering complements we have $k = 5$ or $k = 6$. Let at first $k = 5$. Rows of weights 1 or 7 of P lead to the usual contradictions. Assume P has a row of weight 3. Then Y intersects a hyperplane S in 8 points and $Y \oplus S$ has cardinality 11. This leads to $Y = E_1 \oplus E_2$. It is impossible that all rows of P have weight 5.

Let now $y = 12, k = 6$. Then P is a $(6, 6)$-matrix. None of its rows has weight 1. It is impossible that more than four rows have weight 3. Assume there are two rows of weight 3. Then there are exactly two rows of weight 5 and the completion is uniquely determined. It cannot be that there is only one row of weight 3. The remaining case is when all rows of P have weight 5.

Let $y = 13$. Assume $k = 5$. Consider the $(5, 8)$-matrix P. By the usual argument no row can have weight 1. Assume there is a row of weight 3. This leads to a hyperplane intersection of 9 and a solution for $y = 10$, contradiction. The same argument applies when two rows of weight 7 are present. The cases of one or zero rows of weight 7 are easily excluded as well.

The final case is $y = 13, k = 6$. Assume at first there is an intersection of 4:

$$(1111|10|0), (1111|01|0)\,.$$

There are two rows ending in 1. Those 4 rows can be chosen. There is a row number 5 ending in 0. This can be completed in two ways:

$$\left(\begin{array}{c|c|c} 1111 & 10 & 0 \\ 1111 & 01 & 0 \\ 1100 & 00 & 1 \\ 1010 & 00 & 1 \\ 1110 & 11 & 0 \\ 0001 & 11 & 0 \end{array}\right) \text{ or } \left(\begin{array}{c|c|c} 1111 & 10 & 0 \\ 1111 & 01 & 0 \\ 1100 & 00 & 1 \\ 1010 & 00 & 1 \\ 0001 & 11 & 0 \\ 0110 & 00 & 1 \end{array}\right).$$

Those sets are equivalent. The last case is

$$(11|10|000), (11|01|000)\,,$$

with all other types $(\text{odd}, 11, \text{even})$ or $(\text{even}, 00, \text{odd})$. The third row can be chosen $(10|11|000)$. If there is another row with 11 in the middle the last section

shows that this is impossible. The remaining rows have 00 in the middle. Whenever the last sections intersect the first section yields a contradiction. Now the last section yields a contradiction. □

The non-existence in cases $y \leq 10, y \neq 7, 8$ leads to the following corollary.

Corollary 5.6. *Let $0 < y \leq 10, y \neq 7, 8$. Then there is no pure $[[n, n-r, 3]]$-code with $n = (2^r - 1 - y)/3$.*

In particular pure quantum codes with parameters

$$[[7, 2, 3]], [[39, 32, 3]], [[83, 75, 3]], [[82, 74, 3]]$$

do not exist. By Section 3 the assumption of purity can be dropped: no additive quantum codes with those parameters can exist. In fact, by Proposition 3.1 it can be assumed that the code has strength 1 and there are no multiple codelines. The non-existence of the corresponding impure codes follows from Theorem 3.2. This solves two of the values left open in Grassl's database [13]. Nonexistence in case $y = 13, k = 5$ shows that there is no pure $[[6, 1, 3]]$.

Geometrically the most natural approach is to fix the redundancy $r = n - m$ and determine the values of n for which pure $[[n, n-r, 3]]$-codes exist. Equivalently these are partial spreads of n lines in $V_r = \mathsf{PG}(r-1, 2)$ such that for each secundum S there is an even number of codelines skew to S.

The smallest value of r is $r = 4$ and the only possible length is then $n = 5$. We saw the $[[5, 1, 3]]$, the spread in $\mathsf{PG}(3, 2)$, or equivalently, the projective line $\mathsf{PG}(1, 4)$.

Let $r = 5$. The obvious bound is $n \leq 10$. Length $n = 10$ and $n = 9$ are impossible by Corollary 5.6. We know an $[[8, 3, 3]]$ from Corollary 4.2. An impure $[[6, 1, 3]]$ does exist because of the pure $[[5, 1, 3]]$. Finally a pure $[[5, 0, 3]]$ exists: it may be derived either from a spread of $\mathsf{PG}(3, 2)$ or from a spread of the parabolic quadric in $\mathsf{PG}(4, 2)$. This completes the spectrum of the values of n for which $[[n, n-5, 3]]$-codes exist: $n \in \{5, 6, 8\}$. For $n = 5, 8$ these are pure, for $n = 6$ it is necessarily impure.

Consider redundancy $r = 6$. First of all there are the linear codes, derived from subsets of $\mathsf{PG}(2, 4)$. We saw how this yields examples for $n = 8$, $n = 13$ (double lines and their complements), $n = 6$, $n = 15$ (hyperovals and their complements), $n = 10$, $n = 11$ (a suitable sum of a hyperoval and a double line as well as the complement), $n = 9$, $n = 12$ (union of two disjoint hyperovals and the complement), $n = 7$, $n = 14$ (a Fano plane and its complement), $n = 5$, $n = 16$ (a line and its complement). We also saw a second construction of a pure $[[9, 3, 3]]$ based on a quadric. This completes the spectrum for $5 \leq n \leq 16$. Corollary 4.2 produces $[[21, 15, 3]]$. A (necessarily pure) $[[17, 11, 3]]$ will be constructed later on. Theorem 5.3 and Proposition 5.5 imply nonexistence for $18 \leq n \leq 20$.

Let $r = 7$. Pure codes $[[37, 30, 3]]$ and $[[40, 33, 3]]$ follow from Corollary 4.2. Grassl has existence for all lengths except possibly for those between 36 and 39. We showed non-existence for $n = 39$, existence for $n = 37$. Later we will construct pure codes corresponding to lengths 36 and 38 as well. In redundancy 8 an application of Corollary 4.3 in case $l = 8, i = 1$ to the pure $[[17, 11, 3]]$ yields $[[81, 73, 3]]$. This decides one of the cases left open in Grassl's list.

The next cases for $d = 3$ left open by Grassl are

$$[[83, 74, 3]], [[87, 78, 3]], [[89, 80, 3]], [[91, 82, 3]], [[93, 84, 3]],$$
$$[[95, 86, 3]], [[97, 88, 3]], [[99, 90, 3]], [[101, 92, 3]],$$
$$[[103, 94, 3]], [[105, 96, 3]], [[107, 98, 3]], [[109, 100, 3]],$$

all with $r = 9$. They are expected to exist.

6 A link to APN-functions

Consider the following situation: a pure quantum code $[[n, n-r, 3]]$ as described by a partial spread of n lines in $\mathsf{PG}(r-1, 2)$, and Y the set of $y = 2^r - 1 - 3n$ points not in the codelines. Assume Y is contained in a hyperplane H of $\mathsf{PG}(r-1, 2)$. Then the partial spread must contain 2^{r-2} lines which partition the affine points (those outside H). This leads to the following definition.

Definition 6.1. Let H be a hyperplane of $\mathsf{PG}(r-1, 2)$. A *factor of exterior lines* is a set E of 2^{r-2} pairwise skew lines none of which is in H (equivalently, the lines partition the points off H). Let $S(E) \subset H$ be the set of intersections of the lines of E with H.

The situation can be equivalently described inside H: let the points of H be those with last coordinate $= 0$. The points of $g \in E$ are $(a : 1), (b : 1)$ and $(a + b, 0) \in H$. Let $V_{r-1} = \mathbb{F}_2^{r-1}$ be the space underlying H. With $g \in E$ the pairs $\{a, b\}$ describe a partition of V_{r-1} and the sums $a+b$ are pairwise different. This leads to the following equivalent description.

Definition 6.2. A *sum-disjoint partition* π of V_{r-1} is a partition into pairs such that the sums of those pairs are pairwise different. Let $S(\pi)$ be the set of those sums. Clearly $0 \notin S(\pi)$ and $|S(\pi)| = 2^{r-2}$.

We can view $S(\pi)$ as a subset of $\mathsf{PG}(r-2, 2)$. A third equivalent description of the same concept is in terms of a generalization of the notion of an APN-function.

Definition 6.3. A *local APN bijection* of V_{r-1} with respect to $0 \neq a$ is a bijective mapping $f : V_{r-1} \to V_{r-1}$ which satisfies that its derivative $\delta_{f,a}$ at a defined by

$$\delta_{f,a}(x) = f(x+a) + f(x)$$

is 2 to 1.

Recall that a function is APN if it satisfies the 2 to 1 condition above for all $a \neq 0$. The letters APN stand for *almost perfectly nonlinear.* This notion came up originally in the study of cryptographic S-boxes, see [7].

Theorem 6.4. *The following are equivalent:*

(1) *a factor of external lines of* $\mathsf{PG}(r-1,2)$ *with respect to a hyperplane;*

(2) *a sum-disjoint partition of* V_{r-1}*;*

(3) *a local APN bijection of* V_{r-1} *with respect to some* $a \neq 0$*.*

Proof. The equivalence of the first two concepts has been observed earlier. Let f be a local APN bijection with respect to a. The pairs $\{f(x), f(x+a)\}$ form a sum-disjoint partition. Conversely let π be a sum-disjoint partition. Define the bijection f such that $f(x)$ and $f(x+a)$ form a part of π for all x. Then f is locally APN. □

Proposition 6.5. *Let* $q = 2^{r-1}$*. A bijective APN function of* V_{r-1} *is equivalent with a family of* $q-1$ *factors of exterior lines of* $\mathsf{PG}(r-1,2)$ *with respect to a hyperplane* H *partitioning the set of all exterior lines.*

It is also equivalent to a family of $q-1$ *sum disjoint partitions of* V_{r-1} *which together partition the set of all pairs.*

This follows directly from Theorem 6.4. Observe that the number of exterior lines is indeed $(2^{r-1}-1)2^{r-2} = (q-1)2^{m-2} = \binom{q}{2}$. The expression in terms of sum-disjoint partitions can be equivalently expressed as a 1-factorization of the complete graph on V_{r-1} with the additional property that each of its $q-1$ factors is sum-disjoint.

Proposition 6.6. *Let* $H \subset V_{r-1}$ *be a hyperplane and* M *a linear mapping from* H *to* H *such that both* M *and* $I+M$ *are invertible. Let* $r \in V_{r-1} \setminus H$*. Then* $\pi = \big\{\{x, r+Mx\} \mid x \in H\big\}$ *is a sum-disjoint partition of* V_{r-1} *whose set of sums is* $S(\pi) = \overline{H}$*.*

Proposition 6.6 is a slightly generalized form of the Blokhuis-Brouwer construction, Theorem 4.1. The proof is trivial. Equivalently, there is always a local APN bijection such that the $f(x+a)+f(x)$ run through the complement of a subspace of codimension 1.

This construction is not very useful in the situation when $Y \subset H$, where H is a hyperplane of V_m. The reason is that the remaining spread lines together with Y would fill a V_{m-2}. This would describe a quantum code obtained by the recursive construction of Corollary 4.3. It is therefore desirable to have more constructions of sum-disjoint partitions. We know that bijective APN-functions are examples. Unfortunately no bijective APN-functions on $\mathsf{GF}(2^n)$ are known when n is even.

Elementary moves

Here is what seems to be the most elementary way of constructing a sum-disjoint partition from another one. Let $\Sigma = S(\pi)$ be given and $\{x, x'\}, \{y, y'\} \in \pi$ (so that $x + x', y + y' \in \Sigma$). Assume $x + y, x' + y' \notin \Sigma$. Then replacing the two pairs above by $\{x, y\}, \{x', y'\}$ we obtain another sum-disjoint partition whose set of sums Σ' differs from Σ in that $x + x', y + y'$ have been removed and $x + y, x' + y'$ added.

7 Constructions

In this section we will construct pure quantum codes $[[17, 11, 3]], [36, 29, 3]]$ and $[[38, 31, 3]]$. The latter two parameters are new. For the first two the construction is direct and easy to verify. In length 38 we start from the BB-construction (Proposition 6.6) which is modified by three elementary moves.

Pure $[[17, 11, 3]]$-codes

Let $k = 6$. We work in $\mathbb{F}_2^6, Y$ consists of the vectors of weights 1 and 5 and the quantum code is defined by a family of 17 lines partitioning the points of weights different from 1 and 5. One such partition is closely related to the S_6-generalized quadrangle. Write points of $\mathbb{F}_2^6$ in terms of subsets of $\{1, 2, 3, 4, 5, 6\}$ such that 111000 for example is represented by 123. Our partial spread consists of

- lines $l_1, \ldots l_5$ partitioning the points of weight 4;
- $l_6 = \{123, 456, 123456\}$;
- $l_7 = \{12, 13, 23\}, l_8 = \{45, 46, 56\}$;
- 9 lines containing one point of weight 2 and two of weight 3. Consider the permutations λ, ρ defined by $\lambda = (1, 2, 3), \rho = (4, 5, 6)$. Let

$a \in \{1,2,3\}, b \in \{4,5,6\}$. The line indexed by $\{a,b\}$ is

$$\{ab, a\lambda(a)b, ab\rho(b)\}\,.$$

Here the lines partitioning the weight 4 points are equivalent to a spread of the S_6-generalized quadrangle. There is also a construction using $k = 5$.

Construction of [[36, 29, 3]]

This time $y = 19$ and $k \in \{5,6,7\}$. There is a construction for $k = 5$. We give here a construction in case $k = 7$ which is more symmetric. Let $Y = \langle e_1, e_2, e_3\rangle \oplus \langle e_1, e_4, e_5\rangle \oplus \langle e_1, e_6, e_7\rangle$ be the union of three planes meeting in a common point. The quantum code is described by 36 lines partitioning the points outside Y. Let $V = \mathbb{F}_2^2$. Write $\mathbb{F}_2^7$ as $\mathbb{F}_2 \times V^3$. The points to partition are (ϵ, u, v, w) where $\epsilon \in \mathbb{F}_2$ and at most one of u, v, w is $= 0$. For brevity write those vectors as $1uvw$ or $0uvw$. One way of choosing those lines is as follows: The first 18 lines are

$$\{1abb, 10ab, 0ac0\}, \{1b0a, 1bab, 00ac\}, \{1bba, 1ab0, 0c0a\}\,.$$

Here a, b, c are arbitrary nonzero pairwise different elements of V. In order to describe the remaining 18 lines fix a permutation $\rho = (a, b, c)$ of the nonzero elements of V. With this notation the remaining lines are

$$\{1abc, 10aa, 0acb\}, \{1acb, 1c0c, 0bca\}, \{1aa0, 1bbb, 0ccb\},$$
$$\{00aa, 0abb, 0acc\}, \{0a0a, 0bab, 0cac\}, \{0aaa, 0bb0, 0cca\}\,.$$

Construction of [[38, 31, 3]]

Let $E = \langle e_1, e_2, e_3\rangle, E' = \langle e_4, e_5, e_6\rangle$, $Y = (E \setminus \langle e_3\rangle) \cup (e_3 + (E' \setminus 0))$. The corresponding code, with generator matrix

$$\left(\begin{array}{c|c} 101101 & 0000000 \\ 011011 & 0000000 \\ 000111 & 1111111 \\ \hline 000000 & 1010101 \\ 000000 & 0110011 \\ 000000 & 0001111 \end{array}\right)$$

has weights $4, 6, 8, 10$. Use the hyperplane $H = (x_3 = x_4)$. The codeword corresponding to H has weight 6. In fact,

$$Y \cap H = \{e_1, e_2, e_1 + e_2, e_3 + e_4, e_3 + e_4 + e_5, e_3 + e_4 + e_6, e_3 + e_4 + e_5 + e_6\}$$

is the union of a line and a quadrangle. The strategy is to replace $\overline{H}$ by Σ such that

$$Y \cap \overline{H} = \{e_1 + e_3, e_2 + e_3, e_1 + e_2 + e_3, e_3 + e_5, e_3 + e_6, e_3 + e_5 + e_6\}$$

is removed (by 3 elementary moves) and replaced by a set S of 6 points from H. Those six points should be the union of two lines. It should be possible to partition the remaining 18 points of H (outside $Y \cap H$ and S) into lines as well. The reason to believe this is the BB-construction again: it implies that $H = V_5$ can be partitioned into a quadrangle and 9 lines.

Here are the details. Let $M : H \to H$ and $r = e_1 + e_3 \notin H$. The corresponding sum-disjoint partition consists of the pairs $\{x, e_1 + e_3 + Mx\}$ where $x \in H$. The sum is $e_1 + e_3 + (1 + M)x \in \overline{H}$. We want to replace 6 of those sums corresponding to $x = a_1, \ldots, a_6 \in H$ where $a_1 = 0 = \sum a_i$. Only $a_2, \ldots, a_5$ need to be determined. The conditions are

$$a_2 + Ma_2 = e_2\,, \qquad a_3 + Ma_3 = e_1 + e_2\,,$$
$$a_4 + Ma_4 = e_1 + e_5\,, \qquad a_5 + Ma_5 = e_1 + e_6\,.$$

This makes sure that the six sums above (those we will knock out) vary over the set $Y \cap \overline{H}$ that we wish to remove. The condition that both M and $I + M$ should be invertible is equivalent with:

- a_2, a_3, a_4, a_5 are linearly independent;
- $a_2 + e_2, a_3 + e_1 + e_2, a_4 + e_1 + e_5, a_5 + e_1 + e_6$ linearly independent.

A possible choice is

$$a_2 = e_1 + e_5,\ a_3 = e_1,\ a_4 = e_1 + e_2 + e_6,\ a_5 = e_3 + e_4 + e_6$$

(automatically $a_6 = e_1 + e_2 + e_3 + e_4 + e_5$), and

$$M = \begin{pmatrix} 0 & 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 \end{pmatrix}$$

in terms of the basis $e_1, e_2, e_3 + e_4, e_5, e_6$ of H. We can choose as new pairs on those 12 points

$$\{0, a_2\}, \{a_3, a_4\}, \{a_5, a_6\},$$
$$e_1 + e_3 + \{0, Ma_2\}, e_1 + e_3 + \{Ma_3, Ma_4\}, e_1 + e_3 + \{Ma_5, Ma_6\},$$

with new sums $e_1+e_5, e_2+e_6, e_1+e_2+e_5+e_6$ and their images under M, $e_1+e_2+e_5, e_5+e_6, e_1+e_2+e_6$.

It remains to check if the remaining 18 points are indeed on a partial spread. Those 18 points are the following:

$$\left(\begin{array}{l|l|l|l} Q_1=000010 & P_1=101100 & P_7=011100 & P_{13}=111100 \\ Q_2=000001 & P_2=100001 & P_8=010010 & P_{14}=111110 \\ & P_3=101110 & P_9=011110 & P_{15}=111101 \\ & P_4=101101 & P_{10}=011101 & P_{16}=111111 \\ & P_5=100011 & P_{11}=010011 & \\ & P_6=101111 & P_{12}=011111 & \end{array}\right).$$

A partial spread is as follows:

$$(Q_1,4,6),(Q_2,9,12),(2,10,13),(1,8,14),(3,11,15),(5,7,16)\,.$$

Here we wrote i for point P_i. This produces a $[[38,31,3]]$. Its lines are the 26 surviving lines of the original BB-construction, the 6 lines completing them to the new sum-disjoint partition Σ and the 6 lines just constructed which partition the remaining 18 points.

8 Case $d=4$ and quantum caps

The smallest redundancy of interest is $r=6$. The linear cases can be described in terms of quaternary caps. Let us call a cap in $\mathsf{PG}(m-1,4)$ a *quantum cap* if it satisfies the condition of Theorem 2.8 for $t=3$: the corresponding code has only even weights. In case $r=6$ we have the hyperoval in $\mathsf{PG}(2,4)$. This is an exceptional situation as it has strength 3 and therefore yields $[[6,0,4]]$.

Let $r=7$. For $n\geq 8$ we know from [4] that not even the underlying additive codes exist (in the pure case). In length $n=7$ the underlying additive code would have to be a $[7,3.5,4]_4$-code and we know from [4] that no such code satisfies the quantum condition.

Next let $r=8$. Quantum caps in $\mathsf{PG}(3,4)$ are known for $n=8,12,14,17$, the most obvious case being the elliptic quadric. For $n=10$ no such cap exists. Other examples of quantum caps include one of the two 41-caps in $\mathsf{PG}(4,4)$ (see [9]), the 40-cap in $AG(4,4)$ (see [11]), the Glynn cap in $\mathsf{PG}(5,4)$ (see [12, 10], (its weight distribution is $A_0=1, A_{88}=945, A_{96}=3087, A_{120}=63$), a 756-cap in $\mathsf{PG}(7,4)$ and a 5040-cap in $\mathsf{PG}(9,4)$ (see [8]). This yields pure linear quantum codes

$$[[40,30,4]],[[41,31,4]],[[126,114,4]],[[756,740,4]],[[5040,5020,4]]\,.$$

The union of two hyperovals on two planes of $\mathrm{PG}(3,4)$ intersecting in an exterior line clearly is a quantum cap $[[12,4,4]]$.

References

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

[2] **J. Bierbrauer** and **Y. Edel**, Quantum twisted codes, *J. Combin. Des.* **8** (2000), 174–188.

[3] **J. Bierbrauer**, **G. Faina**, **S. Marcugini** and **F. Pambianco**, Additive quaternary codes of small length, Proceedings ACCT, Zvenigorod (Russia) September 2006, 15–18.

[4] **J. Bierbrauer**, **Y. Edel**, **G. Faina**, **S. Marcugini** and **F. Pambianco**, Short additive quaternary codes, *IEEE Trans. Inform. Theory*, submitted.

[5] **A. Blokhuis** and **A. E. Brouwer**, Small additive quaternary codes, *European J. Combin.* **25** (2004), 161–167.

[6] **A. R. Calderbank**, **E. M. Rains**, **P. M. Shor** and **N. J. A. Sloane**, Quantum error-correction via codes over $\mathrm{GF}(4)$, *IEEE Trans. Inform. Theory* **44** (1998), 1369–1387.

[7] **C. Carlet**, **P. Charpin** and **V. Zinoviev**, Codes, bent functions and permutations suitable for DES-like cryptosystems, *Des. Codes Cryptogr.* **15** (1998), 125–156.

[8] **Y. Edel**, `http://www.mathi.uni-heidelberg.de/~yves`.

[9] **Y. Edel** and **J. Bierbrauer**, 41 is the largest size of a cap in $\mathrm{PG}(4,4)$, *Des. Codes Cryptogr.* **16**(1999), 151–160.

[10] _____, Large caps in small spaces, *Des. Codes Cryptogr.* **23** (2001), 197–212.

[11] _____, The largest cap in $\mathrm{AG}(4,4)$ and its uniqueness, *Des. Codes Cryptogr.* **29** (2003), 99–104.

[12] **D. Glynn**, A 126-cap in $\mathrm{PG}(5,4)$ and its corresponding $[126,6,88]$-code, *Util. Math.* **55** (1999), 201–210.

[13] **M. Grassl**, `http://www.codetables.de`.

Jürgen Bierbrauer

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

e-mail: jbierbra@mtu.edu

Giorgio Faina

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

e-mail: faina@dipmat.unipg.it

Massimo Giulietti

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

e-mail: giuliet@dipmat.unipg.it

Stefano Marcugini

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

e-mail: gino@dipmat.unipg.it

Fernanda Pambianco

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

e-mail: fernanda@dipmat.unipg.it