Available online at www.sciencedirect.com
ScienceDirect
Discrete Mathematics 308 (2008) 6368–6372
DISCRETE MATHEMATICS
www.elsevier.com/locate/disc

Quantum codes from caps

Vladimir D. Tonchev[1]

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

Received 13 September 2007; received in revised form 30 November 2007; accepted 4 December 2007
Available online 7 January 2008

Abstract

Caps in a finite projective geometry over $GF(4)$ are used for the construction of some quantum error-correcting codes, including an optimal [[27, 13, 5]] code.

Keywords: Quantum code; Cap; Projective geometry

1. Introduction

We assume familiarity with the basics of classical error-correcting codes [10] and quantum codes [3]. A linear q-ary $[n, k]$ *code* C is a k-dimensional subspace of the n-dimensional vector space over the field $GF(q)$ of order q. The *dual* code $C^\perp$ of an $[n, k]$ code C is the $[n, n-k]$ code being the orthogonal space of C with respect to a specified inner product. The *ordinary* inner product in $GF(q)^n$ is defined as

$$x \cdot y = \sum_{i=1}^{n} x_i y_i. \tag{1}$$

The *hermitian* inner product in $GF(4)^n$ is defined as

$$(x, y)_H = \sum_{i=1}^{n} x_i y_i^2. \tag{2}$$

The *trace* inner product in $GF(4)^n$ is defined as

$$(x, y)_T = \sum_{i=1}^{n} (x_i y_i^2 + x_i^2 y_i). \tag{3}$$

A code C is *self-orthogonal* if $C \subseteq C^\perp$, and *self-dual* if $C = C^\perp$. A linear code $C \subseteq GF(4)^n$ is self-orthogonal with respect to the trace product (3) if and only if it is self-orthogonal with respect to the hermitian product (2) [3].

E-mail address: tonchev@mtu.edu.
[1] This research was supported by NSA Grant H98230-06-1-0027.

doi:10.1016/j.disc.2007.12.007

An *additive* $(n, 2^k)$ code C over $GF(4)$ is a subset of $GF(4)^n$ consisting of 2^k vectors which is closed under addition. An additive code is *even* if the weight of every codeword is even, and otherwise *odd*. Note that an even additive code is trace self-orthogonal, and a linear self-orthogonal code is even [3]. If C is an $(n, 2^k)$ additive code with weight enumerator

$$W(x, y) = \sum_{j=0}^{n} A_j x^{n-j} y^j, \tag{4}$$

the weight enumerator of the trace-dual code $C^\perp$ is given by

$$W^\perp = 2^{-k} W(x + 3y, x - y). \tag{5}$$

In [3], Calderbank, Rains, Shor and Sloane described a method for the construction of quantum error-correcting codes from additive codes that are self-orthogonal with respect to the trace product (3). Specifically, the following statement was proved in [3].

Theorem 1 ([3]). *An additive trace self-orthogonal* $(n, 2^{n-k})$ *code C such that there are no vectors of weight* $< d$ *in* $C^\perp \setminus C$ *yields a quantum code with parameters* $[[n, k, d]]$.

A quantum code associated with an additive code C is *pure* if there are no vectors of weight $< d$ in $C^\perp$; otherwise, the code is called *impure*. A quantum code is called *linear* if the associated additive code C is linear. We will need also the following result from [3].

Theorem 2 ([3]). *The existence of a linear* $[[n, k, d]]$ *quantum code with associated* $(n, 2^{n-k})$ *additive code C implies the existence of a linear* $[[n - m, k', d']]$ *quantum code with* $k' \geq k - m$ *and* $d' \geq d$*, for any m such that there exists a codeword of weight m in the dual code of the binary code generated by the supports of the codewords of C.*

A table with lower and upper bounds on the minimum distance d for quantum $[[n, k, d]]$ codes of length $n \leq 30$ is given in the paper by Calderbank, Rains, Shor and Sloane [3]. An extended version of this table was compiled by Grassl [8]. An electronic server for bounds on the minimum distance of various codes is available on Andries Brouwer's Web page [2].

An n-cap in $PG(s, q)$, $s \geq 3$, is a set of n points no three of which are collinear (Hirschfeld and Thas [9]). An n-cap is complete if it is not contained in any $(n + 1)$-cap. Tables with bounds on the maximum size of complete caps in various spaces are given in Storme [11].

Suppose that M is an $(s + 1) \times n$ matrix having as columns a set of n vectors in $GF(q)^{s+1}$ representing the points of an n-cap in $PG(s, q)$. Then the dual code $C^\perp$ (with respect to the product (1)) of the linear C code over $GF(q)$ spanned by the rows of M has minimum distance $d \geq 4$, and if the cap is complete, we have $d = 4$. If $q = 4$ and the rows of M are pairwise orthogonal with respect to the trace product (3), the code C defines a quantum code via Theorem 1. The exact minimum distance of the related quantum code can be found by using the identities (4) and (5).

If K is an n-cap in $PG(3, q)$ then $n \leq q^2 + 1$ [12, p. 309]. A $(q^2 + 1)$-cap in $PG(3, q)$, $q \neq 2$, is called an *ovoid*. In [3], an ovoid in $PG(3, 4)$ was used to obtain an optimal quantum $[[17, 9, 4]]$ code, i.e., 4 is the largest possible value of d for $n = 17$ and $k = 7$. Motivated by this example, we investigate in this paper quantum codes obtained from other known complete caps or caps of largest known size in projective spaces over $GF(4)$ of small dimension. One of the complete 41-caps in $PG(4, 4)$ and the known 126-cap in $PG(5, 4)$ lead to a number of quantum codes of various lengths with $d = 4$ that are either optimal or have the largest known value of d for the given n and k. Using a geometric approach similar to the one employed for the construction of an 126-cap in $PG(5, 4)$, we find an incomplete 27-cap in $PG(6, 4)$ that yields an optimal quantum $[[27, 13, 5]]$ code. The best previously known quantum code with $n = 27$ and $k = 13$ had minimum distance $d = 4$ [3].

2. Codes from a complete 41-cap in $PG(4, 4)$

The largest possible size of a complete cap in $PG(4, 4)$ is 41, and up to projective equivalence, there are exactly two 41-caps (Edel and Bierbrauer [4]). The 5×41 matrix (6) of one of these caps, having as columns a set of vectors representing the points of the cap, has pairwise orthogonal rows with respect to the hermitian product (2). Here,

Table 2.1
The weight distribution of $B^{\perp}$

i	0	6	8	10	12	14	15	16	17	18	19	20
$B_i^{\perp}$	1	16	85	220	600	3120	5340	2795	6303	16808	23648	6600

Table 2.2
Quantum codes obtained from a 41-cap in $PG(4, 4)$

No.	m	$[[n, k, d]]$	No.	m	$[[n, k, d]]$	No.	m	$[[n, k, d]]$
1	0	[[41, 31, 4]]	2	6	[[35, 25, 4]]	3	8	[[33, 23, 4]]
4	10	[[31, 21, 4]]	5	12	[[29, 19, 4]]	6	14	[[27, 17, 4]]
7	15	[[26, 16, 4]]	8	16	[[25, 15, 4]]	9	17	[[24, 14, 4]]
10	18	[[23, 13, 4]]	11	19	[[22, 12, 4]]	12	20	[[21, 11, 4]]
13	21	[[20, 10, 4]]	14	22	[[19, 9, 4]]	15	23	[[18, 8, 4]]
16	24	[[17, 7, 4]]	17	25	[[16, 6, 4]]	18	26	[[15, 5, 4]]
19	27	[[14, 4, 4]]	20	29	[[12, 2, 4]]	21	31	[[10, 0, 4]]

and later on throughout this paper, we assume that $GF(4) = \{0, 1, w, w^2\}$, and w and w^2 are labeled by 2 and 3 respectively.

$$M_2 = \begin{pmatrix} 10000112213322333222333020022100311310012 \\ 01000100200210110110130300230321231311222 \\ 00100012002001101101103302003312213311222 \\ 00010110011100011111111111111111111101011 \\ 00001001111122222211133333300022222200113 \end{pmatrix}. \tag{6}$$

The weight enumerator of the linear (41, 5) code C over $GF(4)$ spanned by the rows of (6) is given by

$$W = 1 + 9y^{24} + 12y^{26} + 105y^{28} + 660y^{30} + 90y^{32} + 36y^{34} + 51y^{36} + 60y^{38},$$

while the weight enumerator of the trace-dual code $C^{\perp}$ is

$$W^{\perp} = 1 + 9930y^4 + 176520y^5 + 3178488y^6 + \cdots + 35618160526163496y^{41}.$$

Thus, C defines a quantum [[41, 31, 4]] code via Theorem 1. The dual code $B^{\perp}$ of the binary code B of length 41 spanned by the supports of the vectors in C is of dimension 17. The weight distribution $\{B_i^{\perp}\}$ of $B^{\perp}$ is given in Table 2.1. Since the all-one vector belongs to $B^{\perp}$, we have $B_i^{\perp} = B_{41-i}^{\perp}$ for $0 \leq i \leq 20$.

The parameters of quantum codes obtained from the [[41, 31, 4]] code via Theorem 2 by using vectors of weight m ($0 \leq m \leq 31$) in $B^{\perp}$ are listed in Table 2.2.

Remark 2.3. All codes in Table 2.2 are optimal, that is, $d = 4$ is the largest possible for the given n and k (see [3] for lengths $n \leq 30$ and [8] for lengths 31, 33, 35 and 41). Note that the lower bound on d given in [3] for $n = 29$ and $k = 19$ is $d = 3$.

3. Codes from a 126-cap in $PG(5, 4)$

The largest size of a known complete cap in $PG(5, 4)$ is 126, and there are two known constructions of such a cap (Baker, Bonisoli, Cossidente, and Ebert [1], and Glynn [7]). Glynn [7] uses geometric arguments to determine the weight distribution W of the related linear (126,6) code C over $GF(4)$ spanned by the 6×126 matrix associated with the cap:

$$W = 1 + 945y^{88} + 3087y^{96} + 63y^{120}.$$

Since all weights in C are even, it follows that C is self-orthogonal with respect to the hermitian product (1), as well as with respect to the trace product (3). The minimum distance of its trace-dual code $C^{\perp}$ is 4. Consequently, C yields a quantum $[\![126, 114, 4]\!]$ code via Theorem 1. According to [8], a code with these parameters is optimal, that is, 4 is the largest possible value of d for any quantum $[\![126, 114, d]\!]$ code. The dual code of the binary code spanned by the supports of the nonzero vectors in C contains vectors of weight m, where the values of m are listed in (7).

$$6, 8, 10, 12, 14, 16, 18, 20, 21, \ldots, 106, 108, 110, 112, 114, 116, 118, 120, 126. \tag{7}$$

Consequently, there exist pure quantum $[\![126 - m, 114 - m, 4]\!]$ codes for all values of $m \le 114$ from the list (7) obtained via the shortening construction of Theorem 2. Most of these codes are optimal according to [3,8]: the codes of length $28 \le n \le 126$ obtained for values of m in the range $0 \le m \le 98$ are all optimal; the codes with $20 \le n \le 27$ may be optimal: the theoretical upper bound on d for such codes with $k = n - 12$ is 5. Only the codes of length $n = 12, 14, 16$ and 18 are not optimal: the largest d for an $[\![n, k, d]\!]$ code with $k = n - 12$ is 5 if $n = 14, 16$ or 18, and 6 if $n = 12$ [3].

Several of the codes obtained by shortening of the $[\![126, 112, 4]\!]$ code with respect to a codeword of weight m for various values of m improve upon previously known quantum codes with comparable parameters [5], for examle, $[\![43, 31, 4]\!]$, $[\![63, 51, 4]\!]$, $[\![73, 61, 4]\!]$, $[\![85, 73, 4]\!]$, $[\![105, 93, 4]\!]$, $[\![112, 100, 4]\!]$, $[\![116, 104, 4]\!]$, $[\![118, 106, 4]\!]$.

4. A quantum $[\![27, 13, 5]\!]$ code from an incomplete cap in $PG(6, 4)$

The minimum distance d of a quantum code associated with a complete cap cannot exceed 4. In this section, we describe the construction of an incomplete 27-cap in $PG(6, 4)$ that leads to a quantum $[\![27, 13, 5]\!]$ code. We note that $d = 5$ is the theoretical upper bound for a quantum code with $n = 27$ and $k = 13$, and the best previously known quantum code for these parameters had minimum distance $d = 4$ [3].

The 126-cap in $PG(5, 4)$ was constructed in [1] as a union of six 21-caps, where the caps of size 21 were orbits under a certain projective transformation of order 21. Thus, by construction, the resulting code of length 126 is invariant under a group of order 21. A similar method that employs projective transformations was used by van Eupen and Tonchev earlier in [6] for the construction of certain 3-weight codes over $GF(5)$.

The 7×7 matrix M_7 (8), considered as a matrix over $GF(4)$, defines a projective transformation that partitions the $(4^7 - 1)/3 = 5461$ points of $PG(6, 4)$ into 421 orbits: one fixed point plus 420 orbits of length 13, where the orbits of length 13 are 13-caps:

$$M_7 = \begin{pmatrix} 0 & 0 & 2 & 3 & 0 & 0 & 0 \\ 3 & 3 & 0 & 1 & 1 & 1 & 3 \\ 1 & 1 & 2 & 3 & 2 & 2 & 2 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 3 & 0 & 1 & 1 & 3 & 2 & 1 \\ 0 & 0 & 2 & 3 & 1 & 1 & 1 \\ 2 & 1 & 2 & 0 & 0 & 2 & 3 \end{pmatrix}. \tag{8}$$

The column set of the matrix G_7 (9) consists of two orbits of length 13 plus the fixed point under the transformation defined by M_7:

$$G_7 = \begin{pmatrix} 001001110110101111011111101 \\ 010111121131102200113301011 \\ 032302123023100103001231330 \\ 001223110310311122312302223 \\ 020031021110010203322012213 \\ 020010130130222203101112032 \\ 110331311323210123023133010 \end{pmatrix}. \tag{9}$$

The linear code C over $GF(4)$ spanned by the rows of G_7 is a hermitian self-orthogonal [27, 7, 12] code with weight distribution listed in Table 4.1. The trace-dual code $C^{\perp}$ has minimum distance 5, and weight enumerator (10). Thus, C defines a quantum $[\![27, 13, 5]\!]$ code via Theorem 1. To the best of our knowledge, a code with these parameters was not known before.

$$W_{C^{\perp}} = 1 + 1638y^5 + 13650y^6 + 115518y^7 + 885729y^8 + 5634954y^9 + \cdots. \tag{10}$$

Table 4.1
The weight distribution $\{c_i\}$ of the [27, 7] code C

i	0	12	14	16	18	20	22	24	26
c_i	1	39	3	1170	3705	4953	4797	1677	39

Acknowledgments

The author wishes to thank the referees for their useful constructive remarks that led to several improvements.

References

[1] R.D. Baker, A. Bonisoli, A. Cossidente, G.L. Ebert, Mixed partitions of $PG(5, q)$, Discrete Math. 208/209 (1999) 23–29.
[2] A.E. Brouwer. http://www.win.tue.nl/~aeb/.
[3] A.R. Calderbank, E.M. Rains, P.W. Shor, N.J.A. Sloane, Quantum error correction via codes over $GF(4)$, IEEE Trans. Inform. Theory 44 (1998) 1369–1387.
[4] Y. Edel, J. Bierbrauer, 41 is the largest size of a cap in $PG(4, 4)$, Des. Codes Cryptogr. 16 (1999) 151–160.
[5] Y. Edel, J. Bierbrauer, Quantum twisted codes, J. Combin. Designs 8 (2000) 174–188.
[6] M. van Eupen, V.D. Tonchev, Linear codes and the existence of a reversible Hadamard difference set in $Z_2 \times Z_2 \times Z_5^4$, J. Combin. Theory, Ser. A 79 (1997) 161–167.
[7] D.G. Glynn, A 126-cap of $PG(5, 4)$ and its corresponding [126, 6, 88]-code, Utilitas Math. 55 (1999) 201–210.
[8] M. Grassl. http://www.codetables.de.
[9] J.W.P. Hirschfeld, J.A. Thas, General Galois Geometries, Oxford Science Publications, Clarendon Press, Oxford, 1991.
[10] F.J. MacWilliams, N.J.A. Sloane, The Theory of Error-Correcting Codes, North-Holland, Amsterdam, 1977.
[11] L. Storme, Finite geometry, in: C.J. Colbourn, J.H. Dinitz (Eds.), Handbook of Combinatorial Designs, second ed., Chapman & Hall/CRC, Boca Raton, 2007, pp. 702–729.
[12] J.A. Thas, Projective geometry over a finite field, in: F. Buekenhout (Ed.), Handbook of Incidence Geometry, North-Holland, Amsterdam, 1995, pp. 295–347.