数理解析研究所講究録
第 1656 巻 2009 年 44-54

Quantum Codes from Finite Geometry and Combinatorial Designs

Vladimir D. Tonchev*
Department of Mathematical Sciences
Michigan Technological University
Houghton, Michigan 49931, USA, tonchev@mtu.edu

March 16, 2009

Abstract

Some recent constructions [22], [23] of optimal quantum codes based on finite projective geometry configurations of points, known as caps, and combinatorial structures such as Bhaskar-Rao designs, generalized balanced weighing matrices and generalized Hadamard matrices are discussed.

Keywords: quantum code, self-orthogonal code, cap, projective geometry, Bhaskar-Rao design, generalized balanced weighing matrix, generalized Hadamard matrix.

1 Introduction

We assume familiarity with the basics of classical error-correcting codes [19] and quantum codes [5]. 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

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

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

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

*Research supported by NSA Grant H98230-06-1-0027.

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) [5].

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 [5]. 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 [5], 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 [5].

Theorem 1.1 *[5] 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 [5].

Theorem 1.2 *[5] 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 [5]. An extended version of this table was compiled by Grassl [12]. An electronic server for bounds on the minimum distance of various codes is available on Andries Brouwer's web page [4].

2 Caps

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 [15]). 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 [20].

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 (11)) 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 1.1. 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 $n \leq q^2 + 1$ ([21], p. 309). A (q^2+1)-cap in $PG(3,q)$, $q \neq 2$, is called an *ovoid*. In [5], 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 $PG(4,4)$, as well as 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 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 $d = 4$ [5].

3 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 [7]). 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, 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.

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

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

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

Thus, C defines a quantum $[[41,31,4]]$ code via Theorem 1.1. 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 3.1. Since the all-one vector belongs to $B^{\perp}$, we have $B_i^{\perp} = B_{41-i}^{\perp}$ for $0 \leq i \leq 20$.

Table 3.1 *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

The parameters of quantum codes obtained from the $[[41,31,4]]$ code via Theorem 1.2 by using vectors of weight m $(0 \leq m \leq 31)$ in $B^{\perp}$ are listed in Table 3.2.

Table 3.2 *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]]

Note 3.3 All codes in Table 3.2 are optimal, that is, $d = 4$ is the largest possible for the given n and k (see [5] for lengths $n \leq 30$ and [12] for lengths 31, 33, 35 and 41). Note that the lower bound on d given in [5] for $n = 29$ and $k = 19$ is $d = 3$.

4 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 [11]). Glynn [11] 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 (11), 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 [12], 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).

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

Consequently, there exist pure quantum $[[126-m, 114-m, 4]]$ codes for all values of $m \leq 114$ from the list (7) obtained via the shortening construction of Theorem 1.2. Most of these codes are optimal according to [5] and [12]: the codes of length $28 \leq n \leq 126$ obtained for values of m in the range $0 \leq m \leq 98$ are all optimal; the codes with $20 \leq n \leq 27$ 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 $n = 12$ [5].

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 [8], for examle, $[[43, 31, 4]]$, $[[63, 51, 4]]$, $[[73, 61, 4]]$, $[[85, 73, 4]]$, $[[105, 93, 4]]$, $[[112, 100, 4]]$,
$[[116, 104, 4]]$, $[[118, 106, 4]]$.

5 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 $d = 4$ [5].

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 [9] 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 5.1. 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 1.1. To the best of our knowledge, a code with these parameters was not known before.

Table 5.1 *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

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

6 Generalized weighing matrices

A *generalized weighing matrix* over a multiplicative group G of order g is a $v \times b$ matrix $M = (m_{ij})$ with entries from $G \cup \{0\}$ such that for every two rows $(m_{i1}, \dots, m_{ib}), (m_{j1}, \dots, m_{jb})$, $i \neq j$, the multi-set

$$\{m_{is}m_{js}^{-1} \mid 1 \leq s \leq b,\ m_{js} \neq 0\} \tag{11}$$

contains every element of G the same number of times.

A generalized weighing matrix with the additional properties that every row contains precisely r nonzero entries, each column contains exactly k nonzero entries, and for every two distinct rows the multi-set (11) contains every group element exactly λ/g times is known as a *generalized Bhaskar Rao design* $GBRD(v, b, r, k, \lambda; G)$ [18].

Replacing the nonzero entries of a $GBRD(v, b, r, k, \lambda; G)$ by 1 produces the incidence matrix of a 2-(v, k, λ) design with b blocks of size k and r blocks containing any point. A generalized Bhaskar Rao design with $r = k$ and $v = b$ is also known as a *balanced generalized weighing matrix* $BGW(v, k, \lambda)$ [16], [18]. In this case, the underlying design is a symmetric 2-(v, k, λ) design. A *generalized Hadamard matrix* $GH(\lambda, g)$ over a group G of order g is a balanced generalized weighing matrix with $v = b = k = \lambda$ ([3], [6] IV.11). The process of replacing the 1's in the incidence matrix of a symmetric 2-(v, k, λ) design D with elements from a group G of order g (where g is a divisor of λ) in order to obtain a balanced generalized weighing matrix (called "signing" of D over G) has been studied by Gibbons and Mathon in [10], where a complete enumeration of signings of symmetric designs on $v \leq 19$ points is given.

Lemma 6.1 *Let $q = p^s \geq 4$ be a power of a prime number p, and let M be a $v \times b$ generalized weighing matrix over the multiplicative group of $GF(q)$ such that the Hamming weight of every row of M is a multiple of p. Then the rows of M span a linear code C of length b which is self-orthogonal with respect to the hermitian product (3).*

Proof. Note that $a^{q-2} = a^{-1}$ for every nonzero $a \in GF(q)$. The hermitian product (x, x) of a vector x by itself is equal to the Hamming weight of x reduced modulo p. Thus, every row of M is self-orthogonal with respect to the hermitian product.

It follows by the definition of a generalized weighing matrix that the hermitian product of two distinct rows $m_i = (m_{i1}, \ldots, m_{ib})$, $m_j = (m_{j1}, \ldots, m_{jb})$, $i \neq j$, of M is a multiple of the sum of all nonzero elements of $GF(q)$, i.e.

$$(m_i, m_j) = s(1 + \alpha + \alpha^2 + \ldots + \alpha^{q-2}),$$

where s is the number of occurrences of each nonzero element of $GF(q)$ in the multi-set of differences (11), and α is a primitive element of $GF(q)$. Since $1 + \alpha + \alpha^2 + \ldots + \alpha^{q-2} = (\alpha^{q-1} - 1)/(q-1) = 0$, it follows that every two rows of M are orthogonal to each other, and consequently, the linear code spanned by the rows of M is hermitian self-orthogonal. □

Lemma 6.2 *Let q be a prime power and let M be a $GBRD(v, b, r, k, \lambda; GF(q) \setminus \{0\})$ over the multiplicative group of $GF(q)$ such that $v > k$ and $b < 2v$. The dual code $C^{\perp}$ of the code C spanned by the rows of M has minimum distance $d^{\perp} \geq 3$.*

Proof. Since $v > k$ and $b < 2v$, it follows from the inequality of Mann (cf., e.g. [25], Theorem 1.1.15) that all columns of the incidence matrix of the underlying 2-(v, k, λ) design are distinct. Consequently, for every pair of columns of M there is a row that contains a zero entry in one of the columns and a nonzero entry in the other column. Thus, every two columns of M are linearly independent. □

7 Codes from generalized weighing and Hadamard matrices

Balanced generalized weighing matrices $BGW((q^t - 1)/(q - 1), q^{t-1}, q^{t-1} - q^{t-2})$ over the multiplicative group of $GF(q)$ are known to exist for every prime power q and every integer $t \geq 2$ [2], [18]. Some constructions using traces of elements in $GF(q)$ that give many monomially inequivalent $BGW((q^t - 1)/(q - 1), q^{t-1}, q^{t-1} - q^{t-2})$ for various q and t are given in [17]. The rank of a $BGW((q^t - 1)/(q - 1), q^{t-1}, q^{t-1} - q^{t-2})$ over $GF(q)$ is greater than or equal to t, and up to monomial equivalence, there exists a unique matrix $BGW((q^t - 1)/(q - 1), q^{t-1}, q^{t-1} - q^{t-2})$ of minimum q-rank t [16].

By Lemmas 6.1 and 6.2, we have the following.

Theorem 7.1 *Let $q \geq 4$ be a prime power and $t \geq 2$ be an integer. The code C spanned by the rows of a $BGW((q^t-1)/(q-1), q^{t-1}, q^{t-1}-q^{t-2})$ over $GF(q)$ is a hermitian self-orthogonal code of length $n = (q^t-1)/(q-1)$, dimension $k \geq t$, and dual distance $d^\perp \geq 3$.*

Note 7.2 In the special case when C has dimension t, the dual code $C^\perp$ is equivalent to the q-ary Hamming code [16].

Let q be a prime power. A generalized Hadamard $q^t \times q^t$ matrix $GH(q^{t-1}, q)$ over the elementary abelian group E_q of order q is known to exist for every $t \geq 1$ (cf., e.g. [14], [24]). The group E_q is isomorphic to the additive group of $GF(q)$, hence a $GH(q^{t-1}, q)$ over E_q can be viewed as a matrix with entries from $GF(q)$. We refer to the resulting matrix as an *additive* Hadamard matrix. For an additive Hadamard matrix $GH(q^{t-1}, q)$, over $GF(q)$ the condition about the quotients (11) is replaced by the condition that for every pair of rows i, j $(i \neq j)$ the multi-set of differences

$$\{m_{is} - m_{js} \mid 1 \leq s \leq q^t\} \tag{12}$$

contains every element of $GF(q)$ exactly q^{t-1} times.

The rows of an additive generalized Hadamard matrix $GH(q^{t-1}, q)$ over $GF(q)$ may or may not be pairwise orthogonal with respect to the hermitian product (3). For example, only 150 of the 226 generalized Hadamard matrices $GH(4,4)$ found in [13] span hermitian self-orthogonal codes.

The rank of a $q^t \times q^t$ matrix $GH(q^{t-1}, q)$ over $GF(q)$ is at least t. For any given prime power q and any $t \geq 1$, there exists a unique (up to a permutation of rows and columns) matrix $M = GH(q^{t-1}, q)$ of minimum q-rank equal to t [24]. Algebraically, such a matrix M is the vector space spanned by the rows of a $t \times q^t$ matrix $B(t, q)$ whose set of columns consists of all distinct vectors with t components over $GF(q)$. Thus, M contains one all-zero row, and by the condition for the differences (12), every other row of M contains every nonzero element of $GF(q)$ exactly q^{t-1} times. Thus, every row of M except the zero row has Hamming weight $q^{t-1}(q-1) \equiv 0 \pmod{q}$. In addition, every two rows of M are orthogonal with respect to the hermitian product (3). This can be verified by induction using the recursive structure of $B(t, q)$, namely, up to a permutation of columns

$$B(t,q) = \begin{pmatrix} 0\ldots0 & 1\ldots1 & \ldots & \alpha^{q-2}\ldots\alpha^{q-2} \\ B(t-1,q) & B(t-1,q) & \ldots & B(t-1,q) \end{pmatrix},$$

where α is a primitive element of $GF(q)$. Note that the hermitian product of the two rows of $B(2, q)$ is equal to $(1 + \alpha + \ldots + \alpha^{q-2})^2 = 0$. Thus, we have the following.

Theorem 7.3 *The rows of an additive generalized Hadamard matrix $M = GH(q^{t-1}, q)$ over $GF(q)$ of q-rank equal to t form a linear hermitian self-orthogonal code. Removing the all-zero column of M gives a hermitian self-orthogonal code with parameters $n = q^t - 1$, $k = t$, and dual distance $d^\perp = 2$.*

8 An application to quantum codes

Applying this result of Theorem 1.1 to the codes of Theorem 7.1 and Theorem 7.3 in the special case $q = 4$ gives the following.

Theorem 8.1 *Let $t \geq 2$ be an integer. The code C over $GF(4)$ spanned by the rows of a matrix $M = BGW((4^t - 1)/3, 4^{t-1}, 4^{t-1} - 4^{t-2})$ yields a quantum code with parameters $[[(4^t - 1)/3, (4^t - 1)/3 - 2k, d \geq 3]]$, where k is the rank of M over $GF(4)$.*

Theorem 8.2 *The row space of an additive generalized Hadamard matrix $M = GH(4^{t-1}, 4)$ of 4-rank t yields a quantum code with parameters $[[4^t - 1, 4^t - 1 - 2t, 2]]$.*

Note 8.3 The codes of Theorem 8.1 in the case when the matrix is of minimum rank, that is, $k = t$, have $d = 3$ and meet the sphere-packing bound for quantum $[[n, k, d = 2e + 1]]$ codes:

$$\sum_{j=0}^{e} 3^j \binom{n}{j} \leq 2^{n-k}. \tag{13}$$

According to this bound, a quantum code with parameters $n = 4^t - 1$ and $k = 4^t - 1 - 2t$ cannot have $d \geq 3$. Thus $d = 2$ is the best possible value for the given n and k, hence the codes of Theorem 8.2 are also optimal. Note that the $[[15, 11, 2]]$ obtained from Theorem 8.2 when $t = 2$ is one of the optimal quantum codes found in [13].

9 Acknowledgment

The author wishes to thank RIMS and Professor Hiromichi Yamada for the hospitality and support.

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] G. Berman, Families of generalized weighing matrices, *Canadian J. Math.* **30** (1978), 1016-1028.

[3] T. Beth, D. Jungnickel, H. Lenz, "Design Theory", Second Edition, Cambridge University Press, Cambridge, 1999.

[4] A.E. Brouwer, http://www.win.tue.nl/~aeb/.

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

[6] C. J. Colbourn and J. H. Dinitz, eds., "The CRC Handbook of Combinatorial Designs", CRC Press, Boca Raton, 1996.

[7] Y. Edel, 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, J. Bierbrauer, Quantum Twisted Codes, *J. Combin. Designs* **8** (2000), 174-188.

[9] M. van Eupen and 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.

[10] P. B. Gibbons and R. A. Mathon, Group signings of symmetric balanced incomplete block designs, *Ars Combinatoria* **23A** (1987), 123-134.

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

[12] M. Grassl, http://www.codetables.de

[13] M. Harada, C. Lam, and V.D. Tonchev, Symmetric $(4,4)$-nets and generalized Hadamard matrices over groups of order 4, *Designs, Codes and Cryptography* **34** (2005), 71-87.

[14] A.S. Hedayat, N.J.A. Sloane, J. Stufken, *Orthogonal Arrays*, Springer, New York 1999.

[15] J.W.P. Hirschfeld and J.A. Thas, *General Galois Geometries*, Oxford Science Publications, Clarendon Press, Oxford, 1991.

[16] D. Jungnickel and V.D. Tonchev, Perfect codes and balanced generalized weighing matrices, *Finite Fields and their Appl.* **5** (1999), 294-300.

[17] D. Jungnickel and V.D. Tonchev, Perfect codes and balanced generalized weighing matrices, II, *Finite Fields and their Appl.* **8** (2002), 155-165.

[18] W. de Launey, Bhaskar Rao Designs, in: "The CRC Handbook of Combinatorial Designs", C. J. Colbourn and J. H. Dinitz, eds., CRC Press, Boca Raton, 1996, pp. 241-246.

[19] F.J. MacWilliams and N.J.A. Sloane, *The Theory of Error-Correcting Codes*, North-Holland, Amsterdam 1977. O

[20] L. Storme, Finite Geometry, in: *Handbook of Combinatorial Designs*, Second Ed., edited by C.J. Colbourn and J.H. Dinitz, Chapman & Hall/CRC, Boca Raton, 2007, pp. 702-729.

[21] J.A. Thas, Projective Geometry over a Finite Field, in: *Handbook of Incidence Geometry*, edited by F. Buekenhout, North-Holland, Amsterdam 1995, pp. 295-347.

[22] V.D. Tonchev, Generalized weighing matrices and self-orthogonal codes, *Discrete Math.*, to appear.

[23] V.D. Tonchev, Quantum codes from caps, *Discrete Math.*, **308**, (2008), 6368-6372.

[24] V. D. Tonchev, On generalized Hadamard matrices of minimum rank, *Finite Fields and their Appl.* **10** (2004), 522-529.

[25] V.D. Tonchev, *Combinatorial Configurations*, Wiley, New York 1988.