Maximal arcs, codes, and new links between projective planes of order 16

Mustafa Gezek

Department of Mathematics Tekirdag Namik Kemal University Tekirdag 59030, Turkey

mgezek@nku.edu.tr

Rudi Mathon

Department of Computer Science University of Toronto Toronto, Ontario M5S3G4, Canada

rmathon@gmail.com

Vladimir D. Tonchev

Department of Mathematical Sciences Michigan Technological University Houghton, MI 49931, U.S.A.

tonchev@mtu.edu

Submitted: Sep 12, 2019; Accepted: Mar 6, 2020; Published: Mar 20, 2020 © The authors. Released under the CC BY-ND license (International 4.0).

Abstract

In this paper we consider binary linear codes spanned by incidence matrices of Steiner 2-designs associated with maximal arcs in projective planes of even order, and their dual codes. Upper and lower bounds on the 2-rank of the incidence matrices are derived. A lower bound on the minimum distance of the dual codes is proved, and it is shown that the bound is achieved if and only if the related maximal arc contains a hyperoval of the plane. The binary linear codes of length 52 spanned by the incidence matrices of 2-(52,4,1) designs associated with previously known and some newly found maximal arcs of degree 4 in projective planes of order 16 are analyzed and classified up to equivalence. The classification shows that some designs associated with maximal arcs in nonisomorphic planes generate equivalent codes. This phenomenon establishes new links between several of the known planes. A conjecture concerning the codes of maximal arcs in $PG(2, 2^m)$ is formulated.

Mathematics Subject Classifications: 05B05,51E20,94B05

1 Introduction

We assume familiarity with the basic facts and notions from design theory, finite geometries, and coding theory [3, 5, 10, 13, 23].

A 2- (v, k, λ) design (or shortly, a 2-design) is a pair $D=\{X, B\}$ of a set X of v points and a collection B of subsets of X of size k called blocks, such that every two points appear together in exactly λ blocks. Every point of a 2- (v, k, λ) design is contained in $r = \lambda(v-1)/(k-1)$ blocks, and the total number of blocks is $b = v(v-1)\lambda/k(k-1)$.

The incidence matrix of a design D is a (0,1)-matrix $A=(a_{ij})$ with rows labeled by the blocks, columns labeled by the points, where $a_{i,j}=1$ if the ith block contains the jth point, and $a_{i,j}=0$ otherwise. If p is a prime, the p-rank of a design D is the rank of its incidence matrix over a finite field of characteristic p. Two designs are isomorphic if there is a bijection between their point sets that maps every block of the first design to a block of the second design. An automorphism of a design is any isomorphism of the design to itself. The set of all automorphisms of D form the automorphism group Aut(D) of D. The dual design D^{\perp} of a design D has as points the blocks of D, and as blocks the points of D. A 2- (v, k, λ) design is symmetric if b = v, or equivalently, r = k. The dual design D^{\perp} of a symmetric 2- (v, k, λ) design D is a symmetric design with the same parameters as D. A symmetric design D is self-dual if D and D^{\perp} are isomorphic.

A design with $\lambda = 1$ is called a *Steiner* design. An affine plane of order n $(n \ge 2)$, is a Steiner 2- $(n^2, n, 1)$ design. A projective plane of order n is a symmetric Steiner 2- $(n^2 + n + 1, n + 1, 1)$ design with $n \ge 2$. The classical (or Desarguesian) plane $PG(2, p^t)$ of order $n = p^t$, where p is prime and $t \ge 1$, has as points the 1-dimensional subspaces of the 3-dimensional vector space V_3 over the finite field of order p^t , and as blocks (or *lines*), the 2-subspaces of V_3 .

Let $D = \{X, B\}$ be a Steiner 2-(v, k, 1) design with point set X, collection of blocks B, and let v be a multiple of k, v = nk. Since every point of X is contained in r = (v-1)/(k-1) = (nk-1)/(k-1) blocks, k-1 divides n-1. Thus, n-1 = s(k-1) for some integer $s \ge 1$, and

$$v = nk = (sk - s + 1)k.$$

A parallel class of D is a set of v/k = n pairwise disjoint blocks, and a resolution of D is a partition of the collection of blocks B into r = (v-1)/(k-1) = sk+1 disjoint parallel classes. A design is resolvable if it admits a resolution.

Any 2-((sk - s + 1)k, k, 1) design with s = 1 is an affine plane of order k, and admits exactly one resolution. If s > 1, a resolvable 2-((sk - s + 1)k, k, 1) design may admit more than one resolution.

Let P be a projective plane of order q, and let m and k be positive integers such that $k \leq q+1$ and $k \leq m \leq q^2+q+1$. An (m,k)-arc (or an arc of size m and degree k) is a set A of m points such that every line of P contains at most k points from A. An arc of degree 2 is also called an *oval*. Let x be a point in an (m,k)-arc A, let L_1, \ldots, L_{q+1} be the lines through x, and let $n_i = |A \cap L_i|$, $1 \leq i \leq q+1$. Then

$$m = 1 + \sum_{i=1}^{q+1} (n_i - 1).$$

Since $n_i \leq k$, it follows that

$$m \leqslant qk + k - q$$
,

and the equality m = qk + k - q holds if and only if every line of P is either disjoint from A or meets A in exactly k points. An (m, k)-arc is called maximal if m = qk + k - q. A hyperoval is a maximal arc of degree 2.

Let A be a maximal (qk + k - q, k)-arc with $k \leq q$, thus $m = qk + k - q \leq q^2$, and let y be a point outside A. Let n be the number of lines that meet A in k points. We have

$$nk = qk + k - q.$$

Thus, k divides q, and q = sk for some integer $s \ge 1$ ¹. If q = sk, the size qk + k - q of a maximal arc of degree k can be written in terms of s and k as (sk - s + 1)k.

The set of lines that are disjoint from a maximal ((sk-s+1)k,k)-arc A in a projective plane P of order q=sk, form a maximal ((sk-k+1)s,s)-arc A^{\perp} in the dual plane P^{\perp} , called the dual arc of A.

Maximal arcs with 1 < k < q do not exist in any Desarguesian plane of odd order q [2], and are known to exist in every Desarguesian plane of order $q = 2^t$ [11, 20, 21, 28, 34], as well as in some non-Desarguesian planes of even order $q = 2^t$ [14, 15, 17, 18, 19, 22, 32, 35].

If k > 1, the non-empty intersections of a maximal ((sk - s + 1)k, k)-arc A with lines of a projective plane P of order q = sk are the blocks of a resolvable 2-((sk - s + 1)k, k, 1) design D. Similarly, if s > 1, the dual ((sk - k + 1)s, s)-arc A^{\perp} in the dual plane P^{\perp} is the point set of a resolvable 2-((sk - k + 1)s, s, 1) design D^{\perp} . We will refer to D (resp. D^{\perp}) as a design embeddable in P (resp. P^{\perp}) as a maximal arc.

Two maximal arcs A', A'' in a projective plane P are equivalent if there is a collineation of P that maps A' to A''. Designs associated with equivalent arcs are necessarily isomorphic, while the converse is not true in general.

Let D be a resolvable Steiner 2-(v, k, 1) design. Two resolutions R_1, R_2 of D, where

$$R_1 = P_1^{(1)} \cup P_2^{(1)} \cup \cdots P_r^{(1)}, \ R_2 = P_1^{(2)} \cup P_2^{(2)} \cup \cdots P_r^{(2)},$$
 (1)

are called compatible [36], if they share one parallel class, $P_i^{(1)} = P_i^{(2)}$, and

$$|P_{i'}^{(1)} \cap P_{i'}^{(2)}| \leqslant 1$$

for $(i', j') \neq (i, j)$.

The following theorem gives an upper bound on the number of pairwise compatible resolutions of a resolvable 2-((sk - s + 1)k, k, 1) design, and characterizes the designs for which this upper bound is achieved.

Theorem 1. [36]. Let $S = \{R_1, \ldots, R_m\}$ be a set of m mutually compatible resolutions of a 2-((sk - s + 1)k, k, 1) design $D = \{X, B\}$. Then

$$m \leqslant (sk - k + 1)s$$
.

The equality

$$m = (sk - k + 1)s$$

holds if and only if there exists a projective plane P of order q = sk such that D is embeddable in P as a maximal ((sk - s + 1)k, k)-arc.

 $^{^{1}}$ In all known examples, q is a power of 2.

In Section 2, we consider binary linear codes spanned by the rows of incidence matrices of Steiner 2-designs associated with maximal arcs in projective planes of even order, and their dual codes. Upper and lower bounds on the 2-rank of the incidence matrices are derived. A lower bound on the minimum distance of the dual codes is proved, and it is shown that the bound is achieved if and only if the related maximal arc contains a hyperoval of the plane.

In Section 3, we analyze the binary linear codes of length 52 spanned by the incidence matrices of 2-(52, 4, 1) designs associated with maximal arcs of degree 4 in projective planes of order 16. The codes associated with maximal arcs in PG(2, 16) are distance optimal, while one code associated with an arc in the semi-field plane is shown to be optimal with respect to each of its parameters: minimum distance, dimension, and length. A conjecture concerning the codes of maximal arcs in $PG(2, 2^m)$ is formulated.

The codes are classified according to their dimension, and all codes having the same dimension are further classified up to equivalence. The classification shows that some designs associated with maximal arcs in nonisomorphic planes generate equivalent codes. This phenomenon establishes new links between several of the known planes that are discussed in Section 4.

Section 5 lists explicitly eleven new maximal arcs of degree 4 found recently in the planes DEMP, SEMI2, LMRH, HALL, and BBH1.

2 Binary codes of designs arising from maximal arcs

An *oval* of a Steiner 2-(v, k, 1) design D with $k \ge 2$ is a set S that meets every block in at most two points.

Lemma 2. (a) The size of an oval S of a Steiner 2-(v, k, 1) design is bounded above by

$$|S| \leqslant r + 1$$
,

where r = (v-1)/(k-1) is the number of blocks through a point.

(b) The equality |S| = r + 1 holds if and only if every block is either disjoint from S, or meets S in exactly two points.

Proof. Let n_i (i = 0, 1, 2) denote the number of blocks meeting S in i points. Counting in two ways the incident pairs of points from S and blocks, and incidence pairs of pairs of points from S and blocks, we have

$$n_1 + 2n_2 = |S|r,$$

 $2n_2 = |S|(|S| - 1),$

hence

$$n_1 = |S|r - |S|(|S| - 1) \ge 0,$$

and the statement follows.

An oval of size r + 1 is called a hyperoval.

Note 3. If D is a symmetric Steiner design, that is, a projective plane, a hyperoval is simply a maximal arc of degree two.

Theorem 4. Let C be a binary linear code of length $n = 2^{m+s} - 2^m + 2^s$, spanned by the rows of the incidence matrix A of a Steiner 2- $(2^{m+s} - 2^m + 2^s, 2^s, 1)$ design D with $m \ge s \ge 1$.

- (i) The all-one vector $\bar{1} = (1, ..., 1)$ belongs to $C \cap C^{\perp}$.
- (ii) The dual code C^{\perp} admits majority-logic decoding that corrects up to $t=2^{m-1}$ errors.
- (iii) The minimum distance d^{\perp} of C^{\perp} is an even number equal to $2^m + 2$ if D contains hyperovals, and $d^{\perp} \geqslant 2^m + 4$ if D has no hyperovals.
- (iv) The minimum distance d of C is an even number smaller than or equal to 2^s .
- (v) The dimension k of C, or equivalently, the 2-rank of A, rank₂A, satisfies the inequalities

$$1 + \lceil \log_2(\sum_{i=0}^t \binom{n-1}{i}) \rceil \leqslant rank_2 A \leqslant n - 1 - \lfloor \log_2(\sum_{i=0}^{d/2-1} \binom{n-1}{i}) \rfloor,$$

where $t = 2^{m-1}$ if $d^{\perp} = 2^m + 2$, and $t = d^{\perp}/2 - 1$ if $d^{\perp} \ge 2^m + 4$.

Proof. (i) Since all rows of A are of even weight 2^s , every row is orthogonal to $\bar{1}$ over GF(2), hence $\bar{1} \in C^{\perp}$. Every point of D is contained in $r = 2^m + 1$ blocks. Thus, every column of A contains $2^m + 1$ nonzero entries, and the binary sum of all rows of A is equal to $\bar{1}$, hence $\bar{1} \in C$.

(ii) The rows of A provide a set of checks that can be used to correct up to

$$t = \lfloor \frac{r}{2} \rfloor = \lfloor \frac{2^m + 1}{2} \rfloor = 2^{m-1}$$

errors in C^{\perp} by using the Rudolph majority-logic decoding algorithm (cf. [33], [37, Theorem 8.1, page 1252]).

(iii) It follows from (ii) that $d^{\perp} \ge 2t + 1 = 2^m + 1$. Assume that $d^{\perp} = 2^m + 2$, and let S be the support of a minimum weight codeword in C^{\perp} . Clearly, S meets every block of D in an even number of points. Let n_{2i} denote the number of blocks that meet S in 2i points, $0 \le i \le 2^{s-1}$. Counting in two ways the occurrences of single points, and ordered pairs of points of S in blocks of D, we have

$$\sum_{i=1}^{2^{s-1}} 2in_{2i} = (2^m + 2)(2^m + 1),$$

$$\sum_{i=1}^{2^{s-1}} 2i(2i-1)n_{2i} = (2^m+2)(2^m+1).$$

Subtracting the first of the above equations from the second gives

$$\sum_{i=2}^{2^{s-1}} 4i(i-1)n_{2i} = 0,$$

hence $n_{2i}=0$ for i>1, and S is a hyperoval of D. Consequently, by Lemma 2, the number of codewords of C^{\perp} having weight 2^m+2 is equal to the number of hyperovals of D. If D has no hyperovals, then $d^{\perp}>2^m+2$, and since all weights in C^{\perp} are even by part (i), it follows that $d^{\perp} \geq 2^m+4$.

Part (iv) is obvious. The upper bound in Part (v) follows from applying the sphere packing bound (cf., e.g. [24, 1.12]), to a punctured [n-1, k, d-1] code C' of C. The lower bound in Part (v) follows from applying the sphere packing bound to a punctured $[n-1, n-k, d^{\perp}-1]$ code of C^{\perp} .

Note 5. According to Theorem 4 (ii) and (iii), if D contains hyperovals then the dual code C^{\perp} can correct the maximum number of errors guaranteed by its minimum distance, by using majority-logic decoding, and in addition, the number of codewords in C^{\perp} having minimum weight is equal to the number of hyperovals of D.

As a corollary of Theorem 4, we have the following.

Theorem 6. Let C be a binary code of length $n=2^{m+s}-2^m+2^s$, spanned by the incidence matrix A of a Steiner 2- $(2^{m+s}-2^m+2^s,2^s,1)$ design D with $m \ge s \ge 1$, associated with a maximal arc S of degree 2^s in a projective plane Π of even order $q=2^m$. Let d and d^{\perp} denote the minimum distance of C and C^{\perp} respectively.

- (a) The minimum distance d^{\perp} of C^{\perp} is $d^{\perp}=2^m+2$ if D contains a hyperoval of Π , and $d^{\perp}\geqslant 2^m+4$ otherwise.
- (b) The minimum distance d of C is an even number smaller than or equal to 2^s . If $d = 2^s$ then

$$1 + \lceil \log_2(\sum_{i=0}^t \binom{n-1}{i}) \rceil \leqslant rank_2 A \leqslant n - 1 - \lfloor \log_2(\sum_{i=0}^{2^{s-1}-1} \binom{n-1}{i}) \rfloor,$$

where $t = 2^{m-1}$ if D contains a hyperoval of Π , and $t = d^{\perp}/2 - 1 \geqslant 2^{m-1} + 1$ if D does not contain any hyperoval of Π .

Proof. Since every hyperoval of D is also a hyperoval of Π , (a) and (b) follow from part (iii) and (v) of Theorem 4 respectively.

Note 7. If s=1, the design D from Theorems 4 and 6 is the trivial design on 2^m+2 points having as blocks all pairs of points. In this case, $rank_2A=2^m+1$, and the code C is the unique binary code consisting of all vectors of even weight, while $C^{\perp}=C\cap C^{\perp}=\{\mathbf{0},\bar{1}\}$, where $\mathbf{0}$ denotes the zero vector.

Apart from this trivial case, the question about the 2-rank of designs arising from maximal arcs is widely open, with one notable exception concerning the case s = m - 1: it was proved by Carpenter [9] that the 2-rank of a $2-(2^{2m-1}-2^{m-1},2^{m-1},1)$ design associated with the dual arc of a regular hyperoval in $PG(2,2^m)$ is equal to $3^m - 2^m$.

3 Binary codes associated with maximal arcs of degree 4

A Steiner design D associated with a maximal arc of degree 4 in a projective plane of order 2^m has parameters $2 \cdot (3 \cdot 2^m + 4, 4, 1)$, and its binary code C is of length $n = 3 \cdot 2^m + 4$ and has minimum distance d = 2 or d = 4. In this section, we consider $2 \cdot (3 \cdot 2^m + 4, 4, 1)$ designs and their binary codes when m = 2, 3 and 4.

If m=2, D is the unique (up to isomorphism) 2-(16, 4, 1) design, being isomorphic to the affine plane of order 4, and can be viewed as the design associated with a maximal arc of degree 4 in the projective plane of order 4. The 2-rank of its incidence matrix A is 9, hence the code C spanned by A has dimension 9. The minimum distance of C is 4, and there are exactly 20 codewords of minimum weight 4, being the rows of the incidence matrix A. The design D contains ovals, hence $d^{\perp}=6$ by Theorem 4, (iii). The lower bound, and the upper bound on $rank_2A$ from Theorem 4, are 8 and 11 respectively. The code C is distance optimal in the sense that 4 is the largest possible minimum distance for a binary linear code of length 16 and dimension 9. The dual [16,7,6] code C^{\perp} is also distance optimal (see [16]).

In the next case, m=3, the design parameters are 2-(28,4,1). There are at least 4653 known nonisomorphic designs with these parameters [4, 26], having 2-ranks ranging from 19 to 26 [4], with the exception of 2-rank 20. It was shown in [25] that there are no 2-(28,4,1) designs with 2-rank 20. It was proved in [29] that the minimum 2-rank of any 2-(28,4,1) design is 19, and up to isomorphism, there is only one design of minimum 2-rank 19, being isomorphic to the design D associated with a maximal (28,4)-arc in the projective plane of order 8, PG(2,8) (also referred to as the Ree unital [7]). The minimum distance of the code C of the Ree unital D is 4, and every codeword of minimum weight corresponds to a block of D. The Ree unital contains ovals that are hyperovals in the projective plane of order 8, hence the minimum distance of the dual code C^{\perp} is $d^{\perp} = 10$, and C^{\perp} can correct up to $\lfloor (10-1)/2 \rfloor = 4$ errors by majority-logic decoding. The $\lfloor 28, 19, 4 \rfloor$ code C and its dual $\lfloor 28, 9, 10 \rfloor$ code C^{\perp} are both distance optimal (cf. $\lfloor 16 \rfloor$).

If m = 4, the parameters of the design D from Theorems 4 and 6 are 2-(52, 4, 1), and correspond to a design arising from a maximal (52, 4)-arc in a projective plane of order 16.

Up to isomorphism, there are 22 known projective planes of order 16. The only projective plane of order 16 for which all inequivalent maximal arcs of degree 4 have been completely classified, is the Desarguesian plane PG(2,16). There are exactly two inequivalent maximal (52,4)-arcs in PG(2,16) [1], with collineation groups of order 68 and 408. The maximal arc with group of order 408 admits a cyclic collineation of order 51 [12]. The maximal arcs of degree 4 have not been classified completely in any of the 21 known non-Desarguesian planes of order 16. Maximal arcs of degree 4 have been found in all but four of the known non-Desarguesian planes of order 16 [14, 15, 22]. All previously known maximal (52,4)-arcs can be found in [15] and [22]. Eleven new maximal arcs of degree 4 are given in Section 5 of this paper. The line sets of the projective planes of order 16 and all known maximal arcs of degree 4, including the new arcs described in Section 5, are available online at https://www.combinatorics.org/ojs/index.php/eljc/article/view/v27i1p62/8052 and https://www.combinatorics.org/ojs/index.php/eljc/article/

view/v27i1p62/8051 respectively.

Table 2 contains data about the 2-(52, 4, 1) designs associated with previously known and the eleven newly found maximal arcs of degree 4 described in Section 5. Column 3 lists the orders of the stabilizers of the maximal arcs, which happen to be also the full automorphism groups of the related designs. Column 4 gives the number of parallel classes of the design D associated with the given arc, followed by the number of parallel classes of the design D^{\perp} associated with the dual arc. Column 5 lists the number of resolutions of D and D^{\perp} . The last column lists the orders of the automorphism groups of the codes C(D) and $C(D^{\perp})$ respectively. Cliquer [31] and Magma [8] were used for these computations.

Since the number of parallel classes, resolutions, code dimension and minimum distance are invariant under isomorphism of designs, the data from Table 2 implies that the number of pairwise nonisomorphic resolvable 2-(52, 4, 1) designs associated with maximal arcs is greater than or equal to 55. Further computation of possible isomorphisms using Magma [8] shows that the number of nonisomorphic designs is exactly 55.

We note that the previously known lower bound on the number of nonisomorphic resolvable 2-(52, 4, 1) designs given in [10] is 30.

The 2-ranks of these 55 designs vary from 41 to 49, and the minimum 41 is achieved only by designs associated with maximal arcs in the Desarguesian plane PG(2, 16).

The codes of the 55 nonisomorphic 2-(52, 4, 1) designs arising from maximal (52, 4)-arcs were sorted according to their weight distributions, and codes having the same weight distribution were tested for equivalences using Magma. This classification shows that the 55 codes of the 55 nonisomorphic 2-(52, 4, 1) designs are partitioned into 27 equivalence classes. Table 3 lists the 2-ranks of the designs, and gives a partition of the codes into equivalence classes, the numbers A_2 and A_4 of codewords of weight 2 and 4 respectively, and the orders of the automorphism groups of the codes.

The main result implied by this classification of the codes up to equivalence is the surprising fact that in several instances the codes of designs arising from maximal arcs in different planes are equivalent, hence these codes provide new connections between the corresponding planes (see lines 4, 5, 6, 11, 13, 17, 18, 20, 24, 26 and 27 in Table 3). For example, the Mathon plane MATH is linked to the Johnson plane JOHN, the Lorimer-Rahilly plane LMRH, the semi-field plane SEMI2, and the Hall plane HALL.

Table 4 lists the parameters of the codes and their dual codes, as well as the number $A_{d^{\perp}}$ of codewords of minimum weight in C^{\perp} . We note that according to Theorem 6, in the cases when $d^{\perp} = 18$, $A_{d^{\perp}}$ is equal to the number of hyperovals of the plane contained in the point set of D.

Four of the 55 codes associated with these designs have minimum distance d=4: the codes C', C'' of the two maximal arcs in PG(2,16), and the codes C''' and C^{iv} of dimension 45 associated with the maximal arcs SEMI4.1 and SEMI2.7 (see Table 3 and Table 4). Every codeword of minimum weight in C' and C'' is the incidence vector of a block, while the number $A_4=4469$ of minimum weight codewords in C''' and C^{iv} is larger than the number of blocks. These observations suggest that the following statement may be true in general.

Conjecture 8. The binary code spanned by the incidence matrix A of a design D associated with a maximal arc of degree 4 in $PG(2, 2^m)$, where $m \ge 2$, has minimum distance 4, and every codeword of minimum weight is a row of A.

We note that the codes C''' and C^{iv} are equivalent (see Table 3 that lists the equivalence classes of codes), while the codes C', C'' of the two arcs in PG(2, 16) are inequivalent, despite the fact that both codes have identical weight distributions. It follows from [12] that one of these codes, namely the code with full automorphism group of order 408, is an extended cyclic code. Both (52,4)-arcs in PG(2,16) contain hyperovals, hence $d(C')^{\perp} = d(C'')^{\perp} = 18$ by Theorem 6. In addition, the number of codewords of minimum weight $A_{d^{\perp}}$ in each of the codes $(C')^{\perp}$ and $(C'')^{\perp}$ equals the number of hyperovals contained in the corresponding maximal arcs, namely $A_{d^{\perp}} = 54$ (see Table 4).

A comparison with the parameters of best known error-correcting codes [16] shows that the highest known minimum distance of a binary code of length 52 and dimension 41 is d = 4, while the best known theoretical upper bound is $d \leq 5$.

In comparison, the [52, 45, 4] code C''' of the arc SEMI4.1 is distance optimal. The dimension 45 of C''' is just by one shorter from the upper bound 46 obtained from Theorem 6. However, the minimum distance of any binary [52, 46] code is at most 3 (which is seen by applying the sphere packing bound on a punctured [51, 46, 3] code), therefore the [52, 45, 4] code C''' is both distance and dimension optimal. This implies that if the binary code of a 2-(52, 4, 1) design D has minimum distance 4, the 2-rank of D cannot exceed 45. In addition, since a binary [51, 45, 4] code does not exist, because the parameters of a punctured [50, 45, 3] code violate the sphere packing bound, the [52, 45, 4] code C''' is also length optimal, that is, 52 is the smallest possible length for a binary code of dimension 45 and minimum distance 4.

4 New connections between projective planes

Table 1 lists all previously known connections, as well as some new connections described in this section, between nonisomorphic projective planes of order 16. An entry in a row and a column labeled by the same (non self-dual) plane indicates a connection between the plane and its dual plane that is based on designs associated with maximal arcs or their codes.

An entry 1 indicates that the corresponding planes are connected by derivation [22, 30], 2 indicates that the corresponding planes are connected by super-derivation [27], and 3 indicates that the planes share a semi-biplane [30].

An entry 4 indicates that the planes share isomorphic 2-(52, 4, 1) designs associated with maximal (52, 4)-arcs via the construction based on Theorem 1. Connections of this type were established in [15].

An entry 5 indicates a new connection between a pair of nonisomorphic planes that share equivalent codes of non-isomorphic 2-(52, 4, 1) designs arising from maximal (52, 4)-arcs.

5 New maximal (52, 4)-arcs

The specific line sets of the known projective planes of order 16 that we are using in this paper were graciously provided to the third author by Gordon F. Royle, and are available online at https://www.combinatorics.org/ojs/index.php/eljc/article/view/v27i1p62/8052. All previously known maximal arcs of degree 4 are given in [15] and [22], and are available online at https://www.combinatorics.org/ojs/index.php/eljc/article/view/v27i1p62/8051.

Our notation in this section follows [15]. Recently, the first author found eight new maximal arcs in some of the projective planes of order 16. The new arcs are unions of orbits of appropriate subgroups of the automorphism group of the corresponding plane. Two new arcs, stabilized by a nonabelian group of order 12, were found in the plane DEMP. Five new arcs in the plane SEMI2, and one new arc in the plane LMRH, were found as unions of orbits under subgroups of order 16.

The point sets of these eight new maximal arcs are listed below.

 $\begin{aligned} \text{DEMP.3} &= \{263, 265, 266, 258, 32, 122, 142, 243, 187, 102, 61, 197, 84, 232, \\ 210, 156, 18, 126, 140, 251, 181, 112, 52, 195, 88, 237, 214, 154, 30, 117, 144, 244, \\ 178, 109, 54, 202, 83, 236, 219, 152, 24, 116, 139, 252, 189, 99, 62, 208, 82, 229, \\ 218, 150\}, \end{aligned}$

 $\begin{aligned} \text{DEMP.4} &= \{273, 260, 257, 258, 14, 69, 61, 27, 34, 128, 255, 232, 153, 97, 84, \\ 186, 7, 71, 60, 22, 39, 124, 246, 227, 147, 108, 86, 179, 8, 68, 63, 32, 45, 122, 242, \\ 225, 149, 110, 89, 187, 133, 194, 224, 175, 222, 161, 212, 138, 200, 141, 203, 169\}, \end{aligned}$

 $SEMI2.3 = \{263, 268, 265, 267, 23, 28, 228, 25, 27, 234, 240, 229, 4, 16, 124, 5, 123, 10, 121, 119, 49, 251, 76, 63, 56, 145, 252, 247, 75, 73, 50, 159, 152, 249, 71, 146, 36, 88, 202, 48, 37, 216, 82, 81, 197, 208, 42, 210, 209, 95, 196, 223\},$

$$\begin{split} \text{SEMI2.4} &= \{259, 269, 262, 270, 20, 233, 32, 21, 231, 236, 26, 235, 4, 16, 124, \\ 5, 123, 10, 121, 119, 33, 90, 208, 47, 40, 209, 85, 96, 196, 202, 34, 223, 216, 84, 197, \\ 210, 49, 251, 66, 63, 56, 155, 252, 247, 72, 79, 50, 156, 151, 249, 65, 153\}, \end{split}$$

$$\begin{split} \text{SEMI2.5} &= \{260, 272, 266, 261, 23, 27, 121, 25, 124, 28, 119, 123, 1, 2, 232, \\ 15, 239, 8, 225, 226, 66, 146, 69, 154, 72, 152, 74, 149, 49, 241, 58, 245, 63, 255, 53, \\ 250, 36, 96, 44, 219, 48, 89, 199, 84, 224, 43, 212, 220, 196, 87, 208, 201\}, \end{split}$$

 $SEMI2.6 = \{260, 268, 266, 263, 18, 136, 216, 26, 25, 153, 133, 135, 30, 213, 215, 131, 158, 146, 211, 154, 35, 79, 120, 39, 37, 112, 80, 76, 40, 117, 119, 70, 111, 102, 115, 108, 6, 175, 206, 12, 16, 57, 176, 172, 15, 201, 202, 166, 62, 50, 194, 58\},$

$$\begin{split} \text{SEMI2.7} &= \{261, 263, 271, 262, 25, 58, 250, 30, 32, 31, 128, 50, 60, 242, 252, \\ 54, 246, 127, 121, 126, 85, 110, 139, 88, 91, 93, 206, 105, 111, 141, 133, 112, 136, \\ 201, 207, 208, 5, 149, 70, 8, 11, 13, 226, 152, 155, 76, 66, 157, 74, 234, 230, 236\}, \end{split}$$

193, 171, 37, 70, 64, 195, 69, 147, 224, 38, 246, 208, 86, 51, 85, 211, 245, 160}.

A probabilistic search algorithm developed by the second author was used to find three new maximal arcs in the planes DEMP, HALL and BBH1. Each of these new arcs has a stabilizer of order 4, so it is computationally unfeasible to find these arcs with the previous method that works well for stabilizers of order at least 12.

A randomized local search was performed to find sets in projective planes with prescribed line intersections. At the start of a new experiment, a set of points is selected at random. At each move, a neighborhood of the current subset, defined by a single interchange between a point in the set and a point outside, is examined in order to generate a list of swaps that minimize an objective function formed from the actual and desired line intersections, respectively. A locally optimal move is then randomly selected from that list and the set updated to reflect it. A tabu list of the most recent moves is maintained to prevent cycling, and occasional random moves are performed to improve the search efficiency. This search algorithm worked well for projective planes of order 16 and reproduced all the known (52,4)-arcs with frequencies inversely proportional to their group orders. We have run typically 10^4 experiments with 5×10^4 moves per experiment on a MacBook Pro. The same approach was used to verify the existence of 4-arcs PG(2,32) in [28].

The point sets of these three new maximal arcs are:

 $\begin{aligned} \text{DEMP.5} &= \{1, 3, 8, 15, 23, 24, 25, 28, 36, 38, 41, 43, 51, 54, 61, 64, 66, 69, 70, \\ 78, 81, 82, 89, 96, 100, 104, 106, 109, 129, 133, 139, 140, 149, 154, 156, 160, 178, \\ 183, 189, 190, 195, 202, 206, 207, 228, 231, 235, 239, 257, 260, 271, 272\}, \end{aligned}$

 $HALL.2 = \{1, 2, 5, 14, 19, 27, 28, 32, 34, 39, 40, 45, 49, 53, 54, 63, 81, 84, 88, 95, 103, 107, 108, 109, 131, 134, 142, 143, 147, 153, 154, 155, 166, 169, 170, 173, 180, 183, 184, 185, 197, 202, 204, 208, 210, 212, 222, 224, 257, 260, 262, 266\},$

 $BBH1.3 = \{11, 13, 14, 16, 18, 27, 30, 31, 34, 38, 39, 42, 55, 56, 59, 63, 65, 69, 70, 79, 81, 85, 89, 91, 130, 135, 137, 144, 146, 153, 156, 159, 161, 167, 170, 173, 181, 190, 191, 192, 197, 205, 207, 208, 241, 245, 246, 254, 262, 263, 266, 269\}.$

	PG(2,16)	DEMP	SEMI4	SEMI2	LMRH	MATH	HALL	BBH1	JOWK	JOHN	DSFP	BBH2	BBS4
PG(2,16)							1						
DEMP				1,5	5	5	5		3	5	2,5		
SEMI4			2	3,5	1				1	1	1		1
SEMI2		1,5	3,5		5	5				5			
LMRH		5	1	5	4,5	5			2	5	3		
MATH		5		5	5	5	5		2,5	5			
HALL	1	5				5		1		1		1	
BBH1							1			4,5			
JOWK		3	1		2	2,5				4,5			
JOHN		5	1	5	5	5	1	4,5	4,5				
DSFP		2,5	1		3								
BBH2							1						
BBS4			1										

Table 1: Connections between projective planes of order 16

No.	Arc	Aut(D)	# Par. cl.	# Resol.	$ Aut(C(D)) / Aut(C(D^{\perp})) $
1	PG(2,16).1	68	2329 / 2329	409 / 409	$2^{2}17^{1} / 2^{2}17^{1}$
2	PG(2,16).2	409	2550 / 2550	460 / 460	$2^{3}3^{1}17^{1} / 2^{3}3^{1}17^{1}$
3	DEMP.1	24	250 / 319	52 / 52	$2^{46}3^{19}5^{9}7^{6}11^{3}13^{3}17^{3} / 2^{33}3^{2}$
4	DEMP.2	144	543 / 1023	52 / 214	$2^{44}3^{14} / 2^{18}3^{4}5^{1}7^{1}$
5	DEMP.3	24	611 / 645	52 / 52	$2^{45}3^{13} / 2^{41}3^{11}5^{2}7^{2}$
6	DEMP.4	48	531 / 691	52 / 52	$2^{44}3^{14} / 2^{45}3^{15}$
7	DEMP.5	4	255 / 377	52 / 52	$2^{46}3^{19}5^{9}7^{6}11^{3}13^{3}17^{3} / 2^{33}3^{2}$
8	SEMI4.1	96	2569 / 2569	52 / 52	$2^{17}3^3 / 2^{17}3^3$
9	SEMI2.1	24	327 / 327	52 / 52	$2^{45}3^{15} / 2^{45}3^{15}$
10	SEMI2.2	144	1279 / 1279	55 / 55	$2^{18}3^45^17^1 / 2^{18}3^45^17^1$
11	SEMI2.3	32	1497 / 1497	52 / 52	$2^{26}3^1 / 2^{26}3^1$
12	SEMI2.4	32	1313 / 1313	52 / 52	$2^{25}3^1 / 2^{25}3^1$
13	SEMI2.5	16	1045 / 1045	52 / 52	$2^{37}3^6 / 2^{37}3^6$
14	SEMI2.6	48	547 / 691	52 / 52	$2^{45}3^{15} / 2^{17}3^3$
15	SEMI2.7	48	691 / 547	52 / 52	$2^{17}3^3 / 2^{45}3^{15}$
16	LMRH.1	96	2265 / 2265	104 / 104	$2^{45}3^{15} / 2^{45}3^{15}$
17	LMRH.2	32	2377 / 2289	64 / 64	$2^{45}3^{15} / 2^{45}3^{15}$
18	MATH.1	24	291 / 275	52 / 52	$2^{49}3^{20}5^{9}7^{6}11^{3}13^{3} / 2^{49}3^{20}5^{9}7^{6}11^{3}13^{3}$
19	MATH.2	32	1729 / 1553	52 / 52	$2^{37}3^2 / 2^{45}3^{15}$
20	MATH.3	32	2401 / 2217	64 / 104	$2^{45}3^{15} / 2^{45}3^{15}$
21	MATH.4	32	1665 / 1473	52 / 52	$2^{38}3^{5} / 2^{38}3^{5}$
22	MATH.5	16	1233 / 1457	52 / 52	$2^{43}3^{12}5^{2}7^{2} / 2^{36}3^{4}$
23	MATH.6	16	1329 / 1405	52 / 52	$2^{48}3^{14}5^{6}7^{6} / 2^{45}3^{15}$
24	MATH.7	16	1125 / 1505	52 / 52	$2^{48}3^{14}5^{6}7^{6} / 2^{45}3^{15}$
25	HALL.1	24	274 / 558	52 / 52	$2^{49}3^{20}5^{9}7^{6}11^{3}13^{3} / 2^{6}3^{2}$
26	HALL.2	4	309 / 445	52 / 52	$2^{46}3^{19}5^{9}7^{6}11^{3}13^{3}17^{3} / 2^{15}3^{4}$
27	BBH1.1	24	330 / 330	52 / 52	$2^{40}3^{13}5^{3}7^{3} / 2^{40}3^{13}5^{3}7^{3}$
28	BBH1.2	32	2017 / 2017	136 / 136	$2^{38}3^5 / 2^{38}3^5$
29	BBH1.3	4	285 / 285	52 / 52	$2^{43}3^{16}5^{6}7^{4}11 / 2^{43}3^{16}5^{6}7^{4}11$
30	JOWK.1	16	1389 / 1241	52 / 52	$2^{37}3^2 / 2^{44}3^{14}5^{1}7^{1}$
31	JOWK.2	32	2409 / 2321	104 / 52	$2^{37}3^2 / 2^{38}3^65^1$
32	JOHN.1	32	1953 / 1641	144 / 52	$2^{45}3^{15} / 2^{48}3^{14}5^{6}7^{6}$
33	JOHN.2	32	1953 / 1841	144 / 52	$2^{45}3^{15} / 2^{48}3^{14}5^{6}7^{6}$
34	JOHN.3	32	2017 / 1761	136 / 52	$2^{38}3^5 / 2^{48}3^{14}5^67^6$
35	JOHN.4	32	2409 / 1929	104 / 52	$2^{37}3^2 / 2^{48}3^{14}5^67^6$
36	DSFP.1	24	1045 / 1121	52 / 52	$2^{45}3^{13} / 2^{43}3^{11}$

Table 2: Designs associated with maximal (52,4)-arcs

Acknowledgments

The authors wish to thank the anonymous reviewer for the useful comments that lead to an improvement of the exposition.

References

- [1] Ball, S., Blokhuis A.: The classification of maximal arcs in small Desarguesian planes, Bull. Belg. Math. Soc. 9 (2009), 433-445.
- [2] Ball, S., Blokhuis A., Mazzocca F.: Maximal arcs in Desarguesian planes of odd order do not exist. *Combinatorica* 17 (1997), 31-41.
- [3] Beth T., Jungnickel D., Lenz H.: *Design Theory*, 2nd Edition, Cambridge University Press, 1999.

No.	2-rank	(52,4)-Arc	(A_2,A_4)	Aut(C(D))
1	41	PG(2,16).1	(0,221)	2^217^1
2	41	PG(2,16).2	(0,221)	$2^{3}3^{1}17^{1}$
3	43	HALL.1 [⊥]	(6,1037)	$2^{6}3^{2}$
4	45	$\{DEMP.1^{\perp}, DEMP.5^{\perp}\}$	(24,3989)	$2^{33}3^2$
5	45	$\{DEMP.2^{\perp}, SEMI2.2\}$	(6,4325)	$2^{18}3^45^17^1$
6	45	{SEMI4.1, SEMI2.7}	(0,4469)	$2^{17}3^3$
7	45	SEMI2.3	(18,4165)	$2^{26}3^{1}$
8	45	SEMI2.4	(16,4277)	$2^{25}3^1$
9	45	$\mathrm{HALL}.2^{\perp}$	(12,4229)	$2^{15}3^4$
10	46	JOHN.3	(42,8293)	$2^{38}3^{5}$
11	46	{JOHN.4, JOWK.1, MATH.2}	(26,8613)	$2^{37}3^2$
12	46	JOWK.2 [⊥]	(46,8325)	$2^{38}3^{6}5^{1}$
13	46	$\{MATH.4, MATH.4^{\perp}\}$	(42,8549)	$2^{38}3^{5}$
14	46	$MATH.5^{\perp}$	(42,8549)	$2^{36}3^4$
15	46	SEMI2.5	(50,8453)	$2^{37}3^{6}$
16	47	BBH1.1	(120,16853)	$2^{40}3^{13}5^{3}7^{3}$
17	47	{DEMP.2, DEMP.4}	(72,17045)	$2^{44}3^{14}$
18	47	{DSFP.1, DEMP.3}	(74,16997)	$2^{45}3^{13}$
19	47	DSFP.1 [⊥]	(66,17093)	$2^{43}3^{11}$
20	47	$ \begin{cases} \text{JOHN.1, LMRH.1, LMRH.2, LMRH.2}^{\bot}, \\ \text{MATH.2}^{\bot}, \text{MATH.3, MATH.3}^{\bot}, \text{MATH.6}^{\bot}, \\ \text{MATH.7}^{\bot}, \text{SEMI2.1, SEMI2.6, DEMP.4}^{\bot} \end{cases} $	(78,16901)	$2^{45}3^{15}$
21	47	JOWK.1 [⊥]	(94,16709)	$2^{44}3^{14}5^{1}7^{1}$
22	47	MATH.5	(106,16869)	$2^{43}3^{12}5^{2}7^{2}$
23	47	$DEMP.3^{\perp}$	(98,16965)	$2^{41}3^{11}5^{2}7^{2}$
24	48	$\{\text{JOHN}.1^{\perp}, \text{JOHN}.2^{\perp}, \text{JOHN}.3^{\perp}, \\ \text{JOHN}.4^{\perp}, \text{MATH}.6, \text{MATH}.7\}$	(174,33669)	$2^{48}3^{14}5^{6}7^{6}$
25	48	BBH1.3	(186,33829)	$2^{43}3^{16}5^{6}7^{4}11$
26	49	$\{HALL.1, MATH.1, MATH.1^{\perp}\}$	(366,67205)	$2^{49}3^{20}5^{9}7^{6}11^{3}13^{3}$
27	49	{DEMP.1, DEMP.5, HALL.2}	(408,67541)	$2^{46}3^{19}5^{9}7^{6}11^{3}13^{3}17^{3}$

Table 3: Equivalence classes of codes

- [4] Betten A., Betten D., and Tonchev V. D.: Unitals and codes, *Discrete Math.* **267** (2003), 23 33.
- [5] Betten, A., Braun, M., Fripertinger, H., Kerber, A., Kohnert, A., Wassermann, A.: *Error-Correcting Linear Codes*, Springer, 2006.
- [6] Bose, R. C. and Barlotti, A.: Linear representation of a class of projective planes in a four dimensional representation, *Ann. Mat. Pura Appl.* 88, (4) (1971), 9-31.
- [7] Brouwer A. E.: Some unitals on 28 points and their embedding in projective planes of order 9, *Lecture Notes in Math.* **893** (1981), 183 188.
- [8] Bosma, W., Cannon J.: Handbook of Magma Functions, School of Mathematics and Statistics, University of Sidney, Sidney, July 22 (1999).
- [9] Carpenter L. L.: Oval designs in Desarguesian projective planes, *Designs, Codes, and Cryptography*, **9** (1996), 51-59.
- [10] Colbourn, C.J, Dinitz, J. F. eds.: *Handbook of Combinatorial Designs*, Second Edition, Chapman & Hall/CRC, Boca Raton, 2007.
- [11] Denniston R.H.F.: Some maximal arcs in finite projective planes. *J. Combin. Theory* **6** 317-319 (1969).

No.	Arc	[n,k,d] of $C(D)$	$[\mathrm{n,k^\perp,d^\perp}] ext{ of } C(D)^\perp$	$A_{d^{\perp}}$
1	PG(2,16).1	[52,41,4]	[52,11,18]	54
2	PG(2,16).2	[52,41,4]	[52,11,18]	54
3	$HALL.1^{\perp}$	[52,43,2]	[52,9,18]	24
4	DEMP.1 $^{\perp}$	[52,45,2]	[52,7,20]	3
5	$DEMP.2^{\perp}$	[52,45,2]	[52,7,20]	3
6	$HALL.2^{\perp}$	[52,45,2]	[52,7,20]	3
7	SEMI2.3	[52,45,2]	[52,7,20]	11
8	SENI2.4	[52,45,2]	[52,7,18]	4
9	SEMI4.1	[52,45,4]	[52,7,20]	3
10	JOHN.3	[52,46,2]	[52,6,20]	3
11	JOHN.4	[52,46,2]	[52,6,20]	3
12	JOWK.2 [⊥]	[52,46,2]	[52,6,20]	11
13	MATH.4	[52,46,2]	[52,6,18]	4
14	$MATH.5^{\perp}$	[52,46,2]	[52,6,18]	4
15	SEMI2.5	[52,46,2]	[52,6,18]	4
16	BBH1.1	[52,47,2]	[52,5,18]	6
17	DEMP.2	[52,47,2]	[52,5,20]	3
18	DEMP.3 [⊥]	[52,47,2]	[52,5,18]	4
19	DSFP.1	[52,47,2]	[52,5,20]	3
20	DSFP.1 [⊥]	[52,47,2]	[52,5,20]	1
21	JOHN.1	[52,47,2]	[52,5,20]	3
22	JOWK.1 [⊥]	[52,47,2]	[52,5,20]	7
23	MATH.5	[52,47,2]	[52,5,18]	4
24	BBH1.3	[52,48,2]	[52,4,18]	2
25	JOHN.1 [⊥]	[52,48,2]	[52,4,20]	3
26	DEMP.1	[52,49,2]	[52,3,18]	3
27	HALL.1	[52,49,2]	[52,3,20]	3

Table 4: Parameters of codes and their dual codes

- [12] De Winter, S., Ding, C., Tonchev, V. D.: Maximal arcs and extended cyclic codes, *Designs, Codes and Cryptography*, 87 (2019), 807-816.
- [13] Ding, C.: Designs from Linear Codes, World Scientific, 2019.
- [14] Gezek, M.: Combinatorial problems related to codes, designs and finite geometries, PhD thesis, Michigan Technological University (2017).
- [15] Gezek, M., Wagner, T., Tonchev, V. D.: Maximal arcs in projective planes of order 16 and related designs, *Advances in Geometry* **19** (3) (2019), 345-351.
- [16] Grassl, M.: Code Tables, http://www.codetables.de/.
- [17] Hamilton, N.: Some maximal arcs in Hall planes, J. Geom. 52 (1995), 101-107.
- [18] Hamilton, N.: Some inherited maximal arcs in derived dual dual translation planes, Geom. Dedicata 55 (1995), 165 –173.
- [19] Hamilton, N.: Some maximal arcs in derived dual Hall planes, European J. Combin. 15 (1994), 525 532.
- [20] Hamilton, N., Mathon, R.: More maximal arcs in Desarguesian projective planes and their geometric structure, Adv. Geom. 3 (2003), 251 261.

- [21] Hamilton, N., Mathon, R.: On the spectrum of non-Denniston maximal arcs in $PG(2, 2^h)$, European J. Combin. 25 (2004), 415 421.
- [22] Hamilton N., Stoichev S. D., Tonchev V. D.: Maximal arcs and disjoint maximal arcs in projective planes of order 16. *J. Geometry* **67**, 117-126 (2000).
- [23] Hirschfeld J. W. P.: Projective Geometries over Finite Fields (2nd edition). Oxford University Press (1998).
- [24] Huffman W. Cary and Pless V.: Fundamentals of Error-Correcting Codes, Cambridge University Press, 2003.
- [25] Jaffe D. B. and Tonchev V. D.: Computing linear codes and unitals, *Designs, Codes and Cryptography* **14** (1998), 39 52.
- [26] Krčadinac V.: Steiner 2-designs S(2,4,28) with nontrivial automorphisms, Glasnik Mat. 37 (2002), 259-268.
- [27] Mathon, R.: On a new projective plane of order 16, Second International Conference in Deinze, 1992. Unpublished talk.
- [28] Mathon, R.: New maximal arcs in Desarguesian planes, J. Combin. Theory Ser. A 97 (2002), 353 368.
- [29] McGuire G., Tonchev V. D., and Ward H. N.: Characterizing the Hermitian and Ree unitals on 28 points, *Designs*, *Codes and Cryptography* **13** (1998), 57-61.
- [30] Moorhouse, E.: Projective Planes of Order 16. http://ericmoorhouse.org/pub/planes16/.
- [31] Niskanen, S., Östergård, P. R. J.: Cliquer User's Guide, Version 1.0. Tech. Rep. T48, Communications Laboratory, Helsinki University of Technology, Espoo, Finland, 2003.
- [32] Penttila, T., Royle, G. F., Simpson, M. K.: Hyperovals in the known projective planes of order 16. *J. Combin. Designs* 4 (1996), 59 65.
- [33] Rudolph L. R.: A class of majority-logic decodable codes, IEEE Trans. Inform. Theory 13 (1967), 305-307.
- [34] Thas, J. A.: Construction of maximal arcs and partial geometries, *Geom. Dedicata* 3, 61-64 (1974).
- [35] Thas, J. A.: Construction of maximal arcs and dual ovals in translation planes, *European J. Combin.* **1** (1980), 189-192.
- [36] Tonchev, V. D.: On resolvable Steiner 2-designs and maximal arcs in projective planes. *Designs, Codes, and Cryptography* 84 (2017), 165 172.
- [37] Tonchev V. D.: "Codes and Designs", Chapter 15 in: "Handbook of Coding Theory", V. S. Pless and W. C. Huffman eds., Chapter 15, pp. 1229-1267, Elsevier Science B.V. 1998.