

New Combinatorial Structures in Projective Planes of Order 16

Mustafa Gezek ¹ Vladimir D. Tonchev ²

¹Tekirdag Namik Kemal University

²Michigan Technological University

August 4, 2019

Outline

- 1 Introduction
- 2 New Maximal Arcs of Degree 4 in Planes of Order 16
- 3 New Connections Between Planes of Order 16

Definitions

A 2 - (v, k, λ) **design** $D = \{X, \mathcal{B}\}$ is a pair of a **point set** X of size v and a collection of k -subsets $\mathcal{B} = \{B_j\}_{j=1}^b$ called **blocks**, such that every pair of points is contained in exactly λ blocks.

Definitions

A 2 - (v, k, λ) **design** $D = \{X, \mathcal{B}\}$ is a pair of a **point set** X of size v and a collection of k -subsets $\mathcal{B} = \{B_j\}_{j=1}^b$ called **blocks**, such that every pair of points is contained in exactly λ blocks.

The **incidence matrix** of D is a block by point $(0, 1)$ -matrix whose (i, j) entry is 1 if block i contains point j , and 0 otherwise.

Definitions

A 2 - (v, k, λ) **design** $D = \{X, \mathcal{B}\}$ is a pair of a **point set** X of size v and a collection of k -subsets $\mathcal{B} = \{B_j\}_{j=1}^b$ called **blocks**, such that every pair of points is contained in exactly λ blocks.

The *incidence matrix* of D is a block by point $(0, 1)$ -matrix whose (i, j) entry is 1 if block i contains point j , and 0 otherwise.

A *parallel class* of D is a set of $\frac{v}{k}$ pairwise disjoint blocks,

Definitions

A 2 - (v, k, λ) **design** $D = \{X, \mathcal{B}\}$ is a pair of a **point set** X of size v and a collection of k -subsets $\mathcal{B} = \{B_j\}_{j=1}^b$ called **blocks**, such that every pair of points is contained in exactly λ blocks.

The *incidence matrix* of D is a block by point $(0, 1)$ -matrix whose (i, j) entry is 1 if block i contains point j , and 0 otherwise.

A *parallel class* of D is a set of $\frac{v}{k}$ pairwise disjoint blocks, and a *resolution* of D is a partition of the collection of blocks \mathcal{B} into $r = \frac{(v-1)\lambda}{k-1}$ parallel classes.

Definitions

A 2 - (v, k, λ) **design** $D = \{X, \mathcal{B}\}$ is a pair of a **point set** X of size v and a collection of k -subsets $\mathcal{B} = \{B_j\}_{j=1}^b$ called **blocks**, such that every pair of points is contained in exactly λ blocks.

The *incidence matrix* of D is a block by point $(0, 1)$ -matrix whose (i, j) entry is 1 if block i contains point j , and 0 otherwise.

A *parallel class* of D is a set of $\frac{v}{k}$ pairwise disjoint blocks, and a *resolution* of D is a partition of the collection of blocks \mathcal{B} into $r = \frac{(v-1)\lambda}{k-1}$ parallel classes.

A design is *resolvable* if it admits a resolution.

Maximal Arcs

Let Π be a finite projective plane of order $q = gk$.

Maximal Arcs

Let Π be a finite projective plane of order $q = gk$.

A $\{v; k\}$ -arc is a set \mathcal{A} of v points that meets every line of Π in at most k points.

Maximal Arcs

Let Π be a finite projective plane of order $q = gk$.

A $\{v; k\}$ -arc is a set \mathcal{A} of v points that meets every line of Π in at most k points.

In a $\{v; k\}$ -arc \mathcal{A} $v \leq q(k - 1) + k$ holds.

Maximal Arcs

Let Π be a finite projective plane of order $q = gk$.

A $\{v; k\}$ -arc is a set \mathcal{A} of v points that meets every line of Π in at most k points.

In a $\{v; k\}$ -arc \mathcal{A} $v \leq q(k - 1) + k$ holds.

A $\{v; k\}$ -arc is called **maximal** if $v = q(k - 1) + k$.

Maximal Arcs

Let Π be a finite projective plane of order $q = gk$.

A $\{v; k\}$ -arc is a set \mathcal{A} of v points that meets every line of Π in at most k points.

In a $\{v; k\}$ -arc \mathcal{A} $v \leq q(k - 1) + k$ holds.

A $\{v; k\}$ -arc is called **maximal** if $v = q(k - 1) + k$.

For a maximal $\{v; k\}$ -arc \mathcal{A} , k is called the **degree** of \mathcal{A} .

Maximal Arcs

Let Π be a finite projective plane of order $q = gk$.

A $\{v; k\}$ -arc is a set \mathcal{A} of v points that meets every line of Π in at most k points.

In a $\{v; k\}$ -arc \mathcal{A} $v \leq q(k - 1) + k$ holds.

A $\{v; k\}$ -arc is called **maximal** if $v = q(k - 1) + k$.

For a maximal $\{v; k\}$ -arc \mathcal{A} , k is called the **degree** of \mathcal{A} .

If \mathcal{A} is a maximal $\{v; k\}$ -arc, then every line of Π is either disjoint from \mathcal{A} , or meets \mathcal{A} in k points.

Maximal Arcs

The set of lines of Π which have no points in common with \mathcal{A} determines a maximal $\{(k(g-1)+1)g; g\}$ -arc \mathcal{A}^\perp in the dual plane Π^\perp .

Maximal Arcs

The set of lines of Π which have no points in common with \mathcal{A} determines a maximal $\{(k(g-1)+1)g; g\}$ -arc \mathcal{A}^\perp in the dual plane Π^\perp .

Maximal arcs with $1 < k < q$ do not exist in any Desarguesian planes of odd order [2],

Maximal Arcs

The set of lines of Π which have no points in common with \mathcal{A} determines a maximal $\{(k(g-1)+1)g; g\}$ -arc \mathcal{A}^\perp in the dual plane Π^\perp .

Maximal arcs with $1 < k < q$ do not exist in any Desarguesian planes of odd order [2], and do exist in any Desarguesian plane of even order with $k = 2^i$,

Maximal Arcs

The set of lines of Π which have no points in common with \mathcal{A} determines a maximal $\{(k(g-1)+1)g; g\}$ -arc \mathcal{A}^\perp in the dual plane Π^\perp .

Maximal arcs with $1 < k < q$ do not exist in any Desarguesian planes of odd order [2], and do exist in any Desarguesian plane of even order with $k = 2^i$, and in some non-Desarguesian planes of even order [5, 6].

Maximal Arcs

Let $1 < k < q$.

Maximal Arcs

Let $1 < k < q$.

The non-empty intersections of a maximal $\{(g(k-1)+1)k; k\}$ -arc \mathcal{A} with the lines of Π form a $2 - ((g(k-1)+1)k, k, 1)$ design D .

Maximal Arcs

Let $1 < k < q$.

The non-empty intersections of a maximal $\{(g(k-1)+1)k; k\}$ -arc \mathcal{A} with the lines of Π form a $2 - ((g(k-1)+1)k, k, 1)$ design D .

We say that D is a design *embeddable* in Π as a maximal arc.

Maximal Arcs

Let $1 < k < q$.

The non-empty intersections of a maximal $\{(g(k-1)+1)k; k\}$ -arc \mathcal{A} with the lines of Π form a $2 - ((g(k-1)+1)k, k, 1)$ design D .

We say that D is a design *embeddable* in Π as a maximal arc.

The points of \mathcal{A}^\perp determine a set of $(k(g-1)+1)g$ resolutions of D .

Maximal Arcs

Let $1 < k < q$.

The non-empty intersections of a maximal $\{(g(k-1)+1)k; k\}$ -arc \mathcal{A} with the lines of Π form a $2 - ((g(k-1)+1)k, k, 1)$ design D .

We say that D is a design *embeddable* in Π as a maximal arc.

The points of \mathcal{A}^\perp determine a set of $(k(g-1)+1)g$ resolutions of D .

Every two resolutions of D share one parallel class.

Compatible Resolutions

Let D be a resolvable $2 - (mk, k, 1)$ design.

Compatible Resolutions

Let D be a resolvable $2 - (mk, k, 1)$ design.

Two resolutions, R_1, R_2 of D ,

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

are *compatible* if

Compatible Resolutions

Let D be a resolvable $2 - (mk, k, 1)$ design.

Two resolutions, R_1, R_2 of D ,

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

are *compatible* if

- they share one parallel class, $P_i^{(1)} = P_j^{(2)}$, and

Compatible Resolutions

Let D be a resolvable $2 - (mk, k, 1)$ design.

Two resolutions, R_1, R_2 of D ,

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

are *compatible* if

- they share one parallel class, $P_i^{(1)} = P_j^{(2)}$, and
- $|P_{i'}^{(1)} \cap P_{j'}^{(2)}| \leq 1$ for $(i', j') \neq (i, j)$.

Compatible Resolutions

Let D be a resolvable $2 - (mk, k, 1)$ design.

Two resolutions, R_1, R_2 of D ,

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

are *compatible* if

- they share one parallel class, $P_i^{(1)} = P_j^{(2)}$, and
- $|P_{i'}^{(1)} \cap P_{j'}^{(2)}| \leq 1$ for $(i', j') \neq (i, j)$.

A set of resolutions $\mathcal{R} = \{R_1, R_2, \dots, R_n\}$ is called compatible if every pair of resolutions in \mathcal{R} is compatible.

An Upper Bound

Theorem 1 (Tonchev 2017)

Let $\mathcal{R} = \{R_1, R_2, \dots, R_n\}$ be a set of n mutually compatible resolutions of a $2 - (v, k, 1)$ design D , where $v = (g(k - 1) + 1)k$.

An Upper Bound

Theorem 1 (Tonchev 2017)

Let $\mathcal{R} = \{R_1, R_2, \dots, R_n\}$ be a set of n mutually compatible resolutions of a $2 - (v, k, 1)$ design D , where $v = (g(k - 1) + 1)k$. Then

$$n \leq (k(g - 1) + 1)g.$$

An Upper Bound

Theorem 1 (Tonchev 2017)

Let $\mathcal{R} = \{R_1, R_2, \dots, R_n\}$ be a set of n mutually compatible resolutions of a $2 - (v, k, 1)$ design D , where $v = (g(k - 1) + 1)k$. Then

$$n \leq (k(g - 1) + 1)g.$$

Equality holds if and only if there exist a projective plane Π of order $g = k$ such that D is embeddable in Π as a maximal $\{v; k\}$ -arc.

In [6], Penttila et al did a computer search and classified all degree 2 and 8 maximal arcs in the known planes of order 16.

In [6], Penttila et al did a computer search and classified all degree 2 and 8 maximal arcs in the known planes of order 16.

The degree 4 maximal arcs in the projective planes of order 16 have not been classified completely.

In [6], Penttila et al did a computer search and classified all degree 2 and 8 maximal arcs in the known planes of order 16.

The degree 4 maximal arcs in the projective planes of order 16 have not been classified completely. A complete classification seems computationally infeasible at present time.

In [6], Penttila et al did a computer search and classified all degree 2 and 8 maximal arcs in the known planes of order 16.

The degree 4 maximal arcs in the projective planes of order 16 have not been classified completely. A complete classification seems computationally infeasible at present time.

In [1], Ball and Blokhuis proved that up to isomorphism $PG(2,16)$ contains only two maximal $(52,4)$ -arcs.

#	Maximal (52,4)-arc	Design's Aut Group Order	2-rank of designs	# of parallel classes	# of resolutions	# of compatible resolutions	Plane(s) isomorphic to?
1	<i>desg.1</i>	68	41	2329	409	52 ($\times 1$)	desg
2	<i>desg.2</i>	408	41	2550	460	52 ($\times 1$)	desg
3	<i>demp.1</i>	24	49	250	52	52 ($\times 1$)	demp
4	<i>demp.2</i>	144	47	543	52	52 ($\times 1$)	demp
5	<i>semi4.1</i>	96	45	2569	52	52 ($\times 1$)	semi4
6	<i>semi2.1</i>	24	47	327	52	52 ($\times 1$)	semi2
7	<i>semi2.2</i>	144	45	1279	55	52 ($\times 1$)	semi2
8	<i>lmrh.1</i>	96	47	2265	104	52 ($\times 2$)	lmrh and lmrh ⁻¹
9	<i>math.1</i>	24	49	291	52	52 ($\times 1$)	math
10	<i>hall.1</i>	24	49	274	52	52 ($\times 1$)	hall
11	<i>bbh1.1</i>	24	47	330	52	52 ($\times 1$)	bbh1
12	<i>bbh1.2</i>	32	46	2017	136	52 ($\times 2$)	bbh1 and john
13	<i>jowk.1</i>	16	46	1389	52	52 ($\times 1$)	jowk
14	<i>jowk.2</i>	32	46	2409	104	52 ($\times 2$)	jowk and john
15	<i>john.1</i>	32	47	1953	144	52 ($\times 2$)	john
16	<i>john.2</i>	32	47	1953	144	52 ($\times 2$)	john
17	<i>dsfp.1</i>	24	47	1045	52	52 ($\times 1$)	dsfp

Table 1: The maximal (52,4)-arcs and their designs

#	Maximal (52,4)-arc	Design's Aut Group Order	2-rank of designs	# of parallel classes	# of resolutions	# of compatible resolutions	Plane(s) isomorphic to?
1	<i>desg.1</i>	68	41	2329	409	52 (×1)	desg
2	<i>desg.2</i>	408	41	2550	460	52 (×1)	desg
3	<i>demp.1</i>	24	49	250	52	52 (×1)	demp
4	<i>demp.2</i>	144	47	543	52	52 (×1)	demp
5	<i>demp.3</i>	24	47	611	52	52 (×1)	demp
6	<i>demp.4</i>	48	47	531	52	52 (×1)	demp
7	<i>semi4.1</i>	96	45	2569	52	52 (×1)	semi4
8	<i>semi2.1</i>	24	47	327	52	52 (×1)	semi2
9	<i>semi2.2</i>	144	45	1279	55	52 (×1)	semi2
10	<i>semi2.3</i>	32	45	1497	52	52 (×1)	semi2
11	<i>semi2.4</i>	32	45	1313	52	52 (×1)	semi2
12	<i>semi2.5</i>	16	46	1045	52	52 (×1)	semi2
13	<i>semi2.6</i>	48	47	547	52	52 (×1)	semi2
14	<i>semi2.7</i>	48	45	691	52	52 (×1)	semi2
15	<i>lmrh.1</i>	96	47	2265	104	52 (×2)	lmrh and lmrh ⁺
16	<i>lmrh.2</i>	32	47	2377	64	52 (×1)	lmrh
17	<i>math.1</i>	24	49	291	52	52 (×1)	math
18	<i>math.2</i>	32	46	1729	52	52 (×1)	math
19	<i>math.3</i>	32	47	2401	64	52 (×1)	math
20	<i>math.4</i>	32	46	1665	52	52 (×1)	math
21	<i>math.5</i>	16	47	1233	52	52 (×1)	math
22	<i>math.6</i>	16	48	1329	52	52 (×1)	math
23	<i>math.7</i>	16	48	1125	52	52 (×1)	math
24	<i>hall.1</i>	24	49	274	52	52 (×1)	hall
25	<i>bbh1.1</i>	24	47	330	52	52 (×1)	bbh1
26	<i>bbh1.2</i>	32	46	2017	136	52 (×2)	bbh1 and john
27	<i>jowk.1</i>	16	46	1389	52	52 (×1)	jowk
28	<i>jowk.2</i>	32	46	2409	104	52 (×2)	jowk and john
29	<i>john.1</i>	32	47	1953	144	52 (×2)	john
30	<i>john.2</i>	32	47	1953	144	52 (×2)	john
31	<i>john.3</i>	32	46	2017	136	52 (×2)	john and bbh1
32	<i>john.4</i>	32	46	2409	104	52 (×2)	john and jowk
33	<i>dsfp.1</i>	24	47	1045	52	52 (×1)	dsfp

Table 2: The maximal (52,4)-arcs and their designs

Theorem 2

The number of pairwise non-isomorphic resolvable $2 - (52, 4, 1)$ designs is greater than or equal to 50, previous to our work this bound was 30.

Theorem 2

The number of pairwise non-isomorphic resolvable $2 - (52, 4, 1)$ designs is greater than or equal to 50, previous to our work this bound was 30.

Theorem 3

The number of maximal arcs of degree 4 in planes of order 16 is greater than or equal to 63, previous to our work this bound was 32.

Codes of Maximal Arcs

Let D and $C(D)$ be a design and a linear code (the code spanned by the block by point incidence matrix of D) associated to a maximal arc, respectively.

Codes of Maximal Arcs

Let D and $C(D)$ be a design and a linear code (the code spanned by the block by point incidence matrix of D) associated to a maximal arc, respectively.

The parameters and the order of the automorphism group of $C(D)$ are computed for all known maximal arcs in the planes of order 16.

Codes of Maximal Arcs

Let D and $C(D)$ be a design and a linear code (the code spanned by the block by point incidence matrix of D) associated to a maximal arc, respectively.

The parameters and the order of the automorphism group of $C(D)$ are computed for all known maximal arcs in the planes of order 16.

Furthermore, using Magma [3], codes were sorted according to their weight distributions, and codes having the same weight distributions were tested for equivalences.

No.	2-rank	(52,4)-Arc	(A_2, A_4)	$ Aut(C(D)) $
1	41	desg.1	(0,221)	$2^2 17^1$
2	41	desg.2	(0,221)	$2^3 3^1 17^1$
3	43	hall.1 [±]	(6,1037)	$2^6 3^2$
4	45	demp.1 [±]	(24,3989)	$2^{33} 3^2$
5	45	{demp.2 [±] , semi2.2}	(6,4325)	$2^{18} 3^4 5^1 7^1$
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	46	john.3	(42,8293)	$2^{38} 3^5$
10	46	{john.4, jowk.1, math.2}	(26,8613)	$2^{37} 3^2$
11	46	jowk.2 [±]	(46,8325)	$2^{38} 3^6 5^1$
12	46	{math.4, math.4 [±] }	(42,8549)	$2^{38} 3^5$
13	46	math.5 [±]	(42,8549)	$2^{36} 3^4$
14	46	semi2.5	(50,8453)	$2^{37} 3^6$
15	47	bbh.1.1	(120,16853)	$2^{40} 3^{13} 5^3 7^3$
16	47	{demp.2, demp.4}	(72,17045)	$2^{44} 3^{14}$
17	47	{dsfp.1, demp.3}	(74,16997)	$2^{45} 3^{13}$
18	47	dsfp.1 [±]	(66,17093)	$2^{43} 3^{11}$
19	47	{john.1, lmrh.1, lmrh.2, lmrh.2 [±] , math.2 [±] , math.3, math.3 [±] , math.6 [±] , math.7 [±] , semi2.1, semi2.6, demp.4 [±] }	(78,16901)	$2^{45} 3^{15}$
20	47	jowk.1 [±]	(94,16709)	$2^{44} 3^{14} 5^1 7^1$
21	47	math.5	(106,16869)	$2^{43} 3^{12} 5^2 7^2$
22	47	demp.3 [±]	(98,16965)	$2^{41} 3^{11} 5^2 7^2$
23	48	{john.1 [±] , john.2 [±] , john.3 [±] , john.4 [±] , math.6, math.7}	(174,33669)	$2^{48} 3^{14} 5^6 7^6$
24	49	{hall.1, math.1, math.1 [±] }	(366,67205)	$2^{49} 3^{20} 5^9 7^6 11^3 13^3$
25	49	demp.1	(408,67541)	$2^{46} 3^{19} 5^9 7^6 11^3 13^3 17^3$

Table 3: 2 – (52, 4, 1) designs and their codes

Theorem 4

Theorem 4

- ① Codes associated to desg.1 and desg.2 have the same weight distribution, but they are not equivalent.

Theorem 4

- ① Codes associated to desg.1 and desg.2 have the same weight distribution, but they are not equivalent.
- ② Codes associated to math.4 and math.5^\perp have the same weight distribution, but they are not equivalent,

Theorem 4

- ① Codes associated to desg.1 and desg.2 have the same weight distribution, but they are not equivalent.
- ② Codes associated to math.4 and math.5^\perp have the same weight distribution, but they are not equivalent,
- ③ Planes LMRH and MATH share a $C(D)$ with their duals.

Theorem 4

- ① Codes associated to *desg.1* and *desg.2* have the same weight distribution, but they are not equivalent.
- ② Codes associated to *math.4* and *math.5*[⊥] have the same weight distribution, but they are not equivalent,
- ③ Planes LMRH and MATH share a $C(D)$ with their duals.
- ④ Codes associated with *desg.1*, *desg.2* and *semi4.1* have minimum distance 4, while the minimum distance of all other codes is 2.

Theorem 4

- ① Codes associated to *desg.1* and *desg.2* have the same weight distribution, but they are not equivalent.
- ② Codes associated to *math.4* and $math.5^\perp$ have the same weight distribution, but they are not equivalent,
- ③ Planes LMRH and MATH share a $C(D)$ with their duals.
- ④ Codes associated with *desg.1*, *desg.2* and *semi4.1* have minimum distance 4, while the minimum distance of all other codes is 2.
- ⑤ The code of *semi4.1* is optimal: it has the largest possible minimum distance for the given length 52 and dimension 45.






Theorem 4

- ① Codes associated to *desg.1* and *desg.2* have the same weight distribution, but they are not equivalent.
- ② Codes associated to *math.4* and $math.5^\perp$ have the same weight distribution, but they are not equivalent,
- ③ Planes LMRH and MATH share a $C(D)$ with their duals.
- ④ Codes associated with *desg.1*, *desg.2* and *semi4.1* have minimum distance 4, while the minimum distance of all other codes is 2.
- ⑤ The code of *semi4.1* is optimal: it has the largest possible minimum distance for the given length 52 and dimension 45.
- ⑥ The 50 codes are partitioned into 25 equivalence classes.

	DESG	DEMP	SEMI4	SEMI2	LMRH	MATH	HALL	BBH1	JOWK	JOHN	DSFP	BBH2	BBS4
DESG							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 4: Connections between planes of order 16

Thank you!

-  Ball S., Blokhuis A., The classification of maximal arcs in small Desarguesian planes, *Bull. Belg. Math. Soc. Simon Stevin*, 9(3):433-445 (2002).
-  Ball S., Blokhuis A., Mazzocca F., Maximal arcs in desarguesian planes of odd order do not exist, *Combinatorica*, 17(1):31-41 (1997).
-  Bosma W., Cannon J., *Handbook of Magma Functions*, School of Mathematics and Statistics, University of Sidney, Sidney, July 22 (1999).
-  Gezek, M., Tonchev, V. D., Wagner, T., Maximal arcs in projective planes of order 16 and related designs. *Advances in Geometry*, 19(3), pp. 345-351 (2018).
-  Hamilton N., Stoichev S.D., Tonchev V.D., Maximal arcs and disjoint maximal arcs in projective planes of order 16, *Journal of Geometry*, 67(1-2):117-126 (2000).



Penttila T., Royle G.F., Simpson M.K., Hyperovals in the known projective planes of order 16, *Journal of Combinatorial Designs*, 4(10:59-65 (1996).



Tonchev V.D., On resolvable steiner 2-designs and maximal arcs in projective planes, *Designs, Codes and Cryptography*, 1-8 (2017).