algorithms

MDPI

Article

Cyclotomic Trace Codes

Dean Crnković [1], Andrea Švob [1,*] and Vladimir D. Tonchev [2]

1 Department of Mathematics, University of Rijeka, Radmile Matejčić 2, 51000 Rijeka, Croatia
2 Department of Mathematical Sciences, Michigan Technological University, Houghton, MI 49931, USA
* Correspondence: asvob@math.uniri.hr

Received: 20 June 2019; Accepted: 10 August 2019; Published: 13 August 2019

check for updates

Abstract: A generalization of Ding's construction is proposed that employs as a defining set the collection of the sth powers ($s \geq 2$) of all nonzero elements in $GF(p^m)$, where $p \geq 2$ is prime. Some of the resulting codes are optimal or near-optimal and include projective codes over $GF(4)$ that give rise to optimal or near optimal quantum codes. In addition, the codes yield interesting combinatorial structures, such as strongly regular graphs and block designs.

Keywords: linear code; two-weight code; strongly regular graph; block design

1. Introduction

In Reference [1], Ding introduced a generic construction of linear codes using a defining set D and the trace function. Many classes of known codes can be produced by choosing an appropriate defining set [2–6]. Some of these codes support combinatorial 2-designs [7,8].

In Reference [7], Ding considered linear codes obtained by choosing the defining set D to be the set of all nonzero squares in $GF(p^m)$, where p is an odd prime.

In this paper, we generalize Ding's construction from Reference [7], by choosing the defining set D to be the set of all sth powers of nonzero elements in a field $GF(p^m)$, where $p \geq 2$ can be any prime, and $s \geq 2$. Our construction generalizes and expands Ding's construction [7] in two ways—we use as defining sets arbitrary powers of nonzero elements of $GF(q)$, where q can be odd or even, while Ding uses only the set of nonzero squares ($s = 2$) and q is odd. If s is relatively prime to $p^m - 1$, the resulting code is a one-weight code, hence equivalent to a sequence of dual Hamming codes (cf. References [9–11]), while when s is not relatively prime to $p^m - 1$, some interesting two-weight codes are obtained that give rise to strongly regular graphs, block designs and quantum codes. Block designs are constructed as support designs for a given nonzero weight (for other recent research on block designs arising from codes, see Reference [12]). The resulting strongly regular graphs have as vertices the codewords, where two codewords are adjacent if they are at minimum Hamming distance from each other [13,14].

Besides codes over fields of odd order q, in this paper we also construct linear codes over finite fields of even order.

In particular, we obtain projective codes over $GF(4)$ that give rise to optimal or near optimal quantum codes over $GF(4)$.

The paper is organized as follows. Section 2 provides the necessary definitions and notation used in the paper. In Section 3, a construction of linear codes with a defining set being the set of all nonzero sth powers in a field $GF(p^m)$ is outlined and the newly found two-weight codes and corresponding strongly regular graphs are presented. In Section 4, we describe support designs and generalized block graphs obtained from the resulting codes.

The codes have been constructed and examined using Magma [15].

2. Preliminaries

For background reading in coding theory we refer the reader to Reference [16].

A q-ary linear code C of dimension k for a prime power q, is a k-dimensional subspace of a vector space $\mathbb{F}_q^n$. The elements of C are called codewords. The Hamming distance between two vectors $x = (x_1, ..., x_n), y = (y_1, ..., y_n) \in \mathbb{F}_q^n$ is the number $d(x,y) = |\{i : x_i \neq y_i\}|$. The minimum distance d of a code C is defined as $d = \min\{d(x,y) : x, y \in C,\ x \neq y\}$. The weight of a codeword x is $w(x) = d(x,0) = |\{i : x_i \neq 0\}|$. For a linear code, $d = \min\{w(x) : x \in C, x \neq 0\}$. A q-ary linear code of length n, dimension k and distance d is called a $[n,k,d]_q$ code.

Let w_i denote the number of codewords of weight i in a code C of length n. The weight distribution of C is the list $[\langle i, w_i\rangle : 0 \leq i \leq n]$. A one-weight code is a code which has only one nonzero weight and a two-weight code is a code which has only two nonzero weights. A linear code C is called projective if the minimum distance of its dual code $C^{\perp} = \{y \mid y \cdot x = 0 \text{ for all } x \in C\}$ is greater than 2.

An $[n,k]$ linear code C is optimal if the minimum weight of C achieves the theoretical upper bound on the minimum weight of an $[n,k]$ linear code, and near-optimal if its minimum weight is at most 1 less than the largest possible value. An $[n,k]$ linear code C is said to be a best known linear $[n,k]$ code if C has the highest minimum weight among all known $[n,k]$ linear codes. A catalog of the best known codes is maintained in Reference [17], to which we compare the minimum weight of all codes constructed in this paper.

An incidence structure is an ordered triple $\mathcal{D} = (\mathcal{P}, \mathcal{B}, \mathcal{I})$ where $\mathcal{P}$ and $\mathcal{B}$ are non-empty disjoint sets and $\mathcal{I} \subseteq \mathcal{P} \times \mathcal{B}$. The elements of the set $\mathcal{P}$ are called points, the elements of the set $\mathcal{B}$ are called blocks and $\mathcal{I}$ is called an incidence relation. If $|\mathcal{P}| = |\mathcal{B}|$ then the incidence structure is called symmetric.

A t-(v,k,λ) design is a finite incidence structure $\mathcal{D} = (\mathcal{P}, \mathcal{B}, \mathcal{I})$ satisfying the following requirements:

1. $|\mathcal{P}| = v$,
2. every element of $\mathcal{B}$ is incident with exactly k elements of $\mathcal{P}$,
3. every t elements of $\mathcal{P}$ are incident with exactly λ elements of $\mathcal{B}$.

A 2-(v,k,λ) design is called a block design. Note that this definition allows $\mathcal{B}$ to be a multiset. If $\mathcal{B}$ is a set then $\mathcal{D}$ is called a simple design. If the design $\mathcal{D}$ consists of k copies of some simple design $\mathcal{D}'$ then $\mathcal{D}$ is non-simple design and it is denoted by $\mathcal{D} = k\mathcal{D}'$. We say that a t-(v,k,λ) design $\mathcal{D}$ is a quasi-symmetric design with intersection numbers x and y $(x < y)$ if any two blocks of $\mathcal{D}$ intersect in either x or y points.

A graph is regular if all the vertices have the same degree. A connected graph Γ with diameter d is called distance-regular if there are integers $b_i, c_i, i \geq 0$ such that, for any two vertices $u, v \in \Gamma$ at distance $d(u,v) = i$, there are exactly c_i neighbors of v at distance $i-1$ from u and b_i neighbors of v at distance $i+1$ from u. A distance-regular graph is usually denoted by DRG. The graph Γ is a regular graph of valency $k = b_0$. The numbers c_i, b_i, a_i, where $a_i = k - b_i - c_i$, $i = 0, \ldots, d$ is the number of neighbors of v at distance i from u, are called the intersection numbers of Γ. The sequence $\{b_0, b_1, \ldots, b_{d-1}; c_1, c_2, \ldots, c_d\}$, where d is the diameter of Γ is called the intersection array of Γ. Clearly, $b_0 = k$, $b_d = c_0 = 0$, $c_1 = 0$.

A regular graph is strongly regular of type (v,k,λ,μ) if it has v vertices, degree k and if any two adjacent vertices are together adjacent to λ vertices, while any two non-adjacent vertices are together adjacent to μ vertices. A strongly regular graph of type (v,k,λ,μ) is usually denoted by SRG(v,k,λ,μ). A strongly regular graph is a distance-regular graph with diameter 2 whenever $\mu \neq 0$. The intersection array of a strongly regular graph is given by $\{k, k-1-\lambda, 1, \mu\}$.

The block graph Γ of a quasi-symmetric 2-(v,k,λ) design $\mathcal{D}$ is the graph with vertex set being the blocks of $\mathcal{D}$, where vertices corresponding to blocks B_i and B_j are adjacent if and only if $|B_i \cap B_j| = y$.

The block graph of a quasi-symmetric design is strongly regular (see Reference [18]). More about the theory of quasi-symmetric designs can be found in Reference [19].

For relevant background reading in theory of strongly regular graphs we refer the reader to References [18,20], and for background reading in theory of distance-regular graphs we refer the reader to Reference [21].

3. Construction of Linear Codes

In Reference [1], Ding gave a construction of linear codes over $GF(p)$ with any subset D of $GF(p^m)$. In Reference [7] (Corollary 4) he considered the specific subset D consisting of nonzero squares. In this paper, we consider the case when D is a set of various nonzero powers of s. A necessary condition for obtaining codes with more than one nonzero weight is that s is not relatively prime to $(p^m - 1)$. In some cases obtained codes are two-weight.

In tables presenting codes over finite fields, $*$ denotes that the codes are optimal in the sense that they reach the Griesmer bound.

3.1. Codes Obtained from Fields of Odd Order

In Reference [7], Ding presented the following construction of linear codes from nonzero squares. Let $D = \{d_1, d_2, \ldots, d_n\} \subseteq GF(q)$, such that d_i are nonzero squares in a field $GF(q)$ and $q = p^m$. Let Tr denote the trace function defined in the following way. Let $L = GF(p^m)$ be a finite extension of a field $K = GF(p)$. If α is in L, the trace of α is the sum

$$Tr_{L/K}(\alpha) = \alpha + \alpha^p + \cdots + \alpha^{p^{m-1}}.$$

One can define a linear code of length n over $GF(p)$ by

$$C_D = \{(Tr(xd_1), Tr(xd_2), \ldots, Tr(xd_n)) : x \in GF(q)\},$$

and call D the defining set of this code C_D. Note that by definition, the dimension of the code C_D is at most m.

Result 1 (Corollary 4, [7]). *Let D be the set of all quadratic residues in $GF(p^m)^*$, where p is an odd prime. If m is odd, then C_D is a one-weight code over $GF(p)$ with parameters $[(q-1)/2, m, (p-1)q/2p]$. If m is even, then C_D is a two-weight code over $GF(p)$ with parameters $[(q-1)/2, m, (p-1)(q-\sqrt{q})/2p]$ and weight enumerator $1 + \frac{q-1}{2} z^{(p-1)(q-\sqrt{q})/2p} + \frac{q-1}{2} z^{(p-1)(q+\sqrt{q})/2p}$.*

If D is a set of nonzero squares in $GF(q)$, and depending whether $q \equiv 3 \pmod 4$ or $q \equiv 1 \pmod 4$, using Ding's result presented in Reference Corollary 1, we obtain one or two-weight codes.

From the supports of all codewords of minimum weight of the one-weight codes, one obtains the family of symmetric designs known as point-hyperplane designs. Since all linear one-weight codes are characterized (see References [10,11] for more information), in this paper we were interested only in codes with more weights. In Table 1 we describe the two-weight codes obtained by applying the construction of Ding described above, and the corresponding strongly regular graphs obtained from these codes by the well-known construction (see Reference [13]). We give the parameters of the codes and their weight distribution and the parameters of the strongly regular graphs (SRGs).

Table 1. Two-weight trace codes from nonzero squares.

p, q, m	Code	Weight Dist.	Corr. Proj. Code	SRG
$3, 9, 2$	$[4, 2, 2]_3$	$< 0, 1 >, < 2, 4 >, < 4, 4 >$	$[2, 2, 1]^*, d^\perp = 2$	(9,4,1,2)
$3, 81, 4$	$[40, 4, 24]_3$	$< 0, 1 >, < 24, 40 >, < 30, 40 >$	$[20, 4, 12]^*, d^\perp = 3$	(81,40,19,20)
$3, 729, 6$	$[364, 6, 234]_3$	$< 0, 1 >, < 234, 364 >, < 252, 364 >$	$[182, 6, 117], d^\perp = 3$	(729,364,181,182)
$5, 25, 2$	$[12, 2, 8]_5$	$< 0, 1 >, < 8, 12 >, < 12, 12 >$	$[3, 2, 2]^*, d^\perp = 3$	(25,12,5,6)
$5, 625, 4$	$[312, 4, 240]_5$	$< 0, 1 >, < 240, 312 >, < 260, 312 >$	$[78, 4, 60], d^\perp = 3$	(625,312,155,156)
$7, 49, 2$	$[24, 2, 18]_7$	$< 0, 1 >, < 18, 24 >, < 24, 24 >$	$[4, 2, 3]^*, d^\perp = 3$	(49,24,11,12)
$7, 2401, 4$	$[1200, 4, 1008]_7$	$< 0, 1 >, < 1008, 1200 >, < 1050, 1200 >$	$[200, 4, 168], d^\perp = 3$	(2401,1200,599,600)

Remark 1. *All strongly regular graphs in Table 1 are Paley graphs.*

Using an approach similar to that described above, we obtained results by defining the set $D = \{d_1, d_2, \ldots, d_n\} \subseteq GF(q)$ such that d_i are all nonzero cubes in a field $GF(q)$ and $q = p^m$.

In Table 2 we describe the codes obtained by applying the construction described above. We give the parameters of the codes, their weight distributions and the descriptions of the SRGs related to constructed codes.

Table 2. Two-weight trace codes from nonzero cubes.

p, q, m	Code	Weight Dist.	Corr. Proj. Code	SRG
$5, 25, 2$	$[8, 2, 4]_5$	$< 0, 1 >, < 4, 8 >, < 8, 16 >$	$[2, 2, 1]^*, d^\perp = 2$	(25,8,3,2)
$5, 625, 4$	$[208, 4, 160]_5$	$< 0, 1 >, < 160, 416 >, < 180, 208 >$	$[52, 4, 40]^*, d^\perp = 3$	(625,208,63,72)
$5, 15625, 6$	$[5208, 6, 4100]_5$	$< 0, 1 >, < 4100, 5208 >, < 4200, 10416 >$	$[1302, 6, 1025], d^\perp = 3$	(15625,5208,1763,1722)
$11, 121, 2$	$[40, 2, 30]_{11}$	$< 0, 1 >, < 30, 40 >, < 40, 80 >$	$[4, 2, 3]^*, d^\perp = 3$	(121,40,15,12)
$11, 14641, 4$	$[4880, 4, 4400]_{11}$	$< 0, 1 >, < 4400, 9760 >, < 4510, 4880 >$	$[488, 4, 440], d^\perp = 3$	(14641,4880,1599,1640)
$17, 289, 2$	$[96, 2, 80]_{17}$	$< 0, 1 >, < 80, 96 >, < 96, 192 >$	$[6, 2, 5]^*, d^\perp = 3$	(289,96,35,30)

Remark 2. *We have constructed SRGs with parameters $v = q, k = (q-1)/3, \lambda = [(\sqrt{q}+1)^2 - 9]/9, \mu = (\sqrt{q}+1)(\sqrt{q}-2)/9$, and $q = 25, 121, 289, 15625$. According to Brouwer's table (see Reference [22]), known graphs with these parameters are obtainable from orthogonal arrays $OA(\sqrt{q}, (\sqrt{q}+1)/3)$. Since our method does not use orthogonal arrays, it is likely that our graphs are new. The SRG with parameters (625,208,63,72) is isomorphic to the SRG obtained from projective 5-ary $[52, 4]$ code with weights 40, 45 (see [23]). In fact, the code $[208, 4, 160]_5$ is four copies of the above mentioned projective $[52, 4, 40]$ code. SRG(14641,4880,1599,1640) is isomorphic to the graph obtained by CY2 construction (see Reference [23]) for $q = 11$ and $S = 4$.*

Using an approach similar to that described above, we obtained results by defining the set $D = \{d_1, d_2, \ldots, d_n\} \subseteq GF(q)$, such that d_i are all nonzero powers of 4 in a field $GF(q)$ and $q = p^m$. The results are given in Table 3.

Table 3. Two-weight trace codes from powers of 4.

p, q, m	Code	Weight Dist.	Corr. Proj. Code	SRG
$3, 81, 4$ $3, 729, 6$	$[20, 4, 12]_3^*$ $[182, 6, 108]_3$	$< 0, 1 >, < 12, 60 >, < 18, 20 >$ $< 0, 1 >, < 108, 182 >, < 126, 546 >$	$[10, 4, 6]^*, d^{\perp} = 4$ $[91, 6, 54], d^{\perp} = 3$	(81,20,1,6) (729,182,55,42)
$5, 25, 2$ $5, 15625, 6$	$[6, 2, 4]_5, d^{\perp} = 3$ $[3906, 6, 3100]_5^*$	$< 0, 1 >, < 4, 12 >, < 6, 12 >$ $< 0, 1 >, < 3100, 7812 >, < 3150, 7812 >$	 $[1953, 6, 1550], d^{\perp} = 3$	(25,12,5,6) (15625,7812,3905,3906)
$7, 49, 2$ $7, 2401, 4$	$[12, 2, 6]_7$ $[600, 4, 504]_7$	$< 0, 1 >, < 6, 12 >, < 12, 36 >$ $< 0, 1 >, < 504, 1800 >, < 546, 600 >$	$[2, 2, 1]^*, d^{\perp} = 2$ $[100, 4, 84]^*, d^{\perp} = 3$	(49,12,5,2) (2401,600,131,156)
$11, 121, 2$ $11, 14641, 4$	$[30, 2, 20]_{11}$ $[3660, 4, 3300]_{11}$	$< 0, 1 >, < 20, 30 >, < 30, 90 >$ $< 0, 1 >, < 3300, 10980 >, < 3410, 3660 >$	$[3, 2, 2]^*, d^{\perp} = 3$ $[366, 4, 330], d^{\perp} = 3$	(121,30,11,6) (14641,3660,869,871)
$13, 169, 2$	$[42, 2, 36]_{13}$	$< 0, 1 >, < 36, 84 >, < 42, 84 >$	$[7, 2, 6]^*, d^{\perp} = 3$	(169,84,41,42)
$17, 289, 2$	$[72, 2, 64]_{17}$	$< 0, 1 >, < 64, 144 >, < 72, 144 >$	$[9, 2, 8]^*, d^{\perp} = 3$	(289,144,71,72)
$19, 361, 2$	$[90, 2, 72]_{19}$	$< 0, 1 >, < 72, 90 >, < 90, 270 >$	$[5, 2, 4]^*, d^{\perp} = 3$	(361,90,29,20)

Remark 3. *SRG(81,20,1,6) and SRG(49,12,5,2) are unique SRGs with these parameters. The SRG with parameters (81,20,1,6) is isomorphic to the SRG obtained from projective ternary* $[10, 4]$ *code with weights 6, 9 (see Reference [24]). In fact, the code* $[20, 4, 12]_3$ *is two copies of the above-mentioned projective* $[10, 4, 6]$ *code. SRGs with parameters (25,12,5,6), (15625,7812,3905,3906), (169,84,41,42) and (289,144,71,72) are Paley graphs. We have constructed SRGs with parameters (121,30,11,6), (361,90,29,20) and (14641,3660,869,871). According to Brouwer's table (see Reference [22]), known graphs with these parameters are obtainable from orthogonal arrays. The graph with parameters (729,182,55,42) does not arise from orthogonal array, although it has suitable parameters. It is isomorphic with the SRG obtained from projective ternary* $[91, 6]$ *code with weights 54, 63 (see Reference [22]). The code* $[182, 6, 108]_3$ *is two copies of the above mentioned projective* $[91, 6, 54]$ *code. The SRG(2401,600,131,156) is isomorphic to the graph obtained by CY2 construction (see Reference [23]), for* $q = 7$ *and* $S = 4$.

Using an approach similar to that described above, we obtained results by defining the set $D = \{d_1, d_2, \ldots, d_n\} \subseteq GF(q)$, such that d_i are all nonzero powers of 5 in a field $GF(q)$ and $q = p^m$. The results are given in Table 4.

Table 4. Two-weight trace codes from powers of 5.

p, q, m	Code	Weight Dist.	Corr. Proj. Code	SRG
$3, 81, 4$	$[16, 4, 6]_3$	$< 0, 1 >, < 6, 16 >, < 12, 64 >$	$[8, 4, 3], d^{\perp} = 3$	(81,16,7,2)
$7, 2401, 4$	$[480, 4, 378]_7$	$< 0, 1 >, < 378, 480 >, < 420, 1920 >$	$[80, 4, 63], d^{\perp} = 3$	(2401,480,119,90)
$13, 28561, 4$	$[5712, 4, 5148]_{13}$	$< 0, 1 >, < 5148, 5712 >, < 5304, 22848 >$	$[476, 4, 429], d^{\perp} = 3$	(28561,5712,1223,1122)
$19, 361, 2$	$[72, 2, 54]_{19}$	$< 0, 1 >, < 54, 72 >, < 72, 288 >$	$[4, 2, 3]^*, d^{\perp} = 3$	(361,72,23,12)

Remark 4. *The SRG(81,16,7,2) is a unique strongly regular graph with these parameters. The SRG with parameters (81,16,7,2) is isomorphic to the SRG obtained from the projective ternary [8,4] code with weights 3, 6 (see Reference [13]). The code* $[16, 4, 6]_3$ *is two copies of the above-mentioned projective* $[8, 4, 3]$ *code. Further, we have constructed an SRG with parameters (361,72,23,12), and according to Brouwer's table (see Reference [22]), a known graph with these parameters is obtainable from the orthogonal array. Moreover, SRG(2401,480,119,90) and SRG(28561,5712,1223,1122) have parameters that correspond to SRGs that can be obtained from orthogonal arrays* $OA(49, 10)$ *and* $OA(169, 34)$*, respectively.*

Using an approach similar to that described above, we obtained results by defining the set $D = \{d_1, d_2, \ldots, d_n\} \subseteq GF(q)$, such that d_i are all nonzero powers of 6 in a field $GF(q)$ and $q = p^m$. The results are given in Table 5.

Table 5. Two-weight trace codes from powers of 6.

p, q, m	Code	Weight Dist.	Corr. Proj. Code	SRG
$3, 9, 2$	$[4, 2, 2]_3$	$< 0, 1 >, < 2, 4 >, < 4, 4 >$	$[2, 2, 1]^*, d^\perp = 2$	(9,4,1,2)
$3, 81, 4$	$[40, 4, 24]_3$	$< 0, 1 >, < 24, 40 >, < 30, 40 >$	$[20, 4, 12]^*, d^\perp = 3$	(81,40,19,20)
$3, 729, 6$	$[364, 6, 236]_3$	$< 0, 1 >, < 234, 364 >, < 252, 364 >$	$[182, 6, 117], d^\perp = 3$	(729,364,181,182)
$5, 625, 4$	$[104, 4, 80]_5$	$< 0, 1 >, < 80, 520 >, < 100, 104 >$	$[26, 4, 20]^*, d^\perp = 4$	(625,104,3,20)
$5, 15625, 6$	$[2604, 6, 2000]_5$	$< 0, 1 >, < 2000, 2604 >, < 2100, 13020 >$	$[651, 6, 500], d^\perp = 3$	(15625,2604,503,420)
$7, 49, 2$	$[8, 2, 6]_7$	$< 0, 1 >, < 6, 24 >, < 8, 24 >$	$[4, 2, 3]^*, d^\perp = 3$	(49,24,11,12)
$7, 2401, 4$	$[400, 4, 336]_7$	$< 0, 1 >, < 336, 1200 >, < 350, 1200 >$	$[200, 4, 168], d^\perp = 3$	(2401,1200,599,600)
$11, 121, 2$	$[20, 2, 10]_{11}$	$< 0, 1 >, < 10, 20 >, < 20, 100 >$	$[2, 2, 1]^*, d^\perp = 2$	(121,20,9,2)
$11, 14641, 4$	$[2440, 4, 2200]_{11}$	$< 0, 1 >, < 2200, 12200 >, < 2310, 2440 >$	$[244, 4, 220]^*, d^\perp = 3$	(14641,2440,420,341)
$13, 169, 2$	$[28, 2, 24]_{13}$	$< 0, 1 >, < 24, 84 >, < 28, 84 >$	$[7, 2, 6]^*, d^\perp = 3$	(169,84,41,42)
$13, 28561, 4$	$[4760, 4, 4368]_{13}$	$< 0, 1 >, < 4368, 14280 >, < 4420, 14280 >$	$[1190, 4, 1092], d^\perp = 3$	(28561,14280,7139,7140)
$17, 289, 2$	$[48, 2, 32]_{17}$	$< 0, 1 >, < 32, 48 >, < 48, 240 >$	$[3, 2, 2]^*, d^\perp = 3$	(289,48,17,6)
$19, 361, 2$	$[60, 2, 54]_{19}$	$< 0, 1 >, < 54, 180 >, < 60, 180 >$	$[10, 2, 9]^*, d^\perp = 3$	(361,180,89,90)

Remark 5. *The SRG(121,20,9,2) is a unique SRG with these parameters. SRGs with parameters (9,4,1,2), (81,40,19,20), (729,364,181,182), (49,24,11,12), (2401,1200,599,600), (169,84,41,42), (28561,14280,7139,7140) and (361,180,89,90) are Paley graphs. Further, we have constructed an SRG with parameters (625,104,3,20), which is isomorphic to the graph described in Reference [22]. Moreover, we have constructed an SRG with parameters (289,48,17,6) and according to Brouwer's table (see Reference [22]) a known graph with these parameters is obtainable from orthogonal array. The SRG(15625,2604,503,420) has parameters that correspond to an SRG that can be obtained from an orthogonal array $OA(125, 21)$. The SRG(14641,2440,420,341) is isomorphic to the graph obtained by CY2 construction (see Reference [23]), for $q = 11$ and $S = 4$.*

3.2. Codes Obtained from Fields of Even Order

Using an approach similar to that described above, we obtained results by defining the set $D = \{d_1, d_2, \ldots, d_n\} \subseteq GF(q)$, such that d_i are all nonzero powers of s in a field $GF(2)$ and $q = 2^m$ such that $s|(2^m - 1)$.

In Table 6, we describe two-weight projective binary codes.

Table 6. Two-weight binary trace codes from nonzero powers of 3, 5 and 6.

p, q, m	s	Code	Weight Dist.	SRG
2,16, 4	3,6	$[5, 4, 2]_2^*, d^\perp = 5$	$< 0, 1 >, < 2, 10 >, < 4, 5 >$	(16,5,0,2)
2,64, 6	3,6	$[21, 6, 8]_2, d^\perp = 3$	$< 0, 1 >, < 8, 21 >, < 12, 42 >$	(64,21,8,6)
2,256, 8	3,6	$[85, 8, 40]_2^*, d^\perp = 3$	$< 0, 1 >, < 40, 170 >, < 48, 85 >$	(256,85,24,30)
2,256, 8	5	$[51, 8, 24]_2^*, d^\perp = 3$	$< 0, 1 >, < 24, 204 >, < 32, 51 >$	(256,51,2,12)
2,1024, 10	3,6	$[341, 10, 160]_2, d^\perp = 3$	$< 0, 1 >, < 160, 341 >, < 176, 682 >$	(1024,341,120,110)
2,4096, 12	3,6	$[1365, 12, 672]_2, d^\perp = 3$	$< 0, 1 >, < 672, 2730 >, < 704, 1365 >$	(4096,1365,440,462)
2,4096, 12	5	$[819, 12, 348]_2, d^\perp = 3$	$< 0, 1 >, < 384, 819 >, < 416, 3276 >$	(4096,819,194,156)

Remark 6. *Strongly regular graphs with parameters (16,5,0,2), (64,21,8,6), (256,85,24,30), (1024,341,120,110) and (256,51,2,12) are isomorphic to the graphs described in Reference [22]. The graph with parameters* $(4096, 1365, 440, 462)$ *is isomorphic to the graph obtained by CY1 construction and the graph* $(4096, 819, 194, 156)$ *is isomorphic to the graph obtained by CY4 construction (see Reference [23]).*

Using an approach similar to that described above, we obtained results by defining the set $D = \{d_1, d_2, \ldots, d_n\} \subseteq GF(q)$, such that d_i are all nonzero powers of s in a field $GF(4)$ and $q = 4^m$ such that $s|(4^m - 1)$.

In Table 7 we describe two-weight quaternary codes. Notice that in these cases, some of the obtained two-weights codes have odd dimension, which was not the case in the previous section.

Table 7. Two-weight quaternary trace codes.

p, q, m	s	Code	Weight Dist.	Corr. Proj. Code	SRG
4,64, 3	3	$[21, 3, 12]_4$	$< 0,1 >, < 12,21 >, < 18,42 >$	$[7, 3, 4]^*$, $d^\perp = 3$	(64,21,8,6)
4,64, 3	9	$[7, 3, 4]_4^*$	$< 0,1 >, < 4,21 >, < 6,42 >, d^\perp = 3$		(64,21,8,6)
4,256, 4	5	$[51, 4, 36]_4$	$< 0,1 >, < 36,204 >, < 48,51 >$	$[17, 4, 12]^*$, $d^\perp = 4$	(256,51,2,12)
4,256, 4	15	$[17, 4, 12]_4^*$	$< 0,1 >, < 12,204 >, < 6,51 >, d^\perp = 4$		(256,51,2,12)
4,1024, 5	11	$[93, 5, 48]_4$	$< 0,1 >, < 48,93 >, < 72,930 >$	$[31, 5, 16]$, $d^\perp = 3$	(1024,93,32,6)
4,1024, 5	33	$[31, 5, 16]_4$	$< 0,1 >, < 16,93 >, < 24,930 >, d^\perp = 3$		(1024,93,32,6)
4,4096, 6	3	$[1365, 6, 1008]_4$	$< 0,1 >, < 1008,2730 >, < 1056,1365 >$	$[455, 6, 336]$, $d^\perp = 3$	(4096,1365,440,462)
4,4096, 6	5	$[819, 6, 576]_4$	$< 0,1 >, < 576,819 >, < 624,3276 >$	$[273, 6, 192]$, $d^\perp = 3$	(4096,819,194,156)
4,4096, 6	9	$[455, 6, 336]_4$	$< 0,1 >, < 1336,2730 >, < 352,1365 >, d^\perp = 3$		(4096,1365,440,462)
4,4096, 6	13	$[315, 6, 192]_4$	$< 0,1 >, < 192,315 >, < 240,3780 >$	$[105, 6, 64]$, $d^\perp = 3$	(4096,315,74,20)
4,16384, 7	43	$[381, 7, 192]_4$	$< 0,1 >, < 192,381 >, < 288,16002 >$	$[127, 7, 64]$, $d^\perp = 3$	(16384,381,128,6)
4,16384, 7	129	$[127, 7, 64]_4$	$< 0,1 >, < 64,381 >, < 96,16002 >, d^\perp = 3$		(16384,381,128,6)

Remark 7. *SRGs with parameters (64,21,8,6), (256,51,2,12) and (1024,93,32,6) are isomorphic to the graphs described in Reference [22]. The graph with parameters* $(4096, 819, 194, 156)$ *is isomorphic to the graph obtained by CY1 construction (see Reference [23]). The graph with parameters* $(4096, 1365, 440, 462)$ *is isomorphic to the graph obtained by CY4 construction, although corresponding projective codes are not isomorphic and cannot be obtained by CY4 construction. The graph with parameters* $(4096, 315, 74, 20)$ *is isomorphic to the graph obtained by CY4 construction. The strongly regular graph (16384,381,128,6) has parameters that correspond to the SRG that can be obtained from a orthogonal array* $OA(128, 3)$.

The codes described in Table 7 are a good source for obtaining quantum codes (see References ([25–27])). The case where $q = 4$ is motivated by the construction of quantum-error-correcting codes from Hermitian self-orthogonal linear $GF(4)$ codes. In particular, given a Hermitian self-orthogonal $[n, k]_4$ code C such that no codeword in $C^\perp \setminus C$ has a weight less than d, one can construct a quantum $[n, n - 2k, d]$ code, (see Reference [25] Theorems 2, 3). Projective codes from Table 7 give rise to quantum codes over $GF(4)$. According to the Grassl table [17], these quantum codes are optimal or near optimal. Our construction is different from the constructions given in Reference [17], so our codes are probably new.

Using an approach similar to that described above, we obtained results by defining the set $D = \{d_1, d_2, \ldots, d_n\} \subseteq GF(q)$, such that d_i are all nonzero powers of s in a field $GF(8)$ and $q = 8^m$ such that $s|(8^m - 1)$.

Remark 8. *The SRGs described in Table 8 are isomorphic to the SRGs described in Reference [23] by CY1 and CY4 constructions—the SRGs with parameters (4096,1365,440,462) and (4096,455,6,56) by CY1 construction, and the SRGs with parameters (4096,819,194,156) and (4096,315,74,20) by CY4 construction.*

Table 8. Two-weight trace codes over $GF(8)$.

p, q, m	s	Code	Weight Dist.	Corr. Proj. Code	SRG
8,4096, 4	3	$[1365, 4, 1176]_8$	$< 0, 1 >, < 1176, 2730 >, < 1232, 1365 >$	$[195, 4, 168]$, $d^{\perp} = 3$	(4096,1365,440,462)
8,4096, 4	5	$[819, 4, 672]_8$	$< 0, 1 >, < 672, 819 >, < 728, 3276 >$	$[117, 4, 96]$, $d^{\perp} = 3$	(4096,819,194,156)
8,4096, 4	9	$[455, 4, 392]_8$	$< 0, 1 >, < 392, 3640 >, < 448, 455 >$	$[65, 4, 56]^*$, $d^{\perp} = 4$	(4096,455,6,56)
8,4096, 4	13	$[315, 4, 224]_8$	$< 0, 1 >, < 224, 315 >, < 280, 3780 >$	$[45, 4, 32]$, $d^{\perp} = 3$	(4096,315,74,20)

4. Support Designs and Generalized Block Graphs

In this section, we describe support designs and generalized block graphs obtained from the codes described in Section 3. In Section 3 we presented SRGs constructed from two-weight codes but in this section we construct combinatorial structures from codes with more weights too.

The support of a nonzero vector $x = (x_1, ..., x_n) \in F_q^n$ is the set of indices of its nonzero coordinates, that is, $\mathrm{supp}(x) = \{i | x_i \neq 0\}$. The support design of a code of length n for a given nonzero weight w is the design with points the n coordinate indices and blocks the supports of all codewords of weight w.

From the supports of all codewords of minimum weight of the one-weight codes we obtain the family of symmetric designs (see Reference [28] for more information), known as point-hyperplane designs. Since all linear 1-weight codes are characterized (see References [10,11] we did not include that family in Table 9, so in Table 9 we give designs obtained as support designs of the codes with more than one weight.

Table 9. Support designs.

p, q, m	s	Code	Weight Dist.	Support Design
3,81,4	4	$[10, 4, 6]_3$	$< 0, 1 >, < 6, 60 >, < 9, 20 >$	3-(10,4,1), $b = 30$
5,625,4	6	$[26, 4, 20]_5$	$< 0, 1 >, < 20, 520 >, < 25, 100 >$	3-(26,6,1), $b = 130$
4,64,3	9	$[7, 3, 4]_4$	$< 0, 1 >, < 4, 21 >, < 6, 42 >$	2-(7,3,1), $b = 7$
4,256,4	5	$[17, 4, 12]_4$	$< 0, 1 >, < 12, 204 >, < 16, 51 >$	3-(17,5,1), $b = 68$
4,1024,5	11	$[31, 5, 16]_4$	$< 0, 1 >, < 16, 93 >, < 24, 930 >$	2-(31,15,7), $b = 31$
4,1024,5	11	$[31, 5, 16]_4$	$< 0, 1 >, < 16, 93 >, < 24, 930 >$	2-(31,7,7), $b = 155$
4,1024,5	31	$[11, 5, 6]_4$	$< 0, 1 >, < 6, 155 >, < 7, 165 >, < 8, 165 >, < 9, 330 >, < 10, 165 >, < 11, 33 >$	2-(11,5,10), $b = 55$
4,1024,5	31	$[11, 5, 6]_4$	$< 0, 1 >, < 6, 155 >, < 7, 165 >, < 8, 165 >, < 9, 330 >, < 10, 165 >, < 11, 33 >$	2-(11,3,3), $b = 55$
4,1024,5	31	$[11, 5, 6]_4$	$< 0, 1 >, < 6, 155 >, < 7, 165 >, < 8, 165 >, < 9, 330 >, < 10, 165 >, < 11, 33 >$	2-(11,4,6), $b = 55$
4,16384,7	129	$[127, 7, 64]_4$	$< 0, 1 >, < 64, 381 >, < 96, 16002 >$	2-(127,63,31), $b = 127$
4,16384,7	129	$[127, 7, 64]_4$	$< 0, 1 >, < 16, 93 >, < 24, 930 >$	2-(127,31,155), $b = 2667$
8,4096,4	45	$[13, 4, 9]_8$	$< 0, 1 >, < 9, 364 >, < 10, 546 >, < 11, 1092 >, < 12, 1365 >, < 13, 728 >$	2-(13,4,4), $b = 52$
8,4096,4	45	$[13, 4, 9]_8$	$< 0, 1 >, < 9, 364 >, < 10, 546 >, < 11, 1092 >, < 12, 1365 >, < 13, 728 >$	2-(13,3,3), $b = 78$
8,4096,6	9	$[65, 4, 56]_8$	$< 0, 1 >, < 56, 3640 >, < 64, 455 >$	3-(65,9,1), $b = 520$

Remark 9. *The designs 2-(31,7,7), $b = 155$ and 2-(127,31,155), $b = 2667$ from Table 9 are quasi-symmetric designs with intersection numbers $\{1, 3\}$ and $\{7, 15\}$, respectively (see Reference [29]).*

The following construction of graphs from support designs has been described in Reference [14]. Let $S = \{|x \cap y| \; x, y \in \mathcal{B}\}$, where $\mathcal{B}$ is the block set of the support design and let $A \subset S$. One can define a graph whose vertices are the elements of the block set $\mathcal{B}$ of the support design and two vertices are adjacent if the size of the intersection of the corresponding blocks is an element of A. This construction is a generalization of the construction of the block graph from a quasi-symmetric design, so we call a graph constructed in that way a generalized block graph.

In Table 10 we list distance regular graphs, including strongly regular graphs, constructed from support designs of the codes constructed by applying the construction described in Section 3.

Table 10. Generalized block graphs.

p, q, m	s	Code	Weight Dist.	Gen. Block Graph
2,16,4	3,6	$[5,4,2]_2$	$<0,1>,<2,10>,<4,5>$	SRG(10,3,0,1)
3,81,4	4	$[10,4,6]_3$	$<0,1>,<6,60>,<9,20>$	DRG, $v=30$, $[3,2,2,2;1,1,1,3]$
3,81,4	5	$[8,4,3]_3$	$<0,1>,<3,16>,<6,64>$	SRG(16,6,2,2)
4,256,4	5	$[17,4,12]_4$	$<0,1>,<12,204>,<16,51>$	DRG, $v=68$, $[12,10,3;1,3,8]$
4,1024,5	11	$[31,5,16]_4$	$<0,1>,<16,93>,<24,930>$	SRG(155,42,17,9)
4,1024,5	31	$[11,5,6]_4$	$<0,1>,<6,155>,<7,165>,<8,165>,$ $<9,330>,<10,165>,<11,33>$	SRG(55,18,9,4)
4,16384,7	129	$[127,7,64]_4$	$<0,1>,<64,381>,<96,16002>$	SRG(2667,186,65,9)
8,4096,4	45	$[13,4,9]_8$	$<0,1>,<9,364>,<10,546>,$ $<11,1092>,<12,1365>,<13,728>$	SRG(78,22,11,4)
8,4096,4	15	$[39,4,30]_8$	$<0,1>,<30,546>,<33,1092>,$ $<35,1092>,<36,1365>$	SRG(169,36,13,6)

Remark 10. *SRG(10,3,0,1) is the unique graph with these parameters, known as the Petersen graph. SRG(16,6,2,2) is isomorphic to the graph described in Reference [22], constructed from projective* $[6,4,2]_2$ *code with weights 2, 4. SRGs with parameters (55,18,9,4) and (78,22,11,4) are triangular graphs* $T(11)$ *and* $T(13)$*, respectively. The strongly regular graph (169,36,13,6) has parameters that correspond to the SRG that can be obtained from orthogonal array* $OA(13,3)$*. The graphs with parameters (155,42,17,9) and (2667,186,65,9) are block graphs of the quasi-symmetric designs constructed in Table 9. The distance regular graph on 30 vertices of diameter 4 is the unique graph with this intersection array and is called Tutte's 8-cage. Further, the distance regular graph on 68 vertices of diameter 3 is the unique graph with this intersection array and is called Doro graph. For more information we refer the reader to Reference [21].*

Author Contributions: This is a joint collaboration with all three authors contributing substantially throughout.

Funding: Dean Crnković and Andrea Švob were funded by Croatian Science Foundation under the project 6732.

Acknowledgments: We thank the reviewers for carefully reading the manuscript and making several useful remarks.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Ding, C. A construction of binary linear codes from Boolean functions. *Discret. Math.* **2016**, *339*, 2288–2303. [CrossRef]
2. Ding, C.; Niederreiter, H. Cyclotomic linear codes of order 3. *IEEE Trans. Inf. Theory* **2007**, *53*, 2274–2277. [CrossRef]
3. Ding, C.; Luo, J.; Niederreiter, H. Two weight codes punctured from irreducible cyclic codes. In Proceedings of the First International Workshop on Coding Theory and Cryptography, Wuyi Mountain, China, 11–15 June 2007; pp. 119–124.
4. Shi, M.; Qian, L.; Solé, P. Few-weight codes from trace codes over a local ring. *Appl. Algebra Eng. Commun. Comput.* **2018**, *29*, 335–350. [CrossRef]
5. Wang, X.; Zheng, D.; Liu, H. Several classes of linear codes and their weight distributions. *Appl. Algebra Eng. Commun. Comput.* **2019**, *30*, 75–92. [CrossRef]

6. Zhou, Z. Three-weight ternary linear codes from a family of cyclic difference sets. *Des. Codes Cryptogr.* **2018**, *86*, 2513–2523. [CrossRef]
7. Ding, C. Linear Codes from Some 2-Designs. *IEEE Trans. Inf. Theory* **2015**, *61*, 3265–3275. [CrossRef]
8. Olmez, O. A link between combinatorial designs and three-weight linear codes. *Des. Codes Cryptogr.* **2018**, *86*, 817–833. [CrossRef]
9. Bonisoli, A. Every equidistant code is a sequence of dual Hamming codes. *Ars Combinatoria* **1983**, *18*, 181–186.
10. Jungnickel, D.; Tonchev, V.D. The classification of antipodal two-weight linear codes. *Finite Fields Appl.* **2018**, *50*, 372–381. [CrossRef]
11. Jungnickel, D.; Tonchev, V.D. On Bonisoli's theorem and the block codes of Steiner triple systems. *Des. Codes Cryptogr.* **2018**, *86*, 449–462. [CrossRef]
12. Ding, C.; Munemasa, A.; Tonchev, V.D. Bent Vectorial Functions, Codes and Designs. *IEEE Trans. Inf. Theory* **2019**. [CrossRef]
13. Brouwer, A.E. Some new two-weight codes and strongly regular graphs. *Discrete Appl. Math.* **1985**, *10*, 111–114. [CrossRef]
14. Crnković, D.; Mikulić, V. Self-orthogonal doubly-even codes from Hadamard matrices of order 48. *Adv. Appl. Discret. Math.* **2008**, *1*, 159–170.
15. Bosma, W.; Cannon, J. *Handbook of Magma Functions*; Department of Mathematics, University of Sydney: Sydney, NWS, Australia, 1994.
16. Huffman, W.C.; Pless, V. *Fundamentals of Error-Correcting Codes*; Cambridge University Press: Cambridge, UK, 2003.
17. Grassl, M. Bounds on the Minimum Distance of Linear Codes and Quantum Codes. Available online: http://www.codetables.de (accessed on 11 August 2019).
18. Brouwer, A.E. Strongly Regular Graphs. In *Handbook of Combinatorial Designs*, 2nd ed.; Colbourn, C.J., Dinitz, J.H., Eds.; Chapman & Hall/CRC: Boca Raton, FL, USA, 2007; pp. 852–868.
19. Shrikhande, M.S.; Sane, S.S. *Quasi-Symmetric Designs*; Cambridge University Press: Cambridge, UK, 1991.
20. Tonchev, V.D. *Combinatorial Configurations: Designs, Codes, Graphs*; John Willey & Sons: New York, NY, USA, 1988.
21. Brouwer, A.E.; Cohen, A.M.; Neumaier, A. *Distance-Regular Graphs*; Springer: Berlin, Germany, 1989.
22. Brouwer, A.E. Parameters of Strongly Regular Graphs. Available online: http://www.win.tue.nl/$\sim$aeb/graphs/srg/srgtab.html (accessed on 24 May 2019).
23. Calderbank, A.R.; Kantor, W.M. The geometry of two-weight codes. *Bull. Lond. Math. Soc.* **1986**, *118*, 97–122. [CrossRef]
24. Brouwer, A.E.; Haemers, W.H. Structure and uniqueness of the (81,20,1,6) strongly regular graph. *Discret. Math.* **1992**, *106/107*, 77–82. [CrossRef]
25. Calderbank, A.R.; Rains, E.M.; Shor, P.W.; Sloane, N.J.A. Quantum error correction via codes over $GF(4)$. *IEEE Trans. Inf. Theory* **1998**, *44*, 1369–1387. [CrossRef]
26. Shor, P.W. Scheme for reducing decoherence in quantum computer memory. *Phys. Rev. A* **1995**, *52*, R2493. [CrossRef] [PubMed]
27. Tonchev, V.D. Quantum codes from caps. *Discret. Math.* **2008**, *308*, 6368–6372. [CrossRef]
28. Ionin, Y.J.; van Trung, T. Symmetric Designs. In *Handbook of Combinatorial Designs*, 2nd ed.; Colbourn, C.J., Dinitz, J.H., Eds.; Chapman & Hall/CRC: Boca Raton, FL, USA, 2007; pp. 110–124.
29. Shrikhande, M.S. Quasi-Symmetric Designs. In *Handbook of Combinatorial Designs*, 2nd ed.; Colbourn, C.J., Dinitz, J.H., Eds.; Chapman & Hall/CRC: Boca Raton, FL, USA, 2007; pp. 578–582.