Applicable Algebra in Engineering, Communication and Computing (2022) 33:855–866
https://doi.org/10.1007/s00200-022-00543-w

ORIGINAL PAPER

Quasi-symmetric 2-(41, 9, 9) designs and doubly even self-dual codes of length 40

Akihiro Munemasa[1] · **Vladimir D. Tonchev**[2]

Received: 30 November 2021 / Accepted: 27 January 2022 / Published online: 10 February 2022

Abstract

The existence of a quasi-symmetric 2-(41, 9, 9) design with intersection numbers $x = 1, y = 3$ is a long-standing open question. Using linear codes and properties of subdesigns, we prove that a cyclic quasi-symmetric 2-(41, 9, 9) design does not exist, and if $p < 41$ is a prime number being the order of an automorphism of a quasi-symmetric 2-(41, 9, 9) design, then $p \leq 5$. The derived design with respect to a point of a quasi-symmetric 2-(41, 9, 9) design with block intersection numbers 1 and 3 is a quasi-symmetric 1-(40, 8, 9) design with block intersection numbers 0 and 2. The incidence matrix of the latter generates a binary doubly even code of length 40. Using the database of binary doubly even self-dual codes of length 40 classified by Betsumiya et al. (Electron J Combin 19(P18):12, 2012), we prove that there is no quasi-symmetric 2-(41, 9, 9) design with an automorphism ϕ of order 5 with exactly one fixed point such that the binary code of the derived design is contained in a doubly-even self-dual [40, 20] code invariant under ϕ.

Keywords Quasi-symmetric design · Subdesign · Cyclic code · Self-dual code · Automorphism group

Mathematics Subject Classification 05B05 · 05B20 · 94B05

1 Preliminaries

We assume some basic familiarity with combinatorial designs and algebraic coding theory (cf. e.g. [1, 7, 12]).

✉ Vladimir D. Tonchev
tonchev@mtu.edu

1 Graduate School of Information Sciences, Tohoku University, Sendai, Japan

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

Given integers $v \geq k \geq 2$, $\lambda > 0$, a 2-(v, k, λ) *design* is a pair $\mathcal{D} = (X, \mathcal{B})$ of a set $X = \{x_i\}_{i=1}^{v}$ of v *points*, and a collection $\mathcal{B} = \{B_j\}_{j=1}^{b}$ of k-subsets $B_j \subseteq X$, called *blocks* such that every two points appear together in exactly λ blocks.

The *points by blocks* incidence matrix $A = (a_{i,j})$ of a design $\mathcal{D}$ with v points and b blocks is a $v \times b$ (0, 1)-matrix with $a_{i,j} = 1$ if the ith point belongs to the jth block, and $a_{i,j} = 0$ otherwise. The transposed matrix A^T is called the *blocks by points* incidence matrix of $\mathcal{D}$. The dual design $\mathcal{D}^*$ of $\mathcal{D}$ is the design with incidence matrix A^T.

The *derived design* $\mathcal{D}^x$ of a 2-(v, k, λ) design $\mathcal{D} = (X, \mathcal{B})$ with respect to a point $x \in X$ is a 1-$(v-1, k-1, \lambda)$ design with point set $X \setminus \{x\}$, and blocks $B \setminus \{x\}$, $B \in \mathcal{B}, x \in B$. If a given 1-$(v-1, k-1, \lambda)$ design $\mathcal{D}'$ is a derived design of a 2-(v, k, λ) design, we call $\mathcal{D}'$ *extendable*. The *residual design* $\mathcal{D}_x$ with respect to $x \in X$ is a 1-$(v-1, k, r-\lambda)$ design with point set $X \setminus \{x\}$, and blocks $B \in \mathcal{B}, x \notin B$, where $r = \lambda(v-1)/(k-1)$ is the number of blocks that contain x.

If $\mathcal{D}$ is a 2-(v, k, λ) design with $v > k > 0$, the number of blocks $b = v(v-1)\lambda/(k(k-1))$ satisfies the Fisher inequality

$$b \geq v, \tag{1}$$

and the equality $b = v$ holds if and only if every two blocks share exactly λ points. A 2-(v, k, λ) design D with $b = v$ is called *symmetric*.

A 2-(v, k, λ) design D with $b > v$ is *quasi-symmetric* with intersection numbers x, y $(0 \leq x < y)$ if every two blocks share either x or y points. Quasi-symmetric designs were introduced by Shrikhande and Bhagwandas [11].

A *strongly regular graph* with parameters $\bar{n}, \bar{k}, \bar{\lambda}, \bar{\mu}$ is an undirected graph with $\bar{n}$ vertices, having no multiple edges or loops, such that: every vertex has exactly $\bar{k}$ neighbors, every two adjacent vertices have exactly $\bar{\lambda}$ common neighbors, and every two non-adjacent vertices have exactly $\bar{\mu}$ common neighbors. Strongly regular graphs were introduced by Bose [3]. It was proved by Shrikhande and Bhagwandas [11] that if $\mathcal{D}$ is a quasi-symmetric 2-(v, k, λ) design with intersection numbers x, y, $(0 \leq x < y)$, then the graph Γ having as vertices the blocks of $\mathcal{D}$, where two blocks are adjacent in Γ if they share exactly x points, is strongly regular.

A 2-(v, k, λ) design is called *strongly resolvable* with intersection numbers x, y $(0 \leq x < y)$ if its set of blocks can be partitioned into disjoint subsets in such a way that every two blocks which belong to the same subset intersect each other in exactly x points, while every two blocks that belong to different subsets intersect each other in y points. An example of a strongly resolvable design with $x = 0, y = q^{n-2}$ is the design $AG_{n-1}(n, q)$ with parameters 2-$(q^n, q^{n-1}, (q^{n-1}-1)/(q-1))$ having as points and blocks the points and hyperplanes in the n-dimensional finite affine geometry $AG(n, q)$ over a finite field of order q. The block graph of a strongly resolvable design is a union of disjoint complete graphs.

Some instant examples of quasi-symmetric designs are the following:

1. the union of several identical copies of a symmetric 2-(v, k, λ) design ($x = \lambda$, $y = k$);
2. any non-symmetric 2-$(v, k, 1)$ design ($x = 0$, $y = 1$);
3. any strongly resolvable design;
4. any 2-$((k+1)k/2, k, 2)$ design ($x = 1$, $y = 2$).

A quasi-symmetric 2-(v, k, λ) design with $k \leq v/2$ is called *exceptional* if it does not belong to any of the above four categories [9]. A table of admissible parameters for exceptional quasi-symmetric designs with number of points $v \leq 70$ is given in [10]. There are 73 feasible parameter sets for exceptional quasi-symmetric designs with $v \leq 70$ points [10, Table 48.25]. Currently, the existence (or nonexistence) question has been resolved for 40 out of the 73 feasible parameter sets, while the existence of a quasi-symmetric design in each of the remaining 33 cases is an open question. In 26 of the 40 resolved cases, linear codes, and self-dual codes in particular, have played a crucial role in establishing the existence, nonexistence or the classification up to isomorphism of the quasi-symmetric designs with the given parameters.

The existence of a quasi-symmetric 2-(41, 9, 9), ($x = 1$, $y = 3$) is an open question. This is one of the 33 remaining open cases for plausible exceptional quasi-symmetric designs with $v \leq 70$ points. In this paper, we prove that a cyclic quasi-symmetric 2-(41, 9, 9) design does not exist, and if $p < 41$ is a prime number being the order of an automorphism of a quasi-symmetric 2-(41, 9, 9) design, then $p \leq 5$. We also prove the nonexistence of a quasi-symmetric 2-(41, 9, 9) design with an automorphism ϕ of order 5 with exactly one fixed point such that the binary code of the derived design is contained in a doubly-even self-dual [40, 20] code invariant under ϕ. This may be considered as a first step to prove the nonexistence of a quasi-symmetric 2-(41, 9, 9) design with block intersection numbers 1 and 3, and an analogue of the previous work [4, 5] for quasi-symmetric 2-(37, 9, 8) designs with block intersection numbers 1 and 3.

The organization of this paper is as follows. In Sect. 2, we investigate automorphisms of 2-designs in general. It is shown that (not necessarily quasi-symmetric) 2-(41, 9, 9) design can admit an automorphism of prime order p only if $p = 41$ or $p \leq 7$. In Sect. 3, we show that $p = 41$ and $p = 7$ cannot occur as the order of an automorphism of a quasi-symmetric 2-(41, 9, 9) design. In Sect. 4, we show that $p = 5$ cannot occur as the order of an automorphism of a quasi-symmetric 2-(41, 9, 9) design, under mild conditions (see Theorem 4.5 for the exact assumption).

2 Automorphisms of 2-(41, 9, 9) designs

In this section we investigate the spectrum of prime numbers that could be the order of an automorphism of a 2-(41, 9, 9) design.

Definition 2.1 A 2-(v_0, k, λ) design $\mathcal{D}_0 = (X_0, \mathcal{B}_0)$ is a *subdesign* of a 2-(v, k, λ) design $\mathcal{D} = (X, \mathcal{B})$ if $X_0 \subseteq X$ and $\mathcal{B}_0 \subseteq \mathcal{B}$.

The following statement is given without a proof in [8, II.1.4, page 25].

Lemma 2.2 *If a* 2-(v, k, λ) *design* $\mathcal{D}$ *with* $k \geq 2$ *contains a* 2-(v_0, k, λ) *subdesign* $\mathcal{D}_0$ *then either* $v_0 = v$ *or*

$$v_0 \leq \frac{v-1}{k-1}. \tag{2}$$

Proof Every point of $\mathcal{D}_0$ is contained in $r - r_0$ blocks of $\mathcal{D}$ that are not blocks of $\mathcal{D}_0$. If x, y are two distinct points of $\mathcal{D}_0$ then the set S_x of $r - r_0$ blocks of $\mathcal{D}$ that are not blocks of $\mathcal{D}_0$ and contain x, and the set S_y of $r - r_0$ blocks of $\mathcal{D}$ that are not blocks of $\mathcal{D}_0$ and contain y, are disjoint: $S_x \cap S_y = \emptyset$. Thus, we have

$$v_0(r - r_0) \leq b - b_0. \tag{3}$$

After the substitutions $r = \lambda(v-1)/(k-1)$, $r_0 = \lambda(v_0 - 1)/(k-1)$, $b = \lambda v(v-1)/(k(k-1))$, $b_0 = \lambda v_0(v_0 - 1)/(k(k-1))$, the inequality (3) simplifies to

$$(k-1)v_0^2 + (1 - vk)v_0 + v^2 - v \geq 0.$$

The roots of the quadratic polynomial $f(v_0) = (k-1)v_0^2 + (1 - vk)v_0 + v^2 - v$ are $v_0 = v$ and $v_0 = (v-1)/(k-1)$, and the statement of the lemma follows. □

A trivial lower bound on the number of points of a 2-(v_0, k, λ) subdesign is $v_0 \geq k$, which, combined with (2) gives

$$k \leq v_0 \leq \frac{v-1}{k-1}. \tag{4}$$

The inequalities (4) imply the following.

Corollary 2.3 *A necessary condition for a* 2-(v, k, λ) *design to have a subdesign with* $v_0 < v$ *points is that* $k(k-1) + 1 \leq v$.

Lemma 2.4 *Let* $\mathcal{D} = (X, \mathcal{B})$ *be a* 2-(v, k, λ) *design with an automorphism* ϕ *of prime order* p, *such that* p *does not divide* v *and* $p > \lambda$.

(*i*) *If a block* B *contains two distinct points* x, y *which are fixed by* ϕ, *then* B *is fixed by* ϕ.

(*ii*) *Let* $X_0 = \{x \in X \mid x^\phi = x\}$. *Assume that* $v_0 = |X_0| \geq 2$ *and* $p > k$. *Then* X_0 *is the point set of a* 2-(v_0, k, λ) *subdesign of* $\mathcal{D}$ *with* $v_0 < v$.

Proof

(i) If we assume that B is not fixed by ϕ, then x and y must appear together in every of the p distinct blocks from the orbit of B under the cyclic group $< \phi >$, which is impossible because $p > \lambda$.

(ii) Since $p > k$, every block that is fixed by ϕ must consist entirely of fixed points. Now by part (i), if a block B contains two points from X_0 then $B \subseteq X_0$, hence the set of all blocks of $\mathcal{D}$ that are fixed by ϕ form a 2-(v_0, k, λ) subdesign. □

Theorem 2.5

(i) *If* $\mathcal{D}$ *is a* 2-(41, 9, 9) *design that admits an automorphism of prime order* p *then either* $p = 41$ *or* $p \leq 7$.
(ii) *There exists a* 2-(41, 9, 9) *design with automorphism of order* 41.

Proof (i) Assume that $\mathcal{D}$ is a 2-(41, 9, 9) design with an automorphism ϕ of a prime order $p < 41$. Since the number of blocks of $\mathcal{D}$ is $205 = 5 \cdot 41$, if p is in the range $7 < p < 41$ then ϕ must fix at least one block and at least two points. By Lemma 2.4, part (ii) the set X_0 of all points that are fixed by ϕ is the point set of a 2-$(v_0, 9, 9)$ subdesign with $v_0 < 41$. On the other hand, since $9 \cdot 8 + 1 = 73 > 41$, a 2-(41, 9, 9) design $\mathcal{D}$ cannot have any subdesign with $v_0 < 41$ by Corollary 2.3, a contradiction.

(ii) Let $G = AGL(1, 41)$ be the group of order $41 \cdot 40 = 1640$, being the semidirect product of the additive and the multiplicative groups of the finite field of order 41, $Z_{41} = \{0, 1, 2, \ldots, 40\}$. The group G acts as a 2-transitive permutation group on Z_{41} as the set of transformations

$$\{g = (a, b) : \ g(x) = ax + b \pmod{41},\ x \in Z_{41},\ a, b \in Z_{41},\ a \neq 0\}.$$

Since G is 2-transitive, the orbit B^G of any k-subset $B \subset Z_{41}$ with $k \geq 2$ is a 2-$(41, k, \lambda)$ design with $b = |G|/|G_B|$ blocks, where G_B is the setwise stabilizer of B in G, and $\lambda = bk(k-1)/(v(v-1))$. If we choose B to be a 9-subset which is fixed by the subgroup $H =< (3, 0) >$ of order 8, for example, $B = \{0, 1, 3, 9, 27, 40, 38, 32, 14\}$, then $|G_B| = |H| = 8$ and the orbit of B under G is a cyclic 2-(41, 9, 9) design. □

3 Automorphisms of quasi-symmetric 2-(41, 9, 9) designs

In this section we investigate the spectrum of prime numbers that can be the order of an automorphism of a putative quasi-symmetric 2-(41, 9, 9) design with intersection numbers $x = 1, y = 3$.

Theorem 3.1 *A quasi-symmetric* 2-(41, 9, 9) *design with an automorphism of order* 41 *does not exist.*

Proof Let A be the 205×41 blocks by points incidence matrix of a quasi-symmetric 2-(41, 9, 9) design $\mathcal{D} = (X, \mathcal{B})$, and let A^+ be the 205×42 matrix obtained by adding to A one all-one column. The matrix A^+ has constant row sum 10, and the inner product of every two rows of A^+ is an even number (2 or 4). Thus, the rows of A^+

span a binary self-orthogonal code of length 42, hence the rank of A over the binary field, $rank_2 A$, satisfies the inequality

$$rank_2 A \le 21.$$

On the other hand, since A has $205 > 2^7$ rows, we have

$$rank_2 A > 7.$$

Assume now that $\mathcal{D}$ is invariant under the cyclic group of order 41 acting regularly on the point set X, hence the binary linear code L spanned by the rows of A is a cyclic code (for the fundamentals of cyclic codes, see, e.g. [7, Chapter 4]). There are exactly three cyclotomic cosets of 2 modulo 41, namely $\{0\}$, the set Q of the 20 quadratic residues modulo 41, and the set N of the 20 quadratic non-residues modulo 41. Since

$$7 < rank_2 A \le 21,$$

it follows that L is equivalent to the quadratic residue code QR_{41} (see [7, Sec. 6.6]) of length 41 and dimension 21, having a generator polynomial

$$g(x) = x^{20} + x^{18} + x^{17} + x^{16} + x^{15} + x^{14} + x^{11} + x^{10} + x^9 + x^6 + x^5 + x^4 + x^3 + x^2 + 1.$$

The minimum weight of QR_{41} is 9, and the set of all 410 codewords of weight 9 spans the code, hence the full automorphism group of the code coincides with the automorphism group G of the 1-(41, 9, 90) design D having as blocks the supports of the codewords of weight 9. It turns out that D is also a 2-(41, 9, 18) design. The collection of blocks of the 2-(41, 9, 9) design $\mathcal{D}$ gives rise to a bipartition of 410 codewords of weight 9 into two equal parts, where in each part, the supports intersect pairwise in either one or three positions. We define a graph Γ having as vertices the 410 codewords of QR_{41} of minimum weight, where two codewords are adjacent in Γ if their supports share either one or three positions. A quick check by computer shows that the complement of Γ has a 3-cycle, hence is not bipartite. Therefore, a cyclic quasi-symmetric 2-(41, 9, 9) design with intersection numbers $x = 1$, $y = 3$ does not exist.

Note 1 The automorphism group G of QR_{41} is of order 820, and acts as a transitive permutation group of rank 3 on the set of 41 code coordinates. The group G can be viewed also as the automorphism group of the Paley graph $P(41)$ with vertex set $X = \{0, 1, \ldots 40\}$, with vertices corresponding to the code coordinates, where two vertices i, j are adjacent in $P(41)$ if $i - j$ is a quadratic residue modulo 41. The graph $P(41)$ is a strongly regular graph with parameters $\bar{n} = 41$, $\bar{k} = 20$, $\bar{\lambda} = 9$, $\bar{\mu} = 10$. The group G partitions the collection of all unordered 2-subsets of vertices in two orbits: one orbit consists of the edges of $P(41)$, and the second orbit consists of all on-edges. The stabilizer of a minimum weight codeword in G is of order 2, hence all 410 codewords of weight 9 are in one orbit under the action of G. Thus, all blocks of the 1-(41, 9, 90) design D having as blocks the supports of the codewords of weight 9 in the code QR_{41} are in one orbit under the action of G. It is easy to show that D

is actually a 2-(41, 9, 18) design. Indeed, any block of D can be considered as subgraph of the Paley graph $P(41)$. For example, $B = \{1, 3, 9, 15, 17, 18, 21, 38, 41\}$ is a block corresponding to a codeword of QR_{41} with nonzero positions $1, 3, 9, \dots, 41$. Considered as a subgraph of $P(41)$, B contains exactly 18 edges, that is, there are 18 pairs $i, j \in B$, $i < j$ such that $j - i$ is a quadratic residue modulo 41. Now applying Theorem 3.5.1 from [12, p. 166], it follows that D is a 2-$(41, 9, \lambda)$ design with

$$\lambda = \frac{410 \cdot 9 \cdot 8}{41 \cdot 40} = 18.$$

Theorem 3.2 *A quasi-symmetric* 2-(41, 9, 9) *design with intersection numbers* $x = 1$, $y = 3$ *and an automorphism of order 7 does not exist.*

Proof Assume the contrary, and let ϕ be an automorphism of order 7 of a quasi-symmetric 2-(41, 9, 9) design with intersection numbers $x = 1$, $y = 3$. Since the number of points is $41 \equiv 6 \pmod 7$, ϕ fixes at least 6 points. Pick two points p, p' fixed by ϕ. Since there are 9 blocks containing both p and p', ϕ fixes at least two blocks B, B' containing the points p, p'. Since $x = 1$ and $y = 3$, there is another point in $B \cap B'$ which must be fixed by ϕ. Then the remaining six points of B are also fixed by ϕ.

Now let B'' be an arbitrary block sharing three points q, q', q'' with B. If ϕ does not fix B'', then the orbit of B'' under ϕ consists of 7 blocks all of which contain q, q', q''. These blocks are disjoint outside q, q', q'', so we need $7 \cdot (9 - 3) = 42$ points outside B. Since this is impossible, we conclude that ϕ fixes B'', and hence also all the points of B''.

We have shown that, every block sharing three points with a block fixed by ϕ pointwise is also fixed by ϕ pointwise. Since the block graph is a connected strongly regular graph, this implies that ϕ fixes every block pointwise. Thus, ϕ fixes every point, which contradicts the fact that ϕ has order 7.

Theorems 2.5, 3.1 and 3.2 imply the following. □

Theorem 3.3 *If p is a prime number being the order of an automorphism of a quasi-symmetric* 2-(41, 9, 9) *design, then* $p \leq 5$.

4 Quasi-symmetric 2-(41, 9, 9) designs and doubly-even self-dual codes of length 40

Suppose that $\mathcal{D} = (X, \mathcal{B})$ is a quasi-symmetric 2-(41, 9, 9) design with intersection numbers $x = 1, y = 3$. If $z \in X$, the derived 1-(40, 8, 9) design $\mathcal{D}^z$ is a quasi-symmetric design with block intersection numbers $x' = 0, y' = 2$, and the 40×45 points by blocks incidence matrix M of $\mathcal{D}^z$ has the following properties:

1. M has constant row sum 9.
2. M has constant column sum 8.
3. The inner product of any two columns of M is either 0 or 2.

Properties 2 and 3 imply that the binary linear code spanned by the columns of M is a self-orthogonal code L of length 40 with all weights divisible by 4, hence L is contained in some binary doubly-even self-dual code C of length 40. Thus, the column set of M is a set of 45 codewords of C of weight 8, such that properties 1 and 3 hold. Motivated by Theorem 3.3 and to reduce the search, we will assume that the column set of M is a union of orbits of codewords of weight 8 under an automorphism group of C of order 5.

All binary doubly-even self-dual codes of length 40 were classified up to equivalence by Betsumiya et al. [2]. Among the 16,470 doubly even [40, 20, 8] codes, there are 45 codes with an automorphism of order 5 [2]: 44 codes have a full automorphism group of order not divisible by 25 that contains one conjugacy class of fixed-point-free automorphisms of order 5, and there is a unique code with a full automorphism group of order divisible by 25. The automorphism group of the latter code contains fixed-point-free automorphisms of order 5, as well as automorphisms of order 5 with 20 fixed points. With respect to this automorphism ϕ of order 5 with 20 fixed points, the codewords of weight 8 are classified into three types:

1. codewords whose support is contained in the set of 20 fixed points (hence these codewords are fixed by ϕ);
2. codewords whose support is disjoint from the set of 20 fixed points;
3. codewords whose support consists of 4 fixed points and 4 points that are not fixed by ϕ.

If there is a 1-(40, 8, 9) design with intersection numbers $x' = 0$ and $y' = 2$ invariant under ϕ, then its set of blocks contains no blocks of type 3, hence every block is of type 1 or 2. Since the points covered by 1 and 2 are disjoint, this would result in a 1-(20, 8, 9) design. However, such a design does not exist because $20 \cdot 9/8$ is not an integer.

Any doubly-even self-dual [40, 20, 8] code C contains exactly 285 codewords of weight 8 (see, e.g. [6, Subsec. 2.3]), and if the code is invariant under an automorphism ϕ of order 5 without fixed points, the set of 285 codewords of weight 8 is partitioned into 57 orbits of length 5 under the action of $< \phi >$. Any quasi-symmetric 1-(40, 8, 9) design which is invariant under $< \phi >$ and whose blocks are supports of codewords of C, has a 40×45 incidence matrix with column set comprising of nine orbits of codewords of weight 8 under the action of $< \phi >$.

Example 4.1 The following nine 8-sets

$$\begin{array}{rrrrrrrr}
8 & 11 & 12 & 15 & 21 & 26 & 36 & 38\\
1 & 3 & 15 & 19 & 21 & 24 & 30 & 34\\
7 & 12 & 13 & 20 & 24 & 26 & 30 & 31\\
6 & 14 & 19 & 20 & 21 & 25 & 31 & 38\\
1 & 5 & 7 & 10 & 21 & 25 & 26 & 28\\
2 & 8 & 14 & 17 & 24 & 30 & 35 & 38\\
1 & 4 & 6 & 10 & 34 & 35 & 36 & 38\\
7 & 17 & 19 & 20 & 28 & 34 & 35 & 40\\
4 & 5 & 14 & 17 & 26 & 31 & 36 & 40
\end{array}$$

are the base blocks (that is, block orbit representatives) of a quasi-symmetric 1-(40, 8, 9) design $\mathcal{D}'$ with point set $X' = \{1, 2, \dots, 40\}$ and an automorphism ϕ of order 5,

$$\phi = (1, 2, \dots, 5)(5, \dots, 10) \cdots (36, \dots 40),$$

obtained from a doubly-even [40, 20, 8] self-dual code invariant under ϕ.

The 8×9 orbit matrix $M = (m_{i,j})$ of $\mathcal{D}'$ under the action of $< \phi >$, where $m_{i,j}$ is the number of blocks from the jth block orbit that contain a single point from the ith point orbit, is given in (5).

$$\begin{array}{c}
020021202\\
101121210\\
312101001\\
011201031\\
121221000\\
112021011\\
011101221\\
200101212
\end{array} \tag{5}$$

In order to extend the quasi-symmetric 1-(40, 8, 9) design $\mathcal{D}'$ from Example 4.1 to a quasi-symmetric 2-(41, 9, 9) design with intersection numbers 1 and 3, we need to find a matching residual 1-(40, 9, 36) design such that each of its 160 blocks meets every block of $\mathcal{D}'$ in either 1 or 3 points. Surprisingly, an exhaustive computer search shows that there is no 9-subset of X that meets every block of $\mathcal{D}'$ in either 1 or 3 points. This phenomenon can be explained by the following theorem.

Theorem 4.2 *Suppose that $\mathcal{D} = (X, \mathcal{B})$ is a quasi-symmetric 2-(v, k, λ) design with odd intersection numbers x, y. Let $\mathcal{D}^z$ be a derived 1-$(v-1, k-1, \lambda)$ design of $\mathcal{D}$ with respect to a point $z \in X$. Let M be the points by blocks incidence matrix of $\mathcal{D}^z$, and let $\bar{M}$ be the matrix obtained by adding one all-one row to M:*

$$\bar{M} = \begin{pmatrix} & M & \\ 1 & \cdots & 1 \end{pmatrix}.$$

Let $\bar{C}$ be the binary linear code spanned by the columns of $\bar{M}$. If $c \in \bar{C}$ is a code-word with nonzero last position, then

$$wt(c) \geq 1 + \frac{b-r}{r-\lambda},$$

where $b = |\mathcal{B}|$ *and* $r = bk/v$.

Proof Let $\mathcal{D}_z$ be the residual 1-$(v-1, k, r-\lambda)$ design of $\mathcal{D}$ with respect to z, and let N be the $(v-1) \times (b-r)$ points by blocks incidence matrix of $\mathcal{D}_z$. Let $\bar{N}$ be the matrix obtained by adding one all-one row to N:

$$\bar{N} = \begin{pmatrix} & N & \\ 1 & \cdots & 1 \end{pmatrix}.$$

Since the scalar product of every column of M with every column of N is either x or y and both x and y are odd, the scalar product of every column of $\bar{M}$ with every column of $\bar{N}$ is an even number ($x+1$ or $y+1$). This implies that every column of $\bar{N}$ is orthogonal to $\bar{C}$ over the binary field. In particular, $c^\top \bar{N} \equiv 0 \pmod 2$, and hence $wt(c) \neq 1$.

Let c' be the vector indexed by X obtained from c by deleting the last coordinate. Then ${c'}^\top N$ is the all-one vector modulo 2. In particular, every block of $\mathcal{D}_z$ meets the support of c'. Since every point of $\mathcal{D}_z$ is contained in exactly $r-\lambda$ blocks of $\mathcal{D}_z$, the number of blocks of $\mathcal{D}_z$ is at most $wt(c')(r-\lambda)$. This implies $b-r \leq wt(c')(r-\lambda)$, proving the desired inequality. □

Theorem 4.2 implies the following.

Theorem 4.3 *A necessary condition for an* 1-$(v-1, k-1, \lambda)$ *design* $\mathcal{D}'$ *with even block intersection numbers* x', y' *to be extendable to a quasi-symmetric* 2-(v, k, λ) *design with odd intersection numbers* $x = x'+1$, $y = y'+1$ *is that the binary linear code spanned by the rows of its points by blocks incidence matrix contains the all-one vector.*

Proof Assuming that $\mathcal{D}' = \mathcal{D}^z$ for some quasi-symmetric 2-(v, k, λ) design $\mathcal{D}$, we use the same notation as Theorem 4.2. Let C be the binary code of length r spanned by the rows of M. The condition that C contains the all-one vector $\bar{1} = (1, \ldots, 1)$ is equivalent to the condition that all codewords in its dual code $C^\perp$ have even weights. Thus, $\bar{1} \notin C$ if and only if there is a set S of an odd number of columns of M whose sum over the binary field is the zero column. If S is such a set, then the modulo 2 sum of the corresponding columns of $\bar{M}$ is a vector of weight 1 with nonzero last position. This violates the inequality in Theorem 4.2. □

Note 2 The modulo 2 sum of the first three columns of the orbit matrix (5) is the zero column. Hence, the dual code $C^\perp$ of binary code C of length 45 spanned by the incidence matrix of the 1-(40, 8, 9) design $\mathcal{D}'$ from Example 4.1 contains a codeword of odd weight 15. It follows that C does not contain the all-one vector, thus, by Theorem 4.3, $\mathcal{D}'$ is not extendable to a quasi-symmetric 2-(41, 9, 9) design.

Example 4.4 The following matrix

$$\begin{pmatrix} & & 1 \\ I_{20} & J-B & \vdots \\ & & 1 \\ & 1\dots1 & 0 \end{pmatrix},$$

where I_{20} is the identity matrix of order 20, B is the square circulant (0, 1)-matrix of order 19 with nine nonzero entries in its first row indexed by the quadratic residues modulo 19, and J is the 19×19 all-one matrix, is the generator matrix of a doubly even self-dual [40, 20, 8] code C, known as the double circulant code with these parameters. The full automorphism group of C is of order $6840 = 2^3 \cdot 3^2 \cdot 5 \cdot 19$, and contains an automorphism ϕ of order 5 without fixed points that partitions the 285 codewords of weight 8 in 57 orbits. A short computer search shows that there are exactly 1787 distinct 1-(40, 8, 9) designs with block intersection numbers 0 and 2, whose 40×45 incidence matrices comprise of 9 orbits of codewords of weight 8 under the action of ϕ. None of the 1787 binary codes of length 45 spanned by these incidence matrices contains the all-one vector, hence, according to Theorem 4.3, all 1-(40, 8, 9) designs that arise from C and admit ϕ as an automorphism, are not extendable to a quasi-symmetric 2-(41, 9, 9) design.

Theorem 4.5 *There is no quasi-symmetric* 2-(41, 9, 9) *design with an automorphism ϕ of order 5 with exactly one fixed point such that the incidence matrix of a derived design with respect to the point fixed by ϕ is obtainable as a collection of codewords in a doubly-even self-dual* [40, 20] *code invariant under ϕ.*

The proof of Theorem 4.5 is computational. Table 1 gives a summary of the computational results. From the database of doubly even self-dual [40, 20] codes, we first extract those with automorphism ϕ of order 5 without fixed points. There are 45 (resp. 32) doubly even self-dual [40, 20, 8] (resp. [40, 20, 4]) codes. For each such [40, 20] code C, we decompose the set of codewords of weight 8 into orbits under $< \phi >$, and enumerate all possible union of nine orbits which can form the set of blocks of a quasi-symmetric 1-(40, 8, 9) design with intersection numbers $x' = 0$, $y' = 2$. The designs are then tested to see if the necessary condition given in Theorem 4.3 is satisfied. In this way, we obtain two designs from [40, 20, 8] codes, and 130 designs from [40, 20, 4] codes. It turns out that none of the latter 130 designs is extendable by Theorem 4.2. This is because the code $\bar{C}$ contains a codeword of weight $5 < 1 + (b-r)/(r-\lambda) = 49/9$.

Table 1 Designs from doubly even self-dual [40, 20] codes

	[40, 20, 4]	[40, 20, 8]
No. of codes	16,470	77,873
No. of codes with ϕ	45	32
No. of designs (Theorem 4.3)	2	130
No. of designs (Theorem 4.2)	2	0

For each of the remaining two 1-(40, 8, 9) designs coming from [40, 20, 8] codes, we construct the points by blocks incidence matrix M. Using the notation of the proof of Theorem 4.2, we see that the extendability implies the existence of a 40×160 matrix N which is the points by blocks incidence matrix of the corresponding residual 1-(40, 9, 36) design. The matrix N has row sum 36, so for each $i \in \{1, \dots, 40\}$, there are at least 36 codewords of weight 10 whose support contains $\{i, 41\}$ in $\bar{C}^{\perp}$. Let $\Gamma_i = (X_i, E_i)$ denote the graph, where the vertex set X_i is the set of codewords of weight 10 whose support contains $\{i, 41\}$ in $\bar{C}^{\perp}$. The edge set E_i consists of pairs of codewords whose support intersect at 1 or 3 positions. Since N is the points by blocks incidence matrix of the residual design, the maximum clique size $\omega(\Gamma_i)$ of the graph Γ_i must be at least 36. We have verified by computer that for each of the two designs,

$$\min\left\{\omega(\Gamma_i) \,:\, 1 \le i \le 40\right\} < 36.$$

This shows that none of the 1-(40, 8, 9) designs we found is extendable.

References

1. Beth, T., Jungnickel, D., Lenz, H.: Design Theory, 2nd edn. Cambridge University Press, Cambridge (1999)
2. Betsumiya, K., Harada, M., Munemasa, A.: A complete classification of doubly even self-dual codes of length 40. Electron. J. Combin. **19**(P18), 12 (2012)
3. Bose, R.C.: Strongly regular graphs, partial geometries and partially balanced designs. Pac. J. Math. **13**(2), 389–419 (1963)
4. Bouyuklieva, S., Varbanov, Z.: Quasi-symmetric 2-(37, 9, 8) designs and self-orthogonal codes with automorphisms of order 5. Math. Balkanica (N.S.) **19**, 33–38 (2005)
5. Harada, M., Munemasa, A., Tonchev, V.D.: Self-dual codes and the non-existence of a quasi-symmetric 2-(37, 9, 8) design with intersection numbers 1 and 3. J. Combin. Des. **25**, 469–476 (2017)
6. Cary Huffman, W.: On the classification and enumeration of self-dual codes. Finite Fields Appl. **11**(3), 451–490 (2005)
7. CaryHuffman, W., Pless, V.: Fundamentals of Error-Correcting Codes. Cambridge University Press, Cambridge (2003)
8. Mathon, R., Rosa, A.: 2-(v, k, λ) designs of small order. In: Colbourn, C.J., Dintz,J.H. (eds.) Handbook of Combinatorial Designs, 2nd edn. Chapmanand Hall/CRC, London, pp. 25–58 (2007)
9. Neumaier, A.: Regular sets and quasi-symmetric 2-designs. In: Jungnickel, D., Vedder, K. (eds.) Combinatorial Theory, pp. 258–275. Springer, Berlin (1982)
10. Shrikhande, M. S.: Quasi-Symmetric Designs. In: Colbourn, C.J., Dinitz, J.H. (eds.) Handbook of Combinatorial Designs, 2nd edn, Chapman and Hall/CRC, Boca Raton, pp. 578–582 (2007)
11. Shrikhande, S.S., Bhagwandas: Duals of incomplete block designs. J. Indian Statist. Assoc. **3**, 30–37 (1965)
12. Tonchev, V.D.: Combinatorial Configurations. Wiley, New York (1988)