Non-embeddable quasi-residual quasi-symmetric designs

Vedran Krčadinac[1]

Abstract

Quasi-symmetric (36, 16, 12) designs with intersection numbers $x = 6$, $y = 8$ that cannot be embedded in symmetric (64, 28, 12) designs as residuals are constructed.

1 Introduction

We use standard notation and terminology of design theory and coding theory [2, 3, 7]. Let $\mathcal{D}$ be a symmetric (v, k, λ) design and B_0 one of its blocks. The *residual design* $\mathrm{res}_{B_0}\mathcal{D}$ contains the points outside B_0 and the sets $B \setminus B_0$, $B \neq B_0$ as blocks, and is a 2-design with parameters $(v', b', r', k', \lambda') = (v - k, v - 1, k, k - \lambda, \lambda)$. The *derived design* $\mathrm{der}_{B_0}\mathcal{D}$ contains the points on B_0 and the sets $B \cap B_0$, $B \neq B_0$ as blocks, and is a 2-design with parameters $(v'', b'', r'', k'', \lambda'') = (k, v - 1, k - 1, \lambda, \lambda - 1)$. Here, B denotes an arbitrary block of $\mathcal{D}$.

The parameters of residual designs satisfy $r' = k' + \lambda'$, and of derived designs $k'' = \lambda'' + 1$. Designs with this property are called *quasi-residual* and *quasi-derived*, respectively. They are called *non-embeddable* if they cannot be obtained from a symmetric design $\mathcal{D}$ as $\mathrm{res}_{B_0}\mathcal{D}$ or $\mathrm{der}_{B_0}\mathcal{D}$. The existence of non-embeddable designs had been known for a long time. Bhattacharya [4] constructed a quasi-residual (16, 24, 9, 6, 3) design with a pair of blocks intersecting in 4 points. It cannot be embedded in a symmetric (25, 9, 3) design, with block intersections of size 3. Another easy argument for non-embeddability is the nonexistence of the corresponding symmetric designs. For example, quasi-derived (12, 33, 11, 4, 3) designs exist, but symmetric (34, 12, 4) designs do not exist by the BRC condition for even v [15]. In [24], non-embeddable quasi-residual (25, 40, 16, 10, 6) and (36, 63, 28, 16, 12) designs were constructed. Proofs of non-embeddability are more

✉ Vedran Krčadinac
    vedran.krcadinac@math.hr

1   Department of Mathematics, Faculty of Science, University of Zagreb, Bijenička 30,
    10000 Zagreb, Croatia

involved, but are also based on block intersections. Surveys on (non-)embeddability results appear in [1, 21].

The *degree* of a design is the number of cardinalities $|B_1 \cap B_2|$ occurring as intersections of blocks $B_1 \neq B_2$. Symmetric designs can be defined as designs of degree 1, block intersections always being of cardinality λ. A design is called *quasi-symmetric* if it is of degree 2, i.e. if any pair of blocks intersect in x or in y points, for some integers $x < y$ called the *intersection numbers*. We refer to [20, 22] for results about quasi-symmetric designs (QSDs).

A residual design $\mathrm{res}_{B_0} \mathcal{D}$ is quasi-symmetric with intersection numbers x, y if and only if the corresponding derived design $\mathrm{der}_{B_0} \mathcal{D}$ is quasi-symmetric with intersection numbers $\lambda - y$, $\lambda - x$. This happens e.g. for symmetric designs with the symmetric difference property (SDP designs) [10]. The second smallest example are (64, 28, 12) SDP designs: the derived designs are (28, 12, 11) QSDs with $x = 4$, $y = 6$, and the residual designs are (36, 16, 12) QSDs with $x = 6$, $y = 8$.

Non-embeddability of quasi-residual and quasi-derived QSDs is more difficult to prove because they have the same block intersections as embeddable ones. In Ding et al. [8], quasi-derived (28, 12, 11) QSDs that cannot be embedded in symmetric (64, 28, 12) designs have been constructed. This also settles the existence of non-embeddable quasi-residual QSDs: the complementary (28, 16, 20) designs have intersection numbers $x = 8$, $y = 10$ and cannot be embedded in symmetric (64, 36, 20) designs. It is natural to ask whether there are also quasi-residual (36, 16, 12) QSDs that cannot be embedded in symmetric (64, 28, 12) designs. The purpose of this paper is to construct such examples. In the next two sections, we shall prove the following theorems.

Theorem 1 *There are exactly 921 quasi-symmetric (36, 16, 12) design with an automorphism group isomorphic to the Frobenius group of order 21.*

Theorem 2 *Among the quasi-residual quasi-symmetric designs of Theorem 1, exactly 116 are non-embeddable.*

The proofs are based on computer calculations. We use GAP [23] for group calculations, Cliquer [18, 19] to search for cliques in graphs, nauty [17] for isomorphism testing and to determine full automorphism groups, Magma [5] for calculations with codes, and our own program written in C to find subset orbits.

2 The construction

The symplectic (36, 16, 12) QSD is invariant under the group $Sp(6, 2)$ of order 1451520 and is residual in the symplectic (64, 28, 12) design [10]. This is one of the four (64, 28, 12) SDP designs [9]. Non-SDP examples with residual and derived QSDs were constructed in [14]. The study was continued in [8], where 8784 (36, 16, 12) QSDs were constructed by embedding the (28, 12, 11) QSDs with an automorphism of order 7. All of these (36, 16, 12) QSDs are residual. Many more examples were

constructed in [12] by prescribing automorphism groups and by a construction from [6, 16]. The total number of non-isomorphic examples was shown to be at least 522079. Some of these QSDs might be non-embeddable, but we want a smaller set of examples that is easily described. We shall classify (36, 16, 12) QSDs invariant under the Frobenius group $Frob_{21}$. First we determine the action of an automorphism of order 7.

Lemma 1 *An automorphism of order 7 of a (36, 16, 12) QSD fixes exactly one point.*

Proof Let α be an automorphism of order 7 fixing exactly $f = 1 + 7m$ points. We will prove that $m \geq 1$ implies $m = 5$, making α the identity. Hence, $m = 0$ necessarily holds for an automorphism of order 7.

Assume there are two fixed points F_1, F_2. Then α maps the set of 12 blocks through F_1 and F_2 onto itself, and there are at least 5 fixed blocks $B_1, \ldots, B_5$ among them. We claim that each of these blocks contains either 9 or 16 fixed points. Indeed, if B_i would contain just the two fixed points F_1, F_2 and two point-orbits of size 7, then it would intersect the other blocks B_j in either 2 or 9 points. This is not possible because the intersection numbers are $x = 6$, $y = 8$.

Next we claim that at least one of the blocks B_i contains 16 fixed points, i.e. is fixed pointwise. This is because there are $o = 5 - m \leq 4$ point-orbits of size 7, and each of them can be on at most one of the 5 blocks B_i. Now we already have 16 fixed points, and hence $m \geq 3$. This makes $o \leq 2$ and therefore at least 3 of the blocks $B_1, \ldots, B_5$ are fixed pointwise.

Two blocks containing 16 fixed points imply there are at least 24 fixed points (their intersection is of size $x = 6$ or $y = 8$). This makes $m \geq 4$ and $o \leq 1$. Finally, notice that if there are no more than 7 non-fixed points, then all of the blocks are fixed. For a non-fixed block B intersects its image B^α in at most $y = 8$ points and the remaining 8 points on B would have to be non-fixed. This means that all of the points have to be fixed as well, i.e. $m = 5$. □

Now we know that $Frob_{21}$ acts on the points of a (36, 16, 12) QSD in orbits of size (1, 7, 7, 7, 7, 7) or (1, 7, 7, 21). This determines the action up to permutational isomorphism. We can take as generators the permutation of order 7

$$\alpha = (2, \ldots, 8)(9, \ldots, 15)(16, \ldots, 22)(23, \ldots, 29)(30, \ldots, 36)$$

and one of the permutations of order 3

$$\beta_1 = (3, 4, 6)(5, 8, 7)(10, 11, 13)(12, 15, 14)(17, 18, 20)(19, 22, 21)$$
$$(24, 25, 27)(26, 29, 28)(31, 32, 34)(33, 36, 35),$$
$$\beta_2 = (3, 4, 6)(5, 8, 7)(10, 11, 13)(12, 15, 14)(16, 23, 30)(17, 25, 34)$$
$$(18, 27, 31)(19, 29, 35)(20, 24, 32)(21, 26, 36)(22, 28, 33).$$

The two permutation representations of $Frob_{21}$ will be denoted by $G_i = \langle \alpha, \beta_i \rangle$, $i = 1, 2$. We need a computational method to find all QSDs invariant under the groups G_i. In Ding et al. [8], tactical decomposition matrices (also known as orbit

matrices) were used for (28, 12, 11) QSDs with an automorphism of order 7. The Kramer-Mesner method [11] was adapted to quasi-symmetric designs in [12] and used to find (56, 16, 18) designs with intersection numbers $x = 4$, $y = 8$ and other QSDs. The paper [13] explores different computational approaches to the construction of QSDs with a prescribed automorphism group G. In many cases the following reduction to the clique search problem has proved efficient.

First, find all G-orbits of k-subsets of points such that any pair of subsets intersect in x or in y points (the *good orbits*). Define a graph Γ with the good orbits as vertices and edges between *compatible orbits*, such that sets from one orbit intersect sets from the other orbit in x or in y points. This is the *compatibility graph* of G. Every QSD with G as automorphism group gives rise to a clique of weight b in Γ. Weights of the vertices are sizes of the orbits. The converse is not necessarily true because designs need to be balanced, i.e. to cover every pair of points exactly λ times. However, for small QSD parameters there are usually not many exceptions. We use Cliquer [18, 19] to find the cliques of weight b and then check if the corresponding families of k-subsets are balanced.

Denote the compatibility graphs of G_i by Γ_i, for $i = 1, 2$. We use an algorithm described in [13] to compute the good orbits of 16-subsets of $\{1, \ldots, 36\}$ with intersection numbers $x = 6$, $y = 8$, i.e. vertices of Γ_i. There are 59792 good orbits for G_1 and 142961 good orbits for G_2. The compatibility graphs are fairly sparse: Γ_1 has 524960 edges (density 0.029%), and Γ_2 has 3241532 edges (density 0.032%). Cliquer could perform a complete search for cliques of weight $b = 63$. In Γ_1, the maximum clique weight is 49. Therefore, (36, 16, 12) QSDs with G_1 as automorphism group do not exist. In Γ_2, there are 77238 cliques of weight 63. All the cliques correspond to balanced families, i.e. designs. Using nauty [17], we found that there are 921 non-isomorphic designs among them and computed their full automorphism groups (Table 1). This proves Theorem 1.

3 Test of non-embedability

Suppose a (36, 16, 12) design $\mathcal{R}$ is embedded in a symmetric (64, 28, 12) design. Then, the 64×64 incidence matrix can be written in the following form:

Table 1 Distribution of the QSDs of Theorem 1 by order of full automorphism group

|Aut|	#QSDs
1451520	1
10752	3
1344	8
672	16
168	23
84	72
42	2
21	796

Here R is the 36×63 incidence matrix of $\mathcal{R}$ and D is the 28×63 incidence matrix of the corresponding derived $(28, 12, 11)$ design. The scalar product of a row of R with a row of D is $\lambda = 12$. If R is given, the first task is to find candidates for the rows of D. A straightforward approach to test the $\binom{63}{27} \approx 4.9 \cdot 10^{17}$ $\{0, 1\}$-vectors with 27 ones would be too time-consuming. We borrow an idea from [8] and use the linear code C spanned by the rows of R over $GF(3)$. Rows of D are elements of the dual code $C^\perp$, because 3 divides λ. On the other hand, 3 does not divide the order $n = r - \lambda$ nor the parameter k of $\mathcal{R}$, hence $\dim C = 36$ and $\dim C^\perp = 63 - 36 = 27$. If a generator matrix of $C^\perp$ in row echelon form is used, only $\{0, 1\}$-linear combinations of the rows need to be considered, i.e. $2^{27} \approx 1.3 \cdot 10^8$ possibilities. This can be done effectively by the Magma command `ConstantWords` [5]. The result is summarized in Table 2.

Fifty-two QSDs of Theorem 1 give only 14 candidates for the rows of D. These QSDs are clearly non-embeddable, because 28 rows are needed. We tested the remaining QSDs by searching for cliques in graphs with the row-candidates for D as vertices, and pairs of rows with scalar product equal to 11 as edges. A clique of size 28 in this graph corresponds to a full matrix D, i.e. an embedding of $\mathcal{R}$ in a symmetric design. Cliquer [18, 19] was used and the search was stopped as soon as one embedding was found. Sixty-four more QSDs of Theorem 1 were found to be non-embeddable, proving Theorem 2. Table 2 also contains the distribution of

Table 2 Distribution of the QSDs of Theorem 1 by number of candidates for the rows of D

#cand.	#QSDs	#non-emb.	#cand.	#QSDs	#non-emb.
14	52	52	616	128	0
56	53	0	840	30	0
70	11	0	994	16	0
84	36	20	1008	98	0
98	23	0	1120	40	0
140	35	30	1736	65	0
168	44	0	2632	82	0
224	40	0	8904	57	0
378	14	14	13,384	85	0
392	12	0			

non-embeddable QSDs by number of row-candidates for D. All of the 116 non-embeddable QSDs have $Frob_{21}$ as their full automorphism group.

Base blocks for a single non-embeddable QSD with only 14 row-candidates for D are given below. Blocks of the design are the corresponding G_2-orbits.

$$\{1, 2, 3, 5, 9, 11, 14, 17, 23, 24, 25, 26, 27, 33, 34, 35\}$$
$$\{1, 2, 3, 7, 12, 13, 15, 16, 17, 22, 23, 26, 28, 31, 34, 35\}$$
$$\{2, 3, 4, 5, 6, 7, 15, 16, 19, 22, 23, 24, 29, 31, 33, 36\}$$
$$\{2, 3, 4, 6, 10, 11, 12, 13, 14, 15, 19, 20, 24, 29, 32, 35\}$$
$$\{2, 3, 9, 10, 15, 19, 21, 22, 24, 25, 26, 28, 29, 30, 32, 36\}$$

Incidence matrices of the remaining QSDs constructed in this paper are available on the author's web page https://web.math.pmf.unizg.hr/~krcko/results/quasisym.html.

References

1. Alraqad, T.A., Shrikhande, M.S.: An overview of embedding problems of quasi-residual designs. J. Stat. Theory Pract. **3**(2), 319–347 (2009)
2. Assmus Jr., E.F., Key, J.D.: Designs and Their Codes. Cambridge University Press, Cambridge (1992)
3. Beth, T., Jungnickel, D., Lenz, H.: Design Theory, 2nd edn. Cambridge University Press, Cambridge (1999)
4. Bhattacharya, K.N.: A new balanced incomplete block design. Sci. Cult. **9**, 508 (1944)
5. Bosma, W., Cannon, J., Playoust, C.: The Magma algebra system. I. The user language. J. Symb. Comput. **24**(3–4), 235–265 (1997)
6. Bracken, C., McGuire, G., Ward, H.: New quasi-symmetric designs constructed using mutually orthogonal Latin squares and Hadamard matrices. Des. Codes Cryptogr. **41**(2), 195–198 (2006)
7. Colbourn, C.J., Dinitz, J.H. (eds.): Handbook of Combinatorial Designs, 2nd edn. CRC, Boca Raton (2007)
8. Ding, Y., Houghten, S., Lam, C., Smith, S., Thiel, L., Tonchev, V.D.: Quasi-symmetric 2-$(28,12,11)$ designs with an automorphism of order 7. J. Comb. Des. **6**(3), 213–223 (1998)
9. Jungnickel, D., Tonchev, V.D.: On symmetric and quasi-symmetric designs with the symmetric difference property and their codes. J. Comb. Theory Ser. A **59**(1), 40–50 (1992)
10. Kantor, W.M.: Symplectic groups, symmetric designs, and line ovals. J. Algebra **33**, 43–58 (1975)
11. Kramer, E.S., Mesner, D.M.: t-designs on hypergraphs. Discrete Math. **15**, 263–296 (1976)
12. Krčadinac, V., Vlahović, R.: New quasi-symmetric designs by the Kramer–Mesner method. Discrete Math. **339**(12), 2884–2890 (2016)
13. Krčadinac, V., Vlahović Kruc, R.: Quasi-symmetric designs on 56 points. Adv. Math. Commun. (2019). https://doi.org/10.3934/amc.2020086
14. Lam, C., Thiel, L., Tonchev, V.D.: On quasi-symmetric 2-$(28,12,11)$ and 2-$(36,16,12)$ designs. Des. Codes Cryptogr. **5**(1), 43–55 (1995)
15. Mathon, R., Rosa, A.: 2-(v, k,λ) designs of small order. In: Colbourn, C.J., Dinitz, J.H. (eds.) The Handbook of Combinatorial Designs, 2nd edn, pp. 25–58. CRC, Boca Raton (2007)
16. McDonough, T.P., Mavron, V.C., Ward, H.N.: Amalgams of designs and nets. Bull. Lond. Math. Soc. **41**(5), 841–852 (2009)
17. McKay, B.D., Piperno, A.: Practical graph isomorphism, II. J. Symb. Comput. **60**, 94–112 (2014)
18. Niskanen, S., Östergård, P.R.J.: Cliquer user's guide, version 1.0. Communications Laboratory, Helsinki University of Technology, Espoo, Finland, Tech. Rep. T48 (2003)
19. Östergård, P.R.J.: A fast algorithm for the maximum clique problem. Discrete Appl. Math. **120**(1–3), 197–207 (2002)

20. Shrikhande, M.S.: Quasi-symmetric designs. In: Colbourn, C.J., Dinitz, J.H. (eds.) The Handbook of Combinatorial Designs, 2nd edn, pp. 578–582. CRC Press, Boca Raton (2007)
21. Shrikhande, M.S., Alraqad, T.A.: Recent results on families of symmetric designs and non-embeddable quasi-residual designs. In: Crnković, D., Tonchev, V. (eds.) Information Security, Coding Theory and Related Combinatorics, NATO Sci. Peace Secur. Ser. D Inf. Commun. Secur., vol. 29, pp. 363–403. IOS, Amsterdam (2011)
22. Shrikhande, M.S., Sane, S.S.: Quasi-symmetric Designs. Cambridge University Press, Cambridge (1991)
23. The GAP Group: GAP—Groups, Algorithms, and Programming, Version 4.8.10. http://www.gap-system.org (2018)
24. van Trung, T.: Non-embeddable quasi-residual designs with $k<\frac{1}{2} v$. J. Comb. Theory Ser. A **43**(1), 133–137 (1986)