Quasi-symmetric Designs and Self-dual Codes

VLADIMIR D. TONCHEV

Using the classification of certain binary self-dual codes, we establish the uniqueness of the classical quasi-symmetric 2-(21, 6, 4), 2-(21, 7, 12), 2-(22, 7, 16) designs, related to the unique Steiner System S(5, 8, 24), and the non-existence of quasi-symmetric 2-(28, 7, 16) or 2-(29, 7, 12) designs.

1. Introduction

The terminology and notations from design theory used in this paper are standard (cf. [1], [4], [6]). A 2-(v, k, \lambda) design is quasi-symmetric with intersection numbers x, y (x < y) if the cardinality of the intersection of any two blocks is x or y. Quasi-symmetric designs are extensively studied because of their connections with strongly regular graphs. Well known examples of quasi-symmetric designs are: the Steiner systems S(2, k, v) which are not projective planes; the multiples of symmetric designs; the quasi-residual 2-(v, k, 2) designs; the strongly resolvable 2-designs. Following Neumaier [10], we call a quasi-symmetric design exceptional, if it does not belong to any of the above four classes. Neumaier [10] has investigated quasi-symmetric designs by use of various necessary conditions for strongly regular graphs. In particular, these conditions left 23 sets of parameters for exceptional 2-(v, k, \lambda) designs in the range 2k < v < 40. For 8 of these 23 parameter sets quasi-symmetric designs are known to exist, and the remaining cases were open.

In this paper we apply self-orthogonal codes as a tool for investigating quasi-symmetric designs. Using the classification of certain self-dual codes, we prove that quasi-symmetric 2-(28, 7, 16) or 2-(29, 7, 12) designs do not exist, and the classical quasi-symmetric 2-(21, 6, 4), 2-(21, 7, 12) and 2-(22, 7, 16) designs constructed by Goethals and Seidel [5] on the base of the unique Steiner system S(5, 8, 24) are unique up to isomorphism. The same method was applied in [14] for proving that there are exactly five isomorphism classes of quasi-symmetric 2-(31, 7, 7) designs.

2. Self-orthogonal Codes and Quasi-symmetric Designs

For our consideration we need some facts from coding theory (cf. e.g., [1], [8], [9]). By a q-ary code of length n and dimension k (or a (n, k) code) we mean a k-dimensional subspace of the n-dimensional vector space \( \mathbb{F}^n_q \) over \( \mathbb{F}(q) \). If C is a (n, k) code, the dual code is defined to be the (n, n-k) code \( C^\perp = \{ y \in V_n^* : xy = 0 \text{ for each } x \in C \} \). C is self-orthogonal, if \( C \subseteq C^\perp \), and self-dual, if \( C = C^\perp \). A matrix with the property that the linear span of its rows generates the code C, is a generator matrix of C. The generator matrices of the dual code \( C^\perp \) are called parity check matrices of C. We shall often refer to the elements of a code as codewords, or words only. The weight of a codeword is the number of its non-zero positions, and the minimum weight of a code is the weight of a lightest nonzero codeword. A (n, k, d) code is a (n, k) code with minimum weight d. A code has minimum weight at least d iff every \( d - 1 \) columns in a parity check matrix are linearly independent. The weights of all words in a self-orthogonal binary code are even. If in addition all weights are divisible by four, the code is called doubly-even.

We begin with a simple proposition displaying how one can associate a binary self-orthogonal code with a quasi-symmetric 2-(v, k, \lambda) design provided that \( k = x = y \mod 2 \).
**Lemma 2.1.** Let $A$ be a $b$ by $v$ incidence matrix of a quasi-symmetric 2-$(v, k, \lambda)$ design with intersection numbers $x, y$ such that $k = x = y \pmod{2}$.

(i) If $k$ is even then the binary code of length $v$ with generator matrix $A$ is self-orthogonal.

(ii) If $k$ is odd then the matrix

$$\begin{bmatrix}
1 \\
\vdots \\
A \\
1
\end{bmatrix}$$

generates a binary self-orthogonal code of length $v + 1$.

**Proof.** In both cases the weights of the rows of the corresponding generator matrix are all even, and the scalar product of any two rows is even either, i.e. zero modulo 2.

Let us mention that, if further $k = 0 \pmod{4}$ (resp. $k = 3 \pmod{4}$), then the code of case (i) (resp. (ii)) is doubly-even.

The next two lemmas will not be surprising for those familiar with majority decoding. As usual, $r$ denotes the number of blocks containing a given point of a design.

**Lemma 2.2.** If $A$ is a $b$ by $v$ incidence matrix of a 2-$(v, k, \lambda)$ design, then the dual of the binary code with generator matrix $A$ has minimum weight

$$d \geq \frac{(b + r)}{r}, \quad \frac{(r + \lambda)}{\lambda}.$$  

**Proof.** Suppose that $S$ is a minimal set of linearly dependent columns of $A$. Then every row of $A$ must intersect an even number of these columns in ones. Let $n_i$ denote the number of rows intersecting exactly $i$ columns from $S$ in ones, and let $|S| = m$. Since every column of $A$ contains $r = \lambda(v - 1)/(k - 1)$ ones, and the scalar product (over the reals) of any two columns is $A$, we have:

$$\sum 2n_{2i} = rm,$$

$$\sum 2i(2i - 1)n_{2i} = m(m - 1)\lambda,$$

whence

$$\sum 2i(2i - 2)n_{2i} = m((m - 1)\lambda - r) \geq 0,$$

i.e. $m \geq \frac{(r + \lambda)}{\lambda}$.

**Lemma 2.3.** If $A$ is a $b$ by $v$ incidence matrix of a 2-$(v, k, \lambda)$ design, then the dual of the binary code with generator matrix

$$\begin{bmatrix}
1 \\
\vdots \\
A \\
1
\end{bmatrix}$$  

(1)

has minimum weight

$$d \geq \min\{(b + r)/r, (r + \lambda)/\lambda\}.$$  

**Proof.** Suppose again that $S$ is a minimal set of $m$ linearly dependent columns of the matrix (1). If $S$ does not involve the all-one column, then $m \geq \frac{(r + \lambda)}{\lambda}$ by Lemma 2.2. If the all-one column belongs to $S$, then it must be equal to the sum (modulo 2) of the remaining columns of $S$. Denoting by $n_i$ the number of rows of $A$ intersecting exactly $i$ columns from $S$ in ones, we have

$$\sum n_{2i+1} = b,$$

$$\sum (2i + 1)n_{2i+1} = r(m - 1),$$
whence

\[ \sum 2in_{2i+1} = r(m-1) - b \geq 0, \]

i.e. \( m \geq (b+r)/r \).

Combining the results of the previous lemmas, we get the following:

**Corollary 2.4.** If \( E \) is a self-dual code containing the code from Lemma 2.1, then the minimum weight of \( E \) is at least \( (r+\lambda)/\lambda \) in the case (i), and at least \( \min\{(b+r)/r, (r+\lambda)/\lambda\} \) in the case (ii).

**Proof.** If \( C \) is a code defined as in Lemma 2.1 and \( C \subset E \), then \( E = E^+ \subset C^+ \), hence the minimum weight of \( C^+ \) does not exceed that of \( E \).

**Remark 2.5.** We shall often use the fact that every self-orthogonal code of an even length is contained in self-dual codes, and every doubly-even code of length divisible by 8 is contained in doubly-even self-dual codes of the same length [9, chapter 19, Section 6].

### 3. Uniqueness of Quasi-symmetric Designs arising from Witt Designs

In the Neumaier's table 1 [10] five of the eight parameter sets of known exceptional quasi-symmetric designs belong to designs related to the unique Steiner system \( S(5, 8, 24) \). Two of them, 2-(22, 6, 5) and 2-(23, 7, 21) are those of the unique Steiner systems \( S(3, 6, 22) \) and \( S(4, 7, 23) \) constructed by Witt [15]. The remaining three are 2-(21, 6, 4) \((x = 0, y = 2)\), 2-(21, 7, 12) \((x = 1, y = 3)\), and 2-(22, 7, 16) \((x = 1, y = 3)\). All these quasi-symmetric designs were constructed by Goethals and Seidel [5] by derivation from the unique \( S(5, 8, 24) \). Now we shall see that the last three parameter sets also determine uniquely the corresponding quasi-symmetric designs.

**Theorem 3.1.** A quasi-symmetric 2-(21, 6, 4) design with intersection numbers \( x = 0, y = 2 \) is unique up to isomorphism.

**Proof.** Let \( A \) be a 56 by 21 incidence matrix of such a design and consider the binary code \( C \) of length 22 generated by the matrix

\[
\begin{bmatrix}
1 & \cdots & 1 & 1 \\
0 & \ & \ & \\
A & & & \\
\end{bmatrix}
\]

Evidently, the code \( C \) is self-orthogonal. The dual code \( C^+ \) is obtained from the code with parity check matrix \( A \) by adding a new position equal to 0 for the words of even weight, and 1 for the words of odd weight. Therefore; the minimum weight \( d \) of \( C^+ \) is even, and since \( r = 16 \), by Lemma 2.2 \( d \geq 6 \). Hence by 2.4 and 2.5 \( C \) is contained in a self-dual \((22, 11, 6)\) code. The only self-dual \((22, 11, 6)\) code (up to permutation of the positions) is the shortened Golay code \( G_{22} \) [13]. The code \( G_{22} \) contains exactly 77 words of weight 6 forming an incidence matrix of the unique Steiner system \( S(3, 6, 22) \). Each point in \( S(3, 6, 22) \) is contained in \( 21 = 77 - 56 \) blocks, hence a quasi-symmetric 2-(21, 6, 4) design must be isomorphic with a residual of the unique 3-(22, 6, 1) design.

**Theorem 3.2.** A quasi-symmetric 2-(21, 7, 12) design with intersection numbers \( x = 1, y = 3 \) is unique up to isomorphism.
PROOF. Let $A$ be a 120 by 21 incidence matrix of a quasi-symmetric $2-(21, 7, 12)$ design and consider the code $C$ with generator matrix of the form (1). Since $r = 40$, Lemma 2.3 gives the lower bound $d \geq 4$ for the minimum weight $d$ of $C^\perp$. We shall show however that $d > 4$. Since $(r + \lambda)/\lambda = 52/12 > 4$, no four columns of $A$ are linearly dependent. Suppose that there are three columns of $A$ whose sum is the all-one column. Denoting by $n_i$ the number of rows of $A$ intersecting such three columns in $i$ ones, we get the system

$$
\begin{align*}
n_1 + n_3 &= 120, \\
n_1 + 3n_3 &= 3.40, \\
3n_3 &= 3.12,
\end{align*}
$$

which has no solutions. Hence $d > 4$ and the code $C$ is contained in a self-dual $(22, 11)$ code with minimum weight at least 6; but the minimum weight of a self-dual $(22, 11)$ code is at most 6 [13], thus $C$ is contained in the shortened Golay code $G_{22}$. The set of all 330 words of weight 8 in $G_{22}$ form a 3-$(22, 8, 12)$ design with $r = 120$. This shows that the considered quasi-symmetric $2-(21, 7, 12)$ design must coincide with a derived of this 3-$(22, 8, 12)$ design. Since this 3-design is invariant under the triply transitive Mathieu group $M_{22}$, its derived are all mutually isomorphic.

**Theorem 3.3.** A quasi-symmetric $2-(22, 7, 16)$ design with intersection numbers $x = 1$, $y = 3$ is unique up to isomorphism.

**Proof.** Let $C$ be the code generated by the matrix

$$
\begin{bmatrix}
1 & \cdots & 1 \\
1 & 0 & \\
\vdots & \vdots & A \\
1 & 0
\end{bmatrix},
$$

(2)

where $A$ is a 176 by 22 incidence matrix of a quasi-symmetric $2-(22, 7, 16)$ design. The code $C$ is self-orthogonal and doubly-even. Applying Lemma 2.3 for the code with parity check matrix obtained from (2) by deleting the first row and the last column, we obtain that $C^\perp$ has minimum weight $d \geq 6$, and since $C$ is doubly-even it must be contained in a self-dual doubly-even $(24, 12, 8)$ code. Up to equivalence, the only such code is the extended Golay code $G_{24}$ [3], [11], [13]. The words of weight 8 in $G_{24}$ form the unique Steiner system $S(5, 8, 24)$. The number of blocks in a $S(5, 8, 24)$ containing a fixed point and not containing another fixed point, is exactly 176, and disregarding the two points in such a set of 176 blocks one obtains the required quasi-symmetric $2-(22, 7, 16)$ design.

We shall mention without going into details, that applying the same method for the parameters $2-$(31, 7, 7) ($x = 1, y = 3$) and using the classification of the doubly-even self-dual $(32, 16, 8)$ codes [2], the following proposition can be proved.

**Proposition 3.4.** [14]. There are exactly five isomorphism classes of quasi-symmetric $2-$$(31, 7, 7)$ designs.

One of the five quasi-symmetric $2-$(31, 7, 7) designs is formed by the planes in $PG(4, 2)$. An interesting feature of these designs is that they are not distinguished by the ranks of their incidence matrices over $GF(2)$, hence the designs arising from a finite geometry are not characterized by their ranks in general (cf. [7]). Let us mention also that a quasi-
symmetric 2-(45, 9, 8) design yielding a pseudo-geometric strongly regular graph with parameters \((r, k, t) = (15, 10, 6)\) can be derived in a similar manner from a doubly-even self-dual \((48, 24, 12)\) code [14].

4. The Non-existence of Quasi-symmetric 2-(28, 7, 16) and 2-(29, 7, 12) Designs

For our proofs we need some information about the structure of the binary self-dual \((30, 15, 6)\) codes. All such codes are known [12], and all they have the same weight distribution. In particular, any self-dual \((30, 15, 6)\) code contains exactly 345 words of weight 8.

**Lemma 4.1.** The words of weight 8 in a binary self-dual \((30, 15, 6)\) code form a 1-(30, 8, 92) design.

**Proof.** Any self-dual \((30, 15, 6)\) code \(C\) can be obtained from a doubly-even self-dual \((32, 16, 8)\) code \(C^*\) by taking all words in \(C^*\) containing 00 or 11 in a fixed pair of positions, and deleting these two positions [12]. Since the codewords of a given weight in \(C^*\) form a 3-design on 32 points, the words containing zeros (resp. ones) in two fixed positions, will form a 1-design on 30 points. In particular, the 345 words of weight 8 in a self-dual \((30, 15, 6)\) code form a 1-design with \(r = 345.8/30 = 92\).

**Theorem 4.2.** Quasi-symmetric 2-(29, 7, 12) designs with intersection numbers \(x = 1, y = 3\) do not exist.

**Proof.** If \(A\) is a 232 by 29 incidence matrix of a quasi-symmetric 2-(29, 7, 12) design, then the associated self-orthogonal code \(C\) of length 30 defined as in Lemma 2.1, (ii) have to be contained in a self-dual code \(E\) of length 30. By 2.4 the minimum weight \(d\) of \(E\) is at least 6; and since the minimum weight of a self-dual \((30, 15)\) code is at most 6 [12], we have \(d = 6\). Therefore, \(E\) must contain a set of 232 words of weight 8, all having 1 at the first position, which contradicts to Lemma 4.1.

**Theorem 4.3.** Quasi-symmetric 2-(28, 7, 16) designs with intersection numbers \(x = 1, y = 3\) do not exist.

**Proof.** We proceed as in 3.3. Suppose \(A\) is a 288 by 28 incidence matrix of a quasi-symmetric 2-(28, 7, 16) design, and consider the binary code \(C\) of length 30 generated by the matrix of the form (2). The dual code \(C^\perp\) is obtained by the dual of the code \(L\) generated by the matrix (1) by adding a thirtieth position equal to 0 for the words of even weight, and 1 for the words of odd weight. By Lemma 2.3 the minimum weight of \(L^\perp\) is at least 5, hence that of \(C^\perp\) is at least 6. Since \(C\) is self-orthogonal, the rows of the generator matrix (2) must be contained in a self-dual \((30, 15, 6)\) code, which is impossible by Lemma 4.1.

5. Concluding Remarks

Below we list the updated form of the Neumaier's table with the parameters of exceptional quasi-symmetric designs on less than 40 points. The column 'Enumeration' contains the number of the non-isomorphic solutions, if known.

Evidently, 20 of the 23 parameter sets from Table 1 satisfy the hypothesis of Lemma 2.1, therefore the corresponding designs can be treated by use of binary self-dual codes. The analysis however becomes difficult when the bounds of lemmas 2.2, 2.3 are not very
table 1

exceptional quasi-symmetric 2-(v, k, \lambda) designs with 2k <= v < 40

<table>
<thead>
<tr>
<th>no.</th>
<th>v</th>
<th>k</th>
<th>\lambda</th>
<th>r</th>
<th>b</th>
<th>x</th>
<th>y</th>
<th>existence</th>
<th>enumeration</th>
<th>reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>19</td>
<td>9</td>
<td>16</td>
<td>36</td>
<td>76</td>
<td>3</td>
<td>5</td>
<td>?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>20</td>
<td>10</td>
<td>18</td>
<td>38</td>
<td>76</td>
<td>4</td>
<td>6</td>
<td>?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>20</td>
<td>8</td>
<td>14</td>
<td>38</td>
<td>95</td>
<td>2</td>
<td>4</td>
<td>?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>21</td>
<td>9</td>
<td>12</td>
<td>30</td>
<td>70</td>
<td>3</td>
<td>5</td>
<td>?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>21</td>
<td>8</td>
<td>14</td>
<td>40</td>
<td>105</td>
<td>2</td>
<td>4</td>
<td>?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>21</td>
<td>6</td>
<td>4</td>
<td>16</td>
<td>56</td>
<td>0</td>
<td>2</td>
<td>Yes</td>
<td>1</td>
<td>[5], theorem 3.1</td>
</tr>
<tr>
<td>7</td>
<td>21</td>
<td>7</td>
<td>12</td>
<td>40</td>
<td>120</td>
<td>1</td>
<td>3</td>
<td>Yes</td>
<td>1</td>
<td>[5], theorem 3.2</td>
</tr>
<tr>
<td>8</td>
<td>22</td>
<td>8</td>
<td>12</td>
<td>36</td>
<td>99</td>
<td>2</td>
<td>4</td>
<td>?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>22</td>
<td>6</td>
<td>5</td>
<td>21</td>
<td>77</td>
<td>0</td>
<td>2</td>
<td>Yes</td>
<td>1</td>
<td>[15]</td>
</tr>
<tr>
<td>10</td>
<td>22</td>
<td>7</td>
<td>16</td>
<td>56</td>
<td>176</td>
<td>1</td>
<td>3</td>
<td>Yes</td>
<td>1</td>
<td>[5], theorem 3.3</td>
</tr>
<tr>
<td>11</td>
<td>23</td>
<td>7</td>
<td>21</td>
<td>77</td>
<td>253</td>
<td>1</td>
<td>3</td>
<td>Yes</td>
<td>1</td>
<td>[1], [5], [15]</td>
</tr>
<tr>
<td>12</td>
<td>24</td>
<td>8</td>
<td>7</td>
<td>23</td>
<td>69</td>
<td>2</td>
<td>4</td>
<td>?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>13</td>
<td>28</td>
<td>7</td>
<td>16</td>
<td>72</td>
<td>288</td>
<td>1</td>
<td>3</td>
<td>No</td>
<td></td>
<td>theorem 4.3</td>
</tr>
<tr>
<td>14</td>
<td>28</td>
<td>12</td>
<td>11</td>
<td>27</td>
<td>63</td>
<td>4</td>
<td>6</td>
<td>Yes</td>
<td>?</td>
<td>P. cameron, [10]</td>
</tr>
<tr>
<td>15</td>
<td>29</td>
<td>7</td>
<td>12</td>
<td>56</td>
<td>232</td>
<td>1</td>
<td>3</td>
<td>No</td>
<td></td>
<td>theorem 4.2</td>
</tr>
<tr>
<td>16</td>
<td>31</td>
<td>7</td>
<td>7</td>
<td>35</td>
<td>155</td>
<td>1</td>
<td>3</td>
<td>Yes</td>
<td>5</td>
<td>A. Brouwer, [10], [14]</td>
</tr>
<tr>
<td>17</td>
<td>33</td>
<td>15</td>
<td>35</td>
<td>80</td>
<td>176</td>
<td>6</td>
<td>9</td>
<td>?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>18</td>
<td>33</td>
<td>9</td>
<td>6</td>
<td>24</td>
<td>88</td>
<td>1</td>
<td>3</td>
<td>?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>19</td>
<td>35</td>
<td>7</td>
<td>3</td>
<td>17</td>
<td>85</td>
<td>1</td>
<td>3</td>
<td>?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>20</td>
<td>35</td>
<td>14</td>
<td>13</td>
<td>34</td>
<td>85</td>
<td>5</td>
<td>8</td>
<td>?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>21</td>
<td>36</td>
<td>16</td>
<td>12</td>
<td>28</td>
<td>63</td>
<td>6</td>
<td>8</td>
<td>Yes</td>
<td>?</td>
<td>P. cameron, [10]</td>
</tr>
<tr>
<td>22</td>
<td>37</td>
<td>9</td>
<td>8</td>
<td>36</td>
<td>148</td>
<td>1</td>
<td>3</td>
<td>?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>23</td>
<td>39</td>
<td>12</td>
<td>22</td>
<td>76</td>
<td>247</td>
<td>3</td>
<td>6</td>
<td>?</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

restrictive, or the related code contains too many words of the required weight. In such cases additional assumptions, as e.g. about the automorphism group might be helpful.

We sketch a possible approach in this direction. Let us consider the parameters 2-(24, 8, 7) (x = 2, y = 4). By Lemma 2.2 the incidence matrix A of such a design generates a doubly-even self-orthogonal code C of length 24 such that C^\perp has minimum weight at least 5, hence C must be contained in the extended Golay code G_{24}. In other words, the set of blocks of any quasi-symmetric 2-(24, 8, 7) design is a subset of the block set of a Steiner system S(5, 8, 24). The greatest prime which can be order of an automorphism of a 2-(24, 8, 7) design is 23. Suppose we have a quasi-symmetric design D with these parameters and possessing an automorphism of order 23. Then the code C must be an extension of a nontrivial cyclic code of length 23. The only such code is the Golay code G_{24}. Therefore, A will be a generator matrix of G_{24}, hence the automorphism group of D must be a subgroup of the automorphism group of G_{24}, the Mathieu group M_{24}. All elements of order 23 are conjugate in M_{24}, hence it is sufficient to inspect a fixed element of order 23 and its orbits on the set of 759 blocks of a S(5, 8, 24). We have checked however, that no collection of three orbits form a quasi-symmetric 2-(24, 8, 7) design. Thus, the following proposition holds.

**Proposition 5.1.** A quasi-symmetric 2-(24, 8, 7) design does not possess automorphisms of order 23.

We shall mention finally, that the parameters 17, 20, 23 from Table 1, for which Lemma 2.1 does not apply, all have k = x = y (mod 3). Thus, a similar approach based on ternary self-orthogonal codes might be hopeful.
REFERENCES


Received 21 May 1984 and in revised form 15 October 1984

VLADIMIR D. TONCHEV

*Institute of Mathematics, Bulgarian Academy of Sciences,*

*Sofia 1090, P.O. Box 373, Bulgaria*