Designs, Codes and Cryptography, 3, 63–68 (1993)

Non-symmetric 2-Designs Modulo 2

CHRIS M. SKINNER*
Department of Mathematics, University of Michigan, Ann Arbor, MI 48109

Communicated by D. Jungnickel
Received September 27, 1992; Revised June 9, 1992.

Abstract. Necessary conditions are obtained for the existence of a $2-(v, k, \lambda)$ design, for which the block intersection sizes $s_1, s_2, \ldots, s_n$ satisfy $s_1 \equiv s_2 \equiv \ldots \equiv s_n \equiv s \pmod{2^e}$, where e is odd. These conditions are obtained by combining restrictions on the Smith Normal Form of the incidence matrix of the design with some well known properties of self-orthogonal binary codes with all weights divisible by 4.

1. Introduction

Let $\mathcal{B}$ be a $2-(v, k, \lambda)$ design where the block intersection sizes $s_1, s_2, \ldots, s_n$ satisfy $s_1 \equiv s_2 \equiv \ldots \equiv s_n \equiv s \pmod{p^e}$, where p is a prime and e is odd. Let A be the incidence matrix of $\mathcal{B}$ and put

$$X = \begin{bmatrix} A \\ \\ \lambda_1 \boldsymbol{j} \end{bmatrix} \text{ and } X' = [A^t - \lambda_2 \boldsymbol{j}^t],$$

where λ_1 is a power of p such that $\lambda_1\lambda_2 = \lambda$, $\lambda_1 \mid \lambda_2$ and $0 \leq (\lambda_2)_p - (\lambda_1)_p \leq 1$.

Using X and X', one can construct a sequence of nested codes over $\mathbb{F}_p$. Let L and L' be the integral lattices spanned by the rows of X and the columns of X', respectively. Let $\pi: \mathbb{Z}^v \to \mathbb{F}_p^v$ be the homomorphism that reduces every entry modulo p. For every integer $j \geq 0$, we define a code X_j over $\mathbb{F}_p$ by

$$X_j = \pi(p^{-j}L \cap \mathbb{Z}^v).$$

We define X_j' in like manner. In fact, given any $a \times b$ integer matrix C, we can construct a sequence of nested codes C_j over $\mathbb{F}_p$ in the same way as we did for X.

In [1] Blokhuis and Calderbank prove a number of properties of X_j and X_j'. Using these results they derive necessary conditions for the existence of a $2-(v, k, \lambda)$ design with all block intersection numbers congruent modulo p^e. However, the nature of these conditions are such that they are nontrivial only in the case where p is odd. In this paper we combine the results of Blokhuis and Calderbank on X_j and X_j' with known facts about self-orthogonal binary codes to derive nontrivial necessary conditions in the case $p = 2$. In particular, we prove the following theorem.

*Research done at AT&T Bell Laboratories.

THEOREM. *Let $\mathcal{B}$ be a $2-(v, k, \lambda)$ design where the block intersection sizes $s_1, s_2, \ldots, s_n$ satisfy $s_1 \equiv s_2 \equiv \ldots \equiv s_n \equiv s \pmod{2^e}$ and e is odd. If $2^e \| r - \lambda$ then after possibly taking complements we have either*

i) $v \equiv k + 1 \equiv 0 \pmod 2$ *and* $v \equiv 2 \pmod 8$
ii) $v \equiv k \equiv 1 \pmod 4$ *and* $v \equiv 1 \pmod 8$
iii) $v \equiv k \equiv -1 \pmod 4$ *and* $v \equiv -1 \pmod 8$
iv) $v \equiv k \equiv 0 \pmod 2$ *and either* $\begin{cases} (s)_2 \equiv (v-k)_2 \equiv 1 \pmod 2 \text{ or} \\ v \equiv 2 \pmod 8 \end{cases}$

The proof of the theorem is in the same spirit as the corresponding results of [1] in the case p odd. By extending X or X' if necessary, a self-orthogonal code is constructed. However, instead of appealing to the intrinsic geometry of the code as in [1], we appeal to restrictions on the lengths of self-orthogonal codes to derive the existence conditions. This is an extension of the ideas in [2].

A similar application of self-dual codes to the existence of certain quasi-symmetric 2-designs can be found in [5].

2. Proof of Theorem

The proof of the theorem is broken into various cases, each of which is handled by one of the lemmas proved in this section. First, we set forth the results about binary codes that will be needed.

LEMMA 1 ([3]). *The length of a self-dual binary code C with all weights divisible by 4 is divisible by 8.*

LEMMA 2 ([4]). *For v odd, let C be an $[v, \frac{1}{2}(v-1)]$ self-orthogonal code such that all weights in C are divisible by 4. Then $v \equiv \pm 1 \pmod 8$.*

The next three lemmas provide all the results necessary to prove the theorem. The notation and terminology will be that of [1]. The 2-SNF (Smith Normal Form) of an integral matrix is the number a_i of invariant factors h for which $2^i \| h$. Fix $d = (e+1)/2$.

LEMMA 3. *If $v \equiv k + 1 \equiv 0 \pmod 2$, then $v \equiv 2 \pmod 8$.*

Proof. In Lemma 5.2 of [1] it was proved that in this case $(\lambda)_2$ is odd, that X and X' have different 2-SNFs, and that $\dim X_d' \geq v/2$. Rearranging the identity $\lambda(v-1) = r(k-1)$ gives $\lambda(v-k) = (r-\lambda)(k-1)$ which implies $(v-k)_2 \equiv (k-1)_2 \pmod 2$. Since $v-k$ is odd, we have $(k-1)_2 \equiv 0 \pmod 2$ and therefore $k \equiv 1 \pmod 4$. The complementary design also has the property that v is even and the block size $v-k$ is odd, so we deduce that $v - k \equiv 1 \pmod 4$ and $v \equiv 2 \pmod 4$.

Let

$$C = \begin{bmatrix} A & j^t \\ \lambda_2 j & \lambda_2 \end{bmatrix}$$

and $D = \text{diag}[1, \ldots, 1, -k]$. Recall that $s \equiv k \pmod{2^e}$ and note that $k - 1$ is even so $2^{e+1} | \lambda(v - k) | \lambda_2^2(v - k)$.

Let $z = \Sigma \mu_i r_i$ be a vector in the integer lattice L spanned by the rows r_i of C. Then the inner product with respect to D of z with itself is

$$(z, z) = \sum_i \mu_i^2(r_i, r_i) + 2 \sum_{i>j} \mu_i \mu_j (r_i, r_j)$$

where

$$(r_i, r_i) = \begin{cases} k - k \\ \\ \lambda_2^2(v - k) \end{cases} \equiv 0 \pmod{2^{e+1}}$$

and

$$(r_i, r_j) = \begin{cases} s - k \\ \\ \lambda_2(s - k) \end{cases} \equiv 0 \pmod{2^e}.$$

It follows that $(z, z) \equiv 0 \pmod{2^{e+1}}$.

Next we prove that C_d is self-orthogonal. If the binary vector $a \in C_d$, then there exists $z \in L$ such that $z \equiv 2^d a \pmod{2^{d+1}}$. Thus $z = 2^d a + 2^{d+1} b$ and

$$(z, z) = 2^{2d}(a, a) + 2 \cdot 2^{2d+1}(a, b) + 2^{2d+2}(b, b) \equiv 0 \pmod{2^{2d+2}},$$

so $(a, a) \equiv 0 \pmod 4$.

Since $k \equiv 1 \pmod 4$, the code

$$C_d^* = \{(a_1, \ldots, a_{v-1}) | (a_1, \ldots, a_{v-1}, 0, 0) \text{ or } (a_1, \ldots, a_{v-1}, 1, 1) \in C_d\}$$

is self-orthogonal with all weights divisible by 4. Since $\dim C_d^* \geq \dim X_d' - 1 \geq v/2 - 1$, we have by Lemma 2 that $v - 1 \equiv \pm 1 \pmod 8$, and since $v \equiv 2 \pmod 4$, we may conclude that $v \equiv 2 \pmod 8$. □

LEMMA 4. *If* $v \equiv 1 \pmod 2$ *then after possibly taking complements either*

(1) $k \equiv -1 \pmod 4$ *and* $v \equiv -1 \pmod 8$, *or*
(2) $k \equiv 1 \pmod 4$ *and* $v \equiv 1 \pmod 8$.

Proof. After possibly taking complements we may suppose both k and v are odd. Let

$$C = \begin{bmatrix} A & j^t \\ \lambda_2 j & \lambda_2 \end{bmatrix}$$

and $D = \text{diag}[1, \ldots, 1, -k]$. Note that $2^{e+1} \mid \lambda(v - k)$. Blokhuis and Calderbank prove that X and X' have the same 2-SNF and that $\dim X'_d \geq (v + 1)/2$. Note that $\dim C_d \geq \dim X'_d \geq (v + 1)/2$.

The argument employed in Lemma 3 proves that $(a, a) \equiv 0 \pmod 4$ for all $a \in C_d$. If $k \equiv -1 \pmod 4$ then the weight, $wt(a) \equiv (a, a) \equiv 0 \pmod 4$. Thus C_d is self-dual with all weights divisible by 4, and so by Lemma 1 $v \equiv -1 \pmod 8$.

If $k \equiv 1 \pmod 4$, let

$$C_d^* = \{(a_1, \ldots, a_{v-1}) \mid (a_1, \ldots, a_{v-1}, 0, 0) \text{ or } (a_1, \ldots, a_{v-1}, 1, 1) \in C_d\}.$$

Clearly $wt(a') \equiv 0 \pmod 4$ for all $a' \in C_d^*$. Since $\dim C_d^* \geq \dim C_d - 1$, C_d^* is self-dual with all weights divisible by 4. Hence by Lemma 1 we have $v \equiv 1 \pmod 8$. □

LEMMA 5. *If* $v \equiv k \equiv 0 \pmod 2$ *then either*

(1) $(s)_2 \equiv (v - k)_2 \equiv 1 \pmod 2$, *or*
(2) $v \equiv 0 \pmod 8$.

Proof. If (1) does not hold, then after taking complements if necessary, we may suppose $s = 2^{2n}\sigma$ where σ is odd and $n \geq 1$. If $2n > e$ then X'_d is a self-dual code with all weights divisible by 4, and so $v \equiv 0 \pmod 8$.

Therefore, suppose $2n < e$. Let

$$C = \begin{bmatrix} A & 2^n j^t \\ \lambda_2 j & 2^n \lambda_2 \end{bmatrix}$$

and $D = \text{diag}[1, \ldots, 1, -k/2^{2n}]$. By Lemma 5.2 of [1] $(\lambda)_2$ is odd, X and X' have different 2-SNFs, and $\dim X'_d \geq v/2$. Note $2^e \| \lambda(v - k)$, so that $(v - k)_2$ is even. Hence $v \equiv 0 \pmod 4$. Since $(\lambda)_2$ is odd, we have $2^{e+1} \mid \lambda_2^2(v - k)$ and the arguments employed in Lemma 3 give $(a, a) \equiv 0 \pmod 4$ for all $a \in C_d$.

If $k/2^{2n} \equiv -1 \pmod 4$ then $(a, a) \equiv wt(a) \equiv 0 \pmod 4$. It follows from Lemma 1 that $v + 1 \equiv \pm 1 \pmod 8$ and hence $v \equiv 0 \pmod 8$. If $k/2^{2n} \equiv 1 \pmod 4$ then let C_d^* be as in Lemmas 3 and 4. It follows that $v - 1 \equiv \pm 1 \pmod 8$ and we may conclude $v \equiv 0 \pmod 8$. □

The theorem is the result of combining Lemmas 3, 4 and 5.

3. Conclusion

We conclude this paper with a list of feasible parameter sets for which $2^e \| r - \lambda$, indicating those excluded by the conditions of the theorem (see Table 1). The following is a list for $s_2 - s_1 = 8$ and $v < 1500$. A minus (−) indicates that the parameter set has been

Table 1. Possible parameter sets for 2-designs.

v	k	s_1	s_2	λ	s	Case	Test
71	23	7	15	805	7	*iii*	
93	45	21	29	690	5	*ii*	
130	52	20	28	172	4	*iv*	*
161	65	25	33	520	1	*ii*	
210	70	22	30	418	6	*iv*	*
217	105	49	57	540	1	*ii*	
271	127	55	63	1905	7	*iii*	
273	128	56	64	2176	0	*iic*	
277	117	45	53	2691	5	*ii*	−
283	112	4	48	5264	0	*iiic*	−
301	141	61	69	705	5	*ii*	−
302	106	34	42	4558	2	*iv*	−
309	144	64	72	672	0	*iiic*	
325	117	37	45	810	5	*ii*	−
331	91	19	27	1001	3	*iii*	−
331	155	67	75	465	3	*iii*	−
337	112	32	40	896	0	*iic*	
341	165	77	85	510	5	*ii*	−
342	114	34	42	2046	2	*iv*	−
349	96	24	32	2784	0	*iic*	−
351	111	31	39	3885	7	*iii*	
371	35	3	11	185	3	*iii*	−
378	108	28	36	1508	4	*iv*	*
391	55	7	15	715	7	*iii*	
475	75	11	19	237	3	*iii*	
477	189	69	77	357	5	*ii*	−
495	144	40	48	304	0	*iiic*	
511	175	55	63	425	7	*iii*	
573	144	32	40	672	0	*iic*	−
649	73	1	9	657	1	*ii*	
651	155	35	43	325	3	*iii*	−
657	81	9	17	738	1	*ii*	
715	187	43	51	357	3	*iii*	−
770	110	14	22	1538	6	*iv*	*
771	51	3	11	1309	3	*iii*	−
801	81	1	9	720	1	*ii*	
806	140	20	28	3220	4	*iv*	*
961	465	217	225	480	1	*ii*	
1066	246	54	62	426	6	*iv*	*
1179	171	19	27	589	3	*ii*	−
1198	172	20	28	1204	4	*iv*	*
1353	105	1	9	910	1	*ii*	
1450	190	22	30	874	6	*iv*	*
1497	153	9	17	561	1	*ii*	

excluded by the theorem. An asterisk (*) indicates that though the theorem failed to eliminate this set, it is eliminated by results in [2]. We also indicate to which case of the theorem each parameter set corresponds, with a c denoting a need to take the complement. All together, 26 of the 44 parameter sets are eliminated, 18 by the theorem.

Note that there exists a quasi-symmetric design with parameters $v = 127$, $b = 2007$, $r = 651$, $k = 31$, $\lambda = 155$ with intersection numbers $x = 7$, $y = 15$; the blocks of this design are the 4-dimensional subspaces in $PG(6, 2)$. These parameters do not appear in the table since $r - \lambda = 496$, which is divisible by $2^{e+1} = 16$.

One notes that case i) of the theorem does not occur in the list. In fact, it can be shown that for $e = 1$ this case is impossible (cf. [2]). It would be of interest to know whether or not this case can occur for $e > 1$.

Acknowledgment

The author thanks A.R. Calderbank for suggesting this problem and for many helpful discussions. The author also thanks A. Blokhuis for generating the table of feasible parameter sets.

References

1. A. Blokhuis and A.R. Calderbank, Quasi-symmetric designs and the Smith Normal Form. *Designs, Codes and Cryptography*, Vol. 2, (1992), pp. 189–206.
2. A.R. Calderbank, The application of invariant theory to the existence of quasi-symmetric designs. *J. Combinatorial Theory (A)*, Vol. 44, (1987), pp. 94–109.
3. A.M. Gleason, Weight polynomials of self-dual codes and the MacWilliams indentities, In *Actes Conges Internl. de Mathématique*, Vol. 3, pp. 211–315. Gauthier-Villars, Paris, (1971).
4. C.L. Mallows and N.J.A. Sloane, Weight enumerators of self-orthogonal codes, *Discrete Math.*, Vol. 9, (1974), pp. 391–400.
5. V. Tonchev, Quasi-symmetric designs and self-dual codes, *European J. Comb.*, Vol. 7, (1986), pp. 67–73.