Block Designs with SDP Parameters

Harold N. Ward

Department of Mathematics
University of Virginia
Charlottesville, VA 22904
United States of America

hnw@virginia.edu

For Virginia Warfield
on her retirement from the
University of Washington

Submitted: Apr 19, 2012; Accepted: Jul 27, 2012; Published: Aug 9, 2012

Abstract

It is traditional to call a quasi-symmetric design with certain parameters an SDP design if the symmetric difference of two different blocks is either a block or a block complement. In this note, we delete the requirements on the parameters and demand just that the symmetric difference of two blocks be a block, a block complement, or either the empty set or the whole point set. We obtain the parameters of such designs and use the result to prove Kantor's theorem on the parameters of a symmetric SDP design. A spin-off of an exponential Diophantine equation considered by Ramanujan is at the core.

1 GP designs

For a (v, k, λ) design $\mathcal{D}$, let $\mathcal{P}$ be the point set, of size v, and let $\mathcal{B}$ be the block set, of size $b = \lambda v(v-1)/(k(k-1))$. Each block has size k and each point is in $r = \lambda(v-1)/(k-1)$ blocks. If $\mathcal{D}$ is a symmetric design, $\mathcal{D}$ is said to be an SDP (Symmetric Difference Property) design when the symmetric difference of any three blocks is either a block or a block complement. We identify subsets of $\mathcal{P}$ with their binary characteristic vectors, making the symmetric difference of subsets their (binary) sum. The complement of an SDP symmetric design is also one.

W. M. Kantor proved that any symmetric SDP design (apart from the trivial $(2, 1, 0)$ design) has parameters

$$v = q, \quad k = \frac{q}{2} + \delta\frac{\sqrt{q}}{2}, \quad \lambda = \frac{q}{4} + \delta\frac{\sqrt{q}}{2}, \tag{1}$$

where q is an even power of 2 and $\delta = \pm 1$ [K, Theorem 3]. Both the derived and residual designs, with respect to a block, have the property that the sum of any two different blocks is either a block or a block complement (Lemma 6, ahead). The derived and residual designs have parameters

$$\begin{aligned} &\text{derived:} \qquad v = \frac{q}{2} + \delta\frac{\sqrt{q}}{2}, \quad k = \frac{q}{4} + \delta\frac{\sqrt{q}}{2}, \quad \lambda = \frac{q}{4} + \delta\frac{\sqrt{q}}{2} - 1 \\ &\text{residual:} \qquad v = \frac{q}{2} - \delta\frac{\sqrt{q}}{2}, \quad k = \frac{q}{4}, \quad \lambda = \frac{q}{4} + \delta\frac{\sqrt{q}}{2}, \end{aligned} \tag{2}$$

again with q an even power of 2. The designs of all of these parameter sets have orders $r-\lambda = q/4$. The complements of these designs also have the block-sum property. This collection of parameters also contains those of the complements (recall that the complement of a derived [residual] design is the residual [derived] design of the complement of the original). The block-sum property can be rephrased to say that the set $\{B, B' | B \in \mathcal{B}\} \cup \{\varnothing, \mathcal{P}\}$, where B' is the complement $\mathcal{P} + B$ of B, is a group (an elementary Abelian 2-group). We make the following definition:

Definition 1. *A design is called a GP (group property) design if the set*

$$\mathcal{G} = \{B, B' | B \in \mathcal{B}\} \cup \{\varnothing, \mathcal{P}\}$$

is a group under symmetric difference.

The complement of a GP design is also a GP design. It is traditional to call a nonsymmetric design an SDP design if it is a GP design and it (or its complement) has the parameters in (2) (see the summary by V. D. Tonchev in [CD, VII.1.9]). The purpose of this note is to show that any nonsymmetric GP design (or its complement) that is not a Hadamard 3-design does have the parameters in (2). From that we can infer Kantor's theorem for symmetric SDP designs. Part of the point of doing this is that the proof of our result is an elementary number-theoretic argument, and obtaining Kantor's theorem as a corollary avoids some of the complexities of that theorem's proof. Moreover, the customary attendant specification of the parameters for GP designs can almost be omitted.

Let $\mathcal{D}$ be a GP design. If $B_1 + B_2 = B_3$, with $B_i \in \mathcal{B}$, then as $|B_1 + B_2| = 2(k - |B_1 \cap B_2|)$, $|B_1 \cap B_2| = k/2$. If $B_1 + B_2 = B_3'$ instead, then $|B_1 \cap B_2| = (3k - v)/2$. Suppose first that these two intersection numbers are the same, which means that $v = 2k$. Then $\mathcal{D}$ cannot be symmetric, for if so, the second design equation

$$r(k-1) = \lambda(v-1) \tag{3}$$

would entail the impossibility $k(k-1) = \lambda(2k-1)$. The only other conceivable intersection number is 0, so $\mathcal{D}$ must be a quasi-symmetric design with intersection numbers $x = 0$ and $y = k/2$ (thus the complement of some block is also a block; that fact would imply that $v = 2k$). Then [SS, Proposition 3.17] applies:

$$(r-1)(y-1) = (k-1)(\lambda-1). \tag{4}$$

Solving this along with (3) gives $r = 2k - 1$ and $\lambda = k - 1$. As now $b = 2v - 2$, Theorem 5.8 of [CvL] implies that $\mathcal{D}$ is either a Hadamard 3-design or the unique $(6, 3, 2)$ design [CD, II Example 1.18]. But this latter citation shows that the $(6, 3, 2)$ design does not qualify as a GP design. The Hadamard matrices involved in the 3-designs must actually be of Sylvester type because of the group property. (A Sylvester type Hadamard matrix is one equivalent to a Kronecker power of $\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$, or (equivalently!) to the character table of an elementary Abelian 2-group; see [CvL, Example 1.31], for instance.)

However, we can see all this identification rather more directly: if B is any block of $\mathcal{D}$, then on counting the blocks other than B that meet B (a standard maneuver), we get $k(r-1)/y = 4k - 4 = b - 2$. The missing two blocks can only be B and B'; so the complement of *any* block is also a block. If the group $\mathcal{G}$ for the GP property has size $2q$, q a power of 2, then the design parameters are

$$v = q, \quad b = 2q - 2, \quad r = q - 1, \quad k = q/2, \quad \lambda = q/2 - 1. \tag{5}$$

Moreover, if B_1 and B_2 are different blocks with $B_2 \neq B_1'$, then $B_1 + B_2$ must be a block. From this we infer that $\mathcal{D}$ is a Hadamard 3-design based on a Sylvester matrix. Another way to present the design is as the set of supports of the words of weight $q/2$ in the first order Reed-Muller code $\mathcal{R}(1, m)$, where $q = 2^m$ (see [AK] for these codes). Thus we have

Proposition 2. *If $\mathcal{D}$ is a GP design for which $v = 2k$, then $\mathcal{D}$ is a Hadamard 3-design corresponding to a Sylvester type Hadamard matrix.*

Now take $v \neq 2k$. Then no block complement is also a block, and the two possible intersection numbers $k/2$ and $(3k - v)/2$ are different. Could $\mathcal{D}$ be symmetric? If so, then $\lambda = k/2$ or $(3k - v)/2$. Say that $\lambda = k/2$. Then $k(k-1) = k/2 \times (v-1)$ gives $v = 2k - 1$. Hence $\mathcal{D}$ is a Hadamard 2-design, and the group property again implies that the corresponding Hadamard matrix is of Sylvester type. If $\lambda = (3k - v)/2$, then $v = 2k + 1$ and $\lambda = (k-1)/2$. This is also a Hadamard 2-design, with Sylvester matrix. Thus

Proposition 3. *If $\mathcal{D}$ is a symmetric GP design, then $\mathcal{D}$ is a Hadamard 2-design, and again the corresponding Hadamard matrix is of Sylvester type.*

The design with $v = 2k - 1$ can also be realized as the set of supports of the words of weight $q/2$ in the punctured first-order Reed-Muller code $\mathcal{R}(1, m)^*$, $q = 2^m$. Incidentally, the sum of two different blocks is a block; but for $k > 1$, there are three blocks whose sum is $\varnothing$. Thus the design is not an SDP design–as it better well not be!

There is one more special case: it could be that the intersection number $(3k - v)/2$ is 0, that is, that $v = 3k$. Now when we solve (4) and the design equations we get $k = 3 - 8/(r + 3)$. The possibilities are $r = 1$ and 5, giving the trivial $(3, 1, 0)$ design and the $(6, 2, 1)$ design whose blocks are the 2-subsets of a 6-set. The parameters are those of (2) with $q = 4$ and $\delta = -1$ in the residual set and with $q = 16$ and $\delta = -1$ in the derived set.

Thus finally we may assume that $\mathcal{D}$ is a quasi-symmetric design with intersection numbers $x = (3k - v)/2$ and $y = k/2$, x and y different ($\mathcal{D}$ is *proper*) and both positive. We may also take $k < v/2$ by replacing $\mathcal{D}$ with its complement, if necessary. Let the order of $\mathcal{G}$ be $2q$, q a power of 2 as before, so that now $b = q - 1$, since no block complement is a block. The equation generalizing (4) is

$$k(r-1)(x+y-1) + xy(1-b) = k(k-1)(\lambda-1)$$

[SS, Lemma 3.23(i)]. This becomes (after a cancellation of k)

$$(r-1)(2k - \frac{v}{2} - 1) - (q-2)\frac{3k-v}{4} = (k-1)(\lambda-1).$$

Solving it with the design equations gives

$$r = \frac{k(v-1)}{v-(v-2k)^2}, \quad \lambda = \frac{k(k-1)}{v-(v-2k)^2}, \quad q = \frac{4k(v-k)}{v-(v-2k)^2}.$$

Substituting $v - (v-2k)^2 = 4k(v-k)/q$ from the third equation into the other two, we get

$$\lambda = \frac{q(k-1)}{4(v-k)}, \quad r = \frac{q(v-1)}{4(v-k)}.$$

Now by [SS, Corollary 3.9], $y - x$ divides both $k - x$ and $r - \lambda$. Here

$$y - x = \frac{v-2k}{2}, \quad k - x = \frac{v-k}{2}, \quad r - \lambda = \frac{q}{4}.$$

Thus $(v - 2k)$ divides $q/2$, so that $v - 2k = q_0$, q_0 also a power of 2, with $q_0 < q$ (we have assumed that $k < v/2$). Then $v = q_0 + 2k$ and the equation for q is

$$q = \frac{4k(q_0+k)}{q_0 + 2k - q_0^2}.$$

Thus

$$4k^2 + (4q_0 - 2q)k + qq_0^2 - qq_0 = 0,$$

making

$$k = \frac{q}{4} - \frac{q_0}{2} + \delta\frac{q_0}{2}\sqrt{\left(\frac{q}{2q_0}\right)^2 - q + 1}, \tag{6}$$

$\delta = \pm 1$. So it must be that

$$\left(\frac{q}{2q_0}\right)^2 - q + 1 = z^2 \tag{7}$$

for some integer z.

Equation (7) is a particular case of the exponential Diophantine equation

$$2^N \pm 2^M \pm 2^L = z^2,$$

N, M, L, and z being integers (in the notation of [S], which gives some of the equation's background, along with references). The prototype is $2^N - 2^3 + 1 = z^2$, conjectured by S. Ramanujan in 1913 to have solutions just for $N = 3, 4, 5, 7, 15$. This was proved to be true by T. Nagell in 1948. For $2^N - 2^M + 1 = z^2$, one has the trivial solutions $N = 2t, M = 0, z = 2^t$, $t \geqslant 0$; the cases $N = 5, 7, 15$ in Ramanujan's equation ($M = 3$); and two parameterized families

$$\begin{aligned} N &= 2t, \quad M = t + 1, \quad z = 2^t - 1, \quad t \geqslant 2 \\ N &= M = t, \quad z = 1, \quad t \geqslant 1 \end{aligned}$$

[S, Theorem 2]. We shall give a direct proof for the case relevant to the designs in Lemma 4.

For $\mathcal{D}$, $2^N = (q/2q_0)^2$ and $2^M = q$. We want $q > 1$, of course, so the possibilities are

$$\begin{aligned} \frac{q}{2q_0} &= \frac{q}{2} = 2^t, \quad \text{with } z = \frac{q}{2} - 1, \\ \frac{q^2}{4q_0^2} &= q, \quad \text{with } z = 1 \end{aligned}$$

(the Ramanujan solutions are out because N must be even). The first makes $q_0 = 1$. Then $k = q/4 - 1/2 + \delta(q/2 - 1)/2$. Only $\delta = 1$ works, giving $k = q/2 - 1$ and $v = q - 1$. But then $\mathcal{D}$ is a symmetric design and already dealt with (also excluded here by $x \neq y$). The second has $q_0 = \sqrt{q}/2$, q now being an even power of 2. Then equation (6) becomes

$$k = \frac{q}{4} - \frac{\sqrt{q}}{4} + \delta\frac{\sqrt{q}}{4} = \frac{q}{4} \text{ or } \frac{q}{4} - \frac{\sqrt{q}}{2}.$$

This, with complements, produces the parameters of (2).

Lemma 4. *Suppose that X and Y are two powers of 2 for which $X^2 - Y + 1 = Z^2$, with $Z > 0$. Then one of the following holds:*

$$\begin{aligned} Y &= 1 \text{ and } Z = X \\ Y &= 2X \text{ and } Z = X - 1 \\ Y &= X^2 \text{ and } Z = 1. \end{aligned}$$

Proof. Rewrite the equation as $(X + Z)(X - Z) = Y - 1$. Certainly $Z \leqslant X$, so write $Z = X - A$, with $0 \leqslant A < X$. Then we need $A(2X - A) = Y - 1$. If $A = 0$, we have $Y = 1$ and $Z = X$. If $A = 1$, then $Y = 2X$ and $Z = X - 1$. In addition, $A \leqslant Y - 1$; but if $A = Y - 1$, then $Y = 2X$ again, but now $Z = 1 - X \leqslant 0$. Thus we may assume that $1 < A < Y - 1$ and $2X - A < Y - 1$, wherewith $X < Y - 1$. Then $2X \leqslant Y$, as X and Y are powers of 2. Since $Y = 2X$ has been covered, we take $2X < Y$. Let $B = 2X - A$. As $A > 1$, so $X \geqslant 2$; both Z and A are odd.

Now let $A = 2A' - \Delta$, with $\Delta = \pm 1$ chosen to make A' odd. Then

$$(A + \Delta)(B + \Delta) = AB + \Delta(A + B) + 1$$

implies that

$$\begin{aligned} 2A'(B+\Delta) &= Y + 2\Delta X \\ &= 2X(\frac{Y}{2X} + \Delta). \end{aligned}$$

The second factor here is odd since $2X < Y$. Thus X is the exact power of 2 dividing $B + \Delta$, and $B = XB' - \Delta$, with B' odd. Then

$$2X = A + B = 2A' + XB' - 2\Delta,$$

and

$$\Delta = A' + \frac{X}{2}(B' - 2).$$

Therefore $X/2(B' - 2) = \Delta - A' \leqslant 0$, and it can only be that $B' = 1$. Thus $B = X - \Delta$, $A = X + \Delta$, and $Y - 1 = AB = X^2 - 1$, giving the third possibility, $Y = X^2$. □

The grand summary is then

Proposition 5. *If $\mathcal{D}$ is a (v, k, λ) GP design with $v \neq 2k$ that is not symmetric, then (v, k, λ) is one of the triples given in (2).*

2 SDP designs

In this section, we present a proof of Kantor's theorem giving the parameters of (symmetric) SDP designs. First we verify that the derived and residual designs of an SDP design are GP designs.

Lemma 6. *If $\mathcal{D} = (\mathcal{P}, \mathcal{B})$ is an SDP design and D is a block of $\mathcal{D}$, then both the derived and residual designs of $\mathcal{D}$ with respect to D are GP designs.*

Proof. For $X, Y \subseteq \mathcal{P}$, the characteristic function of $X \cap Y$ is the component-wise product XY. If $B_1, B_2 \in \mathcal{B}$, then $B_1 + B_2 + D$ is either a block B or its complement B'. That is, $(B_1 + B_2 + D)D = BD$ or $B'D$. Hence $B_1D + B_2D = BD + D$ or BD. Thus the sum of two blocks of the derived design, if not $\varnothing$, is either a block or its complement. So the derived design is a GP design. The proof for the residual is similar. □

Now let $\mathcal{D} = (\mathcal{P}, \mathcal{B})$ be a (v, k, λ) SDP design, so that the parameters of a residual design $\mathcal{D}'$ are

$$v' = v - k, \quad b' = v - 1, \quad r' = k, \quad k' = k - \lambda, \quad \lambda' = \lambda \tag{8}$$

(we can safely assume that $v > 2$). By Lemma 6, these must be the parameters of a GP design. We run through the possibilities presented in the propositions in Section 1. The only way $\mathcal{D}'$ can be a symmetric design (Proposition 3) is that $k = 1$. Then SDP requires $\mathcal{D}$ to be the excluded trivial $(2, 1, 0)$ design or the equally trivial $(3, 1, 0)$

design we encountered before. Suppose then that $v' = 2k'$ (Proposition 2), so that $\mathcal{D}'$ is a Hadamard 3-design with parameters given by (5) for some q (this will be true then for *any* residual design). Then $v = 2q - 1$, $k = q - 1$, $\lambda = q/2 - 1$, and $\mathcal{D}$ is a Hadamard 2-design. The key point here is that if $D \in \mathcal{B}$, then in the residual with respect to D, each block complement is also a block. Let $B_1, B_2 \in \mathcal{B}$ be such that the residual blocks B_1D' and B_2D' are complements. Since $|B_1B_2|$, $|B_1D|$, and $|B_2D|$ are all $q/2 - 1$, and B_1D' and B_2D' are disjoint, it can only be that $B_1D = B_2D$. That makes

$$\begin{aligned} B_1 + B_2 + D &= (B_1 + B_2 + D)D' + (B_1 + B_2 + D)D \\ &= B_1D' + B_2D' + DD' + B_1D + B_2D + DD \\ &= D' + D = \mathcal{P}. \end{aligned}$$

But this gainsays SDP.

Thus we are left with $\mathcal{D}'$ being described by Proposition 5. Only the parameters in the residual list of (2) are quasi-residual ($\lambda v = k(k + \lambda - 1)$), so the values in (8) would match a triple in that list. That is,

$$v - k = v' = \frac{q}{2} - \delta\frac{\sqrt{q}}{2}, \quad k - \lambda = k' = \frac{q}{4}, \quad \lambda = \lambda' = \frac{q}{4} + \delta\frac{\sqrt{q}}{2}.$$

So

$$v = q, \quad k = \frac{q}{2} + \delta\frac{\sqrt{q}}{2}, \quad \lambda = \frac{q}{4} + \delta\frac{\sqrt{q}}{2},$$

a parameter triple from (1).

References

[AK] E. F. Assmus, Jr. and J. D. Key, Designs and their Codes, Cambridge Tracts in Mathematics 103, Cambridge University Press, Cambridge, UK, 1992.

[CvL] P. J. Cameron and J. H. van Lint, Designs, Graphs, Codes and their Links, London Math. Soc. Student Texts **22**, Cambridge University Press, Cambridge, UK, 1991.

[CD] Handbook of Combinatorial Designs, second edition, C. J. Colbourn and J. H. Dinitz, editors, Chapman and Hall/CRC, Boca Raton, FL, 2007.

[K] W. M. Kantor, Symplectic groups, symmetric designs, and line ovals, *J. Algebra* **33** (1975), 43–58.

[SS] M. S. Shrikhande and S. S. Sane, Quasi-Symmetric Designs, London Math. Soc. Lecture Note Series **164**, Cambridge University Press, Cambridge, UK, 1991.

[S] L. Szalay, The equations $2^N \pm 2^M \pm 2^L = z^2$, *Indag. Math. (N.S.)* **13**(1) (2002), 131–142.