On a class of symmetric divisible designs which are almost projective planes

Aart Blokhuis
Technical University of Eindhoven
Den Dolech 2
5600 MB Eindhoven
The Netherlands

Dieter Jungnickel and Bernhard Schmidt
Lehrstuhl für Diskrete Mathematik, Optimierung
und Operations Research
Universität Augsburg
86135 Augsburg
Germany

Abstract

We consider a class of symmetric divisible designs $\mathcal{D}$ which are almost projective planes in the following sense: Given any point p, there is a unique point p' such that p and p' are on two lines, whereas any other point is joined to p by exactly one line; and dually. We note that either the block size k or $k-2$ is a perfect square, and exhibit examples for $k = 3$ and $k = 4$. Then we add the condition that $\mathcal{D}$ should admit an abelian Singer group, so that we may study the associated divisible difference sets. Under this additional assumption, we show that k is a square (unless $k = 3$) and that the only possible prime divisors of k are 2 and 3.

1 Preliminaries

About 15 years ago, Zoltan Füredi suggested to consider a class of symmetric divisible designs $\mathcal{D}$ which are in some sense as close to projective planes as possible. More precisely, $\mathcal{D}$ should be a square 1-design satisfying the following two axioms:

(A1) Given any point p, there is a unique point p' such that p and p' are on two lines, whereas any other point is joined to p by exactly one line.

(A2) Given any line L, there is a unique line L' such that L and L' intersect in two points, whereas any other line intersects L uniquely.

For the purposes of this paper, we shall denote such a structure as an APP(k) (for "almost projective plane") if it has line size k.

Example 1.1 Developing the start block $\{0, 1, 3\}$ modulo 6 gives an APP(3); similarly, an APP(4) arises from the start block $\{0, 1, 6, 10\} \subseteq \mathbb{Z}_{12}$.

In the language of design theory, an APP(k) is just a symmetric divisible design with parameters

$$m = k(k-1)/2,\ n = 2,\ k,\ \lambda_1 = 2 \text{ and } \lambda_1 = 1, \tag{1}$$

cf. [2] or [8]. In view of the fact that the axioms (A1) and (A2) are so close to those for projective planes, we prefer to speak of "lines" instead of "blocks". We shall also call the point x' in axiom (A1) the *mate* of the point x, and similarly for lines.

Of course, we hoped to find some more interesting examples than the ones given above, maybe even for values of k where $k-1$ is not a power of a prime. Unfortunately, we did not succeed with this, so our results will all be about non-existence. We begin with the following necessary condition which is a special case of the Bose-Connor theorem [3].

Proposition 1.2 *An APP(k) can only exist if either k or $k-2$ is a perfect square. More precisely, k has to be a square if $k \equiv 0$ or $1 \bmod 4$; if additionally $m = k(k-1)/2 \equiv 2 \bmod 4$, then $k-2$ has to be the sum of two squares. For $k \equiv 2$ or $3 \bmod 4$, $k-2$ must be a square, and the equation*

$$kx^2 + (-1)^{m(m-1)/2} \cdot 2y^2 = z^2 \tag{2}$$

has a non-trivial solution in integers.

Proof. For the convenience of the reader, we shall sketch a proof for the fact that either k or $k-2$ is a square, as this will be the part that we will mainly require in what follows. To this end, let A be an incidence matrix for an APP(k), where points and lines are arranged into consecutive pairs of mates. Then, by (A1) and (A2),

$$AA^T = A^TA = \begin{pmatrix} k & 2 & 1 & 1 & \dots & 1 & 1 \\ 2 & k & 1 & 1 & \dots & 1 & 1 \\ 1 & 1 & k & 2 & \dots & 1 & 1 \\ 1 & 1 & 2 & k & \dots & 1 & 1 \\ & & & & \ddots & & \\ 1 & 1 & 1 & \dots & 1 & k & 2 \\ 1 & 1 & 1 & \dots & 1 & 2 & k \end{pmatrix}$$
$$= (k-1)I + J + E,$$

where E denotes the direct sum of $\binom{k}{2}$ copies of the matrix $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$.

It is a bit tedious but routine to calculate the determinant of this matrix, either directly or by determining its eigenvalues. The result is

$$(\det A)^2 = \det AA^T = (k-2)^{(k^2-k)/2}k^{(k^2-k+2)/2}, \tag{3}$$

which implies the assertion, as the two exponents appearing in (3) always have opposite parity. □

Let us give the following sample application of Proposition 1.2 which will be useful later:

Corollary 1.3 *An APP(3^a) with $a \neq 1$ can only exist if a is even or $a = 3$.*

Proof. let a be odd, so that $3^a - 2$ is a perfect square. By a result of Ljunggren [5] (rediscovered by Nagell [6]), the only solution of the Diophantine equation $3^x - 2 = y^2$ indeed occurs for $x = 3$. □

In the next section, we add the condition that $\mathcal{D}$ should admit an abelian Singer group G, so that we may study the associated divisible difference sets with parameters $(k(k-1)/2, 2, k, 2, 1)$. Recall that a k-element subset D of a group G of order $v = mn$ is called a *divisible difference set* with parameters $(m, n, k, \lambda_1, \lambda_2)$, if the list of differences $(d - d' : d, d' \in D, d \neq d')$ covers every element in $G\backslash N$ exactly λ_2-times, and the elements in $N\backslash\{0\}$ exactly

λ_1 times, where N is a specified subgroup of G of order n. We provided two small cyclic examples above; see [4] or [8] for background on divisible difference sets. Under this additional assumption, we will prove that the only possible prime divisors of k are 2 and 3. The proof will involve a novel trick which is of independent interest and might turn out to be useful in other situations, too. Finally, we shall also obtain some further restrictions using standard tools like the Mann test [1]; in particular, it turns out that k has to be a square provided that $k \neq 3$.

2 Divisible difference sets for APP's

We now consider an APP(k) $\mathcal{D}$ admitting a *Singer group* G, that is, a group of automorphisms which acts regularly on points and thus also on lines, as $\mathcal{D}$ has full rank over $\mathbb{Q}$ by equation (3). Note that we exhibited cyclic examples for the cases $k = 3$ and $k = 4$ is Section 1. Our results will provide strong evidence for the conjecture that only these two cases can occur if we assume G to be abelian; parts of these results would carry over to non-abelian groups, but we will not bother stating this explicitly. As usual, we proceed by studying the group ring equation characterizing the associated divisible difference set D, as summarized in the following lemma; see [4] or [8] for background and details. In particular, we write G multiplicatively from now on and make use of the standard convention of identifying subsets of G with the corresponding formal sums of their elements in $\mathbb{Z}G$. We also require the notation

$$A^{(t)} := \sum_{g \in G} a_g g^t, \quad \text{where } A = \sum_{g \in G} a_g g,$$

and where t is some integer.

Lemma 2.1 *Let $\mathcal{D}$ be an APP(k) admitting a Singer group G. Then $\mathcal{D}$ is the development of a divisible difference set with parameters (1) in G; in particular, G has a unique subgroup N of order 2. Moreover, D may be any subset of G for which the associated group ring element $D = \sum_{d \in D} \in \mathbb{Z}G$ satisfies the equation*

$$DD^{(-1)} = (k-2) + G + N. \tag{4}$$

Proof. The assertions are merely special cases of well-known results on divisible difference sets; the only part which might need some comment is

the bit concerning N. This is an easy consequence of (A1) which shows that the point classes (which are just the cosets of the special subgroup N appearing in the divisible difference set condition) have size 2. Hence only one group ring element can appear as a "difference" twice, and thus G has a unique involution, as the number of "difference" representations $g = d(d')^{-1}$ of an element $g \in G$ always agrees with that of the inverse element g^{-1}. $\Box$

The following theorem gives a strong restriction on the possible values of k. It is our major result, and its proof should be of special interest as it contains a novel trick. First, it seems to be only the second example where a group ring of a characteristic p dividing the order of G is applied to study difference sets (the first case being work of Pott [7] concerning extraneous multipliers of planar difference sets, see also [2]). More importantly, the trick of computing intersection numbers of a certain auxiliary subset mod p and then using square counting in characteristic 0 to obtain a contradiction is certainly new and might well have other interesting applications.

Theorem 2.2 *Let D be a divisible difference set with parameters (1) in an abelian group G. Then $k = 2^a 3^b$ for some non-negative integers a and b.*

Proof. By Lemma 2.1, G has a unique subgroup N of order 2. We apply the canonical epimorphism π from G onto $H = G/N$ to equation (4) and obtain the following identity in the group ring $\mathbb{Z}H$:

$$\widetilde{D}\widetilde{D}^{(-1)} \;=\; k + 2H, \tag{5}$$

where we write $\widetilde{X}$ for the image of $X \in \mathbb{Z}G$ under the canonical extension of π to an epimorphism from $\mathbb{Z}G$ to $\mathbb{Z}H$. We now select a prime divisor p of k and consider equation (5) as an identity in the group algebra $\mathbb{Z}_pH$. Using this in conjunction with the well-known fact $X^p = X^{(p)}$, we get the validity of the following computation in $\mathbb{Z}_pH$:

$$\begin{aligned} \widetilde{D}^{(p)}\widetilde{D}^{(-1)} &= \widetilde{D}^p\widetilde{D}^{(-1)} \;=\; \widetilde{D}^{p-1}(\widetilde{D}\widetilde{D}^{(-1)}) \\ &= \widetilde{D}^{p-1}(k+2H) \;=\; k\widetilde{D}^{p-1} + 2k^{p-1}H \;=\; 0, \end{aligned}$$

as p divides k. This shows that all coefficients appearing in the group ring element

$$A \;=\; \widetilde{D}^{(p)}\widetilde{D}^{(-1)} \;=\; \sum_{h\in H} a_h h \in \mathbb{Z}H$$

are divisible by p. We will now use square counting for the a_h. Trivially,

$$\sum_{h\in H} a_h \;=\; k^2. \tag{6}$$

Next note that $\sum_{h\in H} a_h^2$ equals the coefficient of 1 in the group ring element $AA^{(-1)}$. But

$$\begin{aligned} AA^{(-1)} &= \widetilde{D}^{(p)}\widetilde{D}^{(-1)}\widetilde{D}\widetilde{D}^{(-p)} = \widetilde{D}^{(p)}\widetilde{D}^{(-p)}(k+2H) \\ &= \left[\widetilde{D}\widetilde{D}^{(-1)}\right]^{(p)}(k+2H) = k\left[\widetilde{D}\widetilde{D}^{(-1)}\right]^{(p)} + 2k^2H \\ &= k(k+2H^{(p)}) + 2k^2H. \end{aligned}$$

Thus the coefficient of 1 in $AA^{(-1)}$ is at most $k(k+2k)+2k^2$, depending on the number of elements of order p in H which can be at most $k-1$, as the Sylow p-subgroup of H has order at most k. This gives us the estimate

$$\sum_{h\in H} a_h^2 \le 5k^2. \tag{7}$$

Using (6) and (7) and the fact that all coefficients a_h are divisible by p, we get the following inequality:

$$0 \le \sum_{h\in H} a_h(a_h - p) \le 5k^2 - pk^2. \tag{8}$$

Clearly the preceding inequality gives a contradiction for $p \ge 7$. Now assume $p = 5$ and that (8) holds so that we have equality throughout. In particular, $a_h \in \{0, 5\}$ for all $h \in H$. Moreover, equality in (8) also requires equality in (7). As pointed out above, this implies that k is a power of 5 and that the Sylow 5-subgroup of H is elementary abelian. But then $\widetilde{D}^{(5)} \subseteq H^{(5)}$, which is a group of order $(k-1)/2$. Hence at least one coefficient of $\widetilde{D}^{(5)}$ must be ≥ 3, as D was a k-subset. But $\widetilde{D}^{(-1)}$ has one coefficient 2 (namely that of the element $dN = d'N$ of $H = G/N$, where d and d' are the two elements of D appearing in the "difference" representation of the unique involution in G from D), and so $A = \widetilde{D}^{(5)}\widetilde{D}^{(-1)}$ contains at least one coefficient $a_h \ge 6$. This contradiction rules out the case $p = 5$, too, and finishes the proof. □

3 Some further restrictions

In this final section, we provide some further restrictions on divisible difference sets associated with APP's, mainly using a standard tool, namely the Mann test; cf. [1] and [8].

Theorem 3.1 *Let D be a divisible difference set with parameters (1) in an abelian group G, and assume $k \neq 3$. Then k is a square of the form $k = 2^{2a}3^{2b}$ for some non-negative integers a and b.*

Proof. By Proposition 1.2, either k or $k-2$ is a square. It suffices to show that the latter case cannot arise; assume otherwise. By Theorem 2.2, 2 and 3 are the only primes that can divide k; hence either $k = 2 \cdot 3^b$ or $k = 3^b$, where b is odd.

In the first case, we apply the Mann test by selecting a subgroup U of G for which $H = G/U$ has order $u = 3$; then $N \subseteq U$. As 2 divides k and is selfconjugate modulo u (note $2 \equiv -1 \bmod 3$), the Mann test implies that 2 should divide k to an even power, a contradiction.

In the second case, Corollary 1.3 gives $k = 27$. We will rule out this possibility by an ad hoc argument involving the Mann test and intersection numbers. To this end, we select a subgroup U of G of order 13 and hence of index $u = 54$; thus $N \not\subseteq U$. As 5 divides $k-2$ and is selfconjugate modulo u (note $5^9 \equiv -1 \bmod 54$), the Mann test implies that 5 has to divide $k-2$ to an even power, which is, of course, true. Let us write $H = G/U$, and denote the image of our hypothetical divisible difference set in the group ring $\mathbb{Z}H$ by $\widetilde{D}$. By the proof of the extension of the standard Mann test given by Pott in [8, Theorem 2.4.6], the coefficients of $\widetilde{D} = \sum_{h \in H} a_h h$ are constant modulo 5 on the cosets of the image $\widetilde{N}$ of N. (Note that the conclusion of Pott's result is satisfied; thus we do not get an immediate contradiction but have to analyse the situation more closely.) The image of equation (4) in $\mathbb{Z}H$ in our special case is given by

$$\widetilde{D}\widetilde{D}^{(-1)} \;=\; 25 + 13H + \widetilde{N}. \tag{9}$$

Now $\widetilde{D}$ cannot be absolutely constant on on the cosets of $\widetilde{N}$ since otherwise $\widetilde{D} = \widetilde{N}X$ for some $X \in \mathbb{Z}H$, contradicting equation (9). Thus $\widetilde{D}$ has at least one coefficient ≥ 5. Equating the coefficient of 1 in equation (9), we obtain

$$\sum_{h \in H} a_h^2 \;=\; 39. \tag{10}$$

But $\sum a_h = 27$ and the minimum of $\sum a_h^2$ under the conditions $a_h \geq 5$ for at least one h and $\sum a_h = 27$ is $5^2 + 22 = 47$, contradicting (10). □

We conclude with the following further restriction:

Proposition 3.2 *Let D be a divisible difference set with parameters (1) in an abelian group G, where $k \neq 3$ is a power of 3. Then $k = 3^{4a}$ for some positive integer a.*

Proof. We once again use the Mann test. By Proposition 1.2, k is a square; hence it suffices to rule out the possibility $k = 3^{4a+2}$. In this case, $k \equiv$

9 mod 16 and hence $k-2 \equiv 7 \bmod 16$. In particular, there has to exist some prime $p \equiv 3 \bmod 4$ dividing the square-free part of $k-2$. As k is a square, we see that 2 is a square modulo p, and thus in fact $p \equiv 7 \bmod 8$, by a well-known result from number theory. Now select a subgroup U of G for which $H = G/U$ has order $u = 8$; then $N \not\subseteq U$, as $v = k(k-1) \equiv 8 \bmod 16$. As p divides $k-2$ and is selfconjugate modulo u (note $p \equiv 7 \equiv -1 \bmod 8$), the Mann test implies that p has to divide $k-2$ to an even power, a contradiction. □

Acknowledgments. The authors thank Robert Calderbank for mentioning Füredi's problem to them and for letting them see his unpublished notes about this topic. They are also indebted to J.H.E. Cohn for pointing out references [5] and [6]. Most of the research for this paper was done while the second author visited the Department of Mathematics and Computer Science of the Technical University of Eindhoven; he gratefully acknowledges the hospitality and financial support provided by TUE.

References

[1] K.T. Arasu, D. Jungnickel and A. Pott: The Mann test for divisible difference sets. *Graphs Comb.* **7** (1991), 209–217.

[2] T. Beth, D. Jungnickel and H. Lenz: *Design theory (2nd edition).* Cambridge University Press (1999).

[3] R.C. Bose and W.S. Connor: Combinatorial properties of group divisible incomplete block designs. *Ann. Math. Stat.* **23** (1952), 367–383.

[4] D. Jungnickel: On automorphism groups of divisible designs. *Canadian J. Math.* **34** (1982), 257–297.

[5] W. Ljunggren: Über einige Arcustangensgleichungen, die auf interessante unbestimmte Gleichungen führen. *Ark. Mat. Astr. Fys.* **29A** (1943), no.13.

[6] T. Nagell: Verallgemeinerung eines Fermatschen Satzes. *Archiv Math.* **5** (1954), 153–159.

[7] A. Pott: On abelian difference sets with multiplier -1. *Archiv Math.* **53** (1989), 510–512.

[8] A. Pott: *Finite geometry and character theory.* Lecture Notes in Mathematics **1601**, Springer, Berlin (1995).