Des. Codes Cryptogr. (2009) 51:131–140
DOI 10.1007/s10623-008-9249-8

Polarities, quasi-symmetric designs, and Hamada's conjecture

Dieter Jungnickel · Vladimir D. Tonchev

Received: 10 July 2008 / Revised: 24 September 2008 / Accepted: 17 October 2008 /
Published online: 26 November 2008

Abstract We prove that every polarity of $PG(2k-1, q)$, where $k \geq 2$, gives rise to a design with the same parameters and the same intersection numbers as, but not isomorphic to, $PG_k(2k, q)$. In particular, the case $k = 2$ yields a new family of quasi-symmetric designs. We also show that our construction provides an infinite family of counterexamples to Hamada's conjecture, for any field of prime order p. Previously, only a handful of counterexamples were known.

Keywords Polarity · Projective geometry · Design · Quasi-symmetric design · Hamada's conjecture

Mathematics Subject Classifications (2000) 05B05 · 51E20 · 94B27

1 Introduction

We prove that every polarity of $PG(2k-1, q)$, where $k \geq 2$, gives rise to a design with the same parameters and the same intersection numbers as, but not isomorphic to, $PG_k(2k, q)$, the design of points and k-spaces in projective $2k$-space over $GF(q)$. The new designs are obtained by distorting the classical geometric designs with the help of the given polarity, acting on a fixed hyperplane in $PG(2k, q)$. In particular, the case $k = 2$ yields a new family of quasi-symmetric designs.

Communicated by J. D. Key.

D. Jungnickel (✉)
Lehrstuhl für Diskrete Mathematik, Optimierung, und Operations Research, Universität Augsburg,
86135 Augsburg, Germany
e-mail: jungnickel@math.uni-augsburg.de

V. D. Tonchev
Department of Mathematical Sciences, Michigan Technological University, Houghton, MI 49931, USA
e-mail: tonchev@mtu.edu

By construction, our new examples of designs with classical geometric parameters still share many properties with the geometric designs $PG_k(2k, q)$. In particular, there always is a set H of $q^{2k-1} + \cdots + q + 1$ points on which the blocks of the design induce an isomorphic copy of $PG(2k-1, q)$, while a copy of an affine $2k$-space $AG(2k, q)$ is induced on the set A formed by the remaining q^{2k} points. Moreover, the lines of the design joining two points of H or two points of A still have the natural geometric size, that is, $q+1$ or q, respectively, whereas a point of H and a point of A always determine a line of size 2.

We also show that our construction provides an infinite family of counterexamples to Hamada's conjecture [8] from 1973, for fields of arbitrary prime order, and for any dimension $2k \geq 4$. Previously, only a handful of counterexamples were known, namely two parameter sets, 2-(31, 7, 7) [7,29] and 3-(32, 8, 7) [29] for the binary case, and a single parameter set 2-(64, 16, 5) for the quaternary case ($q = 4$) [10,22].

Hamada's conjecture is of fundamental importance for two reasons. First, it indicates that the classical geometric designs, as designs having minimum p-rank among all possible designs with the given parameters, are the best choice to use for the construction of error-correcting codes with majority-logic decoding [24,25]. It is known that the number of non-isomorphic designs having the same parameters as the classical geometric designs of hyperplanes in $PG(n, q)$ or $AG(n, q)$, $n \geq 3$, grows exponentially with linear growth of n [15,17–19]. Secondly, the conjecture provides an elegant and computationally simple characterization of the classical geometric designs in terms of the p-rank of their incidence matrices: the complexity of computing the rank of a matrix is a cubic polynomial in the number of rows (or columns), while the complexity of finding isomorphisms between block designs is as hard as the notoriously difficult graph isomorphism problem; see [5, Remark VII.6.6].

2 A construction method for pseudo-geometric designs

We begin by describing a general method for constructing 2-designs with the same parameters as some classical geometric designs. To this end, let Π denote $PG(2k, q)$, the $2k$-dimensional projective space over the field $GF(q)$ with q elements. As is well-known, the points and k-spaces of Π form a 2-(v, K, λ) design $\mathcal{D} = PG_k(2k, q)$ with parameters

$$v = \frac{q^{2k+1} - 1}{q - 1}, \ K = \frac{q^{k+1} - 1}{q - 1}, \ \lambda = \frac{(q^{2k-1} - 1) \ldots (q^{k+1} - 1)}{(q^{k-1} - 1) \ldots (q - 1)}. \tag{1}$$

Furthermore, the lines of $\mathcal{D}$ are just the lines of Π and hence all have cardinality $q + 1$.[1]

Now let H denote a fixed hyperplane of Π. Trivially, the subspaces of Π induce a geometry Π_0 isomorphic to $PG(2k-1, q)$ on H. Since the lines of Π_0 are just those lines of $\mathcal{D}$ which are contained in H, we may view H as a copy of the projective space $PG(2k-1, q)$ in the design $\mathcal{D}$. Moreover, let A be the set of points not contained in H. Then the subspaces of Π induce a geometry Σ isomorphic to the affine space $AG(2k, q)$ on A. Now each line of Σ corresponds to a line ℓ of Π; of course, considered as a line of the affine space Σ, the projective line ℓ loses its *infinite point* $\ell \cap H$. Since ℓ is also a line of the design $\mathcal{D}$, we may view A as a copy of the affine space $AG(2k, q)$ in $\mathcal{D}$. In view of the preceding observations, we shall refer to H also as a *hyperplane* of $\mathcal{D}$.

[1] Recall that the *line* determined by two points of a design is defined as the intersection of all blocks containing these two points. See [4] for background on designs, and [12,11] for background on finite projective spaces.

More generally, let $\mathcal{D}'$ be any design with the parameters (1) of $PG_k(2k, q)$. If there exists a set H of $q^{2k-1} + \cdots + q + 1$ points on which the lines of the design induce an isomorphic copy of $PG(2k-1, q)$, while a copy of $AG(2k, q)$ is induced on the set A formed by the remaining q^{2k} points, we shall call H a *hyperplane* of $\mathcal{D}'$. The points of H will be referred to as the *infinite points* of $\mathcal{D}'$, and the points in A as the *affine points* of $\mathcal{D}'$.

If, in addition, the intersection numbers of $\mathcal{D}'$ are the same as those of $PG_k(2k, q)$, we shall call $\mathcal{D}'$ a *pseudo-geometric* design. Our main result will be a construction method for designs which are pseudo-geometric but not actually geometric.

We begin with a more general method yielding designs with the parameters of a geometric design $PG_k(2k, q)$. Given any *affine* block B of $\mathcal{D} = PG_k(2k, q)$—that is, any k-space of Π which is not contained in the hyperplane H—we write B in the form

$$B = B_\infty \cup B_{\text{aff}}, \tag{2}$$

where $B_\infty := B \cap H$ is a projective $(k-1)$-space contained in the hyperplane H and $B_{\text{aff}} := B \cap A$ is a k-space of the affine space Σ induced on A. In particular,

$$|B_{\text{aff}}| = q^k \quad \text{and} \quad |B_\infty| = q^{k-1} + \cdots + q + 1 = \frac{q^k - 1}{q - 1}. \tag{3}$$

If B and C are affine blocks and $B_\infty = C_\infty$, then B_{aff} and C_{aff} are affine translates of each other.

Now let α be any permutation of the projective $(k-1)$-spaces contained in H, and associate with each affine block B of $\mathcal{D}$ a point set $\alpha(B)$ as follows:

$$\alpha(B) := \alpha(B_\infty) \cup B_{\text{aff}}. \tag{4}$$

Thus, we keep the affine points of all affine blocks unchanged, and merely exchange their infinite parts, using the permutation α. We shall denote the incidence structure obtained from $\mathcal{D}$ by replacing each affine block B by its distorted version $\alpha(B)$ as $\alpha(\mathcal{D})$. Then it is easy to prove the following result.

Lemma 2.1 *For each permutation α of the $(k-1)$-spaces contained in H, the incidence structure $\alpha(\mathcal{D})$ is a 2-design with the same parameters as $\mathcal{D} = PG_k(2k, q)$.*

In general, the designs just constructed may have intersection numbers different from those of $\mathcal{D}$. If we wish to preserve intersection sizes, we will have to choose α judiciously. Before we address this problem, let us remark that Lemma 2.1 can be used to show that the number of 2-designs with the parameters of $PG_k(2k, q)$ grows exponentially; this is a special case of a more general result which will be presented elsewhere [16].

As it turns out, our aim can be achieved by choosing α as a polarity of the projective space $\Pi_0 \cong PG(2k-1, q)$ induced on H. Recall that a *polarity* of a projective space $PG(n, q)$ is an involutory isomorphism between $PG(n, q)$ and its dual space; in other words, a polarity is an incidence preserving bijection interchangeing points and hyperplanes. Note that any polarity of Π_0 maps i-spaces to $(2k-i-2)$-spaces, for $i = 0, \ldots, 2k-2$; in particular, α induces a permutation on the $(k-1)$-spaces contained in H, and hence can be used in our construction. We refer the reader to [12] for a thorough discussion of polarities in finite projective spaces.

Lemma 2.2 *For each polarity α of $\Pi_0 \cong PG(2k-1, q)$, the design $\alpha(\mathcal{D})$ has the same intersection numbers as $\mathcal{D} = PG_k(2k, q)$.*

Proof The interesting case to consider concerns the intersection sizes of blocks of $\mathcal{D}'$ which correspond to affine blocks of $\mathcal{D}$. As we will see, α even preserves these intersection sizes:

$$|\alpha(B) \cap \alpha(C)| = |B \cap C| \tag{5}$$

for any two affine blocks B and C of $\mathcal{D}$.

With the notation introduced in (2), the infinite parts B_∞ and C_∞ of the given two blocks are $(k-1)$-subspaces of $H \cong PG(2k-1, q)$. In view of the construction given in (4), the validity of (5) is clear provided that $B_\infty = C_\infty$.

Next, note that B_∞ and C_∞ are disjoint if and only if their images under α are disjoint. Indeed, by the dimension formula, these two $(k-1)$-subspaces of H intersect if and only if they are both contained in a hyperplane H_0 of H; as α is incidence preserving, this holds if and only if their images $\alpha(B_\infty)$ and $\alpha(C_\infty)$ intersect in the point $\alpha(H_0)$. This proves the validity of (5) in the special case where $B_\infty \cap C_\infty = \emptyset$.

We may now assume that $U := B_\infty \cap C_\infty$ is an i-subspace of H, where $0 \le i \le k-2$. Then $\alpha(U)$ is a $(2k-i-2)$-subspace which contains the two $(k-1)$-spaces $\alpha(B_\infty)$ and $\alpha(C_\infty)$, as α is incidence preserving. Again using the dimension formula, $\alpha(B_\infty)$ and $\alpha(C_\infty)$ have to intersect in a j-subspace for some $j \ge i$. Applying this argument to $\alpha(B_\infty)$ and $\alpha(C_\infty)$ and using that α is an involution shows that also $i \ge j$. Hence $\alpha(B_\infty) \cap \alpha(C_\infty)$ is again an i-subspace, and therefore (5) holds also in the case $B_\infty \cap C_\infty \neq \emptyset$.

Finally, note that the multiset of the remaining intersection numbers does not change, as blocks of $\mathcal{D}$ contained in H are kept in $\alpha(\mathcal{D})$ and as the infinite parts of the affine blocks are merely permuted under α. (However, in general, the image $\alpha(B)$ of a given affine block B may intersect a specific infinite block C in a different manner as B does). □

Lemma 2.3 *For each polarity α of $\Pi_0 \cong PG(2k-1, q)$, the design $\alpha(\mathcal{D})$ has line sizes $q+1$, q and 2. More precisely, any line of $\alpha(\mathcal{D})$ joining two infinite points has cardinality $q+1$; any line of $\alpha(\mathcal{D})$ joining two affine points has cardinality q; finally, an infinite point and an affine point always determine a line of size 2 in $\alpha(\mathcal{D})$.*

Proof Let us consider a fixed (affine) $(k-1)$-subspace U_{aff} of the affine space $\Sigma \cong AG(2k, q)$ induced on the set A of affine points of $\mathcal{D}$. Then U_{aff} is contained in exactly $q^k + \cdots q + 1$ affine blocks of $\mathcal{D}$, as this is the number of k-dimensional subspaces of $AG(2k, q)$ containing a given $(k-1)$-space. Recall that each such block B has the form given in (2).

Now U_{aff} extends to a unique $(k-1)$-subspace U of the underlying projective space Π. Note that U contains exactly $q^{k-2} + \cdots + q + 1$ infinite points, as U has to intersect the hyperplane H of Π in a $(k-2)$-dimensional subspace U_∞. Hence any two distinct affine blocks containing U_{aff} share exactly $q^{k-2} + \cdots + q + 1$ infinite points, namely those in U_∞; and by (3), any such block B has precisely q^{k-1} infinite points outside of U_∞. But then the remaining $q^{2k-1} + \cdots + q^k + q^{k-1}$ infinite points are partitioned by the $q^k + \cdots q + 1$ affine blocks through U_{aff}:

$$(q^k + \cdots + q + 1)q^{k-1} = q^{2k-1} + \cdots + q^k + q^{k-1}.$$

Thus, the infinite parts B_∞ of the $q^k + \cdots q + 1$ affine blocks B through U_{aff} form the bundle of $(k-1)$-subspaces of H through the common $(k-2)$-subspace U_∞. Under the polarity α, this bundle is mapped to a set of $q^k + \cdots + q + 1$ $(k-1)$-dimensional subspaces of the k-subspace $\alpha(U_\infty)$. Hence, the images $\alpha(B_\infty)$ are simply all hyperplanes of the projective space $\alpha(U_\infty) \cong PG(k, q)$. Therefore, the images of the infinite parts of any two distinct affine blocks through U_{aff} intersect in a $(k-2)$-dimensional subspace of $\alpha(U_\infty)$. Hence, no point of U_∞ lies in the intersection of all affine blocks $\alpha(B)$ through U_{aff}, and thus the intersection of all these blocks in $\alpha(\mathcal{D})$ is simply U_{aff}.

Now, let ℓ be any line of $\mathcal{D}$ joining two affine points, so that ℓ has size $q+1$ and consists of q affine points and one infinite point ℓ_∞. Note that ℓ is the intersection of all $(k-1)$-dimensional affine subspaces U_{aff} of Σ extended to subspaces U of Π, and we have just seen that the affine part U_{aff} of each such subspace U is simply the intersection of all blocks of $\alpha(\mathcal{D})$ containing U_{aff}. This shows that the line corresponding to ℓ in $\alpha(\mathcal{D})$ is precisely the q-set $\ell \setminus \ell_\infty$: the distortion by α results in ℓ losing its infinite point.[2]

Finally, it is clear that any line joining two infinite points of $\mathcal{D}$ remains a line of $\alpha(\mathcal{D})$. Now it easily follows that an infinite point and an affine point always determine a line of size 2 in $\alpha(\mathcal{D})$. □

Combining the preceding three lemmas, we obtain our main result:

Theorem 2.4 *Consider the design $\mathcal{D} = PG_k(2k, q)$. Let H be a hyperplane of $\mathcal{D}$, and let A be the set of points not in H. In addition, let α be any polarity of the hyperplane $H \cong PG(2k-1, q)$. Then the design $\alpha(\mathcal{D})$ defined above is a pseudo-geometric design with the same parameters as, but not isomorphic to, $PG_k(2k, q)$.* □

We conclude this section by pointing out that any two polarities of $\Pi_0 \cong PG(2k-1, q)$ lead to isomorphic pseudo-geometric designs, even if the polarities are of different types. While this might seem surprising, it is in fact easy to prove: the product of two polarities is a collineation, hence any two polarities differ by a collineation only. Now it is easy to check that applying a non-trivial collineation β in our construction yields a design $\beta(\mathcal{D})$ different from, but isomorphic to, $\mathcal{D}$.

3 New quasi-symmetric designs

In this section, we consider the special case $k = 2$. Here the points and planes of $\Pi = PG(4, q)$ yield a 2-design which is *quasi-symmetric*; that is, it has just two intersection numbers, namely 1 and $q+1$. Also, the lines of this design are just the lines of Π and hence all have cardinality $q+1$.[3]

The designs $PG_2(4, q)$ form a well-known family of quasi-symmetric designs. They have been studied quite intensively, and several characterizations are available. To mention the most natural result, a quasi-symmetric design with the parameters of $PG_2(4, q)$ and intersection numbers 1 and $q+1$ is classical if and only if all lines have size $q+1$. This is due to Sane and Shrikhande [26], who also gave various other characterizations.

Theorem 2.4 specializes to the following construction for a new family of quasi-symmetric designs with the parameters of $PG_2(4, q)$:

Theorem 3.1 *Consider the design $\mathcal{D} = PG_2(4, q)$, let H be a hyperplane of $\mathcal{D}$, and let A be the set of points not in H. In addition, let α be any polarity of the hyperplane $H \cong PG(3, q)$. Then the design $\alpha(\mathcal{D})$ defined in Sect. 2 is a pseudo-geometric quasi-symmetric design with the same parameters as, but not isomorphic to, $PG_2(4, q)$.* □

With the exception of the smallest case, i.e. $q = 2$, none of the designs in Theorem 3.1 was known previously; thus we indeed have a new infinite family of quasi-symmetric designs.

2 More generally, all subspaces of Π of dimension at most $k-1$ which are not contained in H can be recovered as suitable intersections of blocks of $\mathcal{D}$; under α, the intersection of the corresponding distorted blocks no longer contains an infinite point and simply is the original affine part of the subspace.

3 See [27] for a monograph on quasi-symmetric designs.

By a result of Tonchev [29], there are exactly five quasi-symmetric 2—(31,7,7)-designs with intersection numbers 1 and 3; among these designs is, of course, the classical example $PG_2(4, 2)$. It is interesting to note that just one of the further four examples contains a hyperplane; hence this design has to arise from Theorem 3.1. Actually, we discovered our general construction for pseudo-geometric designs when we tried to get a better understanding of this specific design which shares so many properties with the classical example. It seemed to us that there ought to be a geometric way of obtaining it—an intuition which fortunately turned out to be correct.

A more recent characterization of the geometric designs $PG_2(4, q)$ in terms of *good blocks*—a notion introduced in [23]—is due to Mavron, McDonough and Shrikhande [21]. In any quasi-symmetric design with intersection numbers x and y, where $0 \leq x < y$, a block B is said to be *good* if, for any block C with $|B \cap C| = y$ and any point $p \notin C$, there is a (unique) block containing p and $B \cap C$. The result of [21] characterizes the geometric design $PG_2(4, q)$ among all quasi-symmetric designs with the same parameters and with intersection numbers 1 and $q + 1$ by the property that all blocks of the design are good. Subsequently, this result was strengthened by Baartmans and Sane [3] who proved that it suffices to assume that all the blocks passing through a fixed point p are good.

The authors of [21] also knew[4] just one example of a quasi-symmetric design with the parameters of $PG_2(4, q)$ where some of the blocks, but not all blocks, are good, namely the pseudo-geometric 2—(31,7,7)-design discussed above. It is easy to check that if $\alpha(\mathcal{D})$ is a design obtained using a polarity α in a hyperplane H, then precisely the blocks contained in H are good.

4 Counterexamples to Hamada's conjecture

In this section, we shall see that our construction from Sect. 2 provides an infinite family of counterexamples to a famous conjecture by Hamada [8] from 1973. This conjecture reads as follows:

Conjecture 4.1 (Hamada's Conjecture) *Let $\mathcal{D}$ be a design with the parameters of a geometric design $PG_d(n, q)$ or $AG_d(n, q)$, where q is a power of a prime p. Then the p-rank of the incidence matrix of $\mathcal{D}$ is greater than or equal to the p-rank of the corresponding geometric design. Moreover, equality holds if and only if $\mathcal{D}$ is isomorphic to the geometric design.*

Hamada's conjecture has been proved in the following cases: Hamada and Ohmori [9] established the conjecture for the design of hyperplanes in a binary projective or affine space ($q = 2, d = n - 1$). Doyen et al. [6] proved the conjecture for the design of lines in a binary projective space ($q = 2,\ d = 1$), as well as for the design of lines in a ternary affine space ($q = 3,\ d = 1$). Teirlinck [28] proved the conjecture for the design of planes in a binary affine space ($q = 2,\ d = 2$). Tonchev [30] proved a modified version of Hamada's conjecture using generalized incidence matrices with entries over $GF(q)$ instead of (0, 1)-incidence matrices, for the classical designs having as blocks the complements of hyperplanes in $PG(d, q)$ or $AG(d, q)$ ($d = n - 1,\ q$ an arbitrary prime power).

Nevertheless, the strong version of Hamada's conjecture is not true in general: there are designs with the same parameters and the same p-rank as a classical geometric design $\mathcal{D}$, but not isomorphic to $\mathcal{D}$. The smallest examples for this phenomenon are the quasi-symmetric designs with the parameters of $PG_2(4, 2)$, namely, 2-(31, 7, 7) [29], which were

[4] This is not contained in the published paper [21], but was mentioned by Mavron and McDonough to the second author when he was visiting The University of Wales at Aberystwyth.

already discussed in the previous section. We note that one of these 2-(31, 7, 7) designs, namely, the design supported by the minimum weight vectors in the quadratic-residue code of length 31, was mentioned in the paper by Goethals and Delsarte [7]. The extensions of the quasi-symmetric 2-(31, 7, 7) designs are 3-(32, 8, 7) designs having the same parameters and block intersection numbers as $AG_3(5, 2)$ [29]. All these designs have the same 2-rank, namely 16.

The only other previously known parameter set for which a non-geometric design exists that has the same p-rank as the corresponding geometric design is 2-(64, 16, 5): in [10], Harada et al. found two affine 2-(64, 16, 5) designs having the same 2-rank (equal to 16) as the classical geometric design of the planes in $AG(3, 4)$. The two exceptional designs were found as minimum weight vectors in binary codes spanned by incidence matrices of symmetric (4, 4)-nets. Mavron et al. [22] showed that one of the pseudo-geometric 2-(64, 16, 5) designs from [10] can be obtained also by using a certain line spread in $PG(5, 2)$.

However, the weak version of Conjecture 4.1, that is, the statement that the p-rank of any design with the same parameters as a geometric design $PG_d(n, q)$ or $AG_d(n, q)$ is at least as large as that of the corresponding geometric design, is still open in general, with the exception of the few proven cases mentioned above.

Thus, it is rather interesting that the designs described in Theorem 2.4 in the case when q is a prime number provide the first infinite family of counterexamples to the strong version of Hamada's conjecture:

Theorem 4.2 *If $q = p$ is a prime number, the pseudo-geometric designs described in Theorem 2.4 have the same p-rank as the geometric design $PG_k(2k, p)$.*

We will need two lemmas for the proof of Theorem 4.2.

Lemma 4.3 *Let α be a polarity in $PG(2k-1, q)$, where $q = p^s$ and p is a prime. The p-rank $r_p(\alpha)$ of the incidence matrix of the design $\alpha(\mathcal{D})$ from Theorem 2.4 satisfies the inequalities*

$$r_p(\mathcal{D}) \leq r_p(\alpha) \leq \frac{1}{2}\left(\frac{q^{2k+1}-1}{q-1}+1\right), \tag{6}$$

where $r_p(\mathcal{D})$ is the p-rank of the geometric design $\mathcal{D} = PG_k(2k, q)$.

Proof By the construction described in Sect. 2, the design $\alpha(\mathcal{D})$ has an incidence matrix of the form

$$M = \left(\begin{array}{c|c} M_1 & M_2 \\ \hline 0 & M_3 \end{array}\right),$$

where M_1 is a point by block incidence matrix of the geometric design $PG_k(2k-1, q)$, and M_3 is a point by block incidence matrix of the geometric design $AG_k(2k, q)$. Thus, we have

$$r_p(M_1) + r_p(M_3) \leq r_p(\alpha).$$

On the other hand, it follows from [1, Corollary 5.7.3, p. 186], that

$$r_p(PG_k(2k, q)) = r_p(PG_k(2k-1, q)) + r_p(AG_k(2k, q)).$$

Hence, we have

$$r_p(\mathcal{D}) = r_p(M_1) + r_p(M_3).$$

This proves the left-hand side inequality in (6). To prove the right-hand side inequality in (6), we consider the complementary design $\overline{\alpha(\mathcal{D})}$. By Lemma 2.2, the design $\alpha(\mathcal{D})$ has the same intersection numbers as $\mathcal{D} = PG_k(2k, q)$, that is, $(q^i - 1)/(q - 1)$ for i in the range $1 \le i \le k$. Consequently, the block intersection numbers of the complementary design $\overline{\alpha(\mathcal{D})}$ are

$$\frac{q^i(q^{2k+1-i} - 2q^{k+1-i} + 1)}{q - 1}, \ 1 \le i \le k.$$

Note that all these numbers are divisible by q, and that the blocks of $\overline{\alpha(\mathcal{D})}$ are of size

$$\frac{q^{k+1}(q^k - 1)}{q - 1},$$

which is also divisible by q. Thus, the incidence vectors of the blocks of $\overline{\alpha(\mathcal{D})}$ span a linear self-orthogonal code of length $(q^{2k+1} - 1)/(q - 1)$ over $GF(p)$. Hence, the p-rank of the incidence matrix $(J - M)$ of $\overline{\alpha(\mathcal{D})}$, where J denotes the all-one matrix of appropriate size, does not exceed $(\frac{q^{2k+1}-1}{q-1} - 1)/2$ (note that the number of points of $\alpha(\mathcal{D})$, $(q^{2k+1} - 1)/(q - 1)$ is an odd number). The columns of $J - M$ have 0 and 1 entries, and the number of 1's in each column is a multiple of p. Therefore, each column of $J - M$ is orthogonal (over $GF(p)$) to the all-one column $\mathbf{j}$, and consequently, the whole column space is orthogonal to $\mathbf{j}$. Since $\mathbf{j}$ is not orthogonal to itself, $\mathbf{j}$ is not in the column space of $J - M$. On the other hand, $\mathbf{j}$ is a nonzero multiple of the sum of columns of M over $GF(p)$. This implies

$$r_p(M) = r_p(J - M) + 1,$$

and therefore

$$r_p(M) \le \frac{1}{2}\left(\frac{q^{2k+1} - 1}{q - 1} - 1\right) + 1 = \frac{1}{2}\left(\frac{q^{2k+1} + 1}{q - 1} + 1\right).$$

This proves the right-hand side inequality in (6). □

A summation formula for the p-rank of the incidence matrix of a geometric design $PG_r(n, q)$, $1 \le r \le n - 1$, $q = p^t$, p a prime, was found by Hamada [8]. If $r \ne 1, n - 1$, Hamada's formula involves some parameters that have to be computed. A simplified formula for the case when $q = p$ is a prime was found by Hirschfeld and Shaw [13, Theorem 5.10]. In particular, the p-rank of $\mathcal{D} = PG_k(2k, p)$ is given by:

$$r_p(\mathcal{D}) = \frac{p^{2k+1} - 1}{p - 1} - \sum_{i=0}^{k-1}(-1)^i \binom{(k - i)(p - 1) - 1}{i}\binom{k + (k - i)p}{2k - i}. \tag{7}$$

If $p = 2$, the linear code spanned by the blocks of $\mathcal{D} = PG_k(2k, 2)$ is a punctured Reed-Muller code of length $v = 2^{2k+1} - 1$ and order k [1, Proposition 5.3.2], so we have an alternative formula for $r_2(\mathcal{D})$ which can be written in a simple closed form, namely

$$r_2(\mathcal{D}) = \sum_{i=0}^{k}\binom{2k + 1}{i} = 2^{2k}.$$

Note that $2^{2k} = (v + 1)/2$, so the inequalities in (6) are replaced by equalities:

$$r_2(\mathcal{D}) = r_2(\alpha) = 2^{2k} = (v + 1)/2.$$

Thus, the pseudo-geometric designs from Sect. 2 for $q = p = 2$ are counter-examples to the "only if" part of Hamada's conjecture.

In addition, the two formulas for $r_2(\mathcal{D})$ imply the following identity:

$$2^{2k} - 1 = \sum_{i=0}^{k-1} (-1)^i \binom{k-i-1}{i} \binom{3k-2i}{2k-i}. \tag{8}$$

It turns out that a similar closed formula for $r_p(\mathcal{D})$ holds for any prime number p.

Lemma 4.4 *If p is any prime, the p-rank of $\mathcal{D} = PG_k(2k, p)$ is equal to*

$$r_p(\mathcal{D}) = \frac{1}{2}\left(\frac{p^{2k+1}-1}{p-1} + 1\right). \tag{9}$$

Proof We will use the following result by Hirschfeld and Shaw [13, Corollary 5.5]): if p is a prime and $C^*(k, n, p)$ is the dual of the linear code over $GF(p)$ spanned by the incidence vectors of the k-dimensional subspaces of $PG(n, p)$, $1 \le k \le n-1$, then

$$\dim C^*(k, n, p) + \dim C^*(n-k, n, p) = \frac{p^{n+1}-1}{p-1} - 1. \tag{10}$$

In the special case $n = 2k$, (10) implies that

$$\dim C^*(k, 2k, p) = \frac{1}{2}\left(\frac{p^{2k+1}-1}{p-1} - 1\right).$$

Note that $C^*(k, 2k, p)$ is the code having the incidence matrix of $\mathcal{D}$=$PG_k(2k, p)$ as a parity check matrix, hence

$$r_p(\mathcal{D}) = \frac{p^{2k+1}-1}{p-1} - \dim C^*(k, 2k, p) = \frac{1}{2}\left(\frac{p^{2k+1}-1}{p-1} + 1\right).$$

□

Now Theorem 4.2 follows from Lemmas 4.3 and 4.4.

We note that comparing (7) and (9) gives the following identity, which generalizes (8):

Corollary 4.5

$$\frac{1}{2}\left(\frac{p^{2k+1}-1}{p-1} - 1\right) = \sum_{i=0}^{k-1} (-1)^i \binom{(k-i)(p-1)-1}{i} \binom{k+(k-i)p}{2k-i}. \tag{11}$$

It was pointed out to us by one of the reviewers, that Eq. 11 is actually true for all positive integers p and not just for primes; it follows from a formula of J.L.W.V. Jensen [14, Eq. 18], which is given a modern setting in [20, Sect. 14.1]. Of course, with (11) in hand, Lemma 4.4 is an immediate consequence of (7).

We finally remark that Theorem 4.2 does not extend to arbitrary prime powers q: the classical design $PG_2(4, 4)$ has 2-rank 146, whereas the pseudo-geometric design obtained from a polarity has 2-rank 154.

Acknowledgments The second author wishes to thank the University of Augsburg, Germany, for the hospitality during his visit. He is also grateful for the support provided by a grant of the Alexander von Humboldt Foundation. The authors wish to thank James Hirschfeld for providing them with a copy of [13], Jenny Key for valuable references to [2], and the reviewers for their helpful comments, in particular, for pointing out references [3,7,14,20]. Vladimir D. Tonchev research partially supported by a research grant of the Alexander von Humboldt Foundation, and NSA Grant H98230-08-1-0065.

References

1. Assmus E.F. Jr., Key J.D.: Designs and their Codes. Cambridge University Press, Cambridge (1992).
2. Assmus E.F. Jr., Key J.D.: Polynomial codes and finite geometries. In: Pless V., Huffman W.C. (eds.) Handbook of Coding Theory, vol. II, pp. 1269–1343. North Holland, Amsterdam (1998).
3. Baartmans A., Sane S.: A characterization of projective subspaces of codimension two as quasi-symmetric designs with good blocks. Discrete Math. **306**, 1493–1501 (2006).
4. Beth T., Jungnickel D., Lenz H.: Design Theory, 2nd edn. Cambridge University Press (1999).
5. Colbourn C.J., Dinitz J.H.: Handbook of Combinatorial Designs, 2nd edn. CRC Press, Boca Raton (2007).
6. Doyen J., Hubaut X., Vandensavel M.: Ranks of incidence matrices of Steiner triple systems. Math. Z. **163**, 251–259 (1978).
7. Goethals J.-M., Delsarte P.: On a class of majority-logic decodable cyclic codes. IEEE Trans. Inform. Theory **14**, 182–188 (1968).
8. Hamada N.: On the p-rank of the incidence matrix of a balanced or partially balanced incomplete block design and its application to error correcting codes. Hiroshima Math. J. **3**, 154–226 (1973).
9. Hamada N., Ohmori H.: On the BIB-design having the minimum p-rank. J. Combin. Theory Ser. A **18**, 131–140 (1975).
10. Harada M., Lam C.W.H., Tonchev V.D.: Symmetric (4,4)-nets and generalized Hadamard matrices over groups of order 4. Des. Codes Cryptogr. **34**, 71–87 (2005).
11. Hirschfeld J.W.P.: Finite Projective Spaces of Three Dimensions. Oxford University Press (1985).
12. Hirschfeld J.W.P.: Projective Geometries Over Finite Fields, 2nd edn. Oxford University Press (1998).
13. Hirschfeld J.W.P., Shaw R.: Projective geometry codes over prime fields. In: Finite Fields: Theory, Application and Algorithms. Contemporary Math, vol. 168, pp. 151–163. Amer Math. Soc., Providence, R.I. (1994).
14. Jensen J.L.W.V.: Sur une identité d'Abel et sur d'autres formules analogues. Acta Math. **26**, 307–318 (1902).
15. Jungnickel D.: The number of designs with classical parameters grows exponentially. Geom. Dedicata **16**, 167–178 (1984).
16. Jungnickel D., Tonchev V.D.: The number of designs with classical parameters grows exponentially, II. (In preparation).
17. Kantor W.M.: Automorphisms and isomorphisms of symmetric and affine designs. J. Algebraic Combin. **3**, 307–338 (1994).
18. Lam C., Lam S., Tonchev V.D.: Bounds on the number of affine, symmetric, and Hadamard designs and matrices. J. Combin. Theory Ser. A **92**, 186–196 (2000).
19. Lam C., Tonchev V.D.: A new bound on the number of designs with classical affine parameters. Des. Codes Cryptogr. **27**, 111–117 (2002).
20. Larsen M.E.: Summa Summarum. In: CMS Treatises in Mathematics, Canadian Mathematical Society, Ottawa, ON; A K Peters, Ltd., Wellesley, MA (2007).
21. Mavron V.C., McDonough T.P., Shrikhande M.S.: Quasi-symmetric designs with good blocks and intersection number one. Des. Codes Cryptogr. **28**, 147–162 (2003).
22. Mavron V.C., McDonough T.P., Tonchev V.D.: On affine designs and Hadamard designs with line spreads. Discrete Math. **308**, 2742–2750 (2008).
23. McDonough T.P., Mavron V.C.: Quasi-symmetric designs with good blocks. J. Combin. Des. **3**, 433–441 (1995).
24. Rahman M., Blake I.F.: Majority logic decoding using combinatorial designs. IEEE Trans. Inform. Theory **21**, 585–587 (1975).
25. Rudolph L.D.: A class of majority-logic decodable codes. IEEE Trans. Inform. Theory **23**, 305–307 (1967).
26. Sane S.S., Shrikhande M.S.: Some characterizations of quasi-symmetric designs with a spread. Des. Codes Cryptogr. **3**, 155–166 (1993).
27. Shrikhande M.S., Sane S.S.: Quasi-symmetric Designs. Cambridge University Press, Cambridge (1991).
28. Teirlinck L.: On projective and affine hyperplanes. J. Combin. Theory Ser. A **28**, 290–306 (1980).
29. Tonchev V.D.: Quasi-symmetric 2-(31, 7, 7)-designs and a revision of Hamada's conjecture. J. Combin. Theory Ser. A **42**, 104–110 (1986).
30. Tonchev V.D.: Linear perfect codes and a characterization of the classical designs. Des. Codes Cryptogr. **17**, 121–128 (1999).