Des. Codes Cryptogr. (2013) 68:163–177
DOI 10.1007/s10623-012-9636-z

New invariants for incidence structures

Dieter Jungnickel · Vladimir D. Tonchev

Received: 5 September 2011 / Revised: 6 February 2012 / Accepted: 9 February 2012 /
Published online: 29 February 2012

Abstract We exhibit a new, surprisingly tight, connection between incidence structures, linear codes, and Galois geometry. To this end, we introduce new invariants for finite simple incidence structures $\mathcal{D}$, which admit both an algebraic and a geometric description. More precisely, we will associate one invariant for the isomorphism class of $\mathcal{D}$ with each prime power q. On the one hand, we consider incidence matrices M with entries from $GF(q^t)$ for the complementary incidence structure $\mathcal{D}^*$, where t may be any positive integer; the associated codes $C = C(M)$ spanned by M over $GF(q^t)$; and the corresponding trace codes $Tr(C(M))$ over $GF(q)$. The new invariant, namely the *q-dimension* $\dim_q(\mathcal{D}^*)$ of $\mathcal{D}^*$, is defined to be the smallest dimension over all trace codes which may be obtained in this manner. This modifies and generalizes the q-dimension of a design as introduced in Tonchev (Des Codes Cryptogr 17:121–128, 1999). On the other hand, we consider embeddings of $\mathcal{D}$ into projective geometries $\Pi = PG(n, q)$, where an *embedding* means identifying the points of $\mathcal{D}$ with a point set V in Π in such a way that every block of $\mathcal{D}$ is induced as the intersection of V with a suitable subspace of Π. Our main result shows that the q-dimension of $\mathcal{D}^*$ always coincides with the smallest value of N for which $\mathcal{D}$ may be embedded into the $(N-1)$-dimensional projective geometry $PG(N-1, q)$. We also give a necessary and sufficient condition when actually an embedding into the affine geometry $AG(N-1, q)$ is possible. Several examples and applications will be discussed: designs with classical parameters, some Steiner designs, and some configurations.

This is one of several papers published in *Designs, Codes and Cryptography* comprising the "Special Issue on Finite Geometries".

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

Keywords Incidence structure · Design · Steiner system · Configuration · Incidence matrix · Code · Trace · Projective geometry

Mathematics Subject Classification (2010) 51E20 · 94B27 · 05B05

1 Introduction

It is the aim of this paper to exhibit a new, surprisingly tight, connection between incidence structures, linear codes, and Galois geometry. To this end, we shall introduce new invariants for finite simple incidence structures $\mathcal{D}$, which admit both an algebraic and a geometric description. More precisely, we will associate one invariant for the isomorphism class of $\mathcal{D}$ with each prime power q.

We assume that the reader is familiar with basic facts and terminology from design theory [2] and coding theory [26]. Throughout this paper, incidence matrices will have their rows indexed by blocks, and columns indexed by points. Moreover, we will only consider finite *simple* incidence structures, that is, incidence structures *without repeated blocks or points*. While the notion of an incidence structure without repeated blocks is standard, we add here the analogous requirement that there should be no two points which are incident with exactly the same set of blocks. In addition, we also always assume that each point belongs to some block, but not to all blocks, and dually. So our notion of simplicity asks for a bit more than usual: it means that there should be neither isolated points nor empty blocks and that, in standard terminology, both $\mathcal{D}$ and its dual incidence structure are simple. As we want to study, among other things, embeddings of incidence structures into projective or affine spaces, this somewhat strengthened version of simplicity is an entirely natural requirement.

We begin with the algebraic description of our new invariants; this generalizes an idea introduced in our previous paper [24] in connection with a coding theoretic characterization of the classical geometric designs. If A is the usual $(0, 1)$-incidence matrix of some incidence structure $\mathcal{D}$, a *generalized incidence matrix* of $\mathcal{D}$ over E (or simply an E*-incidence matrix*), where E is some finite field, is any matrix obtained by replacing the nonzero entries of A with nonzero elements from E.

Now fix a prime power q, and let $\mathcal{D}$ be a finite simple incidence structure. As usual, the *complementary incidence structure* $\mathcal{D}^*$ of $\mathcal{D}$ is obtained by replacing every block of $\mathcal{D}$ by its complement. We will consider incidence matrices M with entries from $E = GF(q^t)$ for $\mathcal{D}^*$, where t may be any positive integer, and denote by $C = C(M)$ the code spanned by the rows of M over E. We consider also an associated code over $F = GF(q)$, namely the trace code $Tr(C(M))$, obtained by applying the trace function coordinate-wise.

With this setup, our new invariant, the *q-dimension* $\dim_q(\mathcal{D}^*)$ of $\mathcal{D}^*$, is defined as the smallest dimension over all trace codes which can be obtained in the manner just described. This new invariant modifies and generalizes the q-dimension of a design as introduced by the second author in [31], where only incidence matrices over $GF(q)$ were considered, while extension fields played no role at all.

On the other hand, we consider embeddings of $\mathcal{D}$ into projective geometries $\Pi = PG(n, q)$, where an *embedding* means identifying the points of $\mathcal{D}$ with a point set V in Π in such a way that every block of $\mathcal{D}$ is induced as the intersection of V with a suitable subspace of Π. Clearly, any simple design on v points admits a trivial embedding into $PG(v - 1, q)$: just select V as a set of v points of Π in general position.

Our main result shows that the q-dimension of $\mathcal{D}^*$ always coincides with the smallest value of N for which $\mathcal{D}$ may be embedded into the $(N - 1)$-dimensional projective geometry $PG(N-1, q)$. We also give a necessary and sufficient condition when actually an embedding into the affine geometry $AG(N-1, q)$ is possible.

We are, of course, not all that interested in arbitrary incidence structures, but only in more specific cases such as designs and configurations. Several examples and applications will be discussed: designs with classical parameters, some Steiner designs, and some configurations. These examples should suffice to convince the reader that our new approach is not just a theoretical curiosity, but worth pursuing further.

2 Preliminaries from coding theory

We begin by recalling a few facts from coding theory. Let C be a code over some extension field $E = GF(q^t)$ of $F = GF(q)$. The *trace code* $Tr(C)$ of C is the code obtained from C by applying the trace function $Tr = Tr_{E/F}$ from E to F defined by

$$Tr(\xi) = \xi + \xi^q + \xi^{q^2} + \cdots + \xi^{q^{t-1}}$$

coordinate-wise to the words of C. The *subfield subcode* C_F of C consists of all those words in C which have coordinates in F only. Finally, C is called *Galois closed* if it is invariant under applying the Frobenius automorphism $x \mapsto x^q$ of E over F (again coordinate-wise). Such codes have particularly nice properties; see Bierbrauer [4, Theorem 12.17].

Proposition 2.1 *For any Galois closed code C over E, the subfield subcode C_F over F coincides with the trace code $Tr(C)$; moreover, the dimension of C over E equals the dimension of $C_F = Tr(C)$ over F, and both codes have the same minimum weight.*

The following result is contained in the recent work of Giorgetti and Previtali [14]; a simple proof can also be found in our paper [24].

Proposition 2.2 *Let C be a code over an extension field $E = GF(q^t)$ of $F = GF(q)$. Then C is Galois closed if and only if it is the extension code $C = S \otimes E$ of some code S over F. In this case, S actually is the subfield subcode C_F of C, and every basis of C_F over F is also a basis of C over E.*

We also need the notion of the *Galois closure* $\bar{C}$ of an arbitrary code C over $E = GF(q^t)$: this is the smallest Galois closed code over E containing C. It may be obtained from C by taking the span of all images of some set of generators of C under the Frobenius automorphism and its powers. The following simple result is crucial for our work; see Bierbrauer [4, Theorem 12.16].

Proposition 2.3 *Let C be an arbitrary code over $E = GF(q^t)$, and $\bar{C}$ its Galois closure. Then the trace codes $Tr(C)$ and $Tr(\bar{C})$ coincide.*

Finally, we formally define our new invariant as already explained in the introduction.

Definition 2.4 Let $\mathcal{D}^*$ be the complementary incidence structure of a fixed finite simple incidence structure $\mathcal{D}$, and let $E = GF(q^t)$ be some extension field of $F = GF(q)$. Moreover, let M be any E-incidence matrix for $\mathcal{D}^*$, and denote by $C = C(M)$ the code over E generated by the rows of M. Define the *q-dimension* $\dim_q \mathcal{D}^*$ of $\mathcal{D}^*$ as the smallest dimension of any $GF(q)$-code which arises as a trace code $Tr(C(M))$, where E runs over all finite extension fields of $GF(q)$ and where M runs over all E-incidence matrices of $\mathcal{D}^*$.

Recall that the *q-rank* of an incidence structure $\mathcal{D}$, denoted by $r_q(\mathcal{D})$, is defined to be the rank of its (0, 1)-incidence matrix over $GF(q)$. Trivially, the q-rank gives an upper bound for the q-dimension:

Corollary 2.5 *Let $\mathcal{D}^*$ be the complementary incidence structure of a finite simple incidence structure $\mathcal{D}$. Then* $\dim_q \mathcal{D}^* \leq r_q(\mathcal{D}^*)$.

In the case of simple 2-(v, k, λ)-designs, the bound given in Corollary 2.5 is non-trivial only for those prime powers $q = p^e$ for which the prime p divides the order $r - \lambda$ of the complementary 2-design $\mathcal{D}^*$: as is well-known, in all other cases $r_q(\mathcal{D})^* \in \{v-1, v\}$.

3 Embeddings

We begin this section with a formal definition of embeddings, followed by a very general embedding result.

Definition 3.1 Let $\mathcal{D}$ be a simple incidence structure, q a prime power, and $\Pi = PG(N, q)$ some projective geometry over $GF(q)$. We say that $\mathcal{D}$ is *embedded* in Π if its point set V consists of points of Π and if each block X of $\mathcal{D}$ is induced by some subspace W of Π, that is, $X = V \cap W$. Note that there is a unique smallest subspace W with this property, and we will always consider this subspace as *associated* with X.

An embedding will be called *strong* if V spans Π, that is, if V contains $N + 1$ points in general position. Finally, we call $\mathcal{D}$ (*strongly*) *embeddable* if an isomorphic copy of $\mathcal{D}$ is (strongly) embedded in Π.

Proposition 3.2 *Let $\mathcal{D}$ be a simple incidence structure, q a prime power, and $E = GF(q^t)$ an extension field of $F = GF(q)$. Moreover, let M be some E-incidence matrix of the complementary incidence structure $\mathcal{D}^*$, and let $N = N(M)$ denote the dimension of the trace code $Tr(C(M))$ associated with M. Then $\mathcal{D}$ is strongly embeddable into the projective geometry $PG(N-1, q)$.*

Proof In order to study the trace code of $C = C(M)$, we may, in view of Proposition 2.3, replace C with its Galois closure $\bar{C}$. Note that, by Proposition 2.1, the subfield subcode $\bar{C}_F$ and the trace code $Tr(\bar{C}) = Tr(C)$ of $\bar{C}$ coincide. We choose a basis of $\bar{C}_F$ over F, say $\mathbf{b}_1, \ldots, \mathbf{b}_N$; by Proposition 2.2, this is also a basis of $\bar{C}$ over E. Let us write $\mathbf{b}_1, \ldots, \mathbf{b}_N$ as the rows of an $(N \times v)$-matrix B. Then all rows of the given incidence matrix M are linear combinations of the rows of B with coefficients from E.

Now consider the columns of B. Clearly, B cannot contain a column $\mathbf{0}$, since otherwise the corresponding column of M would consist of entries 0 only, and so the associated point of $\mathcal{D}^*$ would not be contained in any blocks at all. Similarly, B cannot contain two linearly dependent non-zero columns; otherwise, for any linear combination of $\mathbf{b}_1, \ldots, \mathbf{b}_N$ with coefficients from E, either both or none of two such columns would contain an entry 0. In particular, the points corresponding to these two columns would be on exactly the same set of blocks of $\mathcal{D}^*$, contradicting the simplicity of the incidence structure.

Hence B consists of v column vectors of length N over F, no two of which are linearly dependent, and therefore the columns of B—and hence also the points of $\mathcal{D}^*$—may be viewed as a set V of v points in $\Pi = PG(N-1, q)$. We will see that this identification gives the desired embedding of $\mathcal{D}$ into Π. Note that the embedding is indeed strong, as B has (row and column) rank N, so that V contains N points in general position.

In this way, each block of $\mathcal{D}^*$—and therefore also each block of the complementary incidence structure $\mathcal{D}$ of $\mathcal{D}^*$—is now identified with some subset of the point set V in Π. Consider an arbitrary block X^* of $\mathcal{D}^*$, and let $\mathbf{x}_1, \ldots, \mathbf{x}_c$ be points of V contained in the complementary block $X = V \backslash X^*$ of $\mathcal{D}$, so that the incidence matrix M has entries 0 in the row corresponding to X^* for all positions indexed by the points $\mathbf{x}_1, \ldots, \mathbf{x}_c$.

As X^* is a linear combination of the rows of B with coefficients from E, we necessarily have entries 0 in row X^* of M in *all* columns which correspond to a point in V given by some linear combination of the columns of B associated with $\mathbf{x}_1, \ldots, \mathbf{x}_c$. In other words, if a block X^* has entries 0 in all positions indexed by some points $\mathbf{x}_1, \ldots, \mathbf{x}_c$, then it has entry 0 in *all* positions corresponding to a point in the intersection of V with the subspace W of Π generated by the given points. In terms of the incidence structure $\mathcal{D}$, this observation simply means that the block X of $\mathcal{D}$ is closed under intersections with subspaces of Π. In particular, if we choose $\{\mathbf{x}_1, \ldots, \mathbf{x}_c\}$ as a *maximal* set of points of X in general position (so that the corresponding columns of B are a maximal set of linearly independent columns in the positions indexed by the points of X), we obviously obtain $X = V \cap W$. Hence each block of $\mathcal{D}$ is indeed induced by some subspace of Π. Finally, we note in passing that the construction just outlined yields for W the subspace associated with X, in the sense of Definition 3.1. □

We next prove a converse of Proposition 3.2:

Proposition 3.3 *Let $\mathcal{D}$ be a simple incidence structure which is embedded in the projective geometry $\Pi = PG(N-1, q)$, and let $E = GF(q^t)$ be any extension field of $F = GF(q)$ satisfying $t \geq N-1-d$, where d is the smallest dimension of a subspace of Π associated with some block of $\mathcal{D}$. Then there exists an E-incidence matrix M for the complementary incidence structure $\mathcal{D}^*$ of $\mathcal{D}$ such that the trace code $Tr(C(M))$ associated with M has dimension at most N over F.*

Proof By definition, the point set of $\mathcal{D}$ is a subset V of the point set of Π. We choose a coordinate vector for each of the $q^{N-1} + \cdots + q + 1$ points of Π and write all these vectors as the columns of a matrix B, where we put the vectors corresponding to the points of V in the first v columns. Thus B is a generator matrix for the (monomially unique) simplex code S of dimension N over $GF(q)$. In what follows, we will use the recent results of Jurrius [25] on the extension code $S \otimes E$ of S over E; we denote this Galois closed code by C.

As explained in Sect. 3 of [25], the subcodes of a given dimension r of the simplex code S correspond bijectively to the subspaces of codimension r of Π. More precisely, if U is such a subcode, then the points of Π corresponding to the *support* of U (that is, the set of positions for which at least one word in U has a non-zero entry) are just the points *not* contained in the associated subspace of codimension r of Π. Jurrius [25] has used this to determine the weight enumerator for the extension code C. It turns out that the non-zero weights occurring are just the cardinalities of the complements of subspaces of codimension r of Π, where $1 \leq r \leq t$. Moreover, the support of any word of weight $(q^N - q^{N-r})/(q-1)$ indeed corresponds to the points not contained in some subspace of codimension r.

In particular, all complements of subspaces of Π with codimension at most $N-1-d$ arise in this manner, since we have assumed $t \geq N-1-d$. Clearly, for any subcode U of dimension $r \leq N-1-d$ of S, we get a corresponding subcode $D = U \otimes E$ of dimension r of C; trivially, the support of D is just the support of U. Thus the subspaces of codimension at most $N-1-d$ (and hence of dimension at least d) of Π are in a one-to-one correspondence with the subspaces U of dimension $r \leq N-1-d$ of S respectively their extensions $D = U \otimes E$. It is not difficult to see that D always contains words which are non-zero over the *entire* support of U; a simple combinatorial proof for this fact can be found in Lemma 2.6

of [24]. Selecting such a word for each subcode U of S with dimension at most $N-1-d$ then gives us an E-incidence matrix $\tilde{M}$ for the incidence structure formed by the points of Π and all complements of subspaces of Π with dimension at least d. By construction, all rows of $\tilde{M}$ are words in the E-extension C of the simplex code S.

We now claim that $\tilde{M}$, when restricted to its first v columns, contains an E-incidence matrix M of $\mathcal{D}^*$. Thus let X be any block of $\mathcal{D}$ and $X^* = V \setminus X$ its complementary block in $\mathcal{D}^*$. As $\mathcal{D}$ is embedded in Π, there is a unique subspace W of Π associated with X. Then $X = V \cap W$, and hence $X^* = V \cap W^*$, where W^* denotes the complement of the subspace W in Π. By hypothesis, the dimension of W is at least d, and thus $\tilde{M}$ contains a row associated with W, which is a word $\mathbf{c} \in C$ with support W^*. Therefore, $\mathbf{c}$ has a non-zero entry in every position associated with a point in X^*, and an entry 0 in every position associated with a point in X. Thus the restriction of $\mathbf{c}$ to the positions indexed by V is indeed an E-incidence vector for X^*. As X was an arbitrary block of $\mathcal{D}$, this verifies the claim.

We have now established that the restriction $C' = C|V$ of C to the positions associated with the common point set V of $\mathcal{D}$ and $\mathcal{D}^*$ contains an E-incidence matrix M of $\mathcal{D}^*$. By Proposition 2.2, C is the E-extension of its trace code $Tr(C) = S$, and thus C' is the E-extension of its trace code $Tr(C') = S|V$. Since the E-code $C(M)$ generated by M is contained in the Galois closed code C', its trace code $Tr(C(M))$ is contained in $Tr(C') = S|V$. Trivially, $S|V$ has dimension at most N, and the assertion follows. □

Under the assumptions of Proposition 3.3, it seems plausible that the trace code $Tr(C(M))$ associated with M has dimension exactly N provided that $\mathcal{D}$ is strongly embedded in Π. While we were unable to prove this in general, it is easy to see that it indeed holds if N is chosen minimally in Proposition 3.3:

Theorem 3.4 *Let $\mathcal{D}$ be a simple incidence structure and q a prime power. Then the q-dimension of $\mathcal{D}^*$ equals the smallest integer N for which $\mathcal{D}$ can be embedded into the projective geometry $\Pi = PG(N-1, q)$.*

Moreover, $\mathcal{D}^*$ can actually be embedded into the affine geometry $AG(N-1, q)$ if and only if $\mathcal{D}^*$ admits an E-incidence matrix M with $\dim Tr(C(M)) = N$ for which the trace code $Tr(C(M))$ contains a word with full support V.

Proof By Proposition 3.2, $\mathcal{D}$ can be embedded into $PG(n-1, q)$ whenever $\mathcal{D}^*$ admits an E-incidence matrix M with $\dim Tr(C(M)) = n$; in particular, this holds for $n = \dim_q \mathcal{D}^*$. Now let N be chosen as in the statement of the theorem, and let M be constructed as in the proof of Proposition 3.3, so that $\dim Tr(C(M)) \leq N$. If we had strict inequality, say $\dim Tr(C(M)) = N' < N$, we would—once more appealing to Proposition 3.2—also obtain an embedding of $\mathcal{D}$ into $PG(N'-1, q)$, contradicting the choice of N. This proves the first assertion.

It remains to consider the existence of affine embeddings or, equivalently, of embeddings into $\Pi = PG(N-1, q)$ where V is disjoint to some hyperplane H of Π. Assume first that the criterion stated in the assertion is satisfied, so that we have an E-incidence matrix M for $\mathcal{D}^*$ with $\dim Tr(C(M)) = N$, such that $C(M)$ contains a word with full support V. Then we may, using the setup of the proof of Proposition 3.2, choose such a word as the first basis vector $\mathbf{b}_1$, so that the columns of the matrix B constructed in the proof of Proposition 3.2 correspond to points of Π which lie in the complement A of the hyperplane H with equation $x_1 = 0$. In this way, we see that $\mathcal{D}$ is indeed embedded in the affine geometry $\Pi \setminus H$.

Conversely, assume the existence of an embedding of $\mathcal{D}$ into $\Pi = PG(N-1, q)$ for which V is disjoint to some hyperplane H of Π. Recall that the first order q-ary Reed–Muller code of dimension N and length q^{N-1} can be defined as the monomially unique code R over

$F = GF(q)$ whose generator matrix consists of coordinate vectors for the points contained in the complement A of the hyperplane H. More explicitly, up to monomial equivalence over F, we may use for H the hyperplane with the equation $x_1 = 0$ and normalize the first coordinates of the points in A to 1 (so that a generator matrix G for R consists of the all-one row as first row, while the other positions in the columns of G contain all possible vectors in F^{N-1}). We can now easily adapt the arguments given in the proof of Proposition 3.3 to this situation, since Jurrius [25] also proved results for extension codes of the first order Reed–Muller codes which are completely analogous to her results for simplex codes discussed before.

Again, the subcodes of a given dimension r of the Reed–Muller code R correspond bijectively to the subspaces of codimension r in Π. More precisely, if U is such a subcode, then the points of Π corresponding to the support of U are just the points *not* contained in the associated subspace W of codimension r of Π. Note, however, that the situation is a bit more involved than in the projective case, as one needs to distinguish two possibilities: either W is contained in H, in which case the support of U is all of A; or W intersects H in a subspace of codimension $r + 1$ of Π, in which case the support of U is a subspace of codimension r of the affine space $\Sigma = AG(N-1, q)$ induced on A.

Jurrius [25] has used this to determine the weight enumerator for the extension code $C = R \otimes E$ of R over $E = GF(q^t)$. It turns out that the non-zero weights occurring are q^{N-1} and the cardinalities of the complements of subspaces of codimension r of Σ, where $1 \leq r \leq t$. Moreover, the support of any word of weight $q^{N-1} - q^{N-1-r}$ indeed corresponds to the points not contained in some subspace of codimension r of Σ. Again, it is not difficult to see that one always obtains words in $U \otimes E$ which are non-zero over the *entire* support of U, where U is the r-dimensional subspace of R associated with any given subspace of codimension r of Σ; a simple combinatorial proof for this fact can be found in Lemma 3.3 of [24].

In particular, all complements of subspaces of codimension $N - 1 - d$ of Σ arise in the manner just described, since we have assumed $t \geq N - 1 - d$. Selecting a word with full support in each of the associated subspaces $U \otimes C$ of C then gives us an E-incidence matrix $\tilde{M}$ for the incidence structure formed by the points of Σ and all complements of subspaces of Σ with dimension at least d. By construction, all rows of $\tilde{M}$ are words in the E-extension C of the first order Reed–Muller code R.

We may now copy the arguments given in the proof of Proposition 3.3 to see that $\tilde{M}$, when restricted to its first v columns, again contains an E-incidence matrix M of $\mathcal{D}^*$, so that that the restriction $C' = C|V$ of C to the positions associated with the common point set V of $\mathcal{D}$ and $\mathcal{D}^*$ contains an E-incidence matrix M of $\mathcal{D}^*$.

By Proposition 2.2, C is the E-extension of its trace code $Tr(C) = R$, and thus C' is the E-extension of its trace code $Tr(C') = R|V$. Since the E-code $C(M)$ generated by M is contained in the Galois closed code C', its trace code $Tr(C(M))$ is contained in $Tr(C') = R|V$. As in the first part of the proof, we can even conclude $Tr(C(M)) = R|V$, since N was chosen to be minimal. But R contains the all-1 vector, and therefore $Tr(C(M))$ indeed contains a word with full support V. □

An interesting application of the second part of Theorem 3.4 is as follows:

Corollary 3.5 *Assume that $\mathcal{D}$ is resolvable with parallel classes of size* 2 (*that is*, *the complement of every block is again a block*), *so that $\mathcal{D}^* = \mathcal{D}$. Then $\mathcal{D}$ can be embedded into $AG(N-1, q)$, where $N = \dim_q \mathcal{D}$.*

Remark 3.6 All results presented in this section actually hold under somewhat weaker conditions: while it is essential that the incidence structure under consideration contains no repeated points, everything can be adapted easily to deal with repeated blocks. However, in the resulting "embeddings", repeated blocks would, of course, be induced by the same associated subspace. This would be contrary to the standard notions of embedding used in geometry, where all objects always are embedded via injections. We therefore prefer to restrict our statements to simple incidence structures as defined in the introduction.

In the next sections, we will provide several examples and applications of Theorem 3.4, namely for designs with classical parameters, for some Steiner designs, and for some configurations. These examples should suffice to show the potential which our general theory of q-dimension and embeddings offers.

4 Designs with classical parameters

We begin our series of examples by discussing designs with classical parameters, since our study [24] of the characterization problem for the classical designs among all simple 2-designs with the same parameters contains, in a very special case, the fundamental ideas of dimension and embeddings presented here in full generality.

Recall that the *classical* or *geometric* designs are the designs $PG_d(n, q)$ and $AG_d(n, q)$ formed by the points and d-spaces in some projective or affine geometry $PG(n, q)$ or $AG(n, q)$, respectively, over a finite field $GF(q)$, where $1 \le d \le n - 1$. The parameters of $PG_d(n, q)$ are as follows:

$$v = \frac{q^{n+1} - 1}{q - 1}, \quad k = \frac{q^{d+1} - 1}{q - 1}, \quad \lambda = \begin{bmatrix} n-1 \\ d-1 \end{bmatrix}_q, \tag{1}$$

where $\begin{bmatrix} m \\ i \end{bmatrix}_q$ denotes the Gaussian coefficient given by

$$\begin{bmatrix} m \\ i \end{bmatrix}_q = \frac{(q^m - 1)(q^{m-1} - 1) \cdots (q^{m-i+1} - 1)}{(q^i - 1)(q^{i-1} - 1) \cdots (q - 1)}.$$

This design has $b = \begin{bmatrix} n+1 \\ d+1 \end{bmatrix}_q$ blocks, and each point is in $r = \begin{bmatrix} n \\ d \end{bmatrix}_q$ blocks. Similarly, $AG_d(n, q)$ has parameters

$$v = q^n, \quad k = q^d, \quad \lambda = \begin{bmatrix} n-1 \\ d-1 \end{bmatrix}_q; \tag{2}$$

in this case, there are $b = q^{n-d} \begin{bmatrix} n \\ d \end{bmatrix}_q$ blocks, and each point is in $r = \begin{bmatrix} n \\ d \end{bmatrix}_q$ blocks.

It is known [7,23] that the number of designs with classical parameters grows exponentially with linear growth of n if one fixes either the dimension d or the codimension $n - d$. It is therefore natural to try to characterize the classical geometric designs among the myriads of designs with the same parameters. There are two main approaches to this problem: one may use either combinatorial properties (e.g., line size), or one may try to give a coding theoretic characterization. We refer the reader to [21] for a recent survey on designs with classical parameters, with particular emphasis on the characterization problem.

While there are rather satisfactory results for the combinatorial approach, the coding theoretic approach has—until recently—met with remarkably little success. The seminal work in this direction is due to Hamada [17] who gave a general—albeit very involved and hard to handle—formula for the p-ranks of the incidence matrices of the geometric designs $PG_d(n, q)$ and $AG_d(n, q)$, where q is a power of the prime p and where $1 \leq d \leq n-1$. He also conjectured that the geometric designs always have minimum p-rank among all designs with the same parameters; later, in the joint paper with Hamada and Ohmori [18], he proposed an even stronger conjecture, namely that the classical designs can be characterized among all designs with the same parameters as those of minimum p-rank.

While this strong version of *Hamada's conjecture* has been established in a few cases [12,18,29], a first counterexample was already contained in a paper by Goethals and Delsarte [15] well before the conjecture was made! A handful of further sporadic counterexamples were discovered later [19,30], and only recently infinite families of counterexamples were constructed [6,22]. In contrast, the original (weak) version of the conjecture is still wide open: not even a single counterexample is known, and the only cases established are those for which actually the strong version of the conjecture holds. The reader may find more details on the status of Hamada's conjecture in [21,24,33].

As the preceding discussion shows, Hamada's original approach cannot possibly characterize the classical designs in general. In 1999, the first result which successfully dealt with a family of classical designs for arbitrary values of q via coding theory appeared. It is due to Tonchev [31] who used codes spanned by matrices with entries from $GF(q)$ to prove a characterization of the complementary designs of $PG_{n-1}(n, q)$ and $AG_{n-1}(n, q)$. Tonchev's approach was recently extended in our joint paper [24] to study a possible Hamada type characterization for *all* classical designs. Using the terminology introduced in the present paper, we may summarize the main results of [24] in the following two theorems:

Theorem 4.1 *Let $\mathcal{D}^*$ be the complementary design of a design $\mathcal{D}$ with the parameters of $PG_d(n, q)$ or $AG_d(n, q)$, where $1 \leq d \leq n-1$. Then $\dim_q \mathcal{D}^* \geq n+1$, and equality holds provided that $\mathcal{D}$ is classical.*

We note in passing that Proposition 3.3 provides an alternative proof for the fact that the classical affine designs $AG_d(n, q)$ have dimension $n+1$. In contrast to the argument used in [24], this proof does not rely on the results of Jurrius [25] concerning extension codes of the first order Reed–Muller codes.

Of course, our aim is to replace "provided that" in Theorem 4.1 with "if and only if". Indeed, we achieved this in [24] for all projective instances, and for more than half of the affine cases:

Theorem 4.2 *Let $\mathcal{D}^*$ be the complementary design of a design $\mathcal{D}$ with the parameters of either $PG_d(n, q)$, where $1 \leq d \leq n-1$, or of $AG_d(n, q)$, where $d = 1$ or $(n-2)/2 < d \leq n-1$, and assume $\dim_q \mathcal{D}^* = n+1$. Then $\mathcal{D}$ is classical.*

A crucial step in dealing with the affine instances of Theorem 4.2 was a special case of Proposition 3.2, namely embedding any such design into the projective geometry $PG(n, q)$. Of course, it would be very desirable to finish the proof of the characterization for the remaining cases, which amounts to solving the following research problem:

Problem 4.3 *Let $\mathcal{D}$ be a design with the parameters of $AG_d(n, q)$, where $2 \leq d \leq (n-2)/2$, and assume that $\mathcal{D}$ is embedded in $PG(n, q)$. Prove that $\mathcal{D}$ has to be classical.*

We note that the results of the present paper go beyond those of [24] in one respect: in [24], it was shown that the solution of Problem 4.3 implies the desired characterization of the classical designs in terms of their q-dimension, whereas the present paper also establishes the converse, so that the two conjectures made in [24] are actually equivalent.

Finally, it would also be interesting to determine the dimension of some other class of designs with classical parameters, for instance, for the infinite families of counterexamples to the strong version of Hamada's conjecture constructed in [6,22]. This problem is dealt with—and reduced to a certain general conjecture concerning embeddings of "distorted" designs—in [13]; moreover, these authors show that there always exists a design $\mathcal{D}$ with the parameters of $PG_d(n, q)$, where $1 \leq d \leq n-1$, such that $\dim_q \mathcal{D}^* = n+2$.

5 Some Steiner systems

In this section, we look at some Steiner systems associated with codes of low dimension. We begin with two of the most famous sporadic Steiner systems, namely the small Witt designs. As in [2], we use the Belgian notation $S(t, k, v)$ for Steiner systems; alternatively, these objects are often referred to as t-$(v, k, 1)$-designs.

Example 5.1 Consider the ternary Golay code C, that is, the unique $[11,6,5]$-code over $GF(3)$. As is well known, the set of 66 distinct supports of the 132 words of C with (minimum) weight 5 form a Steiner system $S(4, 5, 11)$, which is likewise uniquely determined by its parameters. Let us take this Steiner system as our simple incidence structure $\mathcal{D}$. Note that C also contains 132 words of weight 6, which constitute the supports of the blocks of the complementary structure $\mathcal{D}^*$.

Moreover, all words of weight 6 have parity check sum 0, that is, their coordinates always sum to 0. This is easily seen by comparing the weight distributions of C and of its parity check extension C', the extended ternary Golay code. Therefore $\mathcal{D}^*$ is supported by the $[11, 5, 5]$-subcode C_0 of C which consists of all words with parity check sum 0. This shows $\dim_3 \mathcal{D}^* \leq 5$; on the other hand, also $\dim_3 \mathcal{D}^* \geq 5$, as we need $132 > 3^4$ codewords.

By Theorem 3.4, $\mathcal{D}$ can be embedded into $PG(4, 3)$, and this is the smallest possible embedding into a projective space over $GF(3)$. Such an embedding is already contained in the paper of Tallini [28]; its point set is actually the (unique) smallest complete cap in $PG(4, 3)$. See also Hirschfeld [20] for an explicit construction, which takes some effort, and further references. Our theory yields this embedding result in an almost trivial way.

Finally, we note that C_0 cannot contain a word of weight 11, as the zero word and the 110 words of weight 9 of C belong to C_0, which already gives all 243 words. Using Theorem 3.4 again, we conclude that $\mathcal{D}$ cannot be embedded into $AG(4, 3)$.

Example 5.2 Consider the extended ternary Golay code C', that is, the unique $[12,6,6]$-code over $GF(3)$; this is the parity check extension of the code C considered in Example 5.1. As is well known, the set of 132 distinct supports of the 264 words of C' with (minimum) weight 6 form a Steiner system $S(5, 6, 12)$, which is again uniquely determined by its parameters. Let us now take this Steiner system as our simple incidence structure $\mathcal{D}$. Note that $\mathcal{D}$ is resolvable, so that $\mathcal{D} = \mathcal{D}^*$. Hence Corollary 3.5 applies, and we will obtain an affine embedding of $\mathcal{D}$.

As $\mathcal{D}$ is supported by C', we have $\dim_3 \mathcal{D} \leq 6$; on the other hand, also $\dim_3 \mathcal{D} \geq 6$, as we need $264 > 3^5$ codewords. By Theorem 3.4, $\mathcal{D}$ can be embedded into $AG(5, 3)$, and this is the smallest possible embedding into a projective space over $GF(3)$. Again, an embedding into $PG(5, 3)$ is already known: Coxeter [9] gave an explicit construction, which is considerably more involved. As in Example 5.1, our theory yields his result in a very simple way.

As our third example, we consider the classical Möbius planes:

Example 5.3 Recall that a *Möbius plane* (or *inversive plane* in the terminology of [11]) of order q is a one-point extension of an affine plane of order q, that is, a Steiner system $S(3,\ q+1,\ q^2+1)$. The classical (or *Miquelian*) examples of Möbius planes admit several distinct constructions. For our purposes, it is best to define them in the following geometric way: as points, one may take the points of a non-degenerate elliptic quadric Q in $PG(3,\ q)$, and as blocks the intersections of Q with all secant planes of Q. As this already describes an embedding of our Steiner system, we conclude that the complementary structure $\mathcal{D}^*$ of a classical Möbius plane $\mathcal{D}$ of order q always has q-dimension 4.

By Theorem 3.4, there is an associated code C over $GF(q)$ which supports the complementary 3-design $\mathcal{D}^*$. (There is no need to use extension fields of $GF(q)$ here, as the blocks of $\mathcal{D}$ are induced by subspaces of codimension 1.) The code C is a 2-weight code of type TF3 in the notation of [5]. The point set Q of $\mathcal{D}^*$ is an *ovoid* in $PG(3,\ q)$, i.e., a set of q^2+1 points, no three collinear, that meets every plane in either one or $q+1$ points. Thus, Q is a *projective set* with two intersection numbers in Delsarte's sense [10], which defines a linear code C over $GF(q)$ of length q^2+1 and dimension 4 having two nonzero weights $w_1 = q^2-q,\ w_2 = q^2$, and weight distribution (3):

$$A_0 = 1, \quad A_{q^2-q} = (q^2+1)q(q-1), \quad A_{q^2} = (q^2+1)(q-1). \tag{3}$$

A $4 \times (q^2+1)$ generator matrix G is obtained by taking as columns a set of q^2+1 vectors representing the projective coordinates of the points of Q. Since every three columns of G are linearly independent, the dual code $C^{\perp}$ has minimum distance 4. The code C has only one nonzero weight $w_1 = q^2-q$ smaller than $n-3 = q^2-2$, hence, it follows by the Assmus–Mattson theorem that the codewords of C of weight q^2-q support a 3-design $\mathcal{D}^*$. Calculating the number of blocks of $\mathcal{D}^*$ from (3) and taking into account that each block is supported by $(q-1)$ vectors being scalar multiples of each other, one sees that the complementary design of $\mathcal{D}^*$ is indeed an $S(3,\ q+1,\ q^2+1)$.

In general, any set P of points in $PG(N-1,\ q)$ which intersects every hyperplane in either x or y points $(0 \le x < y)$, yields a linear 2-weight code C over $GF(q)$ via Delsarte's construction [10]. The code C is of length $n = |P|$, dimension N, and has nonzero weights $w_1 = n-y,\ w_2 = n-x$. Well-known examples of such sets in $PG(2,\ q)$ are hyperovals, maximal arcs, and unitals.

Example 5.4 A *hyperoval* in $PG(2,\ 2^t)$ is a set P of 2^t+2 points, such that every line is either disjoint from P or meets P in exactly two points. A hyperoval defines a 2-weight code C over $GF(2^t)$ of length $n = 2^t+2$, dimension $k = 3$, weights $w_1 = 2^t,\ w_2 = n = 2^t+2$. Note that $w_1 = 2^t = n-k+1$, hence C is an MDS code. The codewords of weight 2^t support the complete design on 2^t+2 points having as blocks all subsets of P of size 2^t. Thus, for every $t \ge 1$, the dimension of the trivial 2-$(2^t+2,\ 2^t,\ 2^{t-1}(2^t-1))$ design over $GF(2^t)$ is 3, in accordance with a result by Tonchev [32] concerning the connection between the q-dimension of complete designs and MDS codes.

Example 5.5 A *maximal* 2^s*-arc* in $PG(2,\ 2^t)$, where $1 \le s \le t-1$, is a set of $2^s(2^t-2^{t-s}+1)$ points that meets every line in either none or 2^s points. A maximal arc with $s = 1$ is a hyperoval. A maximal 2^s-arc defines a 2-weight code C over $GF(2^t)$ of length $n = 2^s(2^t-2^{t-s}+1)$, dimension 3, and nonzero weights $2^t(2^s-1)$ and $2^s(2^t-2^{t-s}+1)$, which is a code of type TF2 in the terminology of [5]. The points of a maximal 2^s-arc P and the intersections of P with non-disjoint lines considered as blocks form a 2-$(2^s(2^t-2^{t-s}+1),\ 2^s,\ 1)$

design. The complementary design is supported by the minimum weight vectors of the related 2-weight code.

Example 5.6 A *unital* in $PG(2,\ q^2)$ is a set of q^3+1 points that meets every line in either one or $q+1$ points. Any unital in $PG(2,q^2)$ defines a 2-weight code C over $GF(q^2)$ of length $n=q^3+1$, dimension 3, and nonzero weights q^3-q and q^3. The q^3+1 points of a unital together with the line intersections of size $q+1$ form a 2-$(q^3+1,\ q+1,\ 1)$ design $\mathcal{D}$. The blocks of the complementary design $\mathcal{D}^*$ are supported by the minimum weight vectors of C.

6 Some configurations

Finally, we look briefly at some well-known (symmetric) configurations. For our purposes, a *configuration* v_k is a simple 1-design on v points, with k points per block and k blocks per point, and no two points on more than one block; hence one usually speaks of *lines* instead of *blocks* in this situation. We will not consider non-symmetric configurations here. We refer the reader to the book of Grünbaum [16] for a systematic treatment of configurations.

We begin with three famous examples which arise in the axiomatic foundation of projective geometry; see, for instance, [3] for background. The first two of these share the remarkable property that the q-dimension of their complementary incidence structures basically does not depend on the choice of q, with only $q=2$ being an accidental exception.

Example 6.1 The well-known *Desargues configuration*, a configuration 10_3, is used to characterize the (not necessarily finite) projective planes which can be coordinatized via a skewfield (and, more generally, to derive the standard algebraic representation for projective spaces if one starts with a synthetic definition via the famous Veblen-Young axioms). Hence this configuration $\mathcal{D}$ is embedded in $PG(2,\ q)$, so that $\dim_q \mathcal{D}^* = 3$, for every prime power $q \geq 3$. For $q=2$, we have a sort of accident: $\mathcal{D}$ cannot possibly live in $PG(2,\ 2)$, as it just has too many points. Here one easily checks $\dim_2 \mathcal{D}^* = 4$: it is well-known that the Desargues configuration can always be viewed as a configuration of points and lines in projective 3-space.

Example 6.2 The well-known *Pappus configuration*, a configuration 9_3, is used to characterize those projective geometries $PG(n,\ K)$ defined over a skewfield K for which K has commutative multiplication (and is therefore a field). Again, the Pappus configuration $\mathcal{D}$ is always embedded in $PG(2,\ q)$, so that $\dim_q \mathcal{D}^* = 3$ for every prime power $q \geq 3$. As in the case of the Desargues configuration, $\mathcal{D}$ cannot live in $PG(2,\ 2)$, as it has too many points.

Again one obtains $\dim_2 \mathcal{D}^* = 4$, which is less obvious, and therefore we sketch a possible embedding of the Pappus configuration in $\Pi = PG(3,\ 2)$. Let $a,\ b,\ c,\ d$ be four points in general position, which we also view as four pairwise independent vectors in $GF(2)^4$. Now we select three skew lines of Π as the three "carrier" lines for the 9 points of $\mathcal{D}$, say

$$\{\mathbf{a},\ \mathbf{b},\ \mathbf{a}+\mathbf{b}\},\ \{\mathbf{c},\ \mathbf{d},\ \mathbf{c}+\mathbf{d}\} \text{ and } \{\mathbf{a}+\mathbf{d},\ \mathbf{b}+\mathbf{c},\ \mathbf{a}+\mathbf{b}+\mathbf{c}+\mathbf{d}\}.$$

The remaining six lines of $\mathcal{D}$ are transversals for the carrier lines, and three (pairwise skew) of these are indeed realized as lines of Π, namely

$$\{\mathbf{a},\ \mathbf{d},\ \mathbf{a}+\mathbf{d}\},\ \{\mathbf{b},\ \mathbf{c},\ \mathbf{b}+\mathbf{c}\} \text{ and } \{\mathbf{a}+\mathbf{b},\ \mathbf{c}+\mathbf{d},\ \mathbf{a}+\mathbf{b}+\mathbf{c}+\mathbf{d}\}.$$

This is not surprising: in geometric terminology, we have simply used three lines of a regulus together with three lines of its opposite regulus. It is well-known and trivial to see that the remaining three lines of $\mathcal{D}$ cannot be realized as lines of Π; however, they are induced by the three planes of Π spanned by the following 3-sets on the chosen point set V:

$$\{\mathbf{a},\ \mathbf{c},\ \mathbf{a}+\mathbf{b}+\mathbf{c}+\mathbf{d}\},\ \{\mathbf{a}+\mathbf{b},\ \mathbf{d},\ \mathbf{b}+\mathbf{c}\} \text{ and } \{\mathbf{b},\ \mathbf{c}+\mathbf{d},\ \mathbf{a}+\mathbf{d}\},$$

as the reader may easily check. According to Proposition 3.3, $\mathcal{D}^*$ is supported by a 4-dimensional code C over $GF(4)$, since we used subspaces of codimensions 1 and 2 to induce the lines of $\mathcal{D}$ on V.

Example 6.3 The smallest really interesting configuration is the *Fano configuration* $\mathcal{D}$, often simply denoted as 7_3—that is, in other notation, the projective plane $PG(2,\ 2)$ of order 2; it is used to characterize those projective geometries $PG(n,\ K)$ defined over a field K for which K has characteristic 2. In particular, $PG(2,\ q)$ contains $\mathcal{D}$ as a subplane of order 2 if and only if q is even, and we conclude $\dim_q \mathcal{D}^* = 3$ if and only if q is a power of 2.

Our final example is similar to Example 6.3, but probably even more interesting:

Example 6.4 Let $\mathcal{D} = AG(2,\ 3)$ be the unique affine plane of order 3, and let $\mathcal{D}_p$ be the configuration 8_3 which arises from $\mathcal{D}$ by omitting a point p together with all lines through p; this configuration is sometimes called the *biaffine plane* of order 3. Then any embedding of $\mathcal{D}_p$ into a projective plane $PG(2,\ q)$ can be extended to an embedding of $\mathcal{D}$, and such an embedding is possible if and only if q is a power of 3 or a prime power congruent to 1 modulo 3; see [1]. Thus $\dim_q \mathcal{D}^* = \dim_q \mathcal{D}_p^* = 3$ if and only if $q = 3^b$ or $q \equiv 1 \pmod 3$.

We remark that Example 6.4 is quite exceptional: by a result of Rigby [27], the affine plane $AG(2,\ q')$ with $q' \geq 4$ can be embedded into $PG(2,\ q)$ if and only if q is a power of q'. Therefore, $\dim_q AG(2,\ q')^* \geq 4$, whenever q is not a power of q'.

For all the configurations discussed in this section, we are not aware of any result that would give the precise value of $\dim_q \mathcal{D}^*$ for any other case than those presented here. It would certainly be interesting to know such results. In particular, we would like to pose the following research problems.

Problem 6.5 *Let $\mathcal{D}$ be the Fano configuration or the (bi-)affine plane of order 3, and assume $q \neq 2$ or $q \neq 3^b$ and $q \not\equiv 1 \pmod 3$, respectively. Decide if (and when) $\dim_q \mathcal{D}^* = 4$ is possible. Determine $\dim_q AG(2,\ q')^*$ for at least one pair $q,\ q'$, where q and q' are powers of distinct primes > 3.*

7 Conclusion

We have introduced new invariants for finite simple incidence structures $\mathcal{D}$, which admit both an algebraic and a geometric description: the smallest value of N for which $\mathcal{D}$ may be embedded into the $(N-1)$-dimensional projective geometry $PG(N-1,\ q)$ always coincides with the minimum possible dimension of a class of codes over $GF(q)$ associated with the complementary incidence structure $\mathcal{D}^*$, namely the trace codes of all codes over some extension field of $GF(q)$ which support $\mathcal{D}^*$. Thus the theory developed here gives a new, surprisingly tight, connection between simple incidence structures, linear codes, and Galois geometries.

We have also provided several examples to illustrate the new theory, namely for designs with classical parameters, for some Steiner designs, and for some configurations. We are currently investigating further classes of designs, but already the examples considered here indicate that our approach can shed new light on many well-studied classes of incidence structures and should have a considerable potential for significant applications to a wealth of known problems.

While we are convinced of the theoretical importance of our new invariants, we are far less optimistic with regard to their practical applicability. Perhaps the most attractive property of the original Hamada conjecture lies in the fact that it would have provided 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 [8, Remark VII.6.6]. In contrast, our new invariants would, in general, seem rather difficult to determine; indeed, we are not aware of any subexponential time algorithms for computing them.

Acknowledgments We thank Tim Penttila for a helpful discussion concerning configurations and an anonymous reviewer for his careful reading and helpful comments. The second author, Vladimir Tonchev, whose research was partially supported by NSA grant H98230-12-1-0213, would like to thank the University of Augsburg for the hospitality during his visit in the spring of 2011 as a Fellow of the Alexander von Humboldt Foundation: the many discussions during this visit led to the ideas first used in a very special case in [24] and now developed in general.

References

1. Abdul-Elah M.S., Al-Dhahir M.W., Jungnickel D.: 8_3 in $PG(2, q)$. Arch. Math. **49**, 141–150 (1987).
2. Beth T., Jungnickel D., Lenz H.: Design Theory, 2nd edn. Cambridge University Press, Cambridge (1999).
3. Beutelspacher A., Rosenbaum U.: Projective Geometry, 2nd edn. Cambridge University Press, Cambridge (2004).
4. Bierbrauer J.: Introduction to Coding Theory. CRC, Boca Raton (2005).
5. Calderbank R., Kantor W.M.: The geometry of two-weight codes. Bull. Lond. Math. Soc. **18**, 97–122 (1986).
6. Clark D., Jungnickel D., Tonchev V.D.: Affine geometry designs, polarities, and Hamada's conjecture. J. Comb. Theory A. **118**, 231–239 (2011a).
7. Clark D., Jungnickel D., Tonchev V.D.: Correction to: "Exponential bounds on the number of designs with affine parameters". J. Comb. Des. **19**, 156–166 (2011b).
8. Colbourn C.J., Dinitz J.H.: Handbook of Combinatorial Designs, 2nd edn. CRC Press, Boca Raton (2007).
9. Coxeter H.S.M.: Twelve points in *PG*(5, 3) with 95040 self-transformations. Philos. Trans. R. Soc. Lond. A. **247**, 279–293 (1958).
10. Delsarte P.: Weights of linear codes and strongly regular normed spaces. Discret. Math. **3**, 47–64 (1972).
11. Dembowski P.: Finite Geometries. Springer, Berlin (1968).
12. Doyen J., Hubaut X., Vandensavel M.: Ranks of incidence matrices of Steiner triple systems. Math. Z. **163**, 251–259 (1978).
13. Ghinelli D., Jungnickel D., Metsch K.: Remarks on polarity designs (Submitted).
14. Giorgetti M., Previtali A.: Galois invariance, trace codes and subfield subcodes. Finite Fields Appl. **16**, 96–99 (2010).
15. Goethals J.M., Delsarte P.: On a class of majority-logic decodable cyclic codes. IEEE Trans. Inf. Theory **14**, 182–188 (1968).
16. Grünbaum B.: Configurations of points and lines. Graduate Studies in Mathematics 103. American Mathematical Society, Providence (2009).
17. 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).
18. Hamada N., Ohmori H.: On the BIB-design having the minimum p-rank. J. Comb. Theory A. **18**, 131–140 (1975).
19. 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).
20. Hirschfeld J.W.P.H.: Projective spaces of square size. Simon Stevin **65**, 319–329 (1991).

21. Jungnickel D.: Recent results on designs with classical parameters. J. Geom. **101**, 137–155 (2011).
22. Jungnickel D., Tonchev V.D.: Polarities, quasi-symmetric designs, and Hamada's conjecture. Des. Codes Cryptogr. **51**, 131–140 (2009).
23. Jungnickel D., Tonchev V.D.: The number of designs with geometric parameters grows exponentially. Des. Codes Cryptogr. **55**, 131–140 (2010).
24. Jungnickel D., Tonchev V.D.: A Hamada type characterization of the classical geometric designs. Des. Codes Cryptogr. doi:10.1007/s10623-011-9580-3 (2011).
25. Jurrius R.: Weight enumeration of codes from finite spaces. Des. Codes Cryptogr. doi:10.1007/s10623-011-9557-2 (2011).
26. MacWilliams F.J., Sloane N.J.A.: The Theory of Error-Correcting Codes. North-Holland, Amsterdam (1977).
27. Rigby J.F.: Affine subplanes of finite projective planes. Can. J. Math. **17**, 977–1009 (1965).
28. Tallini G.: On caps of kind s in a Galois r-dimensional space. Acta Arith. **7**, 19–28 (1961).
29. Teirlinck L.: On projective and affine hyperplanes. J. Comb. Theory A. **28**, 290–306 (1980).
30. Tonchev V.D.: Quasi-symmetric 2-(31, 7, 7)-designs and a revision of Hamada's conjecture. J. Comb. Theory A. **42**, 104–110 (1986).
31. Tonchev V.D.: Linear perfect codes and a characterization of the classical designs. Des. Codes Cryptogr. **17**, 121–128 (1999).
32. Tonchev V.D.: A note on MDS codes, n-arcs and complete designs. Des. Codes Cryptogr. **29**, 247–250 (2003).
33. Tonchev V.D.: Finite geometry, designs, codes, and Hamada's conjecture. In: Crnković D., Tonchev V. (eds.) Information Security, Coding Theory and Related Combinatorics, pp. 437-448. IOS Press, Amsterdam (2011).