On the additivity of block designs[1] [2]

Andrea Caggegi
Dipartimento di Energia, Ingegneria dell'Informazione e Modelli Matematici
Università degli Studi di Palermo, Viale delle Scienze, 90128 Palermo, Italy
andrea.caggegi@unipa.it

Giovanni Falcone
Dipartimento di Matematica e Informatica
Università degli Studi di Palermo, Via Archirafi 34, 90123 Palermo, Italy
giovanni.falcone@unipa.it

Marco Pavone
Dipartimento di Energia, Ingegneria dell'Informazione e Modelli Matematici
Università degli Studi di Palermo, Viale delle Scienze, 90128 Palermo, Italy
marco.pavone@unipa.it

Abstract

We show that symmetric block designs $\mathcal{D} = (\mathcal{P}, \mathcal{B})$ can be embedded in a suitable commutative group $\mathfrak{G}_\mathcal{D}$ in such a way that the sum of the elements in each block is zero, whereas the only Steiner triple systems with this property are the point-line designs of $\mathrm{PG}(d, 2)$ and $\mathrm{AG}(d, 3)$. In both cases, the blocks can be characterized as the only k-subsets of $\mathcal{P}$ whose elements sum to zero. It follows that the group of automorphisms of any such design $\mathcal{D}$ is the group of automorphisms of $\mathfrak{G}_\mathcal{D}$ that leave $\mathcal{P}$ invariant.

In some special cases, the group $\mathfrak{G}_\mathcal{D}$ can be determined uniquely by the parameters of $\mathcal{D}$. For instance, if $\mathcal{D}$ is a $2-(v, k, \lambda)$ symmetric design of prime order p not dividing k, then $\mathfrak{G}_\mathcal{D}$ is (essentially) isomorphic to $(\mathbb{Z}/p\mathbb{Z})^{\frac{v-1}{2}}$, and the embedding of the design in the group can be described explicitly. Moreover, in this case, the blocks of $\mathcal{B}$ can be characterized also as the v intersections of $\mathcal{P}$ with v suitable hyperplanes of $(\mathbb{Z}/p\mathbb{Z})^{\frac{v-1}{2}}$.

1 Introduction

Many classical examples in Design Theory lead to the following question: what block designs can be seen as subsets of a commutative group in such a way that the sum of the elements in every block is zero?

For some geometric designs, such as any point-flat $2-(v, k, \lambda)$ design $\mathcal{D} = (\mathcal{P}, \mathcal{B})$ of an affine geometry $\mathrm{AG}(d, q)$ over the Galois field $\mathrm{GF}(q)$, such a group is somehow intrinsic, as $\mathcal{P}$ can be seen as the set of elements of the group $\mathrm{GF}(q)^d$, and, for $k > 2$, any block of $\mathcal{B}$ has this property. However, for designs that are defined in a purely combinatorial way, it is not obvious that they should have an algebraic representation of this sort. Moreover, whenever such a group exists, another natural question is whether the blocks of the design $\mathcal{D} = (\mathcal{P}, \mathcal{B})$ are the only k-subsets of $\mathcal{P}$ whose elements add up to zero in the group.

For a $t-(v, k, \lambda_t)$ design $\mathcal{D} = (\mathcal{P}, \mathcal{B})$, there is an essentially unique way to define such a commutative group: let $\mathfrak{G}_\mathcal{D}$ be the finitely presented commutative group whose generators are the points of $\mathcal{P}$ and whose relations are simply the equalities $X_1 + \cdots + X_k = 0$, as

[1] This research was supported by Università di Palermo (2012-ATE-0446)

[2] AMS MSC 05B05, 05B25, 05B07.

$\mathfrak{b} = \{X_1, \ldots, X_k\}$ ranges over the blocks in $\mathcal{B}$. We say that $\mathcal{D}$ is *additive* if distinct points of $\mathcal{P}$ are still distinct in the group $\mathfrak{G}_{\mathcal{D}}$.

As we show here, symmetric 2-designs and, more generally, linked 1-designs are among these. On the contrary, Steiner triple systems very often are not: the only additive Steiner triple systems are the point-line designs of $\mathrm{PG}(d, 2)$ and $\mathrm{AG}(d, 3)$.

For additive Steiner triple systems, as the third point of a block is the opposite of the sum of the other two points, it is trivial that the blocks can be characterized as the only 3-subsets of $\mathcal{P}$ whose elements sum to zero in $\mathfrak{G}_{\mathcal{D}}$. We show that also for linked designs $\mathcal{D}$ the blocks are the only k-subsets of $\mathcal{P}$ whose elements sum to zero in $\mathfrak{G}_{\mathcal{D}}$. As a consequence of this characterization of the blocks, the group of automorphisms of a linked design $\mathcal{D}$ is the group of automorphisms of $\mathfrak{G}_{\mathcal{D}}$ that leave $\mathcal{P}$ invariant.

The additivity property, and the same intrinsic characterizations for the blocks and for the automorphism group, can be proved also for affine 2-designs (see [3]).

The group $\mathfrak{G}_{\mathcal{D}}$ can be determined by the parameters of $\mathcal{D}$ only in special cases (see, for instance, the introduction of section 3, Remark 3.8 (b), and Theorem 4.8), corresponding to the computation of the p-ranks of an incidence matrix of $\mathcal{D}$. In Remark 4.12, moreover, we stress the meaning of the p-rank in relation to the number of blocks necessary to determine all the other blocks. We take the occasion to point out the strong connection with questions on the p-rank in Coding Theory (see Remarks 4.7 and 4.10).

The $2-(11, 5, 2)$ Hadamard design served us as a model throughout the paper: in the Examples 2.3 and 4.11 we represent its set of elements $\mathcal{P}$ as a set of eleven points in $(\mathbb{Z}/3\mathbb{Z})^5$, and describe the eleven blocks both as the only 11-tuples of points of $\mathcal{P}$ whose sum is zero and as the intersections of $\mathcal{P}$ with eleven suitable hyperplanes. According to Theorem 4.8, this general description holds at least for any symmetric design whose order is a prime number p, not dividing k. Accordingly, in Remark 4.13 we represent the automorphism group of the $2-(11, 5, 2)$ Hadamard design as a subgroup of $\mathrm{GL}_5(3)$ and verify that it is isomorphic to $\mathrm{PSL}_2(11)$ and acts 2-transitively on $\mathcal{P}$.

2 Additive designs

Throughout the paper, we denote by $\mathcal{D} = (\mathcal{P}, \mathcal{B})$ a $t-(v, k, \lambda_t)$ design, hence an $s-(v, k, \lambda_s)$ design for any $s \leq t$, with $\lambda_s\binom{k-s}{t-s} = \lambda_t\binom{v-s}{t-s}$. As usual, we shorten λ_1, λ_2, and $|\mathcal{B}|$, by r (the *replication* number), λ, and b, respectively (hence $r = \frac{\lambda(v-1)}{k-1}$; also, $b = \frac{vr}{k}$), and we call the integer $r - \lambda$ the *order* of $\mathcal{D}$. Also, we denote by I and J, respectively, the identity matrix and the (not always necessarily square) matrix all the entries of which are equal to 1. Hence a $b \times v$ matrix A is an incidence matrix of a $2-(v, k, \lambda)$ design if and only if each row of A has k entries equal to 1 and $v - k$ entries equal to 0, and $A'A = (r - \lambda)I + \lambda J$.

As mentioned earlier, in order to find a commutative group where $\mathcal{P}$ can be embedded in such a way that the sum of the elements in any block is zero, let $\mathfrak{G}$ be the free commutative group generated by the v points of $\mathcal{P}$ and let $\mathfrak{R}$ be the subgroup of $\mathfrak{G}$ generated by the b elements of the form $\sum_{X \in \mathfrak{b}} X$, where $\mathfrak{b}$ is a block of $\mathcal{B}$. Fixing an incidence matrix A of $\mathcal{D}$ and, consequently, identifying $\mathfrak{G}$ with $\mathbb{Z}^v$, the subgroup $\mathfrak{R}$ is generated by the b rows of A. Finally, define the group $\mathfrak{G}_{\mathcal{D}} = \mathfrak{G}/\mathfrak{R}$ and consider the map $\chi : \mathcal{P} \longrightarrow \mathfrak{G}_{\mathcal{D}}$, $\chi(X) = X + \mathfrak{R}$. Hereby, χ is a map from $\mathcal{P}$ into the commutative group $\mathfrak{G}_{\mathcal{D}}$ and $\sum_{X\in\mathfrak{b}} \chi(X) = 0$ for any block $\mathfrak{b}$ in $\mathcal{B}$.

If the map χ is injective, then we may identify the points of the design with the corresponding elements of the group. But the map χ is not always injective. For instance, for any design for which there exist $k-1$ points lying in more than one block, the map χ cannot be injective, as (the image of) any point in a block is necessarily the opposite of the sum of the other $k-1$ points.

This happens, for instance, in three of the four non-isomorphic $2-(8,4,3)$ designs. It turns out that χ is injective only for the (affine) point-plane design of $\mathrm{AG}(3,2)$, whereas the other three designs collapse respectively to one, two, four elements of $\mathfrak{G}_{\mathcal{D}}$, thereby confirming, incidentally, that the four designs are mutually non-isomorphic.

It must be said, in this respect, that in general it is not true that $\mathfrak{G}_{\mathcal{D}_1}$ and $\mathfrak{G}_{\mathcal{D}_2}$ are non-isomorphic groups whenever $\mathcal{D}_1$ and $\mathcal{D}_2$ are non-isomorphic designs. For instance, as we will show in the introduction of section 3, for any Steiner triple system $\mathcal{D}$ of order $v \equiv 1$ (12), the group $\mathfrak{G}_{\mathcal{D}}$ is always isomorphic to $\mathbb{Z}/3\mathbb{Z}$, and, furthermore, all the points of $\mathcal{D}$ are mapped by χ onto the same generator of $\mathfrak{G}_{\mathcal{D}}$.

Therefore it makes sense to give the following

2.1 Definition: *If the map χ is injective, then we say that $\mathcal{D}$ is an* additive *design.*

For a 1-design, the group $\mathfrak{G}_{\mathcal{D}}$ can be infinite (for instance, if $\mathcal{P} = \{a,b,c,d\}$ and $\mathcal{B} = \{\{a,b\},\{c,d\}\}$, then $\mathfrak{G}_{\mathcal{D}}$ is isomorphic to $\mathbb{Z}^2$; see, more generally, Remark 2.4 (*ii*)), but the following theorem shows that this is never the case for a 2-design (except in the trivial case where the order $r-\lambda$ is zero, that is, equivalently, $k = v$).

2.2 Theorem: *Let $\mathcal{D} = (\mathcal{P},\mathcal{B})$ be a $2-(v,k,\lambda)$ design with $k < v$, let $\chi : \mathcal{P} \longrightarrow \mathfrak{G}_{\mathcal{D}}$ be as above and let $\Omega = \sum_{Y\in\mathcal{P}} \chi(Y) \in \mathfrak{G}_{\mathcal{D}}$. Then the group $\mathfrak{G}_{\mathcal{D}}$ is finite and, for any $X \in \mathcal{P}$, the following hold:*

(i) $(r-\lambda)\,\chi(X) = -\lambda\,\Omega$;
(ii) $(r-\lambda)\,\chi(X) = 0$, if $\mathcal{P}$ has a partition in blocks;
(iii) $k(r-\lambda)\,\chi(X) = 0$;
(iv) $r(r-\lambda)\,\chi(X) = 0$;
(v) more generally, if $c = \gcd(r,\lambda)$ and $d = \gcd(k, \frac{r}{c})$, then $d\,(r-\lambda)\,\chi(X) = 0$.

Proof. If we let $\mathfrak{X} = (\chi(P_1), \chi(P_2), \ldots, \chi(P_v))$, then

$$A\mathfrak{X}' = \left(\sum_{P\in\mathfrak{b}_1} \chi(P)\,, \ldots, \sum_{P\in\mathfrak{b}_b} \chi(P)\right)' = (0,\ldots,0)',$$

hence $A'(A\mathfrak{X}') = (0,\ldots,0)'$. On the other hand, $(A'A)\mathfrak{X}' = \big((r-\lambda)I + \lambda J\big)\mathfrak{X}'$, that is, (*i*).

The assertion (*ii*) follows directly, because $\Omega = 0$ if $\mathcal{P}$ has a partition in blocks. The assertion (*iii*) follows from (*i*) and from the fact that, for any block $\mathfrak{b} = \{X_1,\ldots,X_k\} \in \mathcal{B}$,

$$-\,k\,\lambda\,\Omega = (r-\lambda)\sum_{i=1}^{k} \chi(X_i) = 0.$$

It follows, in particular, that the commutative, finitely generated group $\mathfrak{G}_{\mathcal{D}}$ is finite. The assertion (iv) follows from (i) and from a double-counting argument, as

$$0 = \sum_{\mathfrak{b}\in\mathcal{B}} \sum_{X\in\mathfrak{b}} \chi(X) = r \sum_{X\in\mathcal{P}} \chi(X) = r\,\Omega. \tag{1}$$

Finally, by (i) and (1),

$$\frac{r}{c}\,(r-\lambda)\,\chi(X) = -\frac{r}{c}\,\lambda\,\Omega = -\frac{\lambda}{c}\,r\Omega = 0,$$

whence the last assertion follows manifestly because of (iii). □

2.3 Example: Let $\mathcal{D} = (\mathcal{P}, \mathcal{B})$ be the $2-(11,5,2)$ Hadamard design and let A be the incidence matrix for $\mathcal{D}$ given below. By combining the Gaussian and the Euclidean algorithms, one can reduce A by elementary integer row operations to its unique *Hermite normal form*, that is, to an echelon matrix where every pivot is a positive integer, above which one finds smaller non-negative integers:

$$A = \begin{pmatrix} 1&1&1&1&1&0&0&0&0&0&0\\ 1&1&0&0&0&1&1&1&0&0&0\\ 1&0&1&0&0&1&0&0&1&1&0\\ 1&0&0&1&0&0&1&0&1&0&1\\ 1&0&0&0&1&0&0&1&0&1&1\\ 0&1&1&0&0&0&1&0&0&1&1\\ 0&1&0&1&0&0&0&1&1&1&0\\ 0&1&0&0&1&1&0&0&1&0&1\\ 0&0&1&1&0&1&0&1&0&0&1\\ 0&0&1&0&1&0&1&1&1&0&0\\ 0&0&0&1&1&1&1&0&0&1&0 \end{pmatrix} \rightsquigarrow H\cdot A = \left(\begin{array}{cccccc|ccccc} 1&0&0&0&0&0&2&1&1&2&3\\ 0&1&0&0&0&0&1&2&1&0&5\\ 0&0&1&0&0&0&0&1&2&1&5\\ 0&0&0&1&0&0&2&2&0&1&4\\ 0&0&0&0&1&0&1&0&2&2&4\\ 0&0&0&0&0&1&1&1&1&1&10\\ \hline 0&0&0&0&0&0&3&0&0&0&12\\ 0&0&0&0&0&0&0&3&0&0&12\\ 0&0&0&0&0&0&0&0&3&0&12\\ 0&0&0&0&0&0&0&0&0&3&12\\ 0&0&0&0&0&0&0&0&0&0&15 \end{array}\right).$$

From the last five rows it follows that $15\chi(P_{11}) = 0$ and $3\chi(P_i) = 3\chi(P_{11})$ for all $i = 7, 8, 9, 10$, whereas from the first six rows it follows that, for all $j = 1, \ldots, 6$, $\chi(P_j)$ depends on $\chi(P_7), \ldots, \chi(P_{11})$. Hence $\mathfrak{G}_{\mathcal{D}}$ is isomorphic to $\mathbb{Z}/5\mathbb{Z} \oplus (\mathbb{Z}/3\mathbb{Z})^5$, and we can assume, up to isomorphism, that

$$\begin{array}{lll} \chi(P_7) = (1;1,0,0,0,0) & \chi(P_8) = (1;0,1,0,0,0) & \chi(P_9) = (1;0,0,1,0,0)\\ \chi(P_{10}) = (1;0,0,0,1,0) & \chi(P_{11}) = (1;0,0,0,0,1). & \end{array}$$

From the first row it now follows that

$$\chi(P_1) = -\Big(2\chi(P_7) + \chi(P_8) + \chi(P_9) + 2\chi(P_{10}) + 3\chi(P_{11})\Big) = -(4;2,1,1,2,3) = (1;1,2,2,1,0).$$

Similar equalities can be obtained for $\chi(P_2), \ldots, \chi(P_6)$ from the corresponding rows of the matrix. As a result, the points of $\mathcal{P}$ can be finally represented in $\mathbb{Z}/5\mathbb{Z} \oplus (\mathbb{Z}/3\mathbb{Z})^5$ as follows:

$$\begin{array}{lll} P_1 \equiv (1;1,2,2,1,0) & P_2 \equiv (1;2,1,2,0,1) & P_3 \equiv (1;0,2,1,2,1)\\ P_4 \equiv (1;1,1,0,2,2) & P_5 \equiv (1;2,0,1,1,2) & P_6 \equiv (1;2,2,2,2,2)\\ P_7 \equiv (1;1,0,0,0,0) & P_8 \equiv (1;0,1,0,0,0) & P_9 \equiv (1;0,0,1,0,0)\\ P_{10} \equiv (1;0,0,0,1,0) & P_{11} \equiv (1;0,0,0,0,1). & \end{array}$$

Hence $\mathcal{D}$ is an additive design. Note that, in accordance with the following Remark 2.4 (i), the first coordinate, constantly equal to $1 \in \mathbb{Z}/5\mathbb{Z}$, can be disregarded.

2.4 Remark: (i) As illustrated in the above example, the Sylow p-subgroups of the commutative group $\mathfrak{G}_{\mathcal{D}}$ can be related to the p-rank of the incidence matrix A of $\mathcal{D}$. The proof of Theorem 2.2 can be compared with that of Theorem 2.1 in [7], where it is stated that, for a prime p not dividing $r-\lambda$: (a) if p does not divide r, then the p-rank of A is v; (b) if p divides r, then the p-rank of A is either v or $v-1$; (c) if p divides r and k, then the p-rank of A is $v-1$; conversely, if the p-rank of A is $v-1$, then p divides r and k (cf. [1, Theorem 2.4.1]). In passing, note that Theorem 2.2 (v) proves that p must also divide the coefficient d defined therein. Moreover, in case (c), as the p-rank of A is $v-1$, one finds that, by reducing A modulo p, the Sylow p-subgroup $\mathfrak{S}_p$ of $\mathfrak{G}_{\mathcal{D}}$ is non-trivial (and cyclic). But, since $(r-\lambda)\,\chi(X) = -\lambda\,\Omega$ by Theorem 2.2 (i), and since $r-\lambda$ is invertible modulo any p-power, the component of $\chi(X)$ in $\mathfrak{S}_p$ is constant and thus may be disregarded, as in Example 2.3.

(ii) As illustrated in Example 2.3, the fact that the group $\mathfrak{G}_{\mathcal{D}}$ is finite for any $2-(v,k,\lambda)$ design $\mathcal{D}=(\mathcal{P},\mathcal{B})$ can also be seen as a direct consequence of standard results on subgroups of finitely generated free commutative groups, because $|A'A| = rk(r-\lambda)^{v-1}$ (cf. [2, Lemma 2.3, p. 65]), hence the v columns of the incidence matrix A are linearly independent over $\mathbb{Q}$ (except in the trivial case where $k=v$, that is, equivalently, the order $r-\lambda$ is zero).

Conversely, the same arguments yield that $\mathfrak{G}_{\mathcal{D}}$ is infinite for any 1-design having more points than blocks. For the sake of completeness, we note that $\mathfrak{G}_{\mathcal{D}}$ can be finite also in the case of a 1-design (which is not a 2-design): for instance, if $\mathcal{D}=(\mathcal{P},\mathcal{B})$, where $\mathcal{P}=\mathbb{Z}/8\mathbb{Z}$ and $\mathcal{B}$ consists of all pairs of elements in $\mathcal{P}$ of the form $\{i,i+1\}$ and $\{i,i+4\}$, then $\mathfrak{G}_{\mathcal{D}}$ is isomorphic to $\mathbb{Z}/2\mathbb{Z}$.

The following proposition gives a condition for the injectivity of χ which will be used in proving that symmetric designs are additive.

2.5 Proposition: *A $t-(v,k,\lambda_t)$ design $\mathcal{D}$ is additive if and only if, for any $\mathbf{v}\in\mathbb{Z}^b$ and for any $v\times v$ permutation matrix Q,*

$$\mathbf{v}A \neq (1,-1,0,\ldots,0)Q,$$

where A is an incidence matrix of $\mathcal{D}$. In particular, if $\mathbf{v}AA'\mathbf{v}'\neq 2$ for any vector $\mathbf{v}\in\mathbb{Z}^b$, then $\mathcal{D}$ is additive.

Proof. The map χ is injective if and only if $P_i - P_j \notin \mathfrak{N}$ whenever $i\neq j$, which is equivalent to the fact that, for any $v\times v$ permutation matrix Q, the row $(1,-1,0,\ldots,0)Q$ is not an integer combination of the rows of A. The latter claim follows because $QQ'=I$ for any permutation matrix Q. □

We take note here of the following result, which, for linked designs, will be completed in Corollary 4.3, where we will prove that every automorphism of $\mathcal{D}$ is induced by a group automorphism of $\mathfrak{G}_{\mathcal{D}}$.

2.6 Proposition: *Let $\mathcal{D}=(\mathcal{P},\mathcal{B})$ be an additive design and let f be an automorphism of $\mathcal{D}$. Then f can be extended to a group automorphism $\widetilde{\mathfrak{f}}$ of $\mathfrak{G}_{\mathcal{D}}$ such that $\widetilde{\mathfrak{f}}\chi=\chi f$.*

Proof. Extend f to an automorphism $\mathfrak{f}$ of the free commutative group $\mathfrak{G}$ generated by the points of $\mathcal{P}$. Since the subgroup $\mathfrak{N}$ of $\mathfrak{G}$ generated by the b elements of the form $\sum_{X\in\mathfrak{b}} X$ (with

$\mathfrak{b} \in \mathcal{B}$) is invariant under $\mathfrak{f}$, the automorphism $\mathfrak{f}$ induces an automorphism $\widetilde{\mathfrak{f}}$ of $\mathfrak{G}_{\mathcal{D}} = \mathfrak{G}/\mathfrak{N}$. Finally, $\widetilde{\mathfrak{f}}(\chi(X)) = \mathfrak{f}(X) + \mathfrak{N} = f(X) + \mathfrak{N} = \chi(f(X))$ for all X in $\mathcal{P}$. □

As we mentioned earlier, the definition of additivity given above is, in an appropriate sense, the only possible one, as the following proposition ultimately shows.

2.7 Proposition: *A design $\mathcal{D}$ is additive if and only if it can be embedded in a commutative group in such a way that the sum of the points in any given block is zero. Moreover, any minimal commutative group in which $\mathcal{D}$ can be embedded in such a way is a homomorphic image of $\mathfrak{G}_{\mathcal{D}}$.*

Proof. Let $\psi : \mathcal{P} \longrightarrow G$ be an embedding such that $\sum_{P \in \mathfrak{b}} \psi(P) = 0$ for any block $\mathfrak{b} \in \mathcal{B}$, and assume that G is generated by $\psi(\mathcal{P})$. Since we can extend by additivity the map ψ to a surjective homomorphism from $\mathfrak{G}$ to G by putting

$$\psi\left(\sum_{i=1}^{v} a_i P_i\right) = \sum_{i=1}^{v} a_i \psi(P_i),$$

and since $\mathfrak{N} \subseteq \mathfrak{K}$, where $\mathfrak{K}$ is the kernel of ψ, we conclude that G is a homomorphic image of $\mathfrak{G}_{\mathcal{D}} = \mathfrak{G}/\mathfrak{N}$. Finally, χ is injective, because if $\chi(P) = \chi(Q)$, then $P - Q \in \mathfrak{N} \subseteq \mathfrak{K}$. Thus $\psi(P) = \psi(Q)$ and we get the assertion, ψ being injective on the points of $\mathcal{P}$. □

3 Steiner triple systems

As mentioned in the previous section, for any design for which there exist $k-1$ points lying in more than one block, the map χ cannot be injective. Thus, it is apparent that a $2-(v,k,\lambda)$ design with $k = 2 < v$ cannot be additive. For the same reason, for $k = 3$, the search for additive 2−designs must be restricted to the class of Steiner triple systems, that is, the class of $2-(v,3,1)$ designs, where necessarily $v \equiv 1, 3\ (6)$. Indeed, in this case the third point of the block through P and Q is necessarily $-(P+Q)$, hence $\lambda = 1$.

In the case where $\mathcal{D}$ is a Steiner triple system of order $v \equiv 1\ (12)$, we can directly say that the map χ is not injective. In fact, as a consequence of [5] and [7], for $v \equiv 1\ (12)$, the $b \times v$ incidence matrix A of $\mathcal{D}$ has rank v over any field of characteristic $p \neq 3$ and rank $v-1$ over a field of characteristic $p = 3$. Therefore, up to a permutations of the columns, we can assume that in the Hermite normal form of A all the pivots are equal to 1, except the last one, which must be a 3-power. This forces $\mathfrak{G}_{\mathcal{D}}$ to be a cyclic group of order 3^d for some d. On the other hand, for $v \equiv 1\ (12)$, we have that $k(r-\lambda) = 3(6s-1)$ for some s, whence the g.c.d. between 3^d and $k(r-\lambda)$ is equal to 3. It follows, by the above Theorem 2.2 (*iii*), that $\mathfrak{G}_{\mathcal{D}}$ is a cyclic group of order 3 (independently of $\mathcal{D}$). Since $\mathcal{P}$ has more than three elements, we can now conclude that χ is not injective.

Furthermore, the reduction to the Hermite normal form leaves the sum of the entries in any row congruent to zero modulo 3, thus in each row (but the last non-zero row, where the pivot is equal to 3) the only non-zero entries are the pivot, which is equal to 1, and the last entry, which is equal to 2. This shows that all the points collapse onto the same element.

Note that, for $p > 3$, the p-rank of any Steiner triple system with $v > 3$ is always equal to v (see [5, p. 252]). But the case $v \equiv 1\ (12)$ is the only one where, for $p = 2, 3$, the p-rank is certainly at least $v-1$, in view of the sufficient conditions given in [5] and [7], which, in the cases $v \equiv 3$ (6) and $v \equiv 7$ (12), might not be satisfied.

In this section we show that the only additive Steiner triple systems are the point-line designs of either a projective space PG$(d,2)$ over GF(2) or an affine space AG$(d,3)$ over GF(3).[3]

Throughout this section, $\mathcal{D} = (\mathcal{P}, \mathcal{B})$ will be a Steiner triple system (STS, for short) with $v > 3$ points (the case $v = 3$ being trivial).

Whenever X and Y are distinct points in $\mathcal{P}$, there exist three distinct triples $\{X, A, B\}, \{X, C, D\}$, and $\{Y, A, C\}$ in $\mathcal{B}$. Indeed, since $v = |\mathcal{P}| > 3$, there exists at least a block $\{X, A, B\}$ not containing Y; it then suffices to take the unique block $\{Y, A, C\}$ through A and Y, and the unique block $\{X, C, D\}$ through X and C. This simple fact, which will be used several times in this section, is also the premise of the following basic definitions.

3.1 Definition: (see [4, p. 211]) *Let $\{X,\ A,\ B\}$, $\{X,\ C,\ D\}$, $\{Y,\ A,\ C\}$, $\{Z,\ B,\ D\}$ be a configuration of four distinct blocks in $\mathcal{B}$.*

(*i*) *If $Z = Y$, then the four-block configuration is called a* Pasch configuration *or* quadrilateral.

(*ii*) *If $Z \neq Y$ and $\{X, Y, Z\}$ is a block in $\mathcal{B}$, then the five-block configuration is called a* mitre.

3.2 Definition: (cf. [4, pp. 147, 149, 213]) *Let again $\mathcal{D}$ be an STS.*

(*i*) *Let X be a point in $\mathcal{P}$. If for any pair of distinct points A, Y in $\mathcal{P}$, with X, A, Y not in the same block, there exists a Pasch configuration $\{X, A, B\}$, $\{X, C, D\}$, $\{Y, A, C\}$, $\{Y, B, D\}$, then X is called a* Veblen point.

(*ii*) *If every three points not lying in a common block generate an STS with* 9 *elements, then $\mathcal{D}$ is called a* Hall triple system *(HTS, for short).*

(*iii*) *If $\mathcal{D}$ contains no Pasch configurations, then it is called* anti-Pasch *or* quadrilateral-free.

3.3 Lemma: *Let $(G, +)$ be a commutative group such that $\mathcal{P} \subseteq G$ and $X + Y + Z = 0$ for any block $\{X, Y, Z\}$ in $\mathcal{B}$.*

(*a*) *If X, Y are points in $\mathcal{P}$ and $2X + Y = 0$, then $X = Y$.*

(*b*) *If $\{X, A, B\}, \{X, C, D\}, \{Y, A, C\}, \{Y, B, D\}$ is a Pasch configuration, then $2X = 2Y$, $3X \neq 0$, and $3Y \neq 0$.*

(*c*) *If $\{X, A, B\}, \{X, C, D\}, \{Y, A, C\}, \{Z, B, D\}$ are blocks in $\mathcal{B}$, with $Y \neq Z$, then $\{X, Y, Z\}$ is a block (hence the five blocks form a mitre) and $3X = 0$.*

Proof. Suppose that X, Y are points in $\mathcal{P}$ and $2X + Y = 0$, that is, $X + Y + X = 0$. If $X \neq Y$, then there exists Z in $\mathcal{P}$ such that $\{X, Y, Z\}$ is a block. Thus $X + Y + Z = 0$, which implies that $X = Z$. This contradiction shows that $X = Y$.

Now let $\{X, A, B\}, \{X, C, D\}, \{Y, A, C\}, \{Z, B, D\}$ be four distinct blocks in $\mathcal{B}$ (where Y and Z are not necessarily distinct; see Figure 1). Then $(X + A + B) + (X + C + D) = 0$, that is, $2X + (A + C) + (B + D) = 0$, whence

$$2X - Y - Z = 0. \tag{2}$$

[3] For the sake of reference, we note that this result had already been announced in [6, p. 892] in a citation to the present paper.

In case (b), $Y = Z$, thus $2X = 2Y$. Also, suppose that $3X = 0$. Then $2Y + X = 2X + X = 0$, hence $X = Y$ by (a), against the hypothesis that $\{X, A, B\}$ and $\{Y, A, C\}$ were distinct triples. This contradiction shows that $3X \neq 0$. Similarly (or by symmetry), $3Y \neq 0$.

In case (c), $Y \neq Z$, thus there exists W in $\mathcal{P}$ such that $\{W, Y, Z\}$ is a block. Therefore $2X + W = 0$ by (2), hence $X = W$ by (a), whence $\{X, Y, Z\}$ is a block and $3X = 0$, as claimed. □

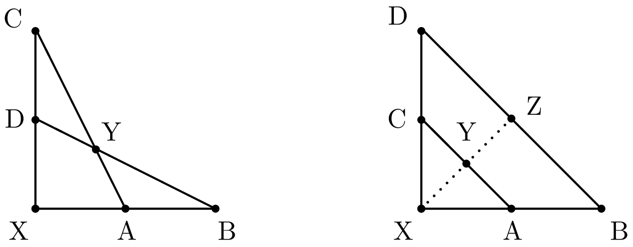

Figure 1: A Pasch configuration (left) and a mitre (right)

3.4 Corollary: *If the Steiner triple system $\mathcal{D} = (\mathcal{P}, \mathcal{B})$ is additive, then either $\mathcal{D}$ is an HTS (in particular, $\mathcal{D}$ is anti-Pasch and there exist no Veblen points in $\mathcal{P}$), or all points in $\mathcal{P}$ are Veblen points.*

Proof. Let $\mathcal{D}$ be an additive STS. By definition, we may assume that $\mathcal{P} \subseteq \mathfrak{G}_{\mathcal{D}}$ and $X + Y + Z = 0$ for any block $\{X, Y, Z\}$ in $\mathcal{B}$.

Let us now assume that there exists at least one Pasch configuration. Then, by Lemma 3.3 (b), there exists X in $\mathcal{P}$ such that

$$3X \neq 0.$$

We claim that all points in $\mathcal{P}$ are Veblen points. Let us suppose, by a contradiction, that there exists a point X' in $\mathcal{P}$ that is not a Veblen point. Then

$$3X' = 0$$

by definition of Veblen point and Lemma 3.3 (c). It follows, in particular, that $X \neq X'$. Then there exist three distinct blocks $\{X, A, B\}, \{X, C, D\}$, and $\{X', A, C\}$ in $\mathcal{B}$. Let Z in $\mathcal{P}$ be such that $\{Z, B, D\}$ is a block. If $Z = X'$, then $3X' \neq 0$ by Lemma 3.3 (b), whereas, if $Z \neq X'$, then $3X = 0$ by Lemma 3.3 (c). In any case we get a contradiction, which shows that all points in $\mathcal{P}$ are Veblen points, as claimed.

This shows that either $\mathcal{D}$ is anti-Pasch or all points in $\mathcal{P}$ are Veblen points. We are now left to show that, in the former case, $\mathcal{D}$ is an HTS.

Let $\mathcal{D}$ be anti-Pasch, and let X, Y, and A be points in $\mathcal{P}$ not in a common block. Let $\{X, A, B\}$, $\{X, C, D\}$, and $\{Y, A, C\}$ be blocks. Then the block $\{B, D, Z\}$ is such that $Z \neq Y$ and, by Lemma 3.3 (c), $\{X, Y, Z\}$ is a block. By applying the same argument to the three blocks $\{Z, B, D\}$, $\{Z, X, Y\}$, and $\{A, B, X\}$, we find a new point E and two new blocks $\{D, Y, E\}$ and $\{Z, A, E\}$. By applying again the same argument to the three blocks $\{A, B, X\}$, $\{A, Z, E\}$, and $\{D, B, Z\}$, we find a new point F and two new blocks $\{X, E, F\}$ and $\{A, D, F\}$. Considering the four blocks $\{Z, A, E\}$, $\{Z, Y, X\}$, $\{C, A, Y\}$, and $\{F, E, X\}$, by Lemma 3.3 (c) the triple

$\{Z, C, F\}$ is a block. Similarly the triples $\{B, F, Y\}$ and $\{B, C, E\}$ are blocks. Therefore these nine points, together with these twelve blocks, form an STS. □

The previous result, which is stated in purely combinatorial terms, provides a necessary condition for an STS to be additive. It is natural to ask whether the condition is also sufficient. If this were the case, then such a condition would provide an intrinsic combinatorial characterization of the additivity of a Steiner triple system. However, this is not the case, since all non-affine HTSs (cf. [4, Theorem 8.17]) provide examples of anti-Pasch STSs that are not additive.

In the following example, we apply the corollary above to the case where the order v is equal to 15. In light of the final theorem of this section, it might appear pleonastic. Still it provides, in our opinion, a better insight into the inner structure of additive STSs in terms of their admissible configurations.

3.5 Example: Among the 80 STSs with 15 elements, one and only one is additive, that is, the point-line design of $\mathrm{PG}(3,2)$. Indeed, if every point is a Veblen point, then it is easy to show that any three points, not in a block, generate an STS with 7 elements, and hence are contained in precisely four Pasch configurations. Thus one can compute the exact number of Pasch configurations as follows.

The total number of non-collinear triples is equal to $\binom{15}{3} - \frac{1}{3}\binom{15}{2}$, whereas the number of non-collinear triples in a Pasch configuration is $\binom{6}{3} - 4$, for 6 is the number of points and 4 is the number of collinear triples (i.e., blocks) in the configuration. Therefore the total number of Pasch configurations is

$$\frac{4\left(\binom{15}{3} - \frac{1}{3}\binom{15}{2}\right)}{\binom{6}{3} - 4} = 105.$$

As shown in [4, Tables 5.8–5.12], this happens only in the case labelled as #1 (that is, $\mathrm{PG}(3,2)$). The same Tables show that the only anti-Pasch STS with 15 elements is that labelled as #80. Since here the triples $\{0, 2, 1\}$, $\{0, 3, 4\}$, $\{9, 2, 3\}$, and $\{7, 1, 4\}$ are blocks, if the STS were additive, the triple $\{0, 7, 9\}$ would be a block completing a mitre, by Lemma 3.3 (c), which is not the case, as the Tables show.

We now need to state a final preliminary result in order to prove the main theorem of this section.

3.6 Corollary: *Let* $(G, +)$ *be a commutative group such that* $\mathcal{P} \subseteq G$ *and* $X + Y + Z = 0$ *for any block* $\{X, Y, Z\}$ *in* $\mathcal{B}$. *Then* $\mathcal{D}$ *satisfies one and only one of the two following conditions.*

(i) $3X = 0$ *for all* X *in* $\mathcal{P}$.

(ii) $2X = 2Y$ *for all* X, Y *in* $\mathcal{P}$.

In either case, $6X = 0$ *for all* X *in* $\mathcal{P}$.

Proof. By Corollary 3.4, either $\mathcal{D}$ is anti-Pasch or all points in $\mathcal{P}$ are Veblen points. In the former case, given any X in $\mathcal{P}$, there exist four blocks $\{X, A, B\}$, $\{X, C, D\}$, $\{Y, A, C\}$, $\{Z, B, D\}$, with $Y \neq Z$, whence $3X = 0$ (and also $6X = 0$) by Lemma 3.3 (c).

If all points in $\mathcal{P}$ are Veblen points, then let X, Y be two distinct points in $\mathcal{P}$. Then there exists a Pasch configuration $\{X, A, B\}$, $\{X, C, D\}$, $\{Y, A, C\}$, $\{Y, B, D\}$, and

$$2X = 2Y$$

by Lemma 3.3 (b). Finally, given any X in $\mathcal{P}$, and any block $\{X, A, B\}$ containing X, $6X = 2X + 2A + 2B = 2(X + A + B) = 0$. □

We may now finally state the main result of this section.

3.7 Theorem: *A Steiner triple system is additive if and only if it is isomorphic to the point-line design of either* $\mathrm{PG}(d, 2)$ *or* $\mathrm{AG}(d, 3)$ *for some integer* $d \geq 1$.

Proof. Any STS that is isomorphic to the point-line design of either $\mathrm{AG}(d, 3)$ or $\mathrm{PG}(d, 2)$ is clearly additive by Proposition 2.7.

Assume, conversely, that a Steiner triple system $\mathcal{D} = (\mathcal{P}, \mathcal{B})$ of order $v > 3$ is additive (the case $v = 3$ being trivial). Thus, by Corollary 3.4, either $\mathcal{D}$ is anti-Pasch, or all points in $\mathcal{P}$ are Veblen points. In the latter case, $\mathcal{D}$ is isomorphic to $\mathrm{PG}(d, 2)$ for some integer $d > 1$, by a well-known combinatorial characterization of finite projective geometries in terms of Veblen points (see, for instance, [4, Theorem 8.15]). Here, however, we wish to give an alternative and self-contained proof of the present characterization of additive STSs, based entirely on some necessary algebraic conditions for the additivity.

Since $\mathcal{D}$ is additive, we may assume, by definition, that $\mathcal{D}$ satisfies the hypotheses of Corollary 3.6, where $G = \mathfrak{G}_{\mathcal{D}}$. Hence $\mathcal{D}$ satisfies one (and only one) of the conditions (i) and (ii) of Corollary 3.6 and, in either case,

$$6X = 0$$

for all X in $\mathcal{P}$.

Given a point X_0 in $\mathcal{P}$, we define a map $\psi : \mathcal{P} \longrightarrow G$ by letting

$$\psi(X) = X + 2X_0$$

for all X in $\mathcal{P}$. Then ψ is injective and, for any block $\{X, Y, Z\}$,

$$\begin{aligned} \psi(X) + \psi(Y) + \psi(Z) &= X + Y + Z + 6X_0 \\ &= X + Y + Z \\ &= 0. \end{aligned} \tag{3}$$

Conversely, let X, Y, Z be three distinct points in $\mathcal{P}$ such that $\psi(X) + \psi(Y) + \psi(Z) = 0$. Then $\{X, Y, Z\}$ is in $\mathcal{B}$. Indeed, if $\{X, Y, Z'\}$ is a block, then $\psi(X) + \psi(Y) + \psi(Z') = 0$ by (3), hence $\psi(Z') = \psi(Z)$, whence $Z' = Z$ by the injectivity of ψ.

First let us suppose that $\mathcal{D}$ satisfies condition (i) of Corollary 3.6, that is, $3X = 0$ for all X in $\mathcal{P}$, corresponding to the case where $\mathcal{D}$ is anti-Pasch. Then

$$3\psi(X) = 0 \tag{4}$$

for all X in $\mathcal{P}$, as $3\psi(X) = 3X + 6X_0 = 0$.

We claim that $\psi(\mathcal{P})$ is a subgroup of G. Indeed, $\psi(X_0) = X_0 + 2X_0 = 3X_0 = 0$, whence $0 \in \psi(\mathcal{P})$. Let now X be a point in $\mathcal{P}$. If $X = X_0$, then $-\psi(X) = -\psi(X_0) = 0 \in \psi(\mathcal{P})$. If $X \neq X_0$, then let $\{X, X_0, Y\}$ be the unique block through X and X_0. Then $\psi(X) + \psi(X_0) + \psi(Y) = 0$ by (3), hence $-\psi(X) = \psi(Y) \in \psi(\mathcal{P})$.

Finally, let X, Y be points in $\mathcal{P}$. If $X = Y$, then, by (4), $\psi(X) + \psi(Y) = 2\psi(X) = -\psi(X) \in \psi(\mathcal{P})$. If $X \neq Y$, then, by (3), $\psi(X) + \psi(Y) = -\psi(Z) \in \psi(\mathcal{P})$, where $\{X, Y, Z\}$ is the unique block through X and Y, and our claim is proved.

By condition (4), we may conclude that $\psi(\mathcal{P})$ is an elementary abelian 3-group. This fact, together with the injectivity of ψ and the one-to-one correspondence between $\mathcal{B}$ and the triples of points summing to zero in $\psi(\mathcal{P})$, shows that $\mathcal{D}$ is isomorphic to the point-line design of $\mathrm{AG}(d, 3)$ for some integer $d > 1$.

We are now left with the case where $\mathcal{D}$ satisfies condition (ii) of Corollary 3.6, that is, $2X = 2Y$ for all X, Y in $\mathcal{P}$, corresponding to the case where all points in $\mathcal{P}$ are Veblen points. In this case

$$2\psi(X) = 0 \tag{5}$$

for all X in $\mathcal{P}$, as $2\psi(X) = 2X + 4X_0 = 6X_0 = 0$. Moreover,

$$0 \notin \psi(\mathcal{P}).$$

Indeed, given any X in $\mathcal{P}$, let Y be a point in $\mathcal{P}$ different from X. Then $\psi(X) \neq 0$, as $\psi(X) = X + 2X_0 = X + 2Y \neq 0$ by Lemma 3.3 (a).

Let us now define

$$H = \psi(\mathcal{P}) \cup \{0\}.$$

We claim that H is a subgroup of G. By condition (5), $-\psi(X) = \psi(X) \in H$ for all X in $\mathcal{P}$, so we only need to show that $\psi(X) + \psi(Y)$ lies in H for any pair of points X, Y in $\mathcal{P}$. If $X = Y$, this follows immediately from (5); if $X \neq Y$, then, by (3), $\psi(X) + \psi(Y) = -\psi(Z) \in H$, where $\{X, Y, Z\}$ is the unique block through X and Y, and our claim is proved.

By condition (5), H is an elementary abelian 2-group. Moreover, $\psi(\mathcal{P})$ consists precisely of the set of all non-zero elements of H. These two facts, together with the injectivity of ψ and the one-to-one correspondence between $\mathcal{B}$ and the triples of non-zero points summing to zero in H, show that $\mathcal{D}$ is isomorphic to the point-line design of $\mathrm{PG}(d, 2)$ for some integer $d > 1$. This completes the proof of the theorem. □

3.8 Final remarks: (a) The existence of non-affine anti-Pasch HTSs (cf. [4, Theorem 8.17]) makes the proof of Theorem 3.7 non-trivial, since if all anti-Pasch STSs were affine (that is, isomorphic to $\mathrm{AG}(d, 3)$ for some integer $d > 1$), then Theorem 3.7 would be an immediate consequence of Corollary 3.4, as $\mathcal{D}$ is isomorphic to $\mathrm{PG}(d, 2)$ for some integer $d > 1$ if and only if all points in $\mathcal{P}$ are Veblen points (see, for instance, [4, Theorem 8.15]).

(b) The proof of Theorem 3.7 tells us also something more precise about the embedding of an additive STS in a minimal commutative group (which, by Proposition 2.7, is a quotient group of $\mathfrak{G}_{\mathcal{D}}$). Indeed, the proof shows that whenever $\varphi : \mathcal{P} \longrightarrow G$ is an additive embedding of an STS $\mathcal{D} = (\mathcal{P}, \mathcal{B})$ in a commutative group $(G, +)$, then, up to translating $\varphi(\mathcal{P})$ in G by a suitable element of G, either $\varphi(\mathcal{P})$ is an elementary abelian 3-group, or $0 \notin \varphi(\mathcal{P})$ and $\varphi(\mathcal{P}) \cup \{0\}$ is an elementary abelian 2-group.

More precisely, since the automorphism group of $\mathrm{AG}(d, 3)$ is transitive, and the automorphism group of $\mathrm{PG}(d, 2)$ is primitive, Propositions 4 and 5 in [5] guarantee that the 2-rank of $\mathrm{AG}(d, 3)$ is $v = 3^d$, and that the 3-rank of $\mathrm{PG}(d, 2)$ is $v - 1 = 2(2^d - 1)$. On the other hand, the

3-rank of $\mathrm{AG}(d,3)$ is $3^d-(d+1)$, the 2-rank of $\mathrm{PG}(d,2)$ is $2^{d+1}-(d+2)$, and, in both cases, the p-rank is v for any other $p \neq 2,3$ (see [5], [7]). With this information, we conclude that:

if $\mathcal{D}$ is the point-line design of $\mathrm{AG}(d,3)$, then $\mathfrak{G}_{\mathcal{D}}$ is isomorphic to $(\mathbb{Z}/3\mathbb{Z})^{d+1}$. Since the sum of the entries of each row of the Hermite normal form of an incidence matrix of $\mathcal{D}$ remains a multiple of $k=3$, the sum of the entries of the image $\chi(P)$ of a point is always $1 \pmod 3$. Thus, by a cardinality argument, $\chi(\mathcal{P})$ coincides with the hyperplane of $(\mathbb{Z}/3\mathbb{Z})^{d+1}$ defined by the equation $x_1+x_2+\cdots+x_{d+1}=1$;

if $\mathcal{D}$ is the point-line design of $\mathrm{PG}(d,2)$, then $\mathfrak{G}_{\mathcal{D}}$ is isomorphic to $\mathbb{Z}/3\mathbb{Z} \oplus (\mathbb{Z}/2\mathbb{Z})^{d+1}$. Since there exists an element $\chi(P)$ with an entry equal to 1 in $\mathbb{Z}/3\mathbb{Z}$, it follows that all the elements must have the entry 1 in $\mathbb{Z}/3\mathbb{Z}$, because each of them belongs to a suitable block through P. Thus, $\chi(\mathcal{P})$ coincides with the punctured coset $\left(1 \oplus (\mathbb{Z}/2\mathbb{Z})^{d+1}\right) \setminus \{(1;0,\ldots,0)\}$.

4 Symmetric 2–designs

In this section we prove the additivity of *linked* designs, that is, $t-(v,k,\lambda_t)$ designs $\mathcal{D}$ such that two distinct blocks meet in a constant number μ of points. By two celebrated results of Ryser [11] and Röhmel [10], the class of linked $2-(v,k,\lambda)$ designs coincides exactly with that of *symmetric* $2-(v,k,\lambda)$ designs (that is, those where the number of blocks is equal to the number of points, or, equivalently, those where $r=k$), and $\mu=\lambda$.

Note, moreover, that the class of all the linked $1-(b,r,k)$ designs $\mathcal{D}'=(\mathcal{B},\mathcal{P})$ coincides exactly with the class of the *dual* designs of all the $2-(v,k,\lambda)$ designs $\mathcal{D}=(\mathcal{P},\mathcal{B})$, that is, the class of the $1-(b,r,k)$ designs obtained by interchanging the rôles of points and blocks (equivalently, A is an incidence matrix for $\mathcal{D}$ if and only if A' is an incidence matrix for $\mathcal{D}'$), and again $\mu=\lambda$.

Hence any $2-(v,k,\lambda)$ design $\mathcal{D}$, even not additive, is the dual of a linked (hence additive) $1-(b,r,k)$ design $\mathcal{D}'$. In the case where $\mathcal{D}$ is not additive, however, the group $\mathfrak{G}_{\mathcal{D}'}$ is infinite, because $\mathcal{D}'$ has more points than blocks, by Fisher's inequality (see Remark 2.4 (*ii*)).

Prominent examples of families of symmetric designs are given by the Hadamard designs (such as that in Example 2.3) and by the point-line designs of finite projective planes.

Given a linked design, the condition $\mu<k-1$ is necessary for the additivity of the design, since, as we noted in section 2, if there exist $k-1$ points lying in more than one block, then the map χ cannot be injective. The following result shows that the condition $\mu<k-1$ is actually also sufficient for the additivity of a linked design. Note that, for a linked $2-(v,k,\lambda)$ design, the condition $\mu=k-1$ is possible only for the trivial $2-(v,v-1,v-2)$ design, and that, for a linked $1-(b,r,k)$ design, dual of a given $2-(v,k,\lambda)$ design, the condition $\mu=r-1$ (that is, $\lambda=r-1$) would also give $v=b$, $k=r=v-1$ and $\lambda=\mu=v-2$.

4.1 Theorem: *Let $\mathcal{D}=(\mathcal{P},\mathcal{B})$ be a linked $t-(v,k,\lambda_t)$ design, not isomorphic to the trivial $2-(v,v-1,v-2)$ design, and let μ be the intersection number of any two distinct blocks. Then the following hold:*

(*i*) *$\mathcal{D}$ is additive;*

(*ii*) *a k-subset $\mathfrak{s}=\{X_1,\ldots,X_k\}$ of $\mathcal{P}$ is a block of $\mathcal{B}$ if and only if $\chi(X_1)+\ldots+\chi(X_k)=0$ in the group $\mathfrak{G}_{\mathcal{D}}$.*

Proof. We assume that $\mu > 0$, the case $\mu = 0$ being trivial. Also, as we noticed earlier, $\mu < k - 1$. For a linked design with incidence matrix A, where any two distinct blocks meet in μ points, $AA' = (k - \mu)I + \mu J$ (let us recall that I and J denote, respectively, the identity matrix and the not-necessarily-square all-1 matrix). Hence, for any non-zero integer b-tuple $\mathbf{v} = (v_1, \ldots, v_b)$,

$$\mathbf{v}AA'\mathbf{v}' = (k - \mu)\sum_{i=1}^{b} v_i^2 + \mu\left(\sum_{i=1}^{b} v_i\right)^2 > 2,$$

as $k - \mu \geq 2$, and the assertion (i) follows from Proposition 2.5.

For the second assertion, let $\mathfrak{s}$ be a k-subset of $\mathcal{P} = \{P_1, \ldots, P_v\}$ such that the sum of (the images of) its elements is zero and let $\mathbf{w} = (w_1, \ldots, w_v) \in \mathbb{Z}^v = \mathfrak{G}$ be defined by $w_i = 1$, if $P_i \in \mathfrak{s}$, and $w_i = 0$, elsewhere. It suffices to prove that $\mathbf{w}$ is a row of A.

As the sum of the elements in $\mathfrak{s}$ is zero in $\mathfrak{G}_\mathcal{D} = \mathfrak{G}/\mathfrak{R}$, we deduce that $\mathbf{w} \in \mathfrak{R}$, hence there exists $\mathbf{u} = (u_1, \ldots, u_b) \in \mathbb{Z}^b$ such that $\mathbf{w} = \mathbf{u}A$. It follows that

$$k(u_1 + \ldots + u_b) = \mathbf{u}k(\underbrace{1, 1, \ldots, 1}_{b})' = \mathbf{u}A(\underbrace{1, 1, \ldots, 1}_{v})' = \mathbf{w}(\underbrace{1, 1, \ldots, 1}_{v})' = w_1 + \ldots + w_v = k,$$

whence $u_1 + \ldots + u_b = 1$. Finally,

$$k = \mathbf{w}\mathbf{w}' = \mathbf{u}AA'\mathbf{u}' = (k - \mu)\sum_{i=1}^{b} u_i^2 + \mu\left(\sum_{i=1}^{b} u_i\right)^2 = (k - \mu)\sum_{i=1}^{b} u_i^2 + \mu,$$

which forces $u_1^2 + \cdots + u_b^2 = 1$, hence $\mathbf{u}$ is a vector of the canonical basis and $\mathbf{w}$ is a row of A, that is, $\mathfrak{s}$ is a block of $\mathcal{B}$. □

4.2 Corollary: *With the only exception of the trivial* $2-(v, v-1, v-2)$ *design, each symmetric* $2-(v, k, \lambda)$ *design* $\mathcal{D} = (\mathcal{P}, \mathcal{B})$ *is additive, and its blocks are characterized as the only* k*-subsets of elements of* $\mathcal{P}$*, whose images add up to zero in* $\mathfrak{G}_\mathcal{D}$.

4.3 Corollary: *The group of automorphisms of a linked design* $\mathcal{D} = (\mathcal{P}, \mathcal{B})$*, not isomorphic to the trivial* $2-(v, v-1, v-2)$ *design, is the stabilizer of* $\mathcal{P}$ *in* $\mathrm{Aut}(\mathfrak{G}_\mathcal{D})$.

Proof. By Proposition 2.6, any automorphism f of an additive design $\mathcal{D}$ can be extended to a group automorphism $\widetilde{\mathfrak{f}}$ of $\mathfrak{G}_\mathcal{D}$. Conversely, let $\widetilde{\mathfrak{f}}$ be a group automorphism of $\mathfrak{G}_\mathcal{D}$ such that $\widetilde{\mathfrak{f}}(\chi(X)) = \chi(f(X))$ for all X in $\mathcal{P}$, where f is a permutation of $\mathcal{P}$. In particular, $\widetilde{\mathfrak{f}}$ induces a permutation of the set of k-tuples of $\chi(\mathcal{P})$ summing to zero. According to the above Theorem 4.1 (ii), if $\mathcal{D}$ is linked, then f is actually an automorphism of $\mathcal{D}$. □

4.4 Remark: Note that the property (ii) in Theorem 4.1 fails to hold when the Hadamard design considered in Example 2.3 is embedded in $(\mathbb{Z}/3\mathbb{Z})^4$, via the homomorphism defined by

$$(x_1, x_2, x_3, x_4, x_5) \mapsto (x_1, x_2, x_3 - x_4, x_5),$$

or in $(\mathbb{Z}/3\mathbb{Z})^3$, via

$$(x_1, x_2, x_3, x_4, x_5) \mapsto (x_1, x_2, x_3 - x_4).$$

In fact, distinct points of $\mathcal{P}$ are still mapped onto distinct points, and clearly blocks are again mapped onto 5-tuples of points summing to 0, but the 5-set $\{P_5, P_7, P_9, P_{10}, P_{11}\}$, which is not a block, is mapped in both cases onto a 5-set summing to 0 (even if, only in the first case, it happens to be the only such 5-set!).

This fact enlightens the distinguished rôle of the embedding χ.

The proof of the above Theorem 4.1 can be adapted in many *ad hoc* ways. Here we just show that, in the case of a symmetric design with $\gcd(r, \lambda) = 1$, one can consider the embeddings into the Sylow subgroups of $\mathfrak{G}_{\mathcal{D}}$.

4.5 Proposition: *Let $\mathcal{D}$ be a symmetric $2-(v, k, \lambda)$ design, let r and λ be relatively prime, and let $r - \lambda = st$, with $1 < s < t$. Then $X \mapsto s\chi(X)$ is injective, and, if* $\gcd(s,t) = 1$ *and t is square-free, then also $X \mapsto t\chi(X)$ is injective.*

Proof. If the map $X \mapsto s\chi(X)$ were not injective, then, arguing as in the proof of Proposition 2.5, there would exist a (non-zero) vector $\mathbf{v} = (v_1, \dots, v_b) \in \mathbb{Z}^b$ such that

$$\mathbf{v}AA'\mathbf{v}' = 2s^2,$$

whence

$$\begin{aligned} 2s^2 &= (r-\lambda)\sum v_i^2 + \lambda\big(\sum v_i\big)^2 \\ &= st\sum v_i^2 + \lambda\big(\sum v_i\big)^2 \\ &> s^2\sum v_i^2, \end{aligned}$$

since $1 < s < t$. Therefore $\sum v_i^2 = 1$, hence $\big(\sum v_i\big)^2 = 1$ and $2s^2 = st + \lambda$. Thus s would divide both λ and $r = \lambda + st$, against the hypothesis that $\gcd(r, \lambda) = 1$.

Now, assume that $\gcd(s,t) = 1$ and t is square-free. If the map $X \mapsto t\chi(X)$ were not injective, then, as above, there would exist a (non-zero) vector $\mathbf{v} = (v_1, \dots, v_b) \in \mathbb{Z}^b$ such that

$$\mathbf{v}AA'\mathbf{v}' = 2t^2,$$

that is, $2t^2 = (r-\lambda)\sum v_i^2 + \lambda\big(\sum v_i\big)^2 = st\sum v_i^2 + \lambda\big(\sum v_i\big)^2$. Since no prime divisor of t can divide λ, we conclude that t divides $\big(\sum v_i\big)^2$. As t is square-free, it divides $\sum v_i$. Moreover, t divides $\sum v_i^2$ as well, because $\gcd(s,t) = 1$, hence

$$2 = s\,\frac{\sum v_i^2}{t} + \lambda\left(\frac{\sum v_i}{t}\right)^2,$$

which forces $s = 2$, $t = \sum v_i^2$, and $\sum v_i = 0$. Therefore $t \equiv \sum v_i = 0 \pmod 2$, thereby contradicting the hypotesis that t and s are relatively prime. □

In the next theorem, we consider the case where the order $r - \lambda$ of a symmetric 2-design $\mathcal{D}$ is a prime p not dividing k, as it happens in Example 2.3. For an incidence matrix A of $\mathcal{D}$, it follows from the equality $A'A = (r-\lambda)I + \lambda J$ that $\det(A)^2 = \det\big((r-\lambda)I + \lambda J\big)$. By the Laplace expansion and by the basic equality $\lambda(v-1) = r(k-1)$, one finds, being $r = k$, that $\det(A)^2 = k^2(k-\lambda)^{v-1} = k^2p^{v-1}$, whence v is necessarily odd and $\det(A) = \pm kp^{\frac{v-1}{2}}$. Moreover, as we show independently in the following lemma, the p-rank of A is $\frac{v+1}{2}$ (see [8]), and, as we prove in the subsequent theorem, the group $\mathfrak{G}_{\mathcal{D}}$ can be determined by the parameters of the design.

4.6 Lemma: *Let $\mathcal{D} = (\mathcal{P}, \mathcal{B})$ be a symmetric $2-(v,k,\lambda)$ design of prime order $p = k - \lambda$ not dividing k, and let A be an incidence matrix for $\mathcal{D}$. Then the p-rank of $\mathcal{D}$ is equal to $\frac{v+1}{2}$ and, if the first $\frac{v+1}{2}$ columns of A are taken to be linearly independent (mod p), the Hermite normal form of A is*

$$N = \left(\begin{array}{c|c} I & -C_{\mathcal{P}} \\ \hline 0 & B \end{array}\right), \text{ where } B = \begin{pmatrix} p & 0 & 0 & \dots & 0 & kp-p \\ 0 & p & 0 & \dots & 0 & kp-p \\ & & & \vdots & & \\ 0 & 0 & \dots & 0 & p & kp-p \\ 0 & 0 & \dots & 0 & 0 & kp \end{pmatrix} \tag{6}$$

is a $\frac{v-1}{2} \times \frac{v-1}{2}$ matrix and $C_{\mathcal{P}}$ is a $\frac{v+1}{2} \times \frac{v-1}{2}$ matrix whose coefficients are non-positive integers.

The matrix $C_{\mathcal{P}}$, reduced modulo p, can be found, alternatively, as the unique solution of the equation

$$A \left(\frac{C_{\mathcal{P}}}{I}\right) \equiv \mathbf{0} \ (mod\ p). \tag{7}$$

Furthermore,

$$C'_{\mathcal{P}} C_{\mathcal{P}} \equiv -I \ (mod\ p). \tag{8}$$

Proof. Let A be an incidence matrix for $\mathcal{D}$, and let n be the p-rank of A. As we recalled earlier, $\det(A) = \pm kp^{\frac{v-1}{2}} \equiv 0 \pmod{p}$, hence $n < v$.

Assume that the the first n columns of A are linearly independent modulo p, and reduce the matrix A by elementary integer row operations to its unique Hermite normal form N. Note that, since $\det(A) \neq 0$, there exist precisely v (non-zero) pivots, all on the main diagonal of the square matrix N. Since in the Hermite normal form the sum of the entries in any row remains a multiple of k, which is not a multiple of p, and since $\det(A) = \pm kp^{\frac{v-1}{2}}$, the last pivot must be kp^m, for some exponent $m \geq 0$. On the other hand, $kp\chi(X) = 0$ for any X in $\mathcal{P}$, by Theorem 2.2 (*iii*), thus the last pivot is equal to either k or kp, and all the other ones are p-powers. Also, the upper-left $n \times n$ minor of N has p-rank equal to n (all the entries below such a minor being zero), thus it contains n pivots all equal to $p^0 = 1$. By definition of Hermite normal form, it follows that the left $v \times n$ minor N_1 of N is of the form $\left(\frac{I}{0}\right)$, where I is the $n \times n$ identity matrix. Moreover, since the p-rank of N is equal to n, there are no other pivots equal to 1 in N, thus all the remaining pivots, but the last one, are a power of p with positive exponent.

We now claim that the last pivot in N is equal to kp. Indeed, if the last pivot were equal to k and the second to last pivot were equal to p^s, $s \geq 1$, then, since p does not divide k, a standard argument, together with a permutation of the last two columns and, possibly, of the last two rows (which would not alter N_1), would reduce the last and second to last pivots to kp^s and 1, respectively, thereby exceeding the number of possible pivots equal to 1. Therefore the last pivot in N is equal to kp.

The same kind of argument shows that all the pivots bigger than 1, but the last one, are equal to p. Indeed, if one of the pivots were equal to p^s, $s \geq 2$, then, up to a permutation of the last $v - n$ columns and a permutation of the last $v - n$ rows, one could reduce the last pivot to kp^t, for some $t \geq 2$, which would contradict the fact that $kp\chi(X) = 0$ for any X in $\mathcal{P}$, by Theorem 2.2 (*iii*). Since $\det(A) = \pm kp^{\frac{v-1}{2}}$, we may now conclude that, the last pivot being equal to kp, there are precisely $\frac{v-3}{2}$ pivots equal to p, whence there are $n = \frac{v+1}{2}$ pivots equal to 1 (that is, the p-rank of A is equal to $\frac{v+1}{2}$).

By the same kind of standard arguments, and since the sum of the entries in any row of N is a multiple of k, one can show that the lower right $\frac{v-1}{2} \times \frac{v-1}{2}$ minor of N has the form B described in the statement of the lemma. Hence, by definition of Hermite normal form, there exists a $\frac{v+1}{2} \times \frac{v-1}{2}$ matrix $C_{\mathcal{P}}$, whose coefficients are non-positive integers, such that N has the described form.

Let $H \in \mathbb{Z}^{v \times v}$ be the unimodular matrix of the reduction of A to its Hermite normal form, that is, $HA = N$. Since $\det(H) = \pm 1$, from $HA \left(\begin{smallmatrix} C_{\mathcal{P}} \\ I \end{smallmatrix}\right) = \left(\begin{array}{c|c} I & -C_{\mathcal{P}} \\ \hline 0 & B \end{array}\right) \left(\begin{smallmatrix} C_{\mathcal{P}} \\ I \end{smallmatrix}\right) \equiv \mathbf{0} \pmod{p}$ it follows that $A \left(\begin{smallmatrix} C_{\mathcal{P}} \\ I \end{smallmatrix}\right) \equiv \mathbf{0} \pmod{p}$.

Let $M = (M_1|M_2)$ be a $\frac{v+1}{2} \times v$ minor of A such that M_1 has $\frac{v+1}{2}$ columns and is invertible $(\bmod\ p)$. It follows from (7) that $M_1 C_{\mathcal{P}} + M_2 \equiv \mathbf{0} \pmod{p}$ and, finally, $C_{\mathcal{P}} \equiv -M_1^{-1} M_2 \pmod{p}$. This shows that the matrix $C_{\mathcal{P}}$, reduced modulo p, is the unique solution of the equation (7), as claimed.

Let $K \in \mathbb{Z}^{\frac{v+1}{2} \times v}$ be the minor consisting of the first $\frac{v+1}{2}$ rows of H, that is, $KA = (I|-C_{\mathcal{P}})$. Let $\mathbb{F}$ be the splitting field of $x^2 + \lambda$ over $\mathrm{GF}(p)$ (hence either a trivial or a quadratic extension of $\mathrm{GF}(p)$), and let $\mathbf{u} = \sqrt{-\lambda}\,(1, 1, \ldots, 1)K' \in \mathbb{F}^{\frac{v+1}{2}}$, where the coefficients of K, reduced modulo p, are taken in $\mathrm{GF}(p) \subseteq \mathbb{F}$. Since $AA' = (k - \lambda)I + \lambda J$,

$$I + C_{\mathcal{P}} C'_{\mathcal{P}} = KAA'K' = K((k - \lambda)I + \lambda J)K' \equiv \lambda KJK' \equiv -\mathbf{u}'\mathbf{u} \pmod{p},$$

and, if one sets $R = (C_{\mathcal{P}}|\mathbf{u}') \in \mathbb{F}^{\frac{v+1}{2} \times \frac{v+1}{2}}$ (where the coefficients of $C_{\mathcal{P}}$, reduced modulo p, are taken in $\mathrm{GF}(p) \subseteq \mathbb{F}$), then $RR' = C_{\mathcal{P}} C'_{\mathcal{P}} + \mathbf{u}'\mathbf{u} \equiv -I \pmod{p}$. Hence the matrix R' is the inverse of the opposite of R in $\mathbb{F}^{\frac{v+1}{2} \times \frac{v+1}{2}}$, thus, $R'R = -I$ in $\mathbb{F}^{\frac{v+1}{2} \times \frac{v+1}{2}}$ as well, and, in particular, $C'_{\mathcal{P}} C_{\mathcal{P}} \equiv -I \pmod{p}$, so the last assertion is proved. □

4.7 Remark: It will be shown in Theorem 4.8 that the columns of the $\frac{v-1}{2} \times v$ matrix $(C'_{\mathcal{P}}|I)$ are the coordinates of the points $P_1, \ldots, P_v$ in $\mathfrak{G}_{\mathcal{D}}$. It is worth stressing here that the equality (7) also means that $(C'_{\mathcal{P}}|I)$, which has maximal rank, is the parity-check matrix of the code $\mathcal{C}_A$ generated over $\mathrm{GF}(p)$ by the rows of A (whose dimension is the p-rank of A, i.e., $\frac{v+1}{2}$), as well as, by (6), by the rows of $KA = (I| - C_{\mathcal{P}})$. Thus, the matrix $C_{\mathcal{P}}$, which, together with the identity matrix, gives the coordinates of the points of $\mathcal{P}$, appears, for the code $\mathcal{C}_A$, both in its parity-check matrix and in its generator matrix! Furthermore, the equality (8) means that the dual code $\mathcal{C}_A^{\perp}$ of $\mathcal{C}_A$ (that is, the code generated by the rows of $(C'_{\mathcal{P}}|I)$) is self-orthogonal.

In the case of the $2-(11, 5, 2)$ Hadamard design in Example 2.3, the matrix $(C'_{\mathcal{P}}|I)$ is the 5×11 matrix whose columns are the coordinates of $P_1, \ldots, P_{11}$, which happens to be precisely the parity-check matrix of the ternary Golay code (see [9], where the matrix S_5, modified by cancelling the column $(0, 1, 1, 1, 1, 1)'$ and permuting rows and columns, gives the 6×5 matrix whose rows are the coordinates of our points $P_1, \ldots, P_6$). The ternary Golay code, on the other hand, may be defined as the subspace generated by the rows of A over the field with 3 elements, and the matrix $KA = (I| - C_{\mathcal{P}})$ over $\mathrm{GF}(3)$ is a generator matrix for the code.

4.8 Theorem: *If $\mathcal{D} = (\mathcal{P}, \mathcal{B})$ is a symmetric $2-(v, k, \lambda)$ design of prime order $p = k - \lambda$ not dividing k, then (the p-rank of $\mathcal{D}$ is equal to $\frac{v+1}{2}$ and) the group $\mathfrak{G}_{\mathcal{D}}$ is isomorphic to $\mathbb{Z}/k\mathbb{Z} \oplus (\mathbb{Z}/p\mathbb{Z})^{\frac{v-1}{2}}$.*

Moreover, for any incidence matrix A for $\mathcal{D}$, whose first $\frac{v+1}{2}$ columns are taken to be linearly independent (mod p), and disregarding the first component, constantly equal to $1 \in \mathbb{Z}/k\mathbb{Z}$:

(i) the last $\frac{v-1}{2}$ points of $\mathcal{P}$ are mapped by χ onto

$$P_{\frac{v+3}{2}} = (1, \dots, 0, 0), \dots, P_{v-1} = (0, \dots, 1, 0), P_v = (0, \dots, 0, 1) \in (\mathbb{Z}/p\mathbb{Z})^{\frac{v-1}{2}},$$

and the first $\frac{v+1}{2}$ points are mapped onto the rows (mod p) $P_1, \dots, P_{\frac{v+1}{2}}$ of the $\frac{v+1}{2} \times \frac{v-1}{2}$ matrix $C_{\mathcal{P}}$ such that $-C_{\mathcal{P}}$ is precisely the upper-right $\frac{v+1}{2} \times \frac{v-1}{2}$ minor of the Hermite normal form of A.

(ii) if $J - A = (\Xi_1|\Xi_2)$, where J is the all-1 matrix, and Ξ_1 and Ξ_2 are, respectively, the minors consisting of the first $\frac{v+1}{2}$ and the last $\frac{v-1}{2}$ columns, then the blocks of $\mathcal{B}$ can be characterized as the v intersections of $\chi(\mathcal{P}) = \{P_1, \dots, P_{\frac{v+1}{2}}, P_{\frac{v+3}{2}}, \dots, P_v\}$ with the v hyperplanes of $(\mathbb{Z}/p\mathbb{Z})^{\frac{v-1}{2}}$ defined by the v equations of the linear system

$$\Xi_2(x_1, \dots, x_{\frac{v-1}{2}})' \equiv \mathbf{0} \ (mod\ p).$$

Proof. Let A be an incidence matrix for $\mathcal{D}$, whose first $\frac{v+1}{2}$ columns are taken to be linearly independent (mod p). Reduce A by elementary integer row operations to its unique Hermite normal form N, as in the above Lemma 4.6. One sees from the matrix B defined in (6) that the group $\mathfrak{G}_{\mathcal{D}}$ is isomorphic to $\mathbb{Z}/k\mathbb{Z} \oplus (\mathbb{Z}/p\mathbb{Z})^{\frac{v-1}{2}}$, and, denoting by $P_{\frac{v+3}{2}}, \dots, P_{v-1}, P_v$ the images under χ of the last $\frac{v-1}{2}$ points of $\mathcal{P}$, that $kpP_v = 0$ and $pP_i = pP_v$, for any $i = \frac{v+3}{2}, \dots, v-1$. Since p is invertible modulo k, the first entry of P_i, lying in $\mathbb{Z}/k\mathbb{Z}$, is constant for all $i = \frac{v+3}{2}, \dots, v$. Hence one can assume that the last $\frac{v-1}{2}$ points of $\mathcal{P}$ are mapped onto

$$P_{\frac{v+3}{2}} = (1; 1, \dots, 0, 0), \dots, P_{v-1} = (1; 0, \dots, 1, 0), P_v = (1; 0, \dots, 0, 1).$$

The first entry, lying in $\mathbb{Z}/k\mathbb{Z}$, is constant and will not be considered here, hence we take $P_{\frac{v+3}{2}}, \dots,$ P_v in $(\mathbb{Z}/p\mathbb{Z})^{\frac{v-1}{2}}$. Similarly, again by (6), the first $\frac{v+1}{2}$ points of $\mathcal{P}$ are mapped onto the $\frac{v+1}{2}$ rows of $C_{\mathcal{P}}$ (reduced modulo p).

Finally, let $J - A = (\Xi_1|\Xi_2)$, as in the claim (*ii*). Let $H \in \mathbb{Z}^{v \times v}$ be the unimodular matrix of the reduction of A to its Hermite normal form, that is, $HA = N$, and let $K \in \mathbb{Z}^{\frac{v+1}{2} \times v}$ be the minor consisting of the first $\frac{v+1}{2}$ rows of H, hence $KA = (I|-C_{\mathcal{P}})$. Notice that $AJ = kJ$, thus, since $AA' = (k-\lambda)I + \lambda J$,

$$-KA \begin{pmatrix} \Xi_1' \\ \hline \Xi_2' \end{pmatrix} = KA(A' - J) = K\big((k-\lambda)I + \lambda J - kJ\big) = K(k-\lambda)(I - J) \equiv 0 \ (\mathrm{mod}\ p).$$

On the other hand, $KA = (I|-C_{\mathcal{P}})$, hence $\Xi_1' - C_{\mathcal{P}}\Xi_2' \equiv 0$ (mod p), thus

$$\Xi_2(C_{\mathcal{P}}'|I) \equiv (\Xi_1|\Xi_2) = J - A \ (\mathrm{mod}\ p), \tag{9}$$

that is, if r_i is the i-th row of Ξ_2, for $1 \le i \le v$, then the products $r_i(x_1, \dots, x_{\frac{v-1}{2}})'$, as $P = (x_1, \dots, x_{\frac{v-1}{2}})$ ranges in $\chi(\mathcal{P})$, give the i-th row of $J - A$ (mod p), hence $r_i(x_1, \dots, x_{\frac{v-1}{2}})' \equiv 0$ (mod p) if and only if $(x_1, \dots, x_{\frac{v-1}{2}})$ belongs to the i-th block of $\mathcal{D}$, as claimed. □

4.9 Remark: The v columns of the matrix $(C'_{\mathcal{P}}|I)$, or equivalently the rows of $\binom{C_{\mathcal{P}}}{I}$, taken modulo p, are the elements of the set $\chi(\mathcal{P}) = \{P_1, \ldots, P_v\}$. Since, by (9), the v columns of $(C'_{\mathcal{P}}|I)$ are all distinct (mod p), the proof of the theorem above also confirms that $\mathcal{D}$ is an additive design (see Corollary 4.2). Moreover, the equality $A\binom{C_{\mathcal{P}}}{I} \equiv \mathbf{0}$ (mod p) in (7) is precisely equivalent to the fact that $\sum_{X\in\mathfrak{b}} \chi(X) = 0$ in $\mathfrak{G}_{\mathcal{D}}$ for any block $\mathfrak{b}$ in $\mathcal{B}$.

4.10 Remark: The modular equality (9) shows that the p-rank of $J-A$ is *at most* the p-rank of $(C'_{\mathcal{P}}|I)$, that is, $\frac{v-1}{2}$. On the other hand, it is easy to see that $K(J-A) = KJ-(I|-C_{\mathcal{P}})$ has rank *at least* $\frac{v-1}{2}$, because KJ has rank equal to 1, hence the elementary row operations that reduce KJ to a matrix with a unique non-zero row change the first $\frac{v+1}{2}$ columns of $(I|-C_{\mathcal{P}})$ in such a way that $KJ-(I|-C_{\mathcal{P}})$ is transformed in a matrix that still has a $\frac{v-1}{2} \times \frac{v-1}{2}$ minor equal to the identity matrix. Thus, the p-rank of $J-A$ is $\frac{v-1}{2}$, and we can complete Remark 4.7 by claiming that $(J-A)'$ is also a parity-check matrix for the code generated over GF(p) by the rows of A, since $A(J-A)' = kJ-(k-\lambda)I-\lambda J \equiv \mathbf{0}$ (mod p).

Throughout the rest of the paper we illustrate the main results of this section by applying them to our example of the $2-(11,5,2)$ Hadamard design.

4.11 Example: Let $\mathcal{D} = (\mathcal{P},\mathcal{B})$ be the $2-(11,5,2)$ Hadamard design considered in Example 2.3, which is the second smallest symmetric design. Hence $\mathcal{D}$ is additive by Corollary 4.2, and, in fact, in Example 2.3 we found that the images under χ of the points of $\mathcal{P}$ in $\mathfrak{G}_{\mathcal{D}} = \mathbb{Z}/5\mathbb{Z} \oplus (\mathbb{Z}/3\mathbb{Z})^5$ are:

$$\begin{array}{lll}
P_1 = (1;1,2,2,1,0) & P_2 = (1;2,1,2,0,1) & P_3 = (1;0,2,1,2,1) \\
P_4 = (1;1,1,0,2,2) & P_5 = (1;2,0,1,1,2) & P_6 = (1;2,2,2,2,2) \\
P_7 = (1;1,0,0,0,0) & P_8 = (1;0,1,0,0,0) & P_9 = (1;0,0,1,0,0) \\
P_{10} = (1;0,0,0,1,0) & P_{11} = (1;0,0,0,0,1). &
\end{array}$$

Again by Corollary 4.2, the eleven blocks of $\mathcal{B}$ are the only 5-tuples of points in $\{P_1, \ldots, P_{11}\}$ whose sum is zero. If A is the incidence matrix given in Example 2.3, then, by Theorem 4.8 (*ii*), the last 5 columns of $J-A$ yield the following equations for the blocks, which consist of the points $(1;x_1,x_2,x_3,x_4,x_5)$ of $\chi(\mathcal{P})$ in the following hyperplanes of $(\mathbb{Z}/3\mathbb{Z})^5$, taken in the same ordering as the rows of $J-A$:

$$\begin{array}{lll}
\mathfrak{b}_1 : x_1+x_2+x_3+x_4+x_5 = 0 & \mathfrak{b}_2 : x_3+x_4+x_5 = 0 & \mathfrak{b}_3 : x_1+x_2+x_5 = 0 \\
\mathfrak{b}_4 : x_2+x_4 = 0 & \mathfrak{b}_5 : x_1+x_3 = 0 & \mathfrak{b}_6 : x_2+x_3 = 0 \\
\mathfrak{b}_7 : x_1+x_5 = 0 & \mathfrak{b}_8 : x_1+x_2+x_4 = 0 & \mathfrak{b}_9 : x_1+x_3+x_4 = 0 \\
\mathfrak{b}_{10} : x_4+x_5 = 0 & \mathfrak{b}_{11} : x_2+x_3+x_5 = 0. &
\end{array}$$

Finally, observe that $\chi(\mathcal{P})$ is not contained in any affine hyperplane of $(\mathbb{Z}/3\mathbb{Z})^5$. This makes this case thoroughly different from that of additive Steiner triple systems (see Remark 3.8 (*b*)).

4.12 Remark: One of the consequences of Theorem 4.8 is that the number of blocks that completely determine the design is equal at most to the p-rank of $\mathcal{D}$ (that is, $\frac{v+1}{2}$). More precisely, for a symmetric $2-(v,k,\lambda)$ design $\mathcal{D} = (\mathcal{P},\mathcal{B})$ of order $k-\lambda = p$ (p a prime not dividing k), any $\frac{v+1}{2}$ blocks, such that the corresponding $\frac{v+1}{2} \times v$ minor of an incidence matrix of $\mathcal{D}$ has p-rank equal to $\frac{v+1}{2}$, are sufficient to uniquely determine $\mathcal{D}$.

We illustrate this by the following argument, which gives an alternative proof of the fact that there exists only one $2-(11,5,2)$ Hadamard design. In fact, for any such a design we can straightaway assume, by adopting the reverse lexicographical order, that the first 5 rows of the incidence matrix are

$$\begin{array}{|c|cccc|ccc|cc|c|}
1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ \cline{2-5}
1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ \cline{6-8}
1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 \\ \cline{9-10}
1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 1 \\ \cline{11-11}
1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1
\end{array}\,,$$

because the scalar product of any two different rows of an incidence matrix is equal to 2 and any two points lie in precisely two blocks. The next row is also uniquely determined as

$$\left(\begin{array}{c|cccc|ccc|cc|c} 0 & 1 & 1 & 0 & 0 & a & b & c & d & e & f \end{array}\right),$$

where, forced again by the scalar product, there are two entries equal to 1 in $\{b,d,f\}$, two in $\{c,e,f\}$, one in $\{a,b,c\}$, and one in $\{a,d,e\}$. This gives two possibilities: $a=c=d=0$ and $b=e=f=1$, or $a=b=e=0$ and $c=d=f=1$, that is, the row is one of the following:

$$\left(\begin{array}{c|cccc|ccc|cc|c} 0 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 \end{array}\right),$$

$$\left(\begin{array}{c|cccc|ccc|cc|c} 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{array}\right).$$

But the second choice can be reduced to the first one by interchanging $P_7 \leftrightarrow P_8$ and $P_9 \leftrightarrow P_{10}$ (and $\mathfrak{b}_4 \leftrightarrow \mathfrak{b}_5$ and $P_4 \leftrightarrow P_5$). Thus, with the reverse lexicographical order, the sixth row is $\begin{pmatrix} 0 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 \end{pmatrix}$. By equation (7) in Lemma 4.6, this choice of the first 6 rows of $A = \left(\begin{array}{c|c} A_{11} & A_{12} \\ \hline A_{21} & A_{22} \end{array}\right)$ gives

$$C_{\mathcal{P}} = -A_{11}^{-1}A_{12} = -\begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 \end{pmatrix}^{-1} \begin{pmatrix} 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 & 1 \end{pmatrix} \equiv \begin{pmatrix} 1 & 2 & 2 & 1 & 0 \\ 2 & 1 & 2 & 0 & 1 \\ 0 & 2 & 1 & 2 & 1 \\ 1 & 1 & 0 & 2 & 2 \\ 2 & 0 & 1 & 1 & 2 \\ 2 & 2 & 2 & 2 & 2 \end{pmatrix} \pmod 3,$$

the rows of which, together with the 5 vectors of the canonical basis of $(\mathbb{Z}/3\mathbb{Z})^5$, are, according to Theorem 4.8 (*i*), the points of a unique $2-(11,5,2)$ Hadamard design, whose blocks are, by Theorem 4.1 (*ii*), the eleven 5-subsets of points summing up to zero.

4.13 Remark: According to Corollary 4.3, the automorphism group of the Hadamard $2-(11,5,2)$ design $\mathcal{D}$, represented in the Example 4.11, is isomorphic to the subgroup of $\mathrm{GL}_5(3)$ consisting of the matrices F that permute the eleven points $P_1,\dots,P_{11}$ in $(\mathbb{Z}/3\mathbb{Z})^5$.

Here we illustrate the usefulness of this characterization by giving an alternative proof that this group is isomorphic to $\mathrm{PSL}_2(11)$ and 2-transitive on $\mathcal{P}$ (cf. [2, Th. 7.10, p. 266; Th. 7.14, p. 268]).

Every automorphism ϕ of $\mathcal{D}$, as a linear map on $(\mathbb{Z}/3\mathbb{Z})^5$, is uniquely determined by the values it takes on the five points $P_7,\dots,P_{11}$ of the canonical basis, but, as we will now show, $\phi(P_9)$ is already determined by the values ϕ takes on the other four points.

Indeed, let us set $Y_7 = \phi(P_7)$ and $Y_8 = \phi(P_8)$. Since P_7 and P_8 are incident with two blocks ($\mathfrak{b}_2$ and $\mathfrak{b}_{10}$) that leave P_4, P_{10}, and P_{11} off, the triple $\{P_4, P_{10}, P_{11}\}$ is mapped by ϕ onto the triple left off the two blocks through Y_7 and Y_8. In particular, the point $Y_4 = \phi(P_4)$ is uniquely determined by the points $Y_{10} = \phi(P_{10})$ and $Y_{11} = \phi(P_{11})$. Finally, the point $Y_9 = \phi(P_9)$ is determined, in turn, by Y_4, as it is uniquely found by looking at the images of the blocks $\mathfrak{b}_4 = \{P_1, P_4, P_7, P_9, P_{11}\}$ and $\mathfrak{b}_7 = \{P_2, P_4, P_8, P_9, P_{10}\}$, which intersect in $\{P_4, P_9\}$, and this proves our claim.

By construction, the ordered quadruple $(Y_7, Y_8, Y_{10}, Y_{11})$ can run through at most $11 \times 10 \times 3 \times 2$ ordered quadruples. Thus there exist at most 660 automorphisms of $\mathcal{D}$. We now want to show that $\mathcal{D}$ has exactly 660 automorphisms.

By choosing $(Y_7, Y_8, Y_{10}, Y_{11}) = (P_4, P_{11}, P_2, P_5)$ (and, consequently, $Y_4 = P_{10}$ and $Y_9 = P_7$), the corresponding linear map ϕ_1, represented by the matrix F_1 below (where, as is customary, we put the images $Y_7, \ldots, Y_{11}$ in columns), can be checked to actually induce a cyclic permutation of the eleven points $P_1, \ldots, P_{11}$, hence ϕ_1 is an automorphism of $\mathcal{D}$ of order 11. Similarly, the choice $(Y_7, Y_8, Y_{10}, Y_{11}) = (P_3, P_9, P_2, P_{11})$ (and, consequently, $Y_4 = P_4$ and $Y_9 = P_8$) induces an automorphism ϕ_2 of order 2, represented by the matrix F_2 below

$$F_1 = \begin{pmatrix} 1 & 0 & 1 & 2 & 2 \\ 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 2 & 1 \\ 2 & 0 & 0 & 0 & 1 \\ 2 & 1 & 0 & 1 & 2 \end{pmatrix}, \quad F_2 = \begin{pmatrix} 0 & 0 & 0 & 2 & 0 \\ 2 & 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 2 & 0 \\ 2 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 \end{pmatrix} \in \mathrm{GL}_5(3).$$

A direct computation shows that $F_1^{11} = F_2^2 = (F_1F_2)^3 = (F_1^6F_2F_1^4F_2)^2 = 1$. Since

$$\langle \phi_1, \phi_2 : \phi_1^{11} = \phi_2^2 = (\phi_1\phi_2)^3 = (\phi_1^6\phi_2\phi_1^4\phi_2)^2 = 1 \rangle$$

is a presentation of the (simple) group $\mathrm{PSL}_2(11)$ (cf. [12]), which has cardinality 660, we deduce that the group $\mathrm{Aut}(\mathcal{D})$ is isomorphic to $\mathrm{PSL}_2(11)$, has 660 elements, is 2-transitive on $\mathcal{P}$, and operates on $\mathcal{P}$ as the group of matrices generated by F_1 and F_2.

Note, in passing, that by construction of the matrices F_1 and F_2, and by Theorem 4.1 (*ii*), the eleven 5-tuples $P_1, \ldots, P_{11}$ in $(\mathbb{Z}/3\mathbb{Z})^5$ ultimately describe the points, the blocks and the automorphisms of the design!

References

[1] E. F. Assmus, J. D. Key, *Designs and Their Codes*, Cambridge University Press (1994).

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

[3] A. Caggegi, G. Falcone, M. Pavone, Additivity of affine designs, submitted.

[4] C. J. Colbourn, A. Rosa, *Triple Systems*, Oxford Science Publications, Oxford (1999).

[5] J. Doyen, X. Hubaut, M. Vandensavel, Ranks of incidence matrices of Steiner triple systems, Math. Z. 163, pp. 251-259 (1978).

[6] G. Falcone, M. Pavone, Kirkman's Tetrahedron and the Fifteen Schoolgirl Problem, Amer. Math. Month. 118 (10), pp. 887-900 (2011).

[7] N. Hamada, On the p-rank of the incidence matrix of a balanced or partially balanced incomplete block design and its applications to error correcting codes, Hiroshima Math. J. 3 (1), pp. 153-226 (1973).

[8] M. Klemm, Über den p-Rang von Inzidenzmatrizen, J. Comb. Th. (A) 43, pp. 138-139 (1986).

[9] V. Pless, Symmetry codes over GF(3) and new five-designs, J. Comb. Th. (A) 12, pp. 119-142 (1972).

[10] J. Röhmel, Über die Existenz von Inzidenzstrukturen mit Regularitätsbedingungen, Math. Z. 133, pp. 203-218 (1973).

[11] H. J. Ryser, A note on a combinatorial problem, Proc. Amer. Math. Soc. 1, pp. 422-424 (1950).

[12] J. G. Sunday, Presentations of the groups $\mathrm{SL}(2, m)$ and $\mathrm{PSL}(2, m)$, Can. J. Math. 24 (6), pp. 1129-1131 (1972).