Research Article

Giovanni Falcone* and Marco Pavone

Permutations of zero-sumsets in a finite vector space

https://doi.org/10.1515/forum-2019-0228
Received August 21, 2019; revised June 26, 2020

Abstract: In this paper, we consider a finite-dimensional vector space $\mathcal{P}$ over the Galois field GF(p), with p being an odd prime, and the family $\mathcal{B}_k^x$ of all k-sets of elements of $\mathcal{P}$ summing up to a given element x. The main result of the paper is the characterization, for $x = 0$, of the permutations of $\mathcal{P}$ inducing permutations of $\mathcal{B}_k^0$ as the invertible linear mappings of the vector space $\mathcal{P}$ if p does not divide k, and as the invertible affinities of the affine space $\mathcal{P}$ if p divides k. The same question is answered also in the case where the elements of the k-sets are required to be all nonzero, and, in fact, the two cases prove to be intrinsically inseparable.

Keywords: Subset sums, subset sum problem, permutations of zero-sums

MSC 2010: Primary 11P70, 11B75; secondary 11B13, 05A18

Communicated by: Manfred Droste

1 Introduction

Let p be an odd prime. We recall that a set $\mathcal{P}$ of cardinality p^d, $d \geq 1$, can be endowed with the structure of a d-dimensional vector space over the prime field GF(p) as well as with the structure of a Galois field GF(p^d). In the latter case, $\mathcal{P}^* = \mathcal{P} \setminus \{0\}$ is the multiplicative group of $\mathcal{P}$. For such a finite vector space $\mathcal{P}$ and for any $k = 1, \dots, p^d$, we consider the natural partition of the family of all $\binom{p^d}{k}$ k-subsets of $\mathcal{P}$ as the disjoint union, as x ranges in $\mathcal{P}$, of the families $\mathcal{B}_k^x$ of all k-sets of elements adding up to x in $\mathcal{P}$. Similarly, we consider the partition of the family of all $\binom{p^d-1}{k}$ k-subsets of $\mathcal{P}^*$ as the disjoint union, as x ranges in $\mathcal{P}$, of the families $\mathcal{B}_k^{x,*}$ of all k-sets of elements adding up to x in $\mathcal{P}^*$.

The elements of the families $\mathcal{B}_k^x$ and $\mathcal{B}_k^{x,*}$ are precisely the solutions of two instances of the *subset sum problem* over finite fields, a well-known NP-complete problem, which arises from a number of relevant applications in Combinatorics, Coding Theory, Cryptography, and Graph Theory. The cardinalities of $\mathcal{B}_k^x$ and $\mathcal{B}_k^{x,*}$ were computed in closed form in two well-known papers by Li and Wan [6, 7], which have started an ongoing production at the crossroads of Additive Combinatorics, Additive Number Theory and Coding Theory.

In Section 2, we recall the cardinalities of the families $\mathcal{B}_k^x$ and $\mathcal{B}_k^{x,*}$, and of the subfamilies $\mathcal{B}_k^x(y)$ and $\mathcal{B}_k^{x,*}(y)$ consisting of all k-sets in $\mathcal{B}_k^x$ and $\mathcal{B}_k^{x,*}$, respectively, that contain a given element y, proving that such cardinalities are always nonzero, but for some trivial cases. Note that, in some of the above applications, settling whether this is true is even more meaningful than computing them explicitly. Also, unlike in the usual instances of *zero-sum problems* (see e.g. [8, 10]), in this context the k elements are required to be pairwise distinct, that is, multisets are not considered, which leads to a significant combinatorial difficulty.

***Corresponding author: Giovanni Falcone,** Dipartimento di Matematica e Informatica, Università degli Studi di Palermo, Via Archirafi 34, 90123 Palermo, Italy, e-mail: giovanni.falcone@unipa.it. https://orcid.org/0000-0002-5210-5416
Marco Pavone, Dipartimento di Ingegneria, Università degli Studi di Palermo, Viale delle Scienze, 90128 Palermo, Italy, e-mail: marco.pavone@unipa.it. https://orcid.org/0000-0002-8674-5841

A natural question to ask is: what are the permutations of $\mathcal{P}$ (respectively of $\mathcal{P}^*$) that, for a given k, induce permutations of the family $\mathcal{B}_k^0$ (respectively of $\mathcal{B}_k^{0,*}$) of all k-sets of elements adding up to 0? In Theorem 3.5, we prove that the only such permutations of $\mathcal{P}$ are the invertible linear mappings of the vector space $\mathcal{P}$ over GF(p) if p does not divide k, and the invertible affinities of the affine space $\mathcal{P}$ over its ground field GF(p) if p divides k. Also, in Theorem 3.2 we prove that the only such permutations of $\mathcal{P}^*$ are (the restrictions to $\mathcal{P}^*$ of) the invertible linear mappings of $\mathcal{P}$ over GF(p).

Besides their intrinsic combinatorial interest, zero-sum subsets occur in a natural manner when one considers the affine subspaces of a fixed dimension of a d-dimensional affine geometry AG(d, p) over GF(p), and, in fact, we came to the present questions when we investigated the 2-(v, k, λ) block designs that can be embedded in a finite abelian group in such a way that the blocks are zero-sum subsets [2, 3]. For a general treatment of block designs, see for instance [1, 4]. In this setting, our characterization, for p dividing k, of the permutations of $\mathcal{P}$ that induce permutations of $\mathcal{B}_k^0$ (Theorem 3.5) as the invertible affinities of the affine space $\mathcal{P}$, over its ground field GF(p), can be seen as an analogue of the fundamental theorem of affine geometry.

One of our present projects is to establish under what conditions on k and x the families $\mathcal{B}_k^x$ and $\mathcal{B}_k^x(y)$ represent the blocks and the blocks through the point y of a 2-design $\mathcal{D} = (\mathcal{P}, \mathcal{B}_k^x)$, respectively [9]. Another question to investigate is the characterization, in the case where $x \neq 0$, of the permutations of $\mathcal{P}$ that induce permutations of the family $\mathcal{B}_k^x$ of all k-sets of elements adding up to x. One may restrict oneself only to the case where p divides k, the other case being trivial (Remark 3.6). In such a case, the permutations of $\mathcal{P}$ that induce permutations of $\mathcal{B}_k^x$ form precisely, from this different viewpoint, the automorphism group of the block design. Also, for $x = 0$, $\mathcal{D}$ would be a sort of *universal* design for many of the designs considered in [3]. The same questions may be asked for $\mathcal{P}^*$, $\mathcal{B}_k^{x,*}$ and $\mathcal{B}_k^{x,*}(y)$.

Moreover, we believe that a further line of research could be found within the frame of Coding theory, also via the use of Assmus–Mattson-type results. Indeed, the family $\mathcal{B}_k^{0,*}$ of the k-sets of nonzero elements summing up to zero can be related to the family $\mathcal{W}_k$ of the codewords of weight k in any p-ary $(n, n-d, \delta)$ linear code $\mathcal{C} = \{w \in \mathrm{GF}(p)^n : Hw' = 0'\}$ defined by a $d \times n$ parity-check matrix H with pairwise linearly independent columns (that is, with $\delta > 2$), and, in particular, it is clear that $|\mathcal{W}_k| \leq |\mathcal{B}_k^{0,*}|$ for all possible weights k. Among these codes, one finds the

$$\left(\frac{p^d-1}{p-1}, \frac{p^d-1}{p-1} - d, 3\right)$$

p-ary Hamming codes ($p \geq 2$ being a prime), and, for $p = 2$, $|\mathcal{W}_k| = |\mathcal{B}_k^{0,*}|$ for all possible weights k. For p odd, it can be easily shown that the equality holds if and only if $p \in \{3, 5\}$ and $k = 3$. It is interesting to ask whether relations between the two parameters can be found also in the general case of the above p-ary $(n, n-d, \delta)$ linear codes.

Finally, the question on the permutations of zero-sumsets can be posed in the more general case where $\mathcal{P}$ is an arbitrary finite abelian group.

2 Subset sums in a finite vector space

Throughout the paper, we will denote by p an odd prime number and by $\mathcal{P}$ a d-dimensional vector space, $d \geq 1$, over a field with p elements. Also, let $\mathcal{P}^* = \mathcal{P} \setminus \{0\}$. Given an integer $1 \leq k \leq p^d$, the following questions arise: how many k-subsets of $\mathcal{P}$ (or of $\mathcal{P}^*$) are such that their elements sum up to a given element b in $\mathcal{P}$? In other words, how many solutions of the equation

$$x_1 + \cdots + x_k = b \tag{2.1}$$

are such that $x_i \neq x_j$ for all $i \neq j$? And how many of these k-subsets contain a given element a in $\mathcal{P}$ (respectively in $\mathcal{P}^*$)? The answer to the first question was first given in a celebrated result by Li and Wan [6, 7], which we will include below as Theorem 2.4 (cf. [5] for an alternative proof). The answer to the second question, in the case of k-subsets of $\mathcal{P}^*$, can be found as well in [6], although in an implicit form.

In this section, we recall the formulas in closed form for all coefficients introduced in the following Definition 2.1, which turn out to be all nonzero, except in the trivial cases described in the subsequent Theorem 2.2, which requires some technical adroitness we cannot dispense the reader of.

Definition 2.1. Let x be an element of $\mathcal{P}$.

(i) For any integer $1 \le k \le p^d$, we denote by $\mathcal{B}_k^x$ the family of all k-sets of elements of $\mathcal{P}$ whose sum is x, and we let $b_k^x = |\mathcal{B}_k^x|$. Moreover, for any $y \in \mathcal{P}$, we denote by $r_k^x(y)$ the number of the k-sets in $\mathcal{B}_k^x$ containing y.

(ii) For any integer $1 \le k \le p^d - 1$, we denote by $\mathcal{B}_k^{x,*}$ the family of all k-sets of elements of $\mathcal{P}^*$ whose sum is x, and we let $b_k^{x,*} = |\mathcal{B}_k^{x,*}|$. Also, we define $b_0^{x,*} = 1 - b_1^{x,*}$. Moreover, for any y in $\mathcal{P}^*$, we denote by $r_k^{x,*}(y)$ the number of the k-sets in $\mathcal{B}_k^{x,*}$ containing y.

Whenever $x = 0$, the superscript x will be always omitted, for short, e.g., $r_k^{0,*}(y)$ will be abbreviated as $r_k^*(y)$.

Theorem 2.2. *Let p be odd. If $1 \le k \le |\mathcal{P}^*| = p^d - 1$, then the following assertions are true:*

(i) *$r_k^{x,*}(y)$ is nonzero for all x in $\mathcal{P}$ and y in $\mathcal{P}^*$, the only exceptions being the trivial cases $k = 1$ for $x \ne y$, $k = 2$ for $x \in \{y, 2y\}$, $k = p^d - 2$ for $x \in \{0, -y\}$, and $k = p^d - 1$ for $x \ne 0$.*

(ii) *For any $2 \le k \le p^d - 4$, and for all x in $\mathcal{P}$ and y in $\mathcal{P}^*$, there exists a k-set of elements of $\mathcal{P}^*$ summing up to x and not containing y. Equivalently, $r_k^{x,*}(y) < b_k^{x,*} = |\mathcal{B}_k^{x,*}|$.*

(iii) *$b_k^{x,*}$ is nonzero for all x in $\mathcal{P}$, the only exceptions being the trivial cases $k = 1$ and $k = p^d - 2$ for $x = 0$, and $k = p^d - 1$ for $x \ne 0$.*

If $1 \le k \le |\mathcal{P}| = p^d$, then the following assertions are true:

(iv) *$r_k^x(y)$ is nonzero for all x, y in $\mathcal{P}$, the only exceptions being the trivial cases $k = 1$ for $x \ne y$, $k = 2$ for $x = 2y$, $k = p^d - 1$ for $x = -y$, and $k = p^d$ for $x \ne 0$.*

(v) *$b_k^x = |\mathcal{B}_k^x|$ is nonzero for all x in $\mathcal{P}$, the only exception being the trivial case $k = p^d$ for $x \ne 0$.*

Proof. Let $1 \le k \le p^d - 1$. In order to prove (i), let x be in $\mathcal{P}$ and let y be in $\mathcal{P}^*$. As $p^d > 2$, the sum of all elements in $\mathcal{P}^*$ is zero. Hence the cases $k = 1$, 2, $p^d - 2$ and $p^d - 1$ are all trivial and can easily be disposed of. Let $3 \le k \le p^d - 3$, forcing p^d to be greater than 5. In this case $r_k^{x,*}(y) \ne 0$, that is, there exists a k-set of elements of $\mathcal{P}^*$ summing up to x and containing y. Indeed, let us first consider the case where $k = 3$. If $a \in \mathcal{P} \setminus \{0, y, x - y, x - 2y, \frac{1}{2}(x - y)\}$ (which is not empty since $p^d > 5$), then $\{y, a, x - y - a\}$ is a 3-set of elements of $\mathcal{P}^*$ summing up to x and containing y. If k is odd and $5 \le k \le p^d - 4$, then, by adding to

$$\{y, a, x - y - a\}$$

$\frac{k-3}{2}$ pairs of opposite elements in $\mathcal{P} \setminus \{0, \pm y, \pm a, \pm(x - y - a)\}$, which has at least cardinality $p^d - 7 \ge k - 3$, one obtains a k-set in $\mathcal{B}_k^{x,*}$ containing y.

Now let k be even, $4 \le k \le p^d - 3$. If we let $h = p^d - k$, then h is odd and $3 \le h \le p^d - 4$. Hence, by the previous case, there exists an h-subset A of $\mathcal{P}^*$ summing up to $y - x$ and containing y. As the sum of all elements in $\mathcal{P}^*$ is zero, $\mathcal{P}^* \setminus A$ is a $(k - 1)$-set of elements of $\mathcal{P}^*$ summing up to $x - y$ and not containing y, thus $(\mathcal{P}^* \setminus A) \cup \{y\}$ is a k-subset of $\mathcal{P}^*$ summing up to x and containing y. Hence (i) is proved.

The same argument on complements shows that, for any $2 \le k \le p^d - 4$ (which forces $p^d \ge 7$), and for all x in $\mathcal{P}$ and y in $\mathcal{P}^*$,

$$r_k^{x,*}(y) < b_k^{x,*}$$

since $h = p^d - 1 - k$ satisfies $3 \le h \le p^d - 3$, thus there exists an h-subset B of $\mathcal{P}^*$ summing up to $-x$ and containing y, whence $\mathcal{P}^* \setminus B$ is a k-set of elements of $\mathcal{P}^*$ summing up to x and not containing y. Thus (ii) is proved. As $r_k^{x,*}(y) \le b_k^{x,*}$ for all x in $\mathcal{P}$ and y in $\mathcal{P}^*$, it follows, by (i) and (ii), that $b_k^{x,*} \ne 0$ for all x in $\mathcal{P}$ and for all $2 \le k \le p^d - 3$ (the case $p^d = 5$ being easily considered separately). Hence (iii) is proved, the cases $k = 1$, $p^d - 2$ and $p^d - 1$ being easily disposed of.

Now let $3 \le k \le p^d - 2$ (which forces $p^d \ge 5$), and let x, y be in $\mathcal{P}$. We claim that $r_k^x(y) \ne 0$. Let us first consider the case where $y = 0$. If we let $h = p^d - k$, then $2 \le h \le p^d - 3$ and, by (iii), there exists an h-set C of elements of $\mathcal{P}^*$ summing up to $-x$. Hence $\mathcal{P} \setminus C$ is a k-set of elements of $\mathcal{P}$ summing up to x and containing $y = 0$, whence $r_k^x(0) \ne 0$. Let us now consider the case where $y \ne 0$. If $3 \le k \le p^d - 3$, then, by case (i),

$$0 < r_k^{x,*}(y) \le r_k^x(y).$$

Thus $r_k^x(y) \neq 0$. Finally, let $k = p^d - 2$. The case $p^d = 5$ is trivial and can be easily proved separately. For $p^d \geq 7$, by (ii) there exists a 2-set D of elements of $\mathcal{P}^*$ summing up to $-x$ and not containing y. Hence $\mathcal{P} \setminus D$ is a $(p^d - 2)$-set of elements of $\mathcal{P}$ summing up to x and containing y, whence $r_k^x(y) \neq 0$. The cases $k = 1, 2$, $p^d - 1$ and p^d are all trivial and can be easily disposed of. Hence (iv) is proved.

For the final case (v), as $\mathcal{B}_{p^d}^x = \emptyset$ for all $x \neq 0$, and since $\mathcal{B}_k^{x,*} \subseteq \mathcal{B}_k^x$ for all x in $\mathcal{P}$ and for all $1 \leq k \leq p^d - 1$, it suffices to show that $\mathcal{B}_k^x$ is nonempty in the three exceptional cases where $\mathcal{B}_k^{x,*}$ is empty. Now $\mathcal{B}_1 = \{\{0\}\}$, and

$$\mathcal{B}_{p^d-1}^x = \{\mathcal{P} \setminus \{-x\}\}$$

for all $x \neq 0$; finally, $\mathcal{B}_{p^d-2}$ consists of all complements in $\mathcal{P}$ of all 2-sets $\{a, -a\}$, as a ranges in $\mathcal{P}^*$.

This completes the proof of the theorem. □

Remark 2.3. In some contexts, the *decision version* of the subset sum problem, that is, settling whether equation (2.1) admits at least one solution with pairwise distinct coordinates x_i, is even more relevant than counting the solutions. For instance, cases (iii) and (v) of the previous theorem already appeared in [6] (cf. also [5]), with a different proof, and have an independent application in Coding Theory, as they are related to the *deep hole problem* for Reed–Solomon codes (cf. [6, Corollaries 2.7, 2.8, 5.2]).

Theorem 2.4 ([6, Theorem 1.2] and [7, Corollary 4.2]). *Let p be odd, let $1 \leq k \leq p^d$ and let $x \in \mathcal{P}$. Define $v(x) = p^d - 1$ if $x = 0$ and $v(x) = -1$ if $x \neq 0$.*

If p does not divide k, then

$$b_k^x = b_k = \frac{1}{p^d}\binom{p^d}{k},$$

whereas, if p divides k, and $m = \frac{k}{p}$, then

$$b_k^x = \frac{1}{p^d}\binom{p^d}{k} + \frac{v(x)}{p^d}\binom{p^{d-1}}{m}.$$

Furthermore, for any $0 \leq k \leq p^d - 1$,

$$b_k^{x,*} = \frac{1}{p^d}\binom{p^d - 1}{k} + (-1)^{k-mp}\frac{v(x)}{p^d}\binom{p^{d-1} - 1}{m}, \tag{2.2}$$

where $m = [\frac{k}{p}]$ is the integral part of $\frac{k}{p}$.

In the following theorem, we compute the numbers $r_k^x(y)$ introduced in Definition 2.1, which play also an essential role in the proof of Theorem 3.5. As for the numbers $r_k^{x,*}(y)$, we note that

$$r_k^{x,*}(y) = r_k^{xy^{-1},*}(1) = N(k-1, xy^{-1} - 1, \mathcal{P} \setminus \{0, 1\}),$$

where the right-most side is the number, computed in closed form in [6, Theorem 1.3], of all $(k-1)$-subsets of $\mathcal{P} \setminus \{0, 1\}$ whose elements add up to $xy^{-1} - 1$, and where it is understood that $\mathcal{P}$ is also endowed with the structure of a Galois field $\mathrm{GF}(p^d)$.

Theorem 2.5. *Let p be odd and let $1 \leq k \leq p^d$. If x and y are in $\mathcal{P}$, then*

$$r_k^x(y) = b_{k-1}^{x-ky,*}.$$

In particular, if p divides k, then $r_k^x(y) = b_{k-1}^{x,*}$ is independent of y.

Proof. By Definition 2.1 and by Theorem 2.2, $r_k^x(y)$ and $b_{k-1}^{x-ky,*}$ are both equal to 0 exactly in the following cases: $k = 1$ and $x \neq y$; $k = 2$ and $x = 2y$; $k = p^d - 1$ and $x = -y$; $k = p^d$ and $x \neq 0$. For all other values of k, x and y, the values of $r_k^x(y)$ and $b_{k-1}^{x-ky,*}$ are both nonzero, and the map $g \mapsto g - y$ is a permutation of $\mathcal{P}$ which induces a one-to-one correspondence between the k-sets in $\mathcal{B}_k^x$ containing y and the k-sets in $\mathcal{B}_k^{x-ky}$ containing zero. Hence the number $r_k^x(y)$ of k-sets in $\mathcal{B}_k^x$ containing y is $b_{k-1}^{x-ky,*}$. □

3 Permutations of zero-sum sets in a finite vector space

In this section, we investigate the symmetries of the structures yielded on the sets $\mathcal{P}$ and $\mathcal{P}^*$ by the families $\mathcal{B}_k = \mathcal{B}_k^0$ and $\mathcal{B}_k^* = \mathcal{B}_k^{0,*}$, respectively. More precisely, we characterize the permutations of $\mathcal{P}$ that induce permutations of $\mathcal{B}_k$, and the permutations of $\mathcal{P}^*$ that induce permutations of $\mathcal{B}_k^*$. Surprisingly enough, these structures turn out to be relatively rigid.

The d-dimensional vector space $\mathcal{P}$ over the ground field GF(p) has a canonical structure of affine space, and it is manifest that the invertible linear mappings over GF(p) permute, together with the elements of $\mathcal{P}$ (respectively of $\mathcal{P}^*$), also the k-sets in $\mathcal{B}_k$ (respectively in $\mathcal{B}_k^*$), and that, as soon as p divides k, the invertible affine mappings do the same.

In Theorem 3.5 and in Theorem 3.2, we prove that the converse is true in both cases, with few trivial, but interesting, exceptions. Note that a permutation φ of $\mathcal{P}^*$ is the restriction of a linear map on $\mathcal{P}$ over the ground field GF(p) if and only if $\varphi(x+y) = \varphi(x) + \varphi(y)$, with the implicit position $\varphi(0) = 0$. These results can be interpreted as analogous to the fundamental theorem of affine geometry, which yields that a collineation over GF(p) is an invertible affine mapping, the analogy being strict in the minimal case where $p^d = 9$ and $k = 3$, that is, for the affine plane AG(2, 3), because in this case lines are precisely 3-sets of elements summing up to zero.

We first characterize the permutations of $\mathcal{P}^*$ that induce permutations of $\mathcal{B}_k^*$, under the necessary assumptions that $p^d \geq 9$ and $3 \leq k \leq p^d - 4$, with $k \neq 4$ in the case where $p^d = 9$. By applying also Theorem 2.5, the characterization of the permutations of $\mathcal{P}$ that induce permutations of $\mathcal{B}_k$ will follow as a corollary. The necessity of the previous assumptions is shown in the following Remark 3.1. Recall that, by Theorem 2.2, $\mathcal{B}_k^*$ is empty for $k = 1$ and $k = p^d - 2$.

Remark 3.1. For any odd p, for any $d \geq 1$, and for $k = 2$, $p^d - 3$ and $p^d - 1$, there are examples of permutations of $\mathcal{P}^*$ that permute the k-sets in $\mathcal{B}_k^*$ and that are not (induced by) linear mappings (with the only exception of the trivial case $p = 3$, $d = 1$, $k = 2$). Indeed, for $p^d > 3$ and $k = p^d - 1$, there exists only one set (that is, $\mathcal{P}^*$) in $\mathcal{B}_k^*$. Hence any permutation of $\mathcal{P}^*$ induces a permutation of $\mathcal{B}_k^*$. For $p^d > 3$ and $k = 2$, given a fixed x in $\mathcal{P}^*$, an example of a permutation of $\mathcal{P}^*$ that permutes the 2-sets in $\mathcal{B}_2^*$, that is, the $\frac{p^d-1}{2}$ pairs of the form $\{z, -z\}$, $z \in \mathcal{P}^*$, is provided by the map φ defined by $\varphi(x) = -x$, $\varphi(-x) = x$ and $\varphi(y) = y$ for all y in $\mathcal{P}^* \setminus \{x, -x\}$. The same map φ also provides an example, for $k = p^d - 3$, of a permutation of $\mathcal{P}^*$ that permutes the k-sets in $\mathcal{B}_k^*$, and that is not (induced by) a linear mapping.

Hence one can restrict oneself to the case where $3 \leq k \leq p^d - 4$ (forcing $p^d \geq 7$). For $p^d = 7$, and (necessarily) $k = 3$, there are examples of permutations of $\mathcal{P}^* = \mathrm{GF}(7)^*$ that permute the 3-sets in $\mathcal{B}_3^*$ and that are not (induced by) linear mappings. For instance, the cyclic permutation $\sigma = (1, 3, 4, 6, 2, 5)$ interchanges the only two 3-sets in $\mathcal{B}_3^*$, that is, $\{1, 2, 4\}$ and $\{3, 5, 6\}$, and is not (induced by) a linear mapping $x \mapsto ax$ because $1 \mapsto 3$ and $2 \mapsto 5 \neq 2 \cdot 3$.

Finally, let us consider the case where $p^d = 9$ and $k = 4$. In this case, $|\mathcal{B}_4^*| = 6$ by (2.2) in Theorem 2.4, thus $\mathcal{B}_4^*$ consists precisely of the six 4-sets of the form $\{x, -x, y, -y\}$, with x, y in $\mathcal{P}^*$. Given a fixed x in $\mathcal{P}^*$, the map φ defined by $\varphi(x) = -x$, $\varphi(-x) = x$ and $\varphi(y) = y$ for all y in $\mathcal{P}^* \setminus \{x, -x\}$ provides again an example of a permutation of $\mathcal{P}^*$ that permutes the 4-sets in $\mathcal{B}_4^*$ and that is not (induced by) a linear mapping.

The proof of the following theorem is mainly based on two basic ideas. The first one is that if φ is a permutation of $\mathcal{P}^*$, then a necessary condition for φ to satisfy $\varphi(x+y) = \varphi(x) + \varphi(y)$ is that the sum $\varphi(x+y) + \varphi(x-y)$ is constant in y.

The second idea is that if φ induces a permutation of $\mathcal{B}_k^*$, then

$$\varphi(x) + \varphi(y) = \varphi(v) + \varphi(w) \tag{3.1}$$

whenever $\{x, y\} \cup S$ and $\{v, w\} \cup S$ are both k-sets in $\mathcal{B}_k^*$ for some common $(k-2)$-set $S \subseteq \mathcal{P}^*$. Indeed, if this is the case, then the images of the two sets under φ are both k-sets in $\mathcal{B}_k^*$ as well, thus

$$\varphi(x) + \varphi(y) + \sum_{z \in S} \varphi(z) = 0 = \varphi(v) + \varphi(w) + \sum_{z \in S} \varphi(z),$$

whence (3.1) follows. For future reference, we call this, for short, the "pair-switching argument", which will systematically be applied throughout the proof.

Theorem 3.2. *Let p be odd, with $p^d \geq 9$, and let k be a fixed integer satisfying $3 \leq k \leq p^d - 4$, with $k \neq 4$ in the case where $p^d = 9$. A permutation φ of $\mathcal{P}^*$ induces a permutation of $\mathcal{B}_k^*$ if and only if φ is (the restriction to $\mathcal{P}^*$ of) an invertible linear mapping of $\mathcal{P}$ over* GF(p).

Proof. As mentioned in the beginning of this section, any restriction to $\mathcal{P}^*$ of an invertible linear mapping of $\mathcal{P}$ over GF(p) induces a permutation of $\mathcal{B}_k^*$, that is,

$$\sum_{x\in B} \varphi(x) = 0 \quad \text{if and only if} \quad \sum_{x\in B} x = 0$$

for any k-set $B \subseteq \mathcal{P}^*$.

Conversely, let $p^d \geq 9$ and let $3 \leq k \leq p^d - 4$, with $k \neq 4$ in the case where $p^d = 9$. Let φ be a permutation of $\mathcal{P}^*$ that induces a permutation of $\mathcal{B}_k^*$, and let us define $\varphi(0) = 0$. In order to prove that

$$\varphi(x + y) = \varphi(x) + \varphi(y) \tag{3.2}$$

for all x, y in $\mathcal{P}^*$, we consider the cases k even and k odd separately.

Case 1: Let k be even, with $4 \leq k \leq p^d - 5$, forcing $p^d \geq 11$ (because the case where $p^d = 9$ and $k = 4$ is excluded). As k is even, we can first prove that

$$\varphi(x) + \varphi(-x) = 0 \tag{3.3}$$

for all $x \in \mathcal{P}^*$. Indeed, let x and z be distinct elements of $\mathcal{P}^*$. One can complete the pairs $\{x, -x\}$ and $\{z, -z\}$ to two k-sets in $\mathcal{B}_k^*$ by adding the same $\frac{k-2}{2}$ pairs of the form $\{a_i, -a_i\} \subseteq \mathcal{P}^* \setminus \{\pm x, \pm z\}$, which exist because $k - 2 \leq p^d - 7 < |\mathcal{P}^* \setminus \{\pm x, \pm z\}|$. Hence

$$\varphi(x) + \varphi(-x) = \varphi(z) + \varphi(-z) \tag{3.4}$$

for any $x, z \in \mathcal{P}^*$ by the "pair-switching argument" (3.1). Therefore, by summing up over all elements $z \in \mathcal{P}^*$,

$$(p^d - 1)(\varphi(x) + \varphi(-x)) = \sum_{z\in\mathcal{P}^*} (\varphi(z) + \varphi(-z)) = \sum_{z\in\mathcal{P}^*} \varphi(z) + \sum_{z\in\mathcal{P}^*} \varphi(-z) = 0 + 0.$$

Hence equality (3.3) holds for all $x \in \mathcal{P}^*$.

Case 1.1: Let $k = 4$. In order to prove (3.2), it suffices to show that, for a given x in $\mathcal{P}^*$, the equality

$$\varphi(x + y) + \varphi(x - y) = 2\varphi(x) \tag{3.5}$$

holds for all $y \in \mathcal{P}^* \setminus \{x, -x\}$. Indeed, if one proves that $\varphi(x + y) = 2\varphi(x) - \varphi(x - y)$ for all $y \in \mathcal{P}^* \setminus \{x, -x\}$, then, the set $\mathcal{P}$ being equal to both $\{\varphi(x + y) : y \in \mathcal{P}\}$ and $\{2\varphi(x) - \varphi(x - y) : y \in \mathcal{P}\}$, one can first conclude, by considering in both sets the three elements obtained for $y \in \{-x, 0, x\}$, that

$$\{0, \varphi(x), \varphi(2x)\} = \{2\varphi(x) - \varphi(2x), \varphi(x), 2\varphi(x)\}.$$

Since $2\varphi(x) \notin \{0, \varphi(x)\}$, it follows that

$$\varphi(2x) = 2\varphi(x). \tag{3.6}$$

Hence equality (3.5) holds for all x and y in $\mathcal{P}^*$, and trivially, by (3.3), also for all x and y in $\mathcal{P}$. Finally, by (3.6) and (3.5), one concludes, with a standard artifice, that

$$\varphi(x + y) = \varphi\Big(2\frac{x + y}{2}\Big) = 2\varphi\Big(\frac{x + y}{2}\Big) = \varphi\Big(\frac{x + y}{2} + \frac{x - y}{2}\Big) + \varphi\Big(\frac{x + y}{2} - \frac{x - y}{2}\Big) = \varphi(x) + \varphi(y)$$

for all x and y in $\mathcal{P}$, as claimed.

In order to prove that equality (3.5) holds for at least one element $y = w \in \mathcal{P}^* \setminus \{x, -x\}$, let us consider, for a given x in $\mathcal{P}^*$, the two 4-sets in $\mathcal{B}_4^*$

$$\{x + w, -x, -z, z - w\} \quad \text{and} \quad \{x - w, -x, z, w - z\},$$

where the following conditions hold:

- x, w, and z are linearly independent over GF(p), if $p = 3$ (hence $d > 2$);
- x and w are linearly independent over GF(p), and $z = 2x$, if $p > 3$ and $d > 1$;
- $w = 5x$ and $z = 3x$, if $p > 3$ and $d = 1$ (hence $p \geq 11$).

Since the images under φ of these two sets belong to $\mathcal{B}_4^*$ as well, one can write, by (3.3),

$$\varphi(x+w) - \varphi(x) - \varphi(z) + \varphi(z-w) = 0,$$
$$\varphi(x-w) - \varphi(x) + \varphi(z) - \varphi(z-w) = 0,$$

whence

$$\varphi(x+w) + \varphi(x-w) = 2\varphi(x), \tag{3.7}$$

that is, equality (3.5) is satisfied by the element $y = w \in \mathcal{P}^* \setminus \{x, -x\}$. For future reference, note that, by the construction above, $w \notin \{4x, -4x\}$ for all p and d, with $p^d \geq 11$.

We are now left with the proof of equality (3.5) for all $y \in \mathcal{P}^* \setminus \{x, -x\}$. By the previous argument, for $p = 3$ there is nothing left to prove since (3.5) holds for all $y = w$ linearly independent of x over GF(p). Thus we can assume henceforth that $p > 3$.

The set $\{x+y, x-y, x, -3x\}$ is a 4-set in $\mathcal{B}_4^*$ for all $y \in \mathcal{P}^* \setminus \{x, -x, 4x, -4x\}$, including $y = w$. Hence equality (3.5) holds for all such elements y by (3.7) and by the "pair-switching argument" (3.1). If $p = 5$, then $4x = -x$, thus (3.5) holds for all $y \in \mathcal{P}^* \setminus \{x, -x\}$ as claimed. For $p > 5$, it suffices to prove that (3.5) holds for $y \in \{4x, -4x\}$, that is, that $\varphi(5x) + \varphi(-3x) = 2\varphi(x)$.

Let p be greater than 5. The equation $a + b = -2x$, in the unknowns a, b in $\mathcal{P}^*$, has exactly $\frac{p^d-1}{2}$ solutions $\{a, b\}$, one of which, that is, $\{-x, -x\}$ is not a 2-subset of $\mathcal{P}^*$. Since $p^d \geq 11$, that is, $\frac{p^d-1}{2} \geq 5$, one can conclude that there exists at least one 2-set $\{a, b\} \subseteq \mathcal{P}^*$ disjoint from $\{5x, -3x, 3x, -x\}$ and such that $a + b = -2x$. Therefore, the two sets $\{5x, -3x, a, b\}$ and $\{3x, -x, a, b\}$ are both 4-sets in $\mathcal{B}_4^*$. Hence, since equality (3.5) holds for $y = 2x$, it follows that

$$\varphi(5x) + \varphi(-3x) = \varphi(3x) + \varphi(-x) = 2\varphi(x)$$

by the "pair-switching argument" (3.1). Thus equality (3.5) holds for all $y \in \mathcal{P}^* \setminus \{x, -x\}$ as claimed.

Case 1.2: Let k be even, with $6 \leq k \leq p^d - 5$. If $\{a, b, c, d\}$ is a 4-set in $\mathcal{B}_4^*$, then one can complete $\{a, b, c, d\}$ to a k-set in $\mathcal{B}_k^*$ by adding $\frac{k-4}{2}$ pairs of the form $\{x_i, -x_i\}$, which exist because

$$k - 4 \leq p^d - 9 \leq |\mathcal{P}^* \setminus \{\pm a, \pm b, \pm c, \pm d\}|.$$

Since φ maps such k-set onto another k-set in $\mathcal{B}_k^*$, by applying equality (3.3) it follows that

$$0 = \varphi(a) + \varphi(b) + \varphi(c) + \varphi(d) + \sum_{i=1}^{\frac{k-4}{2}} (\varphi(x_i) + \varphi(-x_i)) = \varphi(a) + \varphi(b) + \varphi(c) + \varphi(d).$$

Hence φ induces also a permutation of $\mathcal{B}_4^*$, whence, by the previous case 1.1, φ satisfies (3.2).

Case 2: Let k be odd. As the sum of all elements of $\mathcal{P}^*$ is zero, we can confine ourselves, up to considering the complementary sets, to the cases where

$$3 \leq k \leq \frac{p^d - 1}{2}.$$

Case 2.1: Let $k = 3$. Let x be a given element in $\mathcal{P}^*$. If $y \in \mathcal{P}^* \setminus \{x, -x, -\frac{x}{2}, -2x\}$, then the set $\{x+y, -y, -x\}$ is in $\mathcal{B}_3^*$, together with its image under φ, thus

$$\varphi(x+y) = -\varphi(-y) - \varphi(-x). \tag{3.8}$$

If, in addition, $y \notin \{\frac{x}{2}, 2x\}$, then the set $\{x-y, y, -x\}$ is in $\mathcal{B}_3^*$ as well. Thus

$$\varphi(x-y) = -\varphi(y) - \varphi(-x),$$

whence

$$\varphi(x+y) + \varphi(x-y) = -\varphi(-y) - \varphi(y) - 2\varphi(-x).$$

And if, in addition, $y \notin \{3x, -3x\}$, then the set $\{x+y, x-y, -2x\}$ is in $\mathcal{B}_3^*$ as well. Thus

$$\varphi(x+y) + \varphi(x-y) = -\varphi(-2x),$$

whence it follows from the two previous equalities that

$$\varphi(-2x) - 2\varphi(-x) = \varphi(y) + \varphi(-y) \tag{3.9}$$

for all $y \in \mathcal{P}^* \setminus \{\pm x, \pm\frac{x}{2}, \pm 2x, \pm 3x\}$.

Let us first consider the case where $p^d \notin \{11, 13\}$. For x and z in $\mathcal{P}^*$, we let

$$\mathcal{A} = \left\{\pm x, \pm\frac{x}{2}, \pm 2x, \pm 3x, \pm z, \pm\frac{z}{2}, \pm 2z, \pm 3z\right\}.$$

For $p^d = 9$ the set $\mathcal{A}$ has at most 5 elements, and for $p^d = 17$ it can be checked, by direct inspection, that the set $\mathcal{A}$ has at most 14 elements, whereas, for $p^d > 17$, $\mathcal{A}$ has trivially at most 16 elements. Hence, in all cases where $p^d \notin \{11, 13\}$, there exists $y \in \mathcal{P}^* \setminus \mathcal{A}$, thus $\varphi(-2x) - 2\varphi(-x) = \varphi(-2z) - 2\varphi(-z)$ by (3.9). Therefore, by summing up over all elements $z \in \mathcal{P}^*$,

$$(p^d - 1)(\varphi(-2x) - 2\varphi(-x)) = \sum_{z\in\mathcal{P}^*} (\varphi(-2z) - 2\varphi(-z)) = \sum_{z\in\mathcal{P}^*} \varphi(-2z) - 2\sum_{z\in\mathcal{P}^*} \varphi(-z) = 0 + 0.$$

Hence equality (3.6) holds for all $x \in \mathcal{P}^*$. It follows from (3.9) that

$$\varphi(y) + \varphi(-y) = 0$$

for all $y \in \mathcal{P}^* \setminus \{\pm x, \pm\frac{x}{2}, \pm 2x, \pm 3x\}$. On the other hand, for any given $y \in \mathcal{P}^*$, there exists $x \in \mathcal{P}^*$ such that $y \in \mathcal{P}^* \setminus \{\pm x, \pm\frac{x}{2}, \pm 2x, \pm 3x\}$. Hence $\varphi(y) + \varphi(-y) = 0$. Therefore, equality (3.3) holds for all $x \in \mathcal{P}^*$.

This turns equality (3.8) into equality (3.2) for any $y \in \mathcal{P}^* \setminus \{x, -x, -\frac{x}{2}, -2x\}$. The case where $y = -x$ follows from (3.3) because $\varphi(0) = 0$, whereas the cases where $y = x$, $y = -\frac{x}{2}$ and $y = -2x$ follow directly from (3.3) and (3.6). Hence φ satisfies (3.2).

This completes the proof for $k = 3$ in the case where $p^d \notin \{11, 13\}$. In the two remaining cases, the above considered set $\mathcal{P}^* \setminus \mathcal{A}$ can indeed be empty. Hence a separate argument is needed.

Let $p^d = 11$. To prove that the map φ satisfies (3.2) it is sufficient to prove that the map $\psi(x) = \varphi(1)^{-1}\varphi(x)$ (where we are referring to a chosen field structure of $\mathcal{P}$) satisfies $\psi(x+y) = \psi(x) + \psi(y)$. Whenever $\psi(x) = x$ for some x in $\mathcal{P}^*$, the set $\{5x, -2x, -x\}$ of those elements that are not in any 3-set in $\mathcal{B}_3^*$ through x, is invariant under ψ. Hence ψ leaves also the set $\{3x, -3x, -4x\}$ invariant, because each of its elements belongs to a 3-set in $\mathcal{B}_3^*$ with two of the elements in $\{5x, -2x, -x\}$. Since $\{x, 3x, -4x\} \in \mathcal{B}_3^*$, the map ψ leaves, together with the set $\{3x, -3x, -4x\}$, also its subset $\{3x, -4x\}$ and the singleton $\{-3x\}$ invariant. Since $\psi(1) = 1$, and -3 is a generator of $\mathrm{GF}(11)^*$, it follows that ψ is the identity and that φ satisfies (3.2). The theorem is now proved for $k = 3$, the case where $p^d = 13$ being utterly analogous.

Case 2.2: Let k be odd and $5 \le k \le \frac{p^d-1}{2}$, forcing $p^d \ge 11$. In order to show that φ satisfies (3.2), that is, that it is the restriction to $\mathcal{P}^*$ of an invertible linear mapping of $\mathcal{P}$ over $\mathrm{GF}(p)$, it is sufficient to prove equality (3.4) for all x and z in $\mathcal{P}^*$. Indeed, if (3.4) holds, then, as in the previous case 1, one can first conclude that equality (3.3) holds for all x in $\mathcal{P}^*$ as well. Subsequently, if $\{a, b, c\}$ is a 3-set in $\mathcal{B}_3^*$, then one can complete $\{a, b, c\}$ to a k-set in $\mathcal{B}_k^*$ by adding $\frac{k-3}{2}$ pairs of the form $\{x_i, -x_i\}$, which exist because $k - 3 \le p^d - 7 = |\mathcal{P}^* \setminus \{\pm a, \pm b, \pm c\}|$. Since φ maps such k-set onto another k-set in $\mathcal{B}_k^*$, by applying equality (3.3) it follows that

$$0 = \varphi(a) + \varphi(b) + \varphi(c) + \sum_{i=1}^{\frac{k-3}{2}} (\varphi(x_i) + \varphi(-x_i)) = \varphi(a) + \varphi(b) + \varphi(c).$$

Thus φ induces also a permutation of $\mathcal{B}_3^*$, whence, by the previous case 2.1, φ satisfies (3.2).

In order to prove (3.4), let us first consider, as before, the case where $p^d \notin \{11, 13\}$. In this case, it suffices to show that, for any two elements x and z in $\mathcal{P}^*$ with $\{x, -x\} \cap \{z, -z\} = \emptyset$, there exists a 3-set $\{a, b, c\}$ in $\mathcal{B}_3^*$ such that $\{a, b, c\} \cap \{x, -x, z, -z\} = \emptyset$. Indeed, under this assumption, let us first consider the case where $k = 5$. The two 5-sets $\{x, -x\} \cup \{a, b, c\}$ and $\{z, -z\} \cup \{a, b, c\}$ belong to $\mathcal{B}_5^*$. Hence equality (3.4) holds by the "pair-switching argument" (3.1).

If $7 \le k \le \frac{p^d-1}{2}$, then $k \le p^d - 6$ as well, thus one can complete $\{a, b, c\}$ to a $(k-2)$-set S in $\mathcal{B}^*_{k-2}$ by adding $\frac{k-5}{2}$ pairs of the form $\{y, -y\}$, each one disjoint from both $\{x, -x\}$ and $\{z, -z\}$, which exist because

$$k - 5 \le p^d - 11 = |\mathcal{P}^* \setminus \{\pm a, \pm b, \pm c, \pm x, \pm z\}|.$$

By construction, the two k-sets $\{x, -x\} \cup S$ and $\{z, -z\} \cup S$ belong to $\mathcal{B}^*_k$. Hence equality (3.4) holds by the "pair-switching argument" (3.1).

In order to prove that such a 3-set $\{a, b, c\}$ exists, let x and z be two elements in $\mathcal{P}^*$ with

$$\{x, -x\} \cap \{z, -z\} = \emptyset,$$

and let a be a given element in the set $\mathcal{P}^* \setminus \{x, -x, z, -z\}$. The equation $b + c = -a$ in the unknowns b, c in $\mathcal{P}$, has exactly $\frac{p^d+1}{2}$ solutions $\{b, c\}$, three of which, that is, $\{0, -a\}$, $\{-\frac{a}{2}, -\frac{a}{2}\}$ and $\{a, -2a\}$, do not give in turn a 3-subset $\{a, b, c\}$ of $\mathcal{P}^*$. Of the remaining $\frac{p^d-5}{2}$ solutions $\{b, c\}$, at most four intersect the set $\{x, -x, z, -z\}$. Since $\frac{p^d-5}{2} > 4$, there exists at least one 3-set $\{a, b, c\}$ in $\mathcal{B}^*_3$ disjoint from $\{x, -x, z, -z\}$, thereby producing the desired 3-set (in passing, note that this argument fails in the two cases $p^d = 11, 13$).

We are now left with the proof of equality (3.4) in the only cases where $p^d = 11, 13$, and (necessarily) $k = 5$. For $p^d = 11$, the two 5-sets $\{x, -x, 2x, 4x, 5x\}$ and $\{3x, -3x, 2x, 4x, 5x\}$ are in $\mathcal{B}^*_5$ for any x in $\mathcal{P}^*$. Hence, by the "pair-switching argument" (3.1), the equality

$$\varphi(x) + \varphi(-x) = \varphi(\alpha x) + \varphi(-\alpha x)$$

is valid for $\alpha = -3$. Since $\alpha = -3$ is a generator of $\mathrm{GF}(11)^*$, equality (3.4) is valid, by transitivity, for any $x, z \in \mathcal{P}^*$.

Similarly, for $p^d = 13$, the two 5-sets $\{x, -x, 3x, 4x, 6x\}$ and $\{2x, -2x, 3x, 4x, 6x\}$ are in $\mathcal{B}^*_5$ for any x in $\mathcal{P}^*$. Hence the equality

$$\varphi(x) + \varphi(-x) = \varphi(\alpha x) + \varphi(-\alpha x)$$

is valid for $\alpha = 2$. Since $\alpha = 2$ is a generator of $\mathrm{GF}(13)^*$, equality (3.4) is valid, by transitivity, for any $x, z \in \mathcal{P}^*$.

This completes the proof of the theorem. □

Remark 3.3. As we noted in Remark 3.1, Theorem 3.2 fails for $p^d = 7$ and $k = 3$. Note that the argument we used in the case where $k = 3$ and $p^d \in \{11, 13\}$ fails for $p^d = 7$ because, for any $x \in \mathcal{P}^*$, the three elements in $\mathcal{P}^* \setminus \{x\}$ that are not in any 3-set in $\mathcal{B}^*_3$ through x are $-x$, $-2x$ and $\frac{-x}{2}$, which (for $p = 7$ only!) form in turn a 3-set in $\mathcal{B}^*_3$.

We now apply Theorem 3.2 and Theorem 2.5, to characterize the permutations of $\mathcal{P}$ that induce permutations of $\mathcal{B}_k$, under the necessary assumptions that $p^d \ge 9$ and $3 \le k \le p^d - 3$, where, to avoid trivialities, the cases $k = 1$, $k = p^d - 1$ and $k = p^d$ are disregarded (in each of these cases, $\mathcal{B}_k$ consists of only one element). The necessity of such assumptions is shown in the following Remark 3.4.

Remark 3.4. For any odd p and for any $d \ge 1$ with $p^d > 3$, for $k = 2$ and $k = p^d - 2$ there are examples of permutations of $\mathcal{P}$ that permute the k-sets in $\mathcal{B}_k$ and that are not (induced by) linear mappings. Indeed, in either case, given a fixed x in $\mathcal{P}^*$, an example is provided, as in Remark 3.1, by the map φ defined by $\varphi(x) = -x$, $\varphi(-x) = x$ and $\varphi(y) = y$ for all y in $\mathcal{P} \setminus \{x, -x\}$.

Hence one can restrict oneself to the case where $3 \le k \le p^d - 3$. For $p^d = 7$ and $k = 3$, the map

$$\sigma = (1, 3)(2, 5)(4, 6)$$

is a permutation of $\mathcal{P} = \mathrm{GF}(7)$, which interchanges the five 3-sets in $\mathcal{B}_3$, that is, $\{0, 1, 6\}$, $\{0, 2, 5\}$, $\{0, 3, 4\}$, $\{1, 2, 4\}$ and $\{3, 5, 6\}$, and is not (induced by) a linear mapping $x \mapsto ax$ because $1 \mapsto 3$ and $2 \mapsto 5 \ne 2 \cdot 3$. The same map, by complementation, is a permutation of $\mathrm{GF}(7)$ which interchanges the five 4-sets in $\mathcal{B}_4$ and is not (induced by) a linear mapping.

Theorem 3.5. *Let p be odd, with $p^d \ge 9$, and let k be a fixed integer satisfying $3 \le k \le p^d - 3$. If φ is a permutation of $\mathcal{P}$, then the following assertions hold:*

(i) *In the case that p does not divide k, φ induces a permutation of $\mathcal{B}_k$ if and only if φ is an invertible linear map of the vector space $\mathcal{P}$ over $\mathrm{GF}(p)$.*

(ii) *In the case that p divides k, φ induces a permutation of $\mathcal{B}_k$ if and only if φ is an invertible affinity of the affine space $\mathcal{P}$ over the ground field* $\mathrm{GF}(p)$*, that is, if and only if $\varphi(x) = \varphi_0(x) + b$, where φ_0 is an invertible linear map on $\mathcal{P}$ over* $\mathrm{GF}(p)$*, and $b = \varphi(0)$.*

Proof. As mentioned in the beginning of this section, every invertible linear map permutes the elements of $\mathcal{P}$ and the k-sets in $\mathcal{B}_k$, and the same is true for invertible affinities, under the additional assumption that p divides k.

In order to prove the converse, we first show that, in either case, we can reduce to the case where

$$\varphi(0) = 0.$$

Indeed, suppose that $p^d \geq 9$ and $3 \leq k \leq p^d - 3$, and assume that φ is a permutation of $\mathcal{P}$ which induces a permutation of $\mathcal{B}_k$. If p divides k, then it suffices to compose φ with the translation by $-\varphi(0)$. If p does not divide k, then, by Theorem 2.5, given an element $y \in \mathcal{P}$, the number of k-sets in $\mathcal{B}_k$ containing y is equal to $b_{k-1}^{-ky,*}$. As $-ky = 0$ if and only if $y = 0$, it follows from equality (2.2) that the number of k-sets in $\mathcal{B}_k$ containing 0 is different from the number of k-sets in $\mathcal{B}_k$ containing any other element y of $\mathcal{P}$. Since φ maps the k-sets in $\mathcal{B}_k$ containing 0 onto the k-sets in $\mathcal{B}_k$ containing $\varphi(0)$, it now follows that $\varphi(0) = 0$, as claimed.

In either case, we are left to prove that φ is a linear map. By mapping 0 to 0, φ induces a permutation of $\mathcal{P}^*$ which permutes the k-sets in $\mathcal{B}_k^*$, thus φ is linear, by Theorem 3.2, for all $3 \leq k \leq p^d - 4$, with $k \neq 4$ in the case where $p^d = 9$. Thus we are left to prove that φ is linear in the case where either $k = p^d - 3$, or $p^d = 9$ and $k = 4$.

If $k = p^d - 3$ and φ is a permutation of $\mathcal{P}$ which permutes the k-sets in $\mathcal{B}_k$, then, by complementation, φ permutes also the 3-sets in $\mathcal{B}_3$. By mapping 0 to 0, φ induces a permutation of $\mathcal{P}^*$ which permutes the 3-sets in $\mathcal{B}_3^*$, thus φ is linear by Theorem 3.2. Similarly, if $p^d = 9$, and φ is a permutation of $\mathcal{P}$ which permutes the 4-sets in $\mathcal{B}_4$, then, by complementation, φ permutes also the 5-sets in $\mathcal{B}_5$. By mapping 0 to 0, φ induces a permutation of $\mathcal{P}^*$ which permutes the 5-sets in $\mathcal{B}_5^*$, thus φ is linear by Theorem 3.2.

This completes the proof of the theorem. □

Remark 3.6. Under the same hypotheses, a direct consequence of Theorem 3.5 is that, in the case where p does not divide k, one can characterize the permutations of $\mathcal{P}$ that induce permutations of $\mathcal{B}_k^x$, also for x in $\mathcal{P}^*$.

Indeed, for $x \neq 0$, if p does not divide k, then the function $T_x : \mathcal{B}_k^0 \to \mathcal{B}_k^x$ mapping $\{x_1, \dots, x_k\}$ to $\{x_1 + \frac{1}{k}x, \dots, x_k + \frac{1}{k}x\}$ is a bijection. Hence, if φ is a permutation of $\mathcal{P}$, then φ induces a permutation of $\mathcal{B}_k^x$ if and only if $T_x^{-1}\varphi T_x$ induces a permutation of $\mathcal{B}_k = \mathcal{B}_k^0$. This, together with case (i) of Theorem 3.5, shows that φ is such a permutation exactly when φ is an invertible affinity of the affine space $\mathcal{P}$ of the form $\varphi(z) = \varphi_0(z) + b$, where φ_0 is an invertible linear map on $\mathcal{P}$ over $\mathrm{GF}(p)$, and $b = \frac{1}{k}(x - \varphi_0(x))$.

In the case where p divides k, it remains to be investigated whether, besides the invertible affinities of $\mathcal{P}$ of the form $\varphi(z) = \varphi_0(z) + b$, where φ_0 is an invertible linear map on $\mathcal{P}$ over $\mathrm{GF}(p)$ fixing x, there exist other (necessarily nonaffine) permutations of $\mathcal{P}$ that induce permutations of $\mathcal{B}_k^x$.

Similarly, it remains to be investigated whether, under the same hypotheses as in Theorem 3.2, besides the invertible linear maps on $\mathcal{P}$ fixing x, there exist other (necessarily nonlinear) permutations of $\mathcal{P}^*$ that induce permutations of $\mathcal{B}_k^{x,*}$.

Funding: This research was supported by the University of Palermo (FFR).

References

[1] T. Beth, D. Jungnickel and H. Lenz, *Design Theory*, 2nd ed., Cambridge University, Cambridge, 1999.
[2] A. Caggegi, G. Falcone and M. Pavone, On the additivity of block designs, *J. Algebraic Combin.* **45** (2017), no. 1, 271–294.
[3] A. Caggegi, G. Falcone and M. Pavone, Additivity of affine designs, *J. Algebraic Combin.* (2020), DOI 10.1007/s10801-020-00941-8.
[4] C. J. Colbourn and J. H. Dinitz, *The CRC Handbook of Combinatorial Designs*, 2nd ed., CRC Press, Boca Raton, 2007.
[5] M. Kosters, The subset sum problem for finite abelian groups, *J. Combin. Theory Ser. A* **120** (2013), no. 3, 527–530.

[6] J. Li and D. Wan, On the subset sum problem over finite fields, *Finite Fields Appl.* **14** (2008), no. 4, 911–929.
[7] J. Li and D. Wan, Counting subset sums of finite abelian groups, *J. Combin. Theory Ser. A* **119** (2012), no. 1, 170–182.
[8] M. B. Nathanson, *Additive Number Theory*, Grad. Texts in Math. 165, Springer, New York, 1996.
[9] M. Pavone, Subset sums and block designs in a finite vector space, manuscript.
[10] T. Tao and V. Vu, *Additive Combinatorics*, Cambridge Stud. Adv. Math. 105, Cambridge University, Cambridge, 2006.