On the subset sum problem for finite fields[1] [2] [3]

Marco Pavone
Dipartimento di Ingegneria
Università degli Studi di Palermo, Viale delle Scienze, 90128 Palermo, Italy
marco.pavone@unipa.it

Abstract

Let G be the additive group of a finite field. J. Li and D. Wan determined the exact number of solutions of the subset sum problem over G, by giving an explicit formula for the number of subsets of G of prescribed size whose elements sum up to a given element of G. They also determined a closed-form expression for the case where the subsets are required to contain only nonzero elements. In this paper we give an alternative proof of the two formulas. Our argument is purely combinatorial, as in the original proof by Li and Wan, but follows a different and somehow more "natural" approach. We also indicate some new connections with coding theory and combinatorial designs.

1 Introduction

Let $\mathbb{F}_q$ be a finite field, let D be a nonempty subset of $\mathbb{F}_q$ of cardinality $|D|$, and let k be an integer such that $1 \leq k \leq |D|$. The *subset sum problem* over D is to determine whether, for a given b in $\mathbb{F}_q$, there exists a subset $\{x_1, x_2, \ldots, x_k\}$ of D of size k such that

$$x_1 + x_2 + \cdots + x_k = b. \tag{1}$$

The requirement that the x_i's be distinct results in a significant combinatorial difficulty, and, moreover, the problem becomes furtherly harder if D is too small or has no algebraic structure.

This leads to some relevant applications in coding theory and cryptography. For instance, the case $D = \mathbb{F}_q$ is related to the deep hole problem of extended Reed-Solomon codes (see [3, 10]). Further interesting problems occur in combinatorics and additive number theory. For instance, one may ask what is the smallest positive integer n such that, for every subset D of cardinality n and every b in $\mathbb{F}_q$, there is a k-subset of D whose elements sum up to b (see the discussion in [10, §1]). In [10] it is proved that if n is close to q, then the subset sum problem has a solution for every b if $2 < k < n$, else the problem might not have a solution for some b. In the latter case, it would be interesting to find the smallest $k > 1$ such that the problem has a solution for every b.

More generally, for a finite group $(G, +)$, the critical number of G is defined as the smallest positive integer n such that, for every $D \subseteq G \setminus \{0\}$ of size $|D| \geq n$, each element of G is a sum of distinct elements of D (see [4]; cf. [5]). For most groups, this number is not known, and the question is open even for abelian groups.

Another related problem, in the case of a finite field $\mathbb{F}_q$, is to determine the exact number of k-subsets of D whose elements sum up to b, that is, the number

$$N(k, b, D) = \left|\{\{x_1, \ldots, x_k\} \subseteq D \,:\, x_1 + x_2 + \cdots + x_k = b\}\right|.$$

An explicit formula for $N(k, b, D)$ was given by J. Li and D. Wan in 2008 in [10], in the case where either $D = \mathbb{F}_q$ or $D = \mathbb{F}_q^*$ $(= \mathbb{F}_q \setminus \{0\})$, by means of a purely combinatorial method.

[1] This research was supported by Università di Palermo (FFR).
[2] AMS MSC2020: 05A18, 11P70, 11B75.
[3] *Keywords*: Subset sum problem, subset sum, finite field, zero-sum set, zero sumset.

1.1 Theorem: [10, Theorem 1.2] *Let $\mathbb{F}_q$ be a finite field of characteristic p, and let b be a given element of $\mathbb{F}_q$. Define $v(b) = -1$ if $b \neq 0$, and $v(b) = q - 1$ if $b = 0$. If $1 \leq k \leq q$, then*

$$N(k, b, \mathbb{F}_q) = \begin{cases} \dfrac{1}{q}\dbinom{q}{k} & \text{if } k \text{ is not multiple of } p \\ \dfrac{1}{q}\dbinom{q}{k} + (-1)^{k+k/p}\,\dfrac{v(b)}{q}\dbinom{q/p}{k/p} & \text{if } k \text{ is multiple of } p. \end{cases} \tag{2}$$

If $1 \leq k \leq q - 1$, then

$$N(k, b, \mathbb{F}_q^*) = \frac{1}{q}\binom{q-1}{k} + (-1)^{k+\lfloor k/p \rfloor}\,\frac{v(b)}{q}\binom{q/p - 1}{\lfloor k/p \rfloor}, \tag{3}$$

where $\lfloor \cdot \rfloor$ is the floor function.

For $p = 2$ and $D = \mathbb{F}_q^*$, the closed-form expression (3) for $N(k, b, \mathbb{F}_q^*)$ had already been given by T. Etzion and A. Vardy in 1994 in the context of coding theory [6, Proposition 4.1], although the connection between this earlier result and the general formula for $N(k, b, \mathbb{F}_q^*)$ in [10] has remained somehow unnoticed, since the formula in [6] was stated as a general result on the weight distribution of a perfect binary code.

In the special case of a binary Hamming code, the closed-form expression for the weight distribution had already been given by Shapiro and Slotnick in [14, Remark 2, p. 28], whereas, for the general case of a perfect binary code, a new, elementary, proof is given by the present author in [12], where, unlike in the original proof by Etzion and Vardy, we do not rely on the weight distributions of the translates of the code.

To derive the equivalence, for $p = 2$, between the above equality (3) and Proposition 4.1 in [6], it suffices to note that, for $q = 2^m$, $m \geq 3$, the family $\mathcal{B}_k^*(b)$ of the k-subsets of $\mathbb{F}_q^*$ whose elements sum up to b is in a one-to-one correspondence with the codewords of weight k in the $(n = 2^m - 1, 2^m - m - 1, 3)$-Hamming code C, if $b = 0$, and with the codewords of weight k in the translate code $C + e_i$, if $b \neq 0$ is the i-th column in the parity-check matrix of C and e_i is the i-th vector of the canonical basis of $\mathbb{F}_2^n$ (see, for instance, [8]).

In the former case ($b = 0$), $\mathcal{D}_k^* = (\mathbb{F}_q^*, \mathcal{B}_k^*(0))$ is a 2-(n, k, λ) combinatorial design, whose full automorphism group is (isomorphic to) the group of invertible linear maps on $\mathbb{F}_q$ over $\mathbb{F}_2$, and the problem of the computation of $N(k, 0, \mathbb{F}_q^*)$ corresponds to the computation of the number of blocks of the *additive* design $\mathcal{D}_k^*$ ([8]; see also [13, 7] for the case where the point-set of the design is $\mathbb{F}_{p^m}^*$, with p an odd prime. See [1, 2] for the general setting of additive designs).

In 2012, the above formula (2) for $N(k, b, D)$ was extended by Li and Wan to an arbitrary additive subgroup D of $\mathbb{F}_q$ [11, Corollary 4.2], and, more generally, to an arbitrary finite abelian group D [11, Theorem 1.1], by means of a new sieving formula which improves the classical inclusion-exclusion sieve. Finally, in 2013, M. Kosters slightly improved the latter result by giving an explicit formula for $N(k, b, D)$, using character theory, in the case where G is a finite abelian group and D is either G or $G \setminus \{0\}$ [9, Theorems 1.1 and 1.3]. The main difference between [9] and [11] is in the technique used in proving the formula.

In this paper we give an alternative proof of Theorem 1.1. Our argument is purely combinatorial and relies on some recursive relations among the values of $N(k, b, D)$, as in [10], but follows a different and somehow more "natural" and intuitive approach.

2 The proof of Theorem 1.1

Let us first briefly outline the basic steps of the original proof by Li and Wan in [10]. For a matter of convenience, the authors study the value $M(k,b,D) = k!N(k,b,D)$, that is, the number of ordered k-tuples $(x_1,\dots,x_k)$ satisfying the equation (1), with $x_i \in D$ and $x_i \neq x_j$ for $i \neq j$. Moreover, the cases $D = \mathbb{F}_q$ and $D = \mathbb{F}_q^*$ are not considered separately, as they are related in a few recursive relations among the values of $M(k,b,D)$, some of which involve both $D = \mathbb{F}_q$ and $D = \mathbb{F}_q^*$ at the same time. The most important of these relations is a formula for the special case where k is a multiple of p, which expresses $M(k,b,\mathbb{F}_q)$ in terms of $M(k-1,b,\mathbb{F}_q^*)$, and is obtained by considering the p-rank of the coefficient matrix of a suitable system of equations.

Our proof, instead, considers the cases $D = \mathbb{F}_q$ and $D = \mathbb{F}_q^*$ separately, in view of the trivial observation that the formula (3) can be easily reduced to the formula (2) by means of the immediate relation $N(k,b,\mathbb{F}_q^*) = N(k,b,\mathbb{F}_q) - N(k-1,b,\mathbb{F}_q^*)$. The equality (2), in turn, can be proved just for p dividing k, the other case being a trivial consequence of an immediate translation argument. A similar elementary argument, based on the action of the multiplicative group of $\mathbb{F}_q$ on itself, shows at last that it suffices to prove the equality (2) only in the case where p divides k and $b = 0$. This is the most important case of the proof, which is based on the crucial inspiring idea of the whole argument.

The idea is very simple, and relies on the "natural" observation that $N(k,0,\mathbb{F}_q)$ is the number of all the k-subsets $\{x_1,\dots,x_{k-1},-(x_1+\cdots+x_{k-1})\}$ of $\mathbb{F}_q$ for which $x_1,\dots,x_{k-1}$ are pairwise distinct and $-(x_1+\cdots+x_{k-1})$ is different from all the preceding elements, thereby reducing the equation (1) to a smaller number of unknowns. By further iterating this argument, this allows one to get a first-order linear recursive relation between $N(mp,0,\mathbb{F}_q)$ and $N((m-1)p,0,\mathbb{F}_q)$, which, by induction on m, produces the explicit expression for $N(mp,0,\mathbb{F}_q)$. Besides this general scheme, the rest of the proof is just a very easy exercise, which involves only elementary properties of the binomial coefficients.

Let us first introduce some notation. For any $1 \leq k \leq q$, let us denote by $\binom{\mathbb{F}_q}{k}$ the family of all the subsets of $\mathbb{F}_q$ of size k, that is,

$$\binom{\mathbb{F}_q}{k} = \{A \subseteq \mathbb{F}_q \,:\, |A| = k\}.$$

Also, for $1 \leq r \leq p-1$, if $\frac{1}{r}$ denotes the multiplicative inverse of r in $\mathbb{F}_p$, then we let $\Omega(k,r)$ be the family of all the subsets $\{x_1,\dots,x_k\}$ of $\mathbb{F}_q$ of size k that do not contain $-\frac{1}{r}(x_1+\cdots+x_k)$, that is,

$$\Omega(k,r) = \left\{ \{x_1,\dots,x_k\} \in \binom{\mathbb{F}_q}{k} \;\middle|\; \{x_1,\dots,x_k,-\frac{1}{r}(x_1+\cdots+x_k)\} \in \binom{\mathbb{F}_q}{k+1} \right\}.$$

We now consider the following preliminary result, which contains the main combinatorial "cell" of the whole proof.

2.1 Lemma: *If p is an odd prime, $2 \leq k \leq q$, and $1 \leq r \leq p-2$, then*

$$|\Omega(k,r)| = \binom{q}{k} - |\Omega(k-1,r+1)|\,.$$

Moreover, for $2 \leq k \leq q$, and for any prime p,

$$|\Omega(k-1,1)| = kN(k,0,\mathbb{F}_q).$$

Finally, if we let $N(0,0,\mathbb{F}_q) = 1$, then, for $1 \leq k \leq q$, and for any prime p,

$$|\Omega(k,p-1)| = \binom{q}{k} - (q-k+1)\,N(k-1,0,\mathbb{F}_q).$$

Proof. Let p be an odd prime, $2 \leq k \leq q$, and $1 \leq r \leq p-2$. Let $\{x_1,\dots,x_{k-1}\}$ be a $(k-1)$-subset of $\mathbb{F}_q$. Then, for any x_k in $\mathbb{F}_q$,

$$x_k = -\frac{1}{r+1}\,(x_1+\cdots+x_{k-1}) \iff x_k = -\frac{1}{r}\,(x_1+\cdots+x_{k-1}+x_k). \tag{4}$$

Let $\tau : \binom{\mathbb{F}_q}{k-1} \to \binom{\mathbb{F}_q}{k-1} \cup \binom{\mathbb{F}_q}{k}$ be the map defined by

$$\tau(\{x_1,\dots,x_{k-1}\}) = \{x_1,\dots,x_{k-1},\, -\frac{1}{r+1}\,(x_1+\cdots+x_{k-1})\}.$$

By (4), τ induces a map $\bar{\tau}$ from $\Omega(k-1,r+1)$ into $\binom{\mathbb{F}_q}{k}\backslash\Omega(k,r)$. We claim that $\bar{\tau}$ is injective and surjective. Indeed, let $\{x_1,\dots,x_k\}$ be in $\binom{\mathbb{F}_q}{k}\setminus\Omega(k,r)$. Then, by definition, $x_1,\dots,x_k$ are pairwise distinct, and $-\frac{1}{r}\,(x_1+\cdots+x_k) \in \{x_1,\dots,x_k\}$, hence there exists a unique $1 \leq i \leq k$ such that $x_i = -\frac{1}{r}\,(x_1+\cdots+x_k)$. Up to permutation, we may assume that $i=k$, whence, by (4), $\{x_1,\dots,x_{k-1}\} \in \Omega(k-1,r+1)$ and $\bar{\tau}(\{x_1,\dots,x_{k-1}\}) = \{x_1,\dots,x_k\}$. Moreover, $\{x_1,\dots,x_{k-1}\}$ is the only pre-image of $\{x_1,\dots,x_k\}$ under $\bar{\tau}$ by the uniqueness of i. This proves our claim. Hence $|\Omega(k,r)| = \binom{q}{k} - |\Omega(k-1,r+1)|$.

Also, for any prime p and $2 \leq k \leq q$, the map

$$\varphi(\{x_1,\dots,x_{k-1}\}) = \{x_1,\dots,x_{k-1},\, -(x_1+\cdots+x_{k-1})\}$$

is a surjective map from $\Omega(k-1,1)$ onto the family of all the k-subsets $\{x_1,\dots,x_k\}$ of $\mathbb{F}_q$ such that $x_1+\cdots+x_k = 0$. Moreover, for any such k-set $\{x_1,\dots,x_k\}$, $\varphi^{-1}(\{x_1,\dots,x_k\}) = \big\{\{x_1,\dots,x_k\}\setminus\{x_i\} \,\big|\, i=1,2,\dots,k\big\}$. Hence $N(k,0,\mathbb{F}_q) = \frac{1}{k}\,|\Omega(k-1,1)|$.

Finally, for any prime p, in the case where $r = p-1$ $(= -1$ in $\mathbb{F}_p)$, and $k \geq 2$, $\binom{\mathbb{F}_q}{k}\backslash\Omega(k,p-1)$ consists, by definition, of all the k-subsets $\{x_1,\dots,x_k\}$ of $\mathbb{F}_q$ such that $\sum_{j\neq i} x_j = 0$ for some (necessarily unique) $1 \leq i \leq k$. Hence $\binom{\mathbb{F}_q}{k}\setminus\Omega(k,p-1)$ consists of all the sets of the form $\{x_1,\dots,x_{k-1}\}\cup\{x_k\}$, where $\{x_1,\dots,x_{k-1}\}$ is a $(k-1)$-subset of $\mathbb{F}_q$ such that $x_1+\cdots+x_{k-1}=0$, and $x_k \notin \{x_1,\dots,x_{k-1}\}$. Therefore $\Omega(k,p-1)$ has precisely $\binom{q}{k} - (q-(k-1))\,N(k-1,0,\mathbb{F}_q)$ elements. This is true also for $k=1$, since $N(0,0,\mathbb{F}_q)=1$ and $|\Omega(1,p-1)|=0$ by definition.

The proof is now complete. □

Proof of Theorem 1.1. Let b be a given element of $\mathbb{F}_q$, and let $1 \leq k \leq q$. Let us first consider the case where $b=0$ and k is multiple of p, say $k=mp$. The crucial argument of the whole proof is finding a first-order linear recursive relation between $N(mp,0,\mathbb{F}_q)$ and $N((m-1)p,0,\mathbb{F}_q)$.

Let p be an odd prime. Then, by Lemma 2.1,

$$\begin{aligned} N(mp,0,\mathbb{F}_q) &= \frac{1}{mp}\left(\binom{q}{mp-1} - |\Omega(mp-2,2)|\right) \\ &= \frac{1}{mp}\left(\binom{q}{mp-1} - \binom{q}{mp-2} + |\Omega(mp-3,3)|\right). \end{aligned}$$

By further iterating the same argument, and applying again Lemma 2.1,

$$\begin{aligned} mp\,N(mp,0,\mathbb{F}_q) &= \binom{q}{mp-1} - \binom{q}{mp-2} + \cdots + (-1)^p\binom{q}{mp-p+1} \\ &\quad - (-1)^p(q-mp+p)\,N((m-1)p,0,\mathbb{F}_q), \end{aligned}$$

whence

$$mp\,N(mp,0,\mathbb{F}_q) = \binom{q-1}{mp-1} + (-1)^p\binom{q-1}{mp-p} - (-1)^p(q-mp+p)\,N((m-1)p,0,\mathbb{F}_q), \quad (5)$$

which is the desired first-order linear recursive relation. This relation can be easily derived from by Lemma 2.1 also in the case where $p=2$.

We can now prove the equality (2), for $b=0$ and k multiple of p, by induction on $m=k/p$. For $m=1$, by (5) and Lemma 2.1,

$$\begin{aligned} N(p,0,\mathbb{F}_q) &= \frac{1}{p}\left(\binom{q-1}{p-1} + (-1)^p - (-1)^p q\right) \\ &= \frac{1}{q}\binom{q}{p} + (-1)^{p+1}\,\frac{q-1}{q}\binom{q/p}{1}, \end{aligned}$$

hence (2) holds. If (2) is satisfied for $k=(m-1)p$ and $b=0$, then, by (5),

$$\begin{aligned} mp\,N(mp,0,\mathbb{F}_q) &= \binom{q-1}{mp-1} + (-1)^p\binom{q-1}{mp-p} + (-1)^{p+1}\,(q-mp+p)\,\frac{1}{q}\binom{q}{(m-1)p} \\ &\quad +(-1)^{p+1}\,(q-mp+p)\,(-1)^{(m-1)p+(m-1)}\,\frac{q-1}{q}\binom{q/p}{m-1} \\ &= \binom{q-1}{mp-1} + (-1)^p\binom{q-1}{mp-p} - (-1)^p\binom{q-1}{mp-p} \\ &\quad +(-1)^{mp+m}\,p\,(q/p-m+1)\,\frac{q-1}{q}\binom{q/p}{m-1}, \end{aligned}$$

whence

$$N(mp,0,\mathbb{F}_q) = \frac{1}{q}\binom{q}{mp} + (-1)^{mp+m}\,\frac{q-1}{q}\binom{q/p}{m},$$

that is, (2) holds for $k=mp$ and $b=0$. This completes the proof of the equality (2) in the case where $b=0$ and k is multiple of p.

Next, we claim that, if k is multiple of p, then $N(k,b,\mathbb{F}_q)$ is constant in b, as b ranges over $\mathbb{F}_q^*$. Indeed, if b_1, b_2 are two nonzero elements of $\mathbb{F}_q$, then, for any k-subset $\{x_1,\ldots,x_k\}$ of $\mathbb{F}_q$, $x_1+\cdots+x_k=b_2$ if and only if $b_1b_2^{-1}x_1+\cdots+b_1b_2^{-1}x_k=b_1$. Therefore, since the families

$\left\{\{x_1,\ldots,x_k\}\in\binom{\mathbb{F}_q}{k}\;\middle|\;\sum_{i=1}^k x_i=b\right\}$, as b ranges in $\mathbb{F}_q$, give a partition of $\binom{\mathbb{F}_q}{k}$, we conclude that, given any b in $\mathbb{F}_q^*$, $\binom{q}{k}=N(k,0,\mathbb{F}_q)+(q-1)N(k,b,\mathbb{F}_q)$, whence

$$\begin{aligned}N(k,b,\mathbb{F}_q) &= \frac{1}{q-1}\left(\binom{q}{k}-\frac{1}{q}\binom{q}{k}-(-1)^{k+k/p}\,\frac{q-1}{q}\binom{q/p}{k/p}\right)\\ &= \frac{1}{q}\binom{q}{k}+(-1)^{k+k/p}\,\frac{-1}{q}\binom{q/p}{k/p},\end{aligned}$$

that is, the equality (2) holds.

We now consider the case where k is not multiple of p. In this case, k is invertible mod p, and, for any $b\in\mathbb{F}_q$, the map $\{x_1,\ldots,x_k\}\mapsto\{x_1-\frac{1}{k}b,\ldots,x_k-\frac{1}{k}b\}$ is a bijection between the family of the k-subsets $\{x_1,\ldots,x_k\}$ of $\mathbb{F}_q$ such that $x_1+\cdots+x_k=b$, and the family of the k-subsets $\{y_1,\ldots,y_k\}$ of $\mathbb{F}_q$ such that $y_1+\cdots+y_k=0$, whence $N(k,b,\mathbb{F}_q)$ is constant in $b\in\mathbb{F}_q$. Since the above families of k-sets are a partition of $\binom{\mathbb{F}_q}{k}$, it follows that $|\binom{\mathbb{F}_q}{k}|=qN(k,b,\mathbb{F}_q)$ for any $b\in\mathbb{F}_q$, that is, the equality (2) holds.

Finally, it only suffices to prove that the equality (3) is satisfied. In order to do this, note that, for $2\le k\le q-1$,

$$N(k,b,\mathbb{F}_q^*)=N(k,b,\mathbb{F}_q)-N(k-1,b,\mathbb{F}_q^*). \tag{6}$$

This is an immediate consequence of the fact that the family of the k-subsets $\{x_1,\ldots,x_k\}$ of $\mathbb{F}_q$ such that $x_1+\cdots+x_k=b$ is the disjoint union of the family of the k-subsets $\{x_1,\ldots,x_k\}$ of $\mathbb{F}_q^*$ such that $x_1+\cdots+x_k=b$ with the family of all the subsets of $\mathbb{F}_q$ of size k containing zero, whose elements sum up to b. As the latter family is in one-to-one correspondence with the family of all the subsets of $\mathbb{F}_q^*$ of size $k-1$, whose elements sum up to b, the equality (6) follows.

We can now prove the equality (3) by induction on k. For $k=1$, $N(k,b,\mathbb{F}_q^*)$ is equal to 1 (resp., to 0) if $b\neq 0$ (resp., if $b=0$), hence (3) holds. Let us now assume that (3) is satisfied when k is replaced by $k-1$, for some $2\le k\le q-1$. If p does not divide k, then $\lfloor k/p\rfloor=\lfloor(k-1)/p\rfloor$, hence, by (6) and (2),

$$\begin{aligned}N(k,b,\mathbb{F}_q^*) &= \frac{1}{q}\binom{q}{k}-\frac{1}{q}\binom{q-1}{k-1}-(-1)^{k-1+\lfloor(k-1)/p\rfloor}\,\frac{v(b)}{q}\binom{q/p-1}{\lfloor(k-1)/p\rfloor}\\ &= \frac{1}{q}\binom{q-1}{k}+(-1)^{k+\lfloor k/p\rfloor}\,\frac{v(b)}{q}\binom{q/p-1}{\lfloor k/p\rfloor},\end{aligned}$$

that is, the equality (3) holds. Finally, if p divides k, then $\lfloor(k-1)/p\rfloor=k/p-1$, hence, by (6) and (2),

$$\begin{aligned}N(k,b,\mathbb{F}_q^*) &= \frac{1}{q}\binom{q}{k}+(-1)^{k+k/p}\,\frac{v(b)}{q}\binom{q/p}{k/p}\\ &\quad -\frac{1}{q}\binom{q-1}{k-1}-(-1)^{k-1+k/p-1}\,\frac{v(b)}{q}\binom{q/p-1}{k/p-1}\\ &= \frac{1}{q}\binom{q-1}{k}+(-1)^{k+k/p}\,\frac{v(b)}{q}\binom{q/p-1}{k/p},\end{aligned}$$

that is, the equality (3) holds.

This completes the proof of the theorem. □

References

[1] A. Caggegi, G. Falcone, M. Pavone, On the additivity of block designs, *J. Algebr. Comb.* **45**, 271–294 (2017).

[2] A. Caggegi, G. Falcone, M. Pavone, Additivity of affine designs, *J. Algebr. Comb.* **53**, 755–770 (2021).

[3] Q. Cheng, E. Murray, On deciding deep holes of Reed-Solomon codes, In: TAMS 2007, Lecture Notes in Computer Science, Vol. 4484, Springer (2007).

[4] G. Diderrich, An addition theorem for abelian groups of order pq, *J. Number Theory* **7**, 33–48 (1975).

[5] P. Erdös, H. Heilbronn: On the addition of residue classes mod p, *Acta Arithm.* **9**, 149–159 (1964).

[6] T. Etzion, A. Vardy, Perfect binary codes: constructions, properties, and enumeration, *IEEE Trans. Inf. Theory* **40** (3), 754–763 (1994).

[7] G. Falcone, M. Pavone, Permutations of zero-sumsets in a finite vector space, *Forum Math.* **33** (2), 349–359 (2021).

[8] G. Falcone, M. Pavone, Binary Hamming codes and Boolean designs, *Des. Codes Crypt.* **89**, 1261–1277 (2021).

[9] M. Kosters, The subset sum problem for finite abelian groups, *J. Combin. Theory, Ser. A* **120** (3), 527–530 (2013).

[10] J. Li, D. Wan, On the subset sum problem over finite fields, *Finite Fields Appl.* **14** (4), 911–929 (2008).

[11] J. Li, D. Wan, Counting subset sums of finite abelian groups, *J. Combin. Theory, Ser. A* **119** (1), 170–182 (2012).

[12] M. Pavone, On the weight distribution of perfect binary codes, *J. Discret. Math. Sci. Cryptogr.*, DOI : 10.1080/09720529.2021.1932898.

[13] M. Pavone, Subset sums and block designs in a finite vector space (submitted).

[14] H. S. Shapiro, D. L. Slotnick, On the mathematical theory of error-correcting codes, *IBM J. Res. Dev.* **3** (1), 25–34 (1959).