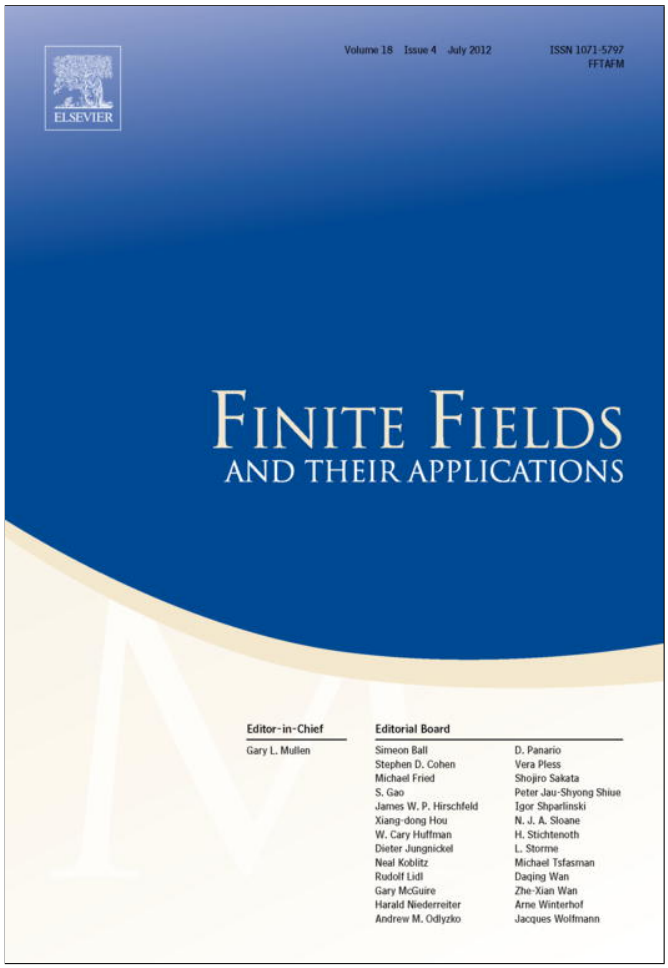

Finite Fields and Their Applications 18 (2012) 791–799

Contents lists available at SciVerse ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

Power sums over subspaces of finite fields

David B. Chandler [b], Junhua Wu [a,2], Qing Xiang [b,*,1]

[a] Department of Mathematics, Lane College, Jackson, TN 38301, USA
[b] Department of Mathematical Sciences, University of Delaware, Newark, DE 19716, USA

ARTICLE INFO

Article history:
Received 31 August 2011
Revised 16 December 2011
Accepted 11 April 2012
Available online 25 April 2012
Communicated by L. Storme

MSC:
05B25
11T24
11T71

Keywords:
Code
p-rank
Power sum
Rank

ABSTRACT

Let K be the finite field of order q^{m+1}, which is regarded as an $(m+1)$-dimensional vector space over $\mathbb{F}_q$. For each h-dimensional $\mathbb{F}_q$-subspace V of K, $\alpha \in K$ and $0 \leqslant t \leqslant q^{m+1}-1$, we define $S_t(V,\alpha) = \sum_{v\in V}(\alpha+v)^t$. For each $1 \leqslant h \leqslant m$, we obtain sufficient conditions on t for the vanishing of $S_t(V,\alpha)$; when $h = m$, combining this result with some p-rank results from coding theory, we obtain necessary and sufficient conditions on t for the vanishing of $S_t(V,\alpha)$.

1. Introduction

Let K be the finite field of order q^{m+1}, where $q = p^e$ is a prime power and $m \geqslant 0$. It is a well-known and very useful fact that

$$\sum_{v\in K} v^t = \begin{cases} 0, & \text{if } t \not\equiv 0 \pmod{q^{m+1}-1} \text{ or } t = 0, \\ -1, & \text{if } t \equiv 0 \pmod{q^{m+1}-1} \text{ and } t > 0. \end{cases}$$

* Corresponding author.
E-mail addresses: davidbchandler@gmail.com (D.B. Chandler), jwu@lanecollege.edu (J. Wu), xiang@math.udel.edu (Q. Xiang).

[1] Research supported in part by NSF Grant DMS 1001557.
[2] Research supported in part by NSF HBCU-UP Grant Award 0929257 at Lane College.

1071-5797/$ – see front matter
http://dx.doi.org/10.1016/j.ffa.2012.04.002

Here we have used the convention that $0^0 = 1$. In connection to this fact, the following question arises naturally. If we restrict the range of the above summation to some subset of K instead of K itself, is it possible to determine for which t the sum vanishes? Probably the most natural subsets to consider are the $\mathbb{F}_q$-subspaces of K, which is now viewed as an $(m+1)$-dimensional vector space over $\mathbb{F}_q$.

Let V be a nonzero $\mathbb{F}_q$-subspace of K. For each $0 \leqslant t \leqslant q^{m+1} - 1$ and $\alpha \in K$, we define

$$S_t(V, \alpha) = \sum_{v \in V} (v + \alpha)^t. \tag{1.1}$$

These sums arose in an investigation of the integral Galois module structure of certain extensions of p-adic fields [4]. They also arose, at least in some special cases, in the study of zeros and nonzeros of certain cyclic codes from finite geometry. In the case where $e = 1$ (i.e., $q = p$ is a prime) and V is an m-dimensional subspace of K, Byott and Chapman [5] give necessary and sufficient conditions for the vanishing of $S_t(V, \alpha)$ in terms of the digit sum of t. In the same paper, the authors also collect some conditions on t under which the sum in (1.1) vanishes in the case where $e \geqslant 1$ and V is an m-dimensional $\mathbb{F}_q$-subspace of K.

In this paper we consider the problem of vanishing or nonvanishing of the sum $S_t(V, \alpha)$ in the general case where $e \geqslant 1$ and V is an arbitrary nonzero $\mathbb{F}_q$-subspace of K. When V is an arbitrary nonzero $\mathbb{F}_q$-subspace of K, we give sufficient conditions on t for the vanishing of the sum in (1.1). Moreover, when V is an m-dimensional $\mathbb{F}_q$-subspace of K, we give necessary and sufficient conditions for the vanishing of the sum in (1.1). It is clear that $S_{q^{m+1}-1}(V, \alpha) = -1$ or 0 according as $\alpha \in V$ or $\alpha \notin V$. So we only need to consider those t such that $0 \leqslant t \leqslant q^{m+1} - 2$. To state our theorem, we need some notation. For $0 \leqslant t \leqslant q^{m+1} - 2$, let $t = \sum_{i=0}^{m} t_i q^i$ be the base-q expansion of t, where $0 \leqslant t_i \leqslant q - 1$. For each $1 \leqslant \ell \leqslant e$, we define

$$s_\ell(t) := \frac{1}{q-1} \sum_{i=0}^{m} \sigma_q\big(p^{e-\ell} t_i\big), \tag{1.2}$$

where $\sigma_q(x)$ is the base-q digit sum of x. We remark that the e-tuples $(s_1(t), s_2(t), \ldots, s_e(t))$ are similar to the twisted degrees which appeared in [6] and [3]. For future use we also denote by $\sigma(x)$ the base-p digit sum of x, where x is a nonnegative integer. Now we can state our main result.

Theorem 1.1. *Let K be the finite field of order q^{m+1}, where $m \geqslant 0$ and $q = p^e$ is a prime power with $e \geqslant 1$. Let $1 \leqslant h \leqslant m$, and V be an h-dimensional $\mathbb{F}_q$-subspace of K. For $0 \leqslant t \leqslant q^{m+1} - 2$ and $\alpha \in K$, let $S_t(V, \alpha)$ be the sum defined in* (1.1)*.*

(i) *When $\alpha \in V$, we have $S_t(V, \alpha) = 0$ if $(q-1) \nmid t$ or $s_\ell(t) < h$ for some $1 \leqslant \ell \leqslant e$. When $\alpha \notin V$, we have $S_t(V, \alpha) = 0$ if $s_\ell(t) < h$ for some $1 \leqslant \ell \leqslant e$.*
(ii) *Assume that $h = m$. Let $\alpha \in V$. Then $S_t(V, \alpha) = 0$ if and only if either $(q-1) \nmid t$ or $s_\ell(t) < m$ for some $1 \leqslant \ell \leqslant e$. Suppose now $\alpha \notin V$. Then $S_t(V, \alpha) = 0$ if and only if $s_\ell(t) < m$ for some $1 \leqslant \ell \leqslant e$.*

We remark that our approach to the proof of Theorem 1.1 is completely different from the one used in [5]. The approach in [5] started by considering the generating function of $(S_t(V, \alpha))_{t \geqslant 0}$. Therefore it can be viewed as external. Our approach is internal in the sense that we try to expand the sum $S_t(V, \alpha)$ in a certain way. When $e = 1$, i.e., $q = p$ is a prime, if V is an m-dimensional $\mathbb{F}_q$-subspace of K, using (ii) of Theorem 1.1 and noting that $S_{p^{m+1}-1}(V, \alpha) = -1$ or 0 according as $\alpha \in V$ or $\alpha \notin V$, we have the following corollary, which is one of the main results in [5].

Corollary 1.2. *(See [5, Theorem 2].) Let $K = \mathbb{F}_{p^{m+1}}$, let V be an m-dimensional $\mathbb{F}_p$-subspace of K, and let $0 \leqslant t \leqslant p^{m+1} - 1$.*

(i) *Suppose* $\alpha \in K \setminus V$. *Then* $S_t(V,\alpha) \neq 0$ *if and only if* $(p-1)m \leqslant \sigma(t) < (p-1)(m+1)$.
(ii) *Suppose* $\alpha \in V$. *Then* $S_t(V,\alpha) \neq 0$ *if and only if* $\sigma(t) = (p-1)m$ *or* $t = p^{m+1}-1$.

We give a brief overview of the paper. In Section 2, we give the proof of part (i) of Theorem 1.1. We expand $S_t(V,\alpha)$ and show that if the conditions of the theorem are met, then every term in the expansion vanishes. In Section 3, we give the proof of part (ii) of Theorem 1.1. The proof is done by combining the result in part (i) of Theorem 1.1 and some p-rank results from coding theory.

2. Proof of the first part of Theorem 1.1

In this section we give a proof of Theorem 1.1(i). The ideas of the proof are similar to those in the proof of Wan's Theorem [7, Theorem 1.3].

Proof of Theorem 1.1(i). Let $t = t_0 + t_1 q + \cdots + t_m q^m$ be the base-q expansion of t, and let $\{x_1, x_2, \ldots, x_h\}$ be an $\mathbb{F}_q$-basis of V. We have

$$\begin{aligned} S_t(V,\alpha) &= \sum_{r_1,r_2,\ldots,r_h \in \mathbb{F}_q} (r_1x_1 + r_2x_2 + \cdots + r_hx_h + \alpha)^t \\ &= \sum_{r_1,r_2,\ldots,r_h \in \mathbb{F}_q} \prod_{i=0}^{m} \left(r_1x_1^{q^i} + r_2x_2^{q^i} + \cdots + r_hx_h^{q^i} + \alpha^{q^i}\right)^{t_i} \end{aligned}$$

because elements of $\mathbb{F}_q$ are fixed when raised to the power q. Then

$$\begin{aligned} S_t(V,\alpha) = \sum_{\substack{t_i = k_{i,1} + k_{i,2} + \cdots + k_{i,h+1} \\ 0 \leqslant i \leqslant m}} \prod_{i=0}^{m} \binom{t_i}{k_{i,1}, k_{i,2}, \ldots, k_{i,h+1}} \left(\prod_{j=1}^{h} x_j^{\sum_{i=0}^{m} q^i k_{i,j}}\right) \\ \cdot \prod_{j=1}^{h} \left(\sum_{r_j \in \mathbb{F}_q} r_j^{\sum_{i=0}^{m} k_{i,j}}\right) \cdot \alpha^{\sum_{i=0}^{m} q^i k_{i,h+1}}. \end{aligned} \tag{2.1}$$

Using Legendre's formula, $\nu_p(r!) = \frac{r - \sigma(r)}{p-1}$ (here ν_p is the p-adic valuation function), we find that the p-adic valuation of the product of the multinomial coefficients in (2.1) is

$$\frac{1}{p-1} \sum_{i=0}^{m} \left(t_i - \sigma(t_i) - \sum_{j=1}^{h+1} \left(k_{i,j} - \sigma(k_{i,j})\right)\right) = \frac{1}{p-1} \sum_{i=0}^{m} \left(\sum_{j=1}^{h+1} \sigma(k_{i,j}) - \sigma(t_i)\right). \tag{2.2}$$

We will show that if $s_\ell(t) < h$ for some ℓ, $1 \leqslant \ell \leqslant e$, then the quantity in the right-hand side of (2.2) is positive, implying that the corresponding term in the expansion (2.1) of $S_t(V,\alpha)$ is zero.

We start by noting that

$$\sum_{x \in \mathbb{F}_q} x^r = \begin{cases} 0, & \text{if } (q-1) \text{ does not divide } r, \\ 0, & \text{if } r = 0, \\ -1, & \text{if } (q-1) \mid r \text{ and } r > 0. \end{cases} \tag{2.3}$$

Therefore in (2.1) we only need to consider those terms for which

$$\sum_{i=0}^{m} k_{i,j} \equiv 0 \pmod{q-1} \quad \text{and} \quad \sum_{i=0}^{m} k_{i,j} > 0 \tag{2.4}$$

for all $j = 1, 2, \ldots, h$. Since $r \equiv \sigma_q(r) \pmod{q-1}$, we see that the congruence in (2.4) implies

$$\sum_{i=0}^{m} \sigma_q(k_{i,j}) \equiv 0 \pmod{q-1} \tag{2.5}$$

for all $j = 1, 2, \ldots, h$. Given nonnegative integers $k_{i,j}$ such that $\sum_{j=1}^{h+1} k_{i,j} = t_i$ for $0 \leqslant i \leqslant m$ and (2.4) is satisfied for each j, $1 \leqslant j \leqslant h$, we consider the following vector of length $h+1$

$$\left(\sum_{i=0}^{m} k_{i,1}, \sum_{i=0}^{m} k_{i,2}, \ldots, \sum_{i=0}^{m} k_{i,h+1} \right). \tag{2.6}$$

The first h entries of the vector in (2.6) are nonzero by assumption. It follows that the corresponding entries of the following vector

$$\left(\sum_{i=0}^{m} \sigma_q(k_{i,1}), \sum_{i=0}^{m} \sigma_q(k_{i,2}), \ldots, \sum_{i=0}^{m} \sigma_q(k_{i,h+1}) \right) \tag{2.7}$$

are at least $(q-1)$.

Therefore we have

$$h(q-1) - \sum_{i=0}^{m} t_i \leqslant \sum_{i=0}^{m} \left(\sum_{j=1}^{h+1} \sigma_q(k_{i,j}) - t_i \right). \tag{2.8}$$

For any nonnegative integer ℓ, we note that (2.5) still holds with $\sigma_q(k_{i,j})$ replaced by $\sigma_q(p^\ell k_{i,j})$. Also $\sum_{i=0}^{m} \sigma_q(p^\ell k_{i,j})$ is still nonzero for the first h subscripts of j. Thus we have

$$h(q-1) - \sum_{i=0}^{m} \sigma_q\big(p^\ell t_i\big) \leqslant \sum_{i=0}^{m} \left(\sum_{j=1}^{h+1} \sigma_q\big(p^\ell k_{i,j}\big) - \sigma_q\big(p^\ell t_i\big) \right). \tag{2.9}$$

Since $\sum_{j=1}^{h+1} k_{i,j} = t_i$ the right-hand side of the above inequality is nonnegative; we sum over ℓ to get

$$\sum_{\ell=0}^{e-1} \max\left\{ 0, h(q-1) - \sum_{i=0}^{m} \sigma_q\big(p^\ell t_i\big) \right\} \leqslant \frac{q-1}{p-1} \sum_{i=0}^{m} \left(\sum_{j=1}^{h+1} \sigma(k_{i,j}) - \sigma(t_i) \right). \tag{2.10}$$

Here we have used the fact that $\sum_{\ell=0}^{e-1} \sigma_q(p^\ell r) = \frac{q-1}{p-1} \sigma(r)$. Recall that by definition (1.2), $s_\ell = \frac{1}{q-1} \sum_{i=0}^{m} \sigma_q(p^{e-\ell} t_i)$. We see that the left-hand side of (2.10) is

$$\sum_{\ell=0}^{e-1} \max\big\{0, (q-1)\big(h - s_{e-\ell}(t)\big)\big\}.$$

If $s_\ell(t) < h$ for some $1 \leqslant \ell \leqslant e$, then by (2.10), we have

$$\sum_{i=0}^{m} \left(\sum_{j=1}^{h+1} \sigma(k_{i,j}) - \sigma(t_i) \right) > 0;$$

it follows that the corresponding term in the right-hand side of (2.1) is zero. Therefore we have shown that if $s_\ell(t) < h$ for some $1 \leqslant \ell \leqslant e$ then $S_t(V, \alpha) = 0$.

Finally when $\alpha \in V$, we have $S_t(V, \alpha) = S_t(V, 0)$. Let θ be a primitive element of $\mathbb{F}_q$. Then

$$S_t(V, 0) = S_t(\theta V, 0) = \theta^t S_t(V, 0).$$

If $t \not\equiv 0 \pmod{q-1}$ then $\theta^t \neq 1$, and thus $S_t(V, \alpha) = 0$.

The proof of Theorem 1.1(i) is now complete. □

3. Proof of the second part of Theorem 1.1

In this section, we always assume that V is an m-dimensional $\mathbb{F}_q$-subspace of K; it follows that $|V| = q^m$. In this case, using some results from coding theory, we prove that the conditions in Theorem 1.1(i) are indeed necessary for the vanishing of (1.1). We start by counting the sizes of two important sets that will be used later.

Let

$$N := \left\{ t \;\middle|\; 0 \leqslant t \leqslant q^{m+1} - 2,\ s_\ell(t) \geqslant m \text{ for each } 1 \leqslant \ell \leqslant e \right\} \tag{3.1}$$

and

$$N' := \left\{ t \;\middle|\; t \in N \text{ and } (q-1) \mid t \right\}. \tag{3.2}$$

Lemma 3.1. *Using the above notation, we have*

$$|N| = \binom{m+p}{m+1}^e - 1 \quad \textit{and} \quad |N'| = \binom{m+p-1}{m}^e.$$

Proof. Let $t = \sum_{i=0}^{m} t_i q^i$ be the base-q expansion of t. It is clear that $s_\ell(q^{m+1} - 1) = m + 1$ and

$$\begin{aligned} s_\ell\left(q^{m+1} - 1 - t\right) &= \frac{1}{q-1} \sum_{i=0}^{m} \sigma_q\left(p^{e-\ell}(q - 1 - t_i)\right) \\ &= \frac{1}{q-1} \sum_{i=0}^{m} \sigma_q\left(p^{e-\ell}(q-1)\right) - \frac{1}{q-1} \sum_{i=0}^{m} \sigma_q\left(p^{e-\ell} t_i\right) \\ &= m + 1 - s_\ell(t) \end{aligned}$$

for each $1 \leqslant \ell \leqslant e$. This implies that $s_\ell(t) \geqslant m$ if and only if $s_\ell(q^{m+1} - 1 - t) \leqslant 1$. Consequently the sets

$$M := \left\{ t \;\middle|\; 1 \leqslant t \leqslant q^{m+1} - 1,\ s_\ell(t) \leqslant 1 \text{ for each } 1 \leqslant \ell \leqslant e \right\}$$

and

$$M' := \left\{ t \;\middle|\; t \in M \text{ and } (q-1) \mid t \right\}$$

are of the same sizes as the sets N and N', respectively. The rest is to count the sizes of M and M'.

Let $t \in M$, $t = \sum_{i=0}^{m} t_i q^i$, $0 \leqslant t_i \leqslant q-1$, $\forall i$, and let $t_i = t_{i,0} + t_{i,1}p + \cdots + t_{i,e-1}p^{e-1}$ be the base-p expansion of t_i for $0 \leqslant i \leqslant m$, where $0 \leqslant t_{i,j} \leqslant p-1$. If

$$\sum_{i=0}^{m} t_{i,k} \geqslant p$$

for some $0 \leqslant k \leqslant e-1$, then

$$\begin{aligned} s_{k+1}(t) &= \frac{1}{q-1}\sum_{i=0}^{m} \sigma_q\big(p^{e-1-k}t_i\big) \\ &\geqslant \frac{1}{q-1}\sum_{i=0}^{m} t_{i,k}p^{e-1} \\ &\geqslant \frac{p\cdot p^{e-1}}{q-1} > 1, \end{aligned}$$

which is not the case by the choice of t. Therefore we must have

$$\sum_{i=0}^{m} t_{i,j} \leqslant p-1, \quad 0 \leqslant j \leqslant e-1. \tag{3.3}$$

On the other hand, if (3.3) is satisfied and $t \neq 0$, then $t \in M$. Thus, $|M|$ is one less than the number of ways to distribute $(p-1)$ indistinguishable balls into $(m+2)$ labeled boxes, e consecutive times. The first result follows.

If (3.3) is satisfied but the inequality is strict for some j, then $\sigma_q(t) < q-1$, which means $t \notin M'$ since $\sigma_q(t) \equiv t \pmod{q-1}$. Hence to get the second result we distribute $(p-1)$ indistinguishable balls into only $(m+1)$ labeled boxes, e consecutive times.

The proof of the lemma is now complete. □

Recall that K is the finite field of order q^{m+1}. In the rest of the article, we will always use G to denote the multiplicative group K^* of K; that is, $G = \langle \xi \rangle$ is a cyclic group of order $q^{m+1}-1$, where ξ is a primitive element of K. It is well known that all the irreducible K-characters of G are linear and form the following set

$$\hat{G} = \big\{ \chi_i \,\big|\, 0 \leqslant i \leqslant q^{m+1}-2 \big\},$$

where $\chi_i(\xi^j) = \xi^{ji}$; in particular, χ_0 is the trivial character of G.

Let $B = \sum_{g\in G} b_g g$ be an element in the group algebra $K[G]$. We associate with B a square matrix $(b_{h^{-1}g})$ whose rows and columns are indexed by $h \in G$ and $g \in G$, respectively. The rank of $(b_{h^{-1}g})$ over K is defined to be the *rank* of B. The following result is well known.

Lemma 3.2. *(See [2, Theorem 3.3].) Let $B = \sum_{g\in G} b_g g \in K[G]$. Then the rank of B is equal to the number of K-characters $\chi \in \hat{G}$ such that $\chi(B) = \sum_{g\in G} b_g \chi(g) \neq 0$.*

Now we remind the reader that V is an m-dimensional $\mathbb{F}_q$-subspace of K; that is, V is a hyperplane through the origin of K regarded as an $\mathbb{F}_q$-vector space. For convenience, we define the following two sets:

$$\mathcal{H} := \{U \mid U \text{ is a codimension-1 subspace of } K\} \tag{3.4}$$

and

$$\mathcal{H}' := \{r + U \mid U \in \mathcal{H},\ r \notin U\}, \tag{3.5}$$

where $r+U = \{r+u \mid u \in U\}$. Let $g \in G$. We define $gU = \{gu \mid u \in U\}$ and $g(r+U) = \{gr+gu \mid u \in U\}$. Then G acts on each of $\mathcal{H}$ and $\mathcal{H}'$.

Lemma 3.3. *Using the above notation, G acts transitively on each of $\mathcal{H}$ and $\mathcal{H}'$.*

Proof. Let $\mathrm{Tr}_{q^{m+1}/q} : \mathbb{F}_{q^{m+1}} \to \mathbb{F}_q$ be the trace map. Every hyperplane of K through the origin has the form $\{\beta\colon\ \mathrm{Tr}_{q^{m+1}/q}(g\beta) = 0\}$ for some $g \in G$. Every hyperplane of K not through the origin has the form $\{\beta\colon\ \mathrm{Tr}_{q^{m+1}/q}(g\beta) = 1\}$ for some $g \in G$. Thus G acts transitively on each of $\mathcal{H}$ and $\mathcal{H}'$. □

Let $\mathbf{1}_{|K|}$ denote the all-1 row vector indexed by K. We define the following matrices:

- **A** is the incidence matrix between the elements of $\mathcal{H}$ and G; that is, **A** is a $(0,1)$-matrix whose rows and columns are labeled by the elements of $\mathcal{H}$ and G, respectively; the (U, g)-entry of **A** is 1 if and only if $g \in U$.
- **B** is the incidence matrix between the elements of $\mathcal{H} \cup \mathcal{H}'$ and K.
- **C** is the incidence matrix between the elements of $\mathcal{H}'$ and K.
- **C**′ is the matrix obtained from **C** by deleting the column of **C** indexed by 0.
- **H** is obtained by adjoining to **C** the row $\mathbf{1}_{|K|}$.

As defined, **B** is the incidence matrix between the hyperplanes and the points of $\mathrm{AG}(m+1, q)$ (the affine space of dimension $m+1$ whose hyperplanes are the cosets of subspaces of dimension m and whose points are the element of K). Then **C** is the incidence matrix between the hyperplanes not through the origin and the points of $\mathrm{AG}(m+1, q)$. The p-rank of a matrix is its rank over any field of characteristic p which contains all the entries of the matrix. For a matrix **E** with entries in K, we let $\mathbf{rk}_p(\mathbf{E})$ denote the p-rank of the matrix **E**.

Lemma 3.4. *Using the above notation, we have*

(i) $\mathbf{rk}_p(\mathbf{A}) = \binom{m+p-1}{m}^e + 1$;
(ii) $\mathbf{rk}_p(\mathbf{B}) = \binom{m+p}{m+1}^e$;
(iii) $\mathbf{rk}_p(\mathbf{C}') = \mathbf{rk}_p(\mathbf{C}) = \binom{m+p}{m+1}^e - 1$.

Proof. Let **D** be the incidence matrix of the hyperplanes and points of $\mathrm{PG}(m, q)$, the finite projective space of dimension m. By [1, Theorem 5.7.1], we have that $\mathbf{rk}_p(\mathbf{D}) = \binom{m+p-1}{m}^e + 1$. Deleting the duplicated columns of **A**, we obtain **D**. Thus $\mathbf{rk}_p(\mathbf{A}) = \mathbf{rk}_p(\mathbf{D}) = \binom{m+p-1}{m}^e + 1$.

By [1, Corollary 5.7.1], it follows that $\mathbf{rk}_p(\mathbf{B}) = \binom{m+p}{m+1}^e$. It remains to establish (iii).

First we note that all the entries in the column of **C** indexed by 0 are zero since no element in $\mathcal{H}'$ contains 0. Therefore, $\mathbf{rk}_p(\mathbf{C}') = \mathbf{rk}_p(\mathbf{C})$. Let B_W denote the row of **B** indexed by $W \in \mathcal{H} \cup \mathcal{H}'$. Since

$$B_U + \sum_{V \in C(U)} B_V = \mathbf{1}_{|K|}$$

for each $U \in \mathcal{H}$, where $C(U) = \{r + U \mid r \in K,\ r \notin U\}$, it is clear that the row span of **H** is the same as that of **B**. Since the entries of the column of **C** indexed by 0 are all zero, $\mathbf{1}_{|K|}$ is not contained in the

span of the rows of **C**. We have proved that

$$\mathbf{rk}_p\left(\mathbf{C}'\right) = \mathbf{rk}_p(\mathbf{C}) = \mathbf{rk}_p(\mathbf{B}) - 1 = \mathbf{rk}_p(\mathbf{H}) - 1 = \binom{m+p}{m+1}^e - 1. \qquad \square$$

Proof of Theorem 1.1(ii). Let $V \subset K$ be an $\mathbb{F}_q$-subspace of dimension m. We first consider the sums $S_t(V, \alpha)$ with $\alpha \in V$. In this case, we clearly have $S_t(V, \alpha) = S_t(V, 0)$.

Define

$$Z' := \left\{ t \mid 0 \leqslant t \leqslant q^{m+1} - 2,\ s_\ell(t) < m \text{ for some } 1 \leqslant \ell \leqslant e \text{ or } q - 1 \nmid t \right\}$$

and

$$Z_1 := \left\{ t \mid 0 \leqslant t \leqslant q^{m+1} - 2,\ S_t(V, 0) = 0 \right\}.$$

By part (i) of Theorem 1.1, we have $Z' \subseteq Z_1$. From Lemma 3.1, we have

$$\left|Z'\right| = q^{m+1} - 1 - \left|N'\right| = q^{m+1} - 1 - \binom{m+p-1}{m}^e, \tag{3.6}$$

where N' is the set defined in (3.2). Consider $B = \sum_{v \in V^*} v \in K[G]$, where $V^* = V \setminus \{0\}$. Since G is transitive on $\mathcal{H}$ by Lemma 3.3, it is clear that, up to permutations of rows and columns and repetition of rows, the matrix associated with B is equal to **A**. By Lemma 3.2, we know that the number of characters in $\hat{G} = \{\chi_t \mid 0 \leqslant t \leqslant q^{m+1} - 2\}$ satisfying

$$\chi_t(B) = \sum_{v \in V^*} \chi_t(v) = \sum_{v \in V^*} v^t \neq 0$$

is equal to $\mathbf{rk}_p(\mathbf{A})$, which in turn is equal to $\binom{m+p-1}{m}^e + 1$ by Lemma 3.4. Furthermore, since when $t = 0$, $\chi_0(B) = q^m - 1 \neq 0$ but $\sum_{v \in V} v^0 = q^m = 0$, we conclude that the number of t with $0 \leqslant t \leqslant q^{m+1} - 2$ satisfying

$$S_t(V, 0) = \sum_{v \in V} v^t \neq 0$$

is $\binom{m+p-1}{m}^e$, and $|Z_1| = q^{m+1} - 1 - \binom{m+p-1}{m}^e$. With (3.6) and $Z' \subseteq Z_1$, we obtain that $Z' = Z_1$. The proof of the first part of Theorem 1.1(ii) is complete.

Next let $\alpha \notin V$. We define

$$Z := \left\{ t \mid 0 \leqslant t \leqslant q^{m+1} - 2,\ s_\ell(t) < m \text{ for some } 1 \leqslant \ell \leqslant e \right\}$$

and

$$Z_2 := \left\{ t \mid 0 \leqslant t \leqslant q^{m+1} - 2,\ S_t(V, \alpha) = 0 \right\}.$$

By part (i) of Theorem 1.1, we have $Z \subseteq Z_2$. From Lemma 3.1, it follows that

$$|Z| = q^{m+1} - 1 - |N| = q^{m+1} - \binom{m+p}{m+1}^e, \tag{3.7}$$

where N is the set defined in (3.1). Let $B \in K[G]$ be the element corresponding to the subset $\{\alpha + v \mid v \in V\}$ of G. That is, $B = \sum_{g \in G} b_g g$, where $b_g = 1$ if $g \in \{\alpha + v \mid v \in V\}$ and $b_g = 0$ otherwise. Since G is transitive on $\mathcal{H}'$ by Lemma 3.3, it is clear that, up to permutations of rows and columns, the matrix associated with B is equal to $\mathbf{C}'$. By Lemma 3.2, we know that the number of characters in $\hat{G} = \{\chi_t \mid 0 \leqslant t \leqslant q^{m+1} - 2\}$ satisfying

$$\chi_t(B) = \sum_{v \in V} \chi_t(\alpha + v) = \sum_{v \in V} (\alpha + v)^t \neq 0$$

is equal to $\mathbf{rk}_p(\mathbf{C}')$, which by Lemma 3.4(iii) in turn is equal to $\binom{m+p}{m+1}^e - 1$. Consequently, the number of t with $0 \leqslant t \leqslant q^{m+1} - 2$ satisfying

$$S_t(V, \alpha) = \sum_{v \in V} (\alpha + v)^t = 0$$

equals $q^{m+1} - \binom{m+p}{m+1}^e$, or equivalently, $|Z_2| = q^{m+1} - \binom{m+p}{m+1}^e$. With (3.7) and $Z \subseteq Z_2$, we obtain that $Z = Z_2$. The proof of the second part of Theorem 1.1(ii) is now complete. □

Remark 3.5. It is natural to ask whether one can obtain necessary and sufficient conditions on t such as those in part (ii) of Theorem 1.1 for the vanishing of $S_t(V, \alpha)$ when the dimension of V is less than m. We believe that the answer to this question is negative. The reason is that while G acts transitively on $\mathcal{H}$, it does not act transitively on the set of h-dimensional $\mathbb{F}_q$-subspaces of K, where $1 < h < m$.

References

[1] E.F. Assmus Jr., J.D. Key, Designs and Their Codes, Cambridge University Press, New York, 1992.
[2] J. MacWilliams, H.B. Mann, On the p-rank of the design matrix of a difference set, Inform. Control 12 (1968) 474–488.
[3] M. Bardoe, P. Sin, The permutation modules for $\mathrm{GL}(n+1, \mathbb{F}_q)$ acting on $\mathbb{P}^n(\mathbb{F}_q)$ and $\mathbb{F}_q^{n+1}$, J. Lond. Math. Soc. 61 (2000) 58–80.
[4] N.P. Byott, Integral Galois module structure of some Lubin–Tate extensions, J. Number Theory 77 (1999) 252–273.
[5] N.P. Byott, R.J. Chapman, Power sums over finite subspaces of a field, Finite Fields Appl. 5 (1999) 254–265.
[6] N. Hamada, The rank of the incidence matrix of points and d-flats in finite geometries, J. Sci. Hiroshima Univ. Ser. A-I 32 (1968) 381–396.
[7] D. Wan, A Chevalley–Warning approach to p-adic estimates of character sums, Proc. Amer. Math. Soc. 123 (1995) 45–54.