A Problem on Linear Functions and Subsets of a Finite Field

W.S. Ng

Institute of Mathematical Sciences
University of Malaya
50603 Kuala Lumpur
Malaysia
E-mail: *ng_wei_shean@hotmail.com*

Abstract

Let $g : \mathbb{F}^m \to \mathbb{F}$ be a linear function on the vector space $\mathbb{F}^m$ over a finite field $\mathbb{F}$. A subset $S \subsetneq \mathbb{F}$ is called *g-thin* iff $g(S^m) \subsetneq \mathbb{F}$. In case $\mathbb{F}$ is the field $\mathbb{Z}_p$ of odd prime order, if S is g-thin and if m divides $p-1$, then it is shown that $|S| \le \frac{p-1}{m}$. We also show that in certain cases S must be an arithmetic progression, and the form of the linear function g can be characterized.

In this paper, some properties of subsets of finite fields are investigated. The results of Vosper and Cauchy-Davenport [1],[2] are applied in the proofs of some of the theorems. For several notations and definitions concerning a finite field and subsets of abelian group, see also [3]. For a set S, we shall use the notation S^m to represent

$$\underbrace{S \times \cdots \times S}_{m \text{ times}} = \{(x_1, \cdots, x_m) \mid x_i \in S, i = 1, \cdots, m\}.$$

Definition 1 *Let $g : \mathbb{F}^m \to \mathbb{F}$ be a linear function on the vector space $\mathbb{F}^m$ over a finite field $\mathbb{F}$. A subset $S \subsetneq \mathbb{F}$ is called g-thin iff $g(S^m) \subsetneq \mathbb{F}$.*

We note that in the case where S is a sum-free subset of $\mathbb{Z}_p$, the linear function

$$g : S^3 \to S$$

defined by

$$g(x_1, x_2, x_3) = x_1 + x_2 - x_3$$

has the property that $g(S^3) \subsetneq \mathbb{Z}_p$. Thus sum-free subsets of $\mathbb{Z}_p$ are g-thin. In fact, interest in the work presented in this paper came about from studying generalizations of sum-free sets. To be more precise, a subset S of $\mathbb{Z}_p$ is said to be of type (k, l) if the equation $x_1 + x_2 + \cdots + x_k - x_{k+1} - \cdots - x_{k+l} = 0$ has no solution in the set S. Thus if S is a subset of $\mathbb{Z}_p$ of type (k, l) and the linear function

$$g : S^{k+l} \to S$$

is defined by

$$g(x_1, \cdots, x_{k+l}) = x_1 + \cdots + x_k - x_{k+1} - \cdots - x_{k+l},$$

then $g(S^{k+l}) \subsetneq \mathbb{Z}_p$.

In this note, we consider the case where $\mathbb{F}$ is the field $\mathbb{Z}_p$ of odd prime order and obtain an upper bound for the cardinalities of g-thin subsets of $\mathbb{F}$. It is shown that under certain conditions,g-thin subsets of $\mathbb{Z}_p$ are in arithmetic progression. A characterization of the forms of linear functions are also given in certain cases.

In order to prove the first theorem, the following lemma, which is a result of Cauchy-Davenport, is needed. The lemma is stated as follows:

Lemma 2 *(Cauchy-Davenport)[1],[2] If $S, T \subseteq \mathbb{Z}_p$ and $|S + T| < p$ where p is an odd prime, then $|S| + |T| - 1 \leq |S + T|$.*

In what follows, the notation S^m shall be used to represent

$$\underbrace{S \times \cdots \times S}_{m \text{ times}} = \{(x_1, \cdots, x_m) \mid x_i \in S, i = 1, \cdots, m\}.$$

Theorem 3 *Let p be an odd prime and $f : (\mathbb{Z}_p)^m \to \mathbb{Z}_p$ such that*

$$f(x_1, \ldots, x_m) = c_1 x_1 + \cdots + c_m x_m$$

where $x_i \in \mathbb{Z}_p$ and $c_i \in \mathbb{Z}_p \setminus \{0\}$ for all $i = 1, \ldots, m \quad (m \geq 2)$. If S is f-thin, then $|S| < \frac{p-1}{m} + 1$. In particular, if $m \mid (p-1)$, then $|S| \leq \frac{p-1}{m}$.

Proof: Let $S_i = c_i \cdot S$, $i = 1, \ldots, m \quad (m \geq 2)$. Since $f(S^m) \subsetneq \mathbb{Z}_p$, so

$$f(S^m) = S_1 + \cdots + S_m \subsetneq \mathbb{Z}_p$$

Hence, $|S_1 + S_2 + \cdots + S_m| < p$ and also $|S_1 + S_2 + \cdots + S_{i-1}| < p$, for $2 \leq i \leq m$. By letting $T' = S_1 + S_2 + \cdots + S_{i-1}$, $S' = S_i$ and applying Lemma 2, we have

$$|T' + S'| \geq |T'| + |S'| - 1 = |S_1 + S_2 + \cdots + S_{i-1}| + |S_i| - 1.$$

We get

$$\begin{aligned} p &> |S_1 + \cdots + S_m| \\ &\geq |S_1 + \cdots + S_{m-1}| + |S| - 1 \\ &\geq |S_1 + \cdots + S_{m-2}| + 2|S| - 2 \\ &\vdots \\ &\geq |S_1 + S_2| + (m-2)|S| - (m-2) \\ &\geq m \cdot |S| - (m-1) \end{aligned}$$

so that $m \cdot |S| < p + m - 1$ and hence $|S| < \frac{p-1}{m} + 1$.
In particular, if $m \mid (p-1)$, then

$$|S| \leq \frac{p-1}{m}.$$

In other words if a set S is f-thin for a linear function in m variables with all nonzero coefficients then the cardinality of S is bounded above by $|S| < \frac{p-1}{m} + 1$. □

We say that S is an arithmetic progression of steplength d if $\exists a, d \in \mathbb{Z}$ such that

$$S = \{a, a+d, \ldots, a+(s-1)d\}.$$

Lemma 4 *(Vosper)[1],[2] Let $S, T \subseteq \mathbb{Z}_p$, $|S+T| < p-1$. If $|S+T| = |S|+|T|-1$, then $\exists a, b, d \in \mathbb{Z}_p$ such that S and T are arithmetic progressions with the same steplength,*

$$S = \{a, a+d, \ldots, a+(s-1)d\};$$

$$T = \{b, b+d, \ldots, b+(t-1)d\}$$

with $s = |S|$ and $t = |T|$. In this case, $S+T$ also is an arithmetic progression with the same steplength d.

Lemma 5 *Let $S \subseteq \mathbb{Z}_p$ and let $S_i = c_i \cdot S$ with $c_i \in \mathbb{Z}_p \setminus \{0\}$ such that*

$$|S_1 + S_2 + \cdots + S_m| \leq p-2$$

holds. If S is not an arithmetic progression, then we have

$$|S_1 + S_2 + \cdots + S_m| \geq m \cdot |S|.$$

Proof: By applying Lemma 4, $(m-1)$ times,

$$\begin{aligned}
|S_1 + S_2 + \cdots + S_m| &\geq |S_1| + |S_2 + S_3 + \cdots + S_m| \\
&\geq |S_1| + |S_2| + |S_3 + \cdots + S_m| \\
&\vdots \\
&\geq |S_1| + |S_2| + \cdots + |S_{m-2}| + |S_{m-1} + S_m| \\
&\geq |S_1| + |S_2| + \cdots + |S_{m-1}| + |S_m| \\
&= m \cdot |S|.
\end{aligned}$$

□

For the next theorem, again let $f : (\mathbb{Z}_p)^m \to \mathbb{Z}_p$ be a linear function of the form

$$f(x_1, \ldots, x_m) = c_1 x_1 + \cdots + c_m x_m$$

with $c_i \in \mathbb{Z}_p \setminus \{0\}$ for all $i = 1, \ldots, m\,(m \geq 2)$.

Theorem 6 *If*

$$|f(S^m)| \leq p - 2$$

and if $|S| \geq \frac{p-1}{m}$, *then the set* S *is an arithmetic progression.*

Proof: Assume that S is not an arithmetic progression. We have

$$f(S^m) = S_1 + S_2 + \cdots + S_m.$$

By Lemma 5, we get

$$p - 2 \geq |f(S^m)| = |S_1 + S_2 + \cdots + S_m| \geq m \cdot |S| \geq p - 1,$$

a contradiction. Therefore S is an arithmetic progression. □

Theorem 7 *If* $|f(S^m)| \leq p - m$ *and* $|S| \geq \frac{p-1}{m}$, *then* $\exists k \in \mathbb{Z}_p \setminus \{0\}$ *such that for all* $i = 1, \ldots, m\,(m \geq 2)$, $c_i = \pm k$.

Proof: We use a similar argument as in the proof of Theorem 3 and Lemma 5.

$$f(S^m) = S_1 + S_2 + \cdots + S_m$$

$$
\begin{aligned}
p-m &\geq |f(S^m)| \\
&= |S_1+S_2+\cdots+S_m| \\
&\geq |S_1|+|S_2+\cdots+S_m|-1 \\
&\geq |S_1|+|S_2|+|S_3+\cdots+S_m|-2 \\
&\vdots \\
&\geq |S_1|+|S_2|+\cdots+|S_{m-2}|+|S_{m-1}+S_m|-(m-2) \\
&\geq |S_1|+|S_2|+\cdots+|S_{m-2}|+|S_{m-1}|+|S_m|-(m-1) \\
&= m\cdot|S|-(m-1) \\
&\geq p-1-m+1 \\
&= p-m.
\end{aligned}
$$

Hence, we must have equality in each step of the chain of inequalities, so that $|S_{m-1}+S_m| = |S_{m-1}|+|S_m|-1$. By Lemma 4, S_{m-1} and S_m are both arithmetic progressions with the same steplength. By Theorem 6, let $S=\{a, a+d, \ldots, a+(s-1)d\}$ with the steplength $d\neq 0$ and $S_i = c_i\cdot S$ for all $i=1,\ldots,m$. Then,

$$S_{m-1} = \{c_{m-1}a, c_{m-1}a+c_{m-1}d, \ldots, c_{m-1}a+(s-1)c_{m-1}d\}$$

and

$$S_m = \{c_m a, c_m a + c_m d, \ldots, c_m a + (s-1)c_m d\}.$$

Hence, by applying Lemma 2.4 (p.53) of [2] to $S_{m-1}(=A), S_{m-2}(=B)$, we see that

$$c_m d = c_{m-1}d \text{ or } c_m d = -c_{m-1}d.$$

$$\Rightarrow \quad c_m = \pm c_{m-1}.$$

Now by induction for all $i=m-2, m-3, \ldots, 1$, we get $c_i = \pm c_{i-1}$. Therefore, $\exists k\in Z_p\setminus\{0\}$ such that $c_i=\pm k$ for all $i=1,\ldots,m$. □

Remarks 8 *If* $s = \frac{p-1}{m}$*, in general on ly some positive integers* n *with* $p - 2 \geq n \geq p - m$ *can occur as* $n = |f(S^m)|$ *for some set* S*, which by Theorem 6 must be in arithmetic progression.*

Example.

Let $p = 19, m = 6$ *and* $s = 3$*. Let* $S = \{0, 1, 2\}$*. In this case* $n = 13, 15, 17$ *are the only values.*

For $n = 13$*, by Theorem 7* $c_i = \pm k$*.*

For $n = 15$*, computation shows that* $c_i = \pm k$ *and at most one* $c_j = \pm 2k$*.*

For $n = 17$*, computation shows that* $c_i = \pm k$ *and at most two* $c_j = \pm 2k$ *or at most one* $c_j = \pm 3k$*.*

References

[1] H. Mann, "Addition Theorems: The Addition Theorems of Group Theory and Number Theory", Interscience Tracts in Pure and Applied Mathematics, No. 18, John Wiley, New York/London/Sydney, 1965.

[2] M. B. Nathanson, "Additive Number Theory: Inverse Problems and the Geometry of Sumsets", GTM 165, Springer, New York/Berlin/Heidelberg 1996

[3] A. P. Street, "Sum-Free Sets", Springer Lecture Notes in Math. 292 (1972), 123–272.