Journal of Combinatorial Theory, Series A **100**, 387–393 (2002)
doi:10.1006/jcta.2002.3294

NOTE

A Lower Bound for $|\{a+b\colon\ a \in A, b \in B, P(a,b) \neq 0\}|$

Hao Pan and Zhi-Wei Sun[1,2]

Department of Mathematics, Nanjing University, Nanjing 210093, People's Republic of China
E-mail: zwsun@nju.edu.cn

Received October 30, 2001

Let A and B be two finite subsets of a field $\mathbb{F}$. In this paper, we provide a non-trivial lower bound for $|\{a+b\colon a \in A,\ b \in B,\ \text{and}\ P(a,b) \neq 0\}|$ where $P(x,y) \in \mathbb{F}[x,y]$. © 2002 Elsevier Science (USA)

1. INTRODUCTION

Let $\mathbb{F}$ be a field and let $\mathbb{F}^{\times}$ be the multiplicative group $\mathbb{F}\setminus\{0\}$. The additive order of the (multiplicative) identity of $\mathbb{F}$ is either infinite or a prime, we call it the *characteristic* of $\mathbb{F}$.

Let A and B be finite subsets of the field $\mathbb{F}$. Set

$$A+B=\{a+b\colon\ a \in A\ \text{ and }\ b \in B\}$$

and

$$A\dot{+}B=\{a+b\colon\ a \in A,\ \ b \in B,\ \text{ and }\ a \neq b\}.$$

The theorem of Cauchy and Davenport (see, e.g. [N, Theorem 2.2]) asserts that if $\mathbb{F}$ is the field of residues modulo a prime p, then

$$|A+B| \geqslant \min\{p,\ |A|+|B|-1\}.$$

In 1964 Erdős and Heilbronn (cf. [EH, G]) conjectured that in this case

$$|A\dot{+}A| \geqslant \min\{p,\ 2|A|-3\},$$

[1] To whom correspondence should be addressed.

[2] Supported by the Teaching and Research Award Program for Outstanding Young Teachers in Higher Education Institutions of MOE, and the National Natural Science Foundation of the People's Republic of China.

0097-3165/02 $35.00
© 2002 Elsevier Science (USA)
All rights reserved.

this was confirmed by Dias da Silva and Hamidoune [DH] in 1994. In 1995–1996 Alon *et al.* [ANR1, ANR2] proposed a polynomial method to handle similar problems, they showed that if $|A| > |B| > 0$ then

$$|A \dot{+} B| \geqslant \min\{p,\ |A| + |B| - 2\},$$

where p is the characteristic of the field $\mathbb{F}$. The method usually yields a nontrivial conclusion provided that certain coefficient of a polynomial, related in some special way to the additive problem under considerations, does not vanish.

What can we say about the cardinality of the restricted sumset

$$C = \{a + b\colon\ a \in A,\ b \in B,\ \text{and}\ P(a,b) \neq 0\}, \tag{1}$$

where $P(x,y) \in \mathbb{F}[x,y]$? We will make progress in this direction by relaxing (to some extent) the limitations of the polynomial method. Our approach allows one to draw conclusions even if no coefficients in question are known explicitly.

Throughout this paper, for $k, l \in \mathbb{Z}$ each of the intervals $(k,l), [k,l)$, $(k,l], [k,l]$ will represent the set of *integers* in it. For a polynomial $P(x_1, \ldots, x_n)$ over a field, we let $\hat{P}(i_1, \ldots, i_n)$ stand for the coefficient of $x_1^{i_1} \cdots x_n^{i_n}$ in $P(x_1, \ldots, x_n)$.

Let $\mathbb{E}$ be an algebraically closed field and $P(x)$ be a polynomial over $\mathbb{E}$. For $\alpha \in \mathbb{E}$, if $(x-\alpha)^m \mid P(x)$ but $(x-\alpha)^{m+1} \nmid P(x)$, then we call m the *multiplicity* of α with respect to $P(x)$ and denote it by $m_P(\alpha)$. For any positive integer q, we set

$$N_q(P) = q|\{\alpha \in \mathbb{E}^\times : m_P(\alpha) \geqslant q\}| - \sum_{\alpha \in \mathbb{E}^\times} \{m_P(\alpha)\}_q, \tag{2}$$

where $\{m\}_q$ denotes the least nonnegative residue of $m \in \mathbb{Z}$ modulo q. Note that $N_1(P)$ is the number of distinct roots in $\mathbb{E}^\times$ of the equation $P(x) = 0$. Let p be the characteristic of $\mathbb{E}$, and

$$\mathscr{P}(p) = \begin{cases} \{1, p, p^2, \ldots\} & \text{if } p < \infty, \\ \{1\} & \text{otherwise.} \end{cases}$$

We also define

$$N(P) = \max_{q \in \mathscr{P}(p)} q|\{\alpha \in \mathbb{E}^\times \setminus \{-1\} : m_P(\alpha) \geqslant q\}|. \tag{3}$$

Clearly $N(P) \leqslant \sum_{\alpha \in \mathbb{E}^\times \setminus \{-1\}} m_P(\alpha) \leqslant \deg P(x)$.

Let $\mathbb{F}$ be a field of characteristic p, and let $\mathbb{E}$ be the algebraic closure of $\mathbb{F}$. Any $P(x) \in \mathbb{F}[x]$ can be viewed as a polynomial over $\mathbb{E}$ so that $N_q(P)$

$(q = 1, 2, 3, \ldots)$ and $N(P)$ are well defined. If $P(x) \in \mathbb{F}[x]$ is irreducible and it has a repeated zero in $\mathbb{E}$, then $p < \infty$ and $P(x) = f(x^p)$ for some irreducible $f(x) \in \mathbb{F}[x]$ (see, e.g. [W, Theorem 9.7]); as $x^p - \alpha^p = (x - \alpha)^p$ for all $\alpha \in \mathbb{E}$, by induction we find that the multiplicity of any zero of $P(x)$ belongs to $\mathscr{P}(p)$.

The key lemma of this paper is the following new result.

LEMMA 1. *Let $P(x)$ be a polynomial over the field $\mathbb{F}$ of characteristic p. Suppose that there exist nonnegative integers $k < l$ such that $\hat{P}(i) = 0$ for all $i \in (k, l)$. Then either $x^l \mid P(x)$, or $\deg P(x) \leqslant k$, or $N_q(P) \geqslant l - k$ for some $q \in \mathscr{P}(p)$.*

With the help of Lemma 1 and the polynomial method, we are able to obtain the following main result.

THEOREM 1. *Let $\mathbb{F}$ be a field of characteristic p, and let A and B be two finite nonempty subsets of $\mathbb{F}$. Furthermore, let $P(x, y)$ be a polynomial over $\mathbb{F}$ of degree $d = \deg P(x, y)$ such that for some $i \in [0, |A| - 1]$ and $j \in [0, |B| - 1]$ we have $\hat{P}(i, d - i) \neq 0$ and $\hat{P}(d - j, j) \neq 0$. Define $P_0(x, y)$ to be the homogeneous polynomial of degree d such that $P(x, y) = P_0(x, y) + R(x, y)$ for some $R(x, y) \in \mathbb{F}[x, y]$ with $\deg R(x, y) < d$, and put $P^*(x) = P_0(x, 1)$. Then, for the set C given by (1), we have*

$$|C| \geqslant \min\{p - m_{P^*}(-1),\ |A| + |B| - 1 - d - N(P^*)\}. \tag{4}$$

Remark 1. In the case $d = \deg P(x, y) = 0$, Theorem 1 yields the Cauchy–Davenport theorem.

Lemma 1 and Theorem 1 will be proved in the next section.

Now we give some consequences of Theorem 1.

COROLLARY 1. *Let $\mathbb{F}$ be a field of characteristic p, and let A and B be finite subsets of $\mathbb{F}$. Let k, m, n be nonnegative integers and $Q(x, y) \in \mathbb{F}[x, y]$ have degree less than $k + m + n$. If $|A| > k$ and $|B| > m$, then*

$$\begin{aligned} &|\{a + b\colon\ a \in A,\ b \in B,\ \text{and } a^k b^m (a + b)^n \neq Q(a, b)\}| \\ &\geqslant \min\{p - n,\ |A| + |B| - k - m - n - 1\}. \end{aligned} \tag{5}$$

Proof. For $P(x, y) = x^k y^m (x + y)^n - Q(x, y)$, clearly $\hat{P}(k, m + n) = \hat{P}(k + n, m) = 1$ and $P^*(x) = x^k (x + 1)^n$. Since $N(P^*) = 0$, the desired result follows from Theorem 1. ∎

Remark 2. When $k = m = 1$, $n = 0$ and $Q(x, y) = 1$, our Corollary 1 yields Theorem 4 of Alon et al. [ANR1], which is also Proposition 4.1 of Alon et al. [ANR2].

COROLLARY 2. *Let $\mathbb{F}$ be a field of characteristic $p \neq 2$, and let A, B and S be finite nonempty subsets of $\mathbb{F}$. Then*

$$|\{a + b\colon\ a \in A,\ b \in B,\ \text{and}\ a - b \notin S\}| \geqslant \min\{p,\ |A| + |B| - |S| - q - 1\}, \tag{6}$$

where q is the largest element of $\mathscr{P}(p)$ not exceeding $|S|$.

Proof. Let $C = \{a + b\colon\ a \in A,\ b \in B,\ \text{and}\ a - b \notin S\}$. By applying Theorem 1 with $P(x, y) = \prod_{s \in S} (x - y - s)$, we obtain the desired lower bound for $|C|$. ∎

Remark 3. In the case $S = \{0\}$, Corollary 2 was first obtained by Alon *et al.* [ANR1, ANR2]. When $|A| = |B| = k$, $2 \mid |S|$ and $|S| < p$, the lower bound in (6) can be replaced by $\min\{p, 2k - |S| - 1\}$ as pointed out by Hou and Sun [HS]. For a field $\mathbb{F}$ with $|\mathbb{F}| = 2^n > 2$, if $A, S \subseteq \mathbb{F}$, $|A| > 2^{n-1} + 1$ and $|S| = 2^n - 1$, then $|\{a + b\colon\ a \in A,\ b \in \mathbb{F},\ \text{and}\ a - b \notin S\}| = |(A + \mathbb{F}) \setminus S| = |\mathbb{F} \setminus S| = 1 < \min\{2, |A| + |\mathbb{F}| - |S| - 2^{n-1} - 1\}$. So we cannot omit the condition $p \neq 2$ from Corollary 2.

COROLLARY 3. *Let $\mathbb{F}$ be a field of characteristic p, and let A and B be finite nonempty subsets of $\mathbb{F}$. Let $\emptyset \neq S \subseteq \mathbb{F}^\times \times \mathbb{F}$ and $|S| < \infty$. Then*

$$\begin{aligned} &|\{a + b\colon\ a \in A,\ b \in B,\ \textit{and}\ a + ub \neq v\ \textit{if}\ \langle u, v\rangle \in S\}| \\ &\quad \geqslant \min\{p - |\{v \in \mathbb{F} : \langle 1, v\rangle \in S\}|,\ |A| + |B| - 2|S| - 1\}. \end{aligned} \tag{7}$$

Proof. Just apply Theorem 1 with $P(x, y) = \prod_{\langle u, v\rangle \in S} (x + uy - v)$ and note that $N(P^*) \leqslant \deg P^* = |S|$. ∎

Remark 4. When $p = \infty$, Corollary 3 is essentially [S, Theorem 1.1] in the case $n = 2$.

2. PROOFS OF LEMMA 1 AND THEOREM 1

Proof of Lemma 1. We use induction on $\deg P(x)$. When $P(x)$ is a constant, we need do nothing. So we let $\deg P(x) > 0$ and proceed to the induction step.

Write $P(x) = x^h Q(x)$ where $h = m_P(0)$ and $Q(x) \in \mathbb{F}[x]$. If $h < l$, then $h \leqslant k$ since $\hat{P}(i) = 0$ for any $i \in (k, l)$, therefore $\hat{Q}(j) = 0$ for all $j \in (k-h, l-h)$. So, without loss of generality, it can be assumed that $P(0) \neq 0$ and that $P(x)$ is monic.

Let $\mathbb{E}$ be the algebraic closure of the field $\mathbb{F}$. Write $P(x) = \prod_{j=1}^{n} (x - \alpha_j)^{m_j}$ where $\alpha_1, \ldots, \alpha_n$ are distinct elements of $\mathbb{E}^{\times}$ and $m_1, \ldots, m_n$ are positive integers. For $j = 1, \ldots, n$ let $P_j(x) = P(x)/(x - \alpha_j)$. As $P(x) = P_j(x)(x - \alpha_j)$, $\hat{P}(i+1) = \hat{P}_j(i) - \alpha_j \hat{P}_j(i+1)$ for $i = 0, 1, 2, \ldots$. Note that $\hat{P}_j(i) = \alpha_j \hat{P}_j(i+1)$ for every $i \in [k, l-1)$. Therefore,

$$\hat{P}_j(i) = \alpha_j^{l-1-i} \hat{P}_j(l-1) \qquad \text{for all } i \in [k, l). \tag{8}$$

Since $P'(x) = \sum_{j=1}^{n} m_j P_j(x)$, we have

$$\sum_{j=1}^{n} m_j \hat{P}_j(i) = 0 \qquad \text{for any } i \in [k, l-1). \tag{9}$$

Combining (8) and (9) we find that

$$\sum_{j=1}^{n} m_j \alpha_j^{l-1-i} \hat{P}_j(l-1) = 0 \qquad \text{for each } i \in [k, l-1). \tag{10}$$

Suppose that $N_q(P) < l - k$ for any $q \in \mathscr{P}(p)$. Then $n = N_1(P) \leqslant l - 1 - k$, hence by (10) we have

$$\sum_{j=1}^{n} \alpha_j^s (m_j \hat{P}_j(l-1)) = 0 \qquad \text{for every } s = 1, \ldots, n.$$

Since the Vandermonde determinant $||\alpha_j^s||_{1 \leqslant s,j \leqslant n}$ does not vanish, by Cramer's rule we have $m_j \hat{P}_j(l-1) = 0$ for all $j = 1, \ldots, n$. Thus, in light of (8), $m_j \hat{P}_j(i) = 0$ for any $i \in [k, l)$ and $j \in [1, n]$.

Case 1: $p = \infty$, or $p \nmid m_j$ *for some* $j \in [1, n]$. In this case there is a $j \in [1, n]$ such that $\hat{P}_j(i) = 0$ for all $i \in (k-1, l)$. Clearly $k > 0$ since $\hat{P}_j(0) = P_j(0) \neq 0$. Also $N_1(P_j) \leqslant n = N_1(P)$, and $N_q(P_j) = N_q(P) + 1$ if $p < \infty$ and $q \in \mathscr{P}(p) \backslash \{1\}$. Thus $N_q(P_j) \leqslant N_q(P) + 1 \leqslant l - k < l - (k-1)$ for all $q \in \mathscr{P}(p)$. In view of the induction hypothesis, we should have $\deg P_j \leqslant k - 1$ and hence $\deg P(x) \leqslant k$.

Case 2: $p < \infty$, *and* $p | m_j$ *for all* $j \in [1, n]$. In this case, $T(x) = \prod_{j=1}^{n} (x - \alpha_j)^{m_j/p} \in \mathbb{E}[x]$ and therefore $P(x) = T(x)^p = (\sum_{i \geqslant 0} \hat{T}(i) x^i)^p = \sum_{i \geqslant 0} \hat{T}(i)^p x^{ip}$. For any real number r let $\lfloor r \rfloor$ denote the greatest integer not exceeding r. Then $\lfloor k/p \rfloor \leqslant \lfloor (l-1)/p \rfloor$ since $k \leqslant l - 1$. Whenever $i \in (\lfloor k/p \rfloor, \lfloor (l-1)/p \rfloor]$, we have $k < ip < l$ and hence $\hat{T}(i)^p = \hat{P}(ip) = 0$. If

$q \in \mathscr{P}(p)$ then

$$N_q(T) = \frac{N_{pq}(P)}{p} \leqslant \frac{l-k-1}{p} < \left(1 + \left\lfloor \frac{l-1}{p} \right\rfloor\right) - \left\lfloor \frac{k}{p} \right\rfloor.$$

By the induction hypothesis, $\deg T \leqslant \lfloor k/p \rfloor$ and hence $\deg P = p \deg T \leqslant k$.
So far we have completed the induction proof. ∎

Proof of Theorem 1. Set $k_1 = |A| - 1$ and $k_2 = |B| - 1$. Clearly (4) holds if $|C| \geqslant k_1 + k_2 - d + 1$. So we assume that $|C| \leqslant k_1 + k_2 - d$ and let $\delta = k_1 + k_2 - d - |C|$.

Since $\hat{P}(d-j, j) \neq 0$ for some $j \in [0, k_2]$, $Q(x,y) = P(x,y)/\prod_{b \in B} (y-b) \notin \mathbb{F}[x,y]$ (otherwise $\hat{P}(d-j,j)$ is zero because it equals the coefficient of $x^{d-j}y^j$ in $y^{|B|}Q(x,y)$). Thus, there exists a $b_0 \in B$ such that $P(x, b_0)$ does not vanish identically; hence $P(a, b_0) = 0$ for at most d elements $a \in \mathbb{F}$. Therefore,

$$|C| \geqslant |\{a + b_0 : a \in A \text{ and } P(a, b_0) \neq 0\}| \geqslant |A| - d$$

and so $\delta < k_2$. Similarly, we have $\delta < k_1$.

Put

$$f(x,y) = P(x,y) \prod_{c \in C} (x + y - c) \text{ and } f_0(x,y) = P_0(x,y)(x+y)^{|C|}.$$

Clearly $\deg f(x,y) = \deg f_0(x,y) = d + |C| = k_1 + k_2 - \delta$. Let $\kappa_1 \in [k_1 - \delta, k_1]$. Then $\kappa_2 = k_1 + k_2 - \delta - \kappa_1 \in (0, k_2]$. As $\kappa_1 + \kappa_2 = \deg f(x,y)$ and $f(x,y)$ vanishes over the Cartesian product $A \times B$, $\hat{f}(\kappa_1, \kappa_2) = 0$ by Alon [A, Theorem 1.2].

Since $\widehat{P^*}(i) = \hat{P}_0(i, d-i) = \hat{P}(i, d-i) \neq 0$ for some $i \in [0, k_1]$, we have $m_{P^*}(0) \leqslant k_1$. Similarly $\widehat{P^*}(d-j) \neq 0$ for some $j \in [0, k_2]$ and hence $\deg P^*(x) \geqslant d - k_2$.

Set $f^*(x) = f_0(x, 1) = P^*(x)(x+1)^{|C|}$. Recall that $\widehat{f^*}(\kappa) = \hat{f}(\kappa, k_1 + k_2 - \delta - \kappa) = 0$ for all $\kappa \in [k_1 - \delta, k_1]$. Since $x^{k_1+1} \nmid f^*(x)$ and $\deg f^*(x) = |C| + \deg P^*(x) \geqslant |C| + d - k_2 = k_1 - \delta$, by Lemma 1 there exists a $q \in \mathscr{P}(p)$ such that $N_q(f^*) \geqslant (k_1 + 1) - (k_1 - \delta - 1) = \delta + 2$.

If $m_{f^*}(-1) = m_{P^*}(-1) + |C| < p$, then $N(P^*) = N(f^*) \geqslant N_q(f^*) - 1 \geqslant k_1 + k_2 - d - |C| + 1$, therefore

$$|C| \geqslant k_1 + k_2 + 1 - d - N(P^*) = |A| + |B| - 1 - d - N(P^*).$$

This concludes our proof. ∎

ACKNOWLEDGMENTS

The authors are indebted to the two referees for their many helpful comments. The revision was done during the second author's visit to the Institute of Mathematics, Academia Sinica (Taiwan); he thanks the Institute for its financial support.

REFERENCES

[A] N. Alon, Combinatorial nullstellenstaz, *Combin. Probab. Comput.* **8** (1999), 7–29.

[ANR1] N. Alon, M. B. Nathanson, and I. Z. Ruzsa, Adding distinct congruence classes modulo a prime, *Amer. Math. Monthly* **102** (1995), 250–255.

[ANR2] N. Alon, M. B. Nathanson, and I. Z. Ruzsa, The polynomial method and restricted sums of congruence classes, *J. Number Theory* **56** (1996), 404–417.

[DH] J. A. Dias da Silva and Y. O. Hamidoune, Cyclic space for Grassmann derivatives and additive theory, *Bull. London Math. Soc.* **26** (1994), 140–146.

[EH] P. Erdős and H. Heilbronn, On the addition of residue classes mod p, *Acta Arith.* **9** (1964), 149–159.

[G] R. K. Guy, "Unsolved Problems in Number Theory" (2nd ed.), pp. 129–131, Springer-Verlag, New York, 1994.

[HS] Q. H. Hou and Z. W. Sun, Restricted sums in a field, *Acta Arith.* **102** (2002), 239–249.

[N] M. B. Nathanson, "Additive Number Theory: Inverse Problems and the Geometry of Sumsets," Graduate Texts in Mathematics, Vol. 165, Springer-Verlag, New York, 1996.

[S] Z. W. Sun, Restricted sums of subsets of $\mathbb{Z}$, *Acta Arith.* **99** (2001), 41–60.

[W] L. M. Weiner, "Introduction to Modern Algebra Harcourt," p. 306, Brace & World, Inc., New York, 1970.