Journal of Mathematical Research with Applications
May, 2016, Vol. 36, No. 3, pp. 272–274
DOI:10.3770/j.issn:2095-2651.2016.03.003
Http://jmre.dlut.edu.cn

A Second Note on a Result of Haddad and Helou

Yujie WANG
School of Mathematics and Computer Science, Anhui Normal University,
Anhui 241003*, P. R. China*

Abstract Let K be a finite field of characteristic $\neq 2$ and G the additive group of $K\times K$. Let k_1, k_2 be integers not divisible by the characteristic p of K with $(k_1,k_2)=1$. In 2004, Haddad and Helou constructed an additive basis B of G for which the number of representations of $g\in G$ as a sum $b_1+b_2(b_1,b_2\in B)$ is bounded by 18. For $g\in G$ and $B\subset G$, let $\sigma_{k_1,k_2}(B,g)$ be the number of solutions of $g=k_1b_1+k_2b_2$, where $b_1,b_2\in B$. In this paper, we show that there exists a set $B\subset G$ such that $k_1B+k_2B=G$ and $\sigma_{k_1,k_2}(B,g)\leqslant 16$.

Keywords additive basis; representation function

MR(2010) Subject Classification 11B34

1. Introduction

Let G be a semi-group. For $A,B\subseteq G$, $g\in G$, and k_1, k_2 be integers with $(k_1,k_2)=1$, we define

$$\sigma_{k_1,k_2}(A,B,g)=\sharp\{(a,b)\in A\times B: k_1a+k_2b=g\},$$

and $\sigma_{k_1,k_2}(A,g)=\sigma_{k_1,k_2}(A,A,g)$. In particular, we denote $\sigma_A(g)=\sigma_{1,1}(A,g)$, $\delta_A(g)=\sigma_{1,-1}(A,g)$.

The well known Erdös-Turán conjecture [1] says that if A is a basis of $\mathbb{N}$, then $\sigma_A(n)$ cannot be bounded. Pŭs [2] first established that the analogue of the Erdös-Turán conjecture fails to hold in some abelian groups. Let K be a field of characteristic $\neq 2$ and G the additive group of $K\times K$. In 2004, Haddad-Helou [3] constructed an additive basis B of G for which the number of representations of $g\in G$ as a sum b_1+b_2 $(b_1,b_2\in B)$ is bounded by 18. In 2010, Tang-Tang [4] investigated the parallel problem for differences. We find that the set constructed by Tang-Tang [4] is the same as the set constructed by Haddad-Helou [3]. That is, there exists a set $A\subseteq G$ such that $1\leqslant\sigma_A(g)\leqslant 18$ and $1\leqslant\delta_A(g)\leqslant 14$ for all $g\in G$. For the related problems we refer to [5–10].

In this paper, we obtain the following result.

Theorem 1.1 *Let K be a finite field of characteristic $\neq 2$, k_1,k_2 be integers not divisible by the characteristic p of K with $(k_1,k_2)=1$ and G the additive group of $K\times K$. Then there exists a set $B\subset G$ such that $k_1B+k_2B=G$, and $\sigma_{k_1,k_2}(B,g)\leqslant 16$.*

Remark 1.2 Indeed, if, for instance k_1 is divisible by the characteristic p of K, then, for any

Received May 14, 2015; Accepted September 18, 2015
Supported by the National Natural Science Foundation of China (Grant No. 11471017).
E-mail address: wangyujie9291@126.com

subset B of G, we have $k_1B = \{(0,0)\}$ and then $k_1B + k_2B = k_2B$ is in bijection with B (since obviously k_2 will not be divisible by p, as $(k_1, k_2) = 1$), so that $k_1B + k_2B = G$ if and only if $B = G$, and in that case, for any $g \in G$, we have

$$\sigma_{k_1,k_2}(G, g) = |\{(\mu, \nu) \in G \times G : k_1\mu + k_2\nu = k_2\nu = g\}| = |G \times \{k_2^{-1}g\}| = |G|.$$

Throughout this paper, we denote by $K^* = K\backslash\{0\}$ the multiplicative group of K and by $S(K^*) = \{x^2 : x \in K^*\}$ the subgroup of the square elements of K^*. For $\alpha \in K^*$, let $Q_\alpha = \{(\mu, \alpha\mu^2) : \mu \in K\} \subset G$.

2. Proofs

Lemma 2.1 *Let k_1, k_2 be integers not divisible by the characteristic p of K with $(k_1, k_2) = 1$. For $g = (a, b) \in G$ and fixed $\alpha, \beta \in K^*$, consider the equation*

$$g = k_1x + k_2y, \quad x \in Q_\alpha,\ y \in Q_\beta.$$

If $\alpha k_2 + \beta k_1 \neq 0$, then the set $k_1Q_\alpha + k_2Q_\beta$ consists of all elements $(a, b) \in G$ such that $k_1k_2(\alpha k_2 + \beta k_1)b - k_1k_2\alpha\beta a^2$ is a square in K, and for any $g \in G$, $\sigma_{k_1,k_2}(Q_\alpha, Q_\beta, g) \leqslant 2$. If $\alpha k_2 + \beta k_1 = 0$, then the equation has at most one solution except if $g = 0$, when it has $|K|$ solutions.

Proof Let $g = (a, b) \in G$. Consider the system of equations

$$a = k_1\mu + k_2\nu, \tag{1}$$

$$b = k_1\alpha\mu^2 + k_2\beta\nu^2. \tag{2}$$

Substituting the value of μ from (1) into (2), we get the equation

$$k_1b = k_2(\alpha k_2 + \beta k_1)\nu^2 - 2a\alpha k_2\nu + \alpha a^2. \tag{3}$$

Case 1 $\alpha k_2 + \beta k_1 \neq 0$. This is a quadratic equation in ν, and it has exactly one or two solutions in the field K if and only if its discriminant $4[k_1k_2(\alpha k_2 + \beta k_1)b - k_1k_2\alpha\beta a^2]$ is a square in K. Since the characteristic of K is $\neq 2$, the non-zero square factor 4 can be discarded in the latter condition. Thus for any $g = (a, b) \in G$, we have $\sigma_{k_1,k_2}(Q_\alpha, Q_\beta, g) \leqslant 2$.

Case 2 $\alpha k_2 + \beta k_1 = 0$. Then (3) is an equation of degree 1. If $a \neq 0$, (3) has one solution. If $a = b = 0$, (3) has $|K|$ solutions. If $a = 0$, $b \neq 0$, (3) has no solution.

This completes the proof of Lemma 2.1. □

Lemma 2.2 ([3, Lemma 3.7]) *If K is a finite field of characteristic $\neq 2$, then the index of the subgroup $S(K^*)$ in the multiplicative group of K^* is 2. Thus the product of two non-square elements of K^* is a square element of K^*.*

Lemma 2.3 *Let k_1, k_2 be integers not divisible by the characteristic p of K with $(k_1, k_2) = 1$. If K is a finite field of characteristic $\neq 2$ and $|K| \geqslant 5$, then there exist elements $\alpha, \beta \in K^*$ such that $\alpha \in S(K^*)$, $\beta \notin S(K^*)$, and $\alpha k_2 + \beta k_1 \neq 0$.*

Proof By Lemma 2.2, $S(K^*) \neq K^*$ and $|S(K^*)| = |K^*|/2 \geqslant 2$, thus we can choose $\alpha \in S(K^*)$, $\beta \in K^* \backslash S(K^*)$, and $\alpha k_2 + \beta k_1 \neq 0$. $\square$

Proof of Theorem 1.1 If $K = \mathbb{F}_3 = \{0, 1, 2\}$, put $B = \{(0,0), (0,1), (0,2), (1,1), (1,0)\}$, then $B \subset \mathbb{F}_3 \times \mathbb{F}_3$, we have $k_1B + k_2B = G$ with $\sigma_{k_1,k_2}(B, g) \leqslant 5$.

Now we consider K to be a finite field of characteristic $\neq 2$ and $|K| \geqslant 5$.

Let $\alpha, \beta \in K^*$ such that $\alpha \in S(K^*)$, $\beta \notin S(K^*)$, and $\alpha k_2 + \beta k_1 \neq 0$. Put $\gamma = \alpha\beta(k_1 + k_2)/(\beta k_1 + \alpha k_2)$, $B = Q_\alpha \cup Q_\beta \cup Q_\gamma$. By the fact that $\beta \neq \alpha$, we have $\alpha \neq \gamma$, $\beta \neq \gamma$.

Case 1 If $k_1k_2 = -1$, then $\gamma = 0$. Let $n = 2\alpha\beta/(\alpha - \beta)$. By [4], $B = Q_\alpha \cup Q_\beta \cup Q_n$ is a basis of G, we have

$$\sigma_{k_1,k_2}(B, g) \leqslant \sum_{r,s \in \{\alpha,\beta,n\}} \sigma_{k_1,k_2}(Q_r, Q_s, g) \leqslant 14.$$

Case 2 If $k_1k_2 \neq -1$, then $\gamma \neq 0$. We have $\alpha k_2 + \beta k_1 \neq 0$ and $\gamma k_2 + \gamma k_1 \neq 0$. By Lemma 2.1,

$$k_1Q_\alpha + k_2Q_\beta = \{(a,b) \in G : k_1k_2(\alpha k_2 + \beta k_1)b - k_1k_2\alpha\beta a^2 \in S(K^*) \cup \{0\}\},$$

$$k_1Q_\gamma + k_2Q_\gamma = \{(a,b) \in G : k_1k_2(\gamma k_2 + \gamma k_1)b - k_1k_2\gamma^2 a^2 \in S(K^*) \cup \{0\}\}.$$

Let

$$e = k_1k_2(\alpha k_2 + \beta k_1)b - k_1k_2\alpha\beta a^2, \quad f = k_1k_2(\gamma k_2 + \gamma k_1)b - k_1k_2\gamma^2 a^2.$$

Thus an element $(a, b) \neq (0, 0)$ of G lies in $k_1Q_\alpha + k_2Q_\beta$ (resp., in $k_1Q_\gamma + k_2Q_\gamma$) if and only if e (resp., f) is square in K.

By simple calculation, we have $f = \beta\alpha\gamma^{-2}e$. Since $\alpha \in S(K^*)$, $\gamma^{-2} \in S(K^*)$, by Lemma 2.2, we have $\beta\alpha\gamma^{-2} \notin S(K^*)$, and thus $f \in S(K^*)$ if and only if $e \notin S(K^*)$. Hence, if an element $(a, b) \neq (0, 0)$ of G does not lie in $k_1Q_\alpha + k_2Q_\beta$, then it lies in $k_1Q_\gamma + k_2Q_\gamma$. Therefore, $G = (k_1Q_\alpha + k_2Q_\beta) \cup (k_1Q_\gamma + k_2Q_\gamma)$, which is stronger than the required $k_1B + k_2B = G$.

Hence, $\sigma_{k_1,k_2}(B, g) \leqslant \sum_{r,s \in \{\alpha,\beta,\gamma\}} \sigma_{k_1,k_2}(Q_r, Q_s, g) \leqslant 16$. This completes the proof of Theorem 1.1. $\square$

Acknowledgement We would like to thank the referee for his/her helpful comments.

References

[1] P. ERDÖS, P. TURÁN. *On a problem of Sidon in additive number theory, and on some related problems.* J. London Math. Soc., 1941, **16**(4): 212–215.

[2] V. PŮS. *On multiplicative bases in abelian groups.* Czechoslovak Math. J., 1991, **41**(2): 282–287.

[3] L. HADDAD, C. HELOU. *Bases in some additive groups and the Erdös-Turán conjecture.* J. Combin. Theory Ser. A, 2004, **108**(1): 147–153.

[4] Chiwu TANG, Min TANG. *Note on a result of Haddad and Helou.* Integers, 2010, **10**(18): 229–232.

[5] Yonggao CHEN. *The analogue of Erdös-Turán conjecture in $\mathbb{Z}_m$.* J. Number Theory, 2008, **128**(9): 2573–2581.

[6] M. B. NATHANSON. *Unique representation bases for integers.* Acta Arith., 2003, **108**(1): 1–8.

[7] S. V. KONYAGIN, V. F. LEV. *The Erdös-Turán Problem in Infinite Groups.* Additive Number Theory, Springer, New York, 2010.

[8] I. Z. RUZSA. *A just basis.* Monatsh. Math., 1990, **109**(2): 145–151.

[9] Min TANG, Yonggao CHEN. *A basis of $\mathbb{Z}$.* Colloq. Math., 2006, **104**(1): 99–103.

[10] Min TANG, Yonggao CHEN. *A basis of $\mathbb{Z}$ (II).* Colloq. Math., 2007, **108**(1), 141–145.