JOURNAL OF NUMBER THEORY **41**, 116–127 (1992)

Extremal Bases for Finite Cyclic Groups

XING-DE JIA

Department of Mathematics, Southwest Texas State University, San Marcos, Texas 78666

Communicated by R. L. Graham

Received November 9, 1990; revised January 1, 1991

Let m and h be positive integers. A set A of integers is called a *basis of order h* for $\mathbf{Z}/(m)$ if every integer n is congruent to a sum of h elements in A modulo m. Let $m(h, A)$ denote the greatest positive integer m such that A is a basis of order h for $\mathbf{Z}/(m)$. For any $k \geqslant 1$, define $m(h, k) = \max_{|A|=k+1} m(h, A)$. This generalizes a function of Graham and Sloane. In this paper, it is proved that, for fixed $k \geqslant 4$ as $h \to \infty$, $m(h, k) \geqslant \alpha_k (256/125)^{\lfloor k/4 \rfloor} (h/k)^k + O(h^{k-1})$, where $\alpha_k = 1$ if $k \equiv 0$ or 1 (mod 4), $\frac{4}{3}$ if $k \equiv 2$ (mod 4), and $\frac{27}{16}$ if $k \equiv 3$ (mod 4). A lower bound for $m(h, k)$ is also obtained for fixed h. Using these results, new lower bounds are proved for the order of subsets of asymptotic bases. © 1992 Academic Press, Inc.

1. INTRODUCTION

Let m and h be positive integers. A set A of integers is called a *basis of order h* for the finite cyclic group $\mathbf{Z}/(m)$ if every n is congruent to a sum of h elements in A modulo m. Let $m(h, A)$ denote the greatest positive integer m such that A is a basis of order h for $\mathbf{Z}/(m)$. For any $k \geqslant 1$, define

$$m(h, k) = \max_{|A| = k+1} m(h, A).$$

A basis $A = \{a_0, a_1, ..., a_k\}$ of order h for $\mathbf{Z}/(m)$ is called *extremal* if $m(h, A) = m(h, k)$.

Graham and Sloane [5] studied this extremal function in the case $h = 2$ and other related functions (see also Guy's problem book [7]). They connected the function $m(2, k)$ to a class of graphs called *harminious graphs*. Graham and Sloane [5] also calculated $m(2, k)$ for $1 \leqslant k \leqslant 9$. More exact values of $m(h, k)$ can be found in [8].

Distributed loop networks are an important type of computer network (see Bermond, Comellas, and Hsu [1], and Erdős and Hsu [3]). Recently, Hsu and Jia [8] showed that the extremal function $m(h, k)$ has applica-

0022-314X/92 $5.00

tions to the construction of distributed loop networks. It follows from their results that

$$m(h, 2) \geqslant \left\lfloor \frac{h(h+4)}{3} \right\rfloor + 1 \qquad \text{for all} \quad h \geqslant 2, \tag{1}$$

$$m(h, 3) \geqslant \tfrac{1}{16} h^3 + O(h^2) \qquad \text{as} \quad h \to \infty. \tag{2}$$

In this paper, we prove the following theorems.

THEOREM 1. *For fixed $k \geqslant 4$ as $h \to \infty$,*

$$m(h, k) \geqslant \alpha_k \left(\frac{256}{125}\right)^{\lfloor k/4 \rfloor} \left(\frac{h}{k}\right)^k + O(h^{k-1}),$$

where

$$\alpha_k = \begin{cases} 1 & \text{if } k \equiv 0 \text{ or } 1 \pmod 4 \\ \frac{4}{3} & \text{if } k \equiv 2 \pmod 4 \\ \frac{27}{16} & \text{if } k \equiv 3 \pmod 4). \end{cases}$$

TEOREM 2. *For fixed $h \geqslant 3$ as $k \to \infty$,*

$$m(h, k) \geqslant \beta_h \left(\frac{4}{3}\right)^{\lfloor h/3 \rfloor} \left(\frac{k}{h}\right)^h + O(k^{h-1}), \tag{3}$$

where

$$\beta_h = \begin{cases} 1 & \text{if } h \equiv 0 \text{ or } 1 \pmod 3) \\ \frac{8}{7} & \text{if } h \equiv 2 \pmod 3). \end{cases}$$

In this paper, we also establish a relation between this problem and the order of subsets of asymptotic bases. A set A of nonnegative integers is called an *asymptotic basis of order h* if every large integer is a sum of h elements in A. Let $g(A)$ denote the least such positive integer h. It is clear that a subset of an asymptotic basis is not necessarily an asymptotic basis again. For any $h \geqslant 2$ and $k \geqslant 1$, define

$$G_k(h) = \max_{g(A) \leqslant h} \max_{\substack{|F| = k \\ g(A \backslash F) < \infty}} g(A \backslash F).$$

Erdős and Graham [4] proved that

$$\tfrac{1}{4}(1 + o(1))h^2 \leqslant G_1(h) \leqslant \tfrac{5}{4}(1 + o(1))h^2.$$

The lower bound of Grekos [6] and the upper bound of Nash [11] are the best estimates for $G_1(h)$ so far:

$$\tfrac{1}{3}h^2+O(h)\leqslant G_1(h)\leqslant \tfrac{1}{2}h^2+h.$$

Nathanson [12] proved that

$$G_k(h)\geqslant\left(\left\lfloor\frac{h}{k+1}\right\rfloor+1\right)^{k+1}-1,$$

where $h>k$. Recently, Jia [9] proved that, for fixed $k\geqslant 1$,

$$G_k(h)\geqslant (k+1)\left(\frac{k+1}{k+2}\right)^k\left(\frac{h}{k+1}\right)^{k+1}+O(h^k)\qquad (\text{as } h\to\infty).$$

Using Theorem 1, we prove that, for fixed $k\geqslant 4$ as $h\to\infty$,

$$G_k(h)\geqslant \alpha_k\left(\frac{256}{125}\right)^{\lfloor k/4\rfloor}\left(\frac{h}{k+1}\right)^{k+1}+O(h^k).$$

Theorem 2 provides a new lower bound for $G_k(h)$ for fixed h.

2. Proof of Theorem 1

In order to prove Theorem 1, we need the following lemmas.

Lemma 1. *For any $h_1\geqslant 2$, $h_2\geqslant 2$, and $k_1\geqslant 1$, $k_2\geqslant 1$, we have*

$$m(h_1+h_2,k_1+k_2)\geqslant m(h_1,k_1)\,m(h_2,k_2).$$

Proof. Suppose that

$$m(h_s,A_s)=m(h_s,k_s)=m_s,$$

where

$$A_s=\{0=a_{s0},a_{s1},a_{s2},\ldots,a_{sk_s}\}$$

for $s=1,2$. Let n be any integer. Since A_1 is a basis of order h_1 for $\mathbf{Z}/(m_1)$, we see that

$$n\equiv a_{1i_1}+\cdots+a_{1i_{h_1}}\pmod{m_1},$$

thus,

$$n=a_{1i_1}+\cdots+a_{1i_{h_1}}+qm_1$$

for some integer q. It follows from the fact that A_2 is a basis of order h_2 for $\mathbf{Z}/(m_2)$ that

$$q \equiv a_{2j_1} + \cdots + a_{2j_{h_2}} \qquad (\bmod\, m_2),$$

i.e.,

$$q = a_{2j_1} + \cdots + a_{2j_{h_2}} + pm_2$$

for some integer p. Therefore,

$$n \equiv a_{1i_1} + \cdots + a_{1i_{h_1}} + m_1 a_{2j_1} + \cdots + m_1 a_{2j_{h_2}} \qquad (\bmod\, m_1 m_2).$$

Define

$$A = A_1 \cup \{m_1 a_{21}, ..., m_1 a_{2k_2}\};$$

then $n \in (h_1 + h_2)A$ (mod $m_1 m_2$), where hA denotes the set of all sums of h not necessarily distinct elements in A. Lemma 1 now follows from the observation that $|A| = k_1 + k_2 + 1$ and A is a basis of order $h_1 + h_2$ for $\mathbf{Z}/(m_1 m_2)$.

LEMMA 2. $m(h, 4) \geqslant \frac{1}{125} h^4 + O(h^3)$.

This is a special case ($k = 4$) of Theorem 1. Since its proof is quite long, we leave the proof to the last section of this paper.

Now we are ready to prove Theorem 1.

Proof of Theorem 1. If $k \equiv 0$ (mod 4), then $k = 4q$. Suppose that

$$h = qu + v, \qquad \text{where} \quad 0 \leqslant v < q.$$

If $h \geqslant h'$, then $m(h, k) \geqslant m(h', k)$. It follows from Lemmas 1 and 2 that

$$\begin{aligned} m(h, k) &\geqslant m(qu, 4q) \\ &\geqslant \underbrace{m(u, 4) \cdots m(u, 4)}_{q} \\ &\geqslant \left\{\frac{1}{125} u^4 + O(u^3)\right\}^q \\ &= \left(\frac{256}{125}\right)^q \left(\frac{u}{4}\right)^{4q} + O(u^{4q-1}) \\ &= \left(\frac{256}{125}\right)^q \left(\frac{h-v}{k}\right)^k + O(h^{k-1}) \\ &= \left(\frac{256}{125}\right)^{k/4} \left(\frac{h}{k}\right)^k + O(h^{k-1}). \end{aligned}$$

It is obvious that

$$m(h, 1) = h + 1 \qquad \text{for all} \quad h. \tag{4}$$

Therefore, from (1), (2), and (4), we have that, for $1 \leqslant v \leqslant 3$,

$$m(h, v) \geqslant \alpha_v \left(\frac{h}{v}\right)^v + O(h^{v-1}), \tag{5}$$

where

$$\alpha_v = \begin{cases} 1 & \text{if} \quad v = 1 \\ \frac{4}{3} & \text{if} \quad v = 2 \\ \frac{27}{16} & \text{if} \quad v = 3. \end{cases}$$

Now suppose that

$$k = u + v, \qquad \text{where} \quad u \equiv 0 \pmod 4 \quad \text{and} \quad 1 \leqslant v \leqslant 3.$$

Let $h = qk + r$, where $0 \leqslant r < k$. Then it follows from (5) and Lemma 1 that

$$\begin{aligned} m(h, k) &\geqslant m(h - r, k) \\ &= m(qu + qv, u + v) \\ &\geqslant m(qu, u)\, m(qv, v) \\ &\geqslant \left\{\left(\frac{256}{125}\right)^{u/4} q^u + O(q^{u-1})\right\} \cdot \{\alpha_v q^v + O(q^{v-1})\} \\ &= \alpha_v \left(\frac{256}{125}\right)^{u/4} \left(\frac{h-r}{k}\right)^{u+v} + O(q^{u+v-1}) \\ &= \alpha_v \left(\frac{256}{125}\right)^{\lfloor k/4 \rfloor} \left(\frac{h}{k}\right)^k + O(h^{k-1}), \end{aligned}$$

where α_v ($v = 1, 2, 3$) are defined as above. The proof of Theorem 1 is complete.

3. Proof of Theorem 2

Let A be a finite set of nonnegative integers. Let $n(h, A)$ denote the largest n so that every integer in $\{0, 1, ..., n\}$ is a sum of h elements in A. Define

$$n_k(h) = \max_{|A| = k+1} n(h, A).$$

It is easy to see that $m(h, k) \geqslant n_k(h)$ for all $h \geqslant 2$ and $k \geqslant 1$. Mrose [13] proved that

$$n_k(2) \geqslant \tfrac{2}{7}k^2 + O(k).$$

Windecker [14] proved that

$$n_k(3) \geqslant \tfrac{4}{81}k^3 + O(k^2).$$

Therefore, we have the following lemma.

LEMMA 3. *For k large,*

$$\begin{aligned} m(1, k) &= k+1, \\ m(2, k) &\geqslant \tfrac{2}{7}k^2 + O(k), \\ m(3, k) &\geqslant \tfrac{4}{81}k^3 + O(k^2). \end{aligned}$$

Proof of Theorem 2. Fix $h \geqslant 3$. Let k be a large positive integer. Suppose that

$$\begin{aligned} h &= 3q + r, \qquad \text{where} \quad 0 \leqslant r \leqslant 2, \\ k &= ph + v, \qquad \text{where} \quad 0 \leqslant v \leqslant h-1. \end{aligned}$$

Noting Lemmas 1 and 3, we have that

$$\begin{aligned} m(h, k) &\geqslant m(h, k-v) = m(3q+r, 3pq+pr) \\ &\geqslant m(3q, 3pq)\, m(r, pr) \\ &\geqslant (m(3, 3p))^q\, m(r, pr) \\ &\geqslant \left\{\frac{4}{3}p^3 + O(p^2)\right\}^q \{\beta_r p^r + O(p^{r-1})\} \\ &= \beta_r \left(\frac{4}{3}\right)^q \left(\frac{k-v}{h}\right)^{3q+r} + O(k^{h-1}) \\ &= \beta_r \left(\frac{4}{3}\right)^{\lfloor h/3 \rfloor} \left(\frac{k}{h}\right)^h + O(k^{h-1}), \end{aligned}$$

where β_h is defined as in Theorem 2. The proof of Theorem 2 is complete.

4. Order of Subsets of Asymptotic Bases

First we prove the following theorem.

Theoem 3. *For fixed $k \geqslant 4$ as $h \to \infty$,*

$$G_k(h) \geqslant \alpha_k \left(\frac{256}{125}\right)^{\lfloor k/4 \rfloor} \left(\frac{h}{k+1}\right)^{k+1} + O(h^k),$$

where α_k is defined as in Theorem 1.

Proof. We need to construct a basis A of order at most h which contains a k-element subset F so that the order of $A \backslash F$ as an asymptotic basis is equal to

$$\alpha_k \left(\frac{256}{125}\right)^{\lfloor k/4 \rfloor} \left(\frac{h}{k+1}\right)^{k+1} + O(h^k).$$

Let h be a large positive integer. Let

$$u = \left\lfloor \frac{h}{k+1} \right\rfloor \qquad \text{and} \quad h' = uk.$$

Suppose that $A_k = \{a_0, a_1, ..., a_k\}$ is an extremal basis of order h', i.e.,

$$m(h', A_k) = m(h', k) = m.$$

We may assume, without loss of generality, that $0 = a_0 < a_1 < \cdots < a_k$. Define

$$F = \{ua_1, ua_2, ..., ua_k\}.$$

Let $A = D \cup F$, where

$$D = \{id, id + 1 \mid i = 0, 1, 2, ...\},$$

and

$$d = um(h', k).$$

It is clear that

$$g(A \backslash F) = g(D) = d - 1 = \alpha_k \left(\frac{256}{125}\right)^{\lfloor k/4 \rfloor} \left(\frac{h}{k+1}\right)^{k+1} + O(h^k).$$

Now we show that A is of order h. Let n be a large positive integer. Suppose that

$$n = qu + r, \qquad \text{where} \quad 0 \leqslant r < u.$$

Since A_k is a basis of order h' for $\mathbf{Z}/(m(h',k))$, we see that

$$q \equiv a_{i_1} + \cdots + a_{i_{h'}} \pmod{m(h',k)}.$$

Hence, for some p,

$$\begin{aligned} n &= pum(h',k) + r + ua_{i_1} + \cdots + ua_{i_{h'}} \\ &= pd + \underbrace{1 + \cdots + 1}_{r} + ua_{i_1} + \cdots + ua_{i_{h'}}. \end{aligned}$$

Noting that

$$1 + r + h' \leqslant u + uk = \left\lfloor \frac{h}{k+1} \right\rfloor (k+1) \leqslant h,$$

we see that A is an asymptotic basis of order h. The proof of Theorem 3 is complete.

In a recent paper, Jia [10] also proved that, for any fixed $h \geqslant 2$,

$$2\left(\frac{k}{h-1}\right)^{h-1} + O(k^{h-2}) \leqslant G_k(h) \leqslant \frac{2k^{h-1}}{(h-1)!} + O(k^{h-2}).$$

The following improvement of the lower bound for $G_k(h)$ is immediate from Theorem 2 and Lemma 4 below.

THEOREM 4. *For fixed* $h \geqslant 3$ *as* $k \to \infty$,

$$G_k(h) \geqslant 2\beta_h \left(\frac{4}{3}\right)^{\lfloor (h-1)/3 \rfloor} \left(\frac{k}{h-1}\right)^{h-1} + O(k^{h-2}),$$

where β_h *is defined as in Theorem* 2.

LEMMA 4. *For any* $h \geqslant 3$ *and* $k \geqslant 1$,

$$G_k(h) \geqslant 2m(h-1,k) - 1.$$

Proof. Suppose that

$$A_k = \{0, a_1, ..., a_k\}$$

is an extremal basis of order $h-1$ for $\mathbf{Z}/(m(h-1,k))$, i.e., $m(h-1, A_k) = m(h-1,k)$. Let

$$D = \{id, id+1 \mid i = 0, 1, 2, ...\},$$

where $d=2m(h-1, k)$. Then D is an asymptotic basis of order

$$g(D)=d-1=2m(h-1, k)-1.$$

Let

$$A=D\cup\{2a_1+1, ..., 2a_k+1\}.$$

We need to show that A is an asymptotic basis of order h. Let n be a large positive integer.

If $n-h+1$ is even, then

$$\frac{n-h+1}{2}\equiv a_{i_1}+\cdots+a_{i_{h-1}} \qquad (\text{mod } m(h-1, k)),$$

where $a_{i_j}\in A_k$. Hence, for some $q\geqslant 0$,

$$n=qd+(2a_{i_1}+1)+\cdots+(2a_{i_{h-1}}+1),$$

thus, $n\in hA$. If $n-h$ is even, then, for some $p\geqslant 0$,

$$\frac{n-h}{2}=pm(h-1, k)+a_{i_1}+\cdots+a_{i_{h-1}}.$$

This implies

$$n=(pd+1)+(2a_{i_1}+1)+\cdots+(2a_{i_{h-1}}+1)\in hA.$$

Therefore, A is an asymptotic basis of order h, proving the lemma.

5. Proof of Lemma 2

Let $h\geqslant 105$. Define

$$t=\left[\frac{h}{5}\right];$$

$$a=4h-15t+7;$$

$$b=at+h-4t+2;$$

$$c=bt+2h-8t+4;$$

$$m=ct+3h-12t+5.$$

Define $A=\{0, 1, a, b, c\}$. We now show that A is a basis of order h for $\mathbf{Z}/(m)$; i.e., we need to show that $hA=\mathbf{Z}/(m)$.

Let n be any integer. We may assume without loss of generality that

$$b+c\leqslant n<m+b+c.$$

The proof divides into the following cases.

Case 1. Suppose $b+c(t+1)\leqslant n<m+b+c$. Since

$$\begin{aligned}(n-c(t+1)-b)+1+(t+1)&\leqslant (m-1-ct)+t+2\\&=3h-11t+6\\&\leqslant 3h-11\left(\frac{h}{5}-1\right)+6\\&=h-\left(\frac{h}{5}-17\right)\leqslant h,\end{aligned}$$

we see that

$$n=(n-c(t+1)-b)\cdot 1+b+c(t+1)\in hA.$$

Case 2. Suppose $b+cz\leqslant n<b+c(z+1)$ for $z\in[1,t]$. We divide this case into the following two subcases.

Case 2a. $b(t+1)+cz\leqslant n<b+c(z+1)$. Since $h\geqslant 105$, we see that

$$(n-b(t+1)-cz)+(t+1)+z\leqslant c-bt+2t+1=2h-6t+5<h.$$

Hence,

$$n=(n-b(t+1)-cz)\cdot 1+b(t+1)+cz\in hA.$$

Case 2b. Suppose $by+cz\leqslant n<b(y+1)+cz$ for $y\in[1,t]$. Again this case can be divided into the following two subcases.

Case 2bi. $at+by+cz\leqslant n<b(y+1)+cz$. Noting

$$(n-at-by-cz)+t+y+z\leqslant b-at-1+3t\leqslant h,$$

we see that

$$n=(n-at-by-cz)\cdot 1+at+by+cz\in hA.$$

Case 2bii. $a(x-1)+by+cz\leqslant n<ax+by+cz$ for $x\in[1,t]$. Let $w=ax+by+cz$. Then $w-a\leqslant n<w$. Once again, this case can be divided into the following four subcases.

Case 2bii.1. $w-a\leqslant n<w+ct-m$. Since

$$\begin{aligned}n-(w-a)&\leqslant \{w+ct-m-1\}-\{w-a\}\\&=ct-m+a-1\leqslant h-3t+1\\&\leqslant h-(x-1)-y-z,\end{aligned}$$

we see that

$$n=(n-w+a)\cdot 1+a(x-1)+by+cz\in hA.$$

Case 2bii.2. $w+ct-m\leqslant n<w+bt-c$. Since

$$\begin{aligned} n-(w+ct-m) &\leqslant \{w+bt-c-1\}-\{w+ct-m\} \\ &= bt-c-1-ct+m\leqslant h-4t \\ &\leqslant h-(x-1)-y-(z+t), \end{aligned}$$

we have that

$$\begin{aligned} n &\equiv (n-w-ct+m)+w+ct \pmod{m} \\ &= (n-w-ct+m)\cdot 1+ax+by+c(z+t)\in hA. \end{aligned}$$

Case 2bii.3. $w+bt-c\leqslant n<w+at-b$. Since

$$\begin{aligned} n-(w+bt-c) &\leqslant \{w+at-b-1\}-\{w+bt-c\} \\ &= at-b-1-bt+c=h-4t+1 \\ &\leqslant h-(x+(y+t)+(z-1)), \end{aligned}$$

we see that

$$n=(n-w-bt+c)\cdot 1+ax+b(y+t)+c(z-1)\in hA.$$

Case 2bii.4. $w+at-b\leqslant n<w$. Since

$$\begin{aligned} n-(w+at-b) &\leqslant (w-1)-(w+at-b)=h-4t+1 \\ &\leqslant h-\{(x+t)+(y-1)+z\}, \end{aligned}$$

we have

$$n=(n-w-at+b)\cdot 1+a(x+t)+b(y-1)+cz\in hA.$$

Therefore, $n\in hA$ for any $n\colon b+c\leqslant n<m+b+c$. Hence A is a basis of order h for $\mathbf{Z}/(m)$. It is clear that

$$m=\tfrac{1}{125}h^4+O(h^3).$$

The proof of Lemma 2 is complete.

References

1. J.-C. Bermond, F. Comellas, and D. F. Hsu, Distributed loop computer networks, a survey, *J. Parallel Distrib. Comput.*, to appear.
2. D. V. Chudnovsky, G. V. Chudnovsky, and M. M. Denneau, Regular graphs with small diameter as models for interconnection networks, preprint.
3. P. Erdős and D. F. Hsu, Distributed loop networks with minimum transmission delay, *Theoret. Comput. Sci.*, to appear.
4. P. Erdös and R. L. Graham, On bases with an exact order, *Acta Arith.* **37** (1980), 201–207.
5. R. L. Graham and N. J. A. Sloane, On additive bases and Harmonious graphs, *SIAM J. Algebra Discrete Math.* **1** (1980), 382–404.
6. G. Grekos, "Quelques aspects de la théorie additive des nombres," Thesis, Université de Bordeaux I, 1982.
7. R. K. Guy, "Unsolved Problems in Number Theory," Unsolved Problems in Intuitive Mathematics, Vol. I, Springer-Verlag, New York, 1981.
8. D. F. Hsu and X.-D. Jia, Extremal problems in the construction of distributed loop networks, *SIAM J. Discrete Math.*, to appear.
9. X.-D. Jia, Exact order of subsets of asymptotic bases in additive number theory, *J. Number Theory* **28** (1988), 205–218.
10. X.-D. Jia, On the order of subsets of asymptotic bases, *J. Number Theory* **37** (1991), 37–46.
11. J. C. M. Nash, "Results on Bases in Additive Number Theory," Thesis, Rutgers University, New Brunswick, NJ, 1985.
12. M. B. Nathanson, The exact order of subsets of additive bases, *in* "Proceedings, Number Theory Seminar, 1982," pp. 273–277, Lecture Notes in Mathematics, Vol. 1052, Springer-Verlag, New York/Berlin, 1984.
13. A. Mrose, Untere Schranken für die Reichweiten von Extremalbasen fester Ordnung, *Abh. Math. Sem. Univ. Hamburg* **48** (1979), 118–124.
14. R. Windecker, Eine Abschittsbasis dritter Ordnung, *Norske Vid. Selsk. Skr. (Trondheim)* **9** (1976), 1–3.