ACTA ARITHMETICA
LXX.1 (1995)

A remark on B_2-sequences in $\mathrm{GF}[p,x]$

by

JOHN R. BURKE (Spokane, Wash.)

In the classical case, a B_2-sequence $A=\{a_i\}_{i=1}^{\infty}$ is an increasing sequence of non-negative integers for which the equation $a_i+a_j=n$, $i\le j$, has at most one solution for any positive integer n. Let $A(n)=|A\cap[1,n]|$. A question posed by Sidon was, in essence, what is the maximum growth rate of $A(n)$ subject to A being a B_2-sequence? It has proven to be a quite difficult problem with one of the major results, due to Erdős and Turán [3], being $A(n)<n^{1/2}+O(n^{1/4})$.

In the following the concept of a B_2-sequence in a polynomial ring over a finite field, denoted by $\mathrm{GF}[p,x]$, will be made precise and a result analogous to the Erdős–Turán result in the integers will be established.

To begin with, we need some kind of ordering on $\mathrm{GF}[p,x]$. Order $\mathrm{GF}(p)$ by $0<1<\ldots<p-1$. For any $f(x)\in\mathrm{GF}[p,x]$, define the *norm* of $f(x)$ to be the value of $f(p)$, viewing $f(x)$ as an element of $\mathbb{Z}[x]$. Denote this by $\|f(x)\|$.

Now for $A\subset\mathrm{GF}[p,x]$ and $f(x)\in\mathrm{GF}[p,x]$ let

$$R_A(f)=\sum_{f(x)=a_i(x)+a_j(x)}1,$$

where $\|a_i(x)\|\le\|a_j(x)\|$, $\deg(a_j(x))\le\deg(f(x))$, $a_i(x),a_j(x)\in A$.

Thus $R_A(f)$ is the number of ways a given polynomial $f(x)$ can be written as the sum of elements of A with smaller degree.

DEFINITION. Let $A\subseteq\mathrm{GF}[p,x]$ be an increasing (in norm) sequence. A is said to be a *B_2-sequence* if $R_A(f)\le1$ for all $f(x)\in\mathrm{GF}[p,x]$. (In general, A is a $B_h(g)$-sequence if the number of solutions to $a_{i_1}(x)+\ldots+a_{i_h}(x)=f(x)$, $\|a_{i_1}(x)\|\le\ldots\le\|a_{i_h}(x)\|$, $\deg(a_{i_j}(x))\le\deg(f(x))$, is no more than g.)

For a sequence $A\subseteq\mathrm{GF}[p,x]$, define

$$A(n)=\sum_{\substack{a(x)\in A\\0\le\deg(a(x))\le n}}1\quad\text{where }\deg(0)=-\infty.$$

Our goal is to study the behavior of $A(n)$ for large n subject to the condition that $R_A(f) \le 1$ for all $f(x) \in \mathrm{GF}[p,x]$. In particular, what is the maximum growth rate of $A(n)$ if A is a B_2-sequence?

DEFINITION. Let $F_h(n)$ be the maximum number of elements in a set $A \subseteq \mathrm{GF}[p,x]$ of degree less than or equal to n such that the sums $a_1(x) + \ldots + a_h(x)$, $a_i(x) \in A$, are all distinct.

The main purpose of this article is to establish the upper bound for $F_2(n)$. To this end we have the following analogue to the result obtained by Erdős and Turán [3].

THEOREM 1. $F_2(n) < p^{(n+1)/2} + O(p^{(n+1)/4})$.

Proof. Let $r = F_2(n)$ and let $A = \{a_i(x)\}_{i=1}^r$ be a set of polynomials for which $\deg(a_i(x)) \le n$ for $1 \le i \le r$ and $R_A(f) \le 1$ for all $f(x) \in \mathrm{GF}[p,x]$. Let u be a positive integer, $u < p^{n+1}$, and consider the sets

$$I_m = \{f(x) : \|f(x)\| \in [-u+m, -1+m]\}, \qquad 1 \le m \le p^{n+1} + u.$$

Let $A_m = |A \cap I_m|$. Since each $a_i(x)$ occurs in exactly u of the sets of the type I_m, it follows that

$$\sum_{m=1}^{p^{n+1}+u} A_m = ru.$$

The number of pairs $(a_i(x), a_j(x))$ with $\|a_i(x)\| < \|a_j(x)\|$ in a given I_m is $\frac{1}{2}A_m(A_m-1)$ so that the total number of such pairs, each lying in some I_m, is

$$\frac{1}{2}\sum_{m=1}^{p^{n+1}+u} A_m(A_m-1).$$

Thus

$$(ru)^2 = \Big(\sum_{m=1}^{p^{n+1}+u} A_m\Big)^2 \le \Big(\sum_{m=1}^{p^{n+1}+u} 1\Big)\Big(\sum_{m=1}^{p^{n+1}+u} A_m^2\Big) = (p^{n+1}+u)\sum_{m=1}^{p^{n+1}+u} A_m^2,$$

so that

$$(*) \quad \frac{1}{2}\sum_{m=1}^{p^{n+1}+u} A_m(A_m-1) = \frac{1}{2}\Big(\sum_{m=1}^{p^{n+1}+u} A_m^2\Big) - \frac{1}{2}\Big(\sum_{m=1}^{p^{n+1}+u} A_m\Big)$$
$$\ge \frac{(ru)^2}{2(p^{n+1}+u)} - \frac{1}{2}ru = \frac{ru}{2}\bigg(\frac{ru}{p^{n+1}+u} - 1\bigg).$$

Now for each pair $(a_i(x), a_j(x))$ with $\|a_i(x)\| < \|a_j(x)\|$ it follows that the differences $a_i(x)-a_j(x)$ are all distinct. If not, there exist distinct i, j, k, l such that $a_i(x)-a_j(x) = a_k(x)-a_l(x)$ so that $a_i(x)+a_l(x) = a_k(x)+a_j(x)$, contrary to $R_A(f) \le 1$ for all $f(x) \in \mathrm{GF}[p,x]$.

There is little that can be said about the polynomial $a_i(x) - a_j(x)$ although it may be noted that each pair $(a_i(x), a_j(x))$ satisfying the condition

$\|a_j(x)\| - \|a_i(x)\| = d$ must occur in $u-d$ of the sets I_m. There are at most $\sum_{d=1}^{u-1}(u-d) = \frac{1}{2}u(u-1)$ such pairs. From (∗) it now follows that

$$\frac{1}{2}u(u-1) \geq \frac{1}{2}\sum_{m=1}^{p^{n+1}+u} A_m(A_m-1) \geq \frac{ru}{2}\left(\frac{ru}{p^{n+1}+u}-1\right)$$

or

$$u(u-1)(p^{n+1}+u) \geq ru(ru-(p^{n+1}+u)) > r(ru-2p^{n+1}).$$

Thus

$$0 > r^2u - 2rp^{n+1} - u(p^{n+1}+u).$$

Solving the inequality for r yields

$$r < \frac{p^{n+1}}{u} + \left(\left(\frac{p^{n+1}}{u}\right)^2 + u + p^{n+1}\right)^{1/2}.$$

Letting $u = p^{3(n+1)/4}$ we have $r < p^{(n+1)/2} + O(p^{(n+1)/4})$ as claimed.

Another natural question to consider is the minimal growth rate of $A(n)$ under the restriction that $R_A(f) \geq 1$.

Definition [1]. A set $B \subset \mathrm{GF}[p,x]$ is a *basis of order* h if for any $f(x) \in \mathrm{GF}[p,x]$ one has

$$f(x) = \sum_{i=1}^{k} b_i(x), \quad b_i(x) \in B,\ \deg(b_i(x)) \leq \deg(f(x)),\ \text{for some } k \leq h.$$

Asking that $R_A(f) \geq 1$ for all $f(x) \in \mathrm{GF}[p,x]$ is equivalent to asking that A be a basis of order 2. There are results on the density of bases for GF$[p,x]$ as well as essential components ([1], [2]), but not on the minimal growth of the function $A(n)$. To this end, let

$$A = \Big\{\sum_{i=0}^{k} a_i x^{2i} : k \in \mathbb{Z}_0, a_i \in \mathrm{GF}(p)\Big\} \cup \Big\{\sum_{j=0}^{l} a_j x^{2j+1} : l \in \mathbb{Z}_0, a_j \in \mathrm{GF}(p)\Big\}.$$

By the construction of A, one observes that the growth rate of $A(n)$ is essentially $p^{(n+1)/2}$. From a combinatoric point of view, the number of elements in $A+A$ of degree n or less is at most $\frac{1}{2}A(n)(A(n)+1)$. Thus $\frac{1}{2}A(n)(A(n)+1) \geq p^{n+1}-1$ if $R_A(f) \geq 1$. For our particular example it is easily seen that $A(2k+1) = 2(p^{k+1}-1)$ and $A(2k) = p^k(p+1)$ so that $A(n) \leq 2p^{(n+1)/2}$. Thus we have

Theorem 2. *There exists a basis of order* 2 *such that* $A(n) \ll p^{(n+1)/2}$ *where the implied constant is no larger than* 2.

A similar question may be asked about the growth rate of $A(n)$ if $R_A(f) \geq 1$ without the restriction that $\deg(a_i(x)) \leq \deg(f(x))$. That is, what can be said about the minimal growth rate of $A(n)$ when A is a "weak basis" of order 2 where a weak basis is defined below.

Definition [1]. A set $B \subset \mathrm{GF}[p,x]$ is a *weak basis of order* h if for any $f(x) \in \mathrm{GF}[p,x]$ one can write

$$f(x) = \sum_{i=1}^{k} b_i(x), \qquad b_i(x) \in B, \text{ for some } k \le h.$$

In this direction we have

Theorem 3. *For each* $\varepsilon > 0$ *there exists a weak basis* A *of order* 2 *such that*

$$\liminf_{n\to\infty} \frac{A(n)}{\ln(n)p^{\ln(n)}} < \varepsilon.$$

Proof. Let k be an arbitrary but fixed integer, $k \ge 2$. Define

$$A^{(n)} = \{x^{k^n} + f(x) : \deg(f(x)) \le n\} \cup \{(p-1)x^{k^n}\} \quad \text{and} \quad A = \bigcup_{n=1}^{\infty} A^{(n)}.$$

To show A is a weak basis of order 2, let $f(x) \in \mathrm{GF}[p,x]$ with $\deg(f(x)) \le n$. Then $f(x) = (x^{k^n} + f(x)) + (p-1)x^{k^n} \in A + A$. To compute the growth rate of $A(n)$, note that $A(k^n) \le n + \sum_{i=1}^{n} p^i \le np^n$. Let $N = k^n$ so that

$$A(N) \le \frac{\ln(N)p^{\ln(N)}p^{1/\ln(k)}}{\ln(k)}$$

or

$$\frac{A(N)}{\ln(N)p^{\ln(N)}} < \frac{p^{1/\ln(k)}}{\ln(k)}.$$

As the limit of the right hand side is 0 as $k \to \infty$, the theorem is established.

References

[1] J. R. Burke, *A notion of density and essential components in* GF$[p,x]$, Acta Arith. 44 (1984), 299–306.

[2] J. Cherly et J.-M. Deshouillers, *Un théorème d'addition dans* $\mathbb{F}_q[x]$, J. Number Theory 34 (1990), 128–131.

[3] P. Erdős and P. Turán, *On a problem of Sidon in additive number thory and some related problems*, J. London Math. Soc. 16 (1941), 212–215; Addendum (by P. Erdős), ibid. 19 (1944), 208.

DEPARTMENT OF MATHEMATICS AND COMPUTER SCIENCE
GONZAGA UNIVERSITY
SPOKANE, WASHINGTON 99258
U.S.A.

Received on 31.5.1994
and in revised form on 11.8.1994 (2623)