Bull. Korean Math. Soc. **50** (2013), No. 2, pp. 399–405
http://dx.doi.org/10.4134/BKMS.2013.50.2.399

THIN ADDITIVE BASES FOR MONIC POLYNOMIALS IN $\mathbb{F}_q[t]$

Andreas O. Bender, Bo-Hae Im, and Yoonjin Lee

Abstract. We explicitly construct a thin basis for the set $\mathbf{M}$ of monic polynomials in one variable t over a finite field $\mathbb{F}_q$.

1. Introduction

Additive problems in the natural numbers are often expressible in terms of bases. In these terms, the Goldbach conjecture says that the primes are a basis of order 2 for the set of even positive integers larger than 2, while the theorem by Lagrange says that the squares are a basis of order 4 for the natural numbers.

Definition 1.1. Let S be a nonempty set with addition and valuation v. For an integer $h \geq 2$ and a subset $A \subset S$, we define the sumset

$$hA = \{f_1 + \cdots + f_h \mid f_i \in A \text{ and } v(f_1 + \cdots + f_h) \geq v(f_i) \text{ for all } i = 1, \ldots, h\}.$$

The set A is called a *basis* of order h for S if $S \subseteq hA$, and A is an *asymptotic basis of order h for S* if hA contains all but finitely many elements of S.

Remark 1.2. Note that for $S = \mathbb{N}$ with the usual absolute value $v = |\cdot|$, there is no need to impose the conditions $v(f_1 + \cdots + f_h) \geq v(f_i)$. For $S = \mathbb{F}_q[t]$ with the degree valuation, however, these conditions are nontrivial if the characteristic of $\mathbb{F}_q$ is not larger than h.

Received February 23, 2011; Revised May 31, 2012.

2010 *Mathematics Subject Classification.* Primary 11B13; Secondary 11T55.

Key words and phrases. additive bases, thin bases, Raikov-Stöhr type bases.

Bo-Hae Im was supported by the Chung-Ang University Research Grant in 2012 and by the National Research Foundation of Korea Grant funded by the Korean Government (MEST) (NRF-2011-0015557) and, Andreas Bender was supported by the Priority Research Centers Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education, Science and Technology (project No.2012047640), and Yoonjin Lee was supported by the Priority Research Centers Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education, Science and Technology (No.2012-0006691) and by the National Research Foundation of Korea (NRF) grant funded by the Korean Government (MEST) (No.2011-0015684).

For the set S of positive integers, Rohrbach [5] showed that the number of elements less than or equal to n in a basis of order h is bounded from below by a constant multiple of $n^{1/h}$. Raikov [4] and Stöhr [6] independently gave an explicit construction of a basis for positive integers which actually achieves this lower bound; this is what is called a *thin basis* and its precise definition will be given in Section 4. An easily accessible reference for these results is a recent survey by Nathanson [3].

The purpose of this paper is to give an analogous result for the set of monic polynomials in the polynomial ring $\mathbb{F}_q[t]$ over the finite field $\mathbb{F}_q$ of order q. We give a lower bound for the size of a basis and we construct a *thin basis* achieving the lower bound for its size.

We begin with some basic definitions in Section 2. Section 3 contains the main result of this paper, an explicit construction of a thin basis for the set $\mathbf{M}$, using a result by Jia [2] on thin bases for finite abelian groups. In Section 4 we establish a lower bound for the size of a basis for the set $\mathbf{M}$ of monic polynomials in $\mathbb{F}_q[t]$. In the last section we also give an example of a basis of Raikov-Stöhr type for $\mathbf{M}$ in $\mathbb{F}_q[t]$ with q prime, which turns out to be a thin basis for $\mathbf{M}$ only if $q = 2$.

2. Monic polynomials in $\mathbb{F}_q[t]$

Rather than considering the whole ring $\mathbb{F}_q[t]$, we restrict our attention to the set of monic polynomials as an analogue of positive integers; for more background on this see [1]. There exists a total order on the ring $\mathbf{Z}$ and the positive integers form a monoid. However, on the ring $\mathbb{F}_q[t]$ there is only a partial order defined by the degree, and the monic polynomials do not form a monoid. This last fact, which amounts to saying that the sum of two monic polynomials of the same degree is not monic, will play a significant role in what follows.

For any set A of polynomials over $\mathbb{F}_q$ and a nonnegative real number x, the *counting function of* A, denoted by $A(x)$, counts the number of polynomials in A whose degree is at most x, that is,

$$A(x) = \sum_{\substack{f \in A \\ 0 \leq \deg(f) \leq x}} 1.$$

We set the degree of the zero polynomial to ∞. We write $f \gg g$ if there exists a constant $c > 0$ such that $|f(x)| \geq c\,|g(x)|$ for all nonnegative real numbers x.

3. Construction of an explicit basis for monic polynomials in $\mathbb{F}_q[t]$

We include the proof of the following lemma because our situation allows a slight improvement of the constant. The proof is almost identical to parts of the proof of the main theorem in [2].

Lemma 3.1. *Let $h \geq 2$ be an integer, $q = p^s$ with p a prime and $c_h = h(1+p^{-1/h})^{h-1}$. For each positive integer n, let H_n be the set of all polynomials in $\mathbb{F}_q[t]$ of degree at most n. Then there exists a basis T_n of order h for H_n such that*

$$|T_n| \leq c_h q^{\frac{n+1}{h}}.$$

Proof. We first note that H_n is an abelian group of order $q^{n+1}(= p^{s(n+1)})$ which we write additively. According to [2, Lemma 1] and the proof of the main theorem in [2], we decompose H_n as $H_n = H \oplus K$, where $|H| = p^{uh}$, $H = A_1 + A_2 + \cdots + A_h$ with $|A_i| = p^u$ and $K = K_1 \oplus \cdots \oplus K_r$ with $r \leq h-1$ and each K_j isomorphic to $\mathbb{F}_p$. In fact, u can be chosen to be the ceiling value $\lceil \frac{s(n+1)-(h-1)}{h} \rceil$, so we have $s(n+1) - uh \leq h-1$. Note that $r + uh = s(n+1)$. By [2, Lemma 2], each cyclic group K_j is a sum of subsets $A_{j1}, \ldots, A_{jh}$ with $|A_{ji}| < |K_j|^{1/h} + 1 = p^{1/h} + 1$. The A_{ji} are constructed as follows. With $v = \lceil p^{1/h} \rceil + 1$, we set $A_{ji} = \{0, v^{i-1}, \ldots, (v-1)v^{i-1}\}$ for $i = 1, \ldots, h$ and $j = 1, \ldots, r$.

Let $T_n := \bigcup_{k=1}^h B_k$, where $B_k = A_k + A_{1k} + \cdots + A_{rk}$. Then T_n forms a basis for H_n as in [2]. Replacing the lower bound equal to 2 for $|K_i|$ by p, the new bound for $|T_n|$ is given by

$$|T_n| \leq \sum_{k=1}^h |B_k| < \sum_{k=1}^h \left(p^u \prod_{1 \leq j \leq r} \left(|K_j|^{1/h} + 1 \right) \right) \leq h \left(1 + p^{-1/h} \right)^{h-1} q^{\frac{n+1}{h}},$$

where we use the identity $q^{n+1} = (p^u)^h p^r$ in the last inequality. Therefore, T_n is a thin basis for H_n with $|T_n| < c_h q^{\frac{n+1}{h}}$. □

The following theorem is our main result, an explicit construction of a basis for the set of monics $\mathbf{M}$ in $\mathbb{F}_q[t]$ with the estimate of its size.

Theorem 3.2. *Suppose $q = p^s$ with p a prime and $h \geq 2$ an integer. Let T_n be a basis for H_n as given in Lemma 3.1. We then define*

$$A_0 = \{0, 1\}, \quad A_1 = \{t + a \mid a \in \mathbb{F}_q\}, \text{ and for each } k \geq 2,$$
$$A_k = \left\{ t^k + at^{k-1} + b(t) \mid a \in \mathbb{F}_q, b(t) \in T_{k-2} \right\} \cup \left\{ t^{k-1} + b(t) \mid b(t) \in T_{k-2} \right\}.$$

Then $A := \bigcup_{k=0}^\infty A_k$ is a basis of order h for $\mathbf{M}$ in $\mathbb{F}_q[t]$ which satisfies

$$A(x) \leq c_h (q+1) \left(\frac{q^{x/h} - 1}{q^{1/h} - 1} \right) \ll q^{x/h}$$

for all real numbers $x \geq 0$, where $c_h = h(1 + p^{-1/h})^{h-1}$.

Proof. For each integer $n \geq 0$, let H_n be the set of all polynomials of degree $\leq n$ in $\mathbb{F}_q[t]$. Then by Lemma 3.1 there exists a basis T_n of order h for H_n such that

$$|T_n| \leq c_h q^{\frac{n+1}{h}},$$

where $c_h = h(1 + p^{-1/h})^{h-1}$.

First we show that A is a basis of order h for $\mathbf{M}$. Let $f(t) \in \mathbf{M}$ be the monic polynomial of degree n given by

$$f(t) = t^n + a_{n-1}t^{n-1} + \cdots + a_0, \text{ where } a_i \in \mathbb{F}_q.$$

For the degrees 0 and 1, this polynomial $f(t)$ can trivially be represented as a sum of h basis elements since we have $1 = 1 + 0 + \cdots + 0$ in case of degree 0 (note that $\deg(0) \leq 0$) and $t - a = t - a + 0 + \cdots 0$ in case of degree 1 (note that $\deg(0) \leq 1$). Now let $n \geq 2$. Then there exist unique nonnegative integers m, r such that

$$h = mp + r \text{ with } 0 \leq r < p.$$

Since $f(t) - t^n - a_{n-1}t^{n-1} \in H_{n-2}$ and T_{n-2} is a basis for H_{n-2}, there exist $g_1, \ldots, g_h \in T_{n-2}$ such that

$$f(t) = t^n + a_{n-1}t^{n-1} + g_1 + g_2 + \cdots + g_h.$$

By the definition of H_{n-2}, we have that $\deg(g_i) \leq n - 2 < n = \deg(f)$.

If $r = 0$, then $h = mp$, so $ht^{n-1} = 0$ and

$$f(t) = (t^n + (a_{n-1} + 1)t^{n-1} + g_1) + (t^{n-1} + g_2) + \cdots + (t^{n-1} + g_h) \in hA_n \subseteq hA.$$

Suppose $0 < r < p$. We set $g(t) = t^n + a_{n-1}t^{n-1} + g_1 + g_2 + \cdots + g_r$. Since we are in characteristic p and $mp = h - r$, we have

$$f(t) - g(t) = mpt^{n-1} + f(t) - g(t) = \sum_{i=r+1}^{h} \left(t^{n-1} + g_i\right),$$

so $f(t) - g(t)$ is in $\underbrace{A_n + \cdots + A_n}_{mp \text{ times}} \subseteq mpA$. We can write

$$\begin{aligned} g(t) = {} & \left(t^n + (a_{n-1} - r + 1)t^{n-1} + g_1\right) \\ & + \left(t^{n-1} + g_2\right) + \cdots + \left(t^{n-1} + g_r\right) \in rA_n \subseteq rA, \end{aligned}$$

where by abuse of notation the letter r denotes both a natural number and its image in $\mathbb{F}_p$. This implies that

$$f(t) = g(t) + g_{r+1} + \cdots + g_h \in (r + mp)A = hA$$

and

$$\deg(g) = n \leq \deg(f) \text{ and } \deg(g_i) \leq n - 2 < \deg(f),$$

so A is indeed a basis of order h for $\mathbf{M}$.

Now we compute $A(x)$ for real numbers $x \geq 0$. Let x be a nonnegative real number and n be the largest integer with $n \leq x$. Then

$$\begin{aligned} A(x) = A(n) &\leq \sum_{k=0}^{n} |A_k| \\ &= |A_0| + |A_1| + \sum_{k=2}^{n} (q|T_{k-2}| + |T_{k-2}|) \end{aligned}$$

$$
\begin{aligned}
&= 2 + q + \sum_{k=2}^{n} (q+1)|T_{k-2}| \\
&\leq 2 + q + c_h(q+1)\left(\frac{q^{n/h} - q^{1/h}}{q^{1/h} - 1}\right) \\
&\leq c_h(q+1)\left(\frac{q^{n/h} - q^{1/h}}{q^{1/h} - 1} + 1\right) \\
&\leq c_h(q+1)\left(\frac{q^{n/h} - 1}{q^{1/h} - 1}\right) \\
&\leq c_h(q+1)\left(\frac{q^{x/h} - 1}{q^{1/h} - 1}\right) \ll q^{x/h}
\end{aligned}
$$

and the proof is complete. □

Corollary 3.3. *Let h be an integer greater than 1. Every monic polynomial in $\mathbb{F}_q[t]$ of degree $n \geq 1$ can be written as a sum of one monic polynomial of degree n and $h-1$ monic polynomials of degree $n-1$.*

Proof. The proof of Theorem 3.2 shows that each monic $f \in \mathbf{M}$ of degree n can be written as follows: If $n = 1$, then

$$
f(t) = t + a = (t + (a - h + 1)) + \underbrace{1 + \cdots + 1}_{(h-1) \text{ summands}}
$$

and if $n \geq 2$, then

$$
f(t) = (t^n + at^{n-1} + b_1(t)) + (t^{n-1} + b_2(t)) + \cdots + (t^{n-1} + b_h(t)),
$$

where $a \in \mathbb{F}_q$ and each $b_i(t) \in \mathbb{F}_q[t]$ is of degree $\leq n-2$. □

4. A lower bound for the size of a basis of finite order

Proposition 4.1. *Let $h \geq 2$ and $A = \{f_k\}_{k=1}^{\infty}$ be a set of polynomials in $\mathbb{F}_q[t]$ with $f_1 = 0$ and f_k monic for each $k \geq 2$ such that $f_i \neq f_j$ for all $i \neq j$ and $\deg(f_k) \leq \deg(f_{k+1})$ for all $k \geq 1$.*

If A is an asymptotic basis of order h for $\mathbf{M}$, then

$$
A(x) \gg q^{x/h} \tag{1}
$$

for all sufficiently large real numbers x. If A is a basis of order h for $\mathbf{M}$, then the inequality (1) holds for all real numbers $x \geq 0$.

Proof. We closely follow the proof of the analogous statement for integers given in [5] (see [3, Theorem 1] for a more easily accessible reference). If A is an asymptotic basis of order h for $\mathbf{M}$, there exists an integer n_0 such that every monic polynomial $f \in \mathbb{F}_q[t]$ with $\deg(f) \geq n_0$ can be represented as a sum of h elements of A whose degrees are less than or equal to $\deg(f)$. Let $x \geq n_0$ be a real number and let n be the largest integer $\leq x$. Then $A(x) = A(n)$. For estimating $A(x)$ we compare the cardinalities of the two sets S and $\tilde{S}$ defined as follows.

$$S = \{f \in \mathbf{M} \mid n_0 \le \deg f \le n\},$$
$$\tilde{S} = \{g_1 + g_2 + \cdots + g_h \mid g_i \in A,\ \deg g_i \le n,\ i = 1, \ldots, h\}.$$

Since certainly $S \subseteq \tilde{S}$, we have

$$q^n < q^n + q^{n-1} + \ldots + q^{n_0} = |S| \le |\tilde{S}| = \binom{A(n)+h}{h} < \frac{(A(n)+h)^h}{h!}$$

and equation (1) follows.

If A is a basis of order h for $\mathbb{F}_q[t]$, then 1, as the monic polynomial of degree 0, must be contained in A and therefore $A(n) > 0$ for all $n \ge 1$. Therefore $A(x) \gg q^{x/h}$ for all $x \ge 1$ and the proof is complete. $\square$

Definition 4.2. Let A be a subset of the set $\mathbf{M}$ of monic polynomials in $\mathbb{F}_q[t]$. If an asymptotic basis A of order h for $\mathbf{M}$ achieves the lower bound for the size $A(x) \gg q^{x/h}$ given by Proposition 4.1, that is, if we have $A(x) \ll q^{x/h}$, then A is called a *thin asymptotic basis* for $\mathbf{M}$. If A is a basis A of order h for $\mathbf{M}$ and $A(x) \ll q^{x/h}$, then A is called a *thin basis* of order h for $\mathbf{M}$.

Remark 4.3. The basis found in Theorem 3.2 is thus in fact a thin basis of order h for $\mathbf{M}$ in $\mathbb{F}_q[t]$.

Remark 4.4. As mentioned in Remark 1.2, if the characteristic of $\mathbb{F}_q$ is not larger than h in the definition of a basis of a set S, then the additional condition $v(f_1 + \cdots + f_h) \ge v(f_i)$ for all $i = 1, \ldots, h$ is not trivial. Finding a lower bound for a basis of S without that condition is therefore still an open question.

5. Another example of a basis

The following theorem gives another example of a basis for $\mathbf{M}$ in $\mathbb{F}_p[t]$ with p a prime. The Raikov-Stöhr construction in [3, Theorem 2] can be carried out over $\mathbb{F}_p[t]$ and it works exactly like the one for the case of integers. In particular, this example provides a thin basis for $\mathbf{M}$ in $\mathbf{F}_2[t]$.

Theorem 5.1 (Raikov-Stöhr type basis for monics in $\mathbb{F}_p[t]$)**.** *Fix a prime p. Let $h \ge \max(2, p-1)$ be given and let $\ell = \left[\frac{h}{p-1}\right]$. For each $i = 0, 1, \ldots, \ell - 1$, let $W_i = \{i, \ell + i, 2\ell + i, \ldots\}$ denote the set of all nonnegative integers that are congruent to i modulo ℓ, and let $\mathcal{E}(W_i)$ be the set of all finite subsets of W_i. Let*

$$A_i = \left\{ g = \sum_{\substack{e \in E \\ c_e \in \mathbb{F}_p}} c_e t^e : E \in \mathcal{E}(W_i) \text{ and } c_{\deg(g)} = 1 \right\}.$$

Then $A := \bigcup_{k=0}^{\ell-1} A_k$ *is a basis of order* h *for* $\mathbf{M}$ *in* $\mathbb{F}_p[t]$ *such that for all* $x > 0$,

$$A(x) \ll p^{(p-1)x/h}.$$

In particular, when $p = 2$, *the set* A *is a thin basis for* $\mathbf{M}$ *in* $\mathbb{F}_2[t]$, *i.e.,* A *satisfies*

$$2^{x/h} \ll A(x) \ll 2^{x/h}.$$

Acknowledgement. We thank the Korea Institute for Advanced Study for their support and hospitality. Our sincere gratitude goes to the anonymous referee for his helpful comments for our manuscript, in particular for the observation that in positive characteristic a bound on the degrees is needed in the definition of a basis.

References

[1] G. W. Effinger, K. Hicks, and G. Mullen, *Integers and polynomials: comparing the close cousins* $\mathbf{Z}$ *and* $\mathbb{F}_q[x]$, Math. Intelligencer **27** (2005), no. 2, 26–34.
[2] X.-D. Jia, *Thin bases for finite abelian groups*, J. Number Theory **36** (1990), no. 2, 254–256.
[3] M. B. Nathanson, *Cassels bases*, In 'Additive Number Theory', Festschrift in honor of the sixtieth birthday of Melvyn B Nathanson. David Chudnovsky and Gregory Chudnovsky, editors. Springer–Verlag New York, 2010. Also available from `http://arxiv.org/abs/0905.3144`.
[4] D. Raikov, *Über die Basen der natürlichen Zahlenreihe*, Mat. Sbornik N.S. **44** (1937), no. 2, 595–597.
[5] H. Rohrbach, *Ein Beitrag zur additiven Zahlentheorie*, Math. Z. **42** (1937), no. 1, 1–30.
[6] A. Stöhr, *Eine Basis h-ter Ordnung für die Menge aller natürlichen Zahlen*, Math. Z. **42** (1937), no. 1, 739–743.

Andreas O. Bender
Pohang Mathematics Institute
Pohang University of Science and Technology
Pohang 790-784, Korea
E-mail address: `andreas@postech.ac.kr`

Bo-Hae Im
Department of Mathematics
Chung-Ang University
Seoul 156-756, Korea
E-mail address: `imbh@cau.ac.kr`

Yoonjin Lee
Department of Mathematics
Ewha Womans University
Seoul 120-750, Korea
E-mail address: `yoonjinl@ewha.ac.kr`