Additive Theory for $\mathbf{F}_q[x]$ by Probability Methods

By JØRGEN CHERLY

Det Kongelige Danske Videnskabernes Selskab
Matematisk-fysiske Meddelelser **40**:12

Kommissionær: Munksgaard
København 1983

Synopsis

Let $\mathbf{F}_q$ be a finite field and let $\mathbf{F}_q[x]$ denote its polynomialring. Let $A \subset \mathbf{F}_q[x]$ denote a sequence of polynomials and $A(n)$ the counting number Card $\{f \in A | \partial f \leq n\}$ where ∂f denotes the degree of f.

A sequence $A \subset \mathbf{F}_q[x]$ is said to be an asymptotic basis of order 2 if all polynomials of sufficiently high degree lie in $A+A = 2A$ and an asymptotic complementary sequence is defined analogously.

Let further P denote the sequence of irreducible polynomials in $\mathbf{F}_q[x]$. The subject of this paper is to translate two principal results of a chapter of the book of H. Halberstam and K. F. Roth to the case of a polynomialring over a finite field.

We shall use an idea of Erdös to make the space of polynomial sequences into a probability space.

We then prove the following two existence theorems by showing that the property one looked for holds with probability 1.

There exist:

— a thin asymptotic basis of order two

— an asymptotic complementary sequence to P such that the counting number $B(n) \ll n^2$.

JØRGEN CHERLY
Université de Bordeaux I
Mathematiques et Informatique
351, cours de la Liberation
33405 Talence Cedex

Det Kongelige Danske Videnskabernes Selskab 1983
Printed in Denmark by Bianco Lunos Bogtrykkeri A/S. ISSN 0023-3323. ISBN 87-7304-138-6

§1. Introduction .

Let $\mathbf{F}_q$ be a finite field of $q = p^m$, $m \in N$ elements and let $\mathbf{F}_q[x]$ denote its polynomialring. The degree of a polynomial is denoted ∂f. We denote by sign f the leading coefficient of f. The absolute value of a polynomial f is defined by $|f| = q^{\partial f}$. We can assume that the polynomials in $\mathbf{F}_q[x]$ are arranged in lexicographical order $(=<)$ based on an arbitrary ordering of $\mathbf{F}_q$.

Let $A \subset \mathbf{F}_q[x]$ denote a sequence of polynomials and $A(n)$ denote Card $\{f \in A | \partial f \leq n\}$. Further let P denote the sequence of irreducible polynomials in $\mathbf{F}_q[x]$.

We denote by $r_f(A)$ the number of representations of f in the form:

$$f = f' + f'', \quad f', f'' \in A, \quad \partial f' = \partial f, \quad \partial f'' < \partial f. \tag{1.1}$$

Also let $R_f(A)$ denote the number of representations of f in the form:

$$f = p + f', \quad p \in P, \quad f' \in A, \quad \partial p = \partial f, \quad \text{sign } p = \text{sign } f. \tag{1.2}$$

Definition 1.1.
$A \subset \mathbf{F}_q[x]$ is said to be an asymptotic basis of order 2 if all polynomials of sufficiently high degree lie in $A + A = 2A$.

Definition 1.2.
For a given sequence $A \subset \mathbf{F}_q[x]$ the sequence B is said to be "complementary" to A if the sequence $A + B$ contains all polynomials of sufficiently high degree.

The subject of this paper is to translate two principal results of a chapter of the book of H. Halbertstam and K. F. Roth to the case of a polynomialring over a finite field.

Discussion and introduction of the first result.
The following question is a direct translation to the polynomialring $\mathbf{F}_q[x]$ of the same question raised by S. Sidon (see [1]) concerning the existence and nature of certain integer sequences A whose representation functions $r_n(A)$ are bounded or in some sense exceptionally small.

Does there exist an asymptotic basis $A \subset \mathbf{F}_q[x]$ of order 2 which is economical in the sense that, for every $\varepsilon > 0$

$$\lim_{\partial f \to \infty} \frac{r_f(A)}{|f|^\varepsilon} = 0$$

By elementary methods we have proved the existence of a subset A of $\mathbf{F}_q[x]$ which is a basis of order two and have zero-density (see [2]).

By probability methods we shall obtain theorem 1.1 below which is mush sharper than is required for an answer to the question above.

Theorem 1.1.
There exists an asymptotic basis of order 2 such that

$$\partial f \ll r_f(A) \ll \partial f \text{ for large } \partial f. \tag{1.3}$$

It should be remarked that the proof of theorem 1.1 is based on Bernstein's improvement of Chebychev's inequality (see the book of A. Renyi: Probability theory [3]).

Discussion and introduction of the second result.

By elementary methods we have proved the existence of a complementary sequence B to P such that

$$B(n) \ll n^3 \qquad \text{(see [2])} \tag{1.4}$$

By probability methods we shall prove that we can reduce the factor n^3 of the right hand side of (1.4) to n^2.

The proof of this result is rather complicated and requires beside the probabilistic machinery also some deep results concerning the distribution of irreducibles in the ring over a finite field. (See the paper of D.R. Hayes and the work of Georges Rhin [4], [5]).

Further is should be remarked that the definition of $R_f(A)$ is essential and will affect the result. If for instance we let $R_f(A)$ be the number of representations of f in the form $f = p + f'$, $p \in P$, $f' \in A$, $\partial p < \partial f$ we would not by this method obtain the estimate n^2 but only n^3 in (1.4). We state the theorem as follows.

Theorem 1.2.
Let P denote the sequence of irreducible polynomials in $\mathbf{F}_q[x]$. There exists a "complementary" sequence such that the counting number

$$B(n) \ll n^2. \tag{1.5}$$

Finally we remark that these theorems correspond to results obtained by Erdös-Renyi for integer sequences (see [1]) and can be considered as their directly translations to the polynomialring $\mathbf{F}_q[x]$.

I am very grateful to professor Georges Rhin (Metz, France) to have communicated his work
"Repartition modulo 1 dans un corps de series formelles sur un corps fini".

Also I would like to thank professor Asmus L. Schmidt, Copenhagen for his comments and very helpful instruction.

§2. Probability methods on the space of sequences of polynomials in $\mathbf{F}_q[x]$

We shal use an idea of Erdös to impose a probability measure on the space of polynomial sequences such that (in the resulting probability space) almost all polynomial sequences have some prescribed rate of growth.

From now on we use w to denote an (infinite) subsequence of $\mathbf{F}_q[x]$. Let Ω denote the space of all such sequences w. We shall need the following variant of a theorem from Halberstam and Roth's book [1] chapter III.

Theorem 2.1.
Let

$$\{p_g | g \in \mathbf{F}_q[x]\} \tag{2.1}$$

be real numbers satisfying

$$0 \leqq p_g \leqq 1 \quad (g \in \mathbf{F}_q[x]) \tag{2.2}$$

Then there exists a probability space (Ω, S, P) with the following two properties:

For every polynomial $g \in \mathbf{F}_q[x]$ the event
$B^{(g)} = \{w : g \in w\}$ is measureable and $P(B^{(g)}) = p_g$. (2.3)

The events $B^{(g)}$, $g \in \mathbf{F}_q[x]$ are independent. (2.4)

Further we assume that the sequence $\{p_g\}$ of probabilities (introduced in theorem 2.1) satisfies the following conditions:

$$0 < p_g < 1, \ \ g \in \mathbf{F}_q[x] . \tag{2.5}$$

$$\text{If } \partial g = \partial f \ \text{ then } \ p_g = p_f . \tag{2.6}$$

$$p_g \downarrow 0 \ \text{ as } \ \partial g \to \infty . \tag{2.7}$$

We denote $\chi_g(w)$ the characteristic function of the event $B^{(g)}$. Then (2.4) is equivalent to saying that χ_g, $g \in \mathbf{F}_q[x]$ are independent (simple) random variables. Further we shall need the following definitions.

Definition 2.1.
Let w be a constituent sequence of the space Ω, and let f be a polynomial. We denote by $w(f)$ the counting number of the sequence w, so that $w(f)$ is the number of polynomials of w which do not exceed f. We denote by $w(n)$ the number of polynomials of w which degree do not exceed n. Furthermore let $r_f(w)$ and $R_f(w)$ be as in the introduction.

Definition 2.2.
Let $x : \Omega \to R$ denote a random variable. We denote by $E(x(w))$ the mean of $x(w)$ and by $V(x(w))$ the variance of $x(w)$.

Definition 2.3.

$$\sum_{\partial\varphi < \partial f} p_\varphi^i p_{f-\varphi}^i = \lambda_f^{(i)}, \ i = 1,2,3,4, \ \lambda_f^{(1)} = \lambda_f \tag{2.8}$$

Obviously we have:

$$w(f) = \text{Card}\{g \in w \,|\, g = < f\} = \sum_{g=<f} \chi_g(w) \tag{2.9}$$

$$w(n) = \text{Card}\{g \in w \,|\, \partial g \leq n\} = \sum_{\partial g \leq n} \chi_g(w) \tag{2.10}$$

$$r_f(w) = \sum_{\partial\varphi < \partial f} \chi_\varphi \chi_{f-\varphi}(w) \tag{2.11}$$

$$R_f(w) = \sum_{\substack{p \in P \\ \partial p = \partial f \\ \text{sign } p = \text{sign } f}} \chi_{f-p}(w) \tag{2.12}$$

§3. A limit distribution for $r_f(w)$

Theorem 3.1.

Let us choose a sequence $\{p_f\}$ of probabilities such that

$$V(r_f) \to \infty \quad \text{as} \quad \partial f \to \infty \tag{3.1}$$

Then we have for $-\infty < x < \infty$:

$$\lim_{\partial f \to \infty} P\left(\frac{r_f - \lambda_f}{\sqrt{V(r_f)}} < x\right) = \Phi(x) \tag{3.2}$$

where $\Phi(x)$ denote the standard form of the normal distribution function.

Proof.

By the central limit theorem (see [3]) we need only to prove that the Lyapunov condition is satisfied.

That is:

$$\forall \varepsilon > 0: \frac{1}{\varepsilon} \sum_{\partial g < \partial f} E \left| \frac{\chi_g \chi_{f-g} - p_g p_{f-g}}{\sqrt{\lambda_f - \lambda_f^{(2)}}} \right|^3 \to 0 \tag{3.3}$$

$$\text{as } \partial f \to \infty$$

We obtain:

$$E \left| \frac{\chi_g \chi_{f-g} - p_g p_{f-g}}{\sqrt{\lambda_f - \lambda_f^{(2)}}} \right|^3$$

$$= \frac{1}{(\lambda_f - \lambda_f^{(2)})^{\frac{3}{2}}} ((1 - p_g p_{f-g})^3 P(B^{(g)} \cap B^{(f-g)}) + p_g^3 p_{f-g}^3 P(C(B^{(g)} \cap B^{(f-g)})))$$

$$= \frac{1}{(\lambda_f - \lambda_f^{(2)})^{\frac{3}{2}}} (p_g p_{f-g} - 3p_g^2 p_{f-g}^2 + 4p_g^3 p_{f-g}^3 - 2p_g^4 p_{f-g}^4)$$

Hence we have:

$$\sum_{\partial g < \partial f} E \left| \frac{\chi_g \chi_{f-g} - p_g p_{f-g}}{\sqrt{\lambda_f - \lambda_f^{(2)}}} \right|^3 = \frac{\lambda_f - 3\lambda_f^{(2)} + 4\lambda_f^{(3)} - 2\lambda_f^{(4)}}{(\lambda_f - \lambda_f^{(2)})^{\frac{3}{2}}} \tag{3.4}$$

By (3.1) and (3.4) we have (3.3) and this proves the theorem.

Application of theorem 3.1.
We will prove that $V(r_f) \to \infty$ as $\partial f \to \infty$ in the case:

$$p_g = \begin{cases} \frac{1}{2} & \partial g < 11 \\ k_1 \sqrt{\frac{\partial g}{|g|}} & \partial g \geqq 11,\ k_1^2 = \frac{65}{4} \frac{\log q}{\sqrt{q}} \end{cases} \tag{3.5}$$

Let Y denote a random variable such that

$$P(Y = k) = \frac{\sqrt{q} - 1}{(\sqrt{q})^k} \text{ for } k = 1, 2, \ldots$$

We need the following lemmas:

Lemma 3.1.

$$\lim_{n \to \infty} \frac{1}{\sqrt{n}\sqrt{q^n}} \sum_{k=1}^{n-1} \sqrt{k}\sqrt{q^k} = \frac{1}{\sqrt{q} - 1}$$

Proof.
First we note $\sum_{k=1}^{n-1} \sqrt{k}\ \sqrt{q^k} = \sum_{k=1}^{n-1} \sqrt{n-k}\sqrt{q^{n-k}}$

Then we have:

$$\frac{1}{\sqrt{n}\sqrt{q^n}} \sum_{k=1}^{n-1} \sqrt{k}\sqrt{q^k} = \sum_{k=1}^{n-1} \frac{1}{\sqrt{q} - 1} \frac{\sqrt{n-k}}{\sqrt{n}} P(Y = k) =$$

$$\frac{1}{\sqrt{q}-1} \quad E\left(\frac{\sqrt{\max(0, n-Y)}}{\sqrt{n}}\right) \rightarrow \frac{1}{\sqrt{q}-1} \cdot E(1) = \frac{1}{\sqrt{q}-1}$$

since $\dfrac{\sqrt{\max(0, n-Y)}}{\sqrt{n}} \rightarrow 1$ and

$$\forall n: \frac{\sqrt{\max(0, n-Y)}}{\sqrt{n}} \leq 1 .$$

Lemma 3.2.

$$\lambda_f \sim k_1^2(\sqrt{q}+1)\partial f \text{ as } \partial f \rightarrow \infty . \tag{3.6}$$

Proof.
We put $\partial f = n$
Hence we obtain:

$$\frac{\lambda_f}{n} = k_1^2(q-1) \quad \frac{1}{\sqrt{n}\sqrt{q^n}} \left(\sum_{k=1}^{n-1} \sqrt{k}\sqrt{q^k} + 0(1) \right)$$

Then by lemma 3.1:

$$\frac{\lambda_f}{n} \rightarrow k_1^2(q-1) \cdot \frac{1}{\sqrt{q}-1} \text{ as } n \rightarrow \infty$$

and the lemma is proved.

Lemma 3.3.

$$\lambda_f^{(2)} \rightarrow 0 \text{ as } \partial f \rightarrow \infty \tag{3.7}$$

Proof.
Obvious.
Then by lemma 3.2 and lemma 3.3

$$V(r_f) = \lambda_f - \lambda_f^{(2)} \rightarrow \infty \text{ as } \partial f \rightarrow \infty$$

§4. The law of large numbers for w(f)

By a variant of the strong law of large numbers (see [1]) we obtain the following theorem.

Theorem 4.1.
If

$$\sum_{g \in \mathbf{F}_q[x]} E(\chi_g) = \sum_{g \in \mathbf{F}_q[x]} p_g = +\infty \tag{4.1}$$

and

$$\sum_{f \in \mathbf{F}_q[x]} \frac{V(\chi_f)}{E^2(w(f))} < +\infty \tag{4.2}$$

Then with probability 1

$$\lim_{\partial f \to \infty} \frac{w(f)}{E(w(f))} = 1 \tag{4.3}$$

Applications of theorem 4.1.
We define:

$$p_g = \begin{cases} \frac{1}{2} & \partial g \leq 4 \\ k_2 \frac{\partial g}{|g|} & \partial g \geq 5,\ k_2 = \frac{20}{3} \frac{\log q}{q-1} \end{cases} \tag{4.4}$$

From this definition follows

Lemma 4.1.

$$E(w(n)) = \sum_{\partial g \leq n} p_g \sim \frac{10}{3} (\log q)\, n^2 \text{ as } n \to \infty$$

Lemma 4.2.
We have with probability 1

$$w(n) \sim \frac{10}{3} \log q \, n^2 \text{ as } n \to \infty \tag{4.5}$$

where $\{p_g\}$ is defined by (4.4).

Proof.
By lemma 4.1 the conditions (4.1), (4.2) are satisfied since

$$\sum_f \frac{V(\chi_f)}{E^2(w(f))} \ll \sum_{k=1}^{\infty} \frac{\frac{k}{q^k}}{k^4} q^k = \sum_{k=1}^{\infty} k^{-3} < \infty$$

Then by (4.3) we have (4.5).

§5. Some results concerning the distribution of irreducibles in the ring over a finite field

Let M denote the multiplicative semigroup consisting of the polynomials f with sign $f = 1$ in the ring $\mathbf{F}_q[x]$.

Let $B = x^n + b_{n-1}x^{n-1} + \ldots + b_{n-k}x^{n-k} + \ldots + b_0$ be a polynomial in M. The field elements $b_{n-1}, b_{n-2}, \ldots, b_{n-k}$ are called the first k coefficients of B, it being understood that $b_i = 0$ if $i < 0$.

Let k be a non-negative integer, and let a sequence of k field elements be given. Let H be a polynomial in $\mathbf{F}_q[x]$ and let K be a polynomial prime to H. We denote by h the degree of H, and $\Phi(H)$ denotes the number of polynomials in M of degree h and prime to H.

Let $\pi(n,H,k,K)$ denote the number of irreducibles in M of degree n which (1) are congruent to K modulo H and (2) have as first k coefficients the given field elements, then by comparing results in [4] and [5] we obtain the following explicit estimate.

$$\left| \pi(n,H,k,K) - \frac{q^n}{nq^k\Phi(H)} \right| \leqq (k+h+1)q^{\frac{n}{2}} \tag{5.1}$$

In the estimate (5.1) we put

$$H = x,\ K = \beta_0 \neq 0\ (\in \mathbf{F}_q),\ \text{then } \partial H = 1,\ (x,\beta_0) = 1 \text{ and } \Phi(x) = q-1.$$

Then we have the following estimate

$$\left| \pi(n,x,k,\beta_0) - \frac{q^n}{nq^k(q-1)} \right| \leqq (k+1+1)q^{\frac{n}{2}} \tag{5.2}$$

(5.2) implies the following lower bound estimate

$$\pi(n,x,k,\beta_0) \geq \frac{q^n}{n} \frac{1}{q^k(q-1)} - (k+2)q^{\frac{n}{2}} \tag{5.3}$$

We denote by $\pi(n,k)$ the number of irreducibles in M of degree n and with the k first coefficients being fixed. Then by (5.3) we obtain the lower bound estimate we need for the proof of theorem 1.2.

$$\pi(n,k) = \sum_{\beta_0 \in \mathbf{F}_q^*} \pi(n,x,k,\beta_0) \geq \frac{q^{n-k}}{n} - (q-1)(k+2)q^{\frac{n}{2}} \tag{5.4}$$

§6. Proof of theorem 1.1 §1

We prove theorem 1.1 by establishing theorem 6.1 below.

Theorem 6.1.
Suppose that Ω is the probability space generated in accordance with theorem 2.1 §2 by the choice (3.5) of the probabilities p_g. Then with probability 1:

$$\partial f \ll r_f(w) \ll \partial f \text{ for large } \partial f. \tag{6.1}$$

Proof.
We have $\{\chi_\varphi \chi_{f-\varphi} | \partial\varphi < \partial f\}$ are independent random variables such that:

$$E\left(\sum_{\partial\varphi < \partial f} \chi_\varphi \chi_{f-\varphi}\right) = E(r_f) = \lambda_f$$

$$V(r_f) = \lambda_f - \lambda_f^{(2)}$$

$$\forall \varphi : \partial\varphi < \partial f \quad |\chi_\varphi \chi_{f-\varphi} - E(\chi_\varphi \chi_{f-\varphi})| \leqq 1$$

We put $\mu = \dfrac{\frac{1}{2}\lambda_f}{\sqrt{\lambda_f - \lambda_f^{(2)}}}$. Then by lemma 3.2 and lemma 3.3 §3: $\mu \leqq \sqrt{V(r_f)}$ for large ∂f. Hence by Bernstein's improvement of Chebychev's inequality (see [3] p. 387) we obtain the following result:

$$P\left(|r_f-\lambda_f|\geq\frac{1}{2}\lambda_f\right)\leqq 2\exp\left\{-\frac{\mu^2}{2\left(1+\frac{\mu}{2\sqrt{V(r_f)}}\right)^2}\right\} \tag{6.2}$$

for large ∂f.

By (3.6) and (3.7) we have for large ∂f:

$$\frac{\mu^2}{2\left(1+\frac{\mu}{2\sqrt{V(r_f)}}\right)^2}=\frac{\frac{1}{4}\lambda_f^2}{2\left(1+\frac{\frac{1}{2}\lambda_f}{2(\lambda_f-\lambda_f^{(2)})}\right)^2\left(\lambda_f-\lambda_f^{(2)}\right)}\geq\frac{\lambda_f^2}{8\left(\lambda_f+\frac{\lambda_f}{8}+\frac{\lambda_f}{2}\right)}=\frac{\lambda_f}{13} \tag{6.3}$$

Hence by (6.2), (6.3) and (3.6) we have for large ∂f:

$$P\left(|r_f-\lambda_f|\geq\frac{1}{2}\lambda_f\right)\leqq 2e^{-\frac{\lambda_f}{13}}\leqq 2q^{-\left\{\frac{1}{\log q}\cdot\frac{k_1^2\sqrt{q}\,\partial f}{13}\right\}}=2q^{-\frac{5}{4}\cdot\partial f}=2|f|^{-1-\frac{1}{4}} \tag{6.4}$$

We put $E_f=\{w:|r_f-\lambda_f|\geq\frac{1}{2}\lambda_f\}$

Then by (6.4):

$$\sum_{f\in\mathbf{F}_q[x]} P(E_f)<\infty \tag{6.5}$$

Hence by the Borel-Cantelli lemma, with probability 1, at most a finite number of the events E_f can occur or equivalently:

$$P(\{w:|r_f-\lambda_f|<\frac{1}{2}\lambda_f \text{ for } \partial f>n_0(w)\})=1 \tag{6.6}$$

(6.6) implies since $\lambda_f\sim k_1^2(\sqrt{q}+1)\,\partial f$ that:

$$P(\{w:\partial f\ll r_f(w)\ll\partial f \text{ for large } \partial f\})=1 \tag{6.7}$$

This completes the proof of theorem 6.1.

§7. Proof of theorem 1.2 §1

We prove theorem 1.2 by establishing theorem 7.1 below.

Theorem 7.1.
Suppose that Ω is the probability space generated, in accordance with theorem 2.1 §2 by the choice (4.4) §4 of the probabilities p_g. Then with probability 1:

$$w(n) \ll n^2 \tag{7.1}$$

$$R_f(w) > 0 \text{ for } \partial f > n_0(w) \tag{7.2}$$

Proof.

By lemma 4.2 §4 we obtain (7.1). To establish the theorem, we must prove that, with probability $1, R_f(w) > 0$ for large ∂f. By the Borel-Cantelli lemma we need only show that

$$\sum_{f \in \mathbf{F}_q[x]} P(\{w : R_f = 0\}) < \infty\,, \tag{7.3}$$

and in view of (7.3) it suffices to establish the existence of a number $\delta > 0$ such that

$$P(\{w : R_f = 0\}) \ll q^{-\partial f(1+\delta)}\,. \tag{7.4}$$

Let f be a fixed polynomial of degree n and sign $f = a\,(\neq 0)$. We have the following estimate

$$P(\{w : R_f(w) = 0\}) = \prod_{\substack{p \in P \\ \partial p = \partial f \\ \text{sign } p = \text{sign } f}} P(\{w : \chi_{f-p} = 0\}) \tag{7.5}$$

$$= \prod_{\substack{p \in P \\ \partial p = \partial f \\ \text{sign } p = \text{sign } f}} P(CB^{(f-p)}) = \prod_{\substack{p \in P \\ \partial p = \partial f \\ \text{sign } p = \text{sign } f}} (1 - p_{f-p})$$

$$\leq \prod_{k=1}^{[\frac{n}{2}(1-\varepsilon)]} \Bigg(\prod_{\substack{p \in P \\ \partial(f-p) = n-k}} (1 - p_{f-p}) \Bigg)$$

$$\leq \prod_{k=1}^{[\frac{n}{2}(1-\varepsilon)]} e^{-P_{f-p} \sum_{\partial(f-p)=n-k} 1}\,, \quad 0 < \varepsilon < 1$$

To obtain the estimate (7.4) we need first to establish a lower bound estimate for $\sum_{\partial(f-p)=n-k} 1$ and secondly an upper bound estimate for

$$e^{-P_{f-p} \sum_{\partial(f-p)=n-k} 1}\,.$$

Let

$$f = ax^n + a_{n-1}x^{n-1} + \ldots + a_{n-k}x^{n-k} + \ldots + a_0$$

$$p = ax^n + \beta_{n-1}x^{n-1} + \ldots + \beta_{n-k}x^{n-k} + \ldots + \beta_0$$

$$\partial(f-p) = n-k \Rightarrow$$

$$\beta_{n-1} = a_{n-1}$$
$$\vdots$$
$$\beta_{n-k+1} = a_{n-k+1}$$

$$\beta_{n-k} \neq a_{n-k}$$

By (5.4) we obtain

$$\sum_{\partial(f-p)=n-k} 1 \tag{7.6}$$

$$= \operatorname{Card}\{p \in P \,|\, \partial p = n;\ \operatorname{sign} p = a;\ \beta_{n-i} = a_{n-i},\ i = 1,2,\ldots k-1;\ \beta_{n-k} \neq a_{n-k}\}$$

$$= \operatorname{Card}\{p \in P \,|\, \partial p = n;\ \operatorname{sign} p = 1;\ \gamma_{n-i} = \frac{a_{n-i}}{a},\ i = 1,2,\ldots k-1;\ \gamma_{n-k} \neq \frac{a_{n-k}}{a}\}$$

$$\geq (q-1)\left(\frac{q^{n-k}}{n} - (q-1)(k+2)q^{\frac{n}{2}}\right)$$

(7.6) implies

$$e^{-P_{f-p}} \sum_{\partial(f-p)=n-k} 1 \leqq e^{-k_2(q-1)\frac{n-k}{n}\left[1-n(q-1)(k+2)q^{k-\frac{n}{2}}\right]}. \tag{7.7}$$

Now take any $\varepsilon_1 : 0 < \varepsilon_1 < 1$. Then for every $k : k = 1,2,\ldots \left[\frac{n}{2}(1-\varepsilon)\right]$ we have

$$n(q-1)(k+2)q^{k-\frac{n}{2}} \leqq \varepsilon_1 \text{ if } n > N_0(\varepsilon, \varepsilon_1, q). \tag{7.8}$$

Then by (7.7) and (7.8)

$$e^{-P_{f-p}} \sum_{\partial(f-p)=n-k} 1 \leqq e^{-k_2(q-1)(1-\frac{k}{n})(1-\varepsilon_1)} \quad \text{if } n > N_0(\varepsilon, \varepsilon_1, q). \tag{7.9}$$

By (7.5) and (7.9)

$$P(\{w : R_f = 0\}) \leqq e^{-k_2(q-1)(1-\varepsilon_1)} \sum_{k=1}^{[\frac{n}{2}(1-\varepsilon)]} {}^{(1-\frac{k}{n})} \tag{7.10}$$

Take $\varepsilon = \sqrt{2}-1\,(<1)$, then we obtain

$$\sum_{k=1}^{[\frac{n}{2}(1-\varepsilon)]} \left(1-\frac{k}{n}\right) \geq \frac{n}{4}-\frac{5}{4}. \tag{7.11}$$

(7.10) and (7.11) implies

$$P(\{w : R_f = 0\}) \ll q^{-n\left(\frac{k_2(q-1)(1-\varepsilon_1)}{4\log q}\right)} \tag{7.12}$$

To obtain (7.4) with $\delta = \frac{1}{4}$ we need only choose in (7.12)

$$\varepsilon_1 = \frac{1}{4}, \quad {}_2 = \frac{(1+\delta)\,4\log q}{(q-1)(1-\varepsilon_1)} = \frac{20}{3}\,\frac{\log q}{q-1}$$

and this proves the theorem.

References

[1] H. HALBERSTAM and K. F. ROTH: "Sequences". Oxford University Press 1966.

[2] J. CHERLY: "On complementary sets of group elements". Archiv der matematik vol. 35, 1980 p. 313-318.

[3] A. RENYI: "Probability theory". North-Holland Publishing Company, Amsterdam-London, 1970.

[4] D. R. HAYES: "The distribution of irreducibles in GF[q,x]". Trans. Amer. Math. Soc 117 (1965), p. 101-127.

[5] GEORGES RHIN: "Repartition modulo 1 dans un corps de series formelles sur un corps fini". Dissertationes mathematicae XCV. Warszawa 1972.

Indleveret til Selskabet august 1982.
Færdig fra trykkeriet oktober 1983.