Atti Accademia Nazionale dei Lincei

Classe Scienze Fisiche Matematiche Naturali

Rendiconti

Calvin T. Long, William A. Webb

Normality in GFq,x

Atti della Accademia Nazionale dei Lincei. Classe di Scienze Fisiche, Matematiche e Naturali. Rendiconti, Serie 8, Vol. **54** (1973), n.6, p. 848–853.

Accademia Nazionale dei Lincei

<http://www.bdim.eu/item?id=RLINA_1973_8_54_6_848_0>

Algebra. — *Normality in* GF $\{q, x\}$. Nota di Calvin T. Long e William A. Webb, presentata (*) dal Socio B. Segre.

Riassunto. — Si mostra come diversi dei risultati classici relativi alla normalità dei numeri reali possano venire trasportati agli elementi (1.1) dell'anello GF $\{q, x\}$ delle serie di potenze formali a coefficienti in un campo di Galais.

1. Introduction

Let q be a power of a prime p, and let GF (q) and GF $[q, x]$ denote the finite field with q elements and the ring of polynomials with coefficients in GF (q) respectively. Let ν denote the degree valuation on the quotient field of GF $[q, x]$, that is, $\nu(A/B) = \deg B - \deg A$; and let GF $\{q, x\}$ denote the completion of this quotient field with respect to ν. The elements of GF $\{q, x\}$ may be written in the form:

$$\alpha = \sum_{i=-\infty}^{n} a_i x^i, \qquad a_i \in \mathrm{GF}(q) \tag{1.1}$$

where n is any integer. For such an α, $\nu(\alpha) = -n$, and $|\alpha| = q^{-\nu(\alpha)}$.

It is known that GF $\{q, x\}$ has many number theoretic properties which are similar to the real numbers. In particular it has been shown by Carlitz [1], Dijksma [2], [3], Hodges [5], [6], [7] and Webb [9] that most of the known results concerning uniform distribution of real numbers also hold for GF $\{q, x\}$. In this paper we consider the closely related area of normal numbers, and prove that many of the well known results about normality of real numbers also hold for GF $\{q, x\}$.

We will use the following notation throughout the paper. Let A, B, C, ... denote elements of GF $[q, x]$, let α and β denote elements of GF $\{q, x\}$, and let $a, b, c, \cdots$ denote rational integers unless otherwise specified. Let (α) denote the fractional part of α, so that, if α is given by (1.1),

$$(\alpha) = \sum_{i=-\infty}^{-1} a_i x^i, \qquad a_i \in \mathrm{GF}(q).$$

As usual, $[\alpha] = \alpha - (\alpha)$ denotes the integral part of α.

Finally, let

$$\begin{aligned} \mathcal{S} &= \{\alpha : \alpha \in \mathrm{GF}\{q, x\}, \nu(\alpha) > 0\} \\ \mathfrak{A}_n(\beta) &= \{\alpha : \alpha \in \mathrm{GF}\{q, x\} \text{ and } \nu(\beta - \alpha) > n\}. \end{aligned} \tag{1.2}$$

(*) Nella seduta del 19 giugno 1973.

II. DEFINITIONS AND PRELIMINARY RESULTS.

Let B be a polynomial in GF $[q, x]$ of degree $b > 0$. It is then possible to write any element $\alpha \in \mathrm{GF}\{q, x\}$ in the form

$$\alpha = \sum_{i=-\infty}^{n} A_{-i} B^{i} \tag{2.1}$$

where $A_i \in \mathrm{GF}[q, x]$ and $\deg A_i < b$. We say that α is written in the base B. The set of polynomials A_i of degree $< b$ can be considered as the digits in the base B. The base B is considered fixed.

If

$$(\alpha) = \sum_{i=-\infty}^{-1} A_{-i} B^{i},$$

we will frequently write (α) in « decimal form » as

$$(\alpha) = \cdot A_1 A_2 A_3 \cdots . \tag{2.2}$$

Y_n will denote the block of the first n digits of (α) in the base B. $\mathfrak{B}_k$ will denote arbitrary, but fixed, block of k digits in the base B.

Now if Z is any block of digits in the base B, let $N(\mathfrak{B}_k, Z)$ denote the number of occurrences of $\mathfrak{B}_k$ in Z, and let $N_s(\mathfrak{B}_k, Z)$ denote the number of occurrences of $\mathfrak{B}_k$ in Z starting in a position which is $\equiv s \pmod{k}$.

DEFINITION 2.1. The element α is *simply normal* to base B if

$$\lim_{n \to \infty} \frac{N(C, Y_n)}{n} = \frac{1}{q^b} \tag{2.3}$$

for every digit C in base B. α is *normal* to base B if each of the numbers α, $B\alpha$, $B^2\alpha, \cdots$ is simply normal to each of the bases $B, B^2, B^3, \cdots$. α is *absolutely normal*, if α is normal in every base B.

These definitions parallel Borel's original definition of normality. Note that, since the normality of α depends only on (α), and $\alpha - (\alpha)$ has a finite number of digits, we may assume $\alpha = (\alpha)$.

DEFINITION 2.2. For any real number $\varepsilon > 0$, the block $\mathfrak{B}_k$ is ε*–irregular with respect to the digit* C if

$$\left| N(C, \mathfrak{B}_k) - \left[\frac{k}{q^b}\right] \right| > \varepsilon k. \tag{2.4}$$

If (2.4) does not hold, $\mathfrak{B}_k$ is said to be ε–regular.

By some purely combinatorial results which are the same for ε–irregular real numbers and can be found in [8, p. 101], the following lemma may be obtained.

LEMMA 2.1. *If k is sufficiently large, the number of blocks $\mathfrak{B}_k$ which are ε–irregular with respect to a fixed digit* C *in base* B *is at most $c_1 q^{kb} e^{-c_2 k}$ where c_1 and c_2 are positive constants independent of k.*

THEOREM 2.2. *Almost all elements of* GF$\{q , x\}$ *are simply normal to a given base* B.

Proof. It clearly suffices to consider $\mathfrak{F}$ instead of GF$\{q , x\}$. Let $\mathfrak{S}$ be the set of elements of $\mathfrak{F}$ not simply normal to base B and let Y_n be as above. If Y_n is ε–regular for every fixed $\varepsilon > 0$, all n sufficiently large (depending on ε), and all digits C to base B, then

$$\lim_{n\to\infty} \frac{N(C , Y_n)}{n} = q^{-b}$$

and α is simply normal to base B. Hence, if $\alpha \in \mathfrak{S}$ there exists at least one digit C for any $\varepsilon > 0$ such that Y_n is ε–irregular with respect to C for infinitely many values of n. Choose k such that $2^{-k} < \varepsilon$, then Y_n is 2^{-k}–irregular with respect to C for infinitely many n. Let $\mathfrak{S}_{C,k}$ denote the set of all such α, and let μ denote the Haar measure on GF$\{q , x\}$. It suffices to show that $\mu(\mathfrak{S}_{C,k}) = 0$ since each α which is not simply normal to base B is an element of some $\mathfrak{S}_{C,k}$ and there are only countably many pairs C and k.

Given any n_0, for every $\alpha \in \mathfrak{S}_{C,k}$ there is an $n > n_0$ such that Y_n is ε–irregular ($\varepsilon = 2^{-k}$) with respect to C in base B. Since $\nu(\alpha - Y_n) > nb$, $\alpha \in \mathfrak{A}_{nb}(Y_n)$, an open ball with volume q^{-nb}. Hence, by Lemma 2.1, we can cover all $a \in \mathfrak{S}_{C,k}$ with an open ball having volume at most

$$\sum_{n=n_0+1}^{\infty} c_1 q^{nb} e^{-c_2 n} q^{-nb} = c_1 \sum_{n=n_0+1}^{\infty} e^{-c_2 n} = c_3 e^{-c_2 n_0}.$$

Since $\mu(\mathfrak{S}_{C,k}) < c_3 e^{-c_2 n_0}$ for any n_0, we must have $\mu(\mathfrak{S}_{C,k}) = 0$ and the proof is complete.

THEOREM 2.3. *Almost all elements of* GF$\{q , x\}$ *are absolutely normal. Hence, a f o r t i o r i , almost all elements of* GF$\{g , x\}$ *are normal to any given base.*

Proof. The proof merely involves taking countable unions of sets of measure zero.

The following theorem gives a useful characterization for normality. The proof involves several counting arguments similar to those used in the proof of the analogous result for real numbers.

THEOREM 2.4. *The element α is normal to base* B *if and only if*

$$\lim_{n\to\infty} \frac{N(\mathfrak{B}_k , Y_n)}{n} = q^{-bk}$$

or all $k \geq 1$ and all blocks $\mathfrak{B}_k$.

Another theorem which we will need later is the following:

THEOREM 2.5. *The element* α *is normal to base* B *if and only if* α *is normal to base* B^k *for some integer* $k \geq 1$.

The proof of this theorem again involves some fairly straight forward counting arguments.

III. FURTHER CONDITIONS FOR NORMALITY

The following theorem relates the concept of normality to that of uniform distribution modulo 1.

THEOREM 3.1. *The element* $\alpha \in GF\{q, x\}$ *is normal to base* B *if and only if the sequence* $\{\alpha B^n\}$ *is uniformly distributed modulo 1.*

Proof. Let $N_h(n, \lambda)$ denote the number of terms among $\alpha B, \alpha B^2, \cdots, \alpha B^n$ such that, $\nu((\alpha B^i - \lambda)) > h$. By definition, see [1], αB^i is uniformly distributed modulo 1 if and only if

$$\lim_{n \to \infty} \frac{N_h(n, \lambda)}{n} = q^{-h} \qquad \text{for all } \lambda \text{ and } h. \tag{3.1}$$

This clearly implies that

$$\lim_{n \to \infty} \frac{N_{bk}(n, \lambda)}{n} = q^{-bk} \qquad \text{for all } \lambda \text{ and } k. \tag{3.2}$$

However, (3.2) implies (3.1) since

$$\mathfrak{A}_h(\lambda) = \{\beta : \nu(\beta - \lambda) > h\}$$

can be written as a disjoint union of $\mathfrak{A}_{bk}(\lambda_i)$ for a suitable k and suitable λ_i.

Now, for an arbitrary but fixed λ, let $\mathfrak{B}_k$ denote the block of the first k digits of (λ) in base B. Also, let $A_0, A_1, \cdots$ denote the digits of (α) to base B. Then $N_{bk}(n, \lambda)$ is the number of terms among $\alpha B, \cdots, \alpha B^n$ such that $(\alpha B^i) \in \mathfrak{A}_{bk}((\lambda))$ and the digits of (αB^i) are just $A_i, A_{i+1}, \cdots$ in base B. Hence, $(\alpha B^i) \in \mathfrak{A}_{bk}((\lambda))$ if and only if the block $A_i A_{i+1} \cdots A_{i+k-1}$ is the block $\mathfrak{B}_k$. Letting Y_m denote the block of the first m digits of (α) to base B, we have

$$N_{bk}(n, \lambda) = N(\mathfrak{B}_k, Y_{n+k-1}) + O(1) = N(\mathfrak{B}_k, Y_n) + O(1). \tag{3.3}$$

($N_{bk}(n, \lambda)$ does not count $\mathfrak{B}_k$ if it appears beginning with A_0, but $N(\mathfrak{B}_k, Y_{n+k-1})$ does).

Therefore, α is uniformly distributed modulo 1 if and only if (3.2) holds, if and only if

$$\lim_{n \to \infty} \frac{N(\mathfrak{B}_k, Y_n)}{n} = q^{-bk} \qquad \text{for all } \lambda \text{ and } k. \tag{3.4}$$

And (3.4) holds if and only if α is normal to base B by Theorem 2.4.

The following theorem is closely related.

THEOREM 3.2. *The element* α *is normal to base* B *if and only if* $[\alpha B^n]$ *is uniformly distributed.*

Proof. If α is normal, αB^n is uniformly distributed modulo 1, which by Theorem 2.1 of [7] implies that $[M\alpha B^n]$ is uniformly distributed for all primary $M \in GF[q, x]$. In particular, it holds for $M = 1$.

Let $\theta(n, C, M)$ denote the number of elements among $[\alpha B], [\alpha B^2], \cdots [\alpha B^n]$ which are $\equiv C \pmod{M}$. By definition, see [5], $[\alpha B^i]$ is uniformly distributed if and only if

$$\lim_{n \to \infty} \frac{\theta(n, C, M)}{n} = q^{-m} \tag{3.5}$$

for all $C \in GF[q, x]$ and all primary M where m denotes the degree of M. Writing everything in base B, let $A_0 A_1 A_2 \cdots$ denote the digits of α, and if $\mathfrak{B}_k = C_1 C_2 \cdots C_k$ is any block of k digits, let $C = C(\mathfrak{B}_k)$ denote the polynomial $C_k + C_{k-1} B + \cdots + C_1 B^{k-1}$. The digits of $[\alpha B^i]$ are easily calculated, and we see that

$$[\alpha B^i] \equiv C \pmod{B^k}$$

if and only if

$$A_{i-1} + A_{i-2} B + \cdots + A_{i-k} B^{k-1} = C_k + C_{k-1} B + \cdots + C_1 B^{k-1}.$$

Hence, $\theta(n, C, B^k)$ is the number of times the block $\mathfrak{B}_k$ appears in $A_0 A_1 \cdots A_{n-1} = N(\mathfrak{B}_k, Y_n)$. Therefore, by (3.5) with $M = B^k$, and C as defined above

$$\lim_{n \to \infty} \frac{N(\mathfrak{B}_k, Y_n)}{n} = q^{-bk} \qquad \text{for all } k \geq 1 \text{ and all } \mathfrak{B}_k. \tag{3.6}$$

Hence, α is normal by Theorem 2.4.

The following theorem shows that addition and multiplication by a rational function does not affect the normality of an element of $GF\{q, x\}$. In general it is easy to construct examples to show that the normality of the sum of two elements does not depend on the normality of the summands.

THEOREM 3.3. *If* α *is normal to base* B *and if* C *and* D *are nonzero elements of* $GF[q, x]$ *then* $\alpha + C/D$ *and* $\alpha \cdot C/D$ *are normal to base B.*

Proof. It suffices to show that, for any $A \neq 0$ in $GF[q, x]$, αA and α/A are normal. This clearly implies $\alpha \cdot C/D$ is normal. Also, $D\alpha$ is then normal so $D\alpha + C$ is clearly normal since $\nu(C) \leq 0$; which implies $(D\alpha + C)/D = \alpha + C/D$ is normal.

Since α is normal to base B, by Theorem 3.1, αB^n is uniformly distributed modulo 1. By applying Theorem 3 of [1] twice, we have that $\alpha A B^n$ is uniformly distributed modulo 1; which by Theorem 3.1 again implies that αA is normal.

To prove that α/A is normal, it clearly suffices to show that α/P is normal where P is irreducible.

If $P \mid B$ then $\alpha/P = (\alpha/B)\cdot(B/P)$ is normal since $B/P \in GF[q, x]$ and α/B is normal; the digits of α/B being the same as the digits of α shifted by one place.

If $P \nmid B$ then by a result completely analogous to Fermat's theorem

$$B^{|P|-1} \equiv 1 \pmod{P}$$

and this implies that

$$B^{(|P|-1)k} \equiv 1 \pmod{P} \qquad \text{for all } k \geq 0. \tag{3.7}$$

Now by Theorem 2.5 α is normal to base $B^{|P|-1}$ which by the first part of this theorem and equation (3.5) implies $\alpha\,(B^{(|P|-1)k} - 1)/P$ is normal to base $B^{|P|-1}$ for all $k \geq 0$. Hence by Theorem 3.1

$$\alpha \cdot \frac{(B^{(|P|-1)k} - 1)}{P} \cdot B^{(|P|-1)n}$$

is uniformly distributed modulo 1 for all $k \geq 0$. Letting $x_n = (\alpha/P)\cdot B^{(|P|-1)n}$ in Theorem 6 of [4] we have that $(\alpha/P)\, B^{(|P|-1)n}$ is uniformly distributed modulo 1. Finally, by Theorem 3.1, α/P is normal to base $B^{|P|-1}$ and by Theorem 2.5, α/P is normal to base B.

REFERENCES

[1] L. CARLITZ, *Diophantine approximation in fields of characteristic p*, « Trans. Amer. Math. Soc. », *72*, 187–208 (1952).

[2] A. DIJKSMA, *Uniform distribution of polynomials over* GF $\{q, x\}$ *in* GF $[q, x]$, I. « Nederl. Akad. Wet., Proc. », Ser. A, *72*, 376–383 (1969).

[3] A. DIJKSMA, *Uniform distribution of polynomials over* GF $\{q, x\}$ *in* GF $[q, x]$, II. « Nederl. Akad. Wet., Proc. », Ser. A, *73*, 187–195 (1970).

[4] E. HLAWKA, *Zur Formalen Theorie der Gleichverteclung in kompakten Gruppen*, « Rend. Circ. Mat. Palermo », Ser. II, *4*, 33–47 (1955).

[5] J. H. HODGES, *Uniform distribution in* GF $[q, x]$, « Acta Aritmetica », *12*, 55–75 (1966).

[6] J. H. HODGES, *Uniform distribution of polynomial-generated sequences in* GF $[q, x]$, « Annali di Mat. pura ed appl. », *81*, 135–142 (1969).

[7] J. H. HODGES, *On uniform distribution of sequences in* GF $\{q, x\}$ *and* GF $[q, x]$, « Annali di Mat. pura ed appl. », *85*, 287–294 (1970).

[8] I. NIVEN, *Irrational Numbers*, « Carus Monograph Number 11 », John Wiley and Sons, 1956.

[9] W. WEBB, *Uniformly distributed functions in* GF $[q, x]$ *and* GF $\{q, x\}$, « Annali di Mat. pura ed appl. », *95*, 285–291 (1973).