On uniform distribution of sequences in $GF\{q, x\}$ and $[GFq, x]$. (*)

by JOHN H. HODGES (U. S. A.) (**)

Summary. - *Analogs are proved for sequences in $\Phi = GF[q, x]$ and $\Phi' = GF\{q, x\}$ of results proved in 1962 by C. L. Vanden Eynden concerning uniform distribution of sequence of integers related to sequences of real numbers. The concept of uniform distribution (mod m), m an integer, in Vanden Eynden's work is sometimes replaced here by modified forms of uniform distribution (mod M) $M \in \Phi$.*

1. - Introduction and preliminaries.

Let $\Phi' = GF\{q, x\}$ denote the field of all formal expressions

$$(1.1) \qquad \alpha = \sum_{i=-\infty}^{m} c_i x^i \qquad (c_i \in GF(q)),$$

where x is an indeterminate and the coefficients c_i all belong to an arbitrary fixed finite field of $q = p^z$ elements. Let $\Phi = GF[q, x]$ denote the subring of Φ' consisting of all polynomials in x over $GF(q)$. Throughout this paper, lower case GREEK letters will denote elements of Φ' and italic capitals will denote elements of Φ, except as indicated.

If α has the representation (1.1) with $c_m \neq 0$, following CARLITZ [1; § 2] we define the *degree* of α by $\deg \alpha = m$, where m is an integer which may be positive, negative or zero. We also define $\deg 0 = -\infty$, where $-\infty < k$ for all integers k. The *integral part* and fractional part of α, denoted by $[\alpha]$ and $((\alpha))$ respectively, are defined by

$$(1.2) \qquad [\alpha] = \sum_{i=0}^{m} c_i x^i \quad \text{and} \quad ((\alpha)) = \alpha - [\alpha] = \sum_{i=-\infty}^{-1} c_i x^i,$$

so that $[\alpha] \in \Phi$ and $\deg((\alpha)) < 0$. We note that for any $\alpha, \beta \in \Phi'$, $[\alpha + \beta] = [\alpha] + [\beta]$ and $((\alpha + \beta)) = ((\alpha)) + ((\beta))$. The statement $\alpha \equiv \beta \pmod 1$ is defined to mean

(*) Supported by NSF Research Grant GP 6515.

(**) Entrata in Redazione il 13 giugno 1969.

that $\alpha = \beta + A$ where $A \in \Phi$, that is, A is a polynomial. Thus every $\alpha \in \Phi'$ is congruent (mod 1) to a unique β, namely $\beta = ((\alpha))$, such that $\deg \beta < 0$.

The following definitions are also due to CARLITZ [1; § 4]. Given an infinite sequence $\Gamma = \{\gamma_i\}$ in Φ', an arbitrary element β of Φ' and any positive integers n and k, let $N_k(n, \beta)$ be the number of γ_i with $1 \leqq i \leqq n$ such that

$$\deg((\gamma_i - \beta)) < -k. \tag{1.3}$$

Then the sequence Γ is said to be ***uniformly distributed*** (mod 1), abbreviated as u.d. (mod 1) in Φ' if and only if for all $k \geqq 1$ and all $\beta \in \Phi'$

$$\lim_{n\to\infty} N_k(n, \beta)/n = q^{-k}, \tag{1.4}$$

and is said to be ***semi-uniformly distributed*** (mod 1), abbreviated as s.u.d. (mod 1), in Φ' if and only if for all $k \geqq 1$ and all $\beta \in \Phi'$

$$\lim_{t\to\infty} N_k(q^t, \beta)/q^t = q^{-k}. \tag{1.5}$$

(We note CARLITZ used the phrase ***weakly uniformly distributed*** for the concept we have called here semi-uniformly distributed. Since a somewhat different concept of weakly uniformly distributed is to be defined below for sequences in Φ, it has seemed appropriate to rename the concept defined for Φ' by (1.5).)

Let M be any monic (leading coefficient equal to 1) element of Φ of degree $m > 0$. The case $M = 1$ would be trivial here and the terminology would conflict with that established above). Let $\theta = \{A_i\}$ be any infinite sequence of elements of Φ and for any $B \in \Phi$ and integer $n \geqq 1$, let $\theta(n, B, M)$ denote the number of terms among $A_1, \ldots, A_n$ such that $A_i \equiv B \pmod{M}$. Then as in [2] we say that the sequence θ is ***uniformly distributed modulo M***, abbreviated as u.d. (mod M), if and only if

$$\lim_{n\to\infty} \theta(n, B, M)/n = q^{-m}, \qquad (\text{all } B \in \Phi), \tag{1.6}$$

and is ***uniformly distributed***, abbreviated as u.d., if and only if it is u.d. (mod M) for every monic M of degree > 0 in Φ. By analogy with (1.5) we define θ to be ***semi-uniformly distributed modulo M***, abbreviated as s.u.d. (mod M) if and only if

$$\lim_{t\to\infty} \theta(q^t\ B, M)/q^t = q^{-m}, \qquad (\text{all } B \in \Phi), \tag{1.7}$$

and ***semi-uniformly distributed*** if and only if it s.u.d. (mod M) for all monic M of degree > 0 in Φ.

For certain questions of interest concerning sequences in Φ a somewhat different condition than (1.6) or (1.7) must be used. Let θ be an infinite sequence in Φ in which no element of Φ appears infinitely many times. For any $B \in \Phi$, any monic $M \in \Phi$ of degree $m > 0$, and any integer $n \geqq 1$, let

$$(1.8) \qquad \begin{cases} \theta(n) = \text{number of terms of } \theta \text{ such that } \deg A_i < n, \\ N(\theta, n, B, M) = \text{number of terms of } \theta \text{ such that } \deg A_i < n \\ \qquad\qquad \text{and } A_i \equiv B (\operatorname{mod} M). \end{cases}$$

Then as in [2] we say that θ is *weakly uniformly distributed* modulo M, abbreviated as w.u.d. (mod M), if and only if

$$(1.9) \qquad \lim_{n\to\infty} N(\theta, n, B, M)/\theta(n) = q^{-m}, \qquad (\text{all } B \in \Phi),$$

and that θ is *weakly uniformly distributed* if and only if it is w.u.d. (mod M) for all monic M of degree > 0 in Φ.

We note that in all of the above definitions there is no loss of generality in restricting M to be monic of degree $m > 0$ and only letting B run through the q^m elements of any complete residue system (mod M). Also, all of the distribution properties defined are unaltered by the omission of any finite number of terms at the beginning of a sequence or the addition of a fixed element of the appropriate set to every term of a sequence.

In this paper we shall prove a number of results relating the distribution of sequences in Φ' to the distribution of certain associated sequences in Φ. The main application of these reselts is to the proof of the fact that if $f(u)$ is a polynomial of degree k with coefficients in Φ', $1 \leqq k < p$, and some coefficient of $f(u)$ besides $f(0)$ is *irrational*, that is, is not a quotient of elements of Φ, then a certain related sequence $\theta_f = \{[f(A_i)]\}$ in Φ is w.u.d. The results obtained here are analogous to (but somewhat more involved than) those proved by VANDEN EYNDEN [4], and reported by NIVEN [3], for uniform distribution of sequences of real number and of integers.

2. - Relationships between uniform distributions in Φ' and in Φ.

Using the definitions given in Section 1 we first prove

THEOREM 2.1. - *A sequence* $\Gamma = \{\gamma_i\}$ *in* Φ' *is* u.d. (mod 1)/s.u.d.(mod 1) *if and only if for all monic* $M \in \Phi$, *the sequence* $\Gamma_M = \{[M\gamma_i]\}$ *is* u.d.(mod M)/s.u.d.(mod M).

PROOF. - We give the proof for uniform distributivitiy. The proof for semi-uniform distributivity is essentially the same.

Suppose that $\Gamma = \{\gamma_i\}$ is u.d. (mod 1) in Φ'. Let M be any monic element of Φ of degree $m > 0$ and $B \in \Phi$ be arbitrary of degree $< m$. Then with $\beta = B/M$, for all $k \geqq 1$, by condition (1.4) we have

$$\lim_{n\to\infty} N_k(n,\ B/M)/n = q^{-k}.$$

If γ_i satisfies $\deg((\gamma_i - B/M)) < -k$, Let

$$\gamma_i - B/M = F_i + ((\gamma_i - B/M)), \qquad F_i \in \Phi. \tag{2.1}$$

If we multiply equation (2.1) by M and take the case $k = m$, we get

$$M\gamma_i = B + MF_i + M((\gamma_i - B/M)),$$

where $\deg M((\gamma_i - B/M)) < 0$. Therefore, for such a γ_i,

$$[M\gamma_i] = B + MF_i \equiv B \pmod{M}. \tag{2.2}$$

Conversely, if γ_i satisfies (2.2), then (2.1) holds with $\deg((\gamma_i - B/M)) < -m$. In view of this equivalence between (2.1) and (2.2), it is clear that for all positive integers n, all monic $M \in \Phi$ of degree m and all $B \in \Phi$,

$$\Gamma_M(n,\ B,\ M) = N_m(n,\ B/M),$$

so that

$$\lim_{n\to\infty} \Gamma_M(n,\ B,\ M)/n = \lim_{n\to\infty} N_m(n,\ B/M)/n = q^{-m}.$$

Thus Γ_M is u.d. (mod M) in Φ.

On the other hand, suppose that for all monic $M \in \Phi$, $\Gamma_M = \{[M\gamma_i]\}$ is u.d. (mod M) in Φ. Then for any $B \in \Phi$, if $\deg M = m$,

$$\lim_{n\to\infty} \Gamma_M(n,\ B,\ M)/n = q^{-m}.$$

Let m be any positive integer and $\beta \in \Phi'$ be arbitrary. Then $\beta = F_\beta + ((\beta))$, with $F_\beta \in \Phi$ so $F_\beta = 0$ or $\deg F_\beta \geqq 0$ and $\deg((\beta)) < 0$. Let M be any fixed monic polynomial of degree m and let

$$M((\beta)) = B + \gamma \quad \text{with} \quad B \in \Phi, \qquad \gamma = ((M((\beta)))),$$

so that $\deg B < m$ and $\deg \gamma < 0$.

Now for any positive integer n, if $1 \leqq i \leqq n$ and $[M\gamma_i] = B \pmod{M}$, then by the equivalence of (2.1) and (2.2) we know that that $\deg((\gamma_i - B/M)) < -m$ But, $B = M((\beta)) - \gamma$ with $\deg \gamma < 0$, so that $B/M = ((\beta)) - \gamma/M$ with $\deg(\gamma/M) < -m$. Thus,

$$\deg((\gamma_i - \beta + \gamma/M)) = \deg((\gamma_i - ((\beta)) + \gamma/M)) < -m,$$

which implies, since $\deg(\gamma/M) < -m$, that $\deg((\gamma_i - \beta)) < -m$. Conversely, if $\deg((\gamma_i - \beta)) < -m$, then $[M\gamma_i] \equiv B \pmod{M}$ so that for all integers $n \geqq 1$ $N_m(n, B) = \Gamma_M(n, B, M)$. Therefore,

$$\lim_{n\to\infty} N_m(n, \beta)/n = \lim_{n\to\infty} \Gamma_M(n, B, M)/n = q^{-m}.$$

Therefore $\Gamma = \{\gamma_i\}$ is u.d. (mod 1) and Theorem 2.1 is proved.

As an immediate consequence of this theorem we can prove

COROLLARY 2.2. - *If* $\{\gamma_i\}$ *is any sequence in* Φ' *such that for all monic* $K \in \Phi$ *the sequence* $\{\gamma_i/K\}$ *is* u.d. (mod 1)/s.u.d. (mod 1), *then the sequence* $\{[\gamma_i]\}$ *is* u.d./s.u.d. *in* Φ, *that is, it is* u.d. (mod K) *for all monic* $K \in \Phi$.

PROOF. - Again we only give the proof for uniform distributivity. Let $\{\gamma_i\}$ satisfy the hypothesis and K be any monic element of Φ so that $\{\gamma_i/K\}$ is u.d. (mod 1) in Φ'. Then by Theorem 2.1, for all monic $M \in \Phi$, $\{[M\gamma_i/K]\}$ is u.d. (mod M). In particular, with $M = K$ it follows that $\{[\gamma_i]\}$ is u.d. (mod K). Since K is arbitrary, it follows by definition that $\{[\gamma_i]\}$ is u.d. in Φ.

In [2; § 2] a sequence $\theta = \{A_i\}$ in Φ was defined to be *rising* if and only if $A_i \neq A_j$ and $\deg A_i \leqq \deg A_j$ for all integers $1 \leqq i < j$. (This is an analog for Φ of a strictly increasing sequence of positive integers.) In particular, any sequence θ containing all of the elements of Φ, each occurring once arranged according to monotonically increasing degree is a rising sequence and is easily seen to be w.u.d. although, as shown in [2 § 2], it need not be u.d. In order to consider the next results, we need to extend the concept of rising sequence to Φ'.

A sequence $\Gamma = \{\gamma_i\}$ in Φ' will be called *rising* if and only if it has the properties:

(2.3)
- (a) $\deg \gamma_i \leqq \deg \gamma_j$ for all $1 \leqq i < j$.
- (b) For every sufficiently large integer t, the number $\Gamma(t)$ of elements of Γ of degree $< t$ is $\gtreqless q^t$.

Furthermore, Γ will be called *linearly rising* if and only if it has property (2.3a) and the additional property

(2.4) There exists a linear polynomial $g(t) = kt + c$ with integral coefficients $k > 0$, c such that for all sufficiently large i, $\deg \gamma_i = g(c_i) \geqq 0$ for some integer $c_i > 0$ and for all sufficiently large t, the number $\Gamma(g(t))$ of elements of Γ of degree $< g(t)$ is equal to q^t.

We note that if a sequence θ in Φ is rising in Φ, then it is also rising in Φ' and if, in addition, it contains all the elements of Φ, then is linearly rising in Φ' with $g(t) = t$.

Now, as a direct consequence of Theorem 2.1 we have

COROLLARY 2.3. – *If sequence* $\Gamma = \{\gamma_i\}$ *in* Φ' *is rising and* u.d. (mod 1), *then for all monic* $M \in \Phi$, *the sequence* $\Gamma_m = \{[M\gamma_i]\}$ *is* w.u.d. (mod M) in Φ.

PROOF. – If Γ satisfies the hypotheses then, by Theorem 2.1, for all monic $M \in \Phi$, Γ_M is u.d. (mod M) in Φ.

Since Γ is rising in Φ', by (2.3b) no element of Φ' appears infinitely often in Γ and by (2.3a) and (2.3b), for sufficiently large $t > 0$, the $\Gamma(t) \leqq q^t$ elements of Γ of degree $< t$ are the *first* $\Gamma(t)$ elements of Γ. Therefore, for any sufficiently large $t > 0$, if $\Gamma_M(t) = j > 0$, these j elements of Γ_M of degree $< t$ are the first j elements of Γ_M so that for any $B \in \Phi$,

$$N(\Gamma_M,\ t,\ B,\ M) = \Gamma_M(j,\ B,\ M).$$

Thus, since Γ_M is u.d. (mod M), if $\deg M = m$,

$$\lim_{t\to\infty} N(_M,\ t,\ B,\ M)/\Gamma_M(t) = \lim_{j\to\infty} \Gamma_m(j,\ B,\ M)/j = q^{-m},$$

since the subsequence of distinct quotients on the left is a subsequence of the convergent sequence of quotients on the right and no quotient in the left sequence appears infinitely often. Therefore, by definition, Γ_M is w.u.d. (mod. M) in Φ.

A result which is similar to Corollary 2.3, but seems to be more useful in the applications we wish to consider, is

THEOREM 2.4. – *If the sequence* $\Gamma = \{\gamma_i\}$ *in* Φ' *is linearly rising and* s.u.d. (mod 1), *then for all monic* $M \in \Phi$, *the sequence* $\Gamma_M = \{[M\gamma_i]\}$ *is* w.u.d. (mod M) *in* Φ.

PROOF. – By definition of linearly rising, there exists a linear polynomial $g(t) = kt + c$ with integral coefficients $k > 0$, c such that for all sufficiently large i, $\deg \gamma_i = g(c_i) \geqq 0$ for some integer $c_i > 0$ and for all sufficiently large t, the number $\Gamma(g(t))$ of elements of Γ of degree $< g(t)$ is $\Gamma(g(t)) = \Gamma(kt + c) = q^t$.

Let monic $M \in \Phi$ be arbitrary of degree $m > 0$. For all integers $i \geqq 1$, $M\gamma_i = M[\gamma_i] + M((\gamma_i))$, so that for all sufficiently large i,

$$\deg [M\gamma_i] = \deg M[\gamma_i] = m + g(c_j) = kc_i + (m + c).$$

Since for all sufficiently large t, $\Gamma(g(t)) = q^t$, it follows that for all sufficiently large t, sequence $\Gamma_M = \{[M\gamma_i]\}$ has the property $\Gamma_M(kt + (m + c)) = q^t$ and by property (2.3a), these q^t elements of Γ_M correspond to the first q^t elements of Γ. Also, by virtue of the equivalence between conditions (2.1) and (2.2), we see that for all $B \in \Phi$

$$N(\Gamma_M,\ kt + (m + c),\ B,\ M) = N_m(q^t,\ B/M).$$

Therefore, for all $B \in \Phi$, since Γ is s.u.d. (mod 1) in Φ',

$$\lim_{n\to\infty} \frac{N(\Gamma_M,\ n,\ B,\ M)}{\Gamma_M(n)} = \lim_{t\to\infty} \frac{N(\Gamma_M,\ kt + (m + c),\ B,\ M)}{\Gamma_M(kt + (m + c))} = \lim_{t\to\infty} N_m(q^t,\ B/M)/q^t = q^{-m}.$$

since for sufficiently large n, the distinct quotients on the left are elements of a subsequence of the convergent sequence of quotients in the niddle and no quotient in the left sequence appears infinitely often. Thus by definition Γ_M is w.u.d. (mod M) in Φ.

COROLLARY 2.5. - *Let $f(u)$ be any polynomial with coefficients in Φ' and $\{A_i\}$ be any rising sequence in Φ which contains all the elements of Φ. If the sequence $\theta = \{f(A_i)\}$ is* s.u.d. (mod 1) *in Φ', then for all monic $M \in \Phi$, the sequence $\theta_M = \{[Mf(A_i)]\}$ is* w.u.d. (mod M) *in Φ.*

PROOF. - Let $f(u)$ have degree k and c be the degree, as an element of Φ', of the leading coefficient of $f(u)$. Then if $\deg A_i = a_i$, $\deg f(A_i) = ka_i + c \geqq 0$ for all sufficiently large a_i. Let $M \in \Phi$ be monic of degree m. Then for all integers $t \geqq 1$, $\deg f(A_i) = (ka_i + c) < kt + c$ if and only if $a_i < t$, and this latter condition holds if and only if $1 \leqq i \leqq q^t$. Thus for all sufficiently large t, the number $\theta(kt + c)$ of elements of θ of degree $< kt + c$ is q^t. Also, since $\{A_i\}$ is a rising sequence, $\deg f(A_i) \leqq \deg f(A_j)$ for all $1 \leqq i < j$. Therefore, by definition, θ is linearly rising sequence in Φ'. Since by hypothesis θ is s.u.d. (mod 1) it follows by Theorem 2.4 that for all monic $M \in \Phi$, the sequence $\theta_M = \{[Mf(A_i)]\}$ is w.u.d. (mod M) in Φ.

3. - An application to sequences in Φ.

The motivation for the introduction in section 2 of the concept of a linearly rising rising sequence in Φ' and its role in Theorem 2.4 and Corollary 2.5 is to be found in the following result.

THEOREM 3.1. - *Let $f(u)$ be any polnomial of degree k, $1 \leqq k < p$, with coefficients in Φ' such that $f(u) - f(0)$ has at least one irrational (not a quotient of elements of Φ) coefficient and let $\{A_i\}$ be any rising sequence in Φ*

which contains all the elements of Φ. *Then the sequence* $\{[f(A_i)]\}$ *is* w.u.d. *in* Φ.

PROOF. - For every monic $K \in \Phi$, the polynomial $f(u)/K$ with coefficients in Φ' has the property of $f(u)$ stated in the hypotheses. Then by a result of CARLITZ [1; Theorem 9] it follows that $\{f(A_i)/K\}$ is s.u.d. (mod 1) in Φ' for all monic $K \in \Phi$.

Thus, by Corollary 2.5, for any fixed monic $K \in \Phi$, the sequence $\{[Mf(A_i)/K]\}$ is w.u.d. (mod M) in Φ. In particular, with $M = K$, $\{[f(A_i)]\}$ is w.u.d. (mod K). Since this result holds for all monic $K \in \Phi$, by definition, $\{[f(A_i)]\}$ is w.u.d. in Φ.

The case of this theorem with $f(u) = \xi u$, where ξ is irrational, has been previously proved by the author [2; Theorem 4.2].

REFERENCES

[1] L. CARLITZ, *Diophantine approximation in fields of characteristic p*, Trans. Amer. Math. Soc. 72 (1951), 187-208.

[2] JOHN H. HODGES, *Uniform distribution of sequences in GF[q, x]*, Acta. Arith. 12 (1966), 55-75.

[3] IVAN NIVAN, *Uniform distribution of sequences of integers*, Compositio Math. 16 Fasc. 1, 2 (1964), 158-160.

[4] C. L. VANDEN EYNDEN, *The uniform distribution of sequences*, dissertation, University of Oregon, 1962.