ON UNIFORM DISTRIBUTION OF SEQUENCES IN $GF[q, x]$ AND $GF\{q, x\}$.

By H. G. Meijer and A. Dijksma

1. Introduction and preliminaries. Let $\Phi = GF[q, x]$ denote the ring of polynomials in the indeterminate x over an arbitrary finite field $GF(q)$ of q elements. If A and M are any two elements of Φ with $\deg M > 0$, let $A(M)$ be the uniquely determined element of Φ such that $\deg A(M) < \deg M$ and $A \equiv A(M) \pmod{M}$.

J. H. Hodges [2; 55] defined the uniform distribution of a sequence $\theta = (A_i)$ of elements of Φ as follows. Let M be any element of Φ with $\deg M = m > 0$. For any $B \varepsilon \Phi$ and integer $n \geq 1$ define $\theta(n, B, M)$ as the number of terms among $A_1, A_2, \cdots, A_n$ such that $A_i(M) = B(M)$. Then the sequence θ is said to be *uniformly distributed modulo* M *in* Φ if

$$\lim_{n\to\infty} n^{-1}\theta(n, B, M) = q^{-m} \quad \text{for all} \quad B \varepsilon \Phi. \tag{1.1}$$

The sequence θ is said to be *uniformly distributed in* Φ if (1.1) holds for every $M \varepsilon \Phi$ with $\deg M = m > 0$.

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

$$\alpha = \sum_{i=-\infty}^{m} c_i x^i \qquad (c_i \varepsilon GF(q)).$$

If α has this representation and $c_m \neq 0$, then we define $\deg \alpha = m$. We extend this definition by writing $\deg 0 = -\infty$. The integral and fractional parts of α, denoted by $[\alpha]$ and $((\alpha))$ respectively, are defined by

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

It follows from the definition, that, for α and β in Φ', we have $[\alpha + \beta] = [\alpha] + [\beta]$. We say $\alpha \equiv \beta \pmod{1}$ if $\alpha = \beta + A$, where $A \varepsilon \Phi$. It follows that $\alpha \varepsilon \Phi'$ is congruent modulo 1 to a unique β, namely $\beta = ((\alpha))$, such that $\deg \beta < 0$.

L. Carlitz [1; 190] defined the uniform distribution of a sequence $\theta = (\alpha_i)$ of elements of Φ' in the following way. For any $\beta \varepsilon \Phi'$ and any positive integers n and k, define $\theta_k(n, \beta)$ as the number of terms among $\alpha_1, \alpha_2, \cdots, \alpha_n$ such that $\deg ((\alpha_i - \beta)) < -k$. Then the sequence θ is *uniformly distributed modulo 1 in* Φ' if

$$\lim_{n\to\infty} n^{-1}\theta_k(n, \beta) = q^{-k} \quad \text{for all} \quad k \quad \text{and} \quad \beta \varepsilon \Phi'. \tag{1.2}$$

Received September 16, 1968.

An element $\alpha \in \Phi'$ is said to be irrational if it is not an element of $GF(q, x)$, i.e., if it cannot be written as a quotient A/B with A and B in Φ. Well known is Kronecker's criterion for irrationality: If $\alpha = \sum_{i=-\infty}^{m} c_i x^i$, then α is irrational if and only if

$$\begin{vmatrix} c_{-1} & c_{-2} & \cdots & c_{-s} \\ c_{-2} & c_{-3} & \cdots & c_{-s-1} \\ \vdots & & & \\ c_{-s} & c_{-s-1} & \cdots & c_{-2s+1} \end{vmatrix} \neq 0 \tag{1.3}$$

for infinitely many $s > 0$.

The aim of this paper is to extend some of the results of L. Carlitz and J. H. Hodges. To do this we introduce a mapping of Φ onto the set of nonnegative integers I. Let τ be a one-to-one correspondence between $GF(q)$ and the set $\{0, 1, \cdots, q-1\}$ such that $\tau(0) = 0$. We extend the domain and range of τ to Φ and I by defining $\tau(a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0) = \tau(a_n)q^n + \tau(a_{n-1})q^{n-1} + \cdots + \tau(a_1)q + \tau(a_0)$. Clearly τ is a one-to-one correspondence between Φ and I. Then the sequence $\Gamma = (C_i) = (\tau^{-1}(i-1))$ consists of all elements of Φ, all occurring exactly once. Hence we have ordered the elements of Φ. We remark that Γ is uniformly distributed in Φ (compare [2; 62–63]).

S. Uchiyama [5] has given a criterion for uniform distribution of a sequence in I. Using the mapping τ, we can give a simple criterion for uniform distribution in Φ. See §2 (Theorem 1).

In §3 we prove that $(C_i\alpha)$ is uniformly distributed modulo 1 in Φ' if and only if α is irrational (Theorems 2 and 3). We furthermore prove that $([C_i\alpha])$ is uniformly distributed in Φ if and only if α is irrational or $\alpha = A/B$ with $A, B \in \Phi$, $\deg A \leq \deg B$, $\alpha \neq 0$ (Theorem 4). We remark that L. Carlitz [1; 191] and J. H. Hodges [2; 65] have already proved that these sequences are weakly uniformly distributed, i.e., they have proved that for these sequences the limits in (1.1) and (1.2) exist if n tends to infinity along the subsequence $n = q^t (t = 1, 2, \cdots)$. (We note that for Φ the concept of "weakly uniformly distributed" defined in [2] is not, in general, the analog of this concept as defined for Φ' in [1]). Furthermore, we observe that Theorem 4 is the complete analog of Hodges' Theorem 4.2.

2. Criterion for uniform distribution in Φ. J. H. Hodges [2] gave a necessary condition for uniform distribution of a sequence in Φ. L. Kuipers [3] modified this condition to a necessary and sufficient one. We will give a somewhat less complicated criterion using the mapping τ. To prove this criterion we use the concept of uniform distribution in I. I. Niven [4] defined this for a sequence $\Psi = (a_n)$ of elements of I as follows. Let j and $m \geq 2$ be any elements of I and define $\Psi(n, j, m)$ to be the number of elements among $a_1, a_2, \cdots, a_n$ satisfying $a_i \equiv j \pmod{m}$. Then the sequence Ψ is said to be uniformly distributed modulo m in I if

$$\lim_{n\to\infty} n^{-1}\Psi(n, j, m) = m^{-1} \quad \text{for all} \quad j \,\varepsilon\, I.$$

S. Uchiyama [5] proved the following criterion: $\Psi = (a_n)$ is uniformly distributed modulo m in I if and only if

$$\lim_{n\to\infty} n^{-1} \sum_{j=1}^{n} \exp(2\pi i h a_j/m) = 0 \quad \text{for} \quad h = 1, 2, \cdots, m - 1. \tag{2.1}$$

For the sake of brevity we shall use the following notation. Let M be any polynomial of degree m. Then we define for any $A \,\varepsilon\, \Phi$ and $h \,\varepsilon\, I$,

$$e_M(A, h) = \exp[2\pi i h \tau(A(M))/q^m].$$

THEOREM 1. *The sequence* $\theta = (A_i)$ *of elements of* Φ *is uniformly distributed modulo* M *in* Φ *if and only if*

$$\lim_{n\to\infty} n^{-1} \sum_{i=1}^{n} e_M(A_i, h) = 0 \quad \text{for} \quad h = 1, 2, \cdots, q^m - 1.$$

Proof. Let $\Psi = (\tau(A_i(M)))$ and B be an arbitrary element of Φ. Then $A_i \equiv B \pmod{M}$ is equivalent to $A_i(M) = B(M)$ or $\tau(A_i(M)) = \tau(B(M))$. Hence

$$\Psi(n, \tau(B(M)), q^m) = \theta(n, B, M).$$

Therefore the sequence θ is uniformly distributed modulo M in Φ if and only if Ψ is uniformly distributed modulo q^m in I. Hence Theorem 1 is a direct consequence of S. Uchiyama's criterion (2.1). This completes the proof.

3. Uniform distribution of $(C_i\alpha)$ and $([C_i\alpha])$.

THEOREM 2. *Let* $\Gamma = (C_i) = (\tau^{-1}(i - 1))$ *and let* $\alpha \,\varepsilon\, \Phi'$ *be irrational. Then the sequence* $\theta = (C_i\alpha)$ *is uniformly distributed modulo 1 in* Φ'.

Proof. Let k be any positive integer and let $\beta = \sum_{i=-\infty}^{n} b_i x^i$ be an arbitrary element of Φ'. Then since $\alpha = \sum_{i=-\infty}^{m} c_i x^i$ is irrational, there exists an integer $s \geq k$ such that (1.3) holds. If $A = a_r x^r + a_{r-1}x^{r-1} + \cdots + a_0$, with $r \geq s - 1$, satisfies the inequality

$$\deg((A\alpha - \beta)) < -k, \tag{3.1}$$

then the coefficients $a_r, a_{r-1}, \cdots, a_0$ satisfy

$$\begin{aligned}
a_0c_{-1} &+ \cdots + a_{s-1}c_{-s} &&= b_{-1} - (a_sc_{-s-1} + \cdots + a_rc_{-r-1})\\
&\vdots\\
a_0c_{-k} &+ \cdots + a_{s-1}c_{-s-k+1} &&= b_{-k} - (a_sc_{-s-k} + \cdots + a_rc_{-r-k})\\
a_0c_{-k-1} &+ \cdots + a_{s-1}c_{-s-k} &&= e_1 \quad - (a_sc_{-s-k-1} + \cdots + a_rc_{-r-k-1})\\
&\vdots\\
a_0c_{-s} &+ \cdots + a_{s-1}c_{-2s+1} &&= e_{s-k} - (a_sc_{-2s} + \cdots + a_rc_{-r-s}),
\end{aligned} \tag{3.2}$$

where $e_i \varepsilon GF(q)$ $(i = 1, 2, \cdots, s - k)$ are arbitrary. If $s = k$, then the equations of (3.2) containing e_i vanish. Using Cramer's rule, it follows that we may write

$$\begin{aligned} a_0 &= c_{0,0} + c_{0,s}a_s + \cdots + c_{0,r}a_r \\ a_1 &= c_{1,0} + c_{1,s}a_s + \quad + c_{1,r}a_r \\ &\cdots \\ a_{s-1} &= c_{s-1,0} + c_{s-1,s}a_s + \cdots + c_{s-1,r}a_r , \end{aligned}$$

where $c_{i,j} \varepsilon GF(q)$. Here the coefficients $c_{i,0}$ $(i = 0, 1, \cdots, s - 1)$ depend on $e_1, e_2, \cdots, e_{s-k}$, while the coefficients $c_{i,j}$ with $j = s, s + 1, \cdots, r$ are independent of $e_1, e_2, \cdots, e_{s-k}$. Moreover if $\{e_1', e_2', \cdots, e_{s-k}'\}$ differs from $\{e_1, e_2, \cdots, e_{s-k}\}$ then the corresponding set of coefficients $\{c_{0,0}', c_{1,0}', \cdots, c_{s-1,0}'\}$ differs from $\{c_{0,0}, c_{1,0}, \cdots, c_{s-1,0}\}$. Therefore the solutions A of (3.1) are of the form

$$\begin{aligned} A &= a_0 + a_1x + \cdots + a_rx^r \\ &= (c_{0,0} + c_{1,0}x + \cdots + c_{s-1,0}x^{s-1}) + a_s(c_{0,s} + c_{1,s}x + \cdots + c_{s-1,s}x^{s-1}) \\ &\quad + \cdots + a_r(c_{0,r} + c_{1,r}x + \cdots + c_{s-1,r}x^{s-1}) \\ &\quad + a_sx^s + a_{s+1}x^{s+1} + \cdots + a_rx^r. \end{aligned}$$

Hence

$$(3.3) \quad A = G_t + a_sF_s + a_{s+1}F_{s+1} + \cdots + a_rF_r + a_sx^s + a_{s+1}x^{s+1} + \cdots + a_rx^r,$$

where $F_s, F_{s+1}, \cdots, F_r$ are fixed polynomials of degree $\leq s - 1$, $a_s, a_{s+1}, \cdots, a_r$ may be chosen arbitrarily in $GF(q)$ and where G_t is a polynomial with coefficients depending on $e_1, e_2, \cdots, e_{s-k}$. Since there are q^{s-k} different sets $\{e_1, e_2, \cdots, e_{s-k}\}$ there are q^{s-k} different polynomials G_t and $t = 1, 2, \cdots, q^{s-k}$.

Now $\theta_k(n, \beta)$ equals the number of polynomials among $C_1, C_2, \cdots, C_n$ which are of the form (3.3); i.e., $\theta_k(n, \beta)$ is the number of polynomials of the form (3.3) with

$$(3.4) \quad \tau(A) = \tau(a_r)q^r + \cdots + \tau(a_s)q^s + \tau(a_rF_r + \cdots + a_sF_s + G_t) \leq n - 1.$$

Suppose first that

$$(3.5) \quad n - 1 = b_rq^r + b_{r-1}q^{r-1} + \cdots + b_sq^s + (q - 1)q^{s-1} + \cdots + (q - 1),$$

where $0 \leq b_i \leq q - 1$ $(i = s, s + 1, \cdots, r)$, i.e., $n = aq^s$ for some integer a. Since $t \varepsilon \{1, 2, \cdots, q^{s-k}\}$, we observe by comparing the equations (3.4) and (3.5) that

$$\begin{aligned} \theta_k(n, \beta) &= q^{s-k}(b_rq^{r-s} + b_{r-1}q^{r-s-1} + \cdots + b_s + 1) \\ &= aq^{s-k} \\ &= q^{-k}n. \end{aligned}$$

Let now n be arbitrary; then

$$|\theta_k(n, \beta) - q^{-k}n| \leq q^{s-k},$$

from which the theorem follows. This completes the proof.

THEOREM 3. *$\theta = (C_i\alpha)$ is uniformly distributed modulo 1 in Φ' if and only if α is irrational.*

Proof. In Theorem 2 we have shown that if α is irrational, then θ is uniformly distributed modulo 1 in Φ'. Suppose now that $\alpha = A/B$ where A and B belong to Φ and set $\deg B = b$. We may, and do, suppose that $(A, B) = 1$. If θ is uniformly distributed modulo 1 in Φ', then we get from (1.2) with $k = b + 1$ and $\beta = 0$,

$$\lim_{n\to\infty} n^{-1}\theta_k(n, 0) = q^{-b-1}.$$

If $\deg ((CA/B)) < -b - 1$, there exist $F \varepsilon \Phi$ and $\delta \varepsilon \Phi'$ such that $\deg \delta < -b - 1$ and

$$CA/B = F + \delta,$$

or

$$CA - FB = B\delta.$$

Since $CA - FB \varepsilon \Phi$ and $\deg (B\delta) \leq -1$, it follows that $\delta = 0$ and B divides C. Conversely, if B divides C, then $\deg ((CA/B)) = -\infty < -b - 1$. Thus $\deg ((CA/B)) < -b - 1$ if and only if $C \equiv 0 \pmod B$. Since the sequence $\Gamma = (C_i)$ is uniformly distributed modulo B in Φ (compare [2; 62–63]), it follows that

$$\lim_{n\to\infty} n^{-1}\theta_{b+1}(n, 0) = \lim_{n\to\infty} n^{-1}\Gamma(n, 0, B) = q^{-b} \neq q^{-b-1}.$$

We have thus arrived at a contradiction, and hence the theorem is proved.

THEOREM 4. *Let $\Gamma = (C_i)$ be as above. Then $\Psi = ([C_i\alpha])$ is uniformly distributed in Φ if and only if α is irrational or $\alpha = A/B$ where $A, B \varepsilon \Phi$, $\alpha \neq 0$ and $a = \deg A \leq b = \deg B$.*

Proof. The proof is divided into three parts: (I) α is irrational; (II) $\alpha = A/B$, $A, B \varepsilon \Phi$ and $a > b$; (III) $\alpha = A/B$, $A, B \varepsilon \Phi$ and $a \leq b$.

I (*α is irrational*). Let M be any polynomial of degree $m > 0$. Then α/M is irrational and according to Theorem 2, $\theta = (C_i\alpha/M)$ is uniformly distributed modulo 1 in Φ'. Hence if $D \varepsilon \Phi$ with $d = \deg D < m$, then for $k > 0$,

$$\lim_{n\to\infty} n^{-1}\theta_k(n, D/M) = q^{-k}. \tag{3.6}$$

If

$$\deg ((C_i\alpha/M - D/M)) < -k \tag{3.7}$$

then there exist $F \varepsilon \Phi$ and $\delta \varepsilon \Phi'$ such that $\deg \delta < -k$ and

$$C_i\alpha/M - D/M = F + \delta$$

or

$$C_i\alpha = FM + D + M\delta,$$

and hence $[C_i\alpha] \equiv D \pmod{M}$ if $k \geq m$. Conversely, if $[C_i\alpha] \equiv D \pmod{M}$, then (3.7) holds for $k = m$. Because of this equivalence we have that

$$\theta_m(n, D/M) = \Psi(n, D, M).$$

From this and (3.6) it follows that

$$\lim_{n\to\infty} n^{-1}\Psi(n, D, M) = q^{-m}.$$

II ($\alpha = A/B; a > b$). If B divides C_i, then obviously $[C_iA/B] \equiv 0 \pmod{A}$. Conversely if $[C_iA/B] \equiv 0 \pmod{A}$, then there exist $F \varepsilon \Phi$ and $\delta \varepsilon \Phi'$ such that $\deg \delta < 0$ and

$$C_iA/B = FA + \delta$$

or

$$C_i - FB = \delta B/A.$$

Since $\deg \delta B/A < 0$, it follows that $C_i = FB$ or $C_i \equiv 0 \pmod{B}$. This implies that $[C_iA/B] \equiv 0 \pmod{A}$ if and only if $C_i \equiv 0 \pmod{B}$. Since $\Gamma = (C_i)$ is uniformly distributed modulo B in Φ, we get

$$\lim_{n\to\infty} n^{-1}\Psi(n, 0, A) = \lim_{n\to\infty} n^{-1}\Gamma(n, 0, B) = q^{-b} > q^{-a},$$

which implies that the sequence Ψ is not uniformly distributed in Φ.

III ($\alpha = A/B; a \leq b$). By definition $\Psi(n, D, M)$ is the number of elements among $C_1, C_2, \cdots, C_n$ which satisfy the equation

$$[XA/B] \equiv D(M) \pmod{M}. \tag{3.8}$$

X_0 satisfies (3.8) if and only if it satisfies

$$[XA/B] \equiv D(M) + E_tM \pmod{AM} \tag{3.9}$$

where E_t is a polynomial of degree $< a$, also $t = 1, 2, \cdots, q^a$. We now discuss for a moment equation (3.9) where t and $D(M)$ are fixed. Let X_0 satisfy (3.9). Let F be a polynomial of degree $< b - a$ and let H be an arbitrary polynomial. Then also

$$X_0 + HBM + F \tag{3.10}$$

is a solution of (3.9). On the other hand, if X_0 and X_1 satisfy (3.9), then

$$[(X_0 - X_1)A/B] \equiv 0 \pmod{AM}.$$

Hence $(X_0 - X_1)A/B = HAM + \delta$, where $\delta \in \Phi'$ with $\deg \delta < 0$. Therefore $X_0 - X_1 = HBM + \delta B/A$. We set $F = \delta B/A$. Then $\deg F < b - a$, and since $F = X_0 - X_1 - HBM$, we have $F \in \Phi$. Thus if (3.9) has a solution X_0, then the other solutions are given by (3.10), where H is arbitrary and F is arbitrary but $\deg F < b - a$. Hence there are q^{b-a} solutions of degree $< b + m$, and we may assume $\deg X_0 < b + m$.

Since there are q^{b+m} polynomials of degree $< b + m$, it follows that $q^{b+m}: q^{b-a} = q^{a+m}$ equations of the form (3.9) are solvable. On the other hand, there are q^m different polynomials $D(M)$ and q^a different polynomials E_t, so that there are q^{m+a} different equations of the form (3.9), and hence all are solvable.

Now we want to determine $\Psi'(n, D, M)$, the number of terms among C_1, C_2, $\cdots$, C_n which are solutions of (3.9) for fixed t and $D(M)$. In other words, we want to determine the number of polynomials of the form (3.10) with

$$\tau(X_0 + HBM + F) \leq n - 1.$$

Let $HBM = G_1 + G_2$ where $\deg G_2 < b + m$ and $G_1 = d_r x^r + \cdots + d_{b+m}x^{b+m}$ with $r = \deg HBM$ (if $H = 0$ so that $r = -\infty$, then $G_1 = 0$). Then

$$\tau(X_0 + F + HBM) = \tau(d_r)q^r + \cdots + \tau(d_{b+m})q^{b+m} + \tau(X_0 + F + G_2).$$

Here F and H are arbitrary with $\deg F < b - a$. BM is fixed, while G_1 depends on the choice of H. In fact, if we compare the coefficients of H, BM and G_1, we conclude that there is a one-to-one correspondence between the polynomials H and G_1. If $n = eq^{b+m}$, we get as in the proof of Theorem 2, that

$$\Psi'(n, D, M) = nq^{-m-a}.$$

Since $t \in \{1, 2, \cdots, q^a\}$, we get

$$\Psi(n, D, M) = q^a\Psi'(n, D, M) = nq^{-m}.$$

From this it follows after some calculation that

$$|\Psi(n, D, M) - nq^{-m}| \leq q^b$$

for all n, so that the sequence is uniformly distributed in Φ. This completes the proof.

4. Complementary sequences. Let $\theta = (A_i)$ be a subsequence of $\Gamma = (C_i) = (\tau^{-1}(i - 1))$. If $\theta \neq \Gamma$, then we denote by θ^* the complementary sequence of θ, which is a subsequence of Γ and consists of all elements of Γ which do not belong to θ. Here θ^* may be finite or infinite. We recall that Γ is uniformly distributed in Φ (compare [2; 62–63]). We now prove the following theorem.

THEOREM 5. *Let $\theta = (A_i)$ be an infinite subsequence of $\Gamma = (\tau^{-1}(i - 1))$. Let $A(n, \theta)$ denote the number of terms A_i with $\tau(A_i) < n$. If $s = \lim\sup n^{-1}A(n, \theta) < 1$ and θ is uniformly distributed modulo M, then θ^* is also uniformly distributed modulo M.*

Proof. Since lim sup $n^{-1}A(n, \theta) < 1$, the sequence θ^* is infinite. For the sake of brevity we write $k_1 = A(n, \theta)$ and $k_2 = n - A(n, \theta) = A(n, \theta^*)$. Then $k_1/n < (1 + s)/2$ and $k_2/n > (1 - s)/2$ if n is sufficiently large. For any polynomial B we have

$$\theta^*(k_2, B, M) = \Gamma(n, B, M) - \theta(k_1, B, M)$$

or

$$k_2^{-1}\theta^*(k_2, B, M) = n^{-1}\Gamma(n, B, M) + (k_1/k_2)\{n^{-1}\Gamma(n, B, M) - k_1^{-1}\theta(k_1, B, M)\}. \tag{4.1}$$

Here $(k_1/k_2) < (1 + s)/(1 - s)$ if n is sufficiently large. As k_2 tends to infinity through the sequence of all positive integers, then obviously n and k_1 tend to infinity through subsequences of the sequence of all integers. Since Γ and θ are uniformly distributed modulo M, the second term in the right-hand side of (4.1) tends to zero. Hence

$$\lim_{k_2\to\infty} k_2^{-1}\theta^*(k_2, B, M) = \lim_{n\to\infty} n^{-1}\Gamma(n, B, M) = q^{-m},$$

which proves the theorem.

References

1. L. Carlitz, *Diophantine approximation in fields of characteristic p*, Trans. Amer. Math. Soc., vol. 72(1952), pp. 187–208.
2. J. H. Hodges, *Uniform distribution in GF[q, x]*, Acta Arithmetica, vol. XII (1966), pp. 55–75.
3. L. Kuipers, *A remark on Hodges' paper on uniform distribution in Galois fields* (Abstract presented by title), Notices Amer. Math. Soc., vol. 15(1968), p. 120.
4. I. Niven, *Uniform distribution of sequences of integers*, Trans. Amer. Math. Soc., vol. 98(1961), pp. 52–61.
5. S. Uchiyama, *On the uniform distribution of sequences of integers*, Proc. Japan Acad., vol. 37(1961), pp. 605–609.

Technische Hogeschool Delft
Delft, Netherlands