1. Introduction

Let $\Phi = GF[q, x]$ denote the ring of polynomials in the indeterminate $x$ over a finite field $GF(q)$ of $q$ elements, where $q = p^r$ for some prime number $p$ and positive integer $r$.

Let $\theta = \{A_i\}$ be a sequence of elements in $\Phi$. Let $M \in \Phi$ be a polynomial of degree $m \geq 1$. If $B$ is an arbitrary element of $\Phi$, then by $\theta(n, B, M)$ we denote the number of elements $A_i$ among $A_1, A_2, \ldots, A_n$ which satisfy $A_i \equiv B \pmod{M}$. Following J. H. Hodges ([2], p. 55) we say $\theta$ is uniformly distributed (mod $M$) in $\Phi$ if for every $B \in \Phi$

$$\lim_{n \to \infty} n^{-1} \theta(n, B, M) = q^{-m}. \quad (1.1)$$

Obviously for $\theta$ to be uniformly distributed (mod $M$) (1.1) has to be satisfied for all residues mod $M$. Furthermore we say $\theta$ is uniformly distributed in $\Phi$ if $\theta$ is uniformly distributed (mod $M$) in $\Phi$ for all $M \in \Phi$ of degree larger than zero.

J. H. Hodges ([2], pp. 69–74) and L. Kuipers ([3]) proved a Weyl criterion concerning uniform distribution (mod $M$) in $\Phi$, and so did H. G. Meijer and A. Dijksma ([4]). However, neither one of these criteria could lead to a Weyl criterion concerning uniform distribution in $\Phi$ without reference to some modulus. In this paper such a criterion is given. See paragraph 2.

This criterion is derived from a criterion proved by L. Carlitz ([1], p. 190) who defined uniform distribution of sequences in $\Phi' = GF[q, x]$, which is the field consisting of all quantities

$$\sum_{t=-\infty}^{m} c_t x^t, \quad (c_t \in GF(q)), \quad (1.2)$$

where $m = \deg(\alpha)$ may attain all integer values.

If $\alpha \in \Phi'$ and $\alpha = AB^{-1}$ for some $A$ and $B$ in $\Phi$, then $\alpha$ is called rational, otherwise $\alpha$ is called irrational. The sum $\sum_{t=0}^{m} c_t x^t$ is called the integral part of $\alpha$ and is denoted by $[\alpha]$. The difference $\alpha - [\alpha]$ is called the fractional
part and is denoted by \( ((\alpha)) \). If \( \alpha \) and \( \beta \) are elements of \( \Phi' \) we say \( \alpha \equiv \beta \) (mod 1) if \( \alpha = \beta + A \) for some \( A \in \Phi \).

Given a sequence \( \Psi = \{\alpha_i\} \) of elements of \( \Phi' \) and an arbitrary element \( \beta \in \Phi' \), let \( \Psi_k(n, \beta) \) be the number of elements \( \alpha_i \) among \( \alpha_1, \alpha_2, \ldots, \alpha_n \) such that \( ((\alpha_i - \beta)) < -k \) where \( k \) is a preassigned positive integer. L. Carlitz ([1], p. 190) defined \( \Psi \) to be uniformly distributed (mod 1) in \( \Phi' \) if

\[
(1.3) \quad \lim_{n \to \infty} n^{-1} \Psi_k(n, \beta) = q^{-k}
\]

for all integers \( k \geq 1 \) and all \( \beta \in \Phi' \).

In paragraph 3 a fundamental inequality is derived (lemma (3.2)). Using this inequality and the above mentioned criterion, we will show that theorems proved in [4] may be shown to be true in a less elaborate (and, in this case, more indirect) way. In fact these theorems are special cases of the more general theorems (3.3) and (3.4). Theorem (3.4) indicates a rather large class of uniformly distributed sequences of elements in \( \Phi \).

In a second paper we will give a necessary and sufficient condition for the uniform distributivity of the sequences \( \{f(Z_i)\} \) and \( \{\gamma(Z_i)\} \) in \( \Phi' \) and \( \Phi \), where \( f(Y) \) is a polynomial over \( \Phi' \) of degree \( k \) with \( 0 < k < p \) (\( p \) is the characteristic of the field \( GF(q) \)) and \( \Gamma = \{Z_i\} \) is the sequence constructed in the first part of paragraph 3.

2. A criterion

Let \( \mu \) define \( GF(q) = GF(p^r) \). Then we may write for \( c_{-1} \) in (1.2)

\[
c_{-1} = a_1p^{r-1} + a_2p^{r-2} + \ldots + a_r \quad \text{for some } a_i \in GF(p), \quad (i = 1, 2, \ldots, r).
\]

We define the exponential function \( e: \Phi' \to \mathbb{C} \), the complex number field, by \( e(\alpha) = \exp(2\pi i a_r p^{-1}) \). The following properties of this function have been proved by L. Carlitz ([1], p. 188):

\[
(2.1) \quad e(\alpha + \beta) = e(\alpha) \cdot e(\beta),
\]

\[
(2.2) \quad e(\alpha) = e(\beta) \text{ if } \alpha \equiv \beta \text{ (mod 1)},
\]

\[
(2.3) \quad \sum_{\text{deg}(A) < m} e(Aa) = \begin{cases} 
q^m & \text{if } \text{deg } ((\alpha)) < -m \\
0 & \text{if } \text{deg } ((\alpha)) \geq -m.
\end{cases}
\]

We set \( \text{deg } (0) = -\infty \), and \( \text{deg } (a) = 0 \) if \( a \in GF(q) - \{0\} \).

Furthermore L. Carlitz ([1], p. 190) proved that the sequence \( \Psi = \{\alpha_i\} \) of elements of \( \Phi' \) is uniformly distributed (mod 1) in \( \Phi' \) if and only if

\[
(2.4) \quad \lim_{n \to \infty} n^{-1} \sum_{i=1}^{s} e(A\alpha_i) = 0
\]

for all \( A \in \Phi \) with \( A \neq 0 \).

We now prove the following criterion.
Theorem (2.1). The sequence $\theta = \{A_i\}$ of elements of $\Phi$ is uniformly distributed (mod $M$) in $\Phi$ if and only if

$$\lim_{n \to \infty} n^{-1} \sum_{i=1}^{n} e(CM^{-1}A_i) = 0$$

for all $C \in \Phi$ with $C \neq 0$ and deg $(C) < \text{deg} (M)$.

Proof. Let (2.5) be given and set $m = \text{deg} (M)$. If $B$ is any polynomial in $\Phi$ with $\text{deg} (B) < m$, then it follows from property (2.3) that

$$e(CM^{-1}(A_i - B)) = \begin{cases} q^m & \text{if } A_i \equiv B \pmod{M}, \\ 0 & \text{if } A_i \not\equiv B \pmod{M}. \end{cases}$$

Summing over $i = 1, 2, \ldots, n$, separating terms for which $C\equiv 0$ and using property (2.1), we see that (2.6) becomes

$$n^{-1} \sum_{C \neq 0} e(CM^{-1}B) \sum_{i=1}^{n} e(CM^{-1}A_i) = q^m \theta(n, B, M)$$

or, because of (2.5),

$$n^{-1} \sum_{C \neq 0} e(CM^{-1}B) \sum_{i=1}^{n} e(CM^{-1}A_i) = q^m \theta(n, B, M), \quad (n \to \infty),$$

from which (1.1) follows.

Conversely, suppose $\theta$ is uniformly distributed (mod $M$) in $\Phi$, or, equivalently, suppose that (2.8) holds for all $B \in \Phi$ with $\text{deg} (B) < m$. From (2.2) it follows that for all $C \in \Phi$ with $\text{deg} (C) < m$,

$$\sum_{i=1}^{n} e(CM^{-1}A_i) = \sum_{B \in \Phi} \theta(n, B, M)e(CM^{-1}B).$$

Substituting (2.8) in the above equation, we obtain

$$\sum_{i=1}^{n} e(CM^{-1}A_i) = \sum_{B \in \Phi} \theta(n, B, M)e(CM^{-1}B) = nq^{-m} \sum_{B \in \Phi} e(CM^{-1}B) + o(n).$$

If $C \neq 0$, then (2.3) implies that the sum on the right hand side of equation (2.9) equals zero, for $\text{deg} (CM^{-1}) = \text{deg} (((CM^{-1}))) \geq -m$. Consequently,

$$\sum_{i=1}^{n} e(CM^{-1}A_i) = o(n)$$

for all $C \in \Phi$ with $C \neq 0$ and $\text{deg} (C) < m$. This completes the proof.

Corollary (2.2). The sequence $\theta = \{A_i\}$ of elements of $\Phi$ is uniformly distributed in $\Phi$ if and only if

$$\lim_{n \to \infty} n^{-1} \sum_{i=1}^{n} e(xA_i) = 0$$

for all rational $x \in \Phi'$ such that $\text{deg} (x) \leq -1$ and $x \neq 0$. 
Remark. Let $\Phi$ have the discrete topology. Every subgroup $H$ of $\Phi$ of compact index (i.e., $\Phi/H$ is compact) has the form $M\Phi$ for some $M \in \Phi$. The non-trivial characters of $\Phi/M\Phi$ are precisely given by $\epsilon_{CM-1}$, $0 \leq \deg (C) < \deg (M)$, where $\epsilon_{CM-1}(A) = \epsilon(CM^{-1}A)$. A direct application of the Weyl criterion also gives the proofs of theorem (2.1) and corollary (2.2). Thus these results are special cases of the more general theory of uniform distribution of sequences in locally compact groups which has been developed by L. A. Rubel ([6]). Since the proofs given above are very simple, it seems rather circumstantial to refer to such deeper theorems.

Corollary (2.3). If the sequence $\{a_t\}$ of elements of $\Phi'$ has the property that for some $M \in \Phi$ of degree $m \geq 1$ the sequence $\{M^{-1}a_t\}$ is uniformly distributed (mod 1) in $\Phi'$, then the sequence $\{[a_t]\}$ is uniformly distributed (mod $M$) in $\Phi$.

Proof. If $0 \neq C \in \Phi$ and $\deg (C) < m$, we have because of (2.4) for $n \to \infty$

$$o(n) = \sum_{i=1}^{n} e(CM^{-1}a_{i})$$
$$= \sum_{i=1}^{n} e(CM^{-1}[a_{i}])e(CM^{-1}((a_{i})))$$
$$= \sum_{i=1}^{n} e(CM^{-1}[a_{i}])$$

since $\deg ((CM^{-1}((a_{i})))) \leq -2$ and therefore $e(CM^{-1}((a_{i}))) = 1$. By theorem (2.1) this implies that the sequence $\{[a_{t}]\}$ is uniformly distributed (mod $M$) in $\Phi$. This completes the proof.

Corollary (2.4). If $\{A_t\}$ is a sequence of elements of $\Phi$ and if for every irrational $\xi \in \Phi'$ the sequence $\{[A_{t}\xi]\}$ is uniformly distributed in $\Phi$, then the sequence $\{A_{t}\xi\}$ is uniformly distributed (mod 1) in $\Phi'$ for every irrational $\xi \in \Phi'$. The converse also holds.

Proof. Let $\xi \in \Phi'$ be irrational and let $0 \neq C \in \Phi$ be arbitrary. If $M$ is any polynomial in $\Phi$ such that $\deg (C) < \deg (M)$, then $\xi M$ is an irrational element of $\Phi'$ and for $n \to \infty$

$$o(n) = \sum_{i=1}^{n} e(CM^{-1}[A_{i}\xi M])$$
$$= \sum_{i=1}^{n} e(CA_{i}\xi).$$

Hence (2.4) holds and the sequence $\{A_{t}\xi\}$ is uniformly distributed (mod 1) in $\Phi'$. The converse follows from corollary (2.3). This completes the proof.

3. Some uniformly distributed sequences

Let $\tau$ be a one-to-one correspondence between $GF(q)$ and the set
\{0, 1, 2, \ldots, q-1\} such that \(\tau(0)=0\). We extend the domain and range of \(\tau\) to \(\Phi\) and the set of nonnegative integers \(I\) by defining \(\tau(a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0) = \tau(a_n) q^n + \tau(a_{n-1}) q^{n-1} + \ldots + \tau(a_1) q + \tau(a_0)\). We observe that now \(\tau\) is a one-to-one correspondence between \(\Phi\) and \(I\).

The sequence \(\Gamma = \{Z_i\}_{i=1}^\infty\) where \(Z_i = \tau^{-1}(i-1)\) consists of all elements of \(\Phi\), all occurring exactly once and is rising (a sequence \(\sigma = \{A_i\}\) is called rising if \(n > m\) implies \(\deg(A_n) \geq \deg(A_m)\)). J. H. Hodges ([2], pp. 62, 63) showed that \(\Gamma\) is uniformly distributed in \(\Phi\). H. G. Meijer and A. Dijkstra ([4]) proved in a direct but rather elaborate way that the sequence \(\{Z_i\}\) is uniformly distributed (mod 1) in \(\Phi\) if and only if \(\alpha\) is an irrational element of \(\Phi\). They also showed that the sequence \(\{[Z_i]\}\) is uniformly distributed in \(\Phi\) if and only if either \(\alpha\) is irrational or \(\alpha\) is rational with \(\alpha \neq 0\) and \(\deg(\alpha) \leq 0\). These results are contained in the more general theorems (3.3) and (3.4).

We first prove some rather useful inequalities.

**Lemma (3.1).** Let \(\alpha\) be an element of \(\Phi\) such that \(\deg((\alpha)) = -t > -\infty\) \((t \geq 1)\), then

\begin{equation}
|\sum_{i=1}^{n} e(Z_i \alpha)| < q^t, \text{ where } Z_i = \tau^{-1}(i-1).
\end{equation}

**Proof.** This lemma is a consequence of property (2.3). If \(n \leq q^t\) the inequality is trivial. We therefore suppose \(n > q^t\) and set

\[n = a_k q^k + a_{k-1} q^{k-1} + \ldots + a_1 q + a_0\]

\((0 < a_k \leq q-1; \quad 0 \leq a_i \leq q-1, \quad i = 0, 1, \ldots, k-1)\).

Suppose \(c \in GF(q)\) such that \(\tau(c) \leq a_k - 1\). Then the sum

\[\sum_{A \in \Phi \atop \deg(A) < k} e((cx^k + A)\alpha)\]

vanishes. Hence the only contribution to the sum in (3.1) comes from those \(Z_i\) for which \(a_k q^k + 1 \leq i \leq n\). We set \(c_k = \tau^{-1}(a_k)\). If \(a_k-1 \neq 0\), let \(c \in GF(q)\) be such that \(\tau(c) \leq a_k - 1\). Then also the sum

\[\sum_{A \in \Phi \atop \deg(A) < k-1} e((cx^k + cx^{k-1} + A)\alpha)\]

vanishes. Consequently we have that the only contribution to the sum in (3.1) comes from those \(Z_i\) for which \(a_k q^k + a_{k-1} q^{k-1} + 1 \leq i \leq n\). If \(a_k-1 = 0\) the last remark is trivial. Fix \(c_{k-1}\) such that \(\tau(c_{k-1}) = a_k-1\). We may continue this way until we have fixed \(c_t \in GF(q)\) such that \(\tau(c_t) = a_t\). Before that the sum sofar equals zero, while now we only have to sum over those polynomials \(Z_i\) with \(a_k q^k + \ldots + a_1 q + a_0 \leq i \leq n\), i.e., over but \(a_{t-1} q^{t-1} + \ldots + a_0 (< q^t)\) polynomials. Therefore the inequality (3.1) holds. This completes the proof.

A generalization of (3.1) is given by the following lemma.
Lemma (3.2). Let $\theta = \{A_i\}$ be a sequence of elements of $\Phi$. Let $a_1$ be the number of elements $A_1, ..., A_i$ such that $\{\tau(A_1), ..., \tau(A_i)\}$ is a strictly increasing sequence of consecutive integers. Suppose $a_1, a_2, ..., a_j$ are determined; let $a_j$ be the number of elements $A_{j+1}, A_{j+2}, ..., A_{k}$ such that $\{\tau(A_{j+1}), \tau(A_{j+2}), ..., \tau(A_k)\}$ is a strictly increasing sequence of consecutive integers ($i_0 = 0$). Let $n = \sum_{j=1}^{k} a_j + m$ with $0 \leq m \leq a_{j+1} - 1$.

Then for any $\alpha \in \Phi'$ with deg $(((\alpha))) = -t > -\infty$ ($t \geq 1$) we have

$$
(3.2) \quad | \sum_{i=1}^{n} e(\alpha A_i) | \leq (2k + 2)q^t.
$$

Proof. \quad \begin{align*}
| \sum_{i=1}^{n} e(\alpha A_i) | & = \left| \sum_{j=1}^{k} \sum_{i=i_j-1+1}^{i_j} e(\alpha A_i) + \sum_{i=i_{j+1}+1}^{i_{j+1}+m} e(\alpha A_i) \right| \\
& \leq \sum_{j=1}^{k} \left[ \left| \sum_{i=i_j-1+1}^{i_j} e(\alpha Z_i) \right| + \left| \sum_{i=i_{j+1}+1}^{i_{j+1}+m} e(\alpha Z_i) \right| \right] \\
& \leq (2k + 2)q^t.
\end{align*}

The last inequality follows from lemma (3.1). This completes the proof.

We observe that lemma (3.2) implies that $| \sum_{i=2}^{r} e(\alpha Z_i) | \leq 2q^t$ where deg $(((\alpha))) = -t > -\infty$ ($t \geq 1$), for here we have that $k = 0$, $a_1 = \infty$ and $n = m = r - s + 1$.

We indicate two possible conditions on the sequence $\{a_j\}_{j=1}$ of integers, defined in lemma (3.2) which we need for the next theorems.

(i) There exists a $j$ such that $a_j = \infty$.

(ii) All $a_j$'s are finite and $k^{-1} \sum_{j=1}^{k} a_j$ tends to infinity as $k$ approaches infinity.

Theorem (3.3). Let $\theta = \{A_i\}$ be a sequence of elements of $\Phi$. Suppose there exists a sequence of integers $\{a_j\}_{j=1}$ defined as in lemma (3.2) such that one of the conditions (i) and (ii) holds, then the sequence $\{A_i\alpha\}$ with $\alpha \in \Phi'$ is uniformly distributed (mod 1) in $\Phi'$ if and only if $\alpha$ is irrational.

Proof. If $\alpha$ is irrational, then so is $A \alpha$ for all $A \in \Phi$ with $A \neq 0$. Then (2.4) follows easily from (3.2). Conversely, suppose $\alpha = AB^{-1}$ for some $A$ and $B \neq 0$ in $\Phi$. Then

$$
\sum_{i=1}^{n} e(RA \alpha) = \sum_{i=1}^{n} e(A_i A) = n.
$$

25 Indagationes
Therefore the sequence \( \{A_iA^{-1}\} \) is not uniformly distributed (mod 1) in \( \Phi' \). This completes the proof.

**Theorem (3.4).** Let \( \theta = \{A_i\} \) be a sequence of elements of \( \Phi \). Suppose there exists a sequence of integers \( \{a_j\}_{j=1}^n \) defined as in lemma (3.2) such that one of the conditions (i) and (ii) holds. Then the sequence \( \{[A_i\alpha]\} \) with \( \alpha \in \Phi' \) is uniformly distributed in \( \Phi \) if and only if one of the following conditions on \( \alpha \) holds.

1. \( \alpha \) is irrational
2. \( \alpha \) is rational, \( \alpha \neq 0 \), and \( \deg (\alpha) \leq 0 \).

**Proof.** If \( \alpha \) is irrational then theorem (3.3) and corollary (2.3) imply the uniform distributivity of \( \{[A_i\alpha]\} \). Let \( \alpha = AB^{-1} \) with \( 0 \leq \deg (A) \leq \deg (B) \), let \( C \) and \( M \) be any two polynomials in \( \Phi \) such that \( 0 \leq \deg (C) \leq \deg (M) \), and set \( \deg (CM^{-1}AB^{-1}) = \deg (((CM^{-1}AB^{-1}))) = -t \). Then \( 1 \leq t < \infty \) and \( e(CM^{-1}[A_iAB^{-1}]) = e(CM^{-1}A_iAB^{-1}) \) for all \( i \), as

\[ \deg (CM^{-1}((A_iAB^{-1}))) \leq -2. \]

If condition (i) holds and \( n = \sum_{i=1}^{j-1} a_i + m \) with \( 0 \leq m < \infty \), then lemma (3.2) implies that

\[ |\sum_{i=1}^{n} e(CM^{-1}[A_iAB^{-1}])| \leq |\sum_{i=1}^{j-1} a_i + 2q^t|. \]

Consequently we have that

\[ |n^{-1} \sum_{i=1}^{n} e(CM^{-1}[A_iAB^{-1}])| \leq m^{-1} (\sum_{i=1}^{j-1} a_i + 2q^t) = o(n) \quad (n \to \infty). \]

If condition (ii) holds and \( n = \sum_{i=1}^{k} a_i + m \) with \( 0 \leq m \leq a_{k+1} - 1 \), then lemma (3.2) implies that

\[ |n^{-1} \sum_{i=1}^{n} e(CM^{-1}[A_iAB])| \leq (2k+2)q^t|\sum_{i=1}^{k} a_i| = o(n), \quad (n \to \infty). \]

Hence both inequalities (3.3) and (3.4) imply the uniform distributivity of the sequence \( \{[A_iAB^{-1}]\} \) where \( 0 \leq \deg (A) \leq \deg (B) \).

Conversely, suppose \( \alpha = AB^{-1} \) with \( \deg (A) > \deg (B) \geq 0 \). Then taking in (2.5) \( M = A \) and \( C = B \), we have

\[ \sum_{i=1}^{n} e(BA^{-1}[A_iAB^{-1}]) = \sum_{i=1}^{n} e(A_i) = n. \]

Hence \( \{[A_iAB^{-1}]\} \) is not uniformly distributed (mod \( A \)) in \( \Phi \). Finally the case \( \alpha = 0 \) is trivial. This completes the proof.

Many examples of uniformly distributed sequences can now be given. For instance if \( \theta = \{A_i\} \) satisfies one of the conditions (i) and (ii) then \( \theta \) itself is uniformly distributed in \( \Phi \) (set \( \alpha \) in theorem (3.4) equal to 1).
Hence the subsequence of \( \{\tau^{-1}(i-1)\} \) consisting of all polynomials of even degree and the sequence
\[
\{\tau^{-1}(1), \tau^{-1}(3), \tau^{-1}(4), \ldots, \tau^{-1}(n^2-n+1), \tau^{-1}(n^2-n+2), \ldots, \tau^{-1}(n^2-1), -1(n^2), \ldots\}
\]
are uniformly distributed in \( \Phi \). The conditions (i) and (ii) are, of course, not necessary for the uniform distributivity of \( \theta \). For, if
\[
\theta = \{0, 0, \tau^{-1}(1), \tau^{-1}(1), \ldots, \tau^{-1}(i-1), \tau^{-1}(i-1), \ldots\},
\]
then we can show that \( \theta \) is uniformly distributed in \( \Phi \): Let \( C, M \in \Phi \) be such that \( 0 \leq \deg (C) < \deg (M) = m \) and let \( 2l \leq n < 2l+2 \), then
\[
(2l+2)^{-1}2^l(I, C, M) \leq n^{-1}\theta(n, C, M) \leq (2l)^{-1}2^l(l+1, C, M)
\]
where \( I = \{\tau^{-1}(i-1)\} \). Since \( I \) is uniformly distributed in \( \Phi \) we have
\[
\lim_{n \to \infty} n^{-1}\theta(n, C, M) = q^{-m}.
\]
Now, in the notation of lemma (3.2), \( a_1 = 1 \) and \( a_j = 1 \) or 2 as \( j \geq 2 \). Thus \( 1 \leq k^{-1} \sum_{j=1}^{k} a_j < 2 \) for all \( k \). Hence while neither condition (i) nor condition (ii) is satisfied, the sequence \( \theta \) is uniformly distributed in \( \Phi \).

It is interesting to note, that under the conditions stated the sequence \( \{\tau(A_i)\} \) is uniformly distributed in \( I \) ([5]). This is easily proved if we use the Weyl criterion for uniform distribution of sequences in \( I \) given by S. Uchiyama ([7]). Theorem (3.4) thus provides a large class of sequences \( \{A_i\} \) of elements of \( \Phi \) which are uniformly distributed in \( \Phi \), whose corresponding sequences \( \{\tau(A_i)\} \) of elements in \( I \) are uniformly distributed in \( I \).

University of Technology, Delft

REFERENCES