Uniform Distribution Theory **3** (2008), no.1, 85–91

uniform distribution theory

# ON THE DISTRIBUTION OF RATIONAL FUNCTIONS ON CONSECUTIVE POWERS

Jaime Gutierrez* — Igor E. Shparlinski**

ABSTRACT. We show that for a prime $p$ and any nontrivial rational function $r(X) \in \mathbb{F}_p(X)$ over the finite field $\mathbb{F}_p$ of $p$ elements, the fractional parts

$$\left\{ \frac{r(x)}{p}, \dots, \frac{r(x^m)}{p} \right\},$$

where $x$ runs through the fields elements which are not the poles of the above functions, are asymptotically uniformly distributed in the $m$-dimensional unit cube for any fixed $m$ and $p \to \infty$.

*Communicated by Henri Faure*

## 1. Introduction

Let $p$ be a prime number and let $\mathbb{F}_p$ be the finite field of $p$ elements. Assume that $\mathbb{F}_p$ is represented by the set $\{0, 1, \dots, p-1\}$.

For an integer $m$ and any rational function $r(X) \in \mathbb{F}_p(X)$ we denote by $\mathcal{E}_m$ the set of poles of the following $m$ functions $r(X), \dots, r(X^m)$.

We use exponential sums to show that the fractional parts

$$\left\{ \frac{r(x)}{p}, \dots, \frac{r(x^m)}{p} \right\}, \quad x \in \{0, \dots, N-1\} \setminus \mathcal{E}_m, \tag{1}$$

are asymptotically uniformly distributed in the $m$-dimensional unit cube for any fixed $m$, and integer $N$ with $Np^{-1/2}(\log p)^{-m-1} \to \infty$ as $p \to \infty$.

---

2000 Mathematics Subject Classification: Primary 11K31, Secondary 11K36, 11L07.
Keywords: Rational functions, exponential sums.
*Partially supported by Spain Ministry of Education and Science Grant MTM2007-67088.
**Partially supported by Australia Research Council Grant DP0556431.

Certainly, a result of this type is expected, but its proof requires a result about linear independency of certain rational functions which can have an independent interest.

Throughout the paper, the involved constants in symbols '$O$' and '$\ll$' may depend on $m$ and the degree of the function $r(X)$ (we recall that $A \ll B$ is equivalent to $A = O(B)$).

## 2. Linear independence of rational functions on consecutive powers

Since the following statement may find some other applications we formulate it in a more general form than it is necessary for our purpose.

**Lemma 1.** *Let $\mathbb{K}$ be an arbitrary field. Assume that a rational function $r(X) \in \mathbb{K}(X)$ is not of the form $r(X) = AX + B$ with $A, B \in \mathbb{K}$. Then, the following $m + 2$ rational functions*

$$1,\ X,\ r(X^i),\ \ i = 1, \dots, m,$$

*are linearly independent.*

Proof. The result is trivial when $r(X) \in \mathbb{K}[X]$, that is, if it is a polynomial.

We now assume that $r(X) \notin \mathbb{K}[X]$. Suppose that for some $a_i \in \mathbb{K}$, $i = -1, 0, 1, \dots, m$ we have

$$a_{-1} + a_0 X + \sum_{i=1}^{m} a_i r(X^i) = 0. \tag{2}$$

As usual, we define the degree of the identically zero polynomial as $-1$, and the degree of any other constant polynomial as 0.

We write

$$r(X) = h(X) + \frac{f(X)}{g(X)},$$

where $f(X), g(X), h(X) \in \mathbb{K}[X]$, $\deg g(X) > \deg f(X) \geq 0$ (since $r(X) \notin \mathbb{K}[X]$). We see from (2) that

$$a_{-1} + a_0 X + \sum_{i=1}^{m} a_i h\left(X^i\right) + \sum_{i=1}^{m} a_i \frac{f\left(X^i\right)}{g\left(X^i\right)} = 0.$$

This implies

$$-a_{-1} - a_0 X - \sum_{i=1}^{m} a_i h\left(X^i\right) = \sum_{i=1}^{m} a_i \frac{f\left(X^i\right)}{g\left(X^i\right)},$$

from which we obtain:

$$-\left(a_{-1} + a_0 X + \sum_{i=1}^{m} a_i h\left(X^i\right)\right) \prod_{j=1}^{m} g\left(X^j\right) = \sum_{i=1}^{m} a_i f\left(X^i\right) \prod_{\substack{j=1 \\ j \neq i}}^{m} g\left(X^j\right). \qquad (3)$$

Clearly,

$$\deg\left(f\left(X^i\right) \prod_{\substack{j=1 \\ j \neq i}}^{m} g\left(X^j\right)\right) = i \deg f(X) + \left(\frac{m(m+1)}{2} - i\right) \deg g(X). \qquad (4)$$

Now, if

$$a_{-1} + a_0 X + \sum_{i=1}^{m} a_i h\left(X^i\right) \neq 0$$

(that is, if it is a non-zero polynomial), then the degree of the polynomial on the left hand side of (3) is at least

$$\sum_{j=1}^{m} j \deg g(X) = \frac{m(m+1)}{2} \deg g(X),$$

which contradicts the fact that, by (4), the degree of the polynomial on the right hand side of (3) is

$$\max_{i=1,\ldots,m} \left(i \deg f(X) + \left(\frac{m(m+1)}{2} - i\right) \deg g(X)\right) < \frac{m(m+1)}{2} \deg g(X).$$

If

$$a_{-1} + a_0 X + \sum_{i=1}^{m} a_i h\left(X^i\right) = 0 \qquad (5)$$

(that is, if it is a zero polynomial), then

$$\sum_{i=1}^{m} a_i f(X^i) \prod_{\substack{j=1 \\ j \neq i}}^{m} g(X^j) = 0.$$

Recalling that $\deg g(X) > \deg f(X) \geq 0$, we now derive from (4) that

$$\begin{aligned}\deg\left( f\left(X^i\right) \prod_{\substack{j=1\\ j\neq i}}^{m} g\left(X^j\right)\right) &= i \deg f(X) + \left(\frac{m(m+1)}{2} - i\right) \deg g(X)\\ &> (i+1) \deg f(X) + \left(\frac{m(m+1)}{2} - i - 1\right) \deg g(X)\\ &= \deg\left( f\left(X^{i+1}\right) \prod_{\substack{j=1\\ j\neq i+1}}^{m} g\left(X^j\right)\right),\end{aligned}$$

for all $i = 1, \ldots, m$. It implies that $a_i = 0$, for all $i = 1, \ldots, m$. Then, from (5) we obtain $a_{-1} = a_0 = 0$, and this ends the proof. □

## 3. Discrepancy and exponential sums

For a sequence of $N$ points

$$\Gamma = (\gamma_{1,n}, \ldots, \gamma_{m,n})_{n=1}^{N} \tag{6}$$

in the half-open interval $[0,1)^m$, denote by $\Delta_\Gamma$ its *discrepancy*, that is,

$$\Delta_\Gamma = \sup_{\mathcal{B}\subseteq[0,1)^m} \left| \frac{T_\Gamma(\mathcal{B})}{N} - |\mathcal{B}| \right|,$$

where $T_\Gamma(B)$ is the number of points of the sequence $\Gamma$ lying in the box

$$\mathcal{B} = [\alpha_1, \beta_1) \times \ldots \times [\alpha_m, \beta_m) \subseteq [0,1)^m$$

of volume

$$|\mathcal{B}| = \prod_{j=1}^{m} (\beta_j - \alpha_j),$$

where $0 \leq \alpha_j < \beta_j \leq 1$, $j = 1, \ldots, m$, and the supremum is taken over all such boxes.

For an integer vector $\mathbf{a} = (a_1, \ldots, a_m) \in \mathbb{Z}^m$ we put

$$|\mathbf{a}| = \max_{i=1,\ldots,m} |a_i|, \qquad r(\mathbf{a}) = \prod_{i=1}^{m} \max\{|a_i|, 1\}. \tag{7}$$

We need the *Erdös–Turán–Koksma inequality* (see [1, Theorem 1.21]), linking the discrepancy with exponential sums, which we present in the following form.

**Lemma 2.** *There exists a constant $C_m > 0$ depending only on the dimension $m$ such that, for any integer $L \ge 1$, for the discrepancy of a sequence of points (6) the bound*

$$\Delta_\Gamma < C_m \left( \frac{1}{L} + \frac{1}{N} \sum_{0<|\mathbf{a}|\le L} \frac{1}{r(\mathbf{a})} \left| \sum_{n=1}^{N} \exp\left( 2\pi i \sum_{j=1}^{m} a_j \gamma_{j,n} \right) \right| \right)$$

*holds, where $|\mathbf{a}|$, $r(\mathbf{a})$ are defined by (7) and the sum is taken over all integer vectors*

$$\mathbf{a} = (a_1, \ldots, a_m) \in \mathbb{Z}^m \quad with \quad 0 < |\mathbf{a}| \le L.$$

We put

$$\mathbf{e}_p(z) = \exp(2\pi i z/p).$$

Our second main tool is the Weil bound on exponential sums (see [3, Chapter 6] or [4, Chapter 5]) which we present in the following form which can be found in [5].

**Lemma 3.** *For any polynomials $g(X), h(X) \in \mathbb{F}_p[X]$ such that the rational function $F(X) = h(X)/g(X)$ is not constant on $\mathbb{F}_p$, the bound*

$$\left| \sum_{\substack{x \in \mathbb{F}_p \\ g(x) \ne 0}} \mathbf{e}_p\left(F(x)\right) \right| \le \left(\max\{\deg g,\, \deg h\} + r - 2\right) p^{1/2} + \delta$$

*holds, where*

$$(r, \delta) = \begin{cases} (s, 1) & \text{if } \deg h \le \deg g, \\ (s+1, 0) & \text{if } \deg h > \deg g, \end{cases}$$

*and $s$ is the number of distinct zeros of $g(X)$ in the algebraic closure of $\mathbb{F}_p$.*

## 4. Main result

Recall that we have assumed that the elements of the field $\mathbb{F}_p$ are represented by the set $\{0, 1, \ldots, p-1\}$. For a rational function $r(X) \in \mathbb{F}_p(X)$ and a positive integer $N < p$, we denote by $\Delta_{r,m}(N, p)$ the discrepancy of the points set (1).

**Theorem 4.** *Assume that a rational function $r(X) \in \mathbb{F}_p(X)$ is not of the form $r(X) = AX + B$ with $A, B \in \mathbb{F}_p$. Then, for any positive integer $N < p$, we have*

$$\Delta_{r,m}(N,p) = O\left(N^{-1}p^{1/2}(\log p)^{m+1}\right).$$

P r o o f. We can certainly assume that $p \geq 3$ since otherwise the result is trivial. Combining Lemmas 1 and 3 we conclude that for any $a_0, a_1, \dots, a_m \in \mathbb{F}_p$, not all equal to zero, we have

$$\sum_{\substack{x=0 \\ x \notin \mathcal{E}_m}}^{p-1} \mathbf{e}_p\left(a_0 x + \sum_{j=1}^{m} a_j r(x^j)\right) = O(p^{1/2}),$$

where, as before, $\mathcal{E}_m$ denotes the set of poles of the functions $r(X), \dots, r(X^m)$.

Using the standard reduction between complete and incomplete sums, see [2, Section 12.2], we derive

$$\sum_{\substack{x=0 \\ x \notin \mathcal{E}_m}}^{N} \mathbf{e}_p\left(\sum_{j=1}^{m} a_j r(x^j)\right) = O(p^{1/2} \log p),$$

provided that at least one coefficient $a_1, \dots, a_m \in \mathbb{Z}$ is not zero modulo $p$. Now, combining this bound with Lemma 2 and taking $L = (p-1)/2$ end the proof. □

## 5. Comments

Let $\mathbb{K}$ be an arbitrary field. Lemma 1 can be extended in the following way.

Assume that a rational function $r(X) \in \mathbb{K}(X)$ is not of the form $r(X) = AX + B$ with $A, B \in \mathbb{K}$ and a rational function $w(X) \in \mathbb{K}(X)$ is not constant. Then, the following $m+2$ rational functions

$$1,\ X,\ r\left(w(X)^i\right),\ i = 1, \dots, m,$$

are linearly independent.

Let $w(X), u(X)$ be two non-constant rational functions. As usual, we denote by $w(X) \circ u(X)$ the element-wise composition of rational functions, that is, $w(X) \circ u(X) = w(u(X))$. For a positive integer number $i$, we write

$$w_i(X) = \overbrace{w(X) \circ \ldots \circ w(X)}^{i \text{ times}}.$$

Now, assume that two rational functions $r(X), w(X) \in \mathbb{K}(X)$ are not of the form $AX + B$ with $A, B \in \mathbb{F}_p$. Then, the following $m+2$ rational functions

$$1,\ X,\ r\left(w_i(X)\right),\ i = 1, \ldots, m,$$

are linearly independent. Accordingly, one can obtain an analogue of Theorem 4 for the discrepancy of the joint distribution of fractional parts with these functions.

**Acknowledgement.** The authors are grateful to the referee for the very careful reading and many useful suggestions.

## REFERENCES

[1] DRMOTA, M. – TICHY, R.F.: *Sequences, Discrepancies and Applications*, Lecture Notes in Mathematics **1651**, Springer–Verlag, Berlin, Heidelberg, 1997.
[2] IWANIEC, H.– KOWALSKI, E.: *Analytic Number Theory*, Colloq. Publ. Amer. Math. Soc. Vol. **53**, Amer. Math. Soc., Providence, RI, 2004.
[3] LI, W.– C.W.: *Number Theory with Applications*, World Scientific, Singapore, 1996.
[4] LIDL, R.–NIEDERREITER, H.: *Finite Fields* (FWD by P. M. Cohn) Encyclopedia of Mathematics and its Applications **20**, Second edition, Cambridge University Press, Cambridge, 1997 (MR1429394(97i:11115)).
[5] MORENO, C. J. – O. MORENO, O.: *Exponential sums and Goppa codes, I,* Proc. Amer. Math. Soc. **111** (1991), no. 2, 523–531.

Received June 6, 2008
Accepted October 10, 2008

**Jaime Gutierrez**
*Department of Applied Mathematics and Computer Science*
*University of Cantabria*
*E-39071 Santander*
*SPAIN*
*E-mail*: jaime.gutierrez@unican.es

**Igor E. Shparlinski**
*Department of Computing*
*Macquarie University*
*Sydney, NSW 2109*
*AUSTRALIA*
*E-mail*: igor@comp.mq.edu.au