Uniform Distribution Theory **8** (2013), no.1, 67–72

uniform distribution theory

JOINT DISTRIBUTION OF DISCRETE LOGARITHMS

Igor E. Shparlinski

Abstract. We improve a recent result by D. J. Gibson on the joint distribution of discrete logarithms modulo a prime p of integers $x_1, \ldots, x_r$ that run independently through short arithmetic progressions. This improvement is based on an alternative approach, which makes use of bounds of multiplicative character sums.

Communicated by Sergei Konyagin

1. Introduction

Let g be a fixed primitive root modulo a prime p. As usual, for an integer x with $\gcd(x,p)=1$ we define the discrete logarithm $\operatorname{ind} x$ by the conditions

$$g^{\operatorname{ind} x} \equiv x \pmod p \qquad \text{and} \qquad 0 \leqslant \operatorname{ind} x < p-1.$$

We also set $\operatorname{ind} x = p-1$ if $p \mid x$. The question of distribution of values of $\operatorname{ind} x$ has a long history that dates back to early works of Vinogradov [11]. Recently, Gibson [2] considered the join distribution of the points

$$\left(\frac{\operatorname{ind} x_1}{p-1}, \ldots, \frac{\operatorname{ind} x_r}{p-1}\right), \quad x_1 \in \mathcal{I}_1, \ldots, x_r \in \mathcal{I}_r, \tag{1}$$

in the r-dimensional unit cube $\mathbb{U}^r$, where the variables $x_1, \ldots, x_r$ run independently trough N-term arithmetic progressions of the form

$$\mathcal{I}_j = \{h_j + k_j n \ : \ n = 1, \ldots, N\}, \tag{2}$$

with some integers h_j and k_j, $\gcd(k_j,p)=1$, $j=1,\ldots,r$. Note that in [2] only the case of equal progressions $\mathcal{I}_1 = \ldots = \mathcal{I}_r$ is considered, but the extension of the method and the result to the general case is immediate. In particular, it is

2010 Mathematics Subject Classification: 11B50, 11L40.
Keywords: Discrete logarithm, joint distribution, character sums.

shown in [2, Theorem 1] that for a very wide class of domains $\Omega \subseteq \mathbb{U}^r$, including all convex domains, the number $T(\mathcal{I}_1, \ldots, \mathcal{I}_r, \Omega)$ of points (1) that fall inside of Ω satisfies the bound

$$T(\mathcal{I}_1, \ldots, \mathcal{I}_r, \Omega) = \mu(\Omega) N^r + O(N^{r-1} p^{1-1/2r} (\log p)^2),$$

where μ is the Lebesgue measure on $\mathbb{U}^r$. Note that the result of [2] is slightly more precise, but the difference is essential only for N that is close to the threshold $p^{1-1/2r}$ when it becomes trivial.

Gibson [2] uses bounds of exponential sums.

Here we show that using multiplicative character sums one almost instantly obtains a stronger result which is nontrivial in a much wide region.

Theorem 1. *For any r arithmetic progressions* (2) *with* $\gcd(k_j, p) = 1$, $j = 1, \ldots, r$, *of length $N < p$ and any domain $\Omega \subseteq \mathbb{U}^r$ whose surface is a manifold of dimension $r - 1$, we have*

$$T(\mathcal{I}_1, \ldots, \mathcal{I}_r, \Omega) = \mu(\Omega) N^r + O\left(N^{r-1/r\nu} p^{(\nu+1)/4r\nu^2 + o(1)}\right),$$

where ν is an arbitrary fixed positive integer and the implied constant depends only on r, ν and the size of the surface of Ω.

Clearly for any fixed $\varepsilon > 0$, Theorem 1, is nontrivial for $N > p^{1/4+\varepsilon}$ (rather than $N > p^{1-1/2r+\varepsilon}$ as in [2]) provided that p is large enough. The same approach (with only small notational changes) also works for the joint distribution of r discrete logarithms taken to r distinct bases.

2. Background on the Theory of Uniform Distribution

Given a sequence Γ of M points

$$\Gamma = \{(\gamma_{m,1}, \ldots, \gamma_{m,r})\}_{m=0}^{M-1}, \tag{3}$$

in $\mathbb{U}^r$, we define its *discrepancy with respect to a domain* $\Omega \subseteq \mathbb{U}^r$ as

$$\Delta(\Gamma, \Omega) = \left| \frac{\# N(\Omega)}{M} - \mu(\Omega) \right|,$$

where, as before, μ is the Lebesgue measure on $\mathbb{U}^r$ where $N(\Omega)$ is the number of points (3) inside Ω.

We now define the *discrepancy* of Γ as

$$D(\Gamma) = \sup_{\Pi \subseteq \mathbb{U}^r} \Delta(\Gamma, \Pi),$$

where the supremum is taken over all boxes

$$\varPi = [\alpha_1, \beta_1) \times \ldots \times [\alpha_r, \beta_r) \subseteq \mathbb{U}^r.$$

Typically the bounds on the discrepancy of a sequence are derived from bounds of exponential sums with elements of this sequence. The relation is made explicit in the celebrated *Koksma–Szüsz inequality*, see [1, Theorem 1.21], which we present in the following form.

Lemma 2. *Suppose that for the sequence of points* (3) *for some integer* $L \geqslant 1$ *and the real number* S *we have*

$$\left| \sum_{m=0}^{M-1} \exp\left(2\pi i \sum_{j=1}^{r} a_j \gamma_{m,j}\right) \right| \leqslant S,$$

for all integers $-L \leqslant a_j \leqslant L$, $j = 1, \ldots, r$, *not all equal to zero. Then,*

$$D(\Gamma) \ll \frac{1}{L} + \frac{(\log L)^r}{M} S,$$

where the implied constant depends only on r.

As usual, we define the distance between a vector $\mathbf{u} \in \mathbb{U}^r$ and a set $\Omega \subseteq \mathbb{U}^r$ by

$$\operatorname{dist}(\mathbf{u}, \Omega) = \inf_{\mathbf{w} \in \Omega} \|\mathbf{u} - \mathbf{w}\|,$$

where $\|\mathbf{v}\|$ denotes the Euclidean norm of $\mathbf{v}$. Given $\varepsilon > 0$ and a domain $\Omega \subseteq \mathbb{U}^r$ we define the sets

$$\Omega_\varepsilon^+ = \{\mathbf{u} \in \mathbb{U}^r \backslash \Omega \ : \ \operatorname{dist}(\mathbf{u}, \Omega) < \varepsilon\}$$

and

$$\Omega_\varepsilon^- = \{\mathbf{u} \in \Omega \ : \ \operatorname{dist}(\mathbf{u}, \mathbb{U}^r \backslash \Omega) < \varepsilon\}.$$

Let $h(\varepsilon)$ be an arbitrary increasing function defined for $\varepsilon > 0$ and such that

$$\lim_{\varepsilon \to 0} h(\varepsilon) = 0.$$

As in [7, 8], we define the class Σ_h of domains $\Omega \subseteq \mathbb{U}^r$ for which

$$\mu\left(\Omega_\varepsilon^+\right) \leqslant h(\varepsilon) \qquad \text{and} \qquad \mu\left(\Omega_\varepsilon^-\right) \leqslant h(\varepsilon)$$

for any $\varepsilon > 0$.

A relation between $D(\Gamma)$ and $\varDelta(\Gamma, \Omega)$ for $\Omega \in \Sigma_h$ is given by the following inequality of [7] (see also [8]).

Lemma 3. *For any domain* $\Omega \in \Sigma_h$, *we have*

$$\varDelta(\Gamma, \Omega) \ll h\left(r^{1/2} D(\Gamma)^{1/r}\right).$$

Finally, the following bound, which is a special case of a more general result of H. Weyl [12] shows that if the boundary of Ω is a manifold then $\Omega \in \Sigma_h$ for some linear function $h(\varepsilon) = C\varepsilon$.

Lemma 4. *If the surface of Ω is a manifold of dimension $r-1$,*

$$\mu\left(\Omega_\varepsilon^{\pm}\right) = O(\varepsilon),$$

where the implied constant depends only on the size of the surface of Ω.

Remark 5. *It is easy to see that for convex domains Ω, the implied constant in Lemma 4 depends only on r.*

3. Background on the Multiplicative Characters

We recall that the set of functions

$$\chi_a(z) = \exp\left(2\pi i a \frac{\operatorname{ind} z}{p-1}\right), \quad a = 0, \ldots, p-2, \tag{4}$$

form the set of multiplicative characters on modulo p (where we also set $\chi_a(0) = 0$).

Our main tool is the following combination of the Pólya-Vinogradov (for $\nu = 1$) and Burgess (for $\nu \geqslant 2$) bounds, see [4, Theorems 12.5 and 12.6].

Lemma 6. *For arbitrary integers W and Z with $1 \leqslant Z \leqslant p$, the bound*

$$\max_{a=1,\ldots,p-2} \left| \sum_{z=W+1}^{W+Z} \chi_a(z) \right| \leqslant Z^{1-1/\nu} p^{(\nu+1)/4\nu^2 + o(1)}$$

holds with any fixed positive integer ν.

4. Proof of Theorem 1

Using (4), we derive that for any integers $-p+2 \leqslant a_j \leqslant p-2$, $j = 1, \ldots, r$, we have

$$\begin{aligned}
&\sum_{x_1 \in \mathcal{I}_1} \ldots \sum_{x_r \in \mathcal{I}_r} \exp\left(2\pi i \frac{1}{p-1} \sum_{j=1}^{r} a_j \operatorname{ind} x_j\right) \\
&\qquad = \sum_{x_1 \in \mathcal{I}_1} \ldots \sum_{x_r \in \mathcal{I}_r} \chi_{a_1}(x_1) \ldots \chi_{a_r}(x_r) = \prod_{j=1}^{r} \sum_{x_j \in \mathcal{I}_j} \chi_{a_j}(x_j) \\
&\qquad = \prod_{j=1}^{r} \sum_{n_j=1}^{N} \chi_{a_j}(h_j + k_j n_j) = \prod_{j=1}^{r} \sum_{x_j \in \mathcal{I}_j} \chi_{a_j}(x_j) \\
&\qquad = \prod_{j=1}^{r} \sum_{n_j=1}^{N} \chi_{a_j}(h_j + k_j n_j) = \prod_{j=1}^{r} \chi_{a_j}(k_j) \sum_{n_j=1}^{N} \chi_{a_j}(\ell_j + n_j),
\end{aligned}$$

where ℓ_j satisfies the congruence $k_j \ell_j \equiv h_j \pmod p$ (we recall that $\gcd(k_j, p) = 1$), $j = 1, \ldots, r$. If not all integers $a_1, \ldots, a_r$ are equal to zero, then applying Lemma 6 we immediately conclude that

$$\left| \sum_{x_1 \in \mathcal{I}_1} \ldots \sum_{x_r \in \mathcal{I}_r} \exp\left(2\pi i \frac{1}{p-1} \sum_{j=1}^{r} a_j \operatorname{ind} x_j\right) \right| \leqslant N^{r-1/\nu} p^{(\nu+1)/4\nu^2 + o(1)}$$

holds with any fixed positive integer ν. Thus, using Lemma 2 with $L = p-2$, we see that the discrepancy of the points (1) is bounded by $N^{-1/\nu} p^{(\nu+1)/4\nu^2+o(1)}$. Now, applying Lemmas 3 and 4, we conclude the proof.

5. Comments

As we see from Remark 5, for convex domains Ω, the implied constant in Theorem 1 depends only on r and ν.

It is easy to see that question of distribution of the points (1) in boxes can be reduced to r independent questions about the number of solutions to congruences of the type

$$g^y \equiv x \pmod p, \quad x \in \mathcal{I},\ y \in J,$$

where $\mathcal{I}$ is an N-term arithmetic progression and $\mathcal{J}$ is an interval of length T. This and several related questions of this kind have been considered in a number of works, see [3, 5, 6] and references therein.

Finally, we note that our result combined with classical results of Schmidt [9] in the theory of uniform distribution and some ideas of [10], can be used to derive a sharp asymptotic formula for the number of points

$$\left(\frac{\operatorname{ind} x_1}{p-1}, \ldots, \frac{\operatorname{ind} x_r}{p-1}\right), \quad (x_1, \ldots, x_r) \in \Theta,$$

that in the r-dimensional unit cube $\mathbb{U}^r$, that fall inside of Ω for two domains $\Theta, \Omega \subseteq \mathbb{U}^r$.

References

[1] M. Drmota and R. Tichy, *Sequences, discrepancies and applications*, Springer-Verlag, Berlin, 1997.
[2] D. J. Gibson, 'Discrete logarithms and their equidistribution', *Unif. Distrib. Theory*, **7** (2012), 147–154.
[3] J. Cilleruelo and M. Z. Garaev, 'Concentration of points on two and three dimensional modular hyperbolas and applications', *Geom. and Func. Anal.*, **21** (2011), 892–904.
[4] H. Iwaniec and E. Kowalski, *Analytic number theory*, Amer. Math. Soc., Providence, RI, 2004.
[5] S. V. Konyagin and I. E. Shparlinski, *Character sums with exponential functions and their applications*, Cambridge Univ. Press, Cambridge, 1999.
[6] S. V. Konyagin and I. E. Shparlinski, 'On the consecutive powers of a primitive root: Gaps and exponential sums', *Mathematika*, **58** (2012), 11–20.
[7] M. Laczkovich, 'Discrepancy estimates for sets with small boundary', *Studia Sci. Math. Hungar.*, **30** (1995), 105–109.
[8] H. Niederreiter and J. M. Wills, 'Diskrepanz und Distanz von Massen bezuglich konvexer und Jordanscher Mengen', *Math. Z.*, **144** (1975), 125–134.
[9] W. Schmidt, 'Irregularities of distribution. IX', *Acta Arith.*, **27** (1975), 385–396.
[10] I. E. Shparlinski, 'On the distribution of solutions to polynomial congruences', *Archiv Math.*, **99** (2012), 345–351 .
[11] I. M. Vinogradov, 'On the distribution of indices', *Doklady Akad. Nauk SSSR*, **20**, 73–76 (in Russian).
[12] H. Weyl, 'On the volume of tubes', *Amer. J. Math.*, **61** (1939), 461–472.

Received June 2, 2012
Accepted August 1, 2012

Department of Computing, Macquarie University, Sydney NSW 2109, Australia
E-mail: igor.shparlinski@mq.edu.au