

EXPONENTIAL SUMS
EQUIDISTRIBUTION
PSEUDORANDOMNESS

(1) Exponential sums over subgroups

General philosophy:

multiplicative subgroups are well-distributed even if they are very small

Conjecture. (M-V-W)

$$H < \mathbb{F}_p^*, \frac{|H|}{\log p} \rightarrow \infty$$

Then

$$\max_{a \in \mathbb{F}_p^*} \left| \sum_{x \in H} e_p(ax) \right| = o(|H|). \quad (0)$$

Equidistribution is known under the stronger assumption

$$\log |H| > C \frac{\log p}{\log \log p} \quad (1)$$

where $C > 1$ is some constant.

This is the strongest result obtained so far towards M-V-W.

Follows from

Theorem 1.

Let $H < \mathbb{F}_p^*$, $|H| = p^\delta$. Then

$$\max_{(a,p)=1} \left| \sum_{x \in H} e_p(ax) \right| < p^{-\delta'} |H|$$

with

$$\delta' > \exp\left(-\frac{C}{\delta}\right).$$

Problem 1. Relax condition (1).

Remark.

There is obviously a wide gap between Theorem 1 and the M-V-W conjecture. Instead of an exponential sum bound, one could consider the following property

$$\max \frac{|I|}{p} \rightarrow 0 \tag{2}$$

where the maximum is taken over all intervals $I \subset [1, p]$ such that $I \cap aH = \emptyset$ for some $a \in \mathbb{F}_p^*$ (note that (0) \Rightarrow (2)).

Again (1) is the weakest density assumption known to imply (2). On the other hand, property (2) always hold if we let H be the multiplicative group generated by two given integers $r, s \in \mathbb{Z}_+$, which are not powers of the same integer (by Furstenberg's theorem). In fact, an effective version of this principle was established in [BLMV]. Assuming $(r, s) = 1$, one has indeed for $p \rightarrow \infty$

$$\max \frac{|I|}{p} < (\log \log \log p)^{-c} \tag{3}$$

with $c > 0$ an absolute constant (same property in $(\mathbb{Z}/N\mathbb{Z})^*$ with $N \rightarrow \infty$ arbitrary, provided $(rs, N) = 1$ and $(a, N) = 1$).

Problem 2. Establish (2) under weaker assumption than (1).

Problem 3. Improve upon (3).

Theorem 1 is obtained from sum/product theory in \mathbb{F}_p . In fact, there are the following statements of more general nature and relevant to the multi-source randomness extractor issue.

Theorem 2 \Rightarrow Theorem 1

Theorem 3 gives equidistribution under optimal entropy condition on the sources.

Theorem 2.

$$0 < \delta < 1, r \in \mathbb{Z}_+, r > C\delta^{-1}$$

$A_1, \dots, A_r \subset \mathbb{F}_p$ arbitrary sets satisfying

$$|A_i| > p^\delta \quad (1 \leq i \leq r).$$

Then

$$\left| \sum_{x_1 \in A_1, \dots, x_r \in A_r} e_p(x_1 \dots x_r) \right| < p^{-\delta'} |A_1| \cdots |A_r| \quad \delta' = C^{-r}$$

Theorem 3.

$$0 < \delta < \frac{1}{4}, r \in \mathbb{Z}_+$$

$A_1, \dots, A_r \subset \mathbb{F}_p$ arbitrary sets satisfying

$$|A_i| > p^\delta \quad (1 \leq i \leq r)$$

$$\prod_{1 \leq i \leq r} |A_i| > p^{1+\delta}.$$

Then

$$\left| \sum_{x_1 \in A_1, \dots, x_r \in A_r} e_p(x_1 \dots x_r) \right| < p^{-\delta'} |A_1| \dots |A_r| \quad \delta' = \left(\frac{\delta}{r} \right)^{Cr}.$$

Theorem 2 implies also an analogue of Theorem 1 for multiplicative orbits (possibly incomplete) of an element $g \in \mathbb{F}_p^*$.

Theorem 4. Let $g \in \mathbb{F}_p^*$ and $\text{ord}_p(g) = |\langle g \rangle| = t$. Assume further

$$t \geq t_1 > p^\delta.$$

Then

$$\max_{(a,p)=1} \left| \sum_{s=1}^{t_1} e_p(ag^s) \right| < p^{-\delta'} \cdot t_1 \quad \delta' = \exp\left(-\frac{C}{\delta}\right).$$

Many applications (cf. book K-S).

Similar theory have been developed for general modulus.

In particular

Theorem 5. Assume $H < (\mathbb{Z}/q\mathbb{Z})^*$, $|H| > q^\delta$. Then

$$\max_{(a,q)=1} \left| \sum_{x \in H} e_q(ax) \right| < |H|q^{-\delta'}$$

with $\delta' = \delta'(\delta)$, independent of q .

The case of incomplete sums requires further assumptions.

Theorem 6. Given $\delta > 0$ there is $\delta' > 0$ such that if $q \in \mathbb{Z}_+$ (suff. large) and $g \in (\mathbb{Z}/q\mathbb{Z})^*$ satisfies

$$q'|q \Rightarrow \text{ord}_{q'}(g) > (q')^\delta.$$

Then

$$\max_{(\xi, q)=1} \left| \sum_{s=1}^t e_q(\xi g^s) \right| < q^{-\delta'} t \text{ for } t > q^\delta.$$

Theorem 4 was also extended to general fields.

Theorem 7. Given $\delta > 0$, there is $\delta' > 0$ such that if $q = p^m$ (suff. large) and $g \in \mathbb{F}_q^*$ of order t with

$$\max_{\substack{1 \leq \nu < m \\ \nu | m}} \gcd(t, p^\nu - 1) < q^{-\delta} t.$$

Then

$$\max_{\xi \in \mathbb{F}_q^*} \left| \sum_{s \leq t_1} \psi(\xi g^s) \right| < q^{-\delta'} t_1 \text{ for } t_1 > q^\delta.$$

$$\psi(x) = e_p(\text{Tr}x) \quad \text{Tr}x = x + x^p + \cdots + x^{p^{m-1}}.$$

(2) Mordell Type Sums (sparse polynomials)

Formulation for prime modulus

Theorem 8. (complete sums)

Given $\varepsilon > 0, r \in \mathbb{Z}_+$, there is $\delta = \delta(r, \varepsilon) > 0$ such that if p prime (suff larger) following holds. Let

$$f(x) = \sum_{i=1}^r a_i \cdot x^{k_i} \in \mathbb{Z}[X] \quad (a_i, p) = 1$$

with exponents $1 \leq k_i < p - 1$ satisfying

$$\begin{aligned} (k_i, p - 1) &< p^{1-\varepsilon} \\ (k_i - k_j, p - 1) &< p^{1-\varepsilon} \text{ if } i \neq j. \end{aligned}$$

Then

$$\left| \sum_{x=1}^p e_p(f(x)) \right| < p^{1-\delta}.$$

Difference condition needed. Ex

$$\sum_x e_p(x^{\frac{p-1}{2}+1} - x) = \frac{p-1}{2} + O(\sqrt{p}).$$

Theorem 5. (*incomplete sums*)

Let $g_1, \dots, g_r \in \mathbb{F}_p^*$ satisfy

$$\begin{aligned} \text{ord}_p(g_i) &> p^\varepsilon \\ \text{ord}_p(g_i g_j^{-1}) &> p^\varepsilon \text{ if } i \neq j. \end{aligned}$$

Let $(a_i, p) = 1$. Then

$$\left| \sum_{s=1}^{t_1} e_p \left(\sum_{i=1}^r a_i g_i^s \right) \right| < p^{-\delta} t_1 \text{ for } t_1 > p^\varepsilon.$$

Dependence of $\delta = \delta(r, \varepsilon)$ of the form

$$\delta(r, \varepsilon) = \exp \left(-Cr \left(\frac{1}{\varepsilon} + \log r \right) \right) \quad (4)$$

$r \lesssim \log \log p$ is a limitation of method.

Problem 4. Improve on (2)

In particular, relax condition in r .

(3) Some Applications to Equidistribution

A). Diffie-Hellman Key

Uniform distribution of blocks of bits of

$$\left(\left\{ \frac{\theta^x}{m} \right\}, \left\{ \frac{\theta^y}{m} \right\}, \text{Big} \left\{ \frac{\theta^{xy}}{m} \right\} \right)_{1 \leq x, y \leq T}$$

(un-distinguishability assumption)

$$m = p \text{ or } m = pq (p \sim q \text{ (Blum integer)}).$$

Results as soon as

$$\begin{aligned} 0_p(\theta), 0_q(\theta) &> m^\varepsilon \\ T &> m^\varepsilon. \end{aligned}$$

B). Linear Congruential Generator

$$X_{n+1} = aX_n + c \pmod{m}$$

m prime (ex. $m = 2^{31} - 1$) or $m = 2^k (k = 32)$
 uniform distribution of short sequences.

C). Power – Generators

$$m = pq \quad (\text{Blum})$$

$$(e, m) = 1 \quad (\theta, m) = 1$$

$$\begin{cases} u_0 = \theta \\ u_{n+1} = u_n^2 \end{cases}$$

$e = 2$ Blum-Blum-Shub

$(e, (p - 1)(q - 1))$ RSA.

Unconditional proofs of joint-distribution properties

D). Estimation of other exponential sums involving exponential functions (in particular related to D-H crypto-system).

Example. Assume $p - 1$ has a divisor $p^\varepsilon < q < p^{1-\varepsilon}$.

Then

$$\left| \sum_{x=0}^{p-2} e_p(ag^x + bg^{x^2}) \right| < p^{1-\delta}$$

for g generator of \mathbb{F}_p^* , $(a, p) = 1 = (b, p)$.

(4) Decimation Conjecture and Related

‘Decimation conjecture’ from

GORESKY-KLAPPER

in

‘Arithmetic Cross-correlation of FCSR sequences’

↓

feedback with carry shift registers

equivalent with the following conjecture.

GK-Conjecture.

p prime

$$(d, p-1) = 1, 0 < |A| < p/2, |d| < p/2$$

$$(A, d) \neq (1, 1)$$

$$E = \{2, 4, \dots, p-1\} \subset \mathbb{Z}/p\mathbb{Z} \text{ even residues.}$$

Then

$$\{Ax^d : x \in E\} \not\subset E$$

except for

$$(p, A, d) = (5, 3, 3), (7, 1, 5), (11, 9, 3), (11, 3, 7), (11, 5, 9), (13, 1, 5).$$

Verified for $p < 2 \cdot 10^6$.

GK-conjecture motivated the following result of B-B-K related to Theorem 8 (but weakening the condition on the exponent differences $k_i - k_j$).

Theorem 10. (BBK)

Given $r \geq 2$ and $\varepsilon > 0$, there are

$$B = B(r, \varepsilon), \delta = \delta(r, \varepsilon)$$

such that the following holds.

Let $1 \leq k_1 < \dots < k_r < p-1$ satisfy

$$(k_i, p-1) < p^{1-\varepsilon}$$

$$(k_i - k_j, p-1) < \frac{p}{B} \text{ if } i \neq j.$$

Let $p > C(r, \varepsilon)$ and $N_i (1 \leq i \leq r)$ such that $N_i > p^{1-\delta}$.

Then, if $\begin{matrix} a_1, \dots, a_r \\ \ell_1, \dots, \ell_r \end{matrix} \in [1, p-1]$, the system of congruences

$$a_i x^{k_i} \equiv \ell_i + y_i \pmod{p}$$

has a solution in the box $(x, y_1, \dots, y_r) \in [1, p-1] \times \prod_{i=1}^r [1, N_i]$.

Proof combines Theorem 8 with geometry of intersections of varieties of Fermat type.

Note that GK-problem amounts to solve

$$\begin{cases} x \equiv y_1 \\ Ax^d = 1 + y_2 \end{cases} \pmod{p} \quad (5)$$

with $(x, y_1, y_2) \in [1, p-1] \times E \times E$.

From Theorem 10, it follows that the GK-conjecture holds for p sufficiently large.

Eventually, (3) was attacked by ‘classical methods’ (Stepanov for binomial sum) in B-C-P-P

involving explicit numerical calculations.

Theorem 11. *G-K conjecture holds for $p > 2.26 \cdot 10^{55}$*

Problem 5. Improve on Theorem 11.