Estimates for Character Sums — Old & New

Ke Gong, Henan University

http://ntg.henu.edu.cn/

Analytic Number Theory Seminar

Mekh-Mat, Moscow State University

August 4, 2014

What is character sum?

Sums of the form

$$S = \sum_{x \in V} F(x)$$

are ubiquitous in number theory, where $V \subset \mathbb{Z}^d$ is a finite set, and $F : V \to \mathbb{C}$ is a periodic function of period q.

Usually we take $F(x) = \chi(f(x))\psi(g(x))$ with χ and ψ being multiplicative and additive characters modulo q respectively, and f, g being rational functions with integral coefficients.

General principle: the sparser the V is, the harder the sum S is to be controlled.

Here we are mainly concern on the sums with multiplicative characters.

I. What's Known

G. Pólya and I. M. Vinogradov

G. Pólya, I. M. Vinogradov (independently, 1918):

For $\chi \neq \chi_0 \pmod{q}$,

$$\left| \sum_{1 \leq n \leq N} \chi(n) \right| \leq c\sqrt{q} \log q.$$

Proved by finite Fourier analysis.

For primitive character, use the property of Gauss sums to replace $\chi(n)$, then perform the summation of geometric progression.

A standard method leads to imprimitive character.

Pólya–Vinogradov inequality gives a nontrivial estimate for the character sum whenever $M < \sqrt{q}\log q$ and is quite close to being best possible.

H. L. Montgomery, R. C. Vaughan (1977):

Assume GRH. For $\chi \neq \chi_0$, we have

$$\sum_{n=M+1}^{M+N} \chi(n) \ll \sqrt{q}\log\log q.$$

R. E. A. C. Paley (1932):

$$\max_N \left| \sum_{n\le N} \left(\frac{d}{n}\right) \right| > \frac{1}{7}\sqrt{d}\log\log d$$

for infinitely many quadratic discriminants $d > 0$.

D. A. Burgess

In 1957, D. A. Burgess improved the Pólya–Vinogradov inequality for short interval for quadratic character. Burgess's method lies at an ingenious use of Weil's deep work on the analogue of the Riemann hypothesis for the zeta function of an algebraic function field over a finite field. As a consequence, Burgess obtained his Fundamental Lemma, which was originated in a paper of H. Davenport and P. Erdős [DE], and then combining some complicated combinatorial method with the *mean-to-maximum principle*, he concluded the proof.

Fundamental Lemma. $\forall\, r \in \mathbb{Z}^+$, $\chi \neq \chi_0$ *modulo a prime* p,

$$\sum_{x=1}^{p} \left| \sum_{y=1}^{h} \chi(x+y) \right|^{2r} \leq C_r(ph^r + p^{\frac{1}{2}} h^{2r}).$$

D. A. Burgess (1957), Y. Wang (1959):

$\chi \neq \chi_0 \pmod{p}$, p prime. $\forall\, \varepsilon > 0$, if $N > p^{1/4+\varepsilon}$, then

$$\sum_{n=M+1}^{M+N} \chi(n) \ll N p^{-\delta}, \quad \delta = \delta(\varepsilon) > 0.$$

D. A. Burgess (1962):

$\chi \neq \chi_0 \pmod{p}$, p prime. $\forall\, r \in \mathbb{Z}^+$,

$$\sum_{n=M+1}^{M+N} \chi(n) \ll N^{1-\frac{1}{r+1}} p^{\frac{1}{4r}} \log p.$$

D. A. Burgess (1957) treated Legendre symbol. Y. Wang (1959) treated general Dirichlet character modulo p, and then applied his character sum estimate to bound the least positive primitive root $g(p)$ modulo p. His method gives $g(p) = O(p^{\frac{1}{4}+\varepsilon})$, which is still best nowadays.

Another achievement of Y. Wang (1959) is an estimate for the least positive primitive root under GRH: $g(p) = O(\omega(p-1)^6 \log^2 p)$, with $\omega(n)$ being the number of distinct prime factors of n. A weighted character sum estimate together Brun's sieve was used.

Burgess $(1962, 1986)$ generalized his method to deal with arbitrary Dirichlet characters having cube-free conductor. Burgess's extension to composite moduli involves an extra new idea that does not extend well when the conductor is divisible by higher powers of primes.

$\longrightarrow$ algebraic number fields

P. D. T. A. Elliott (2001):

> *Burgess's method is surely an outcome of the adoption of explicitly a method and implicitly an aesthetic from the theory of probability. In spite of Davenport's assessment, his work with Erdős partly turned interest away from the Fourier analytic methods employed by Pólya and Vinogradov, ...*
>
> *The character sum estimate of Burgess has hardly been improved in forty years. Is this particular application of the ideas of probability to the estimation of an individual character sum in number theory isolated?*

A. A. Karatsuba's work

A. A. Karatsuba (1968) gave a simplified proof of Burgess. The proof is also "based on *Weil's theorem that the Riemann hypothesis holds for function fields over finite fields*. However Karatsuba has a quite distinct (though related) method for using this hypothesis that is more analytic and less combinatorial than that of the other authors" (D. A. Burgess, Zbl 0246.10020).

This paved the road for M.-C. Chang (2008) and S. V. Konyagin (2010) to generalize Burgess's character sums to general finite fields in full strength, which was left as a problematic issue after H. Davenport and D. J. Lewis (1963). Tools from additive combinatorics and geometry of numbers were introduced ingeniously by M.-C. Chang and by S. V. Konyagin.

Various applications in number theory

- the quadratic non-residue, least primitive root modulo a prime
- character sums over shifted primes
- subconvexity bounds
- ......

II. What's New

i) Extremely short exponential sums

In order to introduce the work of J. Bourgain and S. V. Konyagin on extremely short exponential sums, we should mention first that

What is sum-product phenomenon?

In a seminal paper published in 1983, P. Erdős and E. Szemerédi found the first example of sum-product phenomenon.

Theorem. *For $\emptyset \neq A \subset \mathbb{Z}$, we have*

$$\max(|A+A|, |A \cdot A|) \gg |A|^{1+\alpha}$$

for some absolute constant $\alpha > 0$.

Furthermore, they conjectured that one can take α arbitrarily close to 1. But this conjecture is out of reach at present.

Erdős–Szemerédi theorem says that it's difficult for a finite subset A of $\mathbb{Z}$ to resemble an AP and a GP simultaneously unless A is very small. So we expect at least one of $A+A$ and $A \cdot A$ to be significantly larger than A itself.

Sum-product phenomenon in $\mathbb{F}_p$

In 1999, T. Wolff (a late analyst well-known for his work on *Kakeya problem*) posed the question of whether the sum-product phenomenon held true in finite prime field $\mathbb{F}_p$, and in particular whether

$$\max(|A+A|, |A\cdot A|) \gg |A|^{1+\alpha},$$

for any $A \subset \mathbb{F}_p$ such that $|A| \le p^{1-\delta}$ for some $\delta > 0$. Here α depends on δ.

This conjecture was confirmed by Bourgain, Katz, Tao (GAFA, 2004) in the range $p^\delta \le |A| \le p^{1-\delta}$, and then by Bourgain, Glibichuk, Konyagin (JLMS, 2006) in the full range $1 \le |A| \le p^{1-\delta}$.

J. Bourgain, A. A. Glibichuk, V. Konyagin

Combing the tools from harmonic analysis with the sum-product phenomenon in $\mathbb{F}_p$, J. Bourgain, A. A. Glibichuk, S. V. Konyagin (2006) estimate nontrivially the extremely short exponential sums.

BGK Theorem. *There exist positive constants C_1, C_2 and C_3 such that for $\delta > 0$, $A \subset \mathbb{F}_p^*$ with $|A| \geq p^\delta$, and any $k \geq \delta^{-C_3}$ we have*

$$\max_{\xi \in \mathbb{F}_p^*} \left| \sum_{x_1, \ldots, x_k \in A} e_p\left(\frac{x_1 \cdots x_k \xi}{p} \right) \right| \leq p^{-\gamma} |A|^k$$

with $\gamma = \exp(-C_1/\delta^{C_2})$, where $e_p(x) = \exp(2\pi i x/p)$ for $x \in \mathbb{R}$.

Exponential sums over multiplicative subgroups

Once taking $A = H < \mathbb{F}_p^*$, we obtain the estimate for exponential sums over multiplicative subgroup in $\mathbb{F}_p^*$.

Theorem. *Let $H < \mathbb{F}_p^*$ be a multiplicative subgroup of $\mathbb{F}_p^*$ with $|H| > p^\delta$ for some $0 < \delta < 1$. Then, if p is sufficiently large depending on δ, we have*

$$\max_{\xi \in \mathbb{F}_p^*} \left| \sum_{x \in H} e_p(\xi x) \right| \le p^{-\gamma} |H|$$

for some $\gamma = \gamma(\delta) > 0$.

Why important?

- This is a deep work because it surpasses what could be attained by the methods from arithmetic geometry (A. Weil, P. Deligne) and analytic number theory (S. A. Stepanov, S. V. Konyagin).

- It motivates many studies in cryptography, theoretic computer science, … .

- J. B. Friedlander remarked (MR 2359468) that “the success of this new method in dealing with such short sums instantly raises dreams of other more famous ones, especially sums of the Legendre symbol. So far, such dreams are unfulfilled.”

I. E. Shparlinski (2010) posed the following multiplicative analogue.

Problem. *Estimate*

$$\max_{a\in\mathbb{F}_p^*}\left|\sum_{x_1,\dots,x_k\in A}\chi(x_1\cdots x_k+a)\right|$$

with very small values of N relative to p, where $A\subset\mathbb{Z}_p$, χ is a non-principal multiplicative character modulo p, and $\gcd(a,p)=1$*.*

This is out of reach at present.

We shall return to this with an essential but simple-looking problem due to J. Bourgain.

ii) Pretentious approach

Since 1999, A. Granville and K. Soundararajan have launched the so-called «pretentious approach» to multiplicative number theory. Now they could recover all the main results in H. Davenport's and E. Bombieri's books using pretentious methods.

Their method has been used to improve upon the Pólya–Vinogradov inequality for characters of odd, bounded order.

Theorem. *If* $\chi \pmod{q}$ *is a primitive character of odd order* g, *then*

$$\max_N \left| \sum_{n \le N} \chi(n) \right| \ll_g \begin{cases} \sqrt{q}(\log q)^{1-\frac{\delta_g}{2}+o(1)}, & \textit{unconditionally}, \\ \sqrt{q}(\log\log q)^{1-\frac{\delta_g}{2}+o(1)}, & \textit{assume GRH}, \end{cases}$$

where $\delta_g = 1 - \frac{g}{\pi} \sin \frac{\pi}{g}$.

$\longrightarrow$ L. Goldmakher, ...

III. What’s Expected

i) A folklore

Let q be a prime. For $\chi \neq \chi_0 \pmod q$, prove unconditionally that

$$\sum_{n \le N} \chi(n) \ll N^{1/2} q^{\varepsilon}.$$

Burgess's fundamental lemma: for any $r \in \mathbb{Z}^+$,

$$\sum_{x=1}^{q} \left| \sum_{y=1}^{h} \chi(x+y) \right|^{2r} \le C_r(qh^r + q^{\frac{1}{2}} h^{2r}).$$

H. L. Montgomery (1971):

For $\chi \neq \chi_0 \pmod q$, assume generalized Lindelöf Hypothesis,

$$\sum_{n \leq N} \chi(n) \ll N^{1/2} q^{\varepsilon}.$$

H. L. Montgomery, R. C. Vaughan (1979):

$\forall\, k \in \mathbb{R}^+$,

$$\sum_{\chi \neq \chi_0} \left(\max_N \left| \sum_{n \leq N} \chi(n) \right| \right)^{2k} \ll_k \varphi(q) q^k,$$

which implies that, for most $\chi \neq \chi_0$, $\max_N \left| \sum_{n \leq N} \chi(n) \right| \ll \sqrt{q}$.

ii) Another folklore

Let $\chi \neq \chi_0 \pmod{q}$ *with* q *prime. Estimate nontrivially*

$$\sum_{\substack{p \le N \\ p \text{ prime}}} \chi(p+a), \qquad \gcd(a,q) = 1$$

for $N \sim \sqrt{q}$*.*

I. M. Vinogradov first studied this time. He revisited it for many times during 1930s to 1950s. His best result is a nontrivial estimate in the range $N > q^{\frac{3}{4}+\varepsilon}$, which lies deeper than the generalized Riemann Hypothesis.

The best result was obtained by A. A. Karatsuba (1970).

M.-C. Chang (2010) has some new ideas on this.

Records

q prime

I. M. Vinogradov (1953): $N > q^{\frac{3}{4}+\varepsilon}$

A. A. Karatsuba (1970): $N > q^{\frac{1}{2}+\varepsilon}$

q composite

Z. Kh. Rakhmonov (1986): $N > q^{1+\varepsilon}$

Friedlander–G.–Shparlinski (2010): $N > q^{\frac{8}{9}+\varepsilon}$

Z. Kh. Rakhmonov (2013): $N > q^{\frac{5}{6}+\varepsilon}$

B. Kerr (2013): $N > q^{\frac{5}{6}+\varepsilon}$

iii) A problem

Let p be an odd prime, and $H < \mathbb{F}_p^*$ be a multiplicative subgroup. J. Bourgain posed (2010)

Problem. *Estimate nontrivially*

$$\sum_{n \in H < \mathbb{F}_p^*} \chi(n+a), \qquad a \in \mathbb{F}_p^*$$

for $|H| \sim \sqrt{p}$.

This is a natural *multiplicative analogue* of BGK Theorem of exponential sums over multiplicative subgroups.

As a simplest but essential case of Shparlinski's problem on multilinear character sums, the above problem is believed *to encode all the secrets*.

It is obvious that $|H| > p^{1/2+\varepsilon}$ can be derived from Weil's theorem. However, using Vinogradov's bilinear methods, we can give an alternative elementary approach.

We also have two different types of mean-value estimates, which may suggest what the truth should be.

Mean-value estimates

1). *For any subset $D \subset \mathbb{F}_p^*$, we have the identity*

$$\sum_{a\in\mathbb{F}_p} \left| \sum_{x\in D} \chi(x+a) \right|^2 = p|D| - |D|^2.$$

2). *For $a \in \mathbb{F}_p^*$, we have*

$$\frac{1}{p-1} \sum_{\chi \,(\mathrm{mod}\, p)} \left| \sum_{x\in H} \chi(x+a) \right| \le \sqrt{|H|}.$$

iv) Paley Graph Conjecture

For the background in graph theory, see B. Bollobás's «Random Graphs» (CUP, 2001).

For the applications of Paley Graph Conjecture to computer science, see B. Chor and O. Goldreich (1988), D. Zuckerman (1990), and I. E. Shparlinski (1999).

Paley Graph Conjecture. *Let $\left(\frac{\cdot}{p}\right)$ be the quadratic character modulo a prime p. Then for any $\varepsilon > 0$, there exists an $\delta > 0$ such that for large prime p, if $|S|, |T| \geq p^{\varepsilon}$, then*

$$\left| \sum_{s \in S,\, t \in T} \left(\frac{s+t}{p} \right) \right| \leq |S| \cdot |T| p^{-\delta}.$$

A. A. Karatsuba (1971) made the first advance towards Paley Graph Conjecture.

Theorem. *Let U and V be integers, $p \geq p_0(\varepsilon)$,*

$$p^{1/2+\varepsilon} \leq U < p, \qquad p^{\varepsilon} < V < p,$$

$$W = \sum_{u}^{U} \sum_{v}^{V} \left(\frac{u+v}{p} \right),$$

where u and v in the last sum run over U and V, respectively, different values modulo p. Then

$$|W| \leq cUVp^{-\delta}, \qquad \delta = \delta_0(\varepsilon) > 0, \qquad c = c(\varepsilon).$$

Various variants with additional restrictions were studied by J. Friedlander and H. Iwaniec (1993), A. A. Karatsuba (1992), F. R. K. Chung (1994), M.-C. Chang (2008).

We include here an interesting one due to M.-C. Chang (2008).

Theorem. *Assume that* $A, B \subset \mathbb{F}_p$ *such that*

1) $|A| > p^{4/9+\varepsilon}$, $|B| > p^{4/9+\varepsilon}$,
2) $|B + B| < K|B|$.

Then

$$\left| \sum_{x \in A,\, y \in B} \chi(x+y) \right| < |A| \cdot |B| p^{-\tau},$$

where $\tau = \tau(\varepsilon, K) > 0$, $p > p(\varepsilon, K)$, *and* χ *is a non-principal multiplicative character of* $\mathbb{F}_p$.

Problem (M.-C. Chang). *Estimate nontrivially*

$$\sum_{x\in A,\, y\in B} \chi(x+y)$$

for $A, B \subset \mathbb{F}_p$ *arbitrary, and* $|A|$, $|B| \sim \sqrt{p}$.

Problem (P. Sarnak). *In above problem, consider*

$$A = B = H < \mathbb{F}_p^*$$

with $|H| \sim \sqrt{p}$.

IV. Recent Works

(Joint with Professor Chaohua Jia)

Motivations

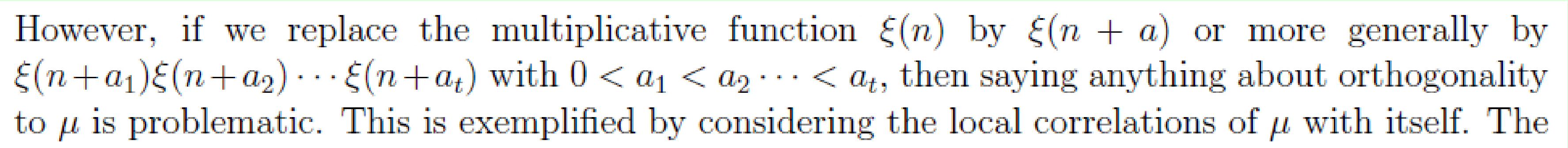
- Möbius Randomness Law

> *The Möbius function μ changes sign randomly so that for any "reasonable" sequence of complex numbers $\mathcal{A} = (a_m)$ the twisted sum*
>
> $$M(\mathcal{A}, x) = \sum_{m \leq x} \mu(m) a_m$$
>
> *is relatively small due to the cancellation of its terms.*

Of course a reasonable sequence means chosen with no bias.

H. Iwaniec and E. Kowalski, «Analytic Number Theory». Amer. Math. Soc., 2004.

- Sarnak's Puzzle



However, if we replace the multiplicative function $\xi(n)$ by $\xi(n+a)$ or more generally by $\xi(n+a_1)\xi(n+a_2)\cdots\xi(n+a_t)$ with $0 < a_1 < a_2 \cdots < a_t$, then saying anything about orthogonality to μ is problematic. This is exemplified by considering the local correlations of μ with itself. The

P. Sarnak, «Three lectures on the Möbius function randomness and dynamics». Notes, 2010.

- The works of D. Hajela, A. Pollington, B. Smith (1988), G. Wang, Z. Zheng (1998), and P. Deng (1999) on Kloosterman sums with oscillating coefficients. $\longleftrightarrow \mu(n)$

- The work of M. Z. Garaev (2010) on Kloosterman sums with primes. $\longleftrightarrow \Lambda(n) \longrightarrow \mu(n)$

- When $t \leq 2$, the works of I. M. Vinogradov and A. A. Karatsuba on linear and nonlinear sums over primes. $\longleftrightarrow \Lambda(n) \longrightarrow \mu(n)$

- When $t \geq 3$, A. A. Karatsuba (1978) had a conditional result for sums over primes.

Karatsuba's Conjecture. *If $f(x) \in \mathbb{Z}[x]$ is not a complete square modulo q, the integers $a_1, \ldots, a_t$ are pairwise non-congruent modulo q, $t \geq 2$, and $F(x,y) = f(x+a_1y) \cdots f(x+a_ty)$, then the estimate*

$$\left| \sum_{x=1}^{q} \sum_{y=1}^{q} \left(\frac{F(x,y)}{q} \right) \right| \ll q$$

holds, where the constant implied in $\ll$ depends only on t and $\deg(f)$.

i) Kloosterman sums with multiplicative coefficients

Let f be a multiplicative function satisfying $|f(n)| \le 1$, q $(\le N^2)$ be a positive integer and a be an integer with $(a, q) = 1$. Let $\overline{n}$ denote the multiplicative inverse of n such that $\overline{n}n \equiv 1 \pmod{q}$. $\tau(\cdot)$ is the divisor function.

G.–Jia (arXiv:1401.4556). *We have*

$$\sum_{\substack{n \le N \\ (n,q)=1}} f(n) e\left(\frac{a\overline{n}}{q}\right) \ll \sqrt{\frac{\tau(q)}{q}} N \log\log(6N)$$

$$+ q^{\frac{1}{4}+\frac{\varepsilon}{2}} N^{\frac{1}{2}} (\log(6N))^{\frac{1}{2}} + \frac{N}{\sqrt{\log\log(6N)}}.$$

Remarks

1) The main tool is a modification of Bourgain–Sarnak–Ziegler's finite version of Vinogradov's inequality.

2) Nontrivial estimate for the range $N > q^{1/2+\varepsilon}$.

Study on the case of $f = \mu$ by

- D. Hajela, A. Pollington, B. Smith (1988): $N > q^{3/2+\varepsilon}$
- G. Wang, Z. Zheng (1998) / P. Deng (1999): $N > q^{1+\varepsilon} \longleftrightarrow$ GRH

Study on the case of *von Mangoldt* weight Λ by

- M. Z. Garaev (2010): $N > q^{\frac{1}{2}+\varepsilon}$

ii) Shifted character sums with multiplicative coefficients

Let f be a multiplicative function satisfying $|f(n)| \leq 1$, q $(\leq N^2)$ be a prime number and a be an integer with $(a,q)=1$, $\chi \neq \chi_0$ be a Dirichlet character modulo q.

G.–Jia (arXiv:1404.2204). *We have*

$$\sum_{n\leq N} f(n)\chi(n+a) \ll \frac{N}{q^{\frac{1}{4}}}\log\log(6N)+q^{\frac{1}{4}}N^{\frac{1}{2}}\log(6N)+\frac{N}{\sqrt{\log\log(6N)}}$$

and

$$\sum_{n\leq N} f(n)\chi((n+a_1)\cdots(n+a_t))$$
$$\ll \frac{N}{q^{\frac{1}{4}}}\log\log(6N)+q^{\frac{1}{4}}N^{\frac{1}{2}}\log(6N)+\frac{N}{\sqrt{\log\log(6N)}},$$

where $t \geq 2$, $a_1, \ldots, a_t$ are pairwise distinct integers modulo q.

Thanks for your attention !