On some computational problems with character sums

N. V. Proskurin

Abstract. For polynomial character sums in finite fields, some theoretical and computational problems similar to the Sato–Tate conjecture are discussed.

1. Kloosterman sums, elliptic curves and Sato–Tate measure

Given the field $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ of prime order p and its additive character $e_p(t) = \exp(2\pi it/p)$, $t \in \mathbb{F}_p$, let us consider *Kloosterman sums*

$$Kl_p(c) = \sum_{t \in \mathbb{F}_p^\star} e_p(t^{-1} + ct),$$

where $c \in \mathbb{Z}$ and summation runs over multiplicative group $\mathbb{F}_p^\star = \mathbb{F}_p \setminus \{0\}$. The Kloosterman sums are real satisfying $|Kl_p(c)| \le 2\sqrt{p}$ and one may look on distribution of the points $Kl_p(c)$ in the interval $[-2\sqrt{p}, 2\sqrt{p}]$. Let $\pi(x)$ denotes the number of all prime $p \le x$. It is expected that

$$\lim_{x\to\infty} \frac{1}{\pi(x)} \sharp \left\{ p \le x \;\middle|\; \frac{Kl_p(c)}{2\sqrt{p}} \in [u,v] \right\} = \frac{2}{\pi} \int_u^v \sqrt{1-t^2}\, dt$$

for all intervals $[u,v] \subset [-1,1]$. The integral in the right-hand side represent *Sato-Tate measure* of the interval $[u,v]$. The same probability measure of the subintervals $[u,v] \subset [-1,1]$ occurs in connection to elliptic curves. By Hasse, given an elliptic curve E_p over $\mathbb{F}_p$, the number of its points is equal to

$$p + 1 + R_p \quad \text{with} \quad R_p \quad \text{satisfying} \quad |R_p| \le 2\sqrt{p}.$$

Let E be an elliptic curve defined over $\mathbb{Q}$. For almost all p, its reduction modulo p is an elliptic curve E_p over $\mathbb{F}_p$ and one has R_p as defined above. Put $R_p = 0$ for

remaining p. The *Sato-Tate conjecture* states

$$\lim_{x\to\infty} \frac{1}{\pi(x)} \sharp \Big\{ p \le x \;\Big|\; \frac{R_p}{2\sqrt{p}} \in [u,v] \Big\} = \frac{2}{\pi} \int\limits_u^v \sqrt{1-t^2}\, dt$$

for all intervals $[u,v] \subset [-1,1]$. See [1], [2].

2. Polynomial character sums

Given polynomials f, g over $\mathbb{Z}$ and a character[1] χ_p of $\mathbb{F}_p^\star$, let

$$S_p = \sum_{t\in\mathbb{F}_p} \chi_p\big(f(t)\big)\, e_p\big(g(t)\big). \tag{1}$$

That are known as *polynomial character sums*. As an example, one has

$$Kl_p(c) = \sum_{t\in\mathbb{F}_p} \kappa_p(t^2-4c)\, e_p(t)$$

with prime $p \ne 2$ and with a unique quadratic character κ_p of $\mathbb{F}_p^\star$.

Under some general assumptions on f, g, and χ_p one has Weil estimate

$$|S_p| \le (n+m-1)\,\sqrt{p}\,, \tag{2}$$

where $n = \deg(g \bmod p)$ and $m = \deg\big(\text{radical}\,(f \bmod p)\big)$.

If $f \bmod p = f_1^{s_1} \dots f_r^{s_r}$ with integers $s_1,\dots,s_r \ge 1$ and irreducible over $\mathbb{F}_p$ polynomials $f_1,\dots,f_r$, then $m = \deg(f_1 \dots f_r)$. If $n = 0$ and χ_p is a character of order $h \ge 2$, then for (2) it is sufficient to assume $\gcd(h, s_1, \dots, s_r) = 1$.

See [1] for review of general theory and [3] for arithmetic of algebraic curves.

3. Set up

To look for possible analogues of the Sato-Tate type conjectures for the polynomial character sums (1) involving characters χ_p of arbitrary order, we suggest [4], [5] the following construction.

Let $w \in \mathbb{C}$ be a primitive root of 1 of degree h. Given $l \in \mathbb{Z}$, let $\Omega_{l,w}$ be the set of all prime $p \equiv 1 \pmod h$ under the condition: there exists a unique character χ_p of order h, such that $\chi_p(l) = w$. Let $\pi_{l,w}(x) = \sharp\,\{\, p \in \Omega_{l,w} \;|\; p \le x \,\}$ for any $x \in \mathbb{R}$.

Here $p \equiv 1 \pmod h$ provides existence of order h characters χ_p of $\mathbb{F}_p^\star$. The uniqueness can be stated as follows: h is coprime with the index of l relative to any generator of $\mathbb{F}_p^\star$. For prime h, that means l is not h-th degree in $\mathbb{F}_p^\star$.

Assume, the sums S_p are majorized as in (2). Let D be the circle of radius $R = n+m-1$ with center at 0, that is $D = \big\{ z \in \mathbb{C} \;\big|\; |z| \le R \big\}$.

---

[1] To extend χ_p to all of $\mathbb{F}_p$, we set $\chi_p(0) = 0$ for non-trivial χ_p and $\chi_p(0) = 1$ for trivial one.

We suggest to treat the measures

$$\lim_{x\to\infty}\frac{1}{\pi_{l,w}(x)}\sharp\Big\{p\in\Omega_{l,w}\;\Big|\;p\le x,\;\;S_p/\sqrt{p}\in V\Big\},\qquad V\subset D,$$

and their densities as analogues of the ones given in §1.

For some classes of character sums (1), we have explicit equalities for $|S_p|$ instead of (2). Say, we have $|S_p|=\sqrt{p}$ for the Gauss sums and the Jacobi sums. In the cases like that we should take V to be circular arc $\subset D=\big\{z\in\mathbb{C}\;\big|\;|z|=1\big\}$.

4. First sample

With notation in §1 and §2, consider the sums (1) with simplest f and g.

If some of f,g is a polynomial of degree 0 and the second one is a polynomial of degree 1, say $ux+v$ with $u,v\in\mathbb{Z}$, $u\ne 0$, then $S_p=0$ for all prime p excepting $p|u$. This is not interesting.

Let $\deg f=\deg g=0$. This case is far from to be trivial. Our polynomials are just some constants $c,d\in\mathbb{Z}$ and S_p is the sum of p terms $\chi_p(c)\,e_p(d)$. Assume $c\ne 0$ to avoid the case $S_p=0$. Following §3, we should consider the limit

$$\lim_{x\to\infty}\frac{1}{\pi_{l,w}(x)}\sharp\Big\{p\in\Omega_{l,w}\;\Big|\;p\le x,\;\;\chi_p(c)\,e_p(d)\in V\Big\}\tag{3}$$

as the measure of the circular arc $V\subset\big\{z\in\mathbb{C}\;\big|\;|z|=1\big\}$. We can prove the limit in (3) is equal to the sum of limits

$$\lim_{x\to\infty}\frac{1}{\pi_{l,w}(x)}\sharp\Big\{p\in\Omega_{l,w}\;\Big|\;p\le x,\;\;\chi_p(c)=v\Big\}\tag{4}$$

expanded over all v under the conditions $v^h=1$ and $v\in V$. Numerical computation with Maple shows (in some cases) the limit (4) does not depend on v.

5. Gauss sums

With notation in (1), let $f(t)=g(t)=t$. The sums in (1) occur to be

$$G(\chi_p)=\sum_{t\in\mathbb{F}_p}\chi_p(t)\,e_p(t).$$

That are the *Gauss sums*. For non-trivial characters χ_p, one has not only (2) but

$$|G(\chi_p,e_p)|=\sqrt{p}$$

as well. From the point of view given in §3, we should consider the limit

$$\lim_{x\to\infty}\frac{1}{\pi_{l,w}(x)}\sharp\Big\{p\in\Omega_{l,w}\;\Big|\;p\le x,\;\;G(\chi_p,e_p)/\sqrt{p}\in V\Big\}$$

as the measure of the circular arc $V\subset\big\{z\in\mathbb{C}\;\big|\;|z|=1\big\}$.

6. Multiplicative sums

Let us consider the sums (1) with zero polynomial g, i. e. the sums

$$S_p = \sum_{z\in\mathbb{F}_p} \chi_p\big(f(z)\big) \tag{5}$$

involving the multiplicative characters only. Looking for the sums convenient for numerical experiments we find the ones (5) with

$$f(z) = az^m + b \quad \text{and} \quad a, b, m \in \mathbb{Z}, \quad ab \neq 0, \quad m \geq 0.$$

For such binomial f and any non-trivial character ψ of $\mathbb{F}_p$ one has expression

$$\sum_{z\in\mathbb{F}_p} \psi\big(f(z)\big) = \psi(b) \sum_{\theta} \theta(-b/a)\, J(\theta,\psi), \tag{6}$$

where the summation runs over characters θ of orders dividing $\gcd(\deg f, p-1)$ and $J(\theta,\psi)$ are the *Jacobi sums*,

$$J(\theta,\psi) = \sum_{z\in\mathbb{F}_p} \theta(z)\,\psi(1-z).$$

For the formula (6) see [6], ch. 5. There are not more than $\deg f$ terms in the right-hand side. One can evaluate the Jacobi sums in terms of the Gauss ones. Say, if all the characters θ, ψ and $\theta\psi$ are non-trivial, then $J(\theta,\psi) = G(\theta)\,G(\psi)/G(\theta\psi)$. This observation provides effective method of computing the sums (6) with any coefficients a, b. It is convenient to use Maple with its number theory package and primroot command.

References

[1] J.-P. Serre, *Majorations de sommes exponentielles*, Société Mathématique de France, Asterisque 41–42, p. 111–126, 1977.

[2] N. M. Katz, *Gauss Sums, Kloosterman Sums, and Monodromy Groups*, Ann. of Math. St. 116, 1988.

[3] S. A. Stepanov, *Arithmetic of algebraic curves*, Moscow, 1991 (in Russian). English translation: Springer–Verlag, 1995.

[4] N. V. Proskurin, *Some problems on character sums in finite fields*, International Conference on Polynomial Computer Algebra, Saint Petersburg, 2020.

[5] N. V. Proskurin, *On character sums in finite fields*, Algebra and number theory 3, Zap. Nauchn. semin. POMI **490**, 104–108, 2020 (in Russian).

[6] R. Lidl, H. Niederreiter, *Finite fields*, Cambridge University Press, sec. ed., 1997.

N. V. Proskurin
St. Petersburg Department of Steklov Institute of Mathematics RAS
191023, Fontanka 27, St. Petersburg, Russia
e-mail: np@pdmi.ras.ru