WEIL BOUND FOR KLOOSTERMAN SUMS

KIM, SUNGJIN

1. The Zeta Function for Kloosterman Sums

Theorem 1. *Let q be a prime power, and χ be a multiplicative character of $\mathbb{F}_q^*$. For a, b prime to p, the Kloosterman sum satisfies the bound*

$$\left| \sum_{x \in \mathbb{F}_q^*} \chi(x) e\left(\frac{ax + bx^{-1}}{q} \right) \right| \leq 2\sqrt{q}. \tag{1}$$

We first consider when χ is trivial. Then the sum in (1) is just

$$\sum_{x \in \mathbb{F}_q^*} e\left(\frac{ax + bx^{-1}}{q} \right) \tag{2}$$

Let ψ and ϕ be the additive characters defined by $\psi(x) = e\left(\frac{\mathrm{Tr}(ax)}{p}\right)$, and $\phi(x) = e\left(\frac{\mathrm{Tr}(bx)}{p}\right)$ respectively. Denote $S(\psi, \phi) = -\sum_{x \in \mathbb{F}^*} \psi(x)\phi(x^{-1})$ where $\mathbb{F} = \mathbb{F}_q$. Then the companion sums over the extension fields $\mathbb{F}_n = \mathbb{F}_{q^n}$ are

$$S_n(\psi, \phi) = -\sum_{x \in \mathbb{F}_n^*} \psi(\mathrm{Tr}(x))\phi(\mathrm{Tr}(x^{-1})). \tag{3}$$

The Kloosterman zeta function is

$$Z(\psi, \phi) = \exp\left(\sum_{n \geq 1} \frac{S_n(\psi, \phi)}{n} T^n \right). \tag{4}$$

Let $G \subset \mathbb{F}(X)$ be the group of quotients of monic polynomials defined and non-vanishing at 0. We define a character $\eta : G \longrightarrow \mathbb{C}^*$ by putting

$$\eta(h) = \psi(a_1)\phi(a_{d-1}/a_d)$$

for a monic polynomial $h \in G$, where we write

$$h = X^d + a_1 X^{d-1} + \cdots + a_{d-1}X + a_d$$

(with $a_d \neq 0$ since $h \in G$). Then the L-function associated to η is given by

$$L(s, \eta) = \sum_h \eta(h) N(h)^{-s} = 1 - S(\psi, \phi) q^{-s} + q^{1-2s}.$$

This identity is verified through rearranging terms according to the degree of h.

$$L(s, \eta) = \sum_{d \geq 0} \left(\sum_{\deg(h) = d} \eta(h) \right) q^{-ds}$$

and evaluating the inner sums. For $d=0$, we have only $h=1$ and $\eta(1)=1$. For $d=1$, we have $h=X+a$ with $a\neq 0$, hence

$$\sum_{\deg(h)=1}\eta(h)=\sum_{a\in\mathbb{F}^*}\eta(X+a)=\sum_{a\in\mathbb{F}^*}\psi(a)\phi(a^{-1})=-S(\psi,\phi).$$

For $d=2$, we get

$$\begin{aligned}\sum_{\deg(h)=2}\eta(h)&=\sum_{\substack{a\in\mathbb{F}\\ b\in\mathbb{F}^*}}\eta(X^2+aX+b)=\sum_{\substack{a\in\mathbb{F}\\ b\in\mathbb{F}^*}}\psi(a)\phi(ab^{-1})\\ &=q-1+\left(\sum_{a\in\mathbb{F}^*}\psi(a)\right)\left(\sum_{b\in\mathbb{F}}\phi(b)\right)=q.\end{aligned}$$

Finally for $d\geq 3$, we get

$$\begin{aligned}\sum_{\deg(h)=3}\eta(h)&=\sum_{\substack{a\in\mathbb{F}^*\\ a_1\cdots,a_{d-1}\in\mathbb{F}}}\eta(X^d+a_1X^{d-1}+\cdots+a_{d-1}X+a)\\ &=q^{d-3}\sum_{\substack{a_1,a_{d-1}\in\mathbb{F}\\ a\in\mathbb{F}^*}}\psi(a_1)\phi(a_{d-1}a^{-1})=0\end{aligned}$$

since there is free summation over $a_1\in\mathbb{F}$.

Lemma 1. *For ψ and ϕ non-trivial, we have the identity*

$$Z(\psi,\phi)(q^{-s})=L(s,\eta)^{-1}=\frac{1}{1-S(\psi,\phi)q^{-s}+q^{1-2s}}. \tag{5}$$

Proof. Taking the logarithmic derivative we get

$$\begin{aligned}-\frac{1}{\log q}\frac{L'(s,\eta)}{L(s,\eta)}&=\sum_P\deg(P)\sum_{r\geq 1}\eta(P)^rq^{-r\deg(P)s}\\ &=\sum_{n\geq 1}\left(\sum_{rd=n}d\sum_{\deg(P)=d}\eta(P)^r\right)q^{-ns}\end{aligned}$$

□

and it suffices to prove the formula

$$\sum_{d=\deg(P)|n}d\eta(P)^{n/d}=-S_n(\psi,\phi) \tag{6}$$

for $n\geq 1$. Let $P=X^d+a_1X^{d-1}+\cdots+a_{d-1}X+a_d$ be one of the irreducible polynomials on the left side of (6), of degree $d|n$, and $x_1,\cdots,x_d$ its roots, which lie in $\mathbb{F}_d$. We have for each i,

$$\begin{aligned}\mathrm{Tr}(x_i)&=\frac{n}{d}\mathrm{Tr}_{\mathbb{F}_d/\mathbb{F}}(x_i)=-\frac{n}{d}a_1\\ \mathrm{Tr}(x_i^{-1})&=\frac{n}{d}\mathrm{Tr}_{\mathbb{F}_d/\mathbb{F}}(x_i^{-1})=-\frac{n}{d}\frac{a_{d-1}}{a_d}.\end{aligned}$$

Hence

$$\eta(P)^{n/d}=\psi\left(\frac{n}{d}a_1\right)\phi\left(\frac{n}{d}\frac{a_{d-1}}{a_d}\right)=\psi(\mathrm{Tr}(-x_i))\phi(\mathrm{Tr}(-x_i^{-1}))$$

and summing over the roots x_i, then over the polynomials P of degree $d|n$, we obtain (6).

Now, we consider the case χ is non-trivial. Denote $S(\chi;\psi,\phi) = -\sum_{x\in\mathbb{F}} \chi(x)\psi(x)\phi(x^{-1})$ and its associated companions S_n and zeta function Z. We consider the same group $G \subset \mathbb{F}(X)$. We define a character η by

$$\eta(h) = \chi(a_d)\psi(a_1)\phi\left(\frac{a_{d-1}}{a_d}\right)$$

The associated L-function is

$$L(s,\eta) = \sum_h \eta(h)N(h)^{-s} = \sum_{d\geq 0}\left(\sum_{\deg(h)=d}\eta(h)\right)q^{-ds}.$$

For $d = 0$, $h = 1$ and $\eta(1) = 1$.
For $d = 1$,

$$\sum_{\deg(h)=1}\eta(h) = \sum_{a\in\mathbb{F}^*}\eta(X+a) = \sum_{a\in\mathbb{F}^*}\chi(a)\psi(a)\phi(a^{-1}) = -S(\chi;\psi,\phi).$$

For $d = 2$,

$$\begin{aligned}\sum_{\substack{x\in\mathbb{F}\\ y\in\mathbb{F}^*}}\chi(y)\psi(x)\phi(xy^{-1}) &= \sum_{\substack{x\in\mathbb{F}^*\\ y\in\mathbb{F}^*}}\chi(xy^{-1})e\left(\frac{\mathrm{Tr}(ax)}{p}\right)e\left(\frac{\mathrm{Tr}(by)}{p}\right)\\ &= \sum_{x,y}\chi(x)\bar{\chi}(y)e\left(\frac{\mathrm{Tr}(ax)}{p}\right)e\left(\frac{\mathrm{Tr}(by)}{p}\right)\\ &= \bar{\chi}(a)\tau(\chi)\chi(-b)\overline{\tau(\chi)}\\ &= \bar{\chi}(-a)\chi(b)q.\end{aligned}$$

For $d \geq 3$,

$$\begin{aligned}\sum_{\deg(h)=d}\eta(h) &= \sum_{\substack{a\in\mathbb{F}^*\\ a_1,\cdots,a_{d-1}\in\mathbb{F}}}\eta(X^d + a_1X^{d-1} + \cdots + a_{d-1}X + a)\\ &= q^{d-3}\sum_{\substack{a_1,a_{d-1}\in\mathbb{F}\\ a\in\mathbb{F}^*}}\chi(a)\psi(a_1)\phi(a_{d-1}a^{-1}) = 0.\end{aligned}$$

To deduce the similar identity as in (5), it suffices to show that

$$\sum_{d=\deg(P)|n} d\eta(P)^{n/d} = -S_n(\chi;\psi,\phi).$$

Only difference in this case is that we have a multiplicative character χ. Let $P = X^d + a_1X^{d-1} + \cdots + a_{d-1}X + a_d$ be an irreducible polynomial with coefficients in $\mathbb{F}$, and $x_1,\cdots,x_d$ its roots.

$$\eta(P)^{n/d} = \psi\left(\frac{n}{d}a_1\right)\phi\left(\frac{n}{d}\frac{a_{d-1}}{a_d}\right)\chi(a_d)^{n/d} = \psi(\mathrm{Tr}(-x_i))\phi(\mathrm{Tr}(-x_i)^{-1})\chi(\mathrm{N}(-x_i)).$$

Summing over roots and irreducible polynomials P of degree $d|n$, we obtain

Lemma 2. *For a nontrivial multiplicative character χ, we have*

$$Z = (1 - S(\chi;\psi,\phi)q^{-s} + \bar{\chi}(-a)\chi(b)q^{1-2s})^{-1}. \tag{7}$$

where $\psi(x) = e\left(\frac{\mathrm{Tr}(ax)}{p}\right)$, $\phi(x) = e\left(\frac{\mathrm{Tr}(bx)}{p}\right)$.

2. Stepanov's Method for Hyperelliptic Curves.

Let $\mathbb{F}$ be a finite field with q element, of characteristic p. We will only consider algebraic curves C_f over $\mathbb{F}$ given by equations of the type

$$C_f : y^2 = f(x) \tag{8}$$

for some polynomial $f \in \mathbb{F}[X]$ of degree $m \geq 3$. We assume moreover the following condition

$$\text{The polynomial } Y^2 - f(X) \in \mathbb{F}[X,Y] \text{ is absolutely irreducible} \tag{9}$$

Stepanov's elementary method yields a good bound for the number of solutions of C_f over $\mathbb{F}$.

Theorem 2. *Assume that $f \in \mathbb{F}[X]$ satisfies (9), and $m = \deg(f) \geq 3$. If $q > 4m^2$, then $N = |C_f(\mathbb{F})|$ satisfies*

$$|N - q| < 8m\sqrt{q}.$$

We need the following lemma which relies on Hilbert Satz 90.

Lemma 3. *For any $n \geq 1$ and any $x \in \mathbb{F}_n$, we have*

$$|\{y \in \mathbb{F}_n | y^q - y = x\}| = \sum_{\psi} \psi(\mathrm{Tr}(x)) \tag{10}$$

where the sum ranges over all additive characters of $\mathbb{F}$ and Tr is the trace $\mathbb{F}_n \longrightarrow \mathbb{F}$.

Denote the Kloosterman sum by

$$S(\psi_a, \psi_b) = -\sum_{x \in \mathbb{F}^*} \psi(ax + bx^{-1})$$

for some $a, b \in \mathbb{F}$. We consider a and b as fixed and write $g = aX + bX^{-1}$. From this lemma we deduce that

$$\begin{aligned} -\sum_{\psi} S_n(\psi_a, \psi_b) &= \sum_{\psi} \sum_{x \in \mathbb{F}_n^*} \psi(\mathrm{Tr} g(x)) \\ &= |\{(x,y) \in \mathbb{F}_n^* \times \mathbb{F}_n | y^q - y = g(x)\}| = N_n \end{aligned}$$

If $\psi = \psi_0$, the trivial character, we have $S_n(\psi_0, \psi_0) = 1 - q^n$.
For $\psi \neq \psi_0$, let α_ψ, β_ψ be the roots of the Kloosterman sum $S(\psi_a, \psi_b)$, so we have $\alpha_\psi \beta_\psi = q$ and

$$S_n(\psi_a, \psi_b) = \alpha_\psi^n + \beta_\psi^n,$$

for all $n \geq 1$.
We can therefore write

$$N_n = q^n - 1 - \sum_{\psi \neq \psi_0} (\alpha_\psi^n + \beta_\psi^n).$$

We can transform the equation $y^q - y = g(x)$ into

$$C_{a,b} : ax^2 - (y^q - y)x + b = 0$$

Because $p \neq 2$, the number of solutions is equal to the number of solutions of the discriminant equation

$$D_{a,b} : (y^q - y)^2 - 4ab = v^2,$$

i.e. $N_n = |D_{a,b}(\mathbb{F}_n)|$. This is of the form (9) with deg(f)= $2q$, and because $4ab \neq 0$ it satisfies the assumptions of Theorem 2. Hence by Theorem 2 we have

$$|N_n - q^n| < 16q^{1+n/2}$$

if n is large enough, so that $q^n > 16q$. This gives a sharp estimate for the roots α_ψ, β_ψ, on average

$$\frac{1}{q}\left|\sum_{\psi\neq\psi_0}(\alpha_\psi^n + \beta_\psi^n)\right| \leq 16q^{n/2} \tag{11}$$

for n large enough. The following lemma shows that the individual roots must be of modulus $\leq \sqrt{q}$.

Lemma 4. *Let $\omega_1, \cdots, \omega_r$ be complex numbers, A, B positive real numbers and assume that*

$$\left|\sum_{j=1}^{r}\omega_j^n\right| \leq AB^n$$

holds for all integers n large enough. Then $|\omega_j| \leq B$ for all j.

Proof. The proof uses the identity

$$f(z) = \sum_{n\geq 1}(\sum_j \omega_j^n)z^n = \sum_j \frac{1}{1-\omega_j z}.$$

Compare the radius of convergence on each side. □

For a nontrivial multiplicative character χ, we denote the Kloosterman sum by

$$S(\chi;\psi_a,\psi_b) = -\sum_{x\in\mathbb{F}^*}\chi(x)\psi(g(x)).$$

Then we have

$$-\sum_\psi S_n(\chi;\psi_a,\psi_b) = \sum_{x\in\mathbb{F}_n^*}\chi(\mathrm{N}x)\sum_\psi \psi(\mathrm{Tr}(g(x))). \tag{12}$$

Note that the inner sum is $q^n + O(q^{n/2})$ by Theorem 2. We sum this equation over all Dirichlet character mod p, then we have

$$N_n' = -\sum_\chi\sum_\psi S_n(\chi;\psi_a,\psi_b) = \sum_\chi\sum_\psi\sum_{x\in\mathbb{F}_n^*}\chi(\mathrm{N}x)\psi(\mathrm{Tr}(g(x))).$$

This sum on the right-hand side denotes the number of solutions in the following equations

$$y^{q-1} = x,$$
$$z^q - z = ax + \frac{b}{x}.$$

with $x, y \in \mathbb{F}_n^*$, $z \in \mathbb{F}_n$.

We state more general version of Theorem 2, which is an extension of Stepanov's elementary methods due to Schmidt.

Theorem 3. *Suppose $f(X,Y) \in \mathbb{F}_q[X,Y]$ is absolutely irreducible and of total degree $d > 0$, let N be the number of zeros of f in $\mathbb{F}_q^2$. If $q > 250d^5$, then*

$$|N - q| < \sqrt{2}d^{5/2}q^{1/2}.$$

The equations we considered before can be put together as

$$z^q - z = ay^{q-1} + \frac{b}{y^{q-1}}$$

with $y \in \mathbb{F}_n^*$, $z \in \mathbb{F}_n$. In polynomial form, this is

$$-y^{2q-2} + (z^q - z)y^{q-1} - a = 0.$$

The polynomial on the left-hand side is absolutely irreducible by Eisenstein's criterion. Thus, we can apply Theorem 3 and obtain the number of solutions N of this equation is $q^n + O(q^{n/2})$.

When χ is trivial, we have an estimate for the inner sum $q^n + O(q^{n/2})$, hence we have

$$\sum_{\chi \neq \chi_0} \sum_{\psi} \sum_{x \in \mathbb{F}_n^*} \chi(\mathrm{N}x)\psi(\mathrm{Tr}(g(x))) = O(q^{n/2}). \tag{13}$$

Let $\alpha_{\chi,\psi}$, $\beta_{\chi,\psi}$ be the roots of Kloosterman sum $S(\chi; \psi_a, \psi_b)$ so that we have

$$S_n(\chi; \psi_a, \psi_b) = \alpha_{\chi,\psi}^n + \beta_{\chi,\psi}^n.$$

Then Lemma 4 and (13) give us the estimates $|\alpha_{\chi,\psi}| \leq \sqrt{q}$, $|\beta_{\chi,\psi}| \leq \sqrt{q}$. This concludes the proof of Theorem 1.

References

[1] H. Iwaniec, I. Kowalski, *Analytic Number Theory*, volume 53, AMS Colloquium Publications.
[2] W. Schmidt, *Equations Over Finite Fields: An Elementary Approach.* Second Edition, Kendrick Press.