L-FUNCTIONS FOR GAUSS AND JACOBI SUMS

KEITH CONRAD

1. Introduction

For a multiplicative character $\chi\colon \mathbf{F}_q^\times \to \mathbf{C}^\times$ and additive character $\psi\colon \mathbf{F}_q \to \mathbf{C}^\times$ on a finite field $\mathbf{F}_q$ of order q, their *Gauss sum* is

$$G(\chi, \psi) = \sum_{c \in \mathbf{F}_q} \chi(c)\psi(c),$$

where we extend χ to 0 by $\chi(0) = 0$. Here are two fundamental properties of Gauss sums.

(1) For nontrivial χ and ψ, $|G(\chi, \psi)| = \sqrt{q}$. (This is not true if one of the characters is trivial: if χ is trivial and ψ is not then $G(\chi, \psi) = -1$, if ψ is trivial and χ is not then $G(\chi, \psi) = 0$, and if χ and ψ are both trivial then $G(\chi, \psi) = q - 1$.)

(2) (Hasse–Davenport) For $n \geq 1$ let $\chi_n = \chi \circ \mathrm{N}_{\mathbf{F}_{q^n}/\mathbf{F}_q}$ and $\psi_n = \psi \circ \mathrm{Tr}_{\mathbf{F}_{q^n}/\mathbf{F}_q}$ be the liftings of χ and ψ to multiplicative and additive characters on $\mathbf{F}_{q^n}$. Then $-G(\chi_n, \psi_n) = (-G(\chi, \psi))^n$. (This suggests $-G(\chi, \psi)$ is more fundamental.)

We will show how both properties of Gauss sums can be interpreted as properties of L-functions on $\mathbf{F}_q[T]$: the first property says a certain L-function satisfies the Riemann hypothesis and the second property follows from comparing the additive (Dirichlet series) and multiplicative (Euler product) representations of an L-function. Analogous results for Jacobi sums, based on the same ideas, are sketched at the end.

2. Gauss sums and the Riemann Hypothesis

Dirichlet characters are group homomorphisms $(\mathbf{Z}/m)^\times \to \mathbf{C}^\times$ and have L-functions. For nonconstant M in $\mathbf{F}_q[T]$, the finite group $(\mathbf{F}_q[T]/M)^\times$ is analogous to $(\mathbf{Z}/m)^\times$ and we call any homomorphism $\eta\colon (\mathbf{F}_q[T]/M)^\times \to \mathbf{C}^\times$ a character mod M. Extend η to $\overline{0}$ by $\eta(\overline{0}) = 0$ and lift η to $\mathbf{F}_q[T]$ by declaring $\eta(A) = \eta(A \bmod M)$. This function η on $\mathbf{F}_q[T]$ is totally multiplicative, and by analogy to the definition of the L-function of a Dirichlet character we define the L-function of η to be

$$L(s, \eta) := \sum_{\text{monic } A} \frac{\eta(A)}{\mathrm{N}(A)^s} = \sum_{n \geq 0} \left(\sum_{\deg A = n} \eta(A) \right) \frac{1}{q^{ns}}$$

for $\mathrm{Re}(s) > 1$, where the inner sum runs over monic A of degree n and $\mathrm{N}(A) = |\mathbf{F}_q[T]/A| = q^{\deg A}$. Note the constant term of $L(s, \eta)$ is 1 (occurring for $A = 1$).

By the change of variables $u = 1/q^s$ we can view $L(s, \eta)$ as a formal power series in u:

$$\widetilde{L}(u, \eta) := \sum_{\text{monic } A} \eta(A) u^{\deg A} = \sum_{n \geq 0} \left(\sum_{\deg A = n} \eta(A) \right) u^n,$$

so $L(s, \eta) = \widetilde{L}(1/q^s, \eta)$.

Theorem 2.1. *If η is nontrivial then for $n \geq \deg M$ the coefficient of u^n vanishes.*

Proof. (This proof is taken from [2, p. 36].) For each monic A of degree n, write $A = MQ+R$ for $Q, R \in \mathbf{F}_q[T]$ with $R = 0$ or $\deg R < \deg M$. Since A is monic of degree n, Q is monic of degree $n - \deg M$. By uniqueness of the quotient and remainder for each A, as A runs over all monics of degree n the pair (Q, R) runs over all pairs of a monic Q of degree $n - \deg M$ and a polynomial R of degree less than $\deg M$ (including $R = 0$). Therefore

$$\sum_{\deg A = n} \eta(A) = \sum_{Q,R} \eta(MQ + R) = \sum_{Q,R} \eta(R) = q^{n-\deg M} \sum_{R} \eta(R)$$

since there are $q^{n-\deg M}$ choices of Q. Since R is running over the polynomials of degree less than M along with 0, which represents all of $\mathbf{F}_q[T]/M$, and η vanishes on polynomials having a factor in common with M, we have

$$\sum_{R} \eta(R) = \sum_{R \in (\mathbf{F}_q[T]/M)^\times} \eta(R) = 0$$

because the sum of a nontrivial character over a finite abelian group is 0. $\square$

Now focus on the case $\deg M = 2$. For nontrivial η the coefficient of u^n is 0 if $n \geq 2$, so

$$\widetilde{L}(u, \eta) = 1 + \left(\sum_{c \in \mathbf{F}_q} \eta(T + c) \right) u. \tag{2.1}$$

We will see that when $M = T^2$, the coefficient of u here is essentially a Gauss sum.

Theorem 2.2. *The characters of $(\mathbf{F}_q[T]/T^2)^\times$ are pairs of a multiplicative and additive character on $\mathbf{F}_q$.*

Proof. We unwind what the elements of $(\mathbf{F}_q[T]/T^2)^\times$ look like. To say $a + bT \bmod T^2$ is invertible means $a \neq 0$. By rewriting b as ab we can write the invertible elements as $a(1 + bT) \bmod T^2$ for $a \in \mathbf{F}_q^\times$ and $b \in \mathbf{F}_q$. Since

$$a(1 + bT)a'(1 + b'T) \equiv aa'(1 + (b + b')T) \bmod T^2,$$

we have an isomorphism

$$(\mathbf{F}_q[T]/T^2)^\times \cong \mathbf{F}_q^\times \times \mathbf{F}_q$$

by $a(1 + bT) \bmod T^2 \mapsto (a, b)$. Therefore the character group of $(\mathbf{F}_q[T]/T^2)^\times$ is the pairs (χ, ψ) for a multiplicative character $\chi\colon \mathbf{F}_q^\times \to \mathbf{C}^\times$ and an additive character $\psi\colon \mathbf{F}_q \to \mathbf{C}^\times$:

$$a(1 + bT) \bmod T^2 \mapsto \chi(a)\psi(b). \tag{2.2}$$

(Saying ψ is trivial is the same as saying this character mod T^2 can be defined modulo T, and thus is not "primitive" mod T^2.) $\square$

Returning to (2.1), the linear polynomials $T + c$ relatively prime to T^2 are those with $c \neq 0$, in which case $T + c = c(1 + (1/c)T)$, so if the character η on $(\mathbf{F}_q[T]/T^2)^\times$ is realized by (2.2) with χ or ψ nontrivial, so η is nontrivial, then the L-function of η is

$$\begin{aligned} 1 + \left(\sum_{c \in \mathbf{F}_q^\times} \chi(c)\psi(1/c) \right) u &= 1 + \left(\sum_{c \in \mathbf{F}_q^\times} \chi(1/c)\psi(c) \right) u \\ &= 1 + \left(\sum_{c \in \mathbf{F}_q^\times} \overline{\chi}(c)\psi(c) \right) u \\ &= 1 + G(\overline{\chi}, \psi)u. \end{aligned}$$

Replacing χ with $\overline{\chi}$ and u with $1/q^s$, the L-function of the character $a(1+bT) \bmod T^2 \mapsto \overline{\chi}(a)\psi(b)$ on $(\mathbf{F}_q[T]/T^2)^\times$ for nontrivial χ or ψ is

$$1 + \frac{G(\chi,\psi)}{q^s}.$$

For the complex zeros s of this L-function we have $|q^s| = |G(\chi,\psi)|$. Since $|q^s| = q^{\mathrm{Re}(s)}$, saying the zeros of this L-function satisfy the Riemann hypothesis – that is, the zeros have $\mathrm{Re}(s) = 1/2$ – is equivalent to saying $|G(\chi,\psi)| = \sqrt{q}$.

3. Euler products and the Hasse–Davenport relation

So far we have used only the additive representation of an L-function, as a Dirichlet series. Using the multiplicative representation, as an Euler product, we will relate the Gauss sum of characters χ and ψ on $\mathbf{F}_q$ with the Gauss sum of lifted characters on $\mathbf{F}_{q^n}$.

Theorem 3.1 (Hasse–Davenport). *For $n \geq 1$ let $\chi_n = \chi \circ \mathrm{N}_{\mathbf{F}_{q^n}/\mathbf{F}_q}$ and $\psi_n = \psi \circ \mathrm{Tr}_{\mathbf{F}_{q^n}/\mathbf{F}_q}$ be liftings of χ and ψ to characters on $\mathbf{F}_{q^n}$. If χ or ψ is nontrivial then $-G(\chi_n,\psi_n) = (-G(\chi,\psi))^n$.*

Proof. For any character $\eta\colon (\mathbf{F}_q[T]/M)^\times \to \mathbf{C}^\times$, its L-function has an Euler product:

$$\widetilde{L}(u,\eta) = \sum_{\text{monic } A} \eta(A) u^{\deg A} = \prod_{\text{monic } \pi} \frac{1}{1-\eta(\pi)u^{\deg \pi}},$$

where π runs over monic irreducibles (with $\eta(\pi) = 0$ if $\pi \mid M$). Using the power series identity $1/(1-au) = \exp(\sum_{k\geq 1} (au)^k/k)$, we can write $\widetilde{L}(u,\eta)$ as an exponential:

$$\begin{aligned} \widetilde{L}(u,\eta) &= \prod_{\text{monic } \pi} \exp\left(\sum_{k\geq 1} \frac{\eta(\pi)^k}{k} u^{k \deg \pi}\right) \\ &= \exp\left(\sum_{\text{monic } \pi} \sum_{k\geq 1} (\deg \pi)\eta(\pi)^k \frac{u^{k\deg \pi}}{k \deg \pi}\right) \\ &= \exp\left(\sum_{n\geq 1}\left(\sum_{d\mid n} \sum_{\deg \pi = d} d\eta(\pi)^{n/d}\right)\frac{u^n}{n}\right). \end{aligned}$$

We will write the two innermost sums as a single sum over the elements of $\mathbf{F}_{q^n}$. Each monic irreducible π in $\mathbf{F}_q[T]$ of degree d has d distinct roots, and the roots lie in $\mathbf{F}_{q^n}$ when $d \mid n$. The term $d\eta(\pi)^{n/d}$ can be regarded as a contribution of $\eta(\pi)^{n/d}$ from each of the d roots of π. For $\alpha \in \mathbf{F}_{q^n}$, let π_α be its minimal polynomial over $\mathbf{F}_q$ and $d_\alpha = \deg \pi_\alpha$. Then

$$\sum_{d\mid n} \sum_{\deg \pi = d} d\eta(\pi)^{n/d} = \sum_{\alpha \in \mathbf{F}_{q^n}} \eta(\pi_\alpha)^{n/d_\alpha}. \tag{3.1}$$

Now set $M = T^2$ and $\eta(a(1+bT) \bmod T^2) = \overline{\chi}(a)\psi(b)$. This is nontrivial since χ or ψ is. For $f(T)$ relatively prime to T^2, set $f(T) \equiv a(1+bT) \bmod T^2$. Then $a = f(0) \neq 0$ and $ab = f'(0)$, so $b = f'(0)/f(0)$. Thus $\eta(f(T) \bmod T^2) = \overline{\chi}(f(0))\psi(f'(0)/f(0))$. If $f(T) = \pi(T)$ is monic irreducible and $\pi(0) \neq 0$ (that is, $\pi(T) \neq T$), then we can write $\overline{\chi}(\pi(0))\psi(\pi'(0)/\pi(0))$ in terms of a norm and trace of a root of π: letting $d = \deg \pi$ and $\alpha_1, \ldots \alpha_d$ be the roots of π in $\mathbf{F}_{q^n}$, for any root α of π we have $\pi(0) = (-1)^d(\alpha_1 \ldots \alpha_d) = \mathrm{N}_{\mathbf{F}_q(\alpha)/\mathbf{F}_q}(-\alpha)$ and

$$\frac{\pi'(T)}{\pi(T)} = \sum_{i=1}^{d} \frac{1}{T-\alpha_i} \Longrightarrow \frac{\pi'(0)}{\pi(0)} = \sum_{i=1}^{d} -\frac{1}{\alpha_i} = \mathrm{Tr}_{\mathbf{F}_q(\alpha)/\mathbf{F}_q}(-1/\alpha).$$

Therefore

$$\sum_{\alpha\in\mathbf{F}_{q^n}^\times}\eta(\pi_\alpha)^{n/d_\alpha}=\sum_{\alpha\in\mathbf{F}_{q^n}^\times}\overline{\chi}(\mathrm{N}_{\mathbf{F}_q(\alpha)/\mathbf{F}_q}(-\alpha))^{n/d_\alpha}\psi(\mathrm{Tr}_{\mathbf{F}_q(\alpha)/\mathbf{F}_q}(-1/\alpha))^{n/d_\alpha}.$$

Replacing α with $-1/\alpha$,

$$\begin{aligned}\sum_{\alpha\in\mathbf{F}_{q^n}^\times}\eta(\pi_\alpha)^{n/d_\alpha} &= \sum_{\alpha\in\mathbf{F}_{q^n}^\times}\overline{\chi}(\mathrm{N}_{\mathbf{F}_q(\alpha)/\mathbf{F}_q}(\alpha))^{-n/d_\alpha}\psi(\mathrm{Tr}_{\mathbf{F}_q(\alpha)/\mathbf{F}_q}(\alpha))^{n/d_\alpha}\\ &= \sum_{\alpha\in\mathbf{F}_{q^n}^\times}\chi(\mathrm{N}_{\mathbf{F}_q(\alpha)/\mathbf{F}_q}(\alpha))^{n/d_\alpha}\psi(\mathrm{Tr}_{\mathbf{F}_q(\alpha)/\mathbf{F}_q}(\alpha))^{n/d_\alpha}\\ &= \sum_{\alpha\in\mathbf{F}_{q^n}^\times}\chi\left(\mathrm{N}_{\mathbf{F}_q(\alpha)/\mathbf{F}_q}(\alpha)^{n/d_\alpha}\right)\psi\left(\frac{n}{d_\alpha}\mathrm{Tr}_{\mathbf{F}_q(\alpha)/\mathbf{F}_q}(\alpha)\right)\\ &= \sum_{\alpha\in\mathbf{F}_{q^n}^\times}\chi(\mathrm{N}_{\mathbf{F}_{q^n}/\mathbf{F}_q}(\alpha))\psi(\mathrm{Tr}_{\mathbf{F}_{q^n}/\mathbf{F}_q}(\alpha)),\end{aligned}$$

where the last step uses the transitivity of the norm and trace mappings. This sum over $\mathbf{F}_{q^n}^\times$ is the Gauss sum of the characters $\chi_n := \chi\circ\mathrm{N}_{\mathbf{F}_{q^n}/\mathbf{F}_q}$ and $\psi_n := \psi\circ\mathrm{Tr}_{\mathbf{F}_{q^n}/\mathbf{F}_q}$ on $\mathbf{F}_{q^n}$, so the right side of (3.1) for our character η mod T^2 is $G(\chi_n,\psi_n)$. Therefore

$$\widetilde{L}(u,\eta)=\exp\left(\sum_{n\geq 1}G(\chi_n,\psi_n)\frac{u^n}{n}\right).$$

At the same time, from Section 2

$$\widetilde{L}(u,\eta)=1+G(\chi,\psi)u=\exp\left(\sum_{n\geq 1}(-1)^{n-1}G(\chi,\psi)^n\frac{u^n}{n}\right).$$

Comparing coefficients of like powers of u in these two exponential formulas for $\widetilde{L}(u,\eta)$ we get $G(\chi_n,\psi_n)=(-1)^{n-1}G(\chi,\psi)^n$, or equivalently $-G(\chi_n,\psi_n)=(-G(\chi,\psi))^n$. □

This proof of the Hasse–Davenport relation is similar to the proof in [1, Chap. 11, Sec. 4], but that proof uses a multiplicative function λ on monic polynomials that isn't a character on any $(\mathbf{F}_q[T]/M)^\times$.

4. Jacobi sums

For two multiplicative characters χ_1 and χ_2 on $\mathbf{F}_q^\times$, their *Jacobi sum* is

$$J(\chi_1,\chi_2)=\sum_{c\in\mathbf{F}_{q^n}}\chi_1(c)\chi_2(1-c).$$

We will realize a Jacobi sum as the linear coefficient of an L-function for a character with modulus $T(T-1)$ rather than T^2.

Since $(\mathbf{F}_q[T]/T(T-1))^\times\cong\mathbf{F}_q^\times\times\mathbf{F}_q^\times$ by $f(T)$ mod $T(T-1)\mapsto(f(0),f(1))$, a character η mod $T(T-1)$ is a pair of multiplicative characters (χ_1,χ_2) on $\mathbf{F}_q^\times$: $\eta(f(T) \bmod T(T-1))=\chi_1(f(0))\chi_2(f(1))$. Assume χ_1 or χ_2 is nontrivial, so η is nontrivial. By the reasoning as in Section 2, since $T(T-1)$ has degree 2 the L-function of η as a series in u is

$$1+\left(\sum_{c\neq 0,-1}\eta(T+c)\right)u=1+\left(\sum_{c\neq 0,-1}\chi_1(c)\chi_2(1+c)\right)u$$

and the coefficient of u here is

$$\sum_{c\neq 0,-1}\chi_1(c)\chi_2(1+c)=\sum_{c\neq 0,1}\chi_1(-c)\chi_2(1-c)=\chi_1(-1)J(\chi_1,\chi_2),$$

which up to the sign $\chi_1(-1)=\pm 1$ is a Jacobi sum. Making the change of variables $u=1/q^s$ we can say

$$\sum_{\text{monic } A}\frac{\eta(A)}{\mathrm{N}(A)^s}=1+\frac{\chi_1(-1)J(\chi_1,\chi_2)}{q^s}. \tag{4.1}$$

It's a classical theorem that $|J(\chi_1,\chi_2)|=\sqrt{q}$ if χ_1 and χ_2 are both nontrivial, and we can interpret this as saying the zeros of (4.1) satisfy the Riemann hypothesis when χ_1 and χ_2 are nontrivial.

To get a Hasse–Davenport relation, write the L-function of η as an exponential in u:

$$1+\chi_1(-1)J(\chi_1,\chi_2)u=\exp\left(\sum_{n\geq 1}(-1)^{n-1}\chi_1(-1)^nJ(\chi_1,\chi_2)^n\frac{u^n}{n}\right).$$

By reasoning as in Section 3, if we set $\chi_{1,n}=\chi_1\circ\mathrm{N}_{\mathbf{F}_{q^n}/\mathbf{F}_q}$ and $\chi_{2,n}=\chi_2\circ\mathrm{N}_{\mathbf{F}_{q^n}/\mathbf{F}_q}$ then the reader can check that writing the L-function of η as an Euler product leads to

$$\begin{aligned}\prod_{\text{monic } \pi}\frac{1}{1-\eta(\pi)u^{\deg\pi}} &= \exp\left(\sum_{n\geq 1}\sum_{\alpha\in\mathbf{F}_{q^n}}\chi_{1,n}(-\alpha)\chi_{2,n}(1-\alpha)\frac{u^n}{n}\right)\\ &= \exp\left(\sum_{n\geq 1}\chi_{1,n}(-1)\sum_{\alpha\in\mathbf{F}_{q^n}}\chi_{1,n}(\alpha)\chi_{2,n}(1-\alpha)\frac{u^n}{n}\right)\\ &= \exp\left(\sum_{n\geq 1}\chi_{1,n}(-1)J(\chi_{1,n},\chi_{2,n})\frac{u^n}{n}\right),\end{aligned}$$

so a comparison of coefficients in the two exponential formulas for the L-function of η implies

$$\chi_{1,n}(-1)J(\chi_{1,n},\chi_{2,n})=(-1)^{n-1}\chi_1(-1)^nJ(\chi_1,\chi_2)^n.$$

Since $\chi_{1,n}(-1)=\chi_1(\mathrm{N}_{\mathbf{F}_{q^n}/\mathbf{F}_q}(-1))=\chi_1((-1)^n)=\chi_1(-1)^n$, we can cancel the common $\chi_1(-1)^n$ on both sides and get

$$-J(\chi_{1,n},\chi_{2,n})=(-J(\chi_1,\chi_2))^n$$

for all $n\geq 1$. This is a Hasse–Davenport relation for Jacobi sums.

References

[1] K. Ireland and M. Rosen, "A Classical Introduction to Modern Number Theory," 2nd ed., Springer-Verlag, New York, 1990.

[2] M. Rosen, "Number Theory in Function Fields," Springer-Verlag, New York, 2002.