On character sums and complex functions over finite fields

N. V. Proskurin

April 17, 2018

In this lecture I want to present the complex functions over finite fields theory. The theory has been developed through parallels with the classical functions theory. It includes: Gauss and Jacobi sums; other character (or trigonometric) sums; Fourier expansions, power series expansions, differentiations; hypergeometric functions and other special functions.

Notation for finite fields

* $\mathbb{F}_q$ — finite field of order $q = p^l$ with prime subfield $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$.
* $\mathbb{F}_q^\star$ — the multiplicative group of $\mathbb{F}_q$.
* $\mathrm{tr}\colon \mathbb{F}_q \to \mathbb{F}_p$ — the trace, $\mathrm{tr}(x) = x + x^p + \ldots + x^{p^{l-1}}$.
* $e_q\colon \mathbb{F}_q \to \mathbb{C}^\star$ — fixed (once for all) a non-trivial additive character (say, $e_q(x) = \exp\bigl(2\pi i\,\mathrm{tr}(x)/p\bigr)$ for all $x \in \mathbb{F}_q$).
* $\widehat{\mathbb{F}}_q^\star$ — the group of multiplicative characters, i. e. the group of homomorphisms $\chi\colon \mathbb{F}_q^\star \to \mathbb{C}^\star$ extended to all of $\mathbb{F}_q$ by $\chi(0) = 0$.
* ϵ — the trivial character, $\epsilon(x) = 1$ for all $x \in \mathbb{F}_q^\star$, $\epsilon(0) = 0$.
* $\delta(0) = 1$ and $\delta(x) = 0$ for all $x \in \mathbb{F}_q^\star$.

Gauss sum

The Gauss sum

$$G(\chi)=\sum_{x\in\mathbb{F}_q^\star}\chi(x)e_q(x),\quad \chi\in\widehat{\mathbb{F}}_q^\star,$$

being considered as a function $\widehat{\mathbb{F}}_q^\star\to\mathbb{C}$, is quite similar to the Euler gamma function

$$\Gamma(s)=\int\limits_0^\infty \exp(-x)\,x^{s-1}dx,\quad s\in\mathbb{C},\quad \operatorname{Re}s>0.$$

In detail, note that $x\mapsto\exp(-x)$ is a character of the additive group of $\mathbb{R}$, that $x\mapsto x^s$ is a character of the $\mathbb{R}_+^\star$, and that the integration over dx/x is invariant under multiplicative translations.

Jacobi sum

Similarly, we see that the Jacobi sum

$$J(\alpha,\beta)=\sum_{x\in\mathbb{F}_q}\alpha(x)\beta(1-x),\quad \alpha,\beta\in\widehat{\mathbb{F}}_q^{\star},$$

being considered as a function $\widehat{\mathbb{F}}_q^{\star}\times\widehat{\mathbb{F}}_q^{\star}\to\mathbb{C}$, is the analogue of the Euler beta function

$$B(a,b)=\int\limits_0^1 x^{a-1}(1-x)^{b-1}\,dx,\quad a,b\in\mathbb{C},$$

$\operatorname{Re} a>0,\ \operatorname{Re} b>0.$

more identities

A lot of identities satisfied by the gamma and beta functions have finite field analogues. Say, the formulas

$$G(\chi)\,G(\bar{\chi}) = \chi(-1)\,q \quad \text{and} \quad J(\alpha,\beta) = \frac{G(\alpha)\,G(\beta)}{G(\alpha\beta)}$$

with $\chi \neq \epsilon$ and $\alpha\beta \neq \epsilon$, are analogues of the reflection formula

$$\Gamma(s)\,\Gamma(1-s) = \frac{\pi}{\sin \pi s}$$

and the formula

$$B(a,b) = \frac{\Gamma(a)\Gamma(b)}{\Gamma(a+b)}$$

with $s, a, b \in \mathbb{C}$. The analogy observed dates back to the XIX century.

more advanced analogy

Given $s \in \mathbb{C}$ and integer $m \geq 1$, one has the multiplication formula

$$\prod_{n=0}^{m-1} \Gamma\left(s + \frac{n}{m}\right) = (2\pi)^{(m-1)/2} m^{1/2-ms} \Gamma(ms).$$

Given a character $\psi \in \widehat{\mathbb{F}_q^\star}$ and an integer $m|(q-1)$, we have a finite field counterpart of the multiplication formula. That is the Davenport–Hasse relation (1934)

$$\prod_{\chi} G(\psi\chi) = \left\{-\bar{\psi}(m)^m \prod_{\chi} G(\chi)\right\} G(\psi^m),$$

where the products range over $\chi \in \widehat{\mathbb{F}_q^\star}$ under the assumption $\chi^m = \epsilon$.

On cubic exponential and Kloosterman sums

A very instructive sample of analogy between classical special functions and character sums is given by Iwaniec and Duke (1993). Consider the integral representation

$$K_{1/3}(u) = u^{1/3} \int_0^\infty \exp\Big(-t - \frac{u^2}{4t}\Big) \frac{dt}{(2t)^{4/3}}$$

for the Bessel–Macdonald function and the Nicholson formula for the Airy integral

$$\int_0^\infty \cos(t^3 + tv)\, dt = \frac{v^{1/2}}{3} K_{1/3}(2(v/3)^{3/2}),$$

which are valid at least for real $u, v > 0$.

From these two formulas, it follows

$$\int\limits_{-\infty}^{\infty} \exp\big(i\,(cx^3+x)\big)\,dx = 3^{-1/2}\int\limits_{0}^{\infty}\Big(\frac{x}{c}\Big)^{1/3}\exp\Big(-x-\frac{1}{27cx}\Big)\frac{dx}{x}$$

with any real $c>0$. Assume $3|(q-1)$. This case there exists cubic character ψ of $\mathbb{F}_q^\star$ and cubic Kloosterman sums, which one can treat as analogue of the integral in the right-hand side. Following the analogue, Iwaniec and Duke deduced very important formula which relates cubic Kloosterman sum to cubic exponential sum. That is

$$\sum_{x\in\mathbb{F}_q} e_q(cx^3+x) = \sum_{x\in\mathbb{F}_q^\star}\psi(xc^{-1})\,e_q(x-(27cx)^{-1}) \quad \text{for} \quad c\in\mathbb{F}_q^\star.$$

The proof involves the Davenport–Hasse relation.

Elements of analysis

Consider the complex vector space Ω_q of all functions $\mathbb{F}_q \to \mathbb{C}$ supplied with the inner product

$$\langle f, g \rangle = \sum_{x \in \mathbb{F}_q} f(x)\overline{g(x)} \quad \text{for all} \quad f, g \in \Omega_q.$$

The additive characters $x \mapsto e_q(hx)$, $x, h \in \mathbb{F}_q$ form an orthogonal bases for the Ω_q.

The multiplicative characters $\chi \in \widehat{\mathbb{F}_q^\star}$ together with the function δ form an orthogonal bases for the Ω_q.

Additive Fourier transform

Given a function $F\colon \mathbb{F}_q \to \mathbb{C}$, its additive Fourier transform is the function $\hat{F}\colon \mathbb{F}_q \to \mathbb{C}$ defined by

$$\hat{F}(x) = \sum_{y\in\mathbb{F}_q} F(y)e_q(yx) \quad \text{for all } x \in \mathbb{F}_q.$$

The Fourier inversion formula

$$F(z) = \frac{1}{q}\sum_{x\in\mathbb{F}_q} \hat{F}(x)e_q(-xz) \quad \text{for all } z \in \mathbb{F}_q$$

allows one to recover F from $\hat{F}$ and can be considered as the expansion of F over basis consisting of additive characters.

Multiplicative Fourier transform

Given a function $F\colon \mathbb{F}_q^\star \to \mathbb{C}$, its multiplicative Fourier transform is the function $\widehat{F}\colon \widehat{\mathbb{F}}_q^\star \to \mathbb{C}$ defined by

$$\widehat{F}(\chi) = \sum_{x\in\mathbb{F}_q^\star} F(x)\chi(x) \quad \text{for all } \chi \in \widehat{\mathbb{F}}_q^\star.$$

The Fourier inversion formula

$$F(z) = \frac{1}{q-1} \sum_{\chi\in\widehat{\mathbb{F}}_q^\star} \widehat{F}(\chi)\bar{\chi}(z) \quad \text{for all } z \in \mathbb{F}_q^\star$$

allows one to recover F from $\widehat{F}$.

Power series expansion

Given a function $F\colon \mathbb{F}_q \to \mathbb{C}$, one has a similar expansion with one additional term

$$F(z) = F(0)\,\delta(z) + \sum_{\chi \in \widehat{\mathbb{F}_q^\star}} C_\chi\, \chi(z) \quad \text{with} \quad C_\chi = \frac{1}{q-1}\,\widehat{F}(\bar{\chi}).$$

One can treat the sum over χ as the sum over $\epsilon, \rho, \rho^2, \dots \rho^{q-1}$, whenever ρ generates the group $\widehat{\mathbb{F}_q^\star}$. So, that is a finite field analogue of power series expansion.

Binomial formula

By Green (1987), given $\rho \in \widehat{\mathbb{F}_q^\star}$ and $x \in \mathbb{F}_q$, one has the expansion

$$\rho(1+x) = \delta(x) + \frac{q}{q-1} \sum_{\chi \in \widehat{\mathbb{F}_q^\star}} \binom{\rho}{\chi} \chi(x) \quad \text{with} \quad \binom{\rho}{\chi} = \frac{\chi(-1)}{q} J(\rho, \bar{\chi}),$$

which is a finite field analogue of the classical binomial formula

$$(1+x)^r = \sum_{k=0}^{r} \binom{r}{k} x^k \quad \text{with} \quad \binom{r}{k} = \frac{r!}{(r-k)!\, k!}, \quad x \in \mathbb{C}.$$

Expansion for the exponent

For another example, let F be additive character e_q. One has

$$e_q(-z) = 1 + \frac{q}{q-1} \sum_{\chi \in \widehat{\mathbb{F}}_q^\star} \frac{\chi(z)}{G(\chi)} \quad \text{for all} \quad z \in \mathbb{F}_q.$$

That is a finite field analogue for the power series expansion for the exponent,

$$e(z) = 1 + \sum_{n=1}^{\infty} \frac{z^n}{n!} \quad \text{for all} \quad z \in \mathbb{C}.$$

Differentiation

Given character $\chi \in \widehat{\mathbb{F}_q^\star}$, define the linear operator $D^\chi \colon \Omega_q \to \Omega_q$ by

$$D^\chi F(x) = \frac{1}{G(\bar\chi)} \sum_{t \in \mathbb{F}_q} F(t)\, \bar\chi(x-t)$$

for all $F \colon \mathbb{F}_q \to \mathbb{C}$ and $x \in \mathbb{F}_q$. If $\chi \neq \epsilon$, one can rewrite this as

$$\frac{1}{G(\chi)} D^\chi F(x) = \frac{1}{q} \sum_{t \in \mathbb{F}_q} F(t)\, \bar\chi(t-x).$$

This should be compared with the Cauchy integral formula

$$\frac{1}{n!}\, f^{(n)}(x) = \frac{1}{2\pi i} \int \frac{f(t)\, dt}{(t-x)^{n+1}}$$

for the derivative $f^{(n)}$ of any order n of the analytic function f.

By Evans (1986), $D^{\chi}F$ is the derivative of order χ of F. One finds easily some standard properties.

* D^{χ} takes constant functions to zero function, whenever $\chi \neq \epsilon$.
* $D^{\alpha}D^{\beta} = D^{\alpha\beta}$ for characters $\alpha, \beta \in \widehat{\mathbb{F}}_q^{\star}$ subject to $\alpha\beta \neq \epsilon$.
* $D^{\epsilon}F(x) = F(x) - \sum_{t\in\mathbb{F}_q} F(t)$, with F and x as above.

Given two functions E and F, $x \in \mathbb{F}_q$, and the character ν we have the formula for integration by parts

$$\sum_{x\in\mathbb{F}_q} E(x)\, D^{\nu}F(x) = \nu(-1) \sum_{x\in\mathbb{F}_q} F(x)\, D^{\nu}E(x)$$

and the Leibniz rule for the ν-th derivative of the product

$$D^{\nu}EF(x) = \frac{1}{q-1} \sum_{\mu\in\widehat{\mathbb{F}}_q^{\star}} \frac{G(\bar{\mu})\, G(\mu\bar{\nu})}{G(\bar{\nu})}\, D^{\mu}E(x)\, D^{\nu\bar{\mu}}F(x).$$

* Given any character ν, let $F(x) = e_q(-x)$ for all $x \in \mathbb{F}_q$. This case we have $D^\nu F = F$.
* For any $F\colon \mathbb{F}_q \to \mathbb{C}$ and $a \in \mathbb{F}_q$, we have expansion

$$F(x) = \frac{1}{q-1} \sum_{\nu \in \widehat{\mathbb{F}}_q^\star} G(\bar{\nu})\, D^\nu F(a)\, \nu(a-x)$$

for all $x \in \mathbb{F}_q$, $x \neq a$. That is a finite field analogue of the Taylor expansion.

Hermite character sums

Given any character $\nu \in \widehat{\mathbb{F}}_q^\star$ and $x \in \mathbb{F}_q$, let

$$H_\nu(x) = \frac{1}{G(\bar{\nu})} \sum_{u \in \mathbb{F}_q} \bar{\nu}(u) e_q(u^2 + 2ux).$$

That is given by Evans (1986) as a finite field analogue of the classical Hermite polynomials H_n, $n \geq 0$. We have

$$H_n(-x) = (-1)^n H_n(x) \text{ for all } x \in \mathbb{R} \text{ and integer } n \geq 0;$$

$$H_\nu(-x) = \nu(-1)\, H_\nu(x) \text{ for all } x \in \mathbb{F}_q,\ \nu \in \widehat{\mathbb{F}}_q^\star.$$

Also, for all $x \in \mathbb{F}_q$, one has

$$H_\nu(x) = \nu(-1)F(x)^{-1}D^\nu F(x), \quad \text{where} \quad F(x) = e_q(x^2).$$

That is a finite field analogue of the Rodriguez formula

$$H_n(x) = (-1)^n \exp(x^2)\frac{d^n}{dx^n}\exp(-x^2), \quad x \in \mathbb{R},$$

for the classical Hermite polynomials H_n.

In a similar manner one can treat the Legendre polynomials, the Bessel functions and other classical polynomials and some special functions.

Hypergeometric functions

For the hypergeometric function ${}_2F_1$ one has the Euler integral representation

$$ {}_2F_1(a,b;c;x) = \frac{\Gamma(c)}{\Gamma(b)\,\Gamma(c-b)} \int\limits_0^1 t^b (1-t)^{c-b} (1-xt)^{-a} \frac{dt}{t\,(1-t)}. $$

Greene (1987) defined the hypergeometric functions on $\mathbb{F}_q$ by

$$ {}_2F_1\left[\begin{matrix}\alpha, & \beta \\ & \gamma\end{matrix}\,\middle|\, x\right] = \epsilon(x)\,\frac{\beta\gamma(-1)}{q} \sum_{t\in\mathbb{F}_q} \beta(t)\,\bar{\beta}\gamma(1-t)\,\bar{\alpha}(1-xt) $$

for any characters $\alpha, \beta, \gamma \in \widehat{\mathbb{F}_q^\star}$ and $x \in \mathbb{F}_q$.

With this definition and notation one has power series expansion

$$ {}_2F_1\left[\begin{matrix}\alpha,\ \beta\\ \gamma\end{matrix}\,\middle|\, x\right] = \frac{q}{q-1}\sum_{\chi\in\widehat{\mathbb{F}}_q^\star}\binom{\alpha\chi}{\chi}\binom{\beta\chi}{\gamma\chi}\chi(x), $$

and one has the more general definition

$$ {}_{n+1}F_n\left[\begin{matrix}\alpha_0,\alpha_1,\dots,\alpha_n\\ \beta_1,\dots,\beta_n\end{matrix}\,\middle|\, x\right] = \frac{q}{q-1}\sum_{\chi\in\widehat{\mathbb{F}}_q^\star}\binom{\alpha_0\chi}{\chi}\binom{\alpha_1\chi}{\beta_1\chi}\dots\binom{\alpha_n\chi}{\beta_n\chi}\chi(x) $$

for any integer $n\geq 1$ and characters $\alpha_0,\dots\beta_n\in\widehat{\mathbb{F}}_q^\star$.

Like their classical counterparts, hypergeometric functions over finite fields satisfy many transformation identities. Say, for classical Pfaff's transformation

$$ {}_2F_1(a,b;c;x) = (1-x)^{-a}\,{}_2F_1\big(a,c-b;c;x/(x-1)\big) $$

one has finite field analogue

$$ {}_2F_1\left[\begin{matrix}\alpha,\ \beta\\ \gamma\end{matrix}\,\middle|\, x\right] = \bar{\beta}(1-x)\,{}_2F_1\left[\begin{matrix}\bar{\alpha}\gamma,\ \beta\\ \gamma\end{matrix}\,\middle|\, \frac{x}{x-1}\right] $$

for any characters $\alpha, \beta, \gamma \in \widehat{\mathbb{F}_q^\star}$ and $x \in \mathbb{F}_q$, $x \neq 1$.

Turn to the function ${}_3F_2$. In the classical context, there are some summation formulas. We mean the formulas of Saalschütz, Dixon, Watson, Whipple. One has finit field analogues for each of them. Say, as analogue for Saalschütz's formula one has

$$ {}_3F_2\left[\begin{matrix}\alpha, & \beta, & \gamma \\ \rho, & \alpha\beta\gamma\bar{\rho} & \end{matrix}\Big| 1\right] = \beta\gamma(-1)\binom{\gamma}{\bar{\alpha}\rho}\binom{\beta}{\bar{\gamma}\rho} - \frac{1}{q}\beta\rho(-1)\binom{\bar{\beta}\rho}{\alpha}. $$

As one more example, consider Clausen's famous identity

$$ {}_3F_2(2c-2s-1, 2s, c-1/2; 2c-1, c; x) = {}_2F_1(c-s-1/2, s; c; x)^2, $$

which was utilized in de Branges' proof of the Bieberbach conjecture. By Evans and Greene (2009), one has a finite field analogue of this formula. That is

$$ {}_3F_2\left[\begin{matrix} \bar{\alpha}^2\gamma^2, & \alpha^2, & \gamma\phi \\ & \gamma^2, & \gamma \end{matrix} \middle| x\right] $$

$$ = -\frac{\bar{\gamma}(x)\,\phi(1-x)}{q} + \frac{\bar{\gamma}(4)\,J(\alpha\bar{\gamma}, \alpha\bar{\gamma})}{J(\alpha, \alpha)}\,{}_2F_1\left[\begin{matrix} \bar{\alpha}\gamma\phi, & \alpha \\ & \gamma \end{matrix} \middle| x\right]^2, $$

where $x \in \mathbb{F}_q$, $x \neq 1$, ϕ is the quadratic character ($\phi \neq \epsilon$, $\phi^2 = \epsilon$), and it is assumed that $\gamma \neq \phi$, $\alpha^2 \neq \epsilon, \gamma, \gamma^2$.

A study of special function analogues over finite fields serve as a useful tool when applied to problems related to character sums.

One can find Magma code to compute the hypergeometric functions over finite fields in Lennon's dissertation (2006).