Notes on character sums and complex functions over finite fields

N. V. Proskurin

Abstract. The intent of this notes is to present briefly the complex functions over finite fields theory. That includes: (a) additive and multiplicative characters; (b) Gauss and Jacobi sums, other trigonometric sums; (c) Fourier expansion, power series expansion, differentiation; (d) special functions like Hermit polynomials, hypergeometric functions and so on. The theory has been developed through parallels with the classical functions theory. The basis for this parallel is the analogy between Gauss sums and the gamma function.

1. Preliminaries

The notation we use is very standard, and we only summarize here the most common. Given prime p, let $\mathbb{F}_q$ be the finite field with $q = p^l$ elements and with prime subfield $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. Let trace: $\mathbb{F}_q \to \mathbb{F}_p$ be the trace function. We write $\mathbb{F}_q^\star$ for the multiplicative group of $\mathbb{F}_q$. Fix (once for all) a non-trivial additive character $e_q\colon \mathbb{F}_q \to \mathbb{C}^\star$. With some $h \in \mathbb{F}_q^\star$, one has $e_q(x) = \exp\bigl(2\pi i \operatorname{trace}(hx)/p\bigr)$ for all $x \in \mathbb{F}_q$. We write $\widehat{\mathbb{F}}_q^\star$ for the group of multiplicative characters of $\mathbb{F}_q$, i. e. for the group of homomorphisms $\chi\colon \mathbb{F}_q^\star \to \mathbb{C}^\star$. Extend each multiplicative character χ to all of $\mathbb{F}_q$ by setting $\chi(0) = 0$. We write ϵ for the trivial character, $\epsilon(x) = 1$ for all $x \in \mathbb{F}_q^\star$, $\epsilon(0) = 0$. Define $\delta\colon \mathbb{F}_q \to \mathbb{C}$ by setting $\delta(0) = 1$ and $\delta(x) = 0$ for all $x \in \mathbb{F}_q^\star$.

2. Background

The Gauss sum $G(\chi) = \sum\limits_{x \in \mathbb{F}_q^\star} \chi(x) e_q(x)$ with $\chi \in \widehat{\mathbb{F}}_q^\star$, being considered as complex function on $\widehat{\mathbb{F}}_q^\star$, is quite similar to the Euler gamma function

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

For better understanding, note that $x \mapsto \exp(-x)$ is a character of the additive group of real numbers field, that $x \mapsto x^s$ is a character of the multiplicative group of positive real numbers, and that the integration over dx/x is invariant under multiplicative translations. Similarly, we see that the Jacobi sum

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

is the analogue of the Euler beta function

$$B(a,b) = \int_0^1 x^{a-1}(1-x)^{b-1}\,dx \quad \text{for} \quad a,b\in\mathbb{C},\ \operatorname{Re} a>0,\ \operatorname{Re} b>0.$$

It occurs that a lot of identities satisfied by the gamma and beta functions have finite field analogues. Say, the formulas

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

where $\chi\neq\epsilon$ and $\alpha\beta\neq\epsilon$, are the finite field analogues of the reflection formula

$$\Gamma(s)\,\Gamma(1-s) = \frac{\pi}{\sin\pi s} \quad \text{for} \quad s\in\mathbb{C}$$

and

$$B(a,b) = \frac{\Gamma(a)\Gamma(b)}{\Gamma(a+b)} \quad \text{with} \quad a,b\in\mathbb{C}.$$

The analogy observed dates back to the nineteenth century. For more advanced analogy we may look on the Gauss multiplication formula for the gamma function,

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

with any $s\in\mathbb{C}$ and integer $m\geq 1$. Given a finite field $\mathbb{F}_q$, 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 [1] relation

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

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

3. 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 [2]. 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 positive u, v. From these two formulas, it follows

$$\int_{-\infty}^{\infty} \exp\bigl(i\,(cx^3+x)\,\bigr)\,dx = 3^{-1/2}\int_0^\infty \Bigl(\frac{x}{c}\Bigr)^{1/3} \exp\Bigl(-x-\frac{1}{27cx}\,\Bigr)\frac{dx}{x}$$

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 in [2] involves Davenport–Hasse relation and Fourier transform. For extended result see [3].

4. 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 form an orthogonal bases for the Ω_q. 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.

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 $\widehat{F}$. 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. The multiplicative characters together with δ form an orthogonal bases for the Ω_q.
For example, 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 finite field analogue of the classical binomial formula

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

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. We refer to Greene [4] for both examples and for properties of the binomial coefficients.

5. 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 $x \in \mathbb{F}_q$. We find easily

$$D^\epsilon F(x) = F(x) - \sum_{t \in \mathbb{F}_q} F(t),$$

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

for all F and x as above and $\chi \neq \epsilon$. According to Evans [5], $D^\chi F$ is the derivative of order χ of F. This definition is motivated by 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 function f.
One finds easily some standard properties. Say, D^χ takes constant functions to zero function, whenever $\chi \neq \epsilon$. Then, $D^\alpha D^\beta = D^{\alpha\beta}$ for characters α, β subject to $\alpha\beta \neq \epsilon$. Also, 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 function $F\colon \mathbb{F}_q \to \mathbb{C}$ 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.

6. Hermite character sums

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

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

The definition is given in [5] as finite field analogue of the classical Hermite polynomials. We find in [5] a lot of formulas involving the character sums H_ν which are quite similar to that for the Hermite polynomials H_n. Say, we have $H_n(-x) = (-1)^n H_n(x)$ for all $x \in \mathbb{R}$ and integer $n \geq 0$, and we have $H_\nu(-x) = \nu(-1)\, H_\nu(x)$ 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 special functions.

7. 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 [4] defined the hypergeometric functions on $\mathbb{F}_q$ by

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

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

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

and one has the more general definition

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

for any integer $n \ge 1$ and characters $\alpha_0,\ldots\beta_n \in \widehat{\mathbb{F}}_q^\star$.
Like their classical counterparts, hypergeometric functions over finite fields satisfy many transformation identities. Say, as analogue for Pfaff's transformation [6], [4] we have

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

for any characters $\alpha,\beta,\gamma \in \widehat{\mathbb{F}}_q^\star$ and $x \in \mathbb{F}_q$, $x \ne 1$.
Let us turn to the function ${}_3F_2$. In the classical context, there are some summation formulas. We mean the formulas of Saalschütz, Dixon, Watson, Whipple. Greene [4] gives analogues for each of them. Say, as analogue for Saalschütz's formula [6] we have

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

As one more example, consider Clausen's famous classical identity [7]

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

which was utilized in de Branges' proof of the Bieberbach conjecture. By Evans and Greene [8], one has a finite field analogue of this formula. That is

$$ {}_3F_2\Big[\begin{matrix}\bar\alpha^2\gamma^2, & \alpha^2, & \gamma\phi\\ & \gamma^2, & \gamma\end{matrix}\Big|\, x\Big] = -\frac{\bar\gamma(x)\,\phi(1-x)}{q} + \frac{\bar\gamma(4)\,J(\alpha\bar\gamma,\alpha\bar\gamma)}{J(\alpha,\alpha)}\,{}_2F_1\Big[\begin{matrix}\bar\alpha\gamma\phi,\ \alpha\\ \gamma\end{matrix}\Big|\, x\Big]^2, $$

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

A study of special function analogues over finite fields serve as a useful tool when applied to problems related to character sums. For more transformation formulas, farther developments and applications we refer to [9, 10, 11, 12, 13, 14, 15]. One can find Magma code to compute the hypergeometric functions over finite fields in the dissertation [10].

References

[1] H. Davenport and H. Hasse, *Die Nullstellen der Kongruenzzetafunktionen in gewissen zyklischen Fällen*, J. reine angew. Math., **172**, 1934, 151–182.

[2] W. Duke and H. Iwaniec, *A relation between cubic exponential and Kloosterman sums*, Contemporary Mathematics, **143**, 1993, 255–258.

[3] Zhengyu Mao, *Airy sums, Kloosterman sums, and Salié sums*, Journal of Number Theory, **65**, 1997, 316–320.

[4] J. Greene, *Hypergeometric functions over finite fields*, Transactions of the American Math. Soc., **301**, No. 1, 77–101, 1987.

[5] R. J. Evans, *Hermite character sums*, Pacific Journal of Mathematics, **122**, No. 2, 357–390, 1986.

[6] L. Slater, *Generalized hypergeometric functions*, Cambridge Univ. Press, 1966.

[7] W. N. Bailey, *Generalized hypergeometric series*, Strechert–Hafner, New York, 1964.

[8] R. Evans, J. Greene, *Clausen's theorem and hypergeometric functions over finite fields*, Finite Fields and Their Applications **15**, 2009, 97–109.

[9] J. Greene, D. Stanton, *A character sum evaluation and Gaussian hypergeometric series*, Journal of Number Theory, **23**, no. 1, 136–148, 1986.

[10] C. Lennon, *Arithmetic and analytic properties of finite field hypergeometric functions*, Submitted for the degree of PhD at the Massachusetts Inst. of technology, June 2006.

[11] J. Rouse, *Hypergeometric functions and elliptic curves*, Ramanujan Journal, **12**, no. 2, 197–205, 2006.

[12] R. Barman, G. Kalita *Elliptic curves and special values of Gaussian hypergeometric series*, Journal of Number Theory, **133**, issue 9, pages 3099–3111, September 2013.

[13] A. Deines, J. G. Fuselier, L. Long, H. Swisher, Fang-Ting Tu, *Hypergeometric series, truncated hypergeometric series, and Gaussian hypergeometric functions*, Directions in Number Theory, Springer, Cham. Association for women in mathematics series, vol. 3, 2016.

[14] J. Fuselier, L. Long, R. Ramakrishna, H. Swisher, Fang-Ting Tu, *Hypergeometric functions over finite fields*, arXiv:1510.02575v2 [math.NT], 1 April 2016.

[15] R. Evans, J. Greene, *A quadratic hypergeometric ${}_2F_1$ transformation over finite fields*, Proc. Amer. Math. Soc. **145**, 2017, 1071–1076.

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