ON QUADRATIC CHARACTER SUMS OVER QUARTICS

BOGDAN NICA

Abstract. We obtain transformation formulas for quadratic character sums with quartic and cubic polynomial arguments.

1. Introduction

Let σ denote the quadratic character on $\mathbb{F}_q$, the finite field with q elements. Throughout, we assume that char $\mathbb{F}_q \neq 2, 3$. This note is concerned with quadratic character sums of the form

$$\sum_{x \in \mathbb{F}_q} \sigma(f(x)). \tag{S_f}$$

Here $f(x)$ is a monic polynomial with coefficients in $\mathbb{F}_q$, usually required to be square-free. The quadratic character sum (**??**) is intimately related to the number of $\mathbb{F}_q$-points on the curve $y^2 = f(x)$:

$$\#\big\{(x, y) \in \mathbb{F}_q \times \mathbb{F}_q : y^2 = f(x)\big\} = q + \sum_{x \in \mathbb{F}_q} \sigma(f(x)).$$

The evaluation of the quadratic character sum (**??**) is easily settled in the case when the monic polynomial $f(x)$ is linear or quadratic:

$$\sum_{x \in \mathbb{F}_q} \sigma(f(x)) = \begin{cases} 0 & \text{if } \deg f = 1, \\ -1 & \text{if } \deg f = 2. \end{cases} \tag{1}$$

When $f(x)$ has degree 3 or higher, explicit evaluations are known only for sporadic families of polynomials. Still, there are several viewpoints that afford considerable insight. How does a quadratic character sum (**??**) *grow*, in terms of the degree of f? This is the search for estimates, a celebrated example being the Hasse–Weil bound. How does a quadratic character sum (**??**) *vary*, as we change (some of) the coefficients for f? This is the statistical viewpoint; we owe to Birch [**?**] an early work in this rich vein, but see also [**?**]. How do quadratic character sums of the form (**??**) *relate* to each other? This is the pursuit of transformation formulas–namely, identities between quadratic character sums associated to two different polynomials. Skillful usage of such transformation formulas often leads to new explicit evaluations of quadratic character sums.

Date: July 16, 2025.

2010 *Mathematics Subject Classification.* Primary: 11L10. Secondary: 11G05.

Key words and phrases. Character sums. Elliptic curves over finite fields.

An illustrative example of a transformation formula for quadratic character sums is the following: for all $b, c \in \mathbb{F}_q$ we have

$$\sum_{x\in\mathbb{F}_q} \sigma(x)\sigma(x^2+bx+c) = \sum_{x\in\mathbb{F}_q} \sigma(x+b)\sigma(x^2-4c). \tag{2}$$

This cubic-to-cubic transformation formula was first obtained by Jacobsthal [**?**], and rediscovered in [**?**, Thm.1]. Compare also the prime case of [**?**, Thm.1.2].

Another example is the following transformation formula: for all $a \in \mathbb{F}_q$ we have

$$\sum_{x\in\mathbb{F}_q} \sigma(x^5+ax^3+x) = \big(1+\sigma(-1)\big) \sum_{x\in\mathbb{F}_q} \sigma\big(x^3+4x^2+(a+2)x\big). \tag{3}$$

This is due to Leprévost and Morain [**?**, Thm.1]. See [**?**, Exer.5.29, Thm.5.20] for generalizations. Compare also results in [**?**, Secs.4,5]. The transformation formula (**??**) is a descent formula: it lowers the degree of the polynomial argument–in some sense, its complexity–from quintic, on the left-hand side, to cubic, on the right-hand side.

2. Transformation formulas over quartics

In this note, we are interested in transformation formulas for quadratic character sums of the form (**??**), in which $f(x)$ is a quartic polynomial.

A simple, yet useful example is the following descent formula for biquadratics: if $b, c \in \mathbb{F}_q$ satisfy $b^2 \neq 4c$ then

$$\sum_{x\in\mathbb{F}_q} \sigma(x^4+bx^2+c) = -1 + \sum_{x\in\mathbb{F}_q} \sigma(x^3+bx^2+cx). \tag{4}$$

This is an instance of a more general descent principle: for any polynomial $g(x)$ we have

$$\sum_{x\in\mathbb{F}_q} \sigma(g(x^2)) = \sum_{x\in\mathbb{F}_q} (1+\sigma(x))\sigma(g(x)) = \sum_{x\in\mathbb{F}_q} \sigma(g(x)) + \sum_{x\in\mathbb{F}_q} \sigma(xg(x)).$$

Taking $g(x) = x^2+bx+c$, in which case $\sum_{x\in\mathbb{F}_q} \sigma(g(x)) = -1$, we get (**??**).

The next descent formula was obtained, in a slightly different form, by Williams [**?**]; see also [**?**, Thm.5.10]. Compared to (**??**), its algebraic origin is harder to detect.

Theorem 2.1. *Let $f(x) = (x^2+b_1x+c_1)(x^2+b_2x+c_2)$ be square-free. Then*

$$\sum_{x\in\mathbb{F}_q} \sigma(f(x)) = -1 + \sum_{x\in\mathbb{F}_q} \sigma\big(x^3+Bx^2+\Delta_1\Delta_2x\big) \tag{5}$$

where $\Delta_1 = b_1^2-4c_1$, $\Delta_2 = b_2^2-4c_2$, and $B = 4(c_1+c_2)-2b_1b_2$.

There is, in fact, a general quartic-to-cubic descent formula. It reads as follows.

Theorem 2.2. *Let $f(x) = x^4 + a_3x^3 + a_2x^2 + a_1x + a_0$ be square-free. Then*

$$\sum_{x\in\mathbb{F}_q} \sigma(f(x)) = -1 + \sum_{x\in\mathbb{F}_q} \sigma(g(x)) \tag{6}$$

where $g(x) = x^3 + a_2x^2 + (a_1a_3 - 4a_0)x + a_0(a_3^2 - 4a_2) + a_1^2$.

Despite its generality, the descent formula (**??**) does not supplant other quartic-to-cubic descent formulas such as (**??**) or (**??**). For neither one of (**??**) or (**??**) is an instance of (**??**), as one might naively hope; and while they can be eventually derived from (**??**), additional ingredients are needed. It turns out that Jacobsthal's cubic-to-cubic formula (**??**) gets used in deriving both (**??**) from (**??**), as well as (**??**) from (**??**). The latter derivation, (**??**) from (**??**), is spelled out in Remark **??**.

We have first arrived at Theorem **??** by interpreting, in the language of quadratic character sums, a well-known fact from the theory of elliptic curves–that a quartic curve $y^2 = f(x)$ can be turned into a cubic curve $y^2 = g(x)$ by means of a rational change of variables over the coefficient field. This fact is seemingly due to Mordell [**?**, p.77]. Here is a convenient version of Mordell's procedure, after Nagao [**?**, p.153]: the curve $y^2 = x^4 + a_3x^3 + a_2x^2 + a_1x + a_0$ turns into $Y^2 = X^3 + a_2X^2 + (a_1a_3 - 4a_0)X + a_0(a_3^2 - 4a_2) + a_1^2$ under the change of variables

$$x := \frac{2(Y - a_1) - a_3X}{4(X + a_2) - a_3^2}, \qquad y := \frac{2x^2 + a_3x - X}{2}.$$

There is a visible issue at $X = -a_2 + a_3^2/4$, which ends up accounting for the -1 term in (**??**).

The search for a direct proof of Theorem **??**, which avoids elliptic curves and rational transformations, led us to a rather general transformation formula. The 'master formula' requires some notational set-up so we will not state it here. Let us emphasize instead its flexibility as a unified tool. Generically, the master formula yields quartic-to-quartic transformation formulas, a sample result being the following.

Theorem 2.3. *Let $a, b, c \in \mathbb{F}_q$ with $c \neq 0$. Then*

$$\sum_{x\in\mathbb{F}_q} \sigma\big(x^4 + (2a - 4b)x^2 - 4cx + a^2\big) = \sum_{x\in\mathbb{F}_q} \sigma\big(x^4 + (2b - 4a)x^2 - 4cx + b^2\big).$$

But we can also use the master formula in order to derive the quartic-to-cubic descent formulas of Theorem **??** and Theorem **??**, and even cubic-to-cubic transformation formulas.

We obtain the master formula in Section **??**, and then we derive the transformation formulas in Section **??**. In Section **??** we discuss some concrete examples.

3. The master formula

The starting point is the idea that a transformation formula is an identity arising from double-counting. Consider a quartic form in two variables u and x, with coefficients in $\mathbb{F}_q$, given by

$$F(u,x)=\begin{pmatrix}u^2\\ u\\ 1\end{pmatrix}^T\begin{pmatrix}a_1 & a_2 & a_3\\ b_1 & b_2 & b_3\\ c_1 & c_2 & c_3\end{pmatrix}\begin{pmatrix}x^2\\ x\\ 1\end{pmatrix}. \tag{7}$$

The quartic $F(u,x)$ can be expanded in two ways: as a quadratic in u,

$$F(u,x)=\alpha(x)u^2+\beta(x)u+\gamma(x) \tag{8}$$

respectively as a quadratic in x,

$$F(u,x)=\delta_1(u)x^2+\delta_2(u)x+\delta_3(u). \tag{9}$$

Here

$$\begin{cases}\alpha(x)=a_1x^2+a_2x+a_3\\ \beta(x)=b_1x^2+b_2x+b_3\\ \gamma(x)=c_1x^2+c_2x+c_3\end{cases},\qquad \begin{cases}\delta_1(u)=a_1u^2+b_1u+c_1\\ \delta_2(u)=a_2u^2+b_2u+c_2\\ \delta_3(u)=a_3u^2+b_3u+c_3\end{cases}. \tag{10}$$

Mnemonically, α, β, γ are the *row polynomials*, while δ_1, δ_2, δ_3 are the *down polynomials*. The 3×3 matrix underlying the quartic form $F(u,x)$ is referred to as the *coefficient matrix*.

We wish to count, in two ways, the number of solutions $(u,x)\in\mathbb{F}_q\times\mathbb{F}_q$ to the equation $F(u,x)=0$. To do so, we need the following lemma.

Lemma 3.1. *Let $f(x)$, $g(x)$, $h(x)$ be polynomials with coefficients in $\mathbb{F}_q$. Then the number of solutions $(x,y)\in\mathbb{F}_q\times\mathbb{F}_q$ to the equation*

$$f(x)y^2+g(x)y+h(x)=0 \tag{11}$$

is given by the formula

$$q\cdot(1+n_{f,g,h})-n_f+\sum_{x\in\mathbb{F}_q}\sigma\big(g(x)^2-4f(x)h(x)\big) \tag{12}$$

where $n_f=\#\{x\in\mathbb{F}_q:f(x)=0\}$ is the number of zeros of $f(x)$, and $n_{f,g,h}=\#\{x\in\mathbb{F}_q:f(x)=g(x)=h(x)=0\}$ is the number of common zeros of $f(x)$, $g(x)$, $h(x)$.

Proof. For each $x\in\mathbb{F}_q$ which satisfies $f(x)\neq 0$, the quadratic equation (**??**) has $1+\sigma\big(g(x)^2-4f(x)h(x)\big)$ solutions $y\in\mathbb{F}_q$. The contribution to the solution count in this generic case is

$$\sum_{x\in\mathbb{F}_q:f(x)\neq 0}\Big(1+\sigma\big(g(x)^2-4f(x)h(x)\big)\Big),$$

which can be rewritten as

$$q-n_f-\sum_{x\in\mathbb{F}_q:f(x)=0}\sigma\big(g(x)^2\big)+\sum_{x\in\mathbb{F}_q}\sigma\big(g(x)^2-4f(x)h(x)\big). \tag{13}$$

Consider now the contribution coming from those $x \in \mathbb{F}_q$ which are zeros of $f(x)$. Then (**??**) turns into the linear equation $g(x)y+h(x)=0$. This has one solution $y \in \mathbb{F}_q$ whenever $g(x) \neq 0$, respectively q solutions whenever $g(x)=h(x)=0$. We can capture the solution count in this singular case by the formula

$$q \cdot n_{f,g,h} + \sum_{x \in \mathbb{F}_q : f(x)=0} \sigma\big(g(x)^2\big). \tag{14}$$

Adding up the counts (**??**) and (**??**), we obtain (**??**). □

We apply the lemma to the two equations, $\alpha(x)u^2+\beta(x)u+\gamma(x)=0$ and $\delta_1(u)x^2+\delta_2(u)x+\delta_3(u)=0$. The solution count is the same since, we recall, they both represent the equation $F(u,x)=0$. We deduce the following.

Theorem 3.2 (Master formula). *Let $\alpha(x)$, $\beta(x)$, $\gamma(x)$ and $\delta_1(u)$, $\delta_2(u)$, $\delta_3(u)$ be the polynomials given by* (**??**). *Then*

$$q \cdot n_{\alpha,\beta,\gamma} - n_\alpha + \sum_{x \in \mathbb{F}_q} \sigma\big(\beta(x)^2 - 4\alpha(x)\gamma(x)\big) =$$
$$q \cdot n_{\delta_1,\delta_2,\delta_3} - n_{\delta_1} + \sum_{u \in \mathbb{F}_q} \sigma\big(\delta_2(u)^2 - 4\delta_1(u)\delta_3(u)\big).$$

Theorem **??** reads as a general transformation formula relating two quadratic character sums whose polynomial argument is at most quartic. The heart of the matter in applying Theorem **??** is a suitable choice of a coefficient matrix.

In each one of the applications of Theorem **??** that follow, we will end up having $n_{\alpha,\beta,\gamma}=0$ and $n_{\delta_1,\delta_2,\delta_3}=0$. In some cases, this will be seen directly. In other cases, the following observation will prove useful.

Lemma 3.3. *Assume that $\beta(x)^2-4\alpha(x)\gamma(x)$ is square-free. Then $n_{\alpha,\beta,\gamma}=0$ and $n_{\delta_1,\delta_2,\delta_3}=0$.*

Proof. If $n_{\alpha,\beta,\gamma}>0$ then $\alpha(x)$, $\beta(x)$, and $\gamma(x)$ have a common linear factor $x-x_0$. Whence $\beta(x)^2-4\alpha(x)\gamma(x)$ is divisible by $(x-x_0)^2$, in contradiction with the square-free hypothesis.

If $n_{\delta_1,\delta_2,\delta_3}>0$ then $\delta_1(u)$, $\delta_2(u)$, and $\delta_3(u)$ have a common zero u_0. From (**??**) we see that $F(u_0,x)=0$, as a polynomial in x. In turn this implies, thanks to (**??**), that $-\gamma(x)=u_0\beta(x)+u_0^2\alpha(x)$ as polynomials. We then get $\beta(x)^2-4\alpha(x)\gamma(x)=(\beta(x)+2u_0\alpha(x))^2$, in contradiction with the square-free hypothesis. □

Henceforth, there is no need to distinguish the two variables in Theorem **??**; the variable u will be relabeled as x.

4. Applications

4.1. **A symmetric formula.**

For the coefficient matrix

$$\begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & a \\ 0 & b & c \end{pmatrix}$$

the associated polynomials are

$$\begin{cases} \alpha(x) = x \\ \beta(x) = x^2 + a \\ \gamma(x) = bx + c \end{cases}, \qquad \begin{cases} \delta_1(x) = x \\ \delta_2(x) = x^2 + b \\ \delta_3(x) = ax + c \end{cases}.$$

We have $n_\alpha = 1$ and $n_{\delta_1} = 1$.

Assuming that $(a, c) \neq (0, 0)$ and $(b, c) \neq (0, 0)$, we also have $n_{\alpha,\beta,\gamma} = 0$ and $n_{\delta_1,\delta_2,\delta_3} = 0$. Theorem **??** yields the pleasantly symmetric, quartic-to-quartic transformation formula

$$\sum_{x\in\mathbb{F}_q} \sigma\big((x^2 + a)^2 - 4x(bx + c)\big) = \sum_{x\in\mathbb{F}_q} \sigma\big((x^2 + b)^2 - 4x(ax + c)\big). \tag{15}$$

The case $c \neq 0$ is Theorem **??**.

The case $c = 0$ is not without interest. Now $a, b \neq 0$, and (**??**) involves biquadratic arguments. By applying the descent formula (**??**) to both sides, we obtain the cubic-to-cubic transformation formula

$$\sum_{x\in\mathbb{F}_q} \sigma(x)\sigma\big((x + a)^2 - 4bx\big) = \sum_{x\in\mathbb{F}_q} \sigma(x)\sigma\big((x + b)^2 - 4ax\big). \tag{16}$$

4.2. **A general descent formula.**

Consider the coefficient matrix

$$\begin{pmatrix} 0 & 0 & -1/4 \\ 1 & a_3/2 & 0 \\ a_2 - a_3^2/4 & a_1 & a_0 \end{pmatrix}.$$

The associated polynomials are

$$\begin{cases} \alpha(x) = -1/4 \\ \beta(x) = x^2 + (a_3/2)x \\ \gamma(x) = (a_2 - a_3^2/4)x^2 + a_1x + a_0 \end{cases}, \qquad \begin{cases} \delta_1(x) = x + (a_2 - a_3^2/4) \\ \delta_2(x) = (a_3/2)x + a_1 \\ \delta_3(x) = -x^2/4 + a_0 \end{cases}.$$

Visibly, $n_\alpha = 0$ and $n_{\delta_1} = 1$. We compute

$$\begin{cases} \beta(x)^2 - 4\alpha(x)\gamma(x) = x^4 + a_3x^3 + a_2x^2 + a_1x + a_0, \\ \delta_2(x)^2 - 4\delta_1(x)\delta_3(x) = x^3 + a_2x^2 + (a_1a_3 - 4a_0)x + a_0(a_3^2 - 4a_2) + a_1^2. \end{cases}$$

Theorem **??**, with a bit of help from Lemma **??**, yields Theorem **??**.

Remark 4.1. In the case of a depressed quartic, Theorem **??** simplifies to the following descent formula: if $f(x) = x^4 + ax^2 + bx + c$ is square-free then

$$\sum_{x\in\mathbb{F}_q} \sigma(f(x)) = -1 + \sum_{x\in\mathbb{F}_q} \sigma(x^3 + ax^2 - 4cx + b^2 - 4ac). \tag{17}$$

Conversely, Theorem **??** can be recovered by employing (**??**) as follows: given a quartic $f(x) = x^4 + a_3x^3 + a_2x^2 + a_1x + a_0$, depress it by the variable shift $x := x - a_3/4$; next, apply (**??**) to the resulting depressed quartic; finally, in the resulting cubic make the variable shift $x := x + a_3^2/8$.

4.3. **Descent for products of quadratics.** Consider the coefficient matrix

$$\begin{pmatrix} 1 & b_1 & c_1 \\ 0 & 0 & 0 \\ -1 & -b_2 & -c_2 \end{pmatrix}.$$

The associated polynomials are

$$\begin{cases} \alpha(x) = x^2 + b_1x + c_1 \\ \beta(x) = 0 \\ \gamma(x) = -(x^2 + b_2x + c_2) \end{cases}, \qquad \begin{cases} \delta_1(x) = x^2 - 1 \\ \delta_2(x) = b_1x^2 - b_2 \\ \delta_3(x) = c_1x^2 - c_2 \end{cases}.$$

We then have

$$\begin{cases} \beta(x)^2 - 4\alpha(x)\beta(x) = 4(x^2 + b_1x + c_1)(x^2 + b_2x + c_2) \\ \delta_2(x)^2 - 4\delta_1(x)\delta_3(x) = \Delta_1x^4 + Bx^2 + \Delta_2 \end{cases}$$

where $\Delta_1 = b_1^2 - 4c_1$, $\Delta_2 = b_2^2 - 4c_2$, $B = 4(c_1 + c_2) - 2b_1b_2$. Note also that $n_\alpha = 1 + \sigma(\Delta_1)$ and $n_{\delta_1} = 2$.

We require that the quartic polynomial $f(x) = (x^2+b_1x+c_1)(x^2+b_2x+c_2)$ be square-free. Then $n_{\alpha,\beta,\gamma} = 0$ and $n_{\delta_1,\delta_2,\delta_3} = 0$ thanks to Lemma **??**. Thus far, Theorem **??** yields the identity

$$\sum_{x\in\mathbb{F}_q} \sigma(f(x)) = -1 + \sigma(\Delta_1) + \sum_{x\in\mathbb{F}_q} \sigma\big(\Delta_1x^4 + Bx^2 + \Delta_2\big). \tag{18}$$

Our assumption that $f(x) = (x^2 + b_1x + c_1)(x^2 + b_2x + c_2)$ be square-free amounts to $\Delta_1 \neq 0$, $\Delta_2 \neq 0$, and $B^2 \neq 4\Delta_1\Delta_2$. Indeed, square-freeness of $f(x)$ means that its discriminant $\Delta(f)$ is non-zero. Now $\Delta(f) = \Delta_1 \cdot \Delta_2 \cdot \Pi^2$ where $\Pi = (z_1 - z_2)(z_1 - w_2)(w_1 - z_2)(w_1 - w_2)$. In the latter formula, z_1, w_1 are the roots of $x^2 + b_1x + c_1$, and z_2, w_2 are the roots of $x^2 + b_2x + c_2$, all in some extension of $\mathbb{F}_q$. We can evaluate Π in terms of the coefficients b_1, b_2, c_1, c_2 as follows:

$$\begin{aligned} \Pi &= (z_1^2 + b_2z_1 + c_2)(w_1^2 + b_2w_1 + c_2) \\ &= (c_1 - c_2)^2 - b_1b_2(c_1 + c_2) + b_1^2c_2 + b_2^2c_1. \end{aligned}$$

A further calculation reveals that $16\Pi = B^2 - 4\Delta_1\Delta_2$. To conclude, $\Delta(f) \neq 0$ amounts to $\Delta_1 \neq 0$, $\Delta_2 \neq 0$, and $B^2 - 4\Delta_1\Delta_2 \neq 0$.

As $\Delta_1 \neq 0$ and $B^2 \neq 4\Delta_1\Delta_2$, we infer from (**??**) that

$$\sum_{x\in\mathbb{F}_q} \sigma\big(\Delta_1x^4 + Bx^2 + \Delta_2\big) = -\sigma(\Delta_1) + \sum_{x\in\mathbb{F}_q} \sigma\big(\Delta_1x^3 + Bx^2 + \Delta_2x\big). \tag{19}$$

Furthermore, the change of variable $x := x/\Delta_1$ in the latter sum gives

$$\sum_{x\in\mathbb{F}_q} \sigma\big(\Delta_1 x^3 + Bx^2 + \Delta_2 x\big) = \sum_{x\in\mathbb{F}_q} \sigma\big(x^3 + Bx^2 + \Delta_1\Delta_2 x\big). \tag{20}$$

Taken together, the identities (**??**), (**??**), (**??**) yield

$$\sum_{x\in\mathbb{F}_q} \sigma(f(x)) = -1 + \sum_{x\in\mathbb{F}_q} \sigma\big(x^3 + Bx^2 + \Delta_1\Delta_2 x\big).$$

We have thereby obtained the descent formula (**??**) of Theorem **??**.

Remark 4.2. As already mentioned, it is possible to obtain the descent formula (**??**) from the general quartic-to-cubic formula (**??**). Here are the steps: (i) reduce the proof of (**??**) to its depressed case by using a variable shift $x := x + e$, (ii) use (**??**), the depressed instance of (**??**), and (iii) use Jacobsthal's cubic-to-cubic formula (**??**) to conclude.

A change of variable $x := x + e$ turns $f(x) = (x^2 + b_1x + c_1)(x^2 + b_2x + c_2)$ into a polynomial of the same form, $f^*(x) = (x^2 + b_1^*x + c_1^*)(x^2 + b_2^*x + c_2^*)$. Crucially, the parameters involved in the right-hand side of (**??**) remain unchanged: $\Delta_1^* = \Delta_1$, $\Delta_2^* = \Delta_2$, and $B^* = B$. The first two are evident; the latter requires a computation, left to the reader. In view of this shifting invariance, we may choose a convenient shift, namely, $e = -(b_1 + b_2)/4$, which depresses $f(x)$. It therefore suffices to obtain (**??**) when $b_1 + b_2 = 0$, in other words $b_2 = -b_1 =: b$.

In the case of a square-free polynomial of the form $f^*(x) = (x^2 - bx + c_1)(x^2 + bx + c_2)$, the quartic-to-cubic formula (**??**) says that

$$\sum_{x\in\mathbb{F}_q} \sigma(f^*(x)) = -1 + \sum_{x\in\mathbb{F}_q} \sigma(g(x))$$

where $g(x) = x^3 + (c_1 + c_2 - b^2)x^2 - 4c_1c_2x + b^2(c_1 + c_2)^2 - 4c_1c_2(c_1 + c_2)$.

We factor $g(x) = (x + c_1 + c_2)\big(x^2 - b^2x + b^2(c_1 + c_2) - 4c_1c_2\big)$. The change of variable $x := x + b^2/2$ leads to

$$\sum_{x\in\mathbb{F}_q} \sigma(g(x)) = \sum_{x\in\mathbb{F}_q} \sigma\bigg(\Big(x + \frac{B^*}{4}\Big)\Big(x^2 - \frac{\Delta_1^*\Delta_2^*}{4}\Big)\bigg)$$

where $B^* = 4(c_1 + c_2) + 2b^2$, $\Delta_1^* = b^2 - 4c_1$, $\Delta_2^* = b^2 - 4c_2$ are the expected parameters. Next, we use the rescaling $x := x/4$, followed by (**??**), to get

$$\begin{aligned}\sum_{x\in\mathbb{F}_q} \sigma(g(x)) &= \sum_{x\in\mathbb{F}_q} \sigma\big((x + B^*)(x^2 - 4\Delta_1^*\Delta_2^*)\big)\\ &= \sum_{x\in\mathbb{F}_q} \sigma\big(x(x^2 + B^*x + \Delta_1^*\Delta_2^*)\big).\end{aligned}$$

Combining these steps, we conclude that

$$\sum_{x\in\mathbb{F}_q} \sigma(f^*(x)) = -1 + \sum_{x\in\mathbb{F}_q} \sigma\big(x(x^2 + B^*x + \Delta_1^*\Delta_2^*)\big).$$

5. Explicit examples

The parametric form of the transformation formulas discussed above confers them generality and applicability. In this final section we consider some explicit examples. We work over a prime field $\mathbb{F}_p$, where $p > 3$. The quadratic character σ is now written classically, as the Legendre symbol $(\cdot/p)$.

For concrete applications, the most effective transformation formula is usually (**??**) or its depressed case, (**??**). Explicit evaluations are known only for sporadic families of cubics or quartics but, comparatively speaking, more is known for cubic arguments than for quartic arguments. So, if we are aiming for an explicit evaluation, then a good strategy is to promptly use a descent formula and turn a given quartic polynomial argument into a cubic. With a bit of luck, we just might land on a known evaluation–possibly after some simple shifting and rescaling.

Example 5.1. We evaluate the quadratic character sum

$$S := \sum_{x\in\mathbb{F}_p} \left(\frac{x^4+14x^3+24x^2+14x+1}{p}\right). \tag{21}$$

The quartic argument is square-free, as its discriminant is $-2^6\cdot 3^9 \neq 0$. Theorem **??** gives

$$S = -1 + \sum_{x\in\mathbb{F}_p} \left(\frac{x^3+24x^2+192x+296}{p}\right).$$

The cubic argument can be written as $(x+8)^3-6^3$. A shift $x := x-8$, and then a scaling $x := -6x$, give

$$S = -1 + \sum_{x\in\mathbb{F}_p} \left(\frac{x^3-6^3}{p}\right) = -1 + \left(\frac{-6}{p}\right) \sum_{x\in\mathbb{F}_p} \left(\frac{x^3+1}{p}\right).$$

The latter sum is a well-known cubic Jacobsthal sum. It evaluates as follows:

$$\sum_{x\in\mathbb{F}_p} \left(\frac{x^3+1}{p}\right) = \begin{cases} 2A_3 & \text{if } p\equiv 1 \bmod 3,\\ 0 & \text{if } p\equiv 2 \bmod 3,\end{cases}$$

where, in the case $p\equiv 1 \bmod 3$, we write $p = A_3^2+3B_3^2$ with the convention that $A_3 \equiv -1 \bmod 3$. See, for instance, [**?**, Chap.3].

As $(-3/p) = 1$ when $p\equiv 1 \bmod 3$, we conclude that

$$S = \begin{cases} -1 + (2/p)\cdot 2A_3 & \text{if } p\equiv 1 \bmod 3,\\ -1 & \text{if } p\equiv 2 \bmod 3.\end{cases} \tag{22}$$

Example 5.2. We evaluate the quadratic character sum

$$S := \sum_{x\in\mathbb{F}_p} \left(\frac{x^4+8x^3+24x^2-44x+16}{p}\right). \tag{23}$$

We first depress the quartic argument by the change of variable $x := x - 2$. We get the simpler quartic $x^4 - 76x + 152$, whose discriminant is $-2^8 \cdot 19^3$. For $p = 19$, we easily get $S = \sum_{x\in\mathbb{F}_p}(x^4/p) = p - 1$.

Assume $p \neq 19$. We may then use (**??**) to get

$$S = -1 + \sum_{x\in\mathbb{F}_p} \left(\frac{x^3 - 608x + 5776}{p}\right).$$

The latter quadratic character sum can be evaluated by the following formula due to Rishi, Parnami, and Rajwade [**?**]: for $\lambda \in \mathbb{F}_p^*$, we have

$$\sum_{x\in\mathbb{F}_p} \left(\frac{x^3 - 2^3 \cdot 19 \cdot \lambda^2 x + 2 \cdot 19^2 \cdot \lambda^3}{p}\right) = \begin{cases} (2\lambda/p) \cdot (A/19) \cdot A & \text{if } (p/19) = 1, \\ 0 & \text{if } (p/19) = -1, \end{cases}$$

where, in the case $(p/19) = 1$, we write $4p = A^2 + 19B^2$.

Taking $\lambda = 2$, we conclude that

$$S = \begin{cases} -1 + (A/19) \cdot A & \text{if } (p/19) = 1, \\ -1 & \text{if } (p/19) = -1. \end{cases} \tag{24}$$

Example 5.3. In a very recent preprint [**?**], Wenpeng Zhang pointed out that two different computations of the fourth moment associated to certain generalized Kloosterman sums imply the identity

$$\left(\frac{-1}{p}\right) \sum_{x\in\mathbb{F}_p^*} \left(\frac{x^3 + x^2 + x}{p}\right) - \sum_{x\in\mathbb{F}_p^*} \left(\frac{(x^2+1)(x^2+4x+1)}{p}\right) = 2.$$

Zhang asked for a direct proof of the identity. We give one below.

After including the terms corresponding to $x = 0$, the above identity can be rewritten as

$$\sum_{x\in\mathbb{F}_p} \left(\frac{(x^2+1)(x^2+4x+1)}{p}\right) = -1 + \left(\frac{-1}{p}\right) \sum_{x\in\mathbb{F}_p} \left(\frac{x^3 + x^2 + x}{p}\right). \tag{25}$$

We have two quartic-to-cubic descent formulas at our disposal, Theorem **??** and Theorem **??**. Using Theorem **??** is a natural choice, and (**??**) can indeed be obtained in this way. But Theorem **??** turns out to offer the quicker road.

Note that $(x^2+1)(x^2+4x+1) = (x+1)^4 - 4x^2$. The change of variable $x := x - 1$ gives

$$\sum_{x\in\mathbb{F}_p} \left(\frac{(x^2+1)(x^2+4x+1)}{p}\right) = \sum_{x\in\mathbb{F}_p} \left(\frac{x^4 - 4(x-1)^2}{p}\right).$$

The quartic argument is square-free, as it has discriminant $-2^{12} \cdot 3 \neq 0$. We apply (**??**)–that is, the depressed case of Theorem **??**–to the latter sum:

$$\sum_{x\in\mathbb{F}_p} \left(\frac{x^4 - 4(x-1)^2}{p}\right) = -1 + \sum_{x\in\mathbb{F}_p} \left(\frac{x^3 - 4x^2 + 16x}{p}\right).$$

Finally, the rescaling $x := -4x$ gives

$$\sum_{x\in\mathbb{F}_p}\left(\frac{x^3-4x^2+16x}{p}\right)=\left(\frac{-1}{p}\right)\sum_{x\in\mathbb{F}_p}\left(\frac{x^3+x^2+x}{p}\right).$$

We deduce (**??**) by combining the above identities.

The quartic polynomials of Example **??** and Example **??** are palindromic–that is to say, of the form $x^4+ax^3+bx^2+ax+1$. A general descent formula for palindromic quartics is discussed in [**?**, Ex.5.18]. We take this opportunity to point out an error in [**?**, Ex.5.18]: in the case $b=6$, the answer should be $-1+\varphi_2(16-a^2)$ instead of $-1+\varphi_2(1)$. The root error occurs earlier, in equation (138) of [**?**, Thm.5.16]: in the case $s=0$, the answer should be $-1+\varphi_2(cr)$ instead of $-1+\varphi_2(r)$.

For further results in the calculus of quadratic character sums, we refer the reader to [**?**, Chap.5].

References

[1] B.J. Birch: *How the number of points of an elliptic curve over a fixed prime field varies*, J. London Math. Soc. 43 (1968), 57–60

[2] E. Jacobsthal: *Anwendungen einer Formel aus der Theorie der quadratischen Reste*, Dissertation, Berlin, 1906

[3] D. Krachun, F. Petrov, Z.-W. Sun, M. Vsemirnov: *On some determinants involving Jacobi symbols*, Finite Fields Appl. 64 (2020), Paper no. 101672

[4] F. Leprévost, F. Morain: *Revêtements de courbes elliptiques à multiplication complexe par des courbes hyperelliptiques et sommes de caractères*, J. Number Theory 64 (1997), no. 2, 165–182

[5] L.J. Mordell: *Diophantine Equations*, Academic Press 1969

[6] K. Nagao: *An example of elliptic curve over $\mathbb{Q}(T)$ with rank ≥ 13*, Proc. Japan Acad. Ser. A Math. Sci. 70 (1994), no. 5, 152–153

[7] B. Nica: *Jacobsthal Sums*, Monographs in Number Theory, World Scientific 2025

[8] B. Nica: *Variance of point-counts for families of cubic curves over $\mathbb{F}_p$ and Jacobsthal sums*, preprint (2025), available at `https://arxiv.org/abs/2504.15505`

[9] J.C. Parnami, M.K. Agrawal, A.R. Rajwade: *Some identities involving character sums and their applications*, J. Indian Math. Soc. (N.S.) 54 (1989), no. 1-4, 125–132

[10] D.B. Rishi, J.C. Parnami, A.R. Rajwade: *Evaluation of a cubic character sum using the $\sqrt{-19}$ division points of the curve $Y^2 = X^3 - 2^3\cdot 19X + 2\cdot 19^2$*, J. Number Theory 19 (1984), no. 2, 184–194

[11] K.S. Williams: *Evaluation of character sums connected with elliptic curves*, Proc. Amer. Math. Soc. 73 (1979), no. 3, 291–299

[12] W. Zhang: *Some interesting number theory problems*, preprint (2025), available at `https://arxiv.org/abs/2506.17235`

Department of Mathematical Sciences
Indiana University Indianapolis
Email address: `bnica@iu.edu`