Additive decompositions induced by multiplicative characters over finite fields

Davide Schipani,* Michele Elia†

July 8, 2011

Abstract

In 1952, Perron showed that quadratic residues in a field of prime order satisfy certain additive properties. This result has been generalized in different directions, and our contribution is to provide a further generalization concerning multiplicative quadratic and cubic characters over any finite field. In particular, recalling that a character partitions the multiplicative group of the field into cosets with respect to its kernel, we will derive the number of representations of an element as a sum of two elements belonging to two given cosets. These numbers are then related to the equations satisfied by the polynomial characteristic functions of the cosets.

Further, we show a connection, a quasi-duality, with the problem of determining how many elements can be added to each element of a subset of a coset in such a way as to obtain elements still belonging to a subset of a coset.

Keywords: Characters, Residuacity, Finite Fields

Mathematics Subject Classification (2010): 12Y05, 12E20, 12E30

1 Introduction

Back in 1952, Perron [7] proved that every quadratic residue in $\mathbb{F}_p$, with p an odd prime, can be written as the sum of two quadratic residues in exactly $\lfloor \frac{p+1}{4} \rfloor - 1$ ways, and as the sum of two quadratic non-residues in exactly $\lfloor \frac{p+1}{4} \rfloor$ ways, a symmetric statement also holding for quadratic non-residues.

Winterhof [10] generalized this result, proving that if x_j is a nonzero element in a finite field $\mathbb{F}_q$, χ a nontrivial multiplicative character of order n and ω a primitive n-th root of unity, then $\sigma_0 + 1 = \sigma_1 = \cdots = \sigma_{n-1} = \frac{q-1}{n}$, where σ_i, $i = 0, \ldots, n-1$, stands for the number of field elements x such that $\chi(x)\bar{\chi}(x + x_j) = \omega^i$.

A generalization in a different direction was provided by Monico and Elia [5, 6]: they proved that the only partition of the field satisfying the additive properties found by Perron is that of

*University of Zurich, Switzerland
†Politecnico di Torino, Italy

quadratic residues and non-residues, providing a sort of converse and a way to define residues additively; moreover, they generalized Perron's result for any multiplicative character defined over a prime field.

Lastly, in his dissertation [8] Raymond showed how to generalize the case of the quadratic character to any finite field.

We provide here further generalizations considering quadratic and cubic characters over any finite field. Section 2 provides notations and preliminaries for the rest of the paper. In Section 3 we derive expressions for the number of (ordered) representations of an element as a sum of two elements belonging to two given cosets of the character partition. Furthermore, these expressions are shown to be related to the equations satisfied by the polynomial characteristic functions of the cosets. In Section 4 we point out a sort of duality relationship with another problem, and mention how the two problems are involved in polynomial factorization.

2 Preliminaries

Let $\mathbb{F}_{p^m}$, p an odd prime, be a finite field with polynomial basis $\{1, \eta, \eta^2, \ldots, \eta^{m-1}\}$ where η is a root of an irreducible polynomial of degree m over $\mathbb{F}_p$, and let $\mathcal{B}_0$ be the set of squares (excluding 0) and $\mathcal{B}_1$ the complementary set in $\mathbb{F}^*_{p^m}$. The quadratic character is a mapping from $\mathbb{F}^*_{p^m}$ into the complex numbers defined as

$$\chi_2(\alpha^h\theta) = (-1)^h \quad \theta \in \mathcal{B}_0, \quad h = 0, 1 \ ,$$

where α is a primitive element in $\mathbb{F}^*_{p^m}$. Furthermore, we set $\chi_2(0) = 0$.

We can define an indicator function of the sets $\mathcal{B}_j$ using the quadratic character, namely, for every $\gamma \neq 0$,

$$I_{\mathcal{B}_j}(\gamma) = \frac{1 + (-1)^j\chi_2(\gamma)}{2} = \begin{cases} 1 & \text{if } \gamma \in \mathcal{B}_j \\ 0 & \text{otherwise} \end{cases} \quad j = 0, 1 \ .$$

Also, writing $\gamma = \gamma_0 + \gamma_1\eta + \cdots + \gamma_{m-1}\eta^{m-1}$, a polynomial characteristic function that identifies the set $\mathcal{B}_j$ can be defined as

$$f_{\mathcal{B}_j}(\mathbf{X}) = \sum_{\gamma \in \mathbb{F}^*_q} I_{\mathcal{B}_j}(\gamma)\mathbf{X}^\gamma \ ,$$

where $\mathbf{X}^\gamma$ is a short notation standing for the monomial $x_0^{\gamma_0}x_1^{\gamma_1}\cdots x_{m-1}^{\gamma_{m-1}}$. Note that this notation allows us to formally write

$$\mathbf{X}^\gamma\mathbf{X}^\delta = \mathbf{X}^{\gamma+\delta} \mod \mathfrak{I}_{\mathbf{X}} \ ,$$

where $\mathfrak{I}_{\mathbf{X}} = \langle (x_1^p - 1), \ldots, (x_m^p - 1)\rangle$ is an ideal in $\mathbb{Q}[\mathbf{X}]$.

It is immediate to see that, if $\Phi_p(x)$ is the p-th cyclotomic polynomial,

$$f_{\mathcal{B}_0}(\mathbf{X}) + f_{\mathcal{B}_1}(\mathbf{X}) + 1 = \sum_{\gamma \in \mathbb{F}^*_{p^m}} \mathbf{X}^\gamma + 1 = \prod_{i=0}^{m-1} \Phi_p(x_i) \ . \tag{1}$$

In the following we will indicate the last product with the notation $\Phi(\mathbf{X})$.

In the case of cubic characters, non-trivial characters exist only if p is 2 with even exponent m, or p is an odd prime congruent to 1 modulo 6, or p is an odd prime congruent to 5 modulo 6 with even exponent m.

Let us write any nonzero element of the field as α^{k+3n}, with $k \in \{0,1,2\}$ and α a primitive element: we define $\mathcal{A}_0 = \{\alpha^{3i} : \ i = 0, \ldots, \frac{p^m-1}{3} - 1\}$, that is the subgroup of the cubic powers in $\mathbb{F}_{p^m}^*$, and let $\mathcal{A}_1 = \alpha\mathcal{A}_0$ and $\mathcal{A}_2 = \alpha^2\mathcal{A}_0$ be the two cosets that complete the coset partition of the set of nonzero elements of $\mathbb{F}_{p^m}$.

Similarly to the case of the quadratic character, we define an indicator function of the sets $\mathcal{A}_j$ using a cubic character, that is a mapping of the type

$$\chi_3(\alpha^h\theta) = \omega^h \quad \theta \in \mathcal{A}_0, \quad h = 0,1,2 \ ,$$

with ω a primitive cubic root of unity in $\mathbb{C}$ (and $\chi_3(0) = 0$ by definition).

The indicator function, for every $x \neq 0$, is then

$$I_{\mathcal{A}_j}(x) = \frac{1 + \omega^{2j}\chi_3(x) + \omega^j\bar{\chi}_3(x)}{3} = \begin{cases} 1 & \text{if } x \in \mathcal{A}_j \\ 0 & \text{otherwise} \end{cases} \quad j = 0,1,2 \ ,$$

(where the bar denotes complex conjugation), and a characteristic function that identifies the set $\mathcal{A}_j$ can be defined in the same way as above:

$$f_{\mathcal{A}_j}(\mathbf{X}) = \sum_{\gamma \in \mathbb{F}_{p^m}^*} I_{\mathcal{A}_j}(\gamma)\mathbf{X}^\gamma \quad j = 0,1,2 \ .$$

Again it is immediate to see that

$$f_{\mathcal{A}_0}(\mathbf{X}) + f_{\mathcal{A}_1}(\mathbf{X}) + f_{\mathcal{A}_2}(\mathbf{X}) + 1 = \sum_{\gamma \in \mathbb{F}_{p^m}^*} \mathbf{X}^\gamma + 1 = \Phi(\mathbf{X}) \ . \tag{2}$$

3 Results

To count the number of representations of a $\beta \neq 0$ in the field $\mathbb{F}_{p^m}$ as the sum of an element in $\mathcal{B}_j$ and an element in $\mathcal{B}_i$ (i not necessarily different from j), it suffices to compute

$$\sum_{z \neq 0,\beta} \frac{1 + (-1)^j\chi_2(z)}{2} \ \frac{1 + (-1)^i\chi_2(\beta - z)}{2} \tag{3}$$

Analogously, when we have a cubic character, to count the number of representations of a $\beta \neq 0$ in the field $\mathbb{F}_{p^m}$ as the sum of an element in $\mathcal{A}_j$ and an element in $\mathcal{A}_i$ (i not necessarily different from j), it suffices to compute

$$\sum_{z \neq 0,\beta} \frac{1 + \omega^{2j}\chi_3(z) + \omega^j\bar{\chi}_3(z)}{3} \ \frac{1 + \omega^{2i}\chi_3(\beta - z) + \omega^i\bar{\chi}_3(\beta - z)}{3}. \tag{4}$$

We summarize the conclusions in the next three theorems.

Theorem 1 *The number of representations $R_{p^m}^{(2)}(\beta, i, j)$ of a $\beta \neq 0$ in the field $\mathbb{F}_{p^m}$, p an odd prime, as the sum of an element in $\mathcal{B}_j$ and an element in $\mathcal{B}_i$ is*

$$R_{p^m}^{(2)}(\beta, i, j) = \frac{1}{4}\left(p^m - 2 - \chi_2(\beta)(-1)^i - \chi_2(\beta)(-1)^j - (-1)^{i+j}\chi_2(-1)\right) \ , \tag{5}$$

and depends only on the quadratic residuacity of β.

PROOF. The proof is immediate from (3), since, for any nontrivial character χ, $\sum_{x\in\mathbb{F}_{p^m}}\chi(x) = 0$ and $\sum_{x\in\mathbb{F}_{p^m}}\chi(x)\bar{\chi}(x+\gamma) = -1$ ([1, 9, 10]).

□

Remark 1. From (5) the desired values can be easily read, depending on whether β is in $\mathcal{B}_0$ or $\mathcal{B}_1$ and whether p^m is congruent to 1 or 3 modulo 4 (which determines $\chi_2(-1)$ by the properties of the Jacobi symbol and the quadratic reciprocity law); in particular, we can also read the values for which $i \neq j$, that are not usually explicitly included in the literature; in this case equation (5) becomes

$$\frac{1}{4}\left(p^m - 2 + \chi_2(-1)\right) \quad . \tag{6}$$

Theorem 2 *The number of representations $R^{(3)}_{p^m}(\beta, i, j)$ of a $\beta \neq 0$ in the field $\mathbb{F}_{p^m}$ as the sum of an element in $\mathcal{A}_j$ and an element in $\mathcal{A}_i$ is*

$$R^{(3)}_{p^m}(\beta, i, j) = \frac{1}{9}(p^m - 2 - K - \bar{K}) \tag{7}$$

with

$$K = \chi_3(\beta)(\omega^{2i} + \omega^{2j}) + \omega^{2i+j} - \omega^{2i+2j}\bar{\chi}_3(\beta)J(\chi_3, \chi_3),$$

$J(\chi_3, \chi_3)$ being a Jacobi sum ($\sum_{c_1+c_2=1}\chi_3(c_1)\chi_3(c_2)$), and depends only on the cubic residuacity of β.

PROOF. Expanding equation (4), using $\sum_{x\in\mathbb{F}_{p^m}}\chi_3(x) = 0$ and $\sum_{x\in\mathbb{F}_{p^m}}\chi_3(x)\bar{\chi}_3(x+\gamma) = -1$, and given that $\chi_3(-1) = 1$, we get

$$\frac{1}{9}\left[p^m - 2 - \chi_3(\beta)(\omega^{2i} + \omega^{2j}) - \bar{\chi}_3(\beta)(\omega^{i} + \omega^{j}) - (\omega^{2i+j} + \omega^{i+2j}) + \omega^{2i+2j}A(\beta) + \omega^{i+j}\bar{A}(\beta)\right]$$

where $A(\beta) = \sum_{x\in\mathbb{F}_{p^m}}\chi_3(x)\chi_3(\beta - x)$; this summation can be manipulated as

$$\sum_{x\in\mathbb{F}_{p^m}}\chi_3(x)\chi_3(\beta - x) = \chi_3(\beta^2)\sum_{x\in\mathbb{F}_{p^m}}\chi_3(\beta^{-1}x)\chi_3(1 - \beta^{-1}x) = \bar{\chi}(\beta)A(1) = \bar{\chi}(\beta)J(\chi_3, \chi_3),$$

whence the conclusion follows.

Remark 2. The last expression can be further simplified taking into account that $J(\chi_3, \chi_3)$ can be computed [4, Th. 5.21] with the Gauss sums of cubic characters (cf. also [3, 9]), as

$$J(\chi_3, \chi_3) = \frac{G_m^2(1, \chi_3)}{G_m(1, \bar{\chi}_3)} \quad .$$

In particular, if $p = 2$,

$$\sum_{x\in\mathbb{F}_{2^m}}\chi_3(x)\chi_3(x+1) = J(\chi_3, \chi_3) = G_m(1, \chi_3) = -(-2)^{m/2} \quad .$$

Theorem 3 *If $p \equiv 1 \bmod 4$, then $R^{(2)}_{p^m}(0,i,j)$ is $\frac{p-1}{2}$ for $i=j$ or 0 if $i \neq j$; if $p \equiv 3 \bmod 4$, then $R^{(2)}_{p^m}(0,i,j)$ is $\frac{p-1}{2}$ for $i \neq j$ or 0 if $i=j$. $R^{(3)}_{p^m}(0,i,j)$ is $\frac{p-1}{3}$ for $i=j$ or 0 if $i \neq j$.*

PROOF. The proof is immediate, taking into account that an element α is in the same coset as $-\alpha$ exactly when $\chi_2(-1)=1$ (resp. $\chi_3(-1)=1$).

$\square$

Working with the characteristic functions, the counterpart of the above theorems would be to multiply $f_{\mathcal{B}_i}(\mathbf{X})$ and $f_{\mathcal{B}_j}(\mathbf{X})$ (or $f_{\mathcal{A}_i}(\mathbf{X})$ and $f_{\mathcal{A}_j}(\mathbf{X})$) modulo $\mathfrak{I}_{\mathbf{X}}$, and then read the coefficients in the output, which involves exactly the same computations as above. But there is more: the characteristic functions $f_{\mathcal{B}_i}(\mathbf{X})$ and $f_{\mathcal{A}_j}(\mathbf{X})$ satisfy equations of second and third degree, respectively, whose coefficients are intrinsicly related to the number of representations of the field elements as sums of elements with given quadratic or cubic residuacity.

Theorem 4 *The characteristic functions $f_{\mathcal{B}_0}(\mathbf{X})$ and $f_{\mathcal{B}_1}(\mathbf{X})$ are roots of a quadratic equation*

$$y^2 - \sigma_1 y + \sigma_2 = 0 \bmod \mathfrak{I}_{\mathbf{X}} \tag{8}$$

in the residue ring of multivariate polynomials $\mathbb{Z}[\mathbf{X}]/\mathfrak{I}_{\mathbf{X}}$. The sum and the product of the roots (polynomials) are

$$\begin{cases} \sigma_1 = -1 + \Phi(\mathbf{X}) \bmod \mathfrak{I}_{\mathbf{X}} \\ \sigma_2 = -\frac{1}{4}\left[p^m \chi_2(-1) - 1 - \Phi(\mathbf{X})(p^m - 2 + \chi_2(-1))\right] \bmod \mathfrak{I}_{\mathbf{X}} \end{cases}$$

PROOF. Throughout the proof all the multivariate polynomials should be intended modulo the ideal $\mathfrak{I}_{\mathbf{X}}$. The coefficient σ_1 is directly obtained from equation (1), that is

$$\sigma_1 = f_{\mathcal{B}_0}(\mathbf{X}) + f_{\mathcal{B}_1}(\mathbf{X}) = \sum_{\gamma \in \mathbb{F}^*_{p^m}} (I_{\mathcal{B}_0}(\gamma) + I_{\mathcal{B}_1}(\gamma))\mathbf{X}^\gamma = -1 + \Phi(\mathbf{X}) \ .$$

The coefficient σ_2 is computed using the symbols $R^{(2)}_{p^m}(\beta,i,j)$ as follows. Starting from

$$\sigma_2 = f_{\mathcal{B}_0}(\mathbf{X}) f_{\mathcal{B}_1}(\mathbf{X}) = \sum_{\gamma \in \mathbb{F}^*_{p^m}} \sum_{\kappa \in \mathbb{F}^*_{p^m}} I_{\mathcal{B}_0}(\gamma) I_{\mathcal{B}_1}(\kappa) \mathbf{X}^{\gamma+\kappa} \ ,$$

and observing that exchanging the summation indices (variables) leaves the result invariant, we may consider the symmetric summation

$$\sigma_2 = \frac{1}{2} \sum_{\gamma \in \mathbb{F}^*_{p^m}} \sum_{\kappa \in \mathbb{F}^*_{p^m}} \left[I_{\mathcal{B}_0}(\gamma) I_{\mathcal{B}_1}(\kappa) + I_{\mathcal{B}_0}(\kappa) I_{\mathcal{B}_1}(\gamma)\right] \mathbf{X}^{\gamma+\kappa} \ ,$$

and perform the index substitution $\kappa = \beta - \gamma$; the index β may be 0 but it cannot assume the value γ; thus we may write

$$\sigma_2 = \frac{1}{2} \sum_{\gamma \in \mathbb{F}^*_{p^m}} \sum_{\substack{\beta \in \mathbb{F}_{p^m} \\ \beta \neq \gamma}} \left[I_{\mathcal{B}_0}(\gamma) I_{\mathcal{B}_1}(\beta-\gamma) + I_{\mathcal{B}_0}(\beta-\gamma) I_{\mathcal{B}_1}(\gamma)\right] \mathbf{X}^{\beta} \ .$$

Now, in the summation over β we separate the term with $\beta = 0$ and write

$$\sigma_2 = \frac{1}{2} \sum_{\gamma \in \mathbb{F}_{p^m}^*} \left\{ \sum_{\substack{\beta \in \mathbb{F}_{p^m}^* \\ \beta \neq \gamma}} \left[I_{\mathcal{B}_0}(\gamma) I_{\mathcal{B}_1}(\beta - \gamma) + I_{\mathcal{B}_0}(\beta - \gamma) I_{\mathcal{B}_1}(\gamma) \right] \mathbf{X}^\beta + C \right\} \quad .$$

where $C = [I_{\mathcal{B}_0}(\gamma) I_{\mathcal{B}_1}(-\gamma) + I_{\mathcal{B}_0}(-\gamma) I_{\mathcal{B}_1}(\gamma)] = \frac{1-\chi_2(-1)}{2}$, thus exchanging the two summations and, noting that $\sum_{\gamma \in \mathbb{F}_{p^m}^*} C = (p^m - 1)C$, we have

$$\sigma_2 = \frac{p^m - 1}{2} C + \frac{1}{2} \sum_{\beta \in \mathbb{F}_{p^m}^*} \mathbf{X}^\beta \left\{ \sum_{\substack{\gamma \in \mathbb{F}_{p^m}^* \\ \gamma \neq \beta}} \left[I_{\mathcal{B}_0}(\gamma) I_{\mathcal{B}_1}(\beta - \gamma) + I_{\mathcal{B}_0}(\beta - \gamma) I_{\mathcal{B}_1}(\gamma) \right] \right\} \quad .$$

Recalling the definition of $R_{p^m}^{(2)}(\beta, i, j)$, we may write the summation over γ as

$$\sigma_2 = \frac{p^m - 1}{2} C + \frac{1}{2} \sum_{\beta \in \mathbb{F}_{p^m}^*} \mathbf{X}^\beta \left\{ R_{p^m}^{(2)}(\beta, 0, 1) + R_{p^m}^{(2)}(\beta, 1, 0) \right\} \quad .$$

In conclusion, since $R_{p^m}^{(2)}(\beta, 0, 1) = R_{p^m}^{(2)}(\beta, 1, 0)$ does not depend on β, we obtain

$$\sigma_2 = \frac{p^m - 1}{2} \frac{1 - \chi_2(-1)}{2} + R_{p^m}^{(2)}(\beta, 0, 1)(\Phi(\mathbf{X}) - 1) \quad ,$$

and, using (6), we finally obtain

$$\sigma_2 = -\frac{1}{4} \left[p^m \chi_2(-1) - 1 - \Phi(\mathbf{X})(p^m - 2 + \chi_2(-1)) \right] \quad .$$

$\square$

Theorem 5 *The characteristic functions $f_{\mathcal{A}_0}(\mathbf{X})$, $f_{\mathcal{A}_1}(\mathbf{X})$, and $f_{\mathcal{A}_2}(\mathbf{X})$ are roots of a cubic equation*

$$y^3 - \sigma_1 y^2 + \sigma_2 y - \sigma_3 = 0 \mod \mathfrak{I}_\mathbf{X} \quad , \tag{9}$$

where

$$\begin{cases} \sigma_1 &= \Phi(\mathbf{X}) - 1 \bmod \mathfrak{I}_\mathbf{X} \\ \sigma_2 &= \frac{1}{3}(p^m - 1)(\Phi(\mathbf{X}) - 1) \bmod \mathfrak{I}_\mathbf{X} \\ \sigma_3 &= \frac{1}{27} \left[(\Phi(\mathbf{X}) - 1)^3 + (3 - 3\Phi(\mathbf{X}) + J(\chi_3, \chi_3) + \bar{J}(\chi_3, \chi_3))(p^m - \Phi(\mathbf{X})) \right] \bmod \mathfrak{I}_\mathbf{X} \end{cases}$$

PROOF. Throughout the proof all the multivariate polynomials should be intended modulo the ideal $\mathfrak{I}_\mathbf{X}$. The coefficient σ_1 is easily computed as

$$f_{\mathcal{A}_0}(\mathbf{X}) + f_{\mathcal{A}_1}(\mathbf{X}) + f_{\mathcal{A}_2}(\mathbf{X}) = \sum_{\gamma \in \mathbb{F}_{p^m}^*} (I_{\mathcal{A}_0}(\gamma) + I_{\mathcal{A}_1}(\gamma) + I_{\mathcal{A}_2}(\gamma)) \mathbf{X}^\gamma = -1 + \Phi(\mathbf{X}) \quad ,$$

because $I_{\mathcal{A}_0}(\gamma)+I_{\mathcal{A}_1}(\gamma)+I_{\mathcal{A}_2}(\gamma)=1$ and equation (1) is used. The elementary symmetric function σ_2 is the sum

$$f_{\mathcal{A}_0}(\mathbf{X})f_{\mathcal{A}_1}(\mathbf{X})+f_{\mathcal{A}_1}(\mathbf{X})f_{\mathcal{A}_2}(\mathbf{X})+f_{\mathcal{A}_2}(\mathbf{X})f_{\mathcal{A}_0}(\mathbf{X}) \ ,$$

then we need to compute the summation

$$\sigma_2=\sum_{\gamma\in\mathbb{F}^*_{p^m}}\sum_{\eta\in\mathbb{F}^*_{p^m}}(I_{\mathcal{A}_0}(\gamma)I_{\mathcal{A}_1}(\theta)+I_{\mathcal{A}_1}(\gamma)I_{\mathcal{A}_2}(\theta)+I_{\mathcal{A}_2}(\gamma)I_{\mathcal{A}_0}(\theta))\mathbf{X}^{\gamma+\theta} \ .$$

Using (7), we get

$$\sigma_2=-\frac{1}{3}(p^m-1)+\frac{1}{3}(p^m-1)\Phi(\mathbf{X}) \ .$$

Lastly, the elementary symmetric function $\sigma_3=f_{\mathcal{A}_0}(\mathbf{X})f_{\mathcal{A}_1}(\mathbf{X})f_{\mathcal{A}_2}(\mathbf{X})$ is given by the summation

$$\sigma_3=\sum_{\gamma\in\mathbb{F}^*_{p^m}}\sum_{\theta\in\mathbb{F}^*_{p^m}}\sum_{\kappa\in\mathbb{F}^*_{p^m}}I_{\mathcal{A}_0}(\gamma)I_{\mathcal{A}_1}(\theta)I_{\mathcal{A}_2}(\kappa)\mathbf{X}^{\gamma+\theta+\kappa} \ .$$

Expanding the product of the indicator functions and performing the summations, most of the 27 sums are cancelled, and it remains to compute the following:

$$\frac{1}{27}\sum_{\gamma\in\mathbb{F}^*_q}\sum_{\theta\in\mathbb{F}^*_{p^m}}\sum_{\kappa\in\mathbb{F}^*_{p^m}}\left(1-3\chi_3(\gamma)\bar{\chi}_3(\theta)+\chi_3(\gamma)\chi_3(\theta)\chi_3(\kappa)+\bar{\chi}_3(\gamma)\bar{\chi}_3(\theta)\bar{\chi}_3(\kappa)\right)\mathbf{X}^{\gamma+\theta+\kappa} \ .$$

To complete the task we then need to compute only three summations.

1. The summation
$$\sum_{\gamma\in\mathbb{F}^*_{p^m}}\sum_{\theta\in\mathbb{F}^*_{p^m}}\sum_{\kappa\in\mathbb{F}^*_{p^m}}\mathbf{X}^{\gamma+\theta+\kappa}=(\Phi(\mathbf{X})-1)^3 \ ;$$
is easily obtained, because the three summations on γ, θ, and κ can be performed independently.

2. The summation $\sum_{\gamma\in\mathbb{F}^*_{p^m}}\sum_{\theta\in\mathbb{F}^*_{p^m}}\sum_{\kappa\in\mathbb{F}^*_{p^m}}\chi_3(\gamma)\bar{\chi}_3(\theta)\mathbf{X}^{\gamma+\theta+\kappa}$ is computed by extending the sum range to include 0; this is done using the function $\delta(\kappa)$ which is 1 if $\kappa=0$, and is 0 otherwise, thus the summation is $\sum_{\gamma\in\mathbb{F}_{p^m}}\sum_{\theta\in\mathbb{F}_{p^m}}\sum_{\kappa\in\mathbb{F}_{p^m}}\chi_3(\gamma)\bar{\chi}_3(\theta)(1-\delta(\kappa))\mathbf{X}^{\gamma+\theta+\kappa}$ which splits into two summations
$$\sum_{\gamma\in\mathbb{F}_{p^m}}\sum_{\theta\in\mathbb{F}_{p^m}}\sum_{\kappa\in\mathbb{F}_{p^m}}\chi_3(\gamma)\bar{\chi}_3(\theta)\mathbf{X}^{\gamma+\theta+\kappa}-\sum_{\gamma\in\mathbb{F}_{p^m}}\sum_{\theta\in\mathbb{F}_{p^m}}\sum_{\kappa\in\mathbb{F}_{p^m}}\chi_3(\gamma)\bar{\chi}_3(\theta)\delta(\kappa)\mathbf{X}^{\gamma+\theta+\kappa} \ .$$
In the triple summations, the sum over κ can be performed independently and gives $\Phi(\mathbf{X})$ for the first, and simply 1 for the second. Thus we have
$$(\Phi(\mathbf{X})-1)\sum_{\gamma\in\mathbb{F}_{p^m}}\sum_{\theta\in\mathbb{F}_{p^m}}\chi_3(\gamma)\bar{\chi}_3(\theta)\mathbf{X}^{\gamma+\theta} \ .$$

The double summation can be easily evaluated with the substitution $\theta = \beta - \gamma$

$$\sum_{\beta\in\mathbb{F}_{p^m}} \sum_{\gamma\in\mathbb{F}_{p^m}} \chi_3(\gamma)\bar{\chi}_3(\beta-\gamma)\mathbf{X}^\beta = p^m - 1 - \sum_{\beta\in\mathbb{F}^*_{p^m}} \mathbf{X}^\beta = p^m - \Phi(\mathbf{X}) \ ,$$

because the sum over γ assumes only two values, namely -1 if $\beta \neq 0$ and $p^m - 1$ if $\beta = 0$. In conclusion we obtain

$$(\Phi(\mathbf{X}) - 1)(p^m - \Phi(\mathbf{X})) \ .$$

3. The sums in the triple summation

$$\sum_{\gamma\in\mathbb{F}^*_{p^m}} \sum_{\theta\in\mathbb{F}^*_{p^m}} \sum_{\kappa\in\mathbb{F}^*_{p^m}} \chi_3(\gamma)\chi_3(\theta)\chi_3(\kappa)\mathbf{X}^{\gamma+\theta+\kappa} = \sum_{\beta\in\mathbb{F}_{p^m}} \sum_{\theta\in\mathbb{F}_{p^m}} \sum_{\gamma\in\mathbb{F}_{p^m}} \chi_3(\gamma)\chi_3(\theta)\chi_3(\beta-(\gamma+\theta))\mathbf{X}^\beta \ ,$$

have been extended throughout $\mathbb{F}_{p^m}$ as $\chi_3(0) = 0$, together with the substitution $\kappa = \beta - (\gamma + \theta)$. Now, the summation over γ has two values, namely 0 if $\beta = \theta$, and $\bar{\chi}_3(\beta - \theta)A(1)$ if $\beta \neq \theta$, $A(1)$ being as above $\sum_{x\in\mathbb{F}_{p^m}} \chi_3(x)\chi_3(1-x) = J(\chi_3, \chi_3)$, therefore we obtain

$$\sum_{\beta\in\mathbb{F}_{p^m}} \sum_{\substack{\theta\in\mathbb{F}_{p^m}\\ \theta\neq\beta}} \chi_3(\theta)\bar{\chi}_3(\beta-\theta)A(1)\mathbf{X}^\beta = \sum_{\beta\in\mathbb{F}_{p^m}} \sum_{\theta\in\mathbb{F}_{p^m}} \chi_3(\theta)\bar{\chi}_3(\beta-\theta)A(1)\mathbf{X}^\beta = A(1)(p^m - \Phi(\mathbf{X}))$$

since the restriction $\theta \neq \beta$ can be removed and the summation over θ is -1 if $\beta \neq 0$ or $p^m - 1$ if $\beta = 0$.

In conclusion, collecting the results we obtain

$$\sigma_3 = \frac{1}{27}\big((\Phi(\mathbf{X}) - 1)^3 - 3(\Phi(\mathbf{X}) - 1)(p^m - \Phi(\mathbf{X})) + [J(\chi_3, \chi_3) + \bar{J}(\chi_3, \chi_3)](p^m - \Phi(\mathbf{X}))\big)$$

□

Remark 3. Note that $J(\chi_3, \chi_3) + \bar{J}(\chi_3, \chi_3)$ is always an integer, being twice the sum of real parts of cubic roots of unity.

Remark 4. Even though its derivation involved handling products of three characters, the expression of σ_3 only involves the Jacobi sum $A(1)$, i.e. fundamentally only the number of representations as the sum of two elements of two given cosets.

4 Connections with other problems

In this section we point out a sort of duality relationship with the following problem.

Suppose that we have t elements of a finite field $\mathbb{F}_{p^m}$ all belonging to one of the cosets determined by the character partition. We would like to know how many βs there are in the field such that, adding β to all the t elements, we get t elements still belonging to a common coset. If the character has order n, we let $N_{p^m}^{(n)}(t)$ be the number of βs; i.e. it is the number of solutions β of a system of t equations in $\mathbb{F}_{p^m}$ of the form

$$\left\{\begin{array}{l} \alpha^j z_1^n + \beta = \alpha^k y_1^n \\ \alpha^j z_2^n + \beta = \alpha^k y_2^n \\ \quad\vdots \\ \alpha^j z_t^n + \beta = \alpha^k y_t^n \end{array}\right. \tag{10}$$

where $\alpha^j z_1^n, \alpha^j z_2^n, \cdots, \alpha^j z_t^n$ are given and distinct, α being a primitive element, whereas the elements y_is must be chosen in the field to satisfy the system, and the n values $\{0, 1, \ldots, n-1\}$ for k and j are all considered. However, we may assume $j = 0$, since dividing each equation by α^j, and setting $\beta' = \beta\alpha^{-j}$ and $k' = k - j \bmod n$, we see that the number of solutions of the system is independent of j.

An explicit solution when the character is quadratic or cubic can be obtained, again by means of the indicator functions. For example, if we have a cubic character over $\mathbb{F}_{2^m}$, given a z_i we can partition the elements $\beta \neq z_i^3$ in $\mathbb{F}_{2^m}$ into subsets depending on the $k \in \{0, 1, 2\}$ such that $\chi(\beta + z_i^3) = \omega^k$. Therefore, a solution of (10) for a fixed k and $j = 0$ is singled out by the product

$$\prod_{i=1}^{t} I_{\mathcal{A}_k}(\beta + z_i^3) = \frac{1}{3^t}[1 + \sum_{i=1}^{t} \sigma_i^{(k)}] \ ,$$

where each $\sigma_i^{(k)}$ is a homogeneous sum of monomials which are products of i characters of the form $\chi(\beta + z_h^3)$ or $\bar{\chi}(\beta + z_h^3)$. Thus $N_{2^m}^{(3)}(t)$ is

$$N_{2^m}^{(3)}(t) = \sum_{\substack{\beta \in \mathbb{F}_{2^m} \\ \beta \notin \{z_i^3\}}} \left[\prod_{i=1}^{t} I_{\mathcal{A}_0}(\beta + z_i^3) + \prod_{i=1}^{t} I_{\mathcal{A}_1}(\beta + z_i^3) + \prod_{i=1}^{t} I_{\mathcal{A}_2}(\beta + z_i^3)\right] \ . \tag{11}$$

The z_i are excluded from the sum, since $z_i^3 + z_i^3 = 0$ does not belong to any coset.

In [2], which deals with this problem to analyse the success rate of the Cantor-Zassenhaus polynomial factorization algorithm, we computed exactly some of the above expressions for small values of t, and gave bounds for more general cases. In particular, we found that

$$1 + \max_{z_1 \neq z_2 \neq z_3} N_{2^m}^{(3)}(3) = \left\{\begin{array}{ll} \frac{1}{9}(2^m + 2^{m/2} - 2) & \text{for } m/2 \text{ even} \\ \frac{1}{9}(2^m + 2^{m/2+1} + 1) & \text{for } m/2 \text{ odd} \end{array}\right.$$

and

$$1 + \max_{z_1 \neq z_2 \neq z_3} N_{p^m}^{(2)}(3) = \left\{\begin{array}{ll} \frac{1}{4}(p^m - 1) & \text{for } p = 4k+1 \\ \frac{1}{4}(p^m + 1) & \text{for } p = 4k+3, \ m \text{ odd} \\ \frac{1}{4}(p^m - 1) & \text{for } p = 4k+3, \ m \text{ even} \end{array}\right. .$$

Recalling that $R_{p^m}^{(n)}(\beta, i, j)$, $n = 2, 3$, denotes the number of representations of a $\beta \neq 0$ in a finite field $\mathbb{F}_{p^m}$ as the sum of two element belonging to two cosets indexed by i and j in the partition given by a character of order n, we find the remarkable identities:

$$\max_{i,j,\beta} R_{2^m}^{(3)}(\beta, i, j) = 1 + \max_{z_1 \neq z_2 \neq z_3} N_{2^m}^{(3)}(3)$$

and

$$\max_{i,j,\beta} R_{p^m}^{(2)}(\beta, i, j) = 1 + \max_{z_1 \neq z_2 \neq z_3} N_{p^m}^{(2)}(3) \ .$$

In [2] this quasi-duality had the following interesting interpretation: the maximum t such that it is still possible to fail to split a polynomial of degree t with two attempts is equal to the maximum number of attempts to split a polynomial of degree 3.

5 Acknowledgments

The Research was supported in part by the Swiss National Science Foundation under grant No. 132256.

References

[1] B. Berndt, R.J. Evans, H. Williams, *Gauss and Jacobi Sums*, Wiley, 1998.

[2] M. Elia, D. Schipani, Improvements on the Cantor-Zassenhaus Factorization Algorithm, *www.arxiv.org*, 2011.

[3] M. Elia, D. Schipani, Gauss sums of cubic characters over $GF(p^r)$, p odd, *www.arxiv.org*, 2011.

[4] R. Lidl, H. Niederreiter, *Finite Fields*, Cambridge Univ. Press, 1997.

[5] C. Monico, M. Elia, Note on an Additive Characterization of Quadratic Residues Modulo p, *Journal of Combinatorics, Information & System Sciences*, vol. 31, 2006, pp.209-215.

[6] C. Monico, M. Elia, An Additive Characterization of Fibers of Characters on $\mathbb{F}_p^*$, *International Journal of Algebra*, Vol. 1-4, n.3, 2010, pp.109-117.

[7] O. Perron, Bemerkungen uber die Verteilung der quadratischen Reste, *Mathematische Zeitschrift*, Vol. 56, 1952, pp.122-130.

[8] D. Raymond, *An Additive Characterization of Quadratic Residues*, Master Degree thesis, Texas Tech University (Lubbock), 2009.

[9] D. Schipani, M. Elia, Gauss Sums of the Cubic Character over $\mathbb{F}_{2^m}$: an elementary derivation, *Bull. Polish Acad. Sci.Math.*, 59, 2011, pp.11-18.

[10] A. Winterhof, On the Distribution of Powers in Finite Fields, *Finite Fields and Their applications*, 4, 1998, pp.43-54.