# An Estimate on the Number of Stable Quadratic Polynomials

Domingo Gomez, Alejandro P. Nicolás*

*Departamento de Matemáticas, Estadística y Computación*
*Universidad de Cantabria. Santander (Spain)*

**Abstract**

In this work we obtain a nontrivial estimate for the size of the set of triples $(a, b, c) \in \mathbb{F}_q^* \times \mathbb{F}_q \times \mathbb{F}_q$ which correspond to stable quadratic polynomials $f(x) = aX^2 + bX + c$ over the finite field $\mathbb{F}_q$ with $q$ odd. This estimate is an step towards the bound $O(q^{11/4})$ conjectured in a recent work of A. Ostafe and I. Shparlinski.

*Keywords:* irreducible polynomials, composition of polynomials, stable quadratic polynomials

## 1. Introduction

Let $\mathbb{F}_q$ be a finite field of $q$ elements with $q$ odd. For a polynomial $f(X) \in \mathbb{F}_q[X]$ we define the following sequence:

$$f^{(0)}(X) = X, \quad f^{(n)}(X) = f^{(n-1)}(f(X)), \quad n \geq 1.$$

We say that $f \in \mathbb{F}_q[X]$ is *stable* if $f^{(n)}$ is irreducible over $\mathbb{F}_q$ for all $n \geq 0$. In the following, we only work with polynomials of degree 2, that is,

$$f(X) = aX^2 + bX + c \in \mathbb{F}_q[X], \text{ with } a \neq 0.$$

Our aim is to study the number of triples $(a, b, c) \in \mathbb{F}_q^* \times \mathbb{F}_q \times \mathbb{F}_q$ which corresponds to these stable polynomials. According to [1], we denote this number

*Corresponding author
*Email addresses:* domingo.gomez@unican.es (Domingo Gomez), alejandro.p.nicolas@unican.es (Alejandro P. Nicolás)

as $S_q$. This problem is related with the measure of multiplicative character sums.

Now, we give a brief introduction in order to maintain the paper self contained. We assume that the reader has a minimum knowledge of commutative algebra, specially in multivariate polynomials. In any case, these results may be found in [2]. Let us denote by $\gamma = -b/(2a)$ the critical point of $f$, that is, the zero of the derivative $f'$. The *adjusted orbit of* $f$ is defined as:

$$Orb(f) = \{\ f^{(n)}(\gamma) \mid n > 1\ \} \bigcup \{\ -f(\gamma)\ \}.$$

It can be proved (see [3] and [4]) that a quadratic polynomial $f$ over $\mathbb{F}_q$ is stable if and only if $Orb(f)$ contains no squares.

The measure of the number of squares of a set can be performed by means of character sums. In particular, it can be done using the only nontrivial quadratic multiplicative character $\chi$ of $\mathbb{F}_q$. The *Weil bound* for character sums will be useful to estimate the bounds of $S_q$ and can be presented in the following form (see Chapter 5 of [5]).

**Lemma 1.** *Let $\chi$ be the multiplicative quadratic character of $\mathbb{F}_q$ and let $F(X) \in \mathbb{F}_q[X]$ be a polynomial of positive degree that is not, up to a multiplicative constant, a square polynomial. Let $d$ be the number of distinct roots in its splitting field over $\mathbb{F}_q$. Under these conditions, the following inequality holds:*

$$\left| \sum_{x \in \mathbb{F}_q} \chi\left(F(x)\right) \right| \leq (d-1)q^{1/2}.$$

## 2. Estimate of $S_q$

This section is devoted to find an estimate of the bounds for $S_q$. Our main result is the following one.

**Theorem 1.** *For any $q$ odd, the number $S_q$ of stable quadratic polynomials $f \in \mathbb{F}_q[X]$ verifies*

$$\frac{q^2-1}{4} \leq S_q \leq q^{14/5}.$$

First, using Proposition 3 of [6], we will establish the lower bound. We can distinguish two different cases:

1. If $q \equiv 1 (\text{mod } 4)$ the adjusted orbit of the polynomial of $\mathbb{F}_q[x]$ given by $f_b(X) = (X-b)^2 + b$ is $Orb(f_b) = \{b, -b\}$. This orbit does not contain any squares provided that $b$ is not a square of $\mathbb{F}_q^*$. Since there exist $(q-1)/2$ elements such that they are not squares in $\mathbb{F}_q^*$, we have, at least, $(q-1)/2$ of such stable quadratic polynomials.
2. If $q \equiv -1 (\text{mod } 4)$ and $u, v \in \mathbb{F}_q$ are such that $u^2 + v^2 = -1$, the adjusted orbit of the polynomial $f_u(X) = (X - 4u^2 - 2)^2 + 4u^2$ is $Orb(f_u) = \{-4u^2, -4v^2\}$, which does not contain any squares of $\mathbb{F}_q$. From Lemma 6.24 of [5] we know that there exist $q+1$ solutions of the equation $u^2 + v^2 = -1$ in $\mathbb{F}_q^2$. Since $f_u = f_v$ if and only of $u^2 = v^2$, there are at least $(q+1)/4$ of such stable quadratic polynomials.

Next result shows that for each stable quadratic polynomial $f(X)$ we can obtain $q-1$ different ones.

**Lemma 2.** *For any quadratic stable polynomial $f(X)$ and $a \in \mathbb{F}_q^*$,*

$$g_a(X) = \frac{f(aX)}{a} \in \mathbb{F}_q[X]$$

*is an stable polynomial.*

*Proof.* It is trivial to notice that

$$g_a^{(n)}(X) = \frac{f^{(n)}(aX)}{a}$$

for all $n \geq 0$. So if $h(X) \mid g_a^{(n)}(X)$, then $h(a^{-1}X) \mid f^{(n)}(X)$. □

Notice that, since $f(X)$ has degree 2, $f(X) \neq g_a(X)$ for all $a \neq 1$. So, the number of stable quadratic polynomials is a multiple of $q-1$. This result with the bounds obtained for $q \equiv 1 (\text{mod } 4)$ and $q \equiv -1 (\text{mod } 4)$ leads us to the lower bound of Theorem 1.
Now, we will establish the upper bound of Theorem 1. Using previous notation, we define $F_{(k)}(a,b,c) = f^{(k)}(\gamma)$, where $a,\ b,\ c$ are variables and $\gamma = -b/(2a)$. From [1], we have that

$$S_q \leq \frac{1}{2^K} \sum_{a \in \mathbb{F}_q^*} \sum_{b,c \in \mathbb{F}_q} \prod_{k=1}^{K} (1 - \chi(F_{(k)}(a,b,c))),\ \forall K \in \mathbb{Z}^+.$$

Expanding the products and rearranging the terms, we conclude that there are $2^K - 1$ sums of the shape

$$(-1)^\mu \sum_{(a,b,c)\in\mathbb{F}_q^*\times\mathbb{F}_q\times\mathbb{F}_q} \chi\left(\prod_{j=1}^{\mu} F_{(k_j)}(a,b,c)\right),$$

where $1 \leq k_1 < \ldots < k_\mu \leq K$. This sum can be transformed in

$$\sum_{(a,b,c)\in\mathbb{F}_q^*\times\mathbb{F}_q\times\mathbb{F}_q} \chi\left(\prod_{j=1}^{\mu} F_{(k_j)}(a,b,c)\right) = \sum_{(a,b,c)\in\mathbb{F}_q^*\times\mathbb{F}_q\times\mathbb{F}_q} \chi\left(\prod_{j=1}^{\mu} F_{(k_j)}(a,b,c+b+b^2)\right) \quad (1)$$

Before deducing our upper bound, we prove a fundamental lemma.

**Lemma 3.** *For fixed integers $k_1, \ldots, k_\mu$ such that $1 \leq k_1 < \ldots < k_\mu \leq K$, the polynomial*

$$\prod_{j=1}^{\mu} F_{(k_j)}(a, X, c - X/2 + X^2/4)$$

*is a square only for at most $2^{4K+1}q$ choices of $(a, c)$.*

*Proof.* We divide the proof in two steps:

- First, we prove that for any index $k_i$ there are at most $2^{4K+1}q$ pairs $(a, c)$ such that $F_{(k_i)}(a, X, c - X/2 + X^2/4)$ has a multiple root.
- Then, we will see that, for almost all choices of the pair $(a, c)$, the polynomial $\prod_{j=1}^{\mu} F_{(k_j)}(a, X, c - X/2 + X^2/4)$ is not a square.

Each $F_{(k_i)}(a, X, c - X/2 + X^2/4)$ is a polynomial of degree less or equal to $2^{2k_i} < 2^{2K}$. Its coefficients can be seen as rational functions of degree at most $2^{k_i} < 2^K$ in both $a$ and $c$. So, the resultant of $F_{(k_i)}(a, X, c - X/2 + X^2/4)$ and its derivative with respect to $X$, $F'_{(k_i)}(a, X, c - X/2 + X^2/4)$, is a polynomial of degree at most $2^{4K+1}$ in both $a$ and $c$. Then, if this polynomial is not identically zero, it will have at most $2^{4K+1}q$ roots, that is, there will be at most $2^{4K+1}q$ pairs $(a, c)$ such that $F_{(k_i)}(a, X, c - X/2 + X^2/4)$ has a multiple root.

Now, we will show that the polynomials

$$F_{(k_i)}(a, X, c - X/2 + X^2/4), \quad F'_{(k_i)}(a, X, c - X/2 + X^2/4)$$

do not share any common factor. It suffices to give a specific example, valid for any finite field $\mathbb{F}_q$. Let us consider $f(X) = (X - b)^2 + b$. For this polynomial $\gamma = b$; so $F_{(k_i)}(1, X, -X/2 + X^2/4) = X$ and $F'_{(k_i)}(1, X, -X/2 + X^2/4) = 1$ for all $k_i$.

Finally, notice that the degree of $F_{(k_\mu)}(a, X, c - X/2 + X^2/4)$ is $2^{2k_\mu}$. If the coefficients $(a, c)$ are neither a root of the leading coefficient of $F_{(k_\mu)}(a, X, c - X/2 + X^2/4)$, nor one of the $2^{4K+1}q$ pairs which make the resultant $r(a, c) = 0$, then the polynomial has $2^{2k_\mu}$ different roots in some extension field. Also,

$$\deg\left(\prod_{j=1}^{\mu-1} F_{(k_j)}(a, X, c - X/2 + X^2/4)\right) \leq 2^{2k_\mu} - 1$$

and the polynomial

$$\prod_{j=1}^{\mu} F_{(k_j)}(a, X, c - X/2 + X^2/4)$$

contains at least one simple root. □

Combining Lemma 3 and the Weil bound (Lemma 1), we obtain $S_q < q^3/2^K + 2^K q^{5/2} + 2^{4K+1}q^2$. Choosing $2^K = q^{1/5}$, we get $S_q < q^{14/5}$. Theorem 1 is proved.

## 3. Final Remarks and Comments

Lemma 2 is still true for polynomials of higher degree. However, $f(X)$ and $g_a(X)$ no longer have to be different for all $a \neq 1$. For instance, for any $q$ odd, if $f(X) = X^3$ and $a = -1$, then $g_{-1}(X) = f(X)$. Thus, the number of stable polynomials has not to be a multiple of $q - 1$. Finally, we highlight that this Lemma is also true for fields of characteristic zero, as can be seen in Lemma 6 of [7].

## 4. Acknowledgments

D. G. was partially supported by the Spanish Ministry of Science, project MTM2007-67088. The authors want to thank Alina Ostafe and Igor Shparlinski for comments and helpful advice. Also, many thanks to Arne Winterhof, who found a slot in his schedule to read the paper.

## References


[1] A. Ostafe, I. Shparlinski, On the length of critical orbits of stable quadratic polynomials, Proc. Amer. Math. Soc. (to appear).

[2] J. von zur Gathen, J. Gerhard, Modern computer algebra, 2nd Edition, Cambridge University Press, Cambridge, 2003.

[3] R. Jones, N. Boston, Settled polynomials over finite fields, Preprint.

[4] M. Ayad, D. L. McQuillan, Irreducibility of the iterates of a quadratic polynomial over a field, Acta Arithmetica 93 (1) (2000) 87–97.

[5] R. Lidl, H. Niederreiter, Finite Fields and Applications, Cambridge, 1997.

[6] N. Ali, Stalilité des polynômes, Acta Arithmetica 119 (2005) 53–63.

[7] O. Ahmadi, F. Luca, A. Ostafe, I. Shparlinski, On Stable Quadratic Polynomials, Preprint.