Acta Math. Univ. Comenianae
Vol. LXXIX, 1(2010), pp. 73–76

ON FAIL-ROLLE POLYNOMIALS WITH FEW ROOTS

L. H. GALLARDO

Abstract. A splitting polynomial in one variable over a field is Fail-Rolle if its formal derivative does not split over the same field. It is known that the finite fields with more than four elements are exactly the finite fields for which there are Fail-Rolle polynomials. We describe all Fail-Rolle polynomials with at most five roots over a finite field of even characteristic.

1. Introduction

Let $\mathbb{F}_q$ be a finite field of characteristic p and with q elements. For a splitting polynomial $A \in \mathbb{F}_q[x]$ we let $\omega(A)$ denote the number of distinct roots of A in $\mathbb{F}$. We denote also by $N_q(d)$ (see [**4**, Theorem 3.25, p. 93]) the number of prime (irreducible) polynomials of degree d in $\mathbb{F}_q[x]$.

Craven [**2**] answering the question of Kaplansky [**3**] proved that the only finite fields in which the set of splitting polynomials $S \in \mathbb{F}_q[x]$ is invariant under formal derivatives S' are $\mathbb{F}_2$ and $\mathbb{F}_4$. Later Ballantine and Roberts [**1**] reproved the same result. Assuming p is odd they considered a Fail-Rolle polynomial with 4 roots. In his MR-review of the latter paper Steve Cohen observed that in order to complete the proof when p is odd we can use the Fail-Rolle polynomial with only 3 roots $R = x^{p-1}(x+1)(x+a)$ where a is a non-square in $\mathbb{F}_q$. On the other hand in the case $p = 2$ they considered a Fail-Rolle polynomial with 6 roots. We become curious to know if we can find Fail-Rolle polynomials with fewer roots when q is even.

Take q even. Clearly, without loss of generality, we may assume that a Fail-Rolle polynomial A is monic, has a root at 0 and is square-free. Since, for even q, the formal derivative of C^2A is C^2A' for any polynomials $A, C \in \mathbb{F}_q[x]$.

The answer is contained in our main result that follows.

Theorem 1. *Let $\mathbb{F}$ be a finite field with an even number q of elements. Let $A \in \mathbb{F}[x]$ be a monic square-free Fail-Rolle polynomial with $A(0) = 0$ and at most 5 roots. Then, either*

(a) $\omega(A) = 4$ *and* $A = x(x-a)(x-b)(x-c)$ *for some non-zero pairwise distinct,* $a, b, c \in \mathbb{F}$*, such that* $a + b + c = 0$*. So, there are, up to permutations, at least* $(q-1)(q-2)$ *such polynomials,*
or

Received November 11, 2008.
2000 *Mathematics Subject Classification.* Primary 11T55, 11T06.
Key words and phrases. quadratic forms; splitting polynomials; formal derivatives; finite fields; characteristic 2.

(b) $\omega(A) = 5$ *and* $A = x(x-a)(x-b)(x-c)(x-d)$ *for some non-zero pairwise distinct* $a, b, c, d \in \mathbb{F}$ *such that* $ab+ac+ad+bc+bd+cd = p_1$ *and* $abcd = p_0$, *where the polynomial* $P = x^2 + p_1 x + p_0$ *is a prime polynomial in* $\mathbb{F}_q[x]$. *Moreover, the map* $M : \mathbb{F}_q^4 \to \mathbb{F}_q^2$ *that takes* (a, b, c, d) *into* $(ab + ac + ad + bc + bd + cd, abcd)$ *is onto. Thus, up to permutations, there are at least* $N_q(2) = (q^2 - q)/2$ *such polynomials.*

The only difficulty is to be sure that for even $q > 4$ the map $M : \mathbb{F}_q^4 \to \mathbb{F}_q^2$ that takes (a, b, c, d) into $(ab + ac + ad + bc + bd + cd, abcd)$ is onto. This was first checked by a computer program for $q = 8$. And then proved in general, by using essentially, the classification of quadratic forms in four variables over $\mathbb{F}_q$.

By α we denote an element in a fixed algebraic closure of $\mathbb{F}_2$ such that $\alpha^2 = \alpha+1$. So that $\mathbb{F}_4 = \mathbb{F}_2[\alpha]$.

2. Proof of the theorem in the cases $\omega(A) < 5$.

When $\omega(A) = 2$ such that $A = x(x - a)$ for some non-zero $a \in \mathbb{F}$, there is no Fail-Rolle polynomial since

$$\frac{A'}{A} = \frac{1}{x} + \frac{1}{x-a} = \frac{a}{A}.$$

Assume $\omega(A) = 3$. We set $A = x(x - a)(x - b)$ for non-zero pairwise distinct $a, b \in \mathbb{F}$. We get

$$\frac{A'}{A} = \frac{1}{x} + \cdots = \frac{x^2 + ab}{A}.$$

Thus, there is no Fail-Rolle polynomial since ab is a square in $\mathbb{F}$.

Assume $\omega(A) = 4$. We set $A = x(x - a)(x - b)(x - c)$ for non-zero pairwise distinct $a, b, c \in \mathbb{F}$. We get

$$\frac{A'}{A} = \frac{1}{x} + \cdots = \frac{(a+b+c)x^2 + abc}{A}.$$

Since abc and $a + b + c$ are squares in $\mathbb{F}$, the numerator splits in $\mathbb{F}[x]$ if and only if $a + b + c \neq 0$. This proves (a).

3. Main lemma in the case $\omega(A) = 5$.

Assume $\omega(A) = 5$. We set $A = x(x-a)(x-b)(x-c)(x-d)$ for non-zero pairwise distinct $a, b, c, d \in \mathbb{F}$. We get

$$\frac{A'}{A} = \frac{1}{x} + \cdots = \frac{x^4 + (ab + ac + ad + bc + bd + cd)x^2 + abcd}{A}.$$

Since all elements of $\mathbb{F}$ are squares it suffices to consider the possible roots in $\mathbb{F}$ of $P = x^2 + (ab+ac+ad+bc+bd+cd)x + abcd$ depending on the values of $a, b, c, d \in \mathbb{F}$.

The following observation can be checked by a simple computation.

Proposition 1. *Consider the quadratic form of rank* 4 *over* $\mathbb{F}$,

$$Q(a, b, c, d) = ab + ac + ad + bc + bd + cd.$$

a) *If* $\mathbb{F}$ *does not contain the field* $\mathbb{F}_4$*, then* Q *is equivalent to the quadratic form* $Q_1(x_1, y_1, x_2, y_2) = x_1^2 + x_1y_1 + sy_1^2 + x_2y_2$ *where* $s = 1$ *and has trace* $Tr(s) = 1$*. More precisely we have*

$$Q(a, b, c, d) = c^2 + cd + 1 \cdot d^2 + (a + c + d)(b + c + d).$$

So, $Q(a, b, c, d) = Q_1(x_1, y_1, x_2, y_2)$ *for*

$$x_1 = c,\ y_1 = d,\ x_2 = a + c + d,\ y_2 = b + c + d.$$

And also equivalently for

$$c = x_1,\ d = y_1,\ b = y_2 + x_1 + y_1,\ a = x_2 + x_1 + y_1.$$

b) *If* $\mathbb{F}$ *does contain the field* $\mathbb{F}_4$*, then* Q *is equivalent to the quadratic form* $Q_1(x_1, y_1, x_2, y_2) = x_1y_1 + x_2y_2$*. More precisely we have*

$$Q(a, b, c, d) = (c + d\alpha)(c + d\alpha^2) + (a + c + d)(b + c + d).$$

So, in this case $Q(a, b, c, d) = Q_1(x_1, y_1, x_2, y_2)$ *for*

$$x_1 = c + d\alpha,\ y_1 = c + d\alpha^2,\ x_2 = a + c + d,\ y_2 = b + c + d.$$

And also equivalently for

$$d = x_1 + y_1,\ c = x_1\alpha^2 + y_1\alpha,\ b = y_2 + x_1\alpha + y_1\alpha^2,\ a = x_2 + x_1\alpha + y_1\alpha^2.$$

We have the crucial lemma.

Lemma 1. *Let* $\mathbb{F}$ *be a finite field with an even number* q *of elements. Then the map* $M : \mathbb{F}^4 \to \mathbb{F}^2$ *that takes* (a, b, c, d) *into* $(ab + ac + ad + bc + bd + cd, abcd)$ *is onto.*

Proof. Let R, S be given elements of $\mathbb{F}$. We shall prove the existence of $a, b, c, d \in \mathbb{F}$ such that $M(a, b, c, d) = (R, S)$.

3.1. Case in which $\mathbb{F}$ does not contain $\mathbb{F}_4$.

If $R = 0$, let choose $y_2 = 1$ and $x_1 = y_1 = t \in \mathbb{F}$ to determine. So, from the equations $0 = R = x_1^2 + x_1y_1 + y_1^2 + x_2y_2$ and $S = x_1y_1(y_2 + x_1 + y_1)(x_2 + x_1 + y_1)$, we get $t^2 = x_2$ and $t^4 = S$. Since S is a fourth power, this system has a solution. Then the Proposition 1 gives us the corresponding a, b, c, d. Assume now that $R \neq 0$. Multiplying by a square, if necessary, we may also assume that $R \neq 1$ and $Tr(R) = 1$. Indeed, if $\delta \in \mathbb{F}$ is an element such that $\delta \neq 1$ and $Tr(\delta) = 1$, then we multiply R by δ/R. So, by Hilbert's 90 theorem $R + 1 = y_1^2 + y_1$ for some non-zero $y_1 \in \mathbb{F}$ such that $y_1 \neq 1$. Take also $x_1 = 1$ and $x_2 = 0$. We get $R = x_1^2 + x_1y_1 + y_1^2 + x_2y_2$. For S we have $S = y_1(y_2 + 1 + y_1)(1 + y_1)$ a linear equation in y_2 that has a solution since $y_1^2 + y_1 \neq 0$. As before, Proposition 1 gives us the corresponding a, b, c, d.

3.2. Case in which $\mathbb{F}$ does contain $\mathbb{F}_4$.

Without loss of generality we can take $R \notin \{1, \alpha, \alpha^2\}$. If $R \neq 0$ just multiply by ϵ/R where $\epsilon \in \mathbb{F}$ satisfies $\epsilon^3 \neq 1$. Thus, we take $x_2 = 0, x_1 = R, y_1 = 1$. We get $R = x_1y_1 + x_2y_2$. The other equation $S = (x_1 + y_1)(x_1\alpha^2 + y_1\alpha)(y_2 + x_1\alpha + y_1\alpha^2)(x_2 + x_1\alpha + y_1\alpha^2)$ becomes

$$S = (R + 1)(R\alpha^2 + \alpha)(R\alpha + \alpha^2)(y_2 + R\alpha + \alpha^2).$$

This a linear equation is y_2 that has a solution $y_2 \in \mathbb{F}$ since the coefficient R^3+1 of y_2 in the equation in non-zero. As before, Proposition 1 gives us the corresponding a, b, c, d.

This proves the lemma. □

4. Proof of the Theorem in the case $\omega(A) = 5$.

We have already seen in the previous section that A is Fail-Rolle if and only if $A' = x^4 + (ab + ac + ad + bc + bd + cd)x^2 + abcd$ is a square P^2 of a prime polynomial $P \in \mathbb{F}[x]$ of degree 2. By Lemma 1 there exist such (a, b, c, d) for each choice of such P. So there are, up to permutations, at least $N_q(2) = (q^2 - q)/2$ such polynomials. This proves (b) thereby, proving the Theorem.

References

1. Ballantine C., Roberts J., *A simple proof of Rolle's theorem for finite fields*, Amer. Math. Monthly **109**(1) (2002), 72–74.
2. Craven T., *A weak version of Rolle's theorem*, Proc. Amer. Math. Soc. **125** (1997), 3147–3153.
3. Kaplansky I., *Fields and Rings*, 2nd ed., University of Chicago Press, Chicago 1972.
4. Lidl R. and Niederreiter H., *Finite Fields*, Encyclopedia of Mathematics and its applications, Cambridge University Press 1983 (Reprinted 1987).

L. H. Gallardo, Department of Mathematics, University of Brest, 6, Avenue Le Gorgeu, C.S. 93837, 29238 Brest Cedex 3, France, *e-mail*: Luis.Gallardo@univ-brest.fr