

# ON SETS OF IRREDUCIBLE POLYNOMIALS CLOSED BY COMPOSITION

ANDREA FERRAGUTI, GIACOMO MICHELI, AND RETO SCHNYDER

ABSTRACT. Let  $\mathcal{S}$  be a set of monic degree 2 polynomials over a finite field and let  $C$  be the compositional semigroup generated by  $\mathcal{S}$ . In this paper we establish a necessary and sufficient condition for  $C$  to be consisting entirely of irreducible polynomials. The condition we deduce depends on the finite data encoded in a certain graph uniquely determined by the generating set  $\mathcal{S}$ . Using this machinery we are able both to show examples of semigroups of irreducible polynomials generated by two degree 2 polynomials and to give some non-existence results for some of these sets in infinitely many prime fields satisfying certain arithmetic conditions.

## 1. INTRODUCTION

Since irreducible polynomials play a fundamental role in applications and in the whole theory of finite fields (see for example [1, 2, 3, 4, 5, 6]), related questions have a long history (see for example [7, 8, 9, 10, 11, 12, 13]). In this paper we specialize on irreducibility questions regarding compositional semigroups of polynomials. This kind of question has been addressed in the specific case of semigroups generated by a single quadratic polynomial, see for example in [6, 5, 11, 10], for analogous results related to additive polynomials, see [14, 15]. It is worth mentioning that one of these results [11, Lemma 2.5] has been recently used in [16] by the first and the second author of the present paper to prove [12, Conjecture 1.2].

Throughout the paper,  $q$  will be an odd prime power,  $\mathbb{F}_q[x]$  the univariate polynomial ring over the finite field  $\mathbb{F}_q$  and  $\text{Irr}(\mathbb{F}_q[x])$  the set of irreducible polynomials in  $\mathbb{F}_q[x]$ . Let us give an example which motivates this paper. For a prime  $p$  congruent to 1 modulo 4, we can fix in  $\mathbb{F}_p[x]$  two quadratic polynomials  $f = (x - a)^2 + a$  and  $g = (x - a - 1)^2 + a$  such that both  $a$  and  $a + 1$  are non-squares in  $\mathbb{F}_p$ . One can experimentally check that any possible composition of a sequence of  $f$ 's and  $g$ 's is irreducible (for a concrete example, take  $q = 13$ ,  $(x - 5)^2 + 5$  and  $g = (x - 6)^2 + 5$ ). Let us denote the set of such compositions by  $C$ . A couple of observations are now necessary:

---

2010 *Mathematics Subject Classification.* 11T06.

*Key words and phrases.* Finite Fields; Irreducible Polynomials; Semigroups; Graphs. The Second Author is thankful to SNSF grant number 161757.

- In principle, it is unclear whether a finite number of irreducibility checks will ensure that  $C$  is a subset of  $\text{Irr}(\mathbb{F}_q[x])$ .
- The fact that  $C \subseteq \text{Irr}(\mathbb{F}_q[x])$  is indeed pretty unlikely to happen by chance, as the density of degree  $2^n$  monic irreducible polynomials over  $\mathbb{F}_q$  is roughly  $1/2^n$ . Thus, if  $C$  satisfies this property, one reasonably expects that there must be an algebraic reason for that.

We address these issues by giving a necessary and sufficient condition for the semigroup  $C \subset \mathbb{F}_q[x]$  to be contained in  $\text{Irr}(\mathbb{F}_q[x])$ . In addition, this condition is algebraic and can be checked by performing only a finite amount of computation over  $\mathbb{F}_q$ , answering both points above.

In Section 2 we describe the criterion (Theorem 2.4 and Corollary 2.5) and provide a non-trivial example (Example 2.7) of a compositional semigroup in  $\mathbb{F}_q[x]$  contained in  $\text{Irr}(\mathbb{F}_q[x])$  and generated by two polynomials.

In Section 3 we show the non-existence of such  $C$  whenever  $q$  is a prime congruent to 3 modulo 4 and the generating polynomials are of a certain form (Proposition 3.2). Example 3.3 shows that these conditions are indeed sharp.

## 2. A GENERAL CRITERION

In order to state our main result, we first need the following definition, which describes how to build a finite graph encoding only the useful (to our purposes) information contained in the generating set of the semigroup.

**Definition 2.1.** Let  $q$  be an odd prime power,  $\mathbb{F}_q$  the finite field of order  $q$  and  $\mathcal{S}$  a subset of  $\mathbb{F}_q[x]$ . We denote by  $G_{\mathcal{S}}$  the directed multigraph defined as follows:

- the set of nodes of  $G_{\mathcal{S}}$  is  $\mathbb{F}_q$ ;
- for any node  $a \in \mathbb{F}_q$  and any polynomial  $f \in \mathcal{S}$ , there is a directed edge  $a \rightarrow f(a)$ . We label that edge with  $f$ .

Before stating the next definition, we recall that for any monic polynomial  $f$  of degree 2 there exist unique pair  $(a_f, b_f) \in \mathbb{F}_q^2$  such that  $f = (x - a_f)^2 - b_f$ .

**Definition 2.2.** Let  $\mathcal{S}$  be a subset of  $\mathbb{F}_q[x]$  consisting of monic polynomials of degree 2. We call the set  $D_{\mathcal{S}} := \{-b_f \mid f \in \mathcal{S}\} \subseteq \mathbb{F}_q$ , the  $\mathcal{S}$ -*distinguished set* of  $\mathbb{F}_q$ .

The following result is just an inductive extension of the classical Capelli's Lemma.

**Lemma 2.3** (Recursive Capelli's Lemma). *Let  $K$  be a field and  $f_1, \dots, f_l$  be a set of irreducible polynomials in  $K[X]$ . The polynomial  $f_1(f_2(\dots(f_l)\dots))$  is*

irreducible if and only if the following conditions are satisfied

$$\left\{ \begin{array}{l} f_1 \text{ is irreducible over } K[X] \\ f_2 - \alpha_1 \text{ is irreducible over } K(\alpha_1)[X] \text{ for a root } \alpha_1 \text{ of } f_1 \\ f_3 - \alpha_2 \text{ is irreducible over } K(\alpha_1, \alpha_2)[X] \text{ for a root } \alpha_2 \text{ of } f_2 - \alpha_1 \\ \dots \\ f_l - \alpha_{l-1} \text{ is irreducible over } K(\alpha_1, \dots, \alpha_{l-1})[X] \text{ for a root } \alpha_{l-1} \text{ of } f_{l-1} - \alpha_{l-2} \end{array} \right.$$

*Proof.* Given Capelli's Lemma [11, Lemma 2.4], the proof is straightforward by induction.  $\square$

We are now ready to state and prove the main theorem.

**Theorem 2.4.** *Let  $\mathcal{S}$  be a set of generators for a compositional semigroup  $C \subseteq \mathbb{F}_q[x]$ . Suppose that  $\mathcal{S}$  consists of polynomials of degree 2. Then we have that  $C \subseteq \text{Irr}(\mathbb{F}_q[x])$  if and only if no element of  $-D_{\mathcal{S}} = \{b_f \mid f \in \mathcal{S}\} \subseteq \mathbb{F}_q$  is a square and in  $G_{\mathcal{S}}$  there is no path of positive length from a node of  $D_{\mathcal{S}}$  to a square of  $\mathbb{F}_q$ .*

*Proof.* It is clear that  $C$  contains a reducible polynomial of degree 2 if and only if one element of  $-D_{\mathcal{S}}$  is a square. Thus we can assume that  $\mathcal{S}$  consists only of irreducible polynomials.

We now show that in  $G_{\mathcal{S}}$  there is a path of positive length from a node of  $D_{\mathcal{S}}$  to a square if and only if  $C$  contains a reducible polynomial of degree greater or equal than 4.

First, suppose that the composition  $f_1 f_2 \cdots f_{l+1}$  is a reducible polynomial of minimal degree, with  $f_i \in \mathcal{S}$  and  $f_i = (x - a_i)^2 - b_i$ , for  $i \in \{1, \dots, l+1\}$  and  $l \geq 1$ . Whenever  $\beta$  is not a square in  $\mathbb{F}_q$ , we denote by  $\sqrt{\beta}$  a root of the polynomial  $T^2 - \beta$  in the algebraic closure of  $\mathbb{F}_q$ . By Capelli's Lemma applied to the composition of  $f_1 \cdots f_l$  and by the minimality of the degree of  $f_1 f_2 \cdots f_{l+1}$ , we have that the following elements are not squares in their field of definition:

$$\begin{aligned} \beta_0 &:= b_1 \in \mathbb{F}_q, \\ \beta_1 &:= b_2 + a_1 + \sqrt{\beta_0} \in \mathbb{F}_{q^2} \\ \beta_2 &:= b_3 + a_2 + \sqrt{\beta_1} \in \mathbb{F}_{q^{2^2}} \\ &\dots \\ \beta_{l-1} &:= b_l + a_{l-1} + \sqrt{\beta_{l-2}} \in \mathbb{F}_{q^{2^{l-1}}}. \end{aligned}$$

On the other hand,  $\beta_l = b_{l+1} + a_l + \sqrt{\beta_{l-1}} \in \mathbb{F}_{q^{2^l}}$  is necessarily a square. For  $j < l$ , let us denote by  $N_i^j : \mathbb{F}_{q^{2^i}} \rightarrow \mathbb{F}_{q^{2^j}}$  the usual norm map. We claim that the  $\mathbb{F}_q$ -norm  $N_l^0 : \mathbb{F}_{q^{2^l}} \rightarrow \mathbb{F}_q$  maps  $\beta_l$  to  $f_1(\cdots f_l(-b_{l+1})\cdots)$ , and this defines a path in  $G_{\mathcal{S}}$  from  $-b_l$  to a square. This can be easily seen by first

decomposing  $N_l^1$ :

$$N_l^1 = N_2^1 \circ N_3^2 \circ \dots \circ N_l^{l-1}$$

and then by directly computing  $N_2^1 \circ N_3^2 \circ \dots \circ N_l^{l-1}(\beta_l)$ . It is important indeed that  $\beta_0, \beta_1, \dots, \beta_{l-1}$  are not squares, as the computation above only gives the desired result when  $(\sqrt{\beta_i})^{q^{2^i}} = -\sqrt{\beta_i}$ .

Conversely, suppose that in  $G_{\mathcal{S}}$  there is a path to a square  $s$ . Choose such a path of minimal length, starting at some  $-b_f$  in the distinguished set, for some  $f \in \mathcal{S}$ . Consider now the composition associated to this path: if

$$s = f_1 f_2 \cdots f_l(-b_f),$$

set  $f_{l+1} = f$  and let  $g := f_1 f_2 \cdots f_{l+1} \in \mathbb{F}_q[x]$ . One can construct the  $\beta_i$ 's as before, i.e.  $\beta_0 = b_1$  and for  $i \in \{1, \dots, l\}$ ,  $\beta_i = b_{i+1} + a_i + \sqrt{\beta_{i-1}}$ . We can suppose that the  $\beta_i$ 's for  $i < l$  are all non-squares as otherwise, by taking the smallest  $d$  such that  $\beta_d$  is square, we find a composition  $f_1 f_2 \cdots f_{d+1}$  that is reducible by Recursive Capelli's Lemma, and then we are done.

As all the  $\beta_i$ 's, for  $i < l$ , can be supposed to be non-squares, we have as above that  $N_l^0(\beta_l) = f_1 f_2 \cdots f_l(-b_{l+1}) = s$ , which we have assumed to be a square. Now, recall that an element of a finite field is a square if and only if its norm is a square: this shows that  $g$  is reducible by Recursive Capelli's Lemma.  $\square$

The reader should observe that this theorem generalizes [11, Proposition 2.3]. It is useful to mention the following corollary, which is immediate.

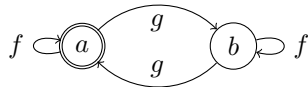
**Corollary 2.5.** *Let  $\mathcal{S}$  be a set of irreducible degree two polynomials and  $C$  defined as in Theorem 2.4. Then  $C \subseteq \text{Irr}(\mathbb{F}_q[x])$  if and only if there is no path of positive length from a node of  $D_{\mathcal{S}}$  to a square of  $\mathbb{F}_q$ .*

*Proof.* It is enough to observe that whenever  $\mathcal{S} \subseteq \text{Irr}(\mathbb{F}_q[x])$  then  $-D_{\mathcal{S}}$  consists of non-squares.  $\square$

*Remark 2.6.* Given that  $C$  is generated by degree 2 polynomials, it is easy to observe that the datum of  $\mathcal{S}$  is equivalent to the datum of  $C$ .

The following example shows a way to find examples of semigroups contained in  $\text{Irr}(\mathbb{F}_q[x])$  when  $q \equiv 1 \pmod{4}$ .

*Example 2.7.* Let  $q \equiv 1 \pmod{4}$  be a prime power, and let  $a \in \mathbb{F}_q$  such that both  $a$  and  $b = a + 1$  are non-squares. Define  $f = (x - a)^2 + a$  and  $g = (x - b)^2 + a$ . In this situation, we have  $D_{\mathcal{S}} = \{a\}$ , and by assumption,  $-a$ ,  $a$  and  $b$  are all non-squares. Since  $f(a) = g(b) = a$  and  $f(b) = g(a) = b$ , all paths in  $G_{\mathcal{S}}$  starting from  $a$  end in a non-square, and the conditions of Theorem 2.4 are satisfied. Figure 1 shows the relevant part of the graph  $G_{\mathcal{S}}$ . The reader should observe that this is indeed the example mentioned in the introduction.


 FIGURE 1. The nodes of  $G_{\mathcal{S}}$  reachable from  $D_{\mathcal{S}}$ .

### 3. THE CASE $p \equiv 3 \pmod{4}$

Whenever  $q = p$  is a prime congruent to 3 modulo 4, we have the following non-existence results.

**Lemma 3.1.** *Let  $p \equiv -1 \pmod{8}$  be a prime, and let  $f = x^2 - b$  be a polynomial in  $\mathbb{F}_p[x]$ . Let  $C$  be the semigroup generated by  $f$ . Then  $C$  contains a reducible polynomial.*

*Proof.* Assume for contradiction that  $C \subset \text{Irr}(\mathbb{F}_p[x])$ . First note that if  $b$  is a square, then  $f$  is reducible, so we can assume that  $b$  is not a square, and thus  $-b$  is a square. Consider the set of iterates  $T = \{f(-b), f^2(-b), \dots\} \subseteq \mathbb{F}_p$ . By Corollary 2.5,  $C$  contains only irreducible polynomials if and only if  $T$  contains only nonsquares. So assume that this condition holds. Since  $T$  is finite, there exist  $k < m \in \mathbb{N}_{>0}$  such that  $f^m(-b) = f^k(-b)$ . Choose  $k$  to be minimal. Now there are two cases: if  $k > 1$ , then there exist two distinct elements  $u, v \in T$  such that  $u^2 - b = v^2 - b$ . Thus,  $u = -v$ , which implies that one between  $u$  and  $v$  is a square, a contradiction. If on the other hand  $k = 1$ , then we have  $f^m(-b) = f(-b) = b^2 - b$ , and so  $f^{m-1}(-b)$  is either  $-b$  or  $b$ . It can't be  $-b$ , since that is a square, so we must have  $f^{m-1}(-b) = b \in T$ . Setting  $u = f^{m-2}(-b)$ , we get that  $u^2 - b = b$  and so  $u^2 = 2b$ , which is a contradiction because 2 is a square in  $\mathbb{F}_p$  and consequently  $2b$  is not.  $\square$

**Proposition 3.2.** *Let  $p \equiv 3 \pmod{4}$  be a prime. Let  $f = x^2 - b_f$  and  $g = x^2 - b_g$  be polynomials in  $\mathbb{F}_p[x]$  with  $b_f, b_g$  distinct non-squares. Let  $\mathcal{S} = \{f, g\}$  and let  $C$  be the semigroup generated by  $\mathcal{S}$ . Then  $C$  contains a reducible polynomial.*

*Proof.* Let  $G_{\mathcal{S}}$  be the graph attached to  $\mathcal{S}$  as in Definition 2.1. Let  $G'_{\mathcal{S}}$  be the induced subgraph consisting of all nodes of  $G_{\mathcal{S}}$  that are reachable by some path of positive length starting from  $-b_f$  or  $-b_g$ . That is, the edges of  $G'_{\mathcal{S}}$  are just the edges of  $G_{\mathcal{S}}$  starting and ending at a node in  $G'_{\mathcal{S}}$ . From now on, when we speak of nodes and edges, we will always be referring to nodes and edges in  $G'_{\mathcal{S}}$ . We call an edge from  $u$  to  $v$  an  $f$ -edge if it comes from the relation  $f(u) = v$ , while we call it a  $g$ -edge if it comes from  $g(u) = v$ . Since  $b_f$  and  $b_g$  are assumed nonsquare, we have by Corollary 2.5 that  $C$  contains a reducible polynomial if and only if at least one of the nodes of  $G'_{\mathcal{S}}$  is a square. In the following, we assume for contradiction that  $G'_{\mathcal{S}}$  consists only of non-squares.

Let us observe the following: suppose that there exists a node  $v$  of  $G'_S$  which is the target of two  $f$ -edges. By definition, this means that there exist two distinct nodes  $u, u' \in G'_S$  such that  $u^2 - b_f = u'^2 - b_f = v$ . This implies that  $u' = -u$ , and thus one between  $u$  and  $u'$  is a square, since  $-1$  is not a square in  $\mathbb{F}_p$ . This contradicts our assumption. By symmetry, the same applies to  $g$ -edges.

By the argument above, we see that every node is the target of at most one  $f$ -edge and one  $g$ -edge, and by counting edges that it is indeed exactly one of each.

Now, consider the sum

$$\sum_{v \in G'_S} (f(v) - g(v)).$$

On one hand, each node  $u \in G'_S$  appears exactly once as  $f(v)$  and once as  $g(v')$  for some  $v, v' \in G'_S$ , so the sum is zero. On the other hand, it clearly holds that  $f(v) - g(v) = b_g - b_f$  for all  $v$ . Letting  $n$  be the number of nodes in  $G'_S$ , we get the equation

$$0 = n(b_g - b_f) \text{ in } \mathbb{F}_p.$$

Since  $b_f \neq b_g$  by hypothesis, we must have  $p \mid n$ . This is impossible however, since  $G'_S$  is not empty and consists only of nonsquares, so  $1 \leq n \leq \frac{p-1}{2}$ .  $\square$

The fact that the polynomials of Proposition 3.2 don't have a linear term is of crucial importance. Let us see why by giving an explicit example of a semigroup of irreducible polynomials in  $\mathbb{F}_p[x]$  for which Proposition 3.2 does not apply (but  $p \equiv 3 \pmod{4}$ ).

*Example 3.3.* Let us fix  $p = 7$  and

$$f = (x - 1)^2 - 5 = x^2 + 5x + 3 \in \mathbb{F}_7[x]$$

$$g = (x - 4)^2 - 5 = x^2 + 6x + 4 \in \mathbb{F}_7[x].$$

The set  $\mathcal{S} = \{f, g\}$  has distinguished set  $D_S = \{-5\}$  and graph as in Figure 2. Since 5 is not a square, and we only look at paths of positive length, the final

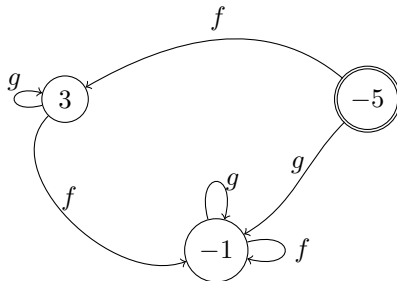


FIGURE 2. The nodes of  $G_S$  reachable from  $-5$ .

claim follows by checking that 3 and  $-1$  are not squares modulo 7.

## REFERENCES

- [1] Rudolf Lidl and Harald Niederreiter. *Finite fields*, volume 20. Cambridge university press, 1997.
- [2] Gary L. Mullen and Daniel Panario. *Handbook of finite fields*. CRC Press, 2013.
- [3] Michael O. Rabin et al. *Fingerprinting by random polynomials*. Center for Research in Computing Techn., Aiken Computation Laboratory, Univ., 1981.
- [4] Razvan Barbulescu, Pierrick Gaudry, Antoine Joux, and Emmanuel Thomé. A heuristic quasi-polynomial algorithm for discrete logarithm in finite fields of small characteristic. In *Advances in Cryptology–EUROCRYPT 2014*, pages 1–16. Springer, 2014.
- [5] Alina Ostafe and Igor E. Shparlinski. On the length of critical orbits of stable quadratic polynomials. *Proceedings of the American Mathematical Society*, 138(8):2653–2656, 2010.
- [6] Omran Ahmadi, Florian Luca, Alina Ostafe, and Igor E. Shparlinski. On stable quadratic polynomials. *Glasgow Mathematical Journal*, 54(02):359–369, 2012.
- [7] Shuhong Gao, Jason Howell, and Daniel Panario. Irreducible polynomials of given forms. *Contemporary Mathematics*, 225:43–54, 1999.
- [8] Shuhong Gao and Daniel Panario. Tests and constructions of irreducible polynomials over finite fields. In *Foundations of Computational Mathematics*, pages 346–361. Springer, 1997.
- [9] Victor Shoup. New algorithms for finding irreducible polynomials over finite fields. *Mathematics of Computation*, 54(189):435–447, 1990.
- [10] Rafe Jones. An iterative construction of irreducible polynomials reducible modulo every prime. *Journal of Algebra*, 369:114–128, 2012.
- [11] Rafe Jones and Nigel Boston. Settled polynomials over finite fields. *Proceedings of the American Mathematical Society*, 140(6):1849–1863, 2012.
- [12] Julio Andrade, Steven J. Miller, Kyle Pratt, and Minh-Tam Trinh. Special sets of primes in function fields. *arXiv preprint arXiv:1309.5597*, 2013.
- [13] Joachim von Zur Gathen. Irreducible trinomials over finite fields. *Mathematics of Computation*, 72(244):1987–2000, 2003.
- [14] Anjula Batra and Patrick Morton. Algebraic dynamics of polynomial maps on the algebraic closure of a finite field, i. *JOURNAL OF MATHEMATICS*, 24(2), 1994.
- [15] Anjula Batra and Patrick Morton. Algebraic dynamics of polynomial maps on the algebraic closure of a finite field, ii. *Rocky Mountain J. Math.*,

24(3):905–932, 09 1994.

- [16] Andrea Ferraguti and Giacomo Micheli. On the existence of infinite, non-trivial  $F$ -sets. *arXiv preprint arXiv:1602.06608*, 2016.

INSTITUTE OF MATHEMATICS, UNIVERSITY OF ZURICH, WINTERTHURERSTRASSE 190, 8057 ZURICH, SWITZERLAND,

*E-mail address:* `andrea.ferraguti@math.uzh.ch`

MATHEMATICAL INSTITUTE, UNIVERSITY OF OXFORD, WOODSTOCK RD., OXFORD OX2 6GG, UNITED KINGDOM

*E-mail address:* `giacomo.micheli@maths.ox.ac.uk`

INSTITUTE OF MATHEMATICS, UNIVERSITY OF ZURICH, WINTERTHURERSTRASSE 190, 8057 ZURICH, SWITZERLAND,

*E-mail address:* `reto.schnyder@math.uzh.ch`