Bull. Austral. Math. Soc. 11T06
Vol. 40 (1989) [407–412]

THE REDUCIBILITY THEOREM FOR LINEARISED POLYNOMIALS OVER FINITE FIELDS

Stephen D. Cohen

A self-contained elementary account is given of the theorem of S. Agou that classifies all composite irreducible polynomials of the form $P\left(x^{p^n} + a_{n-1}x^{p^{n-1}} + \ldots + a_0x\right)$ over a finite field of characteristic p. Written to appeal to a wide readership, it is intended to complement the original rather technical proof and other contributions by the author and by Moreno.

1. Introduction

A *linearised polynomial* $f(x)$ over a field F_q of prime power order $q = p^k$ is one of the form

$$f(x) = a_nx^{p^n} + a_{n-1}x^{p^{n-1}} + \ldots + a_1x^p + a_0x \tag{1}$$

in $F_q[x]$, where $n \geqslant 0$. Because $(x+y)^p = x^p + y^p$ in F_q, evidently a linearised polynomial f represents a linear mapping on F_q as a vector space over the prime field F_p; thus

$$\begin{aligned} f(x+y) &= f(x) + f(y) \text{ for all } x, y \text{ in } F_q, \\ f(cx) &= cf(x) \text{ for all } x \text{ in } F_q \text{ and } c \text{ in } F_p. \end{aligned} \tag{2}$$

A simple consequence is that the set of roots of f form a linear subspace of any field containing them. Not suprisingly, because of this structure, much can be said, both theoretically and practically, about questions of reducibility and root finding for linearised and related polynomials (see [**8**, Chapter 3, Sections 4 and 5 and the Notes on pp.136–138]).

The theorem which is our topic was first proved by S. Agou in a series of papers [**1**, **3**, **4**]. It specifies precisely those composites of linearised polynomials $P(f)$, where P is a polynomial of degree m over F_q, that are irreducible over F_q, asserting, in particular, that $P(f)$ is always reducible when $n > 2$. Moreover, when $n = 2$, irreducible composites only occur if $p = 2$ and m is odd. (The full statement is given later.)

Received 29 November, 1988

https://doi.org/10.1017/S0004972700017445 Published online by Cambridge University Press

Now, composites of linearised polynomials have been most studied when the indices of x in the terms of $f(x)$ are powers of q (not just p as shown in (1)), in which case f is F_q-linear over any extension of F_q. For such, very general theorems exist displaying the explicit reducibility pattern of $P(f)$ over F_q; this comprises a listing of the degrees of the irreducible factors of f with the number of factors of each degree (see, for example, [**9, 10**]). These results are a rich source of supply of irreducible polynomials of arbitrary degree over F_q. On the other hand, although factorising an arbitrary $P(f)$ in any particular case is relatively easy, the task of describing the general reduciblity pattern within a single theorem is a challenge, and even to delineate the relevant f and P for which $P(f)$ is irreducible is a non-trivial exercise. In aggregate, Agou's proof of the reducibility theorem in [**1, 3, 4**] is somewhat lengthy with many technical details and the consideration of particular cases. (In fact, we note that, at the cost of yet more complication, he has extended his argument in some instances [**2, 5**] to yield the minimum degree of an irreducible factor of $P(f)$.)

In [**7**], I gave a much shorter conceptual explanation of the theorem based, however, on relatively sophisticated ideas involving group theory applied to the Galois group of a polynomial associated with f. Finally, a short proof of the theorem for $n > 2$ can be extracted from two more recently published articles of Moreno [**11, 12**]. In qualifying this, we remark that the proof for $p = 2$ in [**11**] is derived from more elaborate considerations while that for $p > 2$ in [**12**] (by induction on n) needs Agou's work for $n = 2$ (itself the product of detailed effort) to start it off. It has also to be said that the exposition is unclear; there are undoubtedly several misprints (for further comments see the review of [**11**] in *Mathematical Reviews*, 88g: 11091). Nevertheless, drawing on the virtues of his work, I found two aspects (mentioned below) that are the key to a brief proof, simple enough I felt to be worthwhile assembling here for general appreciation. Apart from some very basic facts about vector spaces and finite fields it has been made self-contained. The new trick is to split the proof into two parts and apply the easier first part (for which $n = 1$) to the second.

2. Simplifications

Some simplifications are obvious. We can assume that f and P are monic; that is, $a_n = 1$ in (1) and $P(x) = x^m + b_{m-1}x^{m-1} + \ldots + b_0$, say. Trivially $P(f)$ is reducible over F_q whenever P is, and therefore we suppose that P is irreducible. Finally, because *any* polynomial in $F_q[x^p]$ (being the pth power of one in $F_q[x]$) is reducible, we can in (1), without loss, impose the restriction that $a_0 \neq 0$.

Next, let β be a root of $P(x)$ in F_{q^m} and α any root of $f(x) - \beta$ (in a suitable extension); thus α is also a root of $P(f)$. Because $F_q(\beta) = F_{q^m}$ has degree m over F_q, we have that $\deg[F_q(\alpha)\colon F_q] = m\deg[F_q(\alpha)\colon F_q(\beta)]$ and recover the (well-known)

https://doi.org/10.1017/S0004972700017445 Published online by Cambridge University Press

conclusion that $P(f)$ is irreducible over F_q if and only of $f(x) - \beta$ is irreducible over F_{q^m}. In much of our discussion therefore we may take $m = 1$ and concentrate on the reducibility of polynomials of the form $f(x) - b$ over F_q. The latter are referred to as *affine polynomials* and are discussed with applications to coding theory in [6, Chapter 11]. Given one root α of such a polynomial, the full set of roots is the translate $\alpha + L$ of L, the linear space of roots of f. We highlight the fact (featured in [**12**]) that an affine polynomial for which f is non-singular over F_q is bound to be reducible.

LEMMA 1. *Suppose that the linearised polynomial f has no non-zero root in F_q. Then, for any b in F_q, $f(x) - b$ has a linear factor $x - A$, $A \in F_q$.*

PROOF: f is an injective mapping on F_q since, if $x, y \in F_q$ are such that $f(x) = f(y)$ then, by (2), $f(x - y) = 0$ and so $x = y$, by hypothesis. Because F_q is finite, it follows that f is also surjective which implies the result as stated. ∎

3. THE CASE $n = 1$.

We set $f(x) = x^p - ax$, where $a(\neq 0) \in F_q$. Of course the reducibility of $x^p - ax - b$ is well enough known (see [8, pp.127–129]) but we review it here within the present context.

From Lemma 1, $x^p - ax - b$ can be irreducible over F_q only if $x^{p-1} - a$ has a root in F_q. Assume therefore that $A^{p-1} = a$, where $A \in F_q$, in which case irreducibility is equivalent to that of $x^p - x - b/A^p$. Replacing b/A^p by b we may thus suppose that $a = A = 1$.

Let $T_k(x)$ be the linearised polynomial $x + x^p + \ldots + x^{p^{k-1}}$, the *trace function* from F_q to F_p (because $x^{p^k} = x$ for all x in F_q). Clearly the image space of the linear mapping $x^p - x$ acting on F_q has dimension $k - 1$ (because the null space is F_p) and is contained in the null space of the linear mapping $T_k(x)$. Indeed these spaces must be identical because $T_k(x) = 0$ has (at most) p^{k-1} solutions x in F_q. We conclude that $b = x^p - x$ for some x in F_q if and only if $T_k(b) = 0$.

Suppose that $T_k(b) \neq 0$ (so that $b = x^p - x$ is insoluble in F_q). Let α be a root of $x^p - x - b$; thus $\alpha \notin F_q$. The full set of roots is $\{\alpha + c \mid c \in F_p\}$ and the fields $F_q(\alpha + c)$, $c \in F_p$ are identical. Hence $\deg[F_q(\alpha): F_q]$ divides the prime p. The only conclusion possible is that $F_q(\alpha) = F_{q^p}$ and $x^p - x - b$ is irreducible. We summarise the above reasoning in a lemma.

LEMMA 2. *For any b in F_q, $x^p - ax - b$ is irreducible over F_q if and only if $a = A^{p-1}$ for some A in F_q and $T_k(a/A^p) \neq 0$.*

We deduce the first (and smaller) part of Agou's theorem.

https://doi.org/10.1017/S0004972700017445 Published online by Cambridge University Press

THEOREM. Part (i) *Let $P(x) = x^m + b_{m-1}x^{m-1} + \ldots + b_0$ be irreducible over F_q and β be a root of P. Then, for any non-zero a in F_q, $P(x^p - ax)$ is irreducible over F_q if and only if $a^{m_1(q-1)/(p-1)} = 1$ and $T_{km}(\beta/A^p) \neq 0$. Here $m_1 = \text{g.c.d.}(m, p-1)$ and $A^{p-1} = a$, where $A \in F_{q^m}$.*

In particular, if A is in F_q, then $P\left(x^p - A^{p-1}x\right)$ is irreducible over F_q if and only if $T_k(b_{m-1}/A^p) \neq 0$ (or equivalently $x^p - A^{p-1}x - b_{m-1}$ is irreducible over F_q or, indeed, insoluble over F_q).

PROOF: Apply Lemma 2 to $x^p - ax - \beta$ over F_{q^m}. Now, $a = A^{p-1}$ for $A \in F_{q^m}$ if and only if

$$a^{(q^m-1)/(p-1)} = 1. \tag{3}$$

But, since $a^{q-1} = 1$, then (3) holds if and only if $a^h = 1$, where

$$h = \left(\frac{q^m - 1}{p-1}, q-1\right) = \left(\frac{q^m - 1}{q-1}, p-1\right)\frac{q-1}{p-1}.$$

Moreover, $(q^m - 1)/(q-1) = q^{m-1} + q^{m-2} + \ldots + 1 \equiv m \pmod{p-1}$ and consequently $h = m_1(q-1)/(p-1)$.

Finally, if $A \in F_q$, then $A^q = A$ while $\beta + \beta^q + \ldots + \beta^{q^{m-1}} = -b_{m-1}$. Hence $T_{km}(\beta/A^p) = T_k(-b_{m-1}/A^p)$ and the proof is complete. □

4. THE CASE $n > 1$.

Begin with a simple version of the "division algorithm" for linearised polynomials, not necessarily monic, as follows.

LEMMA 3. *Given a linearised polynomial f over F_q, there exists another linearised polynomial g over F_q (g being the zero polynomial if $n = 0$) and an element r in F_q such that*

$$f(x) = g(x^p - x) + rx.$$

PROOF: This is by induction on n, the case $n = 0$ being trivial. Suppose $n \geqslant 1$ and put

$$f^\star(x) = f(x) - a_n(x^p - x)^{p^{n-1}} = (a_{n-1} + a_n)x^{p^{n-1}} + \ldots,$$

another linearised polynomial but of degree (at most) p^{n-1}. By induction, there is a linearised polynomial $g^\star$ such that $f^\star(x) = g^\star(x^p - x) + rx$ and we simply define $g(x) = x^{p^{n-1}} + g^\star(x)$ to reach the conclusion desired. □

Next comes a deduction from Lemma 3 also crucial in [**12**], although used there for a different purpose.

https://doi.org/10.1017/S0004972700017445 Published online by Cambridge University Press

LEMMA 4. *Suppose that the linearised polynomial f over F_q has a non-zero root A in F_q. Then there exists a linearised polynomial g over F_q such that $f(x) = g(x^p - A^{p-1}x)$.*

PROOF: $f(Ax)$ is a linearised polynomial over F_q with 1 as a root. By Lemma 3, for some linearised polynomial g_1 and r in F_q, we have $f(Ax) = g_1(x^p - x) + rx$. Actually, $r = 0$ because $x = 1$ yields $0 = f(A) = g_1(0) + r = r$. The result follows, with $g(x) = g_1(x/A^p)$. □

From now on, we suppose that $n \geqslant 2$ and f is monic.

LEMMA 5. *Suppose that f is a linearised polynomial over F_q with $n \geqslant 2$. Then, for any b in F_q, $f(x) - b$ is irreducible over F_q if and only if $p = n = 2$, f has the form*

$$f(x) = x(x + A)(x^2 + Ax + B) \tag{4}$$

where A and B are (non-zero) elements of F_q and the quadratics $x^2 + Ax + B$ and $x^2 + Bx + b$ are both irreducible over F_q.

Note. By Lemma 2, when $p = 2$, $x^2 + Ax + B$ is irreducible over F_q if and only if $T_k(B/A^2) = 1$ (since 1 is the only non-zero member of F_2); similarly $x^2 + Bx + b$ is irreducible if and only if $T_k(b/B^2) = 1$.

PROOF: By Lemma 1 we may assume that f has a root A in F_q. Using Lemma 4, write $f(x) = g(x^p - A^{p-1}x)$ and put $g^\star(x) = g(x) - b$. Then $f(x) - b = g^\star(x^p - A^{p-1}x)$. Apply the last assertion of Part (i) of the Theorem with $m = \deg g^\star = p^{n-1}$. Since g is a linearised polynomial, the coefficient b_{m-1} of x^{m-1} in $g^\star$ is zero unless $p^{n-1} - 1 = p^{n-2}$ which occurs only if $p = n = 2$. Hence, with this exception, $T_k(b_{m-1}/A^p) = 0$ and $f(x) - b$ is reducible. Finally, suppose $p = n = 2$ and $g^\star(x) = x^2 + Bx + b$. By Part (i) of the Theorem again, $f(x) + b$ is irreducible if and only if both $g^\star(x)$ and $x^2 + Ax + B$ are. This completes the proof. □

We deduce the major part of the Theorem from Lemma 5.

THEOREM. Part (ii) *Let P be an irreducible polynomial of degree m over F_q (as in Part (i)) and f be a monic linearised polynomial over F_q with $n \geqslant 2$. Then $P(f)$ is irreducible over F_q if and only if $p = n = 2$, m is odd, f has the form (4) where A and B are in F_q and both $x^2 + Ax + B$ and $x^2 + Bx + b_{m-1}$ are irreducible over F_q.*

PROOF: Apply Lemma 5 to $f(x) - \beta$ over F_{q^m}, where $P(\beta) = 0$. We conclude that $P(f)$ is irreducible over F_q if and only if $p = n = 2$ and f has the form (4) where A, $B \in F_{q^m}$ with $x^2 + Ax + B$ irreducible over F_{q^m} and $T_{km}(\beta/B^2) = 1$. Assuming therefore that $p = n = 2$, we show that these last conditions are equivalent to those of the theorem. To see this we note that $f(x)/x$, being a polynomial in $F_q[x]$, has an irreducible quadratic factor in F_{q^m} if and only if it has one over F_q and m is odd. (Of course, if $f(x)/x$ is irreducible over F_q it remains so, or is a product of linear factors over F_{q^m}). Hence x^2+Ax+B is irreducible over F_{q^m} if and only if A and hence B are in F_q, x^2+Ax+B is irreducible over F_q and m is odd.

Finally, these last conditions imply that $T_{km}(\beta/B^2) = T_k(b_{m-1}/B^2)$ (as B is in F_q); also $T_k(b_{m-1}/B^2) = 1$ if and only if x^2+Bx+b_{m-1} is irreducible over F_q. This completes the proof. $\square$

References

[1] S. Agou, 'Irréducibilité des polynômes $f\left(X^{p^r}-aX\right)$ sur un corps fini F_{p^s}', *J. Reine Agnew. Math.* **292** (1977), 191–195.

[2] S. Agou, 'Factorisation sur un corps fini F_pn des polynômes composés $f\left(X^{p^r}-aX\right)$ lorsque $f(X)$ est un polynôme irréductible de $F_{p^n}[X]$', *J. Number Theory* **9** (1977), 229–239.

[3] S. Agou, 'Irréductibilité des polynômes $f\left(X^{p^{2r}}-aX^{p^r}-bX\right)$ sur un corps fini F_{p^s}', *J. Number Theory* **10** (1978), 64–69. **11** (1979) 20.

[4] S. Agou, 'Irréductibilité des polynômes $f\left(\sum_{i=0}^{m} a_i X^{p^{ri}}\right)$ sur un corps fini F_{p^s}', *Canad. Math. Bull.* **23** (1980), 207–212.

[5] S. Agou, 'Sur la factorisation des polynômes $f\left(X^{p^{2r}}-aX^{p^r}-bX\right)$ sur un corps fini F_{p^s}', *J. Number Theory* **12** (1980), 447–459.

[6] E.R. Berlekamp, *Algebraic Coding Theory* (McGraw-Hill, New York, 1968).

[7] S.D. Cohen, 'The irreducibility of compositions of linear polynomials over a finite field', *Compositio Math.* **47** (1982), 149–152.

[8] R. Lidl and H. Niederreiter, 'Finite Fields', in *Encyclopedia Math. App. Vol. 20*, now distributed by Cambridge University Press (Addison Wesley, Reading, Mass.).

[9] A.F. Long, 'Factorisation of irreducible polynomials over a finite field with the substitution $x^{q^r}-x$ for x', *Acta Arith.* **25** (1973), 65-80.

[10] A.F. Long and T.P. Vaughan, 'Factorisation of $Q(h(T)(x))$ over a finite field where $Q(x)$ is irreducible and $h(T)(x)$ is linear I, II', *Linear Algebra* **11** (1975), 53–72. **13** (1976), 207–221 .

[11] O. Moreno, 'Discriminants and the irreducibility of a class of polynomials', *Lect. Notes in Comput. Sci.* **228** (1988), 178–181.

[12] O. Moreno, 'Discriminants and the irreducibility of a class of polynomials in a finite field of arbitrary characteristic', *J. Number Theory* **28** (1988), 62–65.

Department of Mathematics
University of Glasgow
Glasgow G12 8QW
Scotland

https://doi.org/10.1017/S0004972700017445 Published online by Cambridge University Press