Bull. Korean Math. Soc. **22**(1985), No. 1, pp. 53-56

REDUCIBILITY OF SUB-LINEAR POLYNOMIALS OVER A FINITE FIELD

STEPHEN D. COHEN

Let $f(x)=\sum_{i=1}^{m} a_i x^i$ be a polynomial of degree m with coefficients in F_q, the finite field of order q. For each positive integer n associate with f the ***linear polynomial*** $\hat{f}_n(x)$, defined by

$$\hat{f}_n(x)=\sum_{i=1}^{m} a_i x^{q^{ni}},$$

and what we shall term the ***sub-linear polynomial*** $f_n^*(x)$, defined by

$$f_n^*(x)=\sum_{i=1}^{m} a_i x^{(q^{ni}-1)/(q^n-1)}$$

Thus $\hat{f}_n(x)=xf_n^*(x^{q^n-1})$. When $n=1$ we write $\hat{f}$ and f^* for $\hat{f}_1$ and f_1^*, respectively.

Suppose f is an irreducible polynomial over F_q. Then (see [4] and [5]) the linear polynomial $\hat{f}$ has the interesting property that the degree of every irreducible factor of $\hat{f}(x)/x$ is equal to N, the *period* (*order* or *exponent*) of f which is the least integer for which $\hat{f}(x)$ divides x^N-1). Further, provided $(N,q-1)=1$, Mills [3] has shown that every irreducible factor of the sub-linear polynomial $f^*(x)$ also has degree N and, in general, that the degree of every such factor of $f_n^*(x)$ always divides nN.

In this note we indicate that there is another number associated with f (which we shall call the *sub-period* and denote by M) which appears to be more relevant than the period N in discussing sub-linear polynomials. Define M as the least positive integer for which $f(x)$ divides x^M-a for some a in F_q. (Hirschfeld [1] and Kang [2] refer to M as, respectively, the *subexponent* and *Shinwon* number of f).

The following properties of the sub-period are fairly obvious (see [1], p. 7).

(i) M divides $(q^m-1)/(q-1)$,
(ii) $N=Me$, where e is the order of a in F_q,
(iii) $M=N$, whenever $(N,q-1)=1$.

Further, Mills [3] has shown that there is a connection between polynomials and their sub-linear associates similar to the connection between polynomials and their linear associates, see [4].

LEMMA 1. *$f(x)$ divides $g(x)$ if and only if $f_n^*(x)$ divides $g_n^*(x)$.*

THEOREM 2. *Suppose that $f(x)$ is an irreducible polynomial over F_q with sub-period M. Then the degree of every irreducible factor of $f_n^*(x)$ divides nM.*

Proof. Since $f(x)$ divides x^M-a then $f_n^*(x)$ divides $x^{(q^{nM}-1)/(q^n-1)}-a$ which, in turn, divides $x^{q^{nM}}-x$.

S. W. Kang [2] has proved that, if $f(x)=x^2-x-a$ is an irreducible quadratic over a prime field F_p with sub-period $p+1$ then $f^*(x)=x^{p+1}-x-a$ is also irreducible over F_p. This is a special case of the following much more general result.

THEOREM 3. *Suppose that $f(x)$ is an irreducible polynomial over F_q with sub-period M. Then the degree of every irreducible factor of $f^*(x)$ is M.*

Proof. We can suppose $f(x)\neq ax$. Suppose that $E(x)$ is an irreducible factor of $f^*(x)$ of degree D. Then, by Theorem 2, D divides M.
Since E is irreducible and divides

$$x^{q^D-1}-1=\prod_{b(\neq 0)\in F_q}(x^{(q^D-1)/(q-1)}-b),$$

$E(x)$ divides $x^{(q^D-1)/(q-1)}-c$ for some c in F_q. Suppose that the remainder on dividing x^D-c by $f(x)$ is $r(x)$ so that the degree of $r(x)$ is less than the degree of $f(x)$. We claim that, in fact, $r(x)=0$. Otherwise, by Lemma 1, we have

$$x^{(q^D-1)/(q-1)}-c=G(x)f^*(x)+r^*(x)$$

so that, in fact, $E(x)$ divides $r^*(x)$. Now, of course, f and r are co-prime so that there are polynomials $u(x)$ and $v(x)$ in $F_q[x]$ such that $u(x)f(x)+v(x)r(x)=1$. Put $g(x)=u(x)f(x)$ and $s(x)=v(x)r(x)$. Then, by Lemma 1 again, $f^*(x)\mid g^*(x)$ and $r^*(x)\mid s^*(x)$ while

$$g^*(x)+s^*(x)=1$$

We conclude that $E(x)$ divides 1, a contradiction. Hence r is the zero polynomial and so $D=M$.

EXAMPLE 1. Since $x^4+4=(x^2+2x+2)(x^2-2x+2)$ it follows that, if $q\equiv -1 \pmod 4$, then $f(x)=x^2+2x+2$ is an irreducible quadratic over F_q with sub-period 4. We deduce from Theorem 3 that in this case $f^*(x)=x^{q+1}+2x+2$ is the product of $\frac{1}{4}(q+1)$ irreducible polynomials of degree 4.

Mills [3] also showed that for certain values of $n>1$ the bound nN for the degree of the factors of $f^*(x)$ can be attained provided $(N, q^n-1)=1$. We now show that, actually, the bound nM of Theorem 2 can be attained, a necessary condition being $(M, (q^n-1)/(q-1))=1$.

THEOREM 4. *Suppose that f is an irreducible polynomial over F_q with sub-period M and n is a positive integer. Let $M^*=M/(M, (q^n-1)/(q-1))$ and suppose that, in fact, every prime which divides n also divides M^*. Then every irreducible factor of $f_n^*(x)$ has degree nM^*.*

Proof. We first prove that, for any n, the sub-period of f regarded as a polynomial in $F_qn[x]$ is equal to M^*.

Suppose $f(x)$ divides x^M-a, where $a\in F_q$. Then there is a primitive element r in F_qn for which $a=r^{(q^n-1)/e}$, where e is the order of a. Now $e/q-1$ and $r^{(q^n-1)/(q-1)}$ is a primitive element of F_q so that $(M, (q-1)/e)=1$. Let $L=(M, (q^n-1)/(q-1))$ and $(q^n-1)/(q-1)=QL$. Then $(M^*, Q(q-1)/e)=1$. Moreover,

$$x^M-a=x^{LM^*}-\beta^L=\prod_{i=1}^{L-1}(x^{M^*}-\zeta^i\beta),$$

where $\beta=r^{Q(q-1)/e}$ and ζ is a primitive L-th root of unity (necessarily in F_qn). Thus, over F_qn, $f(x)$ divides $x^{M^*}-\zeta^i\beta$, say, and M^* is clearly the least integer with such a property.

We deduce from Theorem 3 that the degree of every irreducible factor of $f_n^*(x)$ over F_qn is M^*, or puting this another way, we have deg $(F_qn(\alpha)/F_qn)=M^*$ where α is any zero of $f_n^*(x)$. It follows that $\deg(F_qn(\alpha)/F_q)=nM^*$ and hence, if $I=\deg\ (F_q(\alpha)/F_q)$, then I divides nM^*. To complete the proof, we show that, for the particular values of n stated, $I=nM^*$. If, however, this is not the case, then a prime p which divides nM^*/I also divides M^* and so I divides nM_1 where $M_1=M^*/p$. But this implies that $\alpha\in F_qnM$ and that deg $(F_qn(\alpha)/F_qn)=M_1$, a contradiction.

EXAMPLE 2. Over F_{11}, $x^3+5=(x+3)(x^2-3x-2)$. In fact, clearly x^2-3x-2 is irreducible with sub-period 3 (and period 30). Let $n=3^s$ for any s. Then, by Theorem 4, $x^{11^n+1}-3x-2$ is the product of irreducible polynomials of degree 3^{s+1}.

EXAMPLE 3. Over F_5, x^4+x-1 is an irreducible polynomial dividing $x^{78}-2$ and so has sub-period 78 (and period 312). Let $n=3^s13^t$ for any s and t. Then $\left(\frac{1}{4}(5^n-1), 78\right)=1$, so that $M^*(=M)=78$. Thus $x^{5^{3n}+5^{2n}+5^n+1}+x-1$ is the product of irreducible polynomials of degree $78n$.

References

1. J. W. P. Hirschfeld, *Projective geometries over finite fields*, Oxford, 1979.
2. S. W. Kang, *Remarks on finite fields*, Bull. Korean Math. Soc. **20** (1983), 81–85.

3. W.H. Mills, *The degrees of the factor of certain polynomials over finite fields*, Proc. Amer. Math. Soc. **25**(1970), 860-863.
4. O. Ore, *Contributions to the theory of finite fields*, Trans. Amer. Math. Soc. **36**(1934), 243-274.
5. N. Zierler, *On the theorem of Gleason and Marsh*, Proc. Amer. Math. Soc. **9**(1958), 236-237.

Department of Mathematics,
University of Glasgow,
Glasgow, G12 8QW,
Scotland