Mathematical Problems of Computer Science 35, 63 69. 2011.

Irreducible Compositions of Polynomials Over Finite Fields of Even Characteristic*

Saeid M. Mehrabi and Melsik K. Kyuregyan

Institue for Informatics and Automation Problems of NAS of RA
e-mail smbatt@ipia.sci.am

Abstract

This note presents some results with the constructive theory of synthesis of irreducible polynomials over a Galois field with even characteristic. We prove a theorem that plays an important role for constructing irreducible polynomials. By this theorem a recurrent method for constructing families of irreducible polynomials of degree $n2^k$ $(k = 1, 2, ...)$ over F_{2^s} is proposed.

1. Introduction

Let F_q be the Galois field with $q = p^s$ elements and of characteristic p. The problem of irreducibility of polynomials over finite fields is a case of special interest and plays an important role in modern engineering. such polynomials are used to implement arithmetic in extension fields and are found in many applications, including coding theory [1, 16, 18] cryptography [2. 3, 15] computer algebra systems [4] multivariate polynomial factorization [22] and parallel polynomial arithmetic [8].In particular, since the binary system of notation is mainly used in computing systems, the problem of the construction of irreducible polynomials over $F_{2^s}(s \geq 1)$ remains one of the most important ones from practical point of view(with exception to coding theory and elliptic curves cryptosystems). some results on the construction of irreducible polynomials over F_{2^s} the interested reader can find in [10, 17]. One of the methods for constructing irreducible polynomials is the composition method which allows constructions of irreducible polynomials of higher degree from the given irreducible polynomials with the use of a substitution operator (see [7. 11. 17]). Probably the most powerful result in this area is the following theorem by S. Cohen. Let $f(x), g(x) \in F_q[x]$ and let $P(x) = \sum_{i=0}^{n} c_i x^i \in F_q[x]$ be of degree n. Then the following composition

$$F(x) = g(x)^n P\left(\frac{f(x)}{g(x)}\right) = \sum_{i=0}^{n} c_i f(x)^i g(x)^{n-i},$$

is again a polynomial in F_q .The problem is to determine under what conditions $F(x)$ is irreducible over F_q. Obviously. for $F(x)$ to be irreducible. $P(x)$ must be irreducible and $f(x)$ and $g(x)$ be relatively prime.

*2000 Mathematics subject classifications: 47A68, 47A70

Theorem 1: (Cohen [6]). *Let $f(x).g(x) \in F_q[x]$,and let $P(x) \in F_q[x]$ be an irreducible polynomial of degree n . Then $F(x) = g(x)^n P(\frac{f(x)}{g(x)})$ is irreducible over F_q if and only if $f(x) - \alpha g(x)$ is irreducible over F_{q^n} for some root $\alpha \in F_{q^n}$ of $P(x)$.*
As a special case of Cohen's theorem we suppose quadratic transformation as follows

$$P(x) \to (dx^2 + rx + h)^n P\left(\frac{ax^2 + bx + c}{dx^2 + rx + h}\right).$$

The problem is to determine under what conditions this transformation construct new irreducible polynomials over $F_q[x]$. This quadratic transformation when $a = 1, d = 0. r, c, h \in F_q$ was studied by Kyuregyan in [14].
Suppose q is odd. in this case several authors including Cohen [7], McNay [19], Chapman [5]. Meyn [20] and Kyuregyan [12, 13], studied this problem and gave iterative constructions of irreducible polynomials and N-polynomial. Indeed most of these results are derived in [12, 13].
We suppose q is even. If $F(x) \in F_{2^s}[x]$ is a polynomial of degree n then Q-transformation $F(x)$ is defined by

$$F^Q(x) = x^n F(x + \delta^2 x^{-1}),$$

where $\delta \in F_{2^s}^*$. This transformation is associated with several names, including Varshamov [23], Meyn [20], Gao [9], Menezes et al [17] and Kyuregyan [10, 11]. Varshamov in [23] proved that this transformation can be used to produce an infinite sequence of irreducible polynomials over F_2 . Kyuregyan [10] suggested a more general construction over F_{2^s}.
The aim of this paper is to describe possible quadratic transformations

$$P(x) \to (dx^2 + rx + h)^n P\left(\frac{ax^2 + bx + c}{dx^2 + rx + h}\right).$$

into the ring $F_{2^s}[x]$, allowing to construct explicity irreducible polynomials of higher degree from the given polynomial $P(x)$, so that a and d can be Non-zero together. We begin with definitions and preliminary results in section 2. finally in section 3 we prove irreducibility $(dx^2 + rx + h)^n P(\frac{ax^2+bx+c}{dx^2+rx+h})$ over F_{2^s} in general case and we present a method of recurrent constructions of sequences of irreducible polynomials over F_{2^s}.

2. Definitions and Preliminary Results

Let F_q be a Galois field of order $q = 2^s$, where s is a natural number. with multiplicative group F_q^* . The trace function of F_{q^n} over F_q is

$$Tr_{q^n|q}(\alpha) = \sum_{i=0}^{n} \alpha^{q^i}. \quad \alpha \in F_{q^n}.$$

The trace function is a linear functional from F_{q^n} to F_q.

Proposition 1: (Lidl et al. [16]). *Let K be a finite field. Let F be a finite extension of K and E a finite extension of F.Then*

$$Tr_{E|K}(\alpha) = Tr_{F|K}\left(Tr_{E|F}(\alpha)\right). \quad \alpha \in E.$$

Proposition 2: (Menezes et al. [17]). *For $a, b \in F_q^*$, the trinomial $x^p - ax - b$ is irreducible over F_q if $a = A^{p-1}$ for some $a \in F_q$ and $Tr_{q|p}(\frac{b}{A^p}) \neq 0$.*

3. Irreducibility of Composition of Polynomials

Let $P(x)$ be an irreducible polynomial of degree n over F_{2^s} ,and ax^2+bx+c and dx^2+rx+h be relatively prime polynomials from $F_{2^s}[x]$ with a or d being non-zero. Further, it is always assumed that $P(x)$ is monic. Let

$$H(a,d)=\begin{cases} a^n & \text{for } d=0,\\ d^nP(\frac{a}{d}) & \text{for } d\neq 0.\end{cases}$$

Our goal is to find conditions under which the quadratic mapping

$$P(x)\to H(a,d)^{-1}(dx^2+rx+h)^nP\left(\frac{ax^2+bx+c}{dx^2+rx+h}\right),$$

produces an irreducible polynomial over F_{2^s}. Set

$$F(x)=H(a,d)^{-1}(dx^2+rx+h)^nP\left(\frac{ax^2+bx+c}{dx^2+rx+h}\right).$$

By Theorem 1 we know $F(x)$ is an irreducible polynomial overF_{2^s} if and only if $h(x)=(ax^2+bx+c)-\alpha(dx^2+rx+h)$ is an irreducible over $F_{2^{sn}}$, where α is some root of $P(x)$ in $F_{2^{sn}}$. We have

$$h(x)=(a-\alpha d)x^2+(b-\alpha r)x+(c-\alpha h).$$

But, by proposition 2, $h(x)$ is an irreducible polynomial over $F_{2^{sn}}$ if and only if

$$Tr_{2^{sn}|2}\left(\frac{(a-\alpha d)(c-\alpha h)}{(b-\alpha r)^2}\right)=1.$$

Theorem 2: *Let $P(x)=\sum_{i=0}^{n}c_ix^i$ be an irreducible polynomial of degree $n\geq 1$ over $F_{2^s}(P(x)\neq x)$ and ax^2+bx+c and dx^2+rx+h be relatively prime polynomials from $F_{2^s}[x]$ with a or d being non-zero, and $r\neq 0$. Then the polynomial*

$$F(x)=H(a,d)^{-1}(dx^2+rx+h)^nP\left(\frac{ax^2+bx+c}{dx^2+rx+h}\right),$$

is irreducible over F_{2^s} if and only if

$$Tr_{2^{sn}|2}r^{-2}\left(ac(\frac{P'(\frac{b}{r})}{P(\frac{b}{r})})^2+(ah+cd)(\frac{P'(\frac{b}{r})}{P(\frac{b}{r})})(1+\frac{bP'(\frac{b}{r})}{rP(\frac{b}{r})})+dh(n+(\frac{bP'(\frac{b}{r})}{rP(\frac{b}{r})})^2)\right)=1.$$

Proof: By using the irreducibility of $P(x)$ over F_q, we have the following relation over $F_{2^{sn}}$.

$$P(x)=\prod_{u=0}^{n-1}(x-\alpha^{q^u}). \tag{1}$$

Substituting $\frac{ax^2+bx+c}{dx^2+rx+h}$ for x in (1) and multiplying both sides by $H(a.d)^{-1}(dx^2+rx+h)$ we obtain

$$F(x)=H(a.d)^{-1}(dx^2+rx+h)^nP\left(\frac{ax^2+bx+c}{dx^2+rx+h}\right)$$

$$= \prod_{u=0}^{n-1} \left(\left(a + d\alpha^{q^u}\right) x^2 + \left(b + r\alpha^{q^u}\right) x + \left(c + h\alpha^{q^u}\right) \right).$$

Or since $(a + d\alpha^{q^u}) \neq 0$ we obtain

$$F(x) = \prod_{u=0}^{n-1} \left(a + d\alpha^{q^u}\right) \prod_{u=0}^{n-1} \left(x^2 + \frac{b + r\alpha^{q^u}}{a + d\alpha^{q^u}} x + \frac{c + h\alpha^{q^u}}{a + d\alpha^{q^u}} \right)$$

$$= (a + d\alpha)^{\frac{q^n-1}{q-1}} \prod_{u=0}^{n-1} \left(x^2 + \left(\frac{b + r\alpha}{a + d\alpha}\right)^{q^u} x + \left(\frac{c + h\alpha}{a + d\alpha}\right)^{q^u} \right)$$

$$= H(a.d) \prod_{u=0}^{n-1} \left(x^2 + \left(\frac{b + r\alpha}{a + d\alpha}\right)^{q^u} x + \left(\frac{c + h\alpha}{a + d\alpha}\right)^{q^u} \right).$$

By theorem 1 $F(x)$ is irreducible over F_{2^s} if and only if the polynomial $x^2 + (\frac{b+r\alpha}{a+d\alpha})x + (\frac{c+h\alpha}{a+d\alpha})$ is irreducible over $F_{2^{sn}}$. this polynomial by proposition 2 is irreducible over $F_{2^{sn}}$ if and only if

$$Tr_{2^{sn}|2} \left(\frac{(a + d\alpha)(c + h\alpha)}{(b + r\alpha)^2} \right) \neq 0.$$

For convenience, now let

$$\beta = \left(\frac{(a + d\alpha)(c + h\alpha)}{(b + r\alpha)^2} \right).$$

which is the same as

$$\beta = \frac{ac}{(b + r\alpha)^2} + \frac{\alpha(ah + cd)}{(b + r\alpha)^2} + \frac{\alpha^2 dh}{(b + r\alpha)^2}.$$

Suppose $f(x) = P(\frac{x+b}{r}) = \sum_{i=0}^{n} d_i x^i$, so $b + r\alpha$ is the root of $f(x)$, which yields

$$Tr_{2^{sn}|2^s} \left(\frac{1}{b + r\alpha} \right) = \frac{d_1}{d_0} = \frac{P'(\frac{b}{r})}{rP(\frac{b}{r})}.$$

By this relation we have

$$Tr_{2^{sn}|2^s} \left(\frac{ac}{(b + r\alpha)^2} \right) = ac(\frac{d_1}{d_0})^2 = ac \left(\frac{P'(\frac{b}{r})}{rP(\frac{b}{r})} \right)^2,$$

and

$$Tr_{2^{sn}|2^s} \frac{\alpha(ah + cd)}{(b + r\alpha)^2} = Tr_{2^{sn}|2^s} \frac{(ah + cd)}{r} \left(\frac{r\alpha + b - b}{(b + r\alpha)^2} \right)$$

$$= Tr_{2^{sn}|2^s} \frac{(ah + cd)}{r} \left(\frac{1}{b + r\alpha} + \frac{b}{(b + r\alpha)^2} \right)$$

$$= \frac{(ah + cd)}{r} \left(\frac{P'(\frac{b}{r})}{rP(\frac{b}{r})} + b \left(\frac{P'(\frac{b}{r})}{rP(\frac{b}{r})} \right)^2 \right).$$

also we have

$$Tr_{2^{sn}|2^s} \frac{dh\alpha^2}{(b + r\alpha)^2} = Tr_{2^{sn}|2^s} dh \left(\frac{\alpha}{b + r\alpha} \right)^2 = Tr_{2^{sn}|2^s} \frac{dh}{r^2} \left(\frac{r\alpha + b - b}{b + r\alpha} \right)^2$$

$$= Tr_{2^m|2^r}\frac{dh}{r^2}\left(1+b^2\left(\frac{1}{b+r\alpha}\right)^2\right) = \frac{dh}{r^2}\left(n+b^2\left(\frac{P'\left(\frac{b}{r}\right)}{rP\left(\frac{b}{r}\right)}\right)^2\right).$$

Using these preliminary computations we obtain the relation

$$Tr_{2^m|2}\beta = Tr_{2^s|2}(Tr_{2^m|2^s}\beta)$$

$$= Tr_{2^s|2}r^{-2}\left(ac\left(\frac{P'\left(\frac{b}{r}\right)}{P\left(\frac{b}{r}\right)}\right)^2 + (ah+cd)\left(\frac{P'\left(\frac{b}{r}\right)}{P\left(\frac{b}{r}\right)}\right)\left(1+\frac{bP'\left(\frac{b}{r}\right)}{rP\left(\frac{b}{r}\right)}\right) + dh\left(n+\left(\frac{bP'\left(\frac{b}{r}\right)}{rP\left(\frac{b}{r}\right)}\right)^2\right)\right).$$

This completes proof.

Corollary 1: *Let $P(x)=\sum_{i=0}^{n}c_ix^i$ be an irreducible polynomial of degree $n\geq 1$ over F_{2^s} $(P(x)\neq x)$, then the polynomial*

$$F(x) = (x^2+x+1)^n p\left(\frac{x^2+x}{x^2+x+1}\right).$$

is irreducible over F_{2^s} if and only if

$$Tr_{2^s|2}\left(\left(\frac{P'(1)}{P(1)}\right)^2+n\right)=1.$$

Theorem 3: *Let $P(x)=\sum_{i=0}^{n}c_ix^i$ be an irreducible polynomial of degree $n\geq 1$ over $F_{2^s}(P(x)\neq x)$. Define*

$$F_0(x)=P(x).\quad F_{k+1}(x)=(x^2+x+1)^{n_k}F_k\left(\frac{x^2+x}{x^2+x+1}\right), k\geq 0, \tag{2}$$

where $n_k=n2^k$ denotes the degree of $F_k(x)$ over F_{2^s}. Then $F_{k+1}(x)$ is an irreducible polynomial over F_{2^s} of degree $n=n2^{k+1}$ if and only if

$$Tr_{2^s|2}\left(\left(\frac{P'(1)}{P(1)}\right)^2+n\right).Tr_{2^s|2}(\frac{c_1}{c_0}+n)=1. \tag{3}$$

Proof: The proof of the theorem is by induction. By (2)it is clear that $F_1(0)=P(0)=c_0$ and $F_1'(0)=nP(0)+P'(0)=nc_0+c_1$. Also it is easily proved by induction that

$$F_{k+1}(0)=F_k(0)=c_0 \quad and \quad F_{k+1}'(0)=F_k'(0)=nc_0+c_1,\quad k\geq 0.$$

Now we can use these relations in our proof. Based on corollary 1 and (3) it is clear that $F_1(x)$ is irreducible over F_{2^s}. we suppose that $F_k(x)$. $k\geq 2$ is an irreducible polynomial over F_{2^s}. For irreducibility of $F_{k+1}(x)$ by corollary 1 we need to show that

$$Tr_{2^s|2}\left(\left(\frac{F_k'(1)}{F_k(1)}\right)^2+n_k\right)=Tr_{2^s|2}\left(\frac{F_k'(1)}{F_k(1)}\right)=1.$$

From above relations we obtain

$$F_k(1)=F_{k-1}(0)=c_0 \quad and \quad F_k'(1)=F_{k-1}'(0)=nc_0+c_1$$

$$Tr_{2^s|2}\left(\frac{F_k'(1)}{F_k(1)}\right)=Tr_{2^s|2}(\frac{c_1}{c_0}+n)=1.$$

Thus the theorem is proved.

References

[1] E.R. Berlekamp. Algebraic Coding Theory. McGraw-Hill, New York. 1968.

[2] I.F. Blake, G.Seroussi and N.P.Smart. Elliptic curves in Cryptography, Cambridge University Press, Cambridge, Reprinted 2000.

[3] B. Chor, R. rivest, "A knapsack-type public key cryptosystem based on arithmetic in finite fields", *IEEE Trans.Inform.Theory*, vol. 34. pp. 901-909, 1988.

[4] J. Calmet, "Algebraic algorithms in GF (q)",*Discrete Math*, vol. 56 pp. 101-109, 1985.

[5] R. Chapman, "Completely normal elements in iterated quadratic extensions Of finite fields",*Finite Fields Appl*, vol. 3, pp. 3-10, 1997.

[6] S. D. Cohen,"On irreducible polynomials of certain types in finite fields", *Proc. Cambridge Philos.* Soc, vol. 66, pp. 335-344, 1969.

[7] S. D. Cohen,"The explicit construction of irreducible polynomials over finite fields", *De. Codes Cryptogr*, vol. 2, pp. 169-173, 1992.

[8] W. Eberly," Very fast parallel matrix and polynomial arithmetic", *25th Annual symposium on Foundations of Computer Science*. pp. 21-30, 1984.

[9] S. Gao, Normal bases over finite fields, Ph.D Thesis, Waterloo, 1993.

[10] M.K. Kyuregyan,"Recurrent Methods for Constructing Irreducible Polynomials over" , *Finite Fields Apple*, vol. 8, pp. 52-68. 2002.

[11] M. K. Kyuregyan,"Iterated constructions of irreducible polynomials over finite fields with linearly independent roots" ,*Finite Fields Apple*, vol. 10, pp. 323-431, 2004.

[12] M. K. Kyuregyan,"Recurrent methods for constructing irreducible polynomials over Fq of odd characteristics", *Finite Fields Appl*, vol. 9, pp. 39-58, 2003.

[13] M. K. Kyuregyan, "Recurrent methods for constructing irreducible polynomials over Fq of odd characteristics II", *Finite Fields Appl*, vol. 12, pp. 357-378, 2006.

[14] M.K. Kyuregyan, "Quadratic transformations and synthesis of irreducible polynomials over finite fields", *Dokl, Akad. Nauk Arm, SSR*, vol. 84(2), pp. 67-71, 1987. (in Russian).

[15] N.Koblitz. Algebraic Aspects of Cryptography, Springer, Berlin, 1998.

[16] R. Lidl and H. Niederreiter. Finite Fields. Cambridge University Press, 1987.

[17] A. Menezes. I.F. Blake, X. GAO, R. C. Mullin, S. A. Vanstone. T.Yaghoobian. Applications of Finite Fields, Kluwer Academic Publishers, Boston- Dordrecht- Lancaster. 1993.

[18] F.J.MacWilliams, N.J.A. Sloane. The theory of error-correcting codes. Part. Bell Laboratories Murray Hill. NJ. USA. North-Holland Publishing Company. Amsterdam. New York, Oxford.

[19] G. McNay. Topics in finite fields, Ph.D. Thesis, University of Glasgow. 1995.

[20] H. Meyn." Explicit N-polynomials of 2-power degree over finite fields", *Designs Codes Cryptogr*. vol. 6. pp. 107-116. 1995.

[21] S. Perlis. "Normal bases of cyclic fields of prime-power degree".*Duke Math. J.*, vol. 9. pp. 507-517. 1942.

[22] J.Von zur Gathen. E. Kaltofen,"Factorization of multivariate polynomials over finite fields". *Math.Comput.* vol.45. pp. 251-261. 1985.

[23] R. R. Varshamov." A general method of synthesizing irreducible polynomials over Galois fields". *Soviet Math. Dokl.* vol. 29. pp. 334- 336, 1984.

Զույգ բնութագրիչով չբերվող բազմանդամների բաղադրություններ վերջավոր դաշտերի վրա

Ս. Մեհրաբի և Մ. Կյուրեղյան

Ամփոփում

Այս աշխատանքը ներկայացնում է վերջավոր դաշտերի վրա զույգ բնութագրիչով չբերվող բազմանդամների սինտեզման կոնստրուկտիվ տեսության որոշ արդյունքներ: Մենք ապացուցել ենք թեորեմ, որը մեծ դեր է խաղում չբերվող բազմանդամներ կառուցելուց: Այս թեորեմի օգնությամբ առաջարկվում է $n2^k (k = 1.2 ...)$ աստիճանի չբերվող բազմանդամ կառուցելու ռեկուռենտ մեթոդ: