Canad. Math. Bull. Vol. **49** (1), 2006 pp. 113–116

PSL$(2, 2^n)$-Extensions Over $\mathbb{F}_{2^n}$

Arne Ledet

Abstract. We construct a one-parameter generic polynomial for PSL$(2, 2^n)$ over $\mathbb{F}_{2^n}$.

1 Introduction

Let F be a field, and let G be a finite group. A polynomial $P(\mathbf{s}, X) \in F(\mathbf{s})[X]$, where $\mathbf{s} = (s_1, \dots, s_n)$ are indeterminates, is then called a *generic polynomial* for G over F, if it satisfies the following two conditions:

(a) The splitting field for $P(\mathbf{s}, X)$ over $F(\mathbf{s})$ is a Galois extension with Galois group isomorphic to G;

(b) Whenever M/L is a G-extension over F, *i.e.,* M/L is a Galois extension with Galois group isomorphic to G, and $L \supseteq F$, there exists $\mathbf{a} = (a_1, \dots, a_n) \in L^n$ such that M is the splitting field over L of $P(\mathbf{a}, X)$.

The s_i's are referred to as the *parameters*, and $\mathbf{a}$ as a *specialisation*.

Generic polynomials have been considered in a number of papers, *e.g.,* [KM, JLY, HM]. Also, there is the closely related concept of a *generic extension*, introduced by Saltman [Sa].

In this paper, we prove

Theorem 1 *Let $n \geq 1$ be a natural number, and let $\mathbb{F}_{2^n}$ denote the finite field with 2^n elements. Then the polynomial*

$$X^{2^n+1} + sX^{2^n} + X + 1$$

is generic for the projective special linear group PSL$(2, 2^n)$ *over* $\mathbb{F}_{2^n}$*, with parameter s.*

In particular, $X^3 + sX^2 + X + 1$ is generic for the symmetric group S_3 over $\mathbb{F}_2$, and $X^5 + sX^4 + X + 1$ is generic for the alternating group A_5 over $\mathbb{F}_4$, *cf.* [Hu, II Satz 6.14].

2 Proof of Theorem 1

Let M/L be a PSL$(2, 2^n)$-extension over $\mathbb{F}_{2^n}$. The group PSL$(2, 2^n)$ is equal to the special linear group SL$(2, 2^n)$, *i.e.,* it consists of 2×2 matrices.

By a standard argument (see *e.g.,* [JLY, 1.1]), we can match the Galois action with a matrix action. In fact, if we let $(Ax)_{A \in \mathrm{PSL}(2,2^n)}$ be a normal basis for M/L, the map

$$\varphi \colon \mathbf{u} \mapsto \sum_{A \in \mathrm{PSL}(2,2^n)} \pi(A^{-1}\mathbf{u})Ax,$$

Received by the editors April 26, 2004; revised May 25, 2005.
AMS subject classification: Primary: 12F12; secondary: 12E10.

where $\pi\colon \mathbb{F}_{2^n}^2 \to \mathbb{F}_{2^n}$ is the first coordinate function, will be an injective $\mathrm{PSL}(2,2^n)$-equivariant $\mathbb{F}_{2^n}$-vector space homomorphism from $\mathbb{F}_{2^n}^2$ into M.

Thus, we have elements $x = \varphi((1,0)^t)$ and $y = \varphi((0,1)^t)$ in M, linearly independent over $\mathbb{F}_{2^n}$, such that $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{PSL}(2,2^n)$ acts by $x \mapsto ax + cy$ and $y \mapsto bx + dy$. Letting $t = x/y$, we get $t \mapsto (at+c)/(bt+d)$. This action on $\mathbb{F}_{2^n}(t)$ is faithful. Of necessity, t is then transcendental over $\mathbb{F}_{2^n}$, and we restrict our attention to $\mathbb{F}_{2^n}(t)/\mathbb{F}_{2^n}(t)^{\mathrm{PSL}(2,2^n)}$.

We will need to make use of Lüroth's theorem (see [Ja, 8.14]), and in particular the following facts from it: If $u = p(t)/q(t) \in F(t)$ is a rational function written in reduced form, *i.e.*, with $\gcd(p,q) = 1$, then t is algebraic over $F(u)$ of degree $\max\{\deg p, \deg q\}$; also, if K is an intermediate field $F \subsetneq K \subseteq F(t)$, then t is algebraic over K, and $K = F(u)$ for any non-constant coefficient u in the minimal polynomial for t over K.

We will construct an s such that $\mathbb{F}_{2^n}(t)^{\mathrm{PSL}(2,2^n)} = \mathbb{F}_{2^n}(s)$, and show that for this s, the polynomial in the theorem has $\mathbb{F}_{2^n}(t)$ as its splitting field. The s in the theorem must then simply be specialised to this s in order to produce a polynomial with splitting field $M = L(t)$ over L.

First, we note that $|\,\mathrm{PSL}(2,2^n)| = 2^n(2^n-1)(2^n+1)$.

The matrix $\left(\begin{smallmatrix} 1 & 0 \\ a & 1 \end{smallmatrix}\right)$ acts by $t \mapsto t + a$, for $a \in \mathbb{F}_{2^n}$. These matrices form a subgroup isomorphic to the additive group $(\mathbb{F}_{2^n}, +)$, and clearly the fixed field is

$$\mathbb{F}_{2^n}(t^{2^n} + t),$$

since

$$\begin{aligned}\prod_{a\in\mathbb{F}_{2^n}} (X - (t+a)) &= \prod_{a\in\mathbb{F}_{2^n}} ((X-t) - a) \\ &= (X-t)^{2^n} - (X-t) = X^{2^n} - X - (t^{2^n} - t).\end{aligned}$$

Next, the matrix $\left(\begin{smallmatrix} a & 0 \\ 0 & 1/a \end{smallmatrix}\right)$ acts by $t \mapsto a^2 t$, for $a \in \mathbb{F}_{2^n}^*$. The effect on $t^{2^n} + t$ is multiplication by a^2, since $a^{2^n} = a$. These matrices form a subgroup isomorphic to the multiplicative group $\mathbb{F}_{2^n}^*$, and together with the subgroup above produce a group isomorphic to the semi-direct product $\mathbb{F}_{2^n} \rtimes \mathbb{F}_{2^n}^*$, where $\mathbb{F}_{2^n}^*$ acts on $\mathbb{F}_{2^n}$ by multiplication. The fixed field is

$$\mathbb{F}_{2^n}\left((t^{2^n} + t)^{2^n - 1}\right),$$

as

$$\prod_{a\in\mathbb{F}_{2^n}^*} (X - au) = X^{2^n-1} - u^{2^n-1}.$$

Now, $(t^{2^n} + t)^{2^n-1}$ is algebraic over $\mathbb{F}_{2^n}(t)^{\mathrm{PSL}(2,2^n)}$ of degree $2^n + 1$, and we claim that its minimal polynomial is of the form $X^{2^n+1} + sX^{2^n} + X + 1$ given in the theorem. This allows us to solve for s:

$$s = \frac{1 + (t^{2^n} + t)^{2^n-1} + (t^{2^n} + t)^{4^n-1}}{(t^{2^n} + t)^{2^n(2^n-1)}}.$$

https://doi.org/10.4153/CMB-2006-011-6 Published online by Cambridge University Press

It is obvious that this s is in reduced form, and therefore that $\mathbb{F}_{2^n}(t)$ has degree $2^n(2^n-1)(2^n+1)$ over $\mathbb{F}_{2^n}(s)$. This ensures that s in fact generates $\mathbb{F}_{2^n}(t)^{\mathrm{PSL}(2,2^n)}$, *provided* that s is invariant under the action of $\mathrm{PSL}(2,2^n)$. In which case the minimal polynomial will be as claimed.

We already know that s is invariant under the subgroup $\mathbb{F}_{2^n} \rtimes \mathbb{F}_{2^n}^*$ described above. For the rest, there is a matrix A in $\mathrm{PSL}(2,2^n)$ of order 2^n+1, obtained from $\mathbb{F}_{4^n}$ by expressing multiplication by an element of order 2^n+1 in terms of a basis over $\mathbb{F}_{2^n}$. Together with $\mathbb{F}_{2^n} \rtimes \mathbb{F}_{2^n}^*$, it generates $\mathrm{PSL}(2,2^n)$. Conjugating if necessary, we may assume $A = \left(\begin{smallmatrix} 0 & 1 \\ 1 & a \end{smallmatrix}\right)$ for some $a \in \mathbb{F}_{2^n}$. Since

$$\begin{pmatrix} 0 & 1 \\ 1 & a \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ a & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},$$

this means that $\mathrm{PSL}(2,2^n)$ is generated by $\mathbb{F}_{2^n} \rtimes \mathbb{F}_{2^n}^*$ and $\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$. This last matrix acts by $t \mapsto 1/t$, so to prove $s \in \mathbb{F}_{2^n}(t)^{\mathrm{PSL}(2,2^n)}$ it is enough to show that s is invariant under $t \mapsto 1/t$. To see this, we rewrite

$$\begin{aligned} s &= \frac{1 + (t^{2^n}+t)^{2^n-1} + (t^{2^n}+t)^{4^n-1}}{(t^{2^n}+t)^{2^n(2^n-1)}} = \frac{(t^{2^n}+t) + (t^{2^n}+t)^{2^n} + (t^{2^n}+t)^{4^n}}{(t^{2^n}+t)^{2^n(2^n-1)+1}} \\ &= \frac{t + t^{8^n}}{(t^{2^n}+t)^{2^n(2^n-1)+1}}, \end{aligned}$$

and find

$$\begin{aligned} s(1/t) &= \frac{1/t + 1/t^{8^n}}{(1/t^{2^n} + 1/t)^{2^n(2^n-1)+1}} = \frac{t^{8^n+1}(1/t + 1/t^{8^n})}{t^{8^n+1}(1/t^{2^n} + 1/t)^{2^n(2^n-1)+1}} \\ &= \frac{t^{8^n} + t}{(t + t^{2^n})^{2^n(2^n-1)+1}} = s. \end{aligned}$$

Hence, s is $\mathrm{PSL}(2,2^n)$-invariant, and generates the fixed field.

The polynomial $X^{2^n+1} + sX^{2^n} + X + 1$ is irreducible and has $(t^{2^n}+t)^{2^n-1}$ as a root. Its splitting field is all of $\mathbb{F}_{2^n}(t)$, since the conjugates of $\mathbb{F}_{2^n} \rtimes \mathbb{F}_{2^n}^*$ in $\mathrm{PSL}(2,2^n)$ have trivial intersection. This completes the proof of the theorem. ∎

Remark It is not hard to see that the splitting field for $X^{2^n+1} + sX^{2^n} + X + 1$ over $\mathbb{F}_2$ is also $\mathbb{F}_{2^n}(t)$, with Galois group $\mathrm{PSL}(2,2^n) \rtimes C_n$, where C_n acts entry-wise on $\mathrm{PSL}(2,2^n)$ as the Galois group of $\mathbb{F}_{2^n}/\mathbb{F}_2$. For instance, $X^5 + sX^4 + X + 1$ has Galois group S_5 over $\mathbb{F}_2$. However, $X^{2^n+1} + sX^{2^n} + X + 1$ is not generic for $\mathrm{PSL}(2,2^n) \rtimes C_n$ over $\mathbb{F}_{2^n}$, since the C_n-subextension of $\mathbb{F}_{2^n}(t)/\mathbb{F}_2(s)$ is $\mathbb{F}_{2^n}(s)/\mathbb{F}_2(s)$.

References

[HM] K. Hashimoto and K. Miyake, *Inverse Galois problem for dihedral groups.*In: Number Theory and Its Applications, Developments in Mathematics 2, Kluwer Academic Publishers, 1999, pp. 165–181.

[Hu] B. Huppert, *Endliche Gruppen. I.* Grundlehren der mathematischen Wissenschaften 134, Springer-Verlag, Berlin, 1967.

[Ja] N. Jacobson, *Basic Algebra. II.* W. H. Freeman, New York, 1989.

[JLY] C. U. Jensen, A. Ledet, and N. Yui, *Generic Polynomials: Constructive Aspects of the Inverse Galois Problem.* Mathematical Sciences Research Institute Publication 45, Cambridge University Press, Cambridge, 2002.

[KM] G. Kemper and E. Mattig, *Generic polynomials with few parameters.* J. Symbolic Comput. **30**(2000), no. 6, 843–857.

[Sa] D. J. Saltman, *Generic Galois extensions and problems in field theory.* Adv. in Math. **43** (1982), no. 3, 250–283.

Department of Mathematics and Statistics
Texas Tech University
Lubbock, TX 79409-1042
U.S.A.
e-mail: arne.ledet@ttu.edu