FACTORIZATIONS OVER FINITE FIELDS

By
Shreeram S. Abhyankar*

ABSTRACT. Partitions of roots of unity lead to factorizations of univariate polynomials over finite fields which in turn lead to certain multivariate factorizations of Generalized Artin Schreier polynomials. These and some other multivariate factorizations of Generalized Artin Schreier polynomials give rise to coverings whose Galois groups are symplectic, orthogonal and unitary groups over finite fields. They also give rise to various PPs = Permutation Polynomials and EPs = Exceptional Polynomials.
CONCLUSION: Amazingly, most Lie Type Finite Simple Groups, as well as many PPs and EPs, are born out of polynomial solutions of Artin Schreier Type Equations.
HAPPY THOUGHT: Once again High-School Algebra triumphs.

Section 1: Introduction

Let $q > 1$ be a power of a prime number p, and for every integer $i \geq -1$ let

$$\langle i \rangle = 1 + q + q^2 + \cdots + q^i = \frac{q^{i+1} - 1}{q - 1} \quad \text{(convention: } \langle 0 \rangle = 1 \text{ and } \langle -1 \rangle = 0\text{)}$$

where the second equation is a special case of the geometric series identity

$$1 + Z + Z^2 + \cdots + Z^i = \frac{Z^{i+1} - 1}{Z - 1}$$

which we shall frequently use.

Let $m > 0$ be an integer and let k be an algebraically closed field of characteristic p. In Section 2 we shall consider some partitions of the $\langle m-1 \rangle$-th roots of 1 in k, and show how this leads first to a univariate factorization over the Galois Field GF(p) of p elements and then to a multivariate factorization of a Generalized Artin Schreier polynomial, which is used in [A06] for constructing symplectic group coverings. In Section 5 we shall further consider some more multivariate factorizations of Generalized Artin Schreier polynomials, which are used in [A07] to construct orthogonal group coverings. In Section 6 we shall again consider yet some more factorizations of Generalized Artin Schreier polynomials, which are used in [A05] to construct unitary group coverings. In Section 7 we shall consider factorizations of some Generalized Artin Schreier deformations of the symplectic group

*This work was partly supported by NSF grant DMS 91-01424 and NSA grant MDA 904-92-H-3035.

equations, and in Section 8 we shall indicate that they give rise to certain generalizations of the MCM polynomials which are the PPs = Permutation Polynomials and EPs = Exceptional Polynomials recently (1993-94) discovered by Müller [Mue], Cohen and Matthews [CoM] in response to the seminal paper [FGS] of Fried, Guralnick and Saxl on the Carlitz Conjecture about PPs and EPs. The MCM polynomials are in characteristic 2; more recently (1995), again in response to the Fried-Guralnick-Saxl paper [FGS], a new family of PPs and EPs in characteristic 3 has been discovered by Lenstra and Zieve [Zie]. In Section 9 we shall formulate a Mantra which contains the seeds of most of the previously considered factorizations.

In Section 3 we shall review the definitions of finite classical groups, i.e., linear, symplectic, orthogonal and unitary groups over the Galois field $GF(q)$ of q elements. In Section 4 we shall introduce the concepts of genus zero and strong genus zero equations, and indicate that our previous equations were mostly genus zero, whereas the generalizations of the MCM polynomials provide us with strong genus zero equations. In Section 8 we shall discuss the possible list of strong genus zero groups surmised by Guralnick and Saxl in [GuS] which was a follow-up of the Fried-Guralnick-Saxl paper [FGS].

It may be remarked that the explicit nice equations having the classical and other interesting groups as Galois groups which I have found so far are all special cases of the family of unramified coverings of the affine line in nonzero characteristic which I wrote down in my 1957 paper [A02]. The said family itself was obtained by taking sections of the unsolvable surface coverings with normal crossing branch loci which were discovered in my 1955 Ph.D. Thesis [A01] as a way of explaining why Jung's 1908 method of complex surface desingularization does not extend to nonzero characteristic.

It is my fond memory that my Ph.D. Thesis, as well as much of my later work, was guided by my guru Professor Oscar Zariski. Equally fond are my memories of my father Professor S. K. Abhyankar who initiated me into patee-ganit = basic mathematics. On the group theory side my teachers have been numerous: B. H. and Hanna Neumann, Philip Hall, Reinhold Baer, Richard Brauer, Walter Feit, Danny Gorenstein, Bill Kantor, Peter Neumann, Peter Cameron, Steve Smith, Ernie Shult, Ulrich Meierfrankenfeld, Martin Liebeck, Jan Saxl, and Nick Inglis. What is more mysterious is how my equations were inspired by Drinfeld Module Theory as explained to me by Ernst Gekeler, David Goss and Dinesh Thakur. But then above all it is Serre who over the years has been prodding me to find nice equations.

Section 2: Partitions of Roots of Unity

We may ask if there is a natural partition of the $\langle m-1\rangle$-th roots of 1 in k into two sets of sizes $\langle m-2\rangle$ and q^{m-1}. This is equivalent to asking for a natural factorization $V^{\langle m-1\rangle}-1 = M_1M_2$ where M_1 and M_2 are

monic polynomials of degrees $\langle m-2\rangle$ and q^{m-1} in an indeterminate V with coefficients in k respectively. If we drop the adjective "natural" then of course there are as many factorizations as the number of ways of choosing $\langle m-2\rangle$ things out of $\langle m-1\rangle$ things. So what is natural? Well, we could require M_1 and M_2 to have coefficients in $\mathrm{GF}(p)$ and be expressible by a "universal formula valid for all m and q". For $m=2$ we could take $M_1 = V+1$ and $M_2 = (V^{\langle m-1\rangle}-1)/(V+1)$, and then we would have $-VM_1^q + M_1 + V^{1+q} - 1 = 0$.[1] This suggests that also for general m we could try to find monic $M_1 \in \mathrm{GF}(p)[V]$ such that $-VM_1^q + M_1 + V^{\langle m-1\rangle} - 1 = 0$. This amounts to finding a root $M = -M_1 \in \mathrm{GF}(p)[V]$ of the Generalized Artin Schreier polynomial[2]

$$VR^q - R + V^{\langle m-1\rangle} - 1 \in \mathrm{GF}(p)[V][R].$$

We "find" such a root "telescopically" by putting

$$M = -\sum_{\mu=0}^{m-1} V^{\langle m-2-\mu\rangle}$$

and directly checking that then

$$VM^q - M + V^{\langle m-1\rangle} - 1 = 0.$$

Now by putting

$$M_1 = -M \quad \text{and} \quad M_2 = VM^{q-1} - 1$$

we get

$$\text{monic } M_1 \in \mathrm{GF}(p)[V] \text{ of deg } \langle m-2\rangle$$

and

$$\text{monic } M_2 \in \mathrm{GF}(p)[V] \text{ of deg } q^{m-1}$$

giving the univariate factorization

$$V^{\langle m-1\rangle} - 1 = M_1 M_2$$

which leads to the bivariate factorization

$$VR^q - R + V^{\langle m-1\rangle} - 1 = (R-M)\left[V\left(R^{q-1} + MR^{q-2} + \cdots + M^{q-1}\right) - 1\right].$$

[1] The more obvious choice would be $M_1 = V-1$. But this doesn't "work", maybe because it is so obvious.

[2] The usual Artin Schreier equations is $R^p - R + C = 0$.

In the "More Nice Equations" paper [A06] it is shown how this bivariate factorization leads to a multivariate factorization which gives rise to the following Construction (2.1) of symplectic group coverings where

$$F_m(X,T_1,\dots,T_m,Y) = XY^{\langle m-1\rangle} + \sum_{i=1}^{m}\left(T_i^{q^i}Y^{\langle m-1+i\rangle} + T_iY^{\langle m-1-i\rangle}\right)$$

and

$$\begin{aligned}\Phi_m(X,T_1,\dots,T_m,Y) &= F_m(X,T_1,\dots,T_m,Y^{q-1})\\ &= XY^{q^m-1} + \sum_{i=1}^{m}\left(T_i^{q^i}Y^{q^m+i-1} + T_iY^{q^m-i-1}\right)\end{aligned}$$

and

$$\begin{aligned}\widehat{\Phi}_m(X,T_1,\dots,T_m,Y) &= Y\Phi_m(X,T_1,\dots,T_m,Y)\\ &= XY^{q^m} + \sum_{i=1}^{m}\left(T_i^{q^i}Y^{q^m+i} + T_iY^{q^m-i}\right)\end{aligned}$$

and where $F_{m,e}(Y)$, $\Phi_{m,e}(Y)$, $\widehat{\Phi}_{m,e}(Y)$ are the monic polynomials of degrees $\langle 2m-1\rangle$, $q^{2m}-1$, q^{2m} in Y with coefficients in $\mathrm{GF}(p)[X,T_1,\dots,T_e]$ obtained by putting $T_{e+1} = T_{e+2} = \cdots = T_{m-1} = 0$ and $T_m = 1$ in $F_m(X,T_1,\dots,T_m,Y)$, $\Phi_m(X,T_1,\dots,T_m,Y)$, $\widehat{\Phi}_m(X,T_1,\dots,T_e,Y)$ respectively, i.e., for $0 \le e < m$,

$$F_{m,e}(Y) = Y^{\langle 2m-1\rangle} + 1 + XY^{\langle m-1\rangle} + \sum_{i=1}^{e}\left(T_i^{q^i}Y^{\langle m-1+i\rangle} + T_iY^{\langle m-1-i\rangle}\right)$$

and

$$\Phi_{m,e}(Y) = Y^{q^{2m}-1} + 1 + XY^{q^m-1} + \sum_{i=1}^{e}\left(T_i^{q^i}Y^{q^m+i-1} + T_iY^{q^m-i-1}\right)$$

and

$$\widehat{\Phi}_{m,e}(Y) = Y^{q^{2m}} + Y + XY^{q^m} + \sum_{i=1}^{e}\left(T_i^{q^i}Y^{q^m+i} + T_iY^{q^m-i}\right).$$

Construction (2.1). *For $0 < e < m > 2$ we have*

$$Gal(F_{m,e}, k(X, T_1, \ldots, T_e)) = PSp(2m, q)$$

and

$$Gal(\Phi_{m,e}, k(X, T_1, \ldots, T_e)) = Sp(2m, q)$$

and

$$Gal(\widehat{\Phi}_{m,e}, k(X, T_1, \ldots, T_e)) = Sp(2m, q).$$

[Note that $PSp(2m, q)$ (definition to be reviewed in Section 3) acts on the $(2m-1)$-dimensional projective space $\mathcal{P}(2m-1, q)$ over $GF(q)$ whose cardinality is $\langle 2m-1 \rangle$; also note that $Sp(2m, q)$ (definition to be reviewed in Section 3), as Galois group of $\Phi_{m,e}$ (resp: $\widehat{\Phi}_{m,e}$), acts on the nonzero vectors of $GF(q)^{2m}$ (resp: on the entire vector space $GF(q)^{2m}$)].

Very briefly, the above mentioned multivariate factorization says that the twisted derivative $F'_{m,e}(Y)$ factors into two monic polynomials of degrees $q\langle 2m-3 \rangle$ and q^{2m-1} in Y with coefficients in $\mathrm{GF}(p)(T_1, \ldots, T_e, Z)$ which are irreducible in $k(T_1, \ldots, T_e, Z)[Y]$, and hence by Kantor's [Kan] 1975 Theorem characterizing Rank 3 groups in terms of their subdegrees supplemented by Cameron-Kantor Theorem IV of their 1979 paper [CaK] on collineation groups we get the statement about the Galois group of $F_{m,e}$ and from that the statements about the Galois groups of $\Phi_{m,e}$ and $\widehat{\Phi}_{m,e}$ follow by the Composite Polynomial Lemma (2.4) of my 1994 "Nice Equations" paper [A04]. Recall that the Rank of a transitive permutation group is the number of orbits of its 1-point stabilizer, and the sizes of these orbits are called its subdegrees. Note that Kantor's Rank 3 Theorem uses the Buekenhout-Shult [BuS] characterization of polar spaces which itself depends on Tits' [Tit] classification of spherical buildings. Recall that (see [A03]) the twisted derivative $F'_{m,e}(Y)$ of $F_{m,e}(Y)$ is defined to be

$$F'_{m,e}(Y) = F^{\natural}_{m,e}(Y, \eta) \in \mathrm{GF}(p)(X, T_1, \ldots, T_e, \eta)[Y]$$

where η is a root of $F_{m,e}(Y)$ in an overfield of $\mathrm{GF}(p)(X, T_1, \ldots, T_e)$ and where the formal derivative $F^{\natural}_{m,e}(Y, Z)$ of $F_{m,e}(Y)$ is the bivariate polynomial

$$\frac{F_{m,e}(Y) - F_{m,e}(Z)}{Y - Z} \in \mathrm{GF}(p)(X, T_1, \ldots, T_e)[Y, Z].$$

In our case, since $F_{m,e}(Y)$ is linear in X, its twisted derivative $F'_{m,e}(Y)$ can also be obtained by substituting in $F^{\natural}_{m,e}(Y, Z)$ the value of X found by solving the equation $F_{m,e}(Z) = 0$, and then we get

$$F'_{m,e}(Y) \in \mathrm{GF}(p)(T_1, \ldots, T_e, Z)[Y].$$

Augmenting the MTR = the Method of Throwing away Roots = the Method of Twisted Derivatives, respectively by the Zassenhaus-Feit-Suzuki Theorem [page 83 of A03] characterizing 2-transitive permutation groups in which only the identity fixes 3 points and Cameron-Kantor Theorem I [CaK] characterizing 2-transitive collineation groups of projective spaces of dimension at least 2, in [A03] for $m = 2$ and in [A04] for $m > 3$, we have obtained the following Construction (2.0) of linear group coverings where

$$F^*_{m,0}(Y) = Y^{\langle m-1\rangle} + XY + 1$$

and

$$\Phi^*_{m,0}(Y) = Y^{q^m-1} + XY^{q-1} + 1$$

and

$$\widehat{\Phi}^*_{m,0}(Y) = Y^{q^m} + XY^q + Y$$

and

$$F^{**}_{m,0}(Y) = Y^{\langle m-1\rangle} + Y + X$$

and

$$\Phi^{**}_{m,0}(Y) = Y^{q^m-1} + Y^{q-1} + X$$

and

$$\widehat{\Phi}^{**}_{m,0}(Y) = Y^{q^m} + Y^q + X.$$

Construction (2.0). *For $m > 1$ we have*

$$Gal(F^*_{m,0}, k(X)) = PSL(m,q)$$

and

$$Gal(\Phi^*_{m,0}, k(X)) = SL(m,q)$$

and

$$Gal(\widehat{\Phi}^*_{m,0}, k(X)) = SL(m,q).$$

For $m > 1$ we also have

$$Gal(F^{**}_{m,0}, k(X)) = PGL(m,q)$$

and

$$Gal(\Phi^{**}_{m,0}, k(X)) = GL(m,q)$$

and

$$Gal(\widehat{\Phi}^{**}_{m,0}, k(X)) = GL(m,q).$$

[Note that $PSL(m,q)$ and $PGL(m,q)$ (definitions to be reviewed in Section 3) act on the $(m-1)$-dimensional projective space $\mathcal{P}(m-1,q)$ over

GF(q); also note that SL(m, q) and GL(m, q) (definitions to be reviewed in Section 3), as Galois groups of $\Phi^*_{m,0}$ and $\Phi^{**}_{m,0}$ (resp: $\widehat{\Phi}^*_{m,0}$ and $\widehat{\Phi}^{**}_{m,0}$), act on the nonzero vectors of GF(q)^m (resp: on the entire vector space GF(q)^m)].

Remark (2.2). Note that $F_{1,0} = F^*_{2,0}$ and $\Phi_{1,0} = \Phi^*_{2,0}$ and $\widehat{\Phi}_{1,0} = \widehat{\Phi}^*_{2,0}$. In view of (2.0) and (2.1), this is natural because $\mathrm{PSp}(2,q) = \mathrm{PSL}(2,q)$ and $\mathrm{Sp}(2,q) = \mathrm{SL}(2,q)$. More generally, for any $m > 0$, upon letting $\Phi^{*(m)}_{2,0}$ and $\widehat{\Phi}^{*(m)}_{2,0}$ be obtained by changing q to q^m in $\Phi^*_{2,0}$ and $\widehat{\Phi}^*_{2,0}$ respectively, we have $\Phi_{m,0} = \Phi^{*(m)}_{2,0}$ and $\widehat{\Phi}_{m,0} = \widehat{\Phi}^{*(m)}_{2,0}$, and hence by (2.0) we get $\mathrm{Gal}(\Phi_{m,0}, k(X)) = \mathrm{Sp}(2,q^m) = \mathrm{SL}(2,q^m)$ and $\mathrm{Gal}(\widehat{\Phi}_{m,0}, k(X)) = \mathrm{Sp}(2,q^m) = \mathrm{SL}(2,q^m)$.

Section 3: Review of Classical Groups

We shall now review the definitions of finite classical groups. To start with, the (m-dimensional) general linear group $\mathrm{GL}(m,q)$ is the group of all m by m matrices with entries in $\mathrm{GF}(q)$ and determinant nonzero, the special linear group $\mathrm{SL}(m,q)$ is the subgroup of $\mathrm{GL}(m,q)$ consisting of all those matrices whose determinant is 1, the projective general linear group $\mathrm{PGL}(m,q) = \mathrm{GL}(m,q)/(\text{scalar matrices})$, and the projective special linear group $\mathrm{PSL}(m,q) = \mathrm{SL}(m,q)/(\text{scalar matrices of determinant 1})$. Next, the symplectic group $\mathrm{Sp}(2m,q)$ is the group of all $e \in \mathrm{GL}(2m,q)$ which leave the symplectic form $\psi(x,y) = \sum_{i=1}^{m}(x_i y_{m+i} - y_i x_{m+i})$ unchanged, i.e., for which $\psi(xe, ye) = \psi(x,y)$, and the projective symplectic group $\mathrm{PSp}(2m,q)$ = the image of $\mathrm{Sp}(2m,q)$ under the natural map $\mathrm{GL}(2m,q) \to \mathrm{PGL}(2m,q)$. Note that $\mathrm{Sp}(2m,q) < \mathrm{SL}(2m,q)$ and $\mathrm{SL}(m,q) \lhd \mathrm{GL}(m,q)$ where $<$ and $\lhd$ indicate subgroup and normal subgroup respectively.

The odd dimensional orthogonal group $\mathrm{O}(2m+1,q)$ is defined to be the group of all $e \in \mathrm{GL}(2m+1,q)$ which leave the quadratic form $\psi^0(x) = x_1 x_{m+1} + \cdots + x_m x_{2m} + x^2_{2m+1}$ unchanged, i.e., for which $\psi^0(xe) = \psi^0(x)$; also we define the special orthogonal group $\mathrm{SO}(2m+1,q) = \mathrm{O}(2m+1,q) \cap \mathrm{SL}(2m+1,q)$, and we define $\Omega(2m+1,q) = \mathrm{O}'(2m+1,q)$ where $'$ denotes commutator subgroup and we note that then $\Omega(2m+1,q)$ is a subgroup of $\mathrm{SO}(2m+1,q)$ of index 1 or 2 according as $p = 2$ or $p \neq 2$; finally we define the projective orthogonal groups $\mathrm{PO}(2m+1,q)$, $\mathrm{PSO}(2m+1,q)$ and $\mathrm{P\Omega}(2m+1,q)$ to be the respective images of $\mathrm{O}(2m+1,q)$, $\mathrm{SO}(2m+1,q)$ and $\Omega(2m+1,q)$ under the the natural map $\mathrm{GL}(2m+1,q) \to \mathrm{PGL}(2m+1,q)$. Note that the group $\mathrm{PSL}(m,q)$ is simple provided $m > 1$ and $(m,q) \neq (2,2),(2,3)$, whereas the groups $\mathrm{PSp}(2m,q)$ and $\mathrm{P\Omega}(2m+1,q)$ are simple provided $(m,q) \neq (1,2),(1,3),(2,2)$. Also note that, as partly observed in (2.2), $\mathrm{Sp}(2,q) = \mathrm{SL}(2,q)$ and $\mathrm{PSp}(2,q) = \mathrm{PSL}(2,q) \approx \mathrm{P\Omega}(3,q)$ where $\approx$ stands for isomorphism. Moreover, in case of $p = 2$ we have $\mathrm{P\Omega}(2m+1,q) \approx \Omega(2m+1,q) = \mathrm{O}(2m+1,q) \approx \mathrm{Sp}(2m,q) \approx \mathrm{PSp}(2m,q)$.

To deal with even dimensional orthogonal groups, let $\epsilon \in \{+,-\}$, fix $\nu \in \mathrm{GF}(q)$ such that $T^2+T+\nu$ is irreducible in $\mathrm{GF}(q)[T]$, and consider the quadratic forms $\psi^+(x) = x_1x_{m+1} + \cdots + x_mx_{2m}$ and $\psi^-(x) = x_1x_{m+1} + \cdots + x_{m-1}x_{2m-1} + x_m^2 + x_mx_{2m} + \nu x_{2m}^2$. Define the orthogonal group $\mathrm{O}^\epsilon(2m,q)$ as the group of all $e \in \mathrm{GL}(2m,q)$ which leave the quadratic form ψ^ϵ unchanged, i.e., for which $\psi^\epsilon(xe) = \psi^\epsilon(x)$. Define the special orthogonal group $\mathrm{SO}^\epsilon(2m,q) = \mathrm{SL}(2m,q) \cap \mathrm{O}^\epsilon(2m,q)$. Let $\mathrm{O}'^\epsilon(2m,q)$ be the commutator subgroup of $\mathrm{O}^\epsilon(2m,q)$. Let $\Omega^\epsilon(2m,q) = \mathrm{O}'^\epsilon(2m,q)$ if $(m,q,\epsilon) \neq (2,2,+)$, and let $\Omega^+(4,2)$ be the subgroup of $\mathrm{SO}^+(4,2)$ containing $\mathrm{O}'^+(4,2)$, as defined in Definition 4 on page 30 of [LiK], such that $[\mathrm{SO}^+(4,2) : \Omega^+(4,2)] = 2 = [\Omega^+(4,2) : \mathrm{O}'^+(4,2)]$. Thus we get the sequence $\mathrm{O}'^\epsilon(2m,q) < \Omega^\epsilon(2m,q) < \mathrm{SO}^\epsilon(2m,q) < \mathrm{O}^\epsilon(2m,q)$ of orthogonal groups with $[\mathrm{SO}^\epsilon(2m,q) : \Omega^\epsilon(2m,q)] = 2$, and by taking their images under the natural map $\mathrm{GL}(2m,q) \to \mathrm{PGL}(2m,q)$ we get the corresponding sequence $\mathrm{PO}'^\epsilon(2m,q) < \mathrm{P}\Omega^\epsilon(2m,q) < \mathrm{PSO}^\epsilon(2m,q) < \mathrm{PO}^\epsilon(2m,q)$ of projective orthogonal groups. The number $\epsilon' = (1-\epsilon 1)/2$ is called the Witt defect of the corresponding groups; note that $\epsilon' = 0$ or 1 according as $\epsilon = +$ or $-$, and in these cases we may call the groups positive orthogonal groups and negative orthogonal groups respectively. The group $\mathrm{P}\Omega^-(2m,q)$ is simple provided $m > 1$, whereas the group $\mathrm{P}\Omega^+(2m,q)$ is simple provided $m > 2$.

Assuming q to be a square, i.e., $q = q'^2$ where q' is a power of p, the general unitary group $\mathrm{GU}(m,q')$ is defined to be the group of all $e \in \mathrm{GL}(m,q)$ which leave the unitary form $\psi^\dagger(x) = x_1^{q'+1} + \cdots + x_m^{q'+1}$ unchanged, i.e., for which $\psi^\dagger(xe) = \psi^\dagger(x)$; also we define the special unitary group $\mathrm{SU}(m,q') = \mathrm{GU}(m,q') \cap \mathrm{SL}(m,q)$, and we define the projective general unitary group $\mathrm{PGU}(m,q')$ and the projective special unitary group $\mathrm{PSU}(m,q')$ to be the respective images of $\mathrm{GU}(m,q')$ and $\mathrm{SU}(m,q')$ under the natural map $\mathrm{GL}(m,q) \to \mathrm{PGL}(m,q)$. The group $\mathrm{PSU}(m,q')$ is simple provided $m > 1$ and $(m,q') \neq (2,2),(2,3),(3,2)$. In view of certain divisibility properties of their orders, the even and odd dimensional groups $\mathrm{PSU}(2m,q')$ and $\mathrm{PSU}(2m-1,q')$ could be put into two different boxes.

For the above discussion and other properties of finite classical groups, see the books of Dickson [Dic], Liebeck-Kleidman [LiK] and Taylor [Tay].

It may be noted that, in their action on the relevant projective space, the projective linear groups act 2-transitively, the projective symplectic groups act transitively, the projective unitary groups have 2 orbits, and the projective orthogonal groups have 3 orbits except that for even dimension and even characteristic they have 2 orbits. Moreover, the projective symplectic groups have Rank 3 on the relevant projective space, whereas the unitary and orthogonal groups have Rank 3 on one of their orbits. Kantor's Rank 3 Theorem cited above says that the symplectic, unitary and orthogonal

groups are almost determined by the subdegrees of their Rank 3 action. Liebeck's [LiK] recently proved Orbit Size Theorem shows that the unitary and orthogonal groups are almost determined by their orbit sizes; Liebeck's proof depends on his Rank 3 characterization [Li1] and the Penttila-Praeger-Saxl characterization in terms of primitive prime divisors. This work of Liebeck and Penttila-Praeger-Saxl uses CT = the Classification Theorem of finite simple groups. On the other hand, Kantor's Rank 3 Theorem [Kan] is independent of CT.

Section 4: Genus Zero and Strong Genus Zero

The form of the polynomials $F^*_{m,0}$ and $\Phi^*_{m,0}$ (resp: $F_{m,e}$ and $\Phi_{m,e}$) shows that they are genus zero over $\mathrm{GF}(p)$ (resp: over $\mathrm{GF}(p)(T_1,\dots,T_e)$) in the sense whereby we say that a polynomial $f(Y)$ (or the equation $f(Y) = 0$) is genus zero over a field κ if $f(Y) = h(Y) - X\widehat{h}(Y)$ for some monic $h(Y) \in \kappa[Y]$ and $0 \neq \widehat{h}(Y) \in \kappa[Y]$ with $\deg h(Y) > \deg \widehat{h}(Y)$, and $f(Y)$ is irreducible in $\kappa(X)[Y]$. Likewise, the form of the polynomials $F^{**}_{m,0}$ and $\Phi^{**}_{m,0}$ shows that they are strong genus zero over $\mathrm{GF}(p)$ in the sense whereby we say that a polynomial $f(Y)$ (or the equation $f(Y) = 0$) is strong genus zero over a field κ if $f(Y) = h(Y) - \gamma X$ for some monic $h(Y) \in \kappa[Y] \setminus \kappa$ and $0 \neq \gamma \in \kappa$ (note that then $f(Y)$ is automatically irreducible in $\kappa(X)[Y]$). As weaker notions, the form of the polynomial $\widehat{\Phi}^*_{m,0}$ (resp: $\widehat{\Phi}^{**}_{m,0}$) shows that it is almost genus zero (resp: almost strong genus zero) over $\mathrm{GF}(p)$ whereby we say that a polynomial $f(Y)$ (or the equation $f(Y) = 0$) is almost genus zero (resp: almost strong genus zero) over a field κ if $f(Y) \in \kappa[X][Y]$ is monic in Y, and some irreducible factor of $f(Y)$ in $\kappa(X)[Y]$ is genus zero (resp: strong genus zero) over κ and has the same splitting field over $\kappa(X)$ as $f(Y)$. Note that then the polynomial $\widehat{\Phi}_{m,e}$ is almost genus zero over $\mathrm{GF}(p)(T_1,\dots,T_e)$.

The even dimensional negative orthogonal group equations which we shall deal with in Section 5, as well as the odd dimensional unitary group equations which we shall deal with in Section 6, are almost genus zero. In Sections 7 and 8 we shall talk about the possibility of strong genus zero equations for odd dimensional orthogonal groups, even dimensional positive orthogonal groups, and even dimensional unitary groups.

Section 5: Further Generalized Artin Schreier Polynomials

Slightly changing the polynomial F_m, let

$$F^-_m(T_1,\dots,T_m,Y) = \sum_{i=1}^{m} \left(T_i^{q^i} Y^{\langle m-1+i\rangle} - T_i Y^{\langle m-1-i\rangle} \right)$$

and

$$\Phi_m^-(T_1,\ldots,T_m,Y) = F_m^-(T_1,\ldots,T_m,Y^{q-1}) = \sum_{i=1}^{m}\left(T_i^{q^i}Y^{q^{m+i}-1} - T_iY^{q^{m-i}-1}\right)$$

and

$$\widehat{\Phi}_m^-(T_1,\ldots,T_m,Y) = Y\Phi_m^-(T_1,\ldots,T_m,Y) = \sum_{i=1}^{m}\left(T_i^{q^i}Y^{q^{m+i}} - T_iY^{q^{m-i}}\right)$$

and let $F_{m,e}^-(Y)$, $\Phi_{m,e}^-(Y)$, $\widehat{\Phi}_{m,e}^-(Y)$ be the monic polynomials of degrees $\langle 2m-1\rangle$, $q^{2m}-1$, q^{2m} in Y with coefficients in $\mathrm{GF}(p)[X,T_2,\ldots,T_e]$ obtained by putting $T_1 = X$ and $T_{e+1} = T_{e+2} = \cdots = T_{m-1} = 0$ and $T_m = 1$ in $F_m^-(T_1,\ldots,T_m,Y)$, $\Phi_m^-(T_1,\ldots,T_m,Y)$, $\widehat{\Phi}_m^-(T_1,\ldots,T_e,Y)$ respectively, i.e., for $0 < e < m$, let

$$F_{m,e}^-(Y) = Y^{\langle 2m-1\rangle} - 1 + X^qY^{\langle m\rangle} - XY^{\langle m-2\rangle} + \sum_{i=2}^{e}\left(T_i^{q^i}Y^{\langle m-1+i\rangle} - T_iY^{\langle m-1-i\rangle}\right)$$

and

$$\Phi_{m,e}^-(Y) = Y^{q^{2m}-1} - 1 + X^qY^{q^{m+1}-1} - XY^{q^{m-1}-1} + \sum_{i=2}^{e}\left(T_i^{q^i}Y^{q^{m+i}-1} - T_iY^{q^{m-i}-1}\right)$$

and

$$\widehat{\Phi}_{m,e}^-(Y) = Y^{q^{2m}} - Y + X^qY^{q^{m+1}} - XY^{q^{m-1}} + \sum_{i=2}^{e}\left(T_i^{q^i}Y^{q^{m+i}} - T_iY^{q^{m-i}}\right).$$

We want to find a root $\overline{\Phi}_m(T_1,\ldots,T_m,Y) \in \mathrm{GF}(p)[T_1,\ldots,T_m,Y]$ of the Generalized Artin Schreier polynomial

$$R^q - R - Y^{q^m}\widehat{\Phi}_m^-(T_1,\ldots,T_m,Y) \in \mathrm{GF}(p)[T_1,\ldots,T_m,Y][R].$$