Journal of Algebra **218,** 642–653 (1999)
Article ID jabr.1999.7878, available online at http://www.idealibrary.com on IDEAL®

On the Depth of the Invariants of the Symmetric Power Representations of $SL_2(\mathbf{F}_p)$

R. James Shank

Department of Mathematics and Statistics, Queen's University, Kingston, Ontario, Canada K7L 3N6
E-mail: shank@mast.queensu.ca

and

David L. Wehlau

Department of Mathematics and Computer Science, Royal Military College, Kingston, Ontario, Canada K7K 7B4
E-mail: wehlau@mast.queensu.ca, wehlau@rmc.ca

Communicated by Peter Littelmann

Received October 9, 1998

We study the depth of the ring of invariants of $SL_2(\mathbf{F}_p)$ acting on the nth symmetric power of the natural two-dimensional representation for $n < p$. These symmetric power representations are the irreducible representations of $SL_2(\mathbf{F}_p)$ over $\mathbf{F}_p$. We prove that, when the greatest common divisor of $p - 1$ and n is less than or equal to 2, the depth of the ring of invariants is 3. We also prove that the depth is 3 for $n = 3$, $p \neq 7$ and $n = 4$, $p \neq 5$. However, for $n = 3$, $p = 7$ the depth is 4 and for $n = 4$, $p = 5$ the depth is 5. In these two exceptional cases, the ring of invariants is Cohen–Macaulay. © 1999 Academic Press

1. INTRODUCTION

Let V be a finite-dimensional vector space over a field $\mathbf{k}$. We choose a basis, $\{a_0, \ldots, a_n\}$, for the dual, V^*, of V. Consider a finite subgroup G of $GL(V)$. The action of G on V induces an action on V^*, which extends to an action by algebra automorphisms on the symmetric algebra of V^*, $S = \mathbf{k}[a_0, \ldots, a_n]$. Specifically, for $g \in G$, $f \in S$, and $v \in V$, $(g \cdot f)(v) =$

Research partially supported by grants from ARP and NSERC.

0021-8693/99 $30.00
Copyright © 1999 by Academic Press
All rights of reproduction in any form reserved.

$f(g^{-1} \cdot v)$. The ring of invariants of G is the subring of S given by

$$S^G := \{ f \in S \mid g \cdot f = f \text{ for all } g \in G \}.$$

For an introduction to the invariant theory of finite groups we recommend [2] or [16].

Suppose that R is a graded subalgebra of S and M is an R-module. Let R^+ denote the augmentation ideal of R, i.e., the ideal generated by the homogeneous elements of positive degree. A sequence of homogeneous elements $h_1, \dots, h_k$ in R^+ is *regular* on M if, for each $i \le k$, h_i is not a zero-divisor on $M/(h_1, \dots, h_{i-1})M$. The *depth* of M is the length of the longest regular sequence on M. The depth of a ring is bounded above by its Krull dimension. A ring is *Cohen–Macaulay* if the depth equals the dimension. For a detailed discussion of depth and dimension see [9].

For a nonmodular representation, the ring of invariants is always Cohen–Macaulay. However, when the characteristic of **k** divides the order of the group, the invariants often fail to be Cohen–Macaulay. In this case computing the depth of S^G is an interesting and often difficult problem. Recent progress in understanding the depth of S^G includes the proof of the Landweber–Stong conjecture by Bourguiba and Zarati [4], the use of cohomological methods to compute depth by Kemper [13], and the extension of the work of Ellingsrud and Skjelbred by Campbell et al. [6].

In this paper we are primarily interested in taking V to be the nth symmetric power of the natural two-dimensional representation of $SL_2(\mathbf{F}_p)$. In this case the dimension of V is $n + 1$. We will assume that $p > n$. This means that we are considering the irreducible representations of $SL_2(\mathbf{F}_p)$ over $\mathbf{F}_p$ (see, for example, [1, I.3]). Let P denote a choice of Sylow p-subgroup of $SL_2(\mathbf{F}_p)$, and let B denote the corresponding Borel subgroup. The restricted action of P on V is indecomposable. For $n = 1$, $S^{SL_2(\mathbf{F}_p)}$ is easily seen to be a polynomial algebra. For $n = 2$, $S^{SL_2(\mathbf{F}_p)}$ is a hypersurface (see [8, Lecture III, Sect. 8]). For $n > 2$, $S^{SL_2(\mathbf{F}_p)}$ is not well understood and, as we will see below, is often not Cohen–Macaulay.

We compute the depth of $S^{SL_2(\mathbf{F}_p)}$ for various values of n and p. From the work of Ellingsrud and Skjelbred, we know that, when V is an indecomposable P-module and $n \ge 2$, $\operatorname{depth}(S^P) = 3$ (see [10], or [6, Corollary 3]). Furthermore, since the index of P in $SL_2(\mathbf{F}_p)$ is relatively prime to p, $\operatorname{depth}(S^{SL_2(\mathbf{F}_p)}) \ge \operatorname{depth}(S^P)$ (see [12, Proposition 14]). Therefore, $3 \le \operatorname{depth}(S^{SL_2(\mathbf{F}_p)}) \le n + 1$. In Section 4 we prove that if $\gcd(p - 1, n) \le 2$, then $\operatorname{depth}(S^{SL_2(\mathbf{F}_p)}) = 3$. In Section 5 we prove that, if $n = 3$ and $p \ne 7$, then $\operatorname{depth}(S^{SL_2(\mathbf{F}_p)}) = 3$. However, when $n = 3$ and $p = 7$, $\operatorname{depth}(S^{SL_2(\mathbf{F}_p)}) = 4$. In Section 6 we prove that, if $n = 4$ and $p \ne 5$, then $\operatorname{depth}(S^{SL_2(\mathbf{F}_p)}) = 3$. However, when $n = 4$ and $p = 5$, $\operatorname{depth}(S^{SL_2(\mathbf{F}_p)}) = 5$. Thus in the two exceptional cases the invariants are Cohen–Macaulay.

We say that an ordered homogeneous system of parameters, $f_1, \ldots, f_{n+1}$, *measures* the depth of S^G if $\operatorname{depth}(S^G) = k$ and $f_1, \ldots, f_k$ is regular on S^G. Bourguiba and Zarati [4] prove that, if $\mathbf{k} = \mathbf{F}_p$, the Dickson invariants $c_1, \ldots, c_{n+1}$ measure the depth of S^G for any G (the Dickson invariants are a specific generating set for $S^{GL_{n+1}(\mathbf{F}_p)}$). It is possible to perturb the Dickson invariants, using invariants of $GL_n(\mathbf{F}_p)$ (acting on $a_0, \ldots, a_{n-1}$), to produce a sequence $f_1, \ldots, f_{n+1}$ which measures the depth for any upper-triangular G. This sequence satisfies two properties: the lead monomial of f_i is $a_{n+1-i}^{p^{n+1}-p^{n+1-i}}$ (using the graded reverse lexicographic monomial order with $a_j < a_{j+1}$) and $f_i \equiv c_i \bmod (c_1, \ldots, c_{i-1})S^{GL_n(\mathbf{F}_p)}$. The f_i can be constructed by applying the first steps of the Buchberger algorithm (suitably modified for subalgebras) to the ideal $(c_1, \ldots, c_{n+1})S^{GL_n(\mathbf{F}_p)}$. In fact $\{f_1, \ldots, f_{n+1}\}$ is a Gröbner basis for $(c_1, \ldots, c_{n+1})S$. We made a serious attempt to use the test sequence $f_1, \ldots, f_{n+1}$ to compute the depth of S^B, but we found Theorem 2.1 to be more effective.

2. PRELIMINARIES

All maximal regular sequences on S^G have the same length (see, for example, [5, Theorem 1.2.5]). Therefore $\operatorname{depth}(S^G)$ is the length of any maximal regular sequence on S^G. Suppose that $h_0, \ldots, h_n$ are homogeneous elements in S^G and let $A = \mathbf{k}[h_0, \ldots, h_n]$. If S^G is a finitely generated module over A, then $\{h_0, \ldots, h_n\}$ is a *homogeneous system of parameters* for S^G. For any homogeneous system of parameters, the depth of S^G as an A-module is the same as the depth of S^G as an S^G-module (see, for example, the proof of [9, Corollary 19.15]). The following elementary theorem, inspired by [9, Corollary 17.12], is our primary tool for computing depth.

THEOREM 2.1. *Suppose $\{h_0, \ldots, h_n\}$ is a homogeneous system of parameters for S^G and $\{h_0, \ldots, h_k\}$ is regular on S^G. Further suppose that there exists $m \in S^G$ such that $m \notin (h_0, \ldots, h_k)S^G$ but $mh_i \in (h_0, \ldots, h_k)S^G$ for all i. The* $\operatorname{depth}(S^G) = k + 1$.

Proof. S^G is a finite module over $A = \mathbf{F}_p[h_0, \ldots, h_n]$. Therefore the depth of S^G as an A-module is the same as the depth of S^G as an S^G-module. For any element $f \in A^+$ it is clear that $mf \in (h_0, \ldots, h_k)S^G$. Thus the regular sequence $(h_0, \ldots, h_k)$ has maximal length. ∎

LEMMA 2.2. *Suppose that R is a finitely generated graded algebra and that $f_1, \ldots, f_k$ is regular on R. Then, for a given $g \in R$ and integers e_i, d_i with $0 \le e_i \le d_i$, if $f_1^{e_1} \cdots f_k^{e_k} g \in (f_1^{d_1}, \ldots, f_k^{d_k})R$, then $g \in (f_1^{d_1-e_1}, \ldots, f_k^{d_k-e_k})R$.*

Proof. First note that, since R is a finitely generated graded algebra, any permutation of the sequence $f_1, \ldots, f_k$ is regular (see, for example, [9, Corollary 17.2]). Therefore it is sufficient to prove that $f_k g \in (f_1, \ldots, f_{k-1}, f_k^2)R$ implies $g \in (f_1, \ldots, f_{k-1}, f_k)R$.

Suppose that $f_k g = c_1 f_1 + \cdots + c_{k-1} f_{k-1} + c_k f_k^2$ for some choice of $c_i \in R$. Then $f_k(g - c_k f_k) \in (f_1, \ldots, f_{k-1})R$. However, since $f_1, \ldots, f_k$ is regular, this implies that $g - c_k f_k \in (f_1, \ldots, f_{k-1})R$. Thus $g \in (f_1, \ldots, f_k)R$. ∎

THEOREM 2.3. $\operatorname{depth}(S^B) = \operatorname{depth}(S^{SL_2(\mathbf{F}_p)})$.

Proof. B is the normalizer of the Sylow p-subgroup P in $SL_2(\mathbf{F}_p)$. Thus B is a strongly p-embedded subgroup of $SL_2(\mathbf{F}_p)$, and it follows from [13, Corollary 1.2] that, for any representation, $\operatorname{depth}(S^B) = \operatorname{depth}(S^{SL_2(\mathbf{F}_p)})$. ∎

Define an automorphism σ of S by

$$\sigma(a_m) = \sum_{j=0}^{m} \binom{m}{j} a_{m-j}.$$

Define an automorphism ω by

$$\omega(a_m) = \sum_{j=0}^{n-m} \binom{n-m}{j} a_{m+j}.$$

For each nonzero $t \in \mathbf{F}_p$, define an automorphism ϕ_t by

$$\phi_t(a_t) = t^{n-2i} a_i.$$

Let α be a generator for the group of units in $\mathbf{F}_p$. If $p > n$, then σ has order p, and σ, ω, and ϕ_α generate the action on V^* induced by the usual symmetric power representation of $SL_2(\mathbf{F}_p)$ (see [11, Lectures VII, VIII, and IX]). Let P be the Sylow p-subgroup generated by σ and let B be the corresponding Borel subgroup. The representation of B is generated by σ and ϕ_α. If β is a monomial, then $\phi_t(\beta) = t^\lambda \beta$ for some $\lambda \in \mathbf{Z}/(p-1)$. Define the *weight* of β by $\operatorname{wt}(\beta) = \lambda$. In particular, $\operatorname{wt}(a_i) = n - 2i$. A polynomial that is weight homogeneous is called *isobaric*. Since P is a normal subgroup of B, the quotient $B/P \cong \mathbf{Z}/(p-1)$ acts on S^P, and the ring S^P decomposes into isobaric components. The weight zero component is precisely S^B. The other isobaric components are modules over S^B.

The *transfer homomorphism* is defined by

$$\begin{aligned} \operatorname{Tr}^G \colon S &\to S^G \\ f &\mapsto \sum_{g \in G} g \cdot f \end{aligned}$$

and is a homomorphism of S^G-modules. Clearly, if H is a subgroup of G, then Tr^H is a homomorphism of S^G-modules.

LEMMA 2.4. *If β is a monomial with weight λ, then* $\mathrm{Tr}^P(\beta)$ *and* $\prod_{g \in P} g(\beta)$ *are isobaric of weight λ.*

Proof. Since B normalizes P, conjugation by ϕ_t induces an automorphism of P. Define $g_t = \phi_t g \phi_t^{-1}$. Therefore,

$$\begin{aligned}\phi_t(\mathrm{Tr}^P(\beta)) = \phi_t\left(\sum_{g\in P} g(\beta)\right) &= \sum_{g\in P} \phi_t \cdot g(\beta)\\ &= \sum_{g\in G} g_t \cdot \phi_t(\beta) = \sum_{g\in P} g_t(t^\lambda \beta)\\ &= t^\lambda \sum_{g\in P} g_t(\beta) = t^\lambda \mathrm{Tr}^P(\beta),\end{aligned}$$

and $\mathrm{Tr}^P(\beta)$ is isobaric of weight λ. Similarly,

$$\begin{aligned}\phi_t\left(\prod_{g\in P} g(\beta)\right) = \prod_{g\in P} \phi_t \cdot g(\beta) &= \prod_{g\in G} g_t \cdot \phi_t(\beta)\\ &= \prod_{g\in P} g_t(t^\lambda \beta) = t^\lambda \prod_{g\in P} g_t(\beta),\end{aligned}$$

and $\prod_{g \in P} g(\beta)$ is isobaric of weight λ. ∎

3. LEAD TERMS AND GRÖBNER BASES

We use the graded reverse lexicographic monomial order with $a_m < a_{m+1}$. We direct the reader to [7, Chap. 2] for the appropriate definitions and a detailed discussion of monomial orders. We use the convention that a monomial is a product of variables and that a term is a monomial with a nonzero coefficient. Note that the zero polynomial is neither a monomial nor a term. For $f \in S$ we use $\mathrm{LT}(f)$ to denote the lead term of f and $\mathrm{LM}(f)$ to denote the lead monomial of f. For convenience we set $\mathrm{LT}(0) = \mathrm{LM}(0) = 0$.

Suppose that R is a subalgebra of S. Let $\mathrm{LT}(R)$ denote the vector space spanned by the lead terms of elements of R. $\mathrm{LT}(R)$ is a subalgebra of S. If C is a subset of R, then let $\mathrm{LM}(C)$ denote the set of lead monomials of elements of C. If $\mathrm{LM}(C)$ generates the algebra $\mathrm{LT}(R)$, then C is called a *SAGBI basis* for R. For a detailed discussion of SAGBI bases see [14] or [17, Chap. 11].

Remark 3.1. SAGBI bases were constructed for S^P with $n = 3$ and $n = 4$ in [15]. The basis for V^* used in [15] is different from the one used here, but the change of coordinates transformation between the bases can be chosen to be upper-triangular (i.e., $\mathrm{LT}(x_i) = a_{i-1}$, and the substitution map taking x_i to a_{i-1} induces an isomorphism between the lead term algebras.

LEMMA 3.2. *If $i > 0$, then* $\mathrm{LT}(\mathrm{Tr}^P(a_i^{p-1})) = -a_{i-1}^{p-1}$.

Proof. Recall that

$$\sum_{c \in \mathbf{F}_p} c^l = \begin{cases} -1 & \text{if } l \neq 0 \text{ and } p-1 \text{ divides } l; \\ 0 & \text{if } l = 0 \text{ or } p-1 \text{ does not divide } l. \end{cases}$$

Consider

$$\begin{aligned} \mathrm{Tr}^P\left(a_i^{p-1}\right) &= \sum_{c \in \mathbf{F}_p} \sigma^c\left(a_i^{p-1}\right) = \sum_{c \in \mathbf{F}_p} \left(\sum_{j=0}^{i} \binom{i}{j} c^j a_{i-j} \right)^{p-1} \\ &= \sum_{c \in \mathbf{F}_p} \left(a_i + ica_{i-1} + \sum_{j=2}^{i} \binom{i}{j} c^j a_{i-j} \right)^{p-1}. \end{aligned}$$

Clearly, the coefficient of a_{i-1}^{p-1} in $\sigma^c(a_i^{p-1})$ is $i^{p-1}c^{p-1}$. Therefore, the coefficient of a_{i-1}^{p-1} in $\mathrm{Tr}^P(a_i^{p-1})$ is -1. Furthermore, all monomials appearing in $\sigma^c(a_i^{p-1})$ which are greater than a_{i-1}^{p-1} have coefficients which, as polynomials in c, have degree less than $p-1$, and hence these monomials do not appear in $\mathrm{Tr}^P(a_i^{p-1})$. ∎

Define $d = a_1^2 - a_0 a_2$ and $N = \prod_{g \in P} g(a_n)$. Clearly, $N \in S^P$. A simple computation shows that $\sigma(d) = d$ and, therefore, $d \in S^P$. Furthermore, d is isobaric with weight $2n - 4$ and N is isobaric with weight $-np \equiv -n \pmod{p-1}$. Also, note that $\mathrm{LT}(d) = a_1^2$ and $\mathrm{LT}(N) = a_n^p$.

THEOREM 3.3. *If $n \geq 2$, then $\{a_0, d, N\} \cup \{\mathrm{Tr}^P(a_i^{p-1}) \mid 3 \leq i \leq n\}$ is a homogeneous system of parameters for S^P.*

Proof. Using Lemma 3.2, we see that

$$\begin{aligned} &\mathrm{LM}\left(\{a_0, d, N\} \cup \left\{\mathrm{Tr}^P\left(a_i^{p-1}\right) \mid 3 \leq i \leq n\right\}\right) \\ &\quad = \left\{a_0, a_1^2, a_n^p\right\} \cup \left\{a_j^{p-1} \mid 2 \leq j \leq n-1\right\}. \end{aligned}$$

Since the lead monomials are powers of the variables, the set forms a homogeneous system of parameters. ∎

We say that G is *upper-triangular* if $\mathrm{LM}(g(a_i)) = a_i$ for all i and all $g \in G$. Thus P and B are both upper-triangular. Compare the following lemma with the proof of [6, Proposition 12].

LEMMA 3.4. *Suppose that G is upper-triangular, $h \in S^G$, and $\mathrm{LT}(h) = a_n^l$ with $l > 0$. Then for any $f \in S^G$ there exist unique q and r in S^G such that $f = q \cdot h + r$ and the degree of r, as a polynomial in a_n, is less than l.*

Proof. Consider h and f as polynomials in a_n with coefficients in $\mathbf{F}_p[a_0, \ldots, a_{n-1}]$. Applying the division algorithm gives $f = q \cdot h + r$, where the degree of r, as a polynomial in a_n, is less than l. Suppose $g \in G$. Since f and h are in S^G, $f = g(f) = g(q)h + g(r)$. However, since G is upper-triangular, g does not increase the a_n-degree of a polynomial. Therefore, the a_n-degree of $g(r)$ is less than l, and, by the uniqueness of the division algorithm, $g(r) = r$ and $g(q) = q$. Thus r and q are in S^G. ∎

If R is a subalgebra of S and I is an ideal in R, then the lead term ideal $\mathrm{LT}(I)$ is an ideal in the algebra $\mathrm{LT}(R)$. A Gröbner basis for I is a subset of I whose lead monomials generate $\mathrm{LT}(I)$.

LEMMA 3.5. *If l is a positive integer and $n \geq 2$, then $\{a_0, d^l, N\}$ is a Gröbner basis for the ideal $(a_0, d^l, N)S^P$.*

Proof. We need to show that $\mathrm{LT}((a_0, d^l, N)S^P) = (a_0, a_1^{2l}, a_n^p)\mathrm{LT}(S^P)$. Suppose that $f \in (a_0, d^l, N)S^P$. Then, for some choice of $f_i \in S^P$, $f = f_1 a_0 + f_2 d^l + f_3 N$. View N and f_2 as polynomials in a_n and divide f_2 by N to get $f_2 = qN + r$, with the a_n-degree of r less than p. Thus $f = f_1 a_0 + rd^l + (f_3 + qd^l)N$. Using Lemma 3.4, we see that $q, r \in S^P$. In other words, we may choose f_2 and f_3 so that the a_n-degree of f_2 is less than p. Therefore, $\mathrm{LM}(f_2 d^l)$ and $\mathrm{LM}(f_3 N)$ are distinct. Furthermore, if a_0 divides the lead term of a polynomial then, since we are using the graded reverse lexicographic order and a_0 is the smallest variable, a_0 divides the polynomial. Thus we may choose the polynomials f_i so that either $f_2 = 0$ or a_0 does not divide $\mathrm{LT}(f_2)$, and, moreover, either $f_3 = 0$ or a_0 does not divide $\mathrm{LT}(f_3)$. Therefore, it is possible to choose $f_i \in S^P$ so that the nonzero elements of $\{f_1 a_0, f_2 d^l, f_3 N\}$ have distinct lead monomials. Thus $\mathrm{LM}(f)$ is contained in $\{\mathrm{LM}(f_1 a_0), \mathrm{LM}(f_2 d^l), \mathrm{LM}(f_3 N)\}$ and $\mathrm{LT}(f) \in (a_0, a_1^{2l}, a_n^p)\mathrm{LT}(S^P)$ as required. ∎

We remind the reader that S^B is the weight zero component of S^P. In particular, if $f \in S^P$ is isobaric then $f^{p-1} \in S^B$.

THEOREM 3.6. *If $n \geq 2$, then $\{a_0^{p-1}, d^{p-1}, N^{p-1}\}$ is regular on S^B.*

Proof. If $n = 2$, then, since S^B is Cohen–Macaulay and $\{a_0^{p-1}, d^{p-1}, N^{p-1}\}$ is a homogeneous system of parameters $\{a_0^{p-1}, d^{p-1}, N^{p-1}\}$ is regular.

Suppose $n > 2$. Since $d \in \mathbf{F}_p[a_0, a_1, a_2]$, the result follows from [6, Proposition 12]. We include a proof here for completeness. It is clear that $\{a_0^{p-1}, d^{p-1}\}$ is regular on S^B. Suppose $f, f_1, f_2 \in S^B$ and $N^{p-1}f = f_1 a_0^{p-1} + f_2 d^{p-1}$. Applying Lemma 3.4 to both f_1 and f_2 produces $q_i, r_i \in S^B$ with $f_i = q_i N^{p-1} + r_i$, such that the a_n-degree of r_i is less than $p(p-1)$. Thus $N^{p-1}(f - q_1 a_0^{p-1} - q_2 d^{p-1}) = a_0^{p-1} r_1 + d^{p-1} r_2$. The right-hand side of this equation has a_n-degree less than $p(p-1)$. The left-hand side has a_n-degree at least $p(p-1)$. Thus both sides must be zero, and, therefore, $f = q_1 a_0^{p-1} + q_2 d^{p-1}$. ∎

4. THE TRANSITIVE CASE

If $\gcd(n, p-1) = 1$, then n is odd and multiplication by n is an automorphism of the group of weights $\mathbf{Z}/(p-1)$. Furthermore, in this case, n acts transitively on $\mathbf{Z}/(p-1)$. When n is even, the action of $SL_2(\mathbf{F}_p)$ has a kernel of order two. If $\gcd(n, p-1) = 2$, then n is even, the group of weights is $2\mathbf{Z}/(p-1)$, and again n acts transitively. Define $e = 2a_1^3 - 3a_0 a_1 a_2 + a_0^2 a_3$ (see [11, Lecture XIX]). By direct computation we see that $e \in S^P$. Furthermore, e is isobaric of weight $3n - 6$.

LEMMA 4.1. $e \operatorname{Tr}^P(a_i^{p-1}) \in (a_0, d)S^P$.

Proof. We will show that $e \operatorname{Tr}^P(a_i^{p-1}) = 2d \operatorname{Tr}^P(a_1 a_i^{p-1}) - a_0 \operatorname{Tr}^P((a_1 a_2 - a_0 a_3) a_i^{p-1})$. Since Tr^P is S^P-linear.

$$2d \operatorname{Tr}^P\left(a_1 a_i^{p-1}\right) - a_0 \operatorname{Tr}^P\left((a_1 a_2 - a_0 a_3) a_i^{p-1}\right)$$
$$= \operatorname{Tr}^P\left(\left(2a_1 d - a_0(a_1 a_2 - a_0 a_3)\right) a_i^{p-1}\right).$$

However, $e = 2a_1^3 - 3a_0 a_1 a_2 + a_0^2 a_3$ and $d = a_1^2 - a_0 a_2$. Therefore, $e = 2a_1 d - a_0(a_1 a_2 - a_0 a_3)$ and $e \operatorname{Tr}^P(a_i^{p-1}) = \operatorname{Tr}^P(e a_i^{p-1}) = 2d \operatorname{Tr}^P(a_1 a_i^{p-1}) - a_0 \operatorname{Tr}^P((a_1 a_2 - a_0 a_3) a_i^{p-1})$. ∎

LEMMA 4.2. $e \notin (a_0, d, N)S^P$.

Proof. Suppose, by way of contradiction, that $e \in (a_0, d, N)S^P$. Using Lemma 3.5, it follows that $\operatorname{LT}(e) = 2a_1^3 \in (a_0, a_1^2, a_n^{p-1})\operatorname{LT}(S^P)$. Therefore, $a_1 \in \operatorname{LT}(S^P)$. However, it is clear that the only degree one elements of S^P are the scalar multiples of a_0. ∎

THEOREM 4.3. *If* $p > n > 1$ *and* $\gcd(n, p-1) \leq 2$, *then* $\operatorname{depth}(S^B) = 3$.

Proof. From Theorem 3.6 we see that $\{a_0^{p-1}, d^{p-1}, N^{p-1}\}$ is regular on S^B and thus the depth is at least three. For $n = 2$ the dimension is three and the ring is Cohen–Macaulay. Suppose $n > 2$. Since $\mathrm{wt}(N) = -n$ acts transitively on the group of weights, it is possible to choose l so that $\mathrm{wt}(N^l) = 2$ and $l < p - 1$. Using this value for l, define $m = N^l(a_0 d)^{p-2}e$. Observe that $\mathrm{wt}(m) = 0$ and hence $m \in S^B$. From Lemma 4.1, $e\,\mathrm{Tr}^P(a_i^{p-1}) \in (a_0, d)S^P$. Therefore, $m\,\mathrm{Tr}^P(a_i^{p-1}) = N^l(a_0 d)^{p-2}$ $e\,\mathrm{Tr}^P(a_i^{p-1})$ lies in $(a_0^{p-1}, d^{p-1})S^B \subseteq (a_0^{p-1}, d^{p-1}, N^{p-1})S^B$. However, it follows from Lemmas 4.2 and 2.2 that m is not in $(a_0^{p-1}, d^{p-1}, N^{p-1})S^B$. Using the homogeneous system of parameters described in Theorem 3.3 and applying Theorem 2.1 gives $\mathrm{depth}(S^B) = 3$. ∎

5. THE THIRD SYMMETRIC POWER REPRESENTATION

In this section we consider the third symmetric power representation, i.e., $n = 3$. Since $p > 3$, we have $p \equiv \pm 1 \pmod 3$. If $p \equiv -1 \pmod 3$, then Theorem 4.3 applies and $\mathrm{depth}(S^B) = 3$. Thus we may assume that $p \equiv 1 \pmod 3$. Define $w = 3a_1^2a_2^2 - 4a_1^3a_3 - 4a_0a_2^3 + 6a_0a_1a_2a_3 - a_0^2a_3^2$ (see [11, Lecture XVII]). By direct computation $w \in S^P$. Furthermore, w is isobaric of weight $2n - 6 = 0$. Thus $w \in S^B$.

LEMMA 5.1. $w^3\,\mathrm{Tr}^P(a_3^{p-1}) \in (a_0, d^3)S^P$.

Proof. Since $w = 3a_1^2a_2^2 - 4a_1^3a_3 - 4a_0a_2^3 + 6a_0a_1a_2a_3 - a_0^2a_3^2$ and $d = a_1^2 - a_0a_2$, there is a polynomial f such that $w^3 = d^3(3a_2^2 - 4a_1a_3)^3 + a_0 f$. Since Tr^P is S^P-linear, we have $w^3\,\mathrm{Tr}^P(a_3^{p-1}) = d^3\,\mathrm{Tr}^P((3a_2^2 - 4a_1a_3)^3a_3^{p-1}) - a_0\,\mathrm{Tr}^P(fa_3^{p-1})$. ∎

LEMMA 5.2. *If $p > 7$, then $w^3 \notin (a_0, d^3, N)S^P$.*

Proof. Suppose, by way of contradiction, that $p > 7$ and $w^3 \in (a_0, d^3, N)S^P$. Using Lemma 3.5 with $l = 3$, we see that $\mathrm{LT}(w^3) = 27a_1^6a_2^6 \in (a_0, a_1^6, a_n^p)\mathrm{LT}(S^P)$. Therefore, $a_2^6 \in \mathrm{LT}(S^P)$. However, for $n = 3$, the algebra $\mathrm{LT}(S^P)$ is described in [15, Sect. 4]. From this description we see that a_2^{p-1} is the smallest power of a_2 contained in $\mathrm{LT}(S^P)$. Thus, if $p > 7$, $a_2^6 \notin \mathrm{LT}(S^P)$, giving the required contradiction. ∎

THEOREM 5.3. *If $n = 3$ and $p > 7$, then* $\mathrm{depth}(S^B) = 3$.

Proof. It follows from Theorem 3.6 that $\{a_0^{p-1}, d^{p-1}, N^{p-1}\}$ is regular on S^B and hence the depth is at least three. Take $l = (p - 10)/3$ and define $m = a_0^{p-2}d^{p-4}N^lw^3$. Observe that $\mathrm{wt}(m) = 0$ and hence $m \in S^B$. From Lemma 5.1 we see that $m\,\mathrm{Tr}^P(a_3^{p-1}) \in (a_0^{p-1}, d^{p-1}, N^{p-1})S^B$. However, it follows from Lemmas 5.2 and 2.2 that m is not in $(a_0^{p-1}, d^{p-1}, N^{p-1})S^B$. Using the homogeneous system of parameters described in Theorem 3.3 and applying Theorem 2.1 gives $\mathrm{depth}(S^B) = 3$. ∎

For $n = 3$ and $p = 7$ a calculation, either by hand or using the computer algebra program MAGMA [3], shows that $\operatorname{depth}(S^B) = 4$. Since the Krull dimension is four, this means that, in this case, S^B is Cohen–Macaulay.

6. THE FOURTH SYMMETRIC POWER REPRESENTATION

In this section we consider the fourth symmetric power representation, i.e., $n = 4$. Since $p > 4$, we have $p \equiv \pm 1 \pmod 4$. If $p \equiv -1 \pmod 4$, then Theorem 4.3 applies and $\operatorname{depth}(S^B) = 3$. Thus we may assume that $p \equiv 1 \pmod 4$. Referring to Remark 3.1 and [15, Sect. 2], we see that there is an element of S^P with lead monomial $a_1^2 a_2^2 a_3^2$. Thus we may choose an isobaric $u \in S^P$ with $\operatorname{LT}(u) = a_1^2 a_2^2 a_3^2$. Note that $\operatorname{wt}(u) = 0$.

LEMMA 6.1. *If* $i \in \{3, 4\}$, *then* $u \operatorname{Tr}^P(a_i^{p-1}) \in (a_0, d)S^P$.

Proof. In the graded reverse lexicographic order, every monomial of degree 6 smaller than $a_1^2 a_2^2 a_3^2$ is divisible by either a_0 or a_1^2. It follows from this that there are polynomials f_1 and f_2 such that $u = f_1 d + f_2 a_0$. Since Tr^P is S^P-linear, $u \operatorname{Tr}^P(a_i^{p-1}) = d \operatorname{Tr}^P(f_1 a_i^{p-1}) + a_0 \operatorname{Tr}^P(f_2 a_i^{p-1})$. ∎

LEMMA 6.2. *If* $p > 7$, *then* $u \notin (a_0, d, N)S^P$.

Proof. By way of contradiction, assume that $p > 7$ and $u \in (a_0, d, N)S^P$. Using Lemma 3.5 we see that $\operatorname{LT}(u) = a_1^2 a_2^2 a_3^2 \in (a_0, a_1^2, a_n^p)\operatorname{LT}(S^P)$. Therefore, $a_2^2 a_3^2 \in \operatorname{LT}(S^P)$. However, for $n = 4$, the algebra $\operatorname{LT}(S^P)$ is described in [15, Sect. 5]. Using this description we see that, for $p > 7$, $a_2^2 a_3^2$ is not in $\operatorname{LT}(S^P)$, giving the required contradiction. ∎

THEOREM 6.3. *If* $n = 4$ *and* $p > 5$, *then* $\operatorname{depth}(S^B) = 3$.

Proof. Using Theorem 3.6 we see that $\{a_0^{p-1}, d^{p-1}, N^{p-1}\}$ is regular on S^B and hence the depth is at least three. Take $l = (p - 9)/4$ and define $m = a_0^{p-2} d^{p-2} N^l u$. Observe that $\operatorname{wt}(m) = 0$ and hence $m \in S^B$. From Lemma 6.1 we see that, for $i \in \{3, 4\}$, $m \operatorname{Tr}^P(a_i^{p-1}) \in (a_0^{p-1}, d^{p-1}, N^{p-1})S^B$. However, it follows from Lemmas 6.2 and 2.2 that m is not in the ideal $(a_0^{p-1}, d^{p-1}, N^{p-1})S^B$. Using the homogeneous system of parameters described in Theorem 3.3 and applying Theorem 2.1 gives $\operatorname{depth}(S^B) = 3$. ∎

For $n = p - 1$ the representation of $SL_2(\mathbf{F}_p)$ is projective and P acts as a permutation group. For this representation S^B is Cohen–Macaulay (see [13, Example 1.3]). Thus for $n = 4$, $p = 5$ the depth of S^B is five.

7. CONCLUDING REMARKS

For the four- and five-dimensional irreducible representations of $SL_2(\mathbf{F}_p)$, the ring of invariants has depth three, except for one exceptional prime for each dimension. At these exceptional primes the invariants are Cohen–Macaulay. What happens in higher dimensions? We expect to see a finite number of exceptional primes for each dimension. Are there any examples where the depth is not three and the ring is not Cohen–Macaulay? Certainly when $n = p - 1$ the invariants are Cohen–Macaulay. However, the $n = 3$, $p = 7$ case shows that other exceptions are possible. Extending the methods used here to the dimension six representations would require the construction of a SAGBI basis for the invariants of the Sylow p-subgroup—a nontrivial task. The first candidate for an exceptional prime in dimension six is 11. At present, computing the depth of the Borel invariants for $p = 11$, $n = 5$ is beyond our computational resources.

ACKNOWLEDGMENT

We thank the referee for a careful reading of the paper and many useful remarks.

REFERENCES

1. J. L. Alperin, "Local Representation Theory," Cambridge Studies in Advanced Mathematics, Vol. 11, Cambridge Univ. Press, Cambridge, UK, 1986.
2. D. J. Benson, "Polynomial Invariants of Finite Groups," London Math. Society Lecture Note Series, Vol. 190, Cambridge Univ. Press, Cambridge, UK, 1993.
3. W. Bosma, J. J. Cannon, and C. Playoust, The Magma algebra system. I. The user language, *J. Symbolic Comput*. **24** (1997), 235–265.
4. D. Bourguiba and S. Zarati, Depth and the Steenrod algebra, *Invent. Math*. **128** (1997), 589–602.
5. W. Bruns and J. Herzog, "Cohen–Macaulay Rings," Cambridge Studies in Advanced Mathematics, Vol. 39, Cambridge Univ. Press, Cambridge, UK, 1993.
6. H. E. A. Campbell, I. P. Hughes, G. Kemper, R. J. Shank, and D. L. Wehlau, Depth of modular invariant rings, preprint, 1997, pp. 1–11.
7. D. Cox, J. Little, and D. O'Shea, "Ideals, Varieties, and Algorithms," Springer-Verlag, Berlin/New York, 1992.
8. L. E. J. Dickson, "On Invariants and the Theory of Numbers," The Madison Colloquium (1913), Amer. Math. Society; reprinted, Dover, New York, 1966.
9. D. Eisenbud, "Commutative Algebra with a View Toward Algebraic Geometry," Graduate Texts in Mathematics, Vol. 150, Springer-Verlag, New York/Berlin, 1996.
10. G. Ellingsrud and T. Skjelbred, Profonder d'anneaux d'invariants en caractéristique p, *Compositio Math*. **41** (1980), 233–244.
11. D. Hilbert, "Theory of Algebraic Invariants," (R. C. Laubenbacher, trans.; B. Sturmfels, Ed.), Cambridge Univ. Press, Cambridge, UK, 1993.

12. G. Kemper, Calculating invariant rings of finite groups over arbitrary fields, *J. Symbolic Comput.* **21** (1996), 351–366.
13. G. Kemper, On the Cohen–Macaulay property of modular invariant rings, *J. Algebra*, to appear.
14. L. Robbiano and M. Sweedler, Subalgebra bases, *Lecture Notes in Math.* **1430** (1990), 61–87.
15. R. J. Shank, S.A.G.B.I. bases for rings of formal modular seminvariants, *Comment. Math. Helv.* **73**, No. 4 (1998).
16. L. Smith, ‘‘Polynomial Invariants of Finite Groups,’’ Peters, Wellesley, MA, 1995.
17. B. Sturmfels, ‘‘Gröbner Bases and Convex Polytopes,’’ University Lecture Note Series, Vol. 8, American Math. Society, Providence, RI, 1996.