SYMMETRIC DETERMINANTS AND JORDAN NORM SIMILARITIES IN CHARACTERISTIC 2

WILLIAM C. WATERHOUSE[1]

ABSTRACT. We first determine all linear changes of variable formally preserving symmetric determinants in characteristic 2; there are just slightly more of them than in other characteristics. We then restate this result in terms of affine group schemes. This allows us to apply descent theory, and thereby we prove a theorem on norm similarities of Jordan algebras in the one case left open by Jacobson.

Consider an $n \times n$ symmetric matrix with indeterminate entries X_i on the diagonal and Y_{ij} (for $i < j$) in the (i, j) and (j, i) positions. Let $D(X, Y)$ be its determinant. We are interested in the linear changes of variable (in X and Y), with coefficients in a fixed commutative ring R, that take D to a constant multiple of itself. When 2 is not a zero-divisor in R, these maps are known [5, §6]. In this paper we will consider only the case where R has characteristic 2.

Once the characteristic is 2, we can evaluate D by the classical formula [4, p. 410] for a determinant with skew off-diagonal entries:

$$D = \sum_I \mathrm{Pf}_I (Y_{ij})^2 \cdot \prod_{i \notin I} X_i,$$

where Pf_I means the Pfaffian of the alternating matrix having entries Y_{ij} with i, j in I. The sum runs over all subsets I of $\{1, 2, \ldots, n\}$ containing an even number of elements; it includes $I = \varnothing$, with the Pfaffian put equal to 1. Indeed, if we expand out a determinant and look at the terms containing just a specified set of diagonal entries, we find that the remaining factors in those terms are the diagonal-avoiding terms in the complementary principal minor (an observation due to Cayley). In our case the off-diagonal entries are skew, and so these remaining factors add up to the square of the Pfaffian (giving zero, of course, for odd sizes). As Pf_I is a polynomial with coefficients in the prime field $\mathbf{F}_2$, we can move the square inside and write

$$D = \sum_I \mathrm{Pf}_I (Y_{ij}^2) \cdot \prod_{i \notin I} X_i.$$

1. A determinant identity.

LEMMA 1. *Let* (a_i^j) *be elements in a ring of characteristic 2, with* $1 \leqslant i, j \leqslant n$. *Then*

$$\sum_I \mathrm{Pf}_I\left(\sum_k a_i^k a_j^k X_k^2 + \sum_{r<s} \left(a_i^r a_j^s + a_i^s a_j^r\right)Y_{rs}^2\right) \cdot \prod_{i \notin I}\left(\sum_j a_i^j X_j\right)$$
$$= \det\left(a_i^j\right) \cdot D(X, Y).$$

PROOF. It is enough to prove this identity for a_i^j indeterminates over $\mathbf{F}_2$. Extend the ring $\mathbf{F}_2[(a_i^j)]$ by adjoining square roots p_i^j, so $a_i^j = (p_i^j)^2$. Let P be the matrix (p_i^j). The map replacing our original X, Y matrix by

$$P\begin{pmatrix} X_1 & Y_{12} & \cdots \\ \vdots & & \vdots \\ \cdots & \cdots & \cdots \end{pmatrix}P^{\mathrm{tr}}$$

multiplies the determinant by $(\det P)^2 = \det(a_i^j)$. But it is straightforward to compute that this map replaces the diagonal entry X_i by $\sum_j (p_i^j)^2 X_j$, or $\sum_j a_i^j X_j$, while it replaces the off-diagonal entry Y_{ij} by

$$\sum_k p_i^k p_j^k X_k + \sum_{r<s} \left(p_i^r p_j^s + p_i^s p_j^r\right)Y_{rs}.$$

As the characteristic is 2, the square of this expression is

$$\sum_k a_i^k a_j^k X_k^2 + \sum_{r<s} \left(a_i^r a_j^s + a_i^s a_j^r\right)Y_{rs}^2.$$

Thus the formula for D, applied to our new determinant, does yield the left side of the identity stated in the lemma. □

2. Changes of variable perserving $D(X, Y)$.

THEOREM 2. *Let*

$$U_i = \sum a_i^j X_j + \sum b_i^{jk} Y_{jk} \quad and \quad V_{ij} = \sum c_{ij}^k X_k + \sum d_{ij}^{rs} Y_{rs},$$

where the coefficients lie in a ring of characteristic 2. These expressions will be new independent variables with $D(U, V)$ *a constant multiple of* $D(X, Y)$ *precisely when*:
  (1) $\det(a_i^j)$ *is invertible,*
  (2) *all* $b_i^{jk} = 0$,
  (3) $(c_{ij}^k)^2 = a_i^k a_j^k$, *and*
  (4) $(d_{ij}^{rs})^2 = a_i^r a_j^s + a_i^s a_j^r$.
Under these conditions, $D(U, V) = \det(a_i^j)D(X, Y)$.

PROOF. It follows from Lemma 1 that the conditions are sufficient. Indeed, only $(V_{ij})^2$ enters the formula for $D(U, V)$, and conditions (3) and (4) allow us to express the coefficients in $(V_{ij})^2$ in terms of the a_r^s. Since condition (2) shows that no Y_{jk} terms occur in U_i, we have $D(U, V) = \det(a_i^j)D(X, Y)$ by the lemma.

Suppose now, conversely, that we have an arbitrary change of variables for which

$$D(U, V) = \sum_I \mathrm{Pf}_I\left(V_{ij}^2\right) \cdot \prod_{i \notin I} U_i$$

is a constant multiple α times $D(X, Y)$. We assume, of course, that the change of variables is invertible, so the U_i and V_{ij} are again independent variables. To analyze the identity $D(U(X, Y), V(X, Y)) = \alpha D(X, Y)$, we can use a method due originally (I believe) to Frobenius [1]. What we do is to introduce a new variable Z, add it to one of X_i or Y_{ij}, expand the resulting identity, and compare the terms of the same degree in Z.

First, let us add Z to Y_{pq}. In $D(X, Y)$, the variable Y_{pq} occurs only as Y_{pq}^2. Thus there will be no terms of degree 1 in Z. Similarly, $D(U, V)$ will not give any terms of degree 1 in Z arising from the Y_{pq} in $\mathrm{Pf}_I(V_{ij}^2)$. Thus the only terms of degree 1 in Z are those occuring in

$$\sum_I \mathrm{Pf}_I\left(V_{ij}^2\right) \cdot \prod_{i \notin I}\left(U_i + b_i^{pq}Z\right),$$

namely,

$$\sum_I \mathrm{Pf}_I\left(V_{ij}^2\right) \cdot \sum_{r \notin I}\left(\prod_{\substack{j \notin I \\ j \neq r}} U_j\right) b_r^{pq}Z.$$

The coefficient of Z in this sum must therefore be identically zero. In particular, looking only at the terms involving no V_{ij}^2, we find that

$$\sum_r \left(\prod_{j \notin r} U_j\right) b_r^{pq}$$

must be identically zero. As the U_j are independent variables, this implies condition (2) of the theorem.

At this point we might look back at the identity $D(U, V) = \alpha D(X, Y)$. The term $\alpha X_1 \cdots X_n$ on the right can arise only from the term $U_1 \cdots U_n$ on the left, since all other terms there involve squares. But the coefficient of $X_1 \cdots X_n$ in $U_1 \cdots U_n$ is just $\det(a_i^j)$, since the characteristic is 2 and signs are irrelevant in the determinant. As our change of variables can be inverted, α is invertible, and thus condition (1) must hold.

Continuing with the identity $D(U, V) = \alpha D(X, Y)$, let us look for terms of the form $Y_{pq}^2(\Pi_{i \neq p,q}X_i)$. Such a term occurs exactly once in $D(X, Y)$. In $D(U, V)$, no such monomial will occur for any I containing 4 or more indices, since each term in $\mathrm{Pf}_I(V^2)$ either will have a higher degree in Y or will involve the square of some X_i. By condition (2), no terms of our form occur in $U_1 \cdots U_n$. Thus such terms arise only from subsets I containing exactly two indices. These subsets give

$$\sum_{r<s} \left(d_{pq}^{rs}\right)^2 Y_{pq}^2 \cdot \prod_{j \neq r,s} U_j.$$

Now the coefficient of $\Pi_{i \neq u,v}X_i$ in $\Pi_{j \neq r,s}U_j$ is simply an $(n-2) \times (n-2)$ minor determinant of (a_i^j), since again signs are irrelevant in characteristic 2. Let us denote this minor by M_{uv}^{rs}. We know that $D(X, Y)$ does not contain any term with Y_{pq}^2 times any other product of X's. Thus

$$\sum_{r<s} \left(d_{pq}^{rs}\right)^2 \cdot M_{uv}^{rs} = \begin{cases} \alpha = \det\left(a_i^j\right) & \text{if } p = u, q = v, \\ 0 & \text{otherwise.} \end{cases}$$

As an equation on square matrices of size $n(n-1)/2$, this says that

$$\left[\left(d_{pq}^{rs}\right)^2\right] \cdot \left[\wedge^{n-2}\left(a_i^j\right)\right] = \det\left(a_i^j\right) \cdot Id.$$

But there is a classical identity on adjoints, and once we ignore signs it tells us that

$$\left[\wedge^2\left(a_i^j\right)\right] \cdot \left[\wedge^{n-2}\left(a_i^j\right)\right] = \det\left(a_i^j\right) \cdot Id.$$

Since we already know $\det(a_i^j)$ is invertible, we know that $\wedge^{n-2}(a_i^j)$ is an invertible matrix, and hence we can deduce

$$\left[\left(d_{pq}^{rs}\right)^2\right] = \left[\wedge^2\left(a_i^j\right)\right].$$

When we read this off entry by entry, we get condition (4).

Finally, to determine the c_{ij}^k we consider the effect of changing X_k to $X_k + Z$. In $D(X, Y)$, the factor X_k occurs only to the first power, and thus we will get no terms at all that involve Z^2. Hence when we make the corresponding change in U and V, the Z^2-terms must all cancel. The expression we have, to begin with, is

$$\sum_I \mathrm{Pf}_I\left(V_{ij}^2 + \left(c_{ij}^k Z\right)^2\right) \cdot \prod_{i \notin I}\left(U_i + a_i^k Z\right).$$

Let us focus on the terms that involve Z^2 and $(n-2)$ distinct U_i, with no V_{ij} factors or higher U_i-powers. As in the previous argument, we see that such terms can come only from I with less than 4 elements. Those with 2 elements give

$$\sum_{i<j}\left(c_{ij}^k\right)^2 Z^2 \cdot \prod_{r \neq i,j} U_r,$$

while $I = \varnothing$ gives

$$\sum_{i<j} a_i^k a_j^k Z^2 \cdot \prod_{r \neq i,j} U_r.$$

The U_r are independent, and these terms must cancel each other; thus condition (3) must hold. □

3. Interpretation using affine group schemes. The conditions in Theorem 2 define an affine group scheme F over $\mathbf{F}_2$. That is [5], for every R of characteristic 2 they single out a subgroup $F(R)$ inside $GL_{n(n+1)/2}(R)$, and this subgroup is defined by polynomial equations on the matrix entries. Our goal now is to analyze this affine group scheme. One result will be a more explicit determination of $F(R)$ when R is reduced.

PROPOSITION 3. *The Lie algebra* $\mathrm{Lie}(F)$ *has dimension* $1 + n^2(n^2 - 1)/4$.

PROOF. Let $R = \mathbf{F}_2[\varepsilon]$ with $\varepsilon^2 = 0$. The Lie algebra of a group scheme, in one of its equivalent forms [5, Chapter 12], consists of those elements in $F(R)$ that reduce to the identity when we reduce ε to 0. Condition (2) tells us that the b_i^{jk} are zero. The other entries will have the form

$$a_i^j = \delta_i^j + \varepsilon A_i^j, \quad c_{ij}^k = \varepsilon C_{ij}^k, \quad d_{ij}^{rs} = \delta_i^r \delta_j^s + \varepsilon D_{ij}^{rs}$$

for scalars A, C, D. The invertibility of $\det(a_i^j)$ is automatic for such elements. Condition (3) requires $(c_{ij}^k)^2$, which is $= \varepsilon^2(C_{ij}^k)^2 = 0$, to equal

$$a_i^k a_j^k = \varepsilon\left(\delta_i^k A_j^k + \delta_j^k A_i^k\right).$$

This imposes no restrictions on the c_{ij}^k, but it forces $\delta_i^k A_j^k + \delta_j^k A_i^k = 0$. This says that $A_p^q = 0$ for $p \neq q$.

Finally, condition (4) deals with $(d_{ij}^{rs})^2$, which $= (\delta_i^r \delta_j^s + \varepsilon D_{ij}^{rs})^2 = \delta_i^r \delta_j^s$; this must equal $a_i^r a_j^s + a_i^s a_j^r$. Since $A_p^q = 0$ for $p \neq q$, this condition is automatic unless $i = r$ and $j = s$; in that case, it gives us $1 = 1 + \varepsilon(A_i^i + A_j^j)$. Thus all A_i^i are equal.

All in all, then, we have one degree of freedom among the A_i^j and free choice of the $n \cdot n(n-1)/2$ different C_{ij}^k and the $[n(n-1)/2]^2$ different D_{ij}^{rs}. These dimensions add up to $1 + n^2(n^2 - 1)/4$. $\square$

In characteristic zero, the dimension of the Lie algebra equals the dimension of the group. In positive characteristics, this is true only for "smooth" group schemes. In characteristic $\neq 2$, the group scheme preserving symmetric determinants up to scalar is, in fact, still smooth. (This was first stated explicitly in [6, 7], but it is an immediate consequence of results proved earlier by Jacobson [2, 3].) Here in characteristic 2, however, we shall see that for $n > 2$ the group scheme F is not smooth. To show this, we use two maps interrelating F and GL_n.

First of all, the computation in the proof of Lemma 1 shows that there is a homomorphism $GL_n(R) \to F(R)$ sending P to $P(\ )P^{tr}$. The kernel of this map is easily computed: it is $\mu_2(R)$, the scalars α with $\alpha^2 = 1$. (There may be nontrivial such α even in characteristic 2, since R in general is not assumed to be a field.) Group schemes like this kernel, trivial on fields, may be called "infinitesimal".

The formulas in Theorem 2 show that there is also a natural homomorphism $F(R) \to GL_n(R)$, sending an element in $F(R)$ to (a_i^j). The kernel of this map is again infinitesimal: for when $a_i^j = \delta_i^j$, we have $(c_{ij}^k)^2 = 0$ and $(d_{ij}^{rs})^2 = \delta_i^r \delta_j^s$, and these conditions force an element in $F(R)$ to be the identity when R is a field. Finally, the computations in Lemma 1 show that the composite map $GL_n \to F \to GL_n$ sends (p_i^j) to $([p_i^j]^2)$. This is what is called the Frobenius endomorphism in characteristic 2, and on smooth groups like GL_n it is an epimorphism (surjective when R is an algebraically closed field). Hence $F \to GL_n$ is an epimorphism. Since the infinitesimal kernel is connected of dimension 0, and GL_n is connected of dimension n^2, we have

PROPOSITION 4. *The group scheme F is connected and has dimension n^2.* $\square$

Comparing this with the result in Proposition 3, we immediately have

COROLLARY 5. *If $n \geqslant 3$, the group scheme F is not smooth.* $\square$

Let A be the algebra over $\mathbf{F}_2$ constructed by taking the formal ring

$$\mathbf{F}_2\left[a_i^j, c_{ij}^k, d_{ij}^{rs}, 1/\det\left(a_i^j\right)\right]$$

and dividing by the relations in Theorem 2. Then Corollary 5 says that (for $n \geqslant 3$) there are nontrivial nilpotent elements in A. We can define a smooth subgroup

$F_{red}(R)$ of $F(R)$ by imposing the further condition that all nilpotent expressions in A vanish on the entries of elements in F_{red}. (When R is a field, $F_{red}(R) = F(R)$.) We already have GL_n mapping into F with kernel μ_2, and hence the group scheme quotient GL_n/μ_2 is embedded as a closed subgroup of F. As GL_n is smooth, so is GL_n/μ_2, and thus GL_n/μ_2 is inside F_{red}. But F_{red} is connected (since F is), and by Proposition 4 it has the same dimension as GL_n/μ_2. By [5, 12.4], we have equality:

PROPOSITION 6. *We have $F_{red} \simeq GL_n/\mu_2$.* $\square$

If R is reduced (i.e., without nilpotents), then any solution in R of the equations defining F will satisfy the further conditions defining F_{red}. Thus

COROLLARY 7. *If R is reduced, $F(R) \simeq (GL_n/\mu_2)(R)$.* $\square$

This corollary answers a question raised in [6], where the case $n = 3$ was worked out. It does *not* imply that the map from $GL_n(R)$ to $F(R)$ is surjective, since the map $GL_n \to GL_n/\mu_2$ is only a group scheme epimorphism. As shown in [6], the true conclusion is

PROPOSITION 8. *Suppose R is reduced. Then the maps $\lambda P(\ )P^{tr}$ (for invertible scalar λ, matrix P) are a normal subgroup of $F(R)$. When n is odd, they are all of $F(R)$. When n is even, the quotient is isomorphic to the group of invertible R-modules M satisfying $M \otimes M \simeq R$ and $\oplus_1^n M \simeq R^n$.* $\square$

For R containing nilpotents, this proposition will not hold. That is illustrated by the computation with $R = \mathbf{F}_2[\varepsilon]$ in Proposition 3.

4. Application to Jordan algebras.

THEOREM 9. *Let k be a field. Let A be a central simple algebra over k, and suppose J is an involution of orthogonal type on A. Let $H(A, J)$ be the fixed set of J, a (quadratic) Jordan algebra over k, and let N be its generic norm polynomial. The only invertible linear maps $\varphi: H \to H$ for which $N(\varphi X)$ is a constant multiple of $N(X)$ are those of the form $\varphi(X) = \lambda cXc^J$, for invertible λ in k and c in A.*

PROOF. This result was proved by Jacobson [2, 3] except in characteristic 2, so we may assume char$(k) = 2$. (An argument like the one here would, of course, work also in other characteristics.) Let F_1 be the affine group scheme preserving the polynomial N. Let G be the affine group scheme defined by $G(R) = (A \otimes R)^\times$. We have a group scheme homomorphism $G_m \times G \to F_1$ sending (λ, c) to the map $X \mapsto \lambda cXc^J$. We want to show that $G_m(k) \times G(k)$ maps onto $F_1(k)$.

We know that over the algebraic closure $\bar{k}$ there is an isomorphism of $A \otimes \bar{k}$ to some $M_n(k)$ taking J to the transposition map. Thus over $\bar{k}$ we see that the Jordan algebra H becomes isomorphic to the symmetric matrices. Hence N becomes the determinant, and F_1 becomes the F of the previous section, while G becomes GL_n. In particular, this shows that $G_m \times G$ is smooth, since it is so after base extension. It follows that $G_m \times G$ has a smooth image G_1, a closed subgroup of F_1. Over $\bar{k}$, this G_1 becomes GL_n/μ_2, and is equal to F_{red}.

The argument now is routine. Let A_1 be the ring representing F_1; over $\bar{k}$, we know that $A_1 \otimes \bar{k}$ is isomorphic to $A \otimes \bar{k}$, where A is the ring introduced just before Proposition 6. The closed subgroup G_1 of F_1 is represented by some quotient ring A_1/I. As G_1 becomes F_{red} over $\bar{k}$, we see that

$$(A_1/I) \otimes \bar{k} = (A \otimes \bar{k})/(\text{nilpotents}).$$

Hence I consists of nilpotents. Since the field k is certainly reduced, it follows that all elements of $F_1(k)$ are actually in $G_1(k)$. Finally now we observe that $G_m \times G \to G_1$ has kernel consisting of the $(\lambda, \alpha I)$ with $\lambda \alpha^2 = 1$, since this is true after we extend to $\bar{k}$. This kernel is isomorphic to G_m under the map $(\lambda, \alpha I) \to \alpha$. But the cohomology group $H^1(\bar{k}/k, G_m)$ is trivial, and it follows that $(G_m \times G)(k) \to G_1(k)$ is surjective [5, 18.1]. $\square$

Thus we see that the norm similarities here in characteristic 2 are the same as in other characteristics. But a related question brings out the special nature of characteristic 2. The Lie algebra of the group scheme F_1 in this theorem is, in Jacobson's terms, the Lie algebra leaving the generic norm semi-invariant. In other characteristics, F_1 equals the structure group G_1, and so Lie F_1 is the same as the n^2-dimensional algebra Lie G_1. But in characteristic 2, since F_1 becomes isomorphic to F over $\bar{k}$, the dimension of Lie F_1 is given by Proposition 3, and for $n \geqslant 3$ this is much larger than n^2. In other words, though the norm similarities F_1 here differ only "infinitesimally" from the structure group G_1, the difference reveals itself in the Lie algebra preserving the norm.

REFERENCES

1. G. Frobenius, *Über die Darstellung der endlichen Gruppen durch lineare Substitutionen*, Berlin Sitzungsber, 1897, pp. 994–1015; Abhandlungen III, pp. 83–103.

2. N. Jacobson, *Structure and representations of Jordan algebras*, Amer. Math. Soc., Colloq. Publ., vol. 39, Amer. Math. Soc., Providence, R. I., 1968.

3. _____, *Structure groups and Lie algebras of Jordan algebras of symmetric elements of associative algebras with involution*, Adv. in Math. **20** (1976), 106–150.

4. T. Muir, *A treatise on the theory of determinants*, Dover, New York, 1960.

5. W. C. Waterhouse, *Introduction to affine group schemes*, Graduate Texts in Math., No. 66, Springer-Verlag, New York, 1979.

6. _____, *Automorphisms of* det(X_{ij}): *The group scheme approach*, Adv. in Math. (to appear)

7. _____, *Twisted forms of the determinant*, J. Algebra **86** (1984), 60–75.

DEPARTMENT OF MATHEMATICS, PENNSYLVANIA STATE UNIVERSITY, UNIVERSITY PARK, PENNSYLVANIA 16802