Invariants of Binary Bilinear Forms Modulo Two

Larry Smith and R. E. Stong

AG-INVARIANTENTHEORIE UNIVERSITY OF VIRGINIA

20.7.2008@14:15

SUMMARY : *In this note we examine the invariant theory of binary bilinear forms over the field $\mathbb{F}_2$ of two elements that arises in the classification of standardly graded Poincaré duality algebras with two generators over the field $\mathbb{F}_2$ of two elements. We compute the corresponding ring of invariants and find seperating invariants for the orbit space.*

MATHEMATICS SUBJECT CLASSIFICATION : 13A50 Invariant Theory

Typeset by $\mathcal{LS}$ TEX

INVARIANTS of binary forms occur in many places in mathematics. This note is devoted to a case where they arise in connection with the classification of Poincaré duality algebras. Recall that a commutative graded[1] connected algebra H over a field $\mathbb{F}$ is called a **Poincaré duality algebra** of **formal dimension** d if the following conditions are satisfied.

(1) $H_i = 0$ for $i > d$.
(2) H_d is a 1-dimensional vector space over $\mathbb{F}$.
(3) An element $u \in H_i$ is nonzero if and only if there exists an element $u^\vee \in H_{d-i}$, called a **Poincaré dual** for u, such that the product $u \cdot u^\vee \neq 0 \in H_d$.

A nonzero element $[H] \in H_d$ is called a **fundamental class**. If H is generated by its homogeneous component of degree one then it is said to be **standardly graded**. A standardly graded Poincaré duality algebra may be written as a quotient $\mathbb{F}[z_1, \ldots, z_n]/I$ of the polynomial algebra $\mathbb{F}[z_1, \ldots, z_n]$, where $I \subset \mathbb{F}[z_1, \ldots, z_n]$ is an irreducible ideal primary for the maximal ideal $\mathfrak{m}$ (see e.g., [8] Part I). The smallest possible $n \in \mathbb{N}_0$, which is just the dimension of H_1 over $\mathbb{F}$, is called the **rank** of H and denoted by $\operatorname{rank}(H)$.

We are interested in determining the isomorphism classes of standardly graded Poincaré duality algebras of a given rank and formal dimension. The case of rank one is simple: For a given formal dimension d there is the algebra $\mathbb{F}[x]/(x^{d+1})$ and up to isomorphism nothing else. For algebras of rank two or more the situation is richer in examples and their classification more intricate.

If $\mathbb{F} = \mathbb{F}_2$ and $\text{f-dim}(H) = 2 = \operatorname{rank}(H)$ there are only three isomorphism classes and they are listed in [8] §II.3. For $\text{f-dim}(H) = 3$ and $\operatorname{rank}(H) = 2$ there are five isomorphism classes as shown by [8] Theorem I.6.6. What are they and how does one distinguish them? We choose to use the invariant theory of binary bilinear forms (noncommutative and over the finite field $\mathbb{F}_2$) to deal with these problems.[2] Here is how.

If we write $H = \mathbb{F}_2[x, y]/I$ the matrix of products between H_1 and H_2, viz.,

$cat_H(1, 2)$	x^2	y^2	xy
x	a	b	c
y	c	d	b

determines H up to isomorphism. Moreover two such tables of products determine isomorphic algebras if and only if they are in the same $\mathrm{GL}(2, \mathbb{F}_2)$-orbit of the transpose action of $\mathrm{GL}(2, \mathbb{F}_2)$ on the 2×3 matrices given by sending $\mathbf{C} \in \mathrm{Mat}_{\mathbb{F}_2}(2, 3)$ and $g \in \mathrm{GL}(2, \mathbb{F}_2)$ into $g \cdot \mathbf{C} \cdot g^{\mathrm{tr}}$, where g^{tr} denotes the transpose of g. We are thus led to a modular version of a problem of classical invariant theory: In this case the classification of nonsymmetric bilinear forms.

Specifically, the matrix $cat_H(1, 2)$ is completely determined by the square submatrix $\mathbf{Q}_H \in \mathrm{Mat}_{\mathbb{F}_2}(2, 2)$ composed of the first two columns of of $cat_H(1, 2)$. This matrix determines, and is determined by, the bilinear form

$$\varphi : H_1 \times H_1 \longrightarrow \mathbb{F}_2 \text{ defined by } \varphi(u, v) = u \cdot v^2, \qquad u, v \in H_1,$$

[1] We advise the reader that we adhere to the grading conventions of J. C. Moore and therefore all elements in graded objects are homogeneous unless explicitly stated to the contrary. For a graded object $-$ we denote by $-_i$ its homogeneous component of degree $i \in \mathbb{N}_0$.

[2] This is not the only approach possible; see e.g., [1] or [5] for geometric approaches to the classifiaction of binary biliner forms.

obtained[3] by identifying H_3 with $\mathbb{F}_2$. The five isomorphism classes of standardly graded Poincaré duality algebras of formal dimension three and rank two are thus in bijective correspondence with the orbits of $\mathrm{GL}(2, \mathbb{F}_2)$ on the nonzero elements of $\mathrm{Mat}_{\mathbb{F}_2}(2, 2)$. The elements of $\mathbb{F}_2[\mathrm{Mat}_{\mathbb{F}_2}(2, 2)]^{\mathrm{GL}(2, \mathbb{F}_2)}$ are invariants of these algebras. It is to provide a new computation of this invariant algebra that is the main objective of this note. Such a computation has already been given by N. Anghel (see [2]) but his paper is quite long and requires special auxiliary arguments (loc. cit. §3) in the case of characteristic two.[4]

Before beginning the actual work we make a few remarks concerning this problem. Note that $\mathrm{Mat}_{\mathbb{F}_2}(2, 2)$ is 4-dimensional and $\mathrm{GL}(2, \mathbb{F}_2) \cong \Sigma_3$. So the vector space is low dimensional and the group is small. There will therefore be no difficulty in opening the modern invariant theorist's standard tool box (transfer, Chern classes, Steenrod operations, etc.) and constructing lots of invariants. The depth (sic!) of the problem lies in the fact that we have no a priori useful upper bound on the complexity of the problem: Since $\mathbb{F}_2$ has characteristic 2, and $2 \mid |\mathrm{GL}(2, \mathbb{F}_2)|$ we are in the modular case. Noether's bound does not apply, and the degree bounds of [6] or [4] §3 are far too large even in this small example to be of practical use. So we have no a priori acceptable *stopping condition*.

There are smaller degree bounds than those just mentioned, such as for example Broer's Bound (see e.g., [9] Corollary 5.5.6), but these usually require additional structural information about the invariants. To apply Broer's Bound one would need to know that $\mathbb{F}_2[\mathrm{Mat}_{\mathbb{F}_2}(2, 2)]^{\mathrm{GL}(2, \mathbb{F}_2)}$ is Cohen–Macaulay. Since $\dim(\mathrm{Mat}_{\mathbb{F}_2}(2, 2)) = 4$ the results of [10] do not apply[5] and one needs some other argument if the goal is to show $\mathbb{F}_2[\mathrm{Mat}_{\mathbb{F}_2}(2, 2)]^{\mathrm{GL}(2, \mathbb{F}_2)}$ is Cohen–Macaulay.

Our strategy will be **not** to begin with computation, but instead to first show that $\mathbb{F}_2[\mathrm{Mat}_{\mathbb{F}_2}(2, 2)]^{\mathrm{GL}(2, \mathbb{F}_2)}$ is Cohen–Macaulay. In fact we will show it is a hypersurface algebra, i.e., it is generated by five elements. On the way to proving this structural result we find a system of parameters for $\mathbb{F}_2[\mathrm{Mat}_{\mathbb{F}_2}(2, 2)]^{\mathrm{GL}(2, \mathbb{F}_2)}$ from which Broer's Bound tells us that this algebra can be generated by forms of degree at most four. Finally we write down five generators and one relation that determine it. As aids in accomplishing this we determine the structure of $\mathrm{Mat}_{\mathbb{F}_2}(2, 2)$ as both a $\mathrm{GL}(2, \mathbb{F}_2)$-set and linear representation.

The various tasks are divided into sections as follows.

§1 Counting the Orbits of $\mathrm{Mat}_{\mathbb{F}_2}(2, 2)$
§2 The Orbit and Linear Structure of $\mathrm{Mat}_{\mathbb{F}_2}(2, 2)$
§3 The Invariant Algebra $\mathbb{F}_2[\mathrm{Mat}_{\mathbb{F}_2}(2, 2)]^{\mathrm{GL}(2, \mathbb{F}_2)}$
§4 Separating Orbits by Invariants

The invariant theory problem considered here is one of a family of similar problems in more variables. The present manuscript serves as a model for the computations of [14] §4-6 where we take up the invariants $\mathbb{F}_2[\mathrm{Mat}_{\mathbb{F}_2}(3, 3)]^{\mathrm{GL}(2, \mathbb{F}_2)}$ which are considerably more complicated. We would like to thank David Benson and Peter Webb for several critical comments on a preliminary version of this manuscript.

[3] The bilinear form φ is defined for any standardly graded Poincaré duality algebra of formal dimension three, but need not determine that algebra up to isomorphism (see e.g., [13]).

[4] For the case of odd characteristics the proof has been simplified in [12] but the tricks used there do not apply in characteristic two at all. In particular, the splitting derived from the transfer does not exist in characteristic two.

[5] See e.g. [3] for an example of a ring of invariants $\mathbb{F}_2[z_1, z_2, z_3, z_4]^G$ that is not Cohen–Macaulay.

§1. Counting the Orbits of $\mathrm{Mat}_{\mathbb{F}_2}(2,\,2)$

There are only 16 elements in $\mathrm{Mat}_{\mathbb{F}_2}(2,\,2)$ so of course one could determine the orbit structure directly by hand. For the sake of completeness however we first reproduce the relevant computation from [8] Section I.6 that shows there are six orbits. This also allows us to develop a number of formulae that will be of use in further sections.

If G is a finite group and X is a finite G-set, then the Cauchy–Frobenius Lemma says[6]

$$(\divideontimes) \qquad |X/G| = \frac{1}{|G|}\sum_{g\in G}|X^g|,$$

where X/G is the orbit space, X^g the fixed point set of $g \in G$, and $|\text{–}|$ denotes the cardinality of the set –. Since conjugate elements of G have the same number of fixed points we may avoid duplicate computations and sum over representatives $g_1, \ldots, g_m$ for the conjugacy classes weighted by their cardninality. The following table supplies the needed information about conjugacy classes for $\mathrm{GL}(2,\,\mathbb{F}_2) \cong \Sigma_3$.

class	χ_1	χ_2	χ_3
matrix representative	$\mathbf{I} = \begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix}$	$\mathbf{S} = \begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix}$	$\mathbf{T} = \begin{bmatrix}1 & 1\\ 1 & 0\end{bmatrix}$
order	1	2	3
cardinality	1	3	2

TABLE 1.1: Conjugacy Classes of $\mathrm{GL}(2,\,\mathbb{F}_2)$

Next we count the number of fixed points of the matrices $\mathbf{S}$ and $\mathbf{T}$ representing the conjugacy classes χ_2 and χ_3. One has (we write $*$ for the action of $\mathrm{GL}(2,\,\mathbb{F}_2)$ on $\mathrm{Mat}_{\mathbb{F}_2}(2,\,2)$ given by the **transpose action** which sends $(g,\,\mathbf{M}) \in \mathrm{GL}(2,\,\mathbb{F}_2)\times\mathrm{Mat}_{\mathbb{F}_2}(2,\,2)$ into $g\cdot\mathbf{M}\cdot g^{\mathrm{tr}}$)

$$(\maltese) \qquad \mathbf{S} * \begin{bmatrix}a & b\\ c & d\end{bmatrix} = \begin{bmatrix}d & c\\ b & a\end{bmatrix}$$

and

$$(\bigstar) \qquad \mathbf{T} * \begin{bmatrix}a & b\\ c & d\end{bmatrix} = \begin{bmatrix}a+b+c+d & a+c\\ a+b & a\end{bmatrix}.$$

From formula $(\maltese)$ one sees that $\mathbf{M}$ is fixed by $\mathbf{S}$ if and only if $a = d$ and $b = c$. This means the fixed point set of $\mathbf{S}$ consists of the four matrices

$$\begin{bmatrix}0 & 0\\ 0 & 0\end{bmatrix},\quad \begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix},\quad \begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix},\quad \begin{bmatrix}1 & 1\\ 1 & 1\end{bmatrix}.$$

Note that these span a 2-dimensional linear subspace with basis $\mathbf{I}$, $\mathbf{S}$ of $\mathrm{Mat}_{\mathbb{F}_2}(2,\,2)$.

[6] One way to verify the validity of this formula is to note that both sides are additive with respect to taking disjoint unions of G-sets. This allows one to reduce to the case of a transitive G-set $X = G/H$, $H \le G$. If one decomposes G into its H-cosets one sees that only the elements of the identity coset, viz., $1\cdot H$, have any fixed points on G/H. There are $|H|$ such elements and each one of them fixes X pointwise, so has $|G/H|$ fixed points. So the right hand side of the formula becomes $\frac{1}{|G|}\cdot|H|\cdot|G/H| = 1$ as it should.

Likewise formula $(\bigstar)$ shows that $\mathbf{M}$ is fixed by $\mathbf{T}$ if and only if

$$\begin{aligned} a &= a + b + c + d \\ b &= a + c \\ c &= a + b \\ d &= c, \end{aligned}$$

which reduces to the two conditions $a = d$ and $c = a + b$. This shows the forms fixed by $\mathbf{T}$ span a 2-dimensional subspace so there are four $\mathbf{T}$-fixed points.

Putting these facts into the Cauchy–Frobenius Formula $(\divideontimes)$ then yields

$$\begin{aligned} |\mathrm{Mat}_{\mathbb{F}_2}(2,\,2)/\mathrm{GL}(2,\,\mathbb{F}_2)| &= \frac{1}{6}\left[|\mathrm{Mat}_{\mathbb{F}_2}(2,\,2)| + 3\cdot|\mathrm{Mat}_{\mathbb{F}_2}(2,\,2)^{\mathbf{S}}| + 2\cdot|\mathrm{Mat}_{\mathbb{F}_2}(2,\,2)^{\mathbf{T}}|\right] \\ &= \frac{1}{6}[16 + 3\cdot 4 + 2\cdot 4] = \frac{36}{6} = 6. \end{aligned}$$

So there are six orbits. What are they?

§2. The Orbit and Linear Structure of $\mathrm{Mat}_{\mathbb{F}_2}(2,\,2)$

The formula $(\bigstar)$ shows that $\mathbf{T}$ fixes $\mathbf{S}$, and, since $\mathbf{S}$ is a symmetric involution $\mathbf{S} * \mathbf{S} = \mathbf{S}\cdot\mathbf{S}\cdot\mathbf{S} = \mathbf{S}$ so $\mathbf{S}$ is also fixed by $\mathbf{S}$. Since $\mathbf{T}$ and $\mathbf{S}$ generate $\mathrm{GL}(2,\,\mathbb{F}_2)$ it follows that $\mathbf{S}$ is a fixed point of the action of $\mathrm{GL}(2,\,\mathbb{F}_2)$ on $\mathrm{Mat}_{\mathbb{F}_2}(2,\,2)$.

Next note that the action of $\mathrm{GL}(2,\,\mathbb{F}_2)$ on $\mathrm{Mat}_{\mathbb{F}_2}(2,\,2)$ preserves the determinant and therefore $\mathrm{GL}(2,\,\mathbb{F}_2) \subset \mathrm{Mat}_{\mathbb{F}_2}(2,\,2)$ is a $\mathrm{GL}(2,\,\mathbb{F}_2)$-invariant subset. The subgroup $\langle\mathbf{T}\rangle$ of $\mathrm{GL}(2,\,\mathbb{F}_2)$ generated by $\mathbf{T} \in \mathrm{GL}(2,\,\mathbb{F}_2)$ is normal, and since $\mathbf{S}^{\mathrm{tr}} = \mathbf{S}^{-1} = \mathbf{S}$ one obtains $\mathbf{S} * \mathbf{T} = \mathbf{S}\cdot\mathbf{T}\cdot\mathbf{S}^{\mathrm{tr}} = \mathbf{S}\cdot\mathbf{T}\cdot\mathbf{S} = \mathbf{T}^2 \in \langle\mathbf{T}\rangle$, so this subgroup, which consists of the three matrices

$$\mathbf{I} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad \mathbf{T} = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}, \quad \mathbf{T}^2 = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix},$$

is in fact an $\mathbf{S}$-invariant subset. Since $\mathbf{S}$ and $\mathbf{T}$ generate $\mathrm{GL}(2,\,\mathbb{F}_2)$ we conclude this subgroup is also a $\mathrm{GL}(2,\,\mathbb{F}_2)$-orbit. Note that $\mathbf{T}$ cyclically permutes the elements of this orbit, and $\mathbf{S}$ fixes $\mathbf{I}$ and exchanges $\mathbf{T}$ with $\mathbf{T}^2$.

The two remaining elements of $\mathrm{GL}(2,\,\mathbb{F}_2)$, namely

$$\mathbf{S}' = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}, \quad \mathbf{S}'' = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$$

are interchanged by the action of $\mathbf{S}$ (use formula (Θ)) and fixed by $\mathbf{T}$ (use formula $(\bigstar)$) so they too form an orbit. To summarize, $\mathrm{GL}(2,\,\mathbb{F}_2) \subset \mathrm{Mat}_{\mathbb{F}_2}(2,\,2)$ is a $\mathrm{GL}(2,\,\mathbb{F}_2)$-invariant subset and has the following orbit structure.

$$\mathrm{GL}(2,\,\mathbb{F}_2) = \{\mathbf{I},\,\mathbf{T},\,\mathbf{T}^2\} \sqcup \{\mathbf{S}\} \sqcup \{\mathbf{S}',\,\mathbf{S}''\}$$

Together with the second fixed point $\mathbf{Z}$ (the zero matrix) we have found four of the six orbits of $\mathrm{GL}(2,\,\mathbb{F}_2)$ on $\mathrm{Mat}_{\mathbb{F}_2}(2,\,2)$.

There are nine remaining matrices in $\mathrm{Mat}_{\mathbb{F}_2}(2,\,2)$ (the nonzero singular matrices) and they must divide between the remaining two orbits. The only way this can happen (Lagrange's Theorem tells us the number of elements in an orbit must be a divisor of 6) is for one of the remaining orbits to have cardinality three and the other six.

In addition to preserving the determinant the action of $\mathrm{GL}(2, \mathbb{F}_2)$ on $\mathrm{Mat}_{\mathbb{F}_2}(2, 2)$ preserves whether a matrix is symmetric or not. Among the eight symmetric matrices four are singular and four are nonsingular, viz.,

$$\text{singular: } \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix},$$
$$\text{nonsingular: } \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}.$$

We have already accounted for the zero matrix $\mathbf{Z}$ and a little matrix computation using the formulae (Φ) and $(\bigstar)$ shows that the remaining three symmetric singular matrices form a $\mathrm{GL}(2, \mathbb{F}_2)$-orbit. This completes the description of the decomposition of $\mathrm{Mat}_{\mathbb{F}_2}(2, 2)$ into $\mathrm{GL}(2, \mathbb{F}_2)$-orbits which we summarize in Table 2.1.

Orbit	Elements	Description	
#0	$\mathbf{Z} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$	trivial fixed point	fixed point set
#1	$\mathbf{S} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$	involutive fixed point	fixed point set
#2	$\mathbf{I} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \mathbf{T} = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}, \mathbf{T}^2 = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}$	A_3	
#3	$\mathbf{S}' = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}, \mathbf{S}'' = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$	nonfixed involutions	
#4	$\begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}$	symmetric, nonzero, singular	
#5	$\begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 \\ 1 & 1 \end{bmatrix}$	nonsymmetric, nonzero, singular	
	$\begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 0 & 1 \end{bmatrix}$	nonsymmetric, nonzero, singular	

TABLE 2.1**:** Orbits of $\mathrm{GL}(2, \mathbb{F}_2)$ on $\mathrm{Mat}_{\mathbb{F}_2}(2, 2)$

We next make use of the orbit structure of $\mathrm{Mat}_{\mathbb{F}_2}(2, 2)$ to determine its linear structure, i.e., its structure as a $\mathrm{GL}(2, \mathbb{F}_2)$-representation. First note that the three matrices

$$\mathbf{I} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad \mathbf{T} = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}, \quad \mathbf{T}^2 = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix},$$

forming orbit #2 are the nonzero vectors of the $\mathrm{GL}(2, \mathbb{F}_2)$-invariant 2-dimensional subspace $\mathcal{T}$ spanned by $\mathbf{T}$ and $\mathbf{T}^2$, since $\mathbf{I} + \mathbf{T} + \mathbf{T}^2 = \mathbf{Z}$. Likewise the two matrices

$$\mathbf{S}' = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}, \quad \mathbf{S}'' = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$$

span a $\mathrm{GL}(2, \mathbb{F}_2)$-invariant 2-dimensional subspace $\mathcal{S}$ consisting of the union of the orbits #0, #1, and #3, since $\mathbf{S} = \mathbf{S}' + \mathbf{S}''$. Since the subspaces $\mathcal{S}$ and $\mathcal{T}$ have just the zero matrix $\mathbf{Z}$ in common we have determined the linear structure of $\mathrm{Mat}_{\mathbb{F}_2}(2, 2)$ as stated in the following result.

PROPOSITION 2.1**:** *There is an isomorphism of representations* $\mathrm{Mat}_{\mathbb{F}_2}(2, 2) \cong \mathcal{T} \oplus \mathcal{S}$ *over* $\mathrm{GL}(2, \mathbb{F}_2)$ *where,* $\mathcal{T} = \mathrm{Span}_{\mathbb{F}_2}\{\mathbf{T}, \mathbf{T}^2\}$ *is isomorphic to the defining representation* $V = \mathbb{F}_2^2$ *of* $\mathrm{GL}(2, \mathbb{F}_2)$*, and* $\mathcal{S} = \mathrm{Span}_{\mathbb{F}_2}\{\mathbf{S}', \mathbf{S}''\}$ *is isomorphic to the pullback along the quotient map* $\mathrm{GL}(2, \mathbb{F}_2) \longrightarrow \mathbb{Z}/2$ *of the regular representation of* $\mathbb{Z}/2$*.*

PROOF: The structure of $\mathcal{T}$ and $\mathcal{S}$ is easily verified using the given bases. □

REMARK: As an alternative proof for Proposition 2.1 we note that in the group algebra $\mathbb{F}_2(\mathrm{GL}(2,\mathbb{F}_2))$ the elements $e = \mathbf{T} + \mathbf{T}^2$, $f = \mathbf{I} + \mathbf{T} + \mathbf{T}^2$ are primitive orthogonal idempotents and split the subspaces $\mathcal{T}$, $\mathcal{S}$ off of $\mathrm{Mat}_{\mathbb{F}_2}(2,2)$: To wit $\mathcal{S} = \mathrm{Im}(f)$.

We conclude this section with the following observation which is due to Dave Benson and replaces a much more complicated argument of our own. The automorphism α of $\mathrm{GL}(2,\mathbb{F}_2)$ defined by sending an element $g \in \mathrm{GL}(2,\mathbb{F}_2)$ to $(g^{-1})^{\mathrm{tr}}$ is by a low dimensional accident an inner automorphism. It is given by conjugation with the matrix $\mathbf{S} \in \mathrm{GL}(2,\mathbb{F}_2)$. This automorphism (which usually is outer) exchanges the action of $\mathrm{GL}(2,\mathbb{F}_2)$ on $\mathrm{Mat}_{\mathbb{F}_2}(2,2)$ defined by

$$(g, \mathbf{M}) \rightsquigarrow g \cdot \mathbf{M} \cdot g^{-1} \quad \text{for} \quad g \in \mathrm{GL}(2,\mathbb{F}_2), \quad \mathbf{M} \in \mathrm{Mat}_{\mathbb{F}_2}(2,2),$$

with the action studied here. It therefore follows that up to change of bases these actions have the same orbit, linear, and invariant structures.

§3. The Invariant Algebra $\mathbb{F}_2[\mathrm{Mat}_{\mathbb{F}_2}(2,2)]^{\mathrm{GL}(2,\mathbb{F}_2)}$

As noted in the introduction, since $\mathrm{Mat}_{\mathbb{F}_2}(2,2)$ is a small representation,[7] but the representation is modular, the major stumbling block to computing the algebra of invariants $\mathbb{F}_2[\mathrm{Mat}_{\mathbb{F}_2}(2,2)]^{\mathrm{GL}(2,\mathbb{F}_2)}$ is not to find invariants, but to know we have found enough of them. Therefore we begin with results that place an upper bound on the number of algebra generators as well as their degrees.

PROPOSITION 3.1: *The algebra of invariants* $\mathbb{F}_2[\mathrm{Mat}_{\mathbb{F}_2}(2,2)]^{\mathrm{GL}(2,\mathbb{F}_2)}$ *is Cohen–Macaulay. It contains a system of parameters with degrees* 1, 2, 2, 3 *and hence is generated as an algebra by forms of degree at most* 4.

PROOF: We make use of Proposition 2.1 to replace $\mathrm{Mat}_{\mathbb{F}_2}(2,2)$ with the direct sum $\mathcal{T} \oplus \mathcal{S}$ in the computation. To verify that $\mathbb{F}_2[\mathrm{Mat}_{\mathbb{F}_2}(2,2)]^{\mathrm{GL}(2,\mathbb{F}_2)}$ is Cohen–Macaulay we apply [11] Proposition 8.3.1 and check instead that the algebra of invariants of a 2-Sylow subgroup $\mathbb{Z}/2 = \mathrm{Syl}_2(\mathrm{GL}(2,\mathbb{F}_2)) < \mathrm{GL}(2,\mathbb{F}_2)$, viz., $\mathbb{F}_2[\mathcal{T} \oplus \mathcal{S}]^{\mathrm{Syl}_2(\mathrm{GL}(2,\mathbb{F}_2))}$ is Cohen–Macaulay. Proposition 2.1 shows that as $\mathbb{Z}/2$-representations both $\mathcal{T}$ and $\mathcal{S}$ are the regular representation of $\mathbb{Z}/2$ over $\mathbb{F}_2$. The corresponding algebra of invariants[8] is well known (see e.g., [11] §1.5 Example 2, §4.3 Example 4); it is a hypersurface algebra and hence Cohen–Macaulay.

Also from the descriptions of $\mathcal{T}$ and $\mathcal{S}$ in Proposition 2.1 one sees

$$\mathbb{F}_2[\mathcal{T}]^{\mathrm{GL}(2,\mathbb{F}_2)} \cong \mathbb{F}_2[\mathbf{d}_{2,0}, \mathbf{d}_{2,1}],$$
$$\mathbb{F}_2[\mathcal{S}]^{\mathrm{GL}(2,\mathbb{F}_2)} \cong \mathbb{F}_2[e_1, e_2],$$

where, $\mathbf{d}_{2,1} = u^2 + uv + v^2$ and $\mathbf{d}_{2,0} = u^2v + uv^2$ are the Dickson polynomials in the linear forms u and v which are dual to the elements $\mathbf{T}$ and $\mathbf{T}^2$ of $\mathcal{T}$, and e_1 and e_2 are the elementary symmetric polynomials in the linear forms z', z'' which are dual to $\mathbf{S}'$, $\mathbf{S}'' \in \mathcal{S}$. Since $\mathbb{F}_2[\mathcal{T}]^{\mathrm{GL}(2,\mathbb{F}_2)} \otimes \mathbb{F}_2[\mathcal{S}]^{\mathrm{GL}(2,\mathbb{F}_2)} \subset \mathbb{F}_2[\mathcal{T} \oplus \mathcal{S}]^{\mathrm{GL}(2,\mathbb{F}_2)} = \mathbb{F}_2[\mathrm{Mat}_{\mathbb{F}_2}(2,2)]^{\mathrm{GL}(2,\mathbb{F}_2)}$ is a finite extension it follows that e_1, e_2, $\mathbf{d}_{2,1}$, $\mathbf{d}_{2,0} \in \mathbb{F}_2[\mathrm{Mat}_{\mathbb{F}_2}(2,2)]^{\mathrm{GL}(2,\mathbb{F}_2)}$ form a system of parameters. The final conclusion then follows from Broer's Bound (see e.g., [9] Corollary 5.5.6). □

---

[7] It is well described at this point: both the orbit and linear structure are known.

[8] This is the algebra of vector invariants $\mathbb{F}_2\begin{bmatrix} x_1 & y_1 \\ x_2 & y_2 \end{bmatrix}^{\mathbb{Z}/2}$ where $\mathbb{Z}/2$ acts by simultaneous interchange of x_i with y_i for $i = 1, 2$.

COROLLARY 3.2: *The algebra of invariants* $\mathbb{F}_2[\mathrm{Mat}_{\mathbb{F}_2}(2,\,2)]^{\mathrm{GL}(2,\,\mathbb{F}_2)}$ *is a hypersurface algebra generated by* $e_1,\ e_2,\ \mathbf{d}_{2,1},\ \mathbf{d}_{2,0}$ *and a form* $f \in \mathbb{F}_2[\mathrm{Mat}_{\mathbb{F}_2}(2,\,2)]^{\mathrm{GL}(2,\,\mathbb{F}_2)}$ *of minimal degree not contained in the subalgebra* $\mathbb{F}_2[e_1,\ e_2,\ \mathbf{d}_{2,1},\ \mathbf{d}_{2,0}]$.

PROOF: By Proposition 3.1 the forms $e_1,\ e_2,\ \mathbf{d}_{2,1},\ \mathbf{d}_{2,0}$ are a system of parameters for the invariant algebra $\mathbb{F}_2[\mathrm{Mat}_{\mathbb{F}_2}(2,\,2)]^{\mathrm{GL}(2,\,\mathbb{F}_2)}$. Since the product of the degrees of these forms is $1\cdot 2\cdot 3\cdot 2 = 12 = 2\cdot|\mathrm{GL}(2,\,\mathbb{F}_2)|$ the result follows from [12] Proposition 2.3. □

The following Lemma determines the degree of the one relation from the degree of the missing generator in a case such as that of Corollary 3.2.

LEMMA 3.3: *Let* $\rho : G \hookrightarrow \mathrm{GL}(n,\,\mathbb{F})$ *be a representation of a finite group over the field* $\mathbb{F}$. *Suppose* $\mathbb{F}[V]^G$ *is Cohen–Macaulay and that there is a system of parameters* $f_1,\ \ldots,\ f_n \in \mathbb{F}[V]^G$ *satisfying*

$$\prod_{i=1}^{n}\deg(f_i) = 2\cdot|G|.$$

Then there is an invariant form f *and a form* $h \in \mathbb{F}_2[V]$ *such that* $\deg(h) = 2\cdot\deg(f)$ *with* $\mathbb{F}[V]^G = \mathbb{F}[f_1,\ \ldots,\ f_n,\ f]/(h)$.

PROOF: By [12] Proposition 2.3 $\mathbb{F}[V]^G$ is a hypersurface algebra so we may find $f \in \mathbb{F}[V]^G$ and $h \in \mathbb{F}[V]$ such that $\mathbb{F}[V]^G = \mathbb{F}[f_1,\ \ldots,\ f_n,\ f]/(h)$. Let the degrees of f and h be d and e. The Poincaré series of $\mathbb{F}[V]^G$ is

$$P(\mathbb{F}[V]^G,\ t) = \frac{1-t^e}{1-t^d}\prod_{i=1}^{n}\frac{1}{1-t^{d_i}},$$

where $d_i = \deg(f_i)$ for $i = 1,\ \ldots,\ n$. Multiply this expression by $(1-t)^n$ (to remove the pole of order n at $t = 1$) and evaluate the resulting function at $t = 1$. From the Degree Theorem (see e.g., [11] Theorem 5.5.6) we obtain

$$\begin{aligned}\frac{1}{|G|} &= \Big[(1-t)^n P(\mathbb{F}[V]^G,\ t)\Big]\Big|_{t=1}\\ &= \left[\frac{1+t+\cdots+t^{e-1}}{1+t+\cdots+t^{d-1}}\prod_{i=1}^{n}\frac{1}{1+t+\cdots+t^{d_i-1}}\right]\Big|_{t=1} = \frac{e}{d}\cdot\frac{1}{d_1\cdots d_n} = \frac{e}{d}\frac{1}{2\cdot|G|}\end{aligned}$$

whence $\frac{e}{d} = 2$ and the result follows. □

Putting these results together with a bit of computation leads to the final form for the invariants.

PROPOSITION 3.4: *Let* $\mathrm{GL}(2,\,\mathbb{F}_2)$ *act on* $\mathrm{Mat}_{\mathbb{F}_2}(2,\,2)$ *by*

$$g * \mathbf{M} = g\mathbf{M}g^{\mathrm{tr}} \quad \text{for} \quad g \in \mathrm{GL}(2,\,\mathbb{F}_2),\ \mathbf{M} \in \mathrm{Mat}_{\mathbb{F}_2}(2,\,2).$$

Then the algebra of invariants is given by $\mathbb{F}_2[\mathrm{Mat}_{\mathbb{F}_2}(2,\,2)]^{\mathrm{GL}(2,\,\mathbb{F}_2)} = \mathbb{F}_2[e_1,\ e_2,\ \mathbf{d}_{2,1},\ \mathbf{d}_{2,0},\ f]/(h)$ *where* f *is the quartic form (the notation being as in Proposition 3.1)*

$$f = z'u^2v + z''uv^2,$$

and the relation h *has degree eight.*

PROOF: We know $\mathrm{Mat}_{\mathbb{F}_2}(2,\,2)] \cong \mathcal{T} \oplus \mathcal{S}$ as $\mathrm{GL}(2,\,\mathbb{F}_2)$-representations by Proposition 2.1. Let $A_3 \lhd \mathrm{GL}(2,\,\mathbb{F}_2)$ be the alternating subgroup, so $\mathbb{F}_2[\mathrm{Mat}_{\mathbb{F}_2}(2,\,2)]^{\mathrm{GL}(2,\,\mathbb{F}_2)} \cong \left(\mathbb{F}_2[\mathcal{T} \oplus \mathcal{S}]^{A_3}\right)^{\mathbb{Z}/2}$. Restricted to $A_3 \lhd \mathrm{GL}(2,\,\mathbb{F}_2)$ the representation over $\mathcal{S}$ is trivial and $\mathcal{T}$ is the quotient of the regular representation over $\mathbb{F}_2$ of A_3 by the fixed point set. From [11] Proposition 1.3.5 it follows that $\mathbb{F}_2[\mathcal{T}]^{A_3}$ is generated by the elementary symmetric polynomials in u and v together with ∇' or ∇'' where $\nabla' = u^2v$ and $\nabla'' = uv^2$. The action of $\mathbb{Z}/2$ on $\mathbb{F}_2[\mathcal{T}]^{A_3}$ exchanges the elements ∇' and ∇''. Likewise the action of $\mathbb{Z}/2$ on $\mathbb{F}_2[\mathcal{S}]$ exchanges the linear forms z' and z''. Hence the quartic form $f = z'\nabla' + z''\nabla''$ belongs to $\left(\mathbb{F}_2[\mathcal{T} \oplus \mathcal{S}]^{A_3}\right)^{\mathbb{Z}/2}$ but not to the subalgebra generated by e_1, e_2, $\mathbf{d}_{2,1}$, $\mathbf{d}_{2,0}$ completing the proof. □

§4. Separating Orbits by Invariants

Of the five algebra generators for $\mathbb{F}_2[\mathrm{Mat}_{\mathbb{F}_2}(2,\,2)]^{\mathrm{GL}(2,\,\mathbb{F}_2)}$ found in § 3 only three are needed to separate the orbits of $\mathrm{GL}(2,\,\mathbb{F}_2)$ on $\mathrm{Mat}_{\mathbb{F}_2}(2,\,2)$. To see this we evaluate all five of the forms in Proposition 3.4 on representatives for the orbits as listed in Table 2.1. The result is Table 4.1. Since the rows of the 3×6 matrix formed from the first three columns are distinct, one sees from Table 4.1 that the three forms e_1, e_2, and $\mathbf{d}_{2,1}$ separate the orbits.

orbit # and representative		e_1	e_2	$\mathbf{d}_{2,1}$	$\mathbf{d}_{2,0}$	f
#0	$\begin{bmatrix}0&0\\0&0\end{bmatrix}$	0	0	0	0	0
#1	$\begin{bmatrix}0&1\\1&0\end{bmatrix}$	0	1	0	0	0
#2	$\begin{bmatrix}1&0\\0&1\end{bmatrix}$	0	0	1	0	0
#3	$\begin{bmatrix}1&1\\0&1\end{bmatrix}$	1	0	0	0	0
#4	$\begin{bmatrix}1&0\\0&0\end{bmatrix}$	0	1	1	0	0
#5	$\begin{bmatrix}0&1\\0&0\end{bmatrix}$	1	0	1	0	1

TABLE 4.1**:** Values of Invariants on Orbits

Using this table one can determine the orbit of a matrix

$$\mathbf{M} = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{Mat}_{\mathbb{F}_2}(2,\,2)$$

by evaluating the functions

$$\begin{aligned} e_1(\mathbf{M}) &= b + c \\ e_2(\mathbf{M}) &= (a + c + d)(a + b + d) \\ \mathbf{d}_{2,1}(\mathbf{M}) &= (a + d)^2 + (a + b + c)(b + c + d) \end{aligned}$$

on the matrix. Since

$$\det(\mathbf{M}) = \mathbf{d}_{2,1} + e_2 + e_1^2 \in \mathbb{F}_2[\mathrm{Mat}_{\mathbb{F}_2}(2,\,2)]^{\mathrm{GL}(2,\,\mathbb{F}_2)}$$

one could equally well use the three forms e_1, e_2, and det to distinguish orbits.

References

[1] E. Artin, *Geometric Algebra,* Interscience Publ. Inc., New York, 1957.

[2] N. Anghel, *$SL_2(k)$-Polynomial Invariance,* Rev. Roumaine de Math. Pures et Appl. 43, (1998), 17–46.

[3] M.-J. Bertin, *Anneaux d'invariants d'anneaux de polynômes en caractéristique p,* C. R. Acad. Sci. Paris t. 264 (Série A) (1967), 653–656.

[4] H. Derksen and G. Kemper, *Computational Invariant Theory,* Encyclopedia of Mathematical Sciences 130, Springer-Verlag, Heidelberg, Berlin, 2000..

[5] J.W.P. Hirschfeld, *Projective Geometries over Finite Fields,* Oxford Mathematical Monographs, Oxford Univ. Press, Oxford, UK, 1979.

[6] D. B. Karagueuzian and P. Symonds, *The Module Structure of a Group Action on a Polynomial Ring : the general case,* preprint.

[7] F. S. Macaulay, *The Algebraic Theory of Modular Systems,* Camb. Math. Lib., Camb. Camb. Univ. Press, Cambridge 1916 (reissued with an introduction by P. Roberts 1994).

[8] D. M. Meyer and L. Smith, *Poincaré Duality Algebras, Macaulay's Dual Systems, and Steenrod Operations,* Cambridge University Press, Cambridge, UK, Tracts in Mathematics 167, 2005.

[9] M. D. Neusel and L. Smith, *Invariant Theory of Finite Groups,* Surveys and Monographs 94 American Mathematical Society, Providence RI, 2002.

[10] L. Smith, *Some Rings of Invariants that are Cohen-Macaulay,* Canad. Math. Bull. 39 (1996), 238 – 240.

[11] L. Smith, *Polynomial Invariants of Finite Groups,* A.K. Peters, Ltd., Wellesley, MA, 1995, second printing 1997.

[12] L. Smith, *Invariants of 2×2 Matrices over Finite Fields,* Finite Fields and their Applications 8 (2002), 504–510.

[13] L. Smith and R. E. Stong, *Poincaré Duality Algebras Modulo Two,* Preprint, 2005.

[14] L. Smith and R. E. Stong, *Invariants of Ternary Bilinear Forms Modulo Two,* Preprint, 2005.

Larry Smith
AG-Invariantentheorie
Mittelweg 3
D 37133 Friedland
Federal Republic of Germany
larry_smith@GMX.net

R. E. Stong
Department of Mathemtics
University of Virginia
Charlottesville, VA 22904-4137
USA