ELSEVIER Discrete Mathematics 185 (1998) 51–61

DISCRETE MATHEMATICS

Matrix representatives for three-dimensional bilinear forms over finite fields

B. Corbas*, G.D. Williams

Department of Mathematics, University of Reading, Whiteknights, P.O. Box 220, Reading RG6 6AF, UK

Received 15 November 1996; received in revised form 30 June 1997; accepted 21 July 1997

Abstract

The purpose of this paper is to obtain a complete set of matrix representatives for the bilinear forms on a three-dimensional vector space over a finite field of any characteristic, without assuming that the form is symmetric or non-degenerate.

1. Introduction

Let $\mathscr{B}$ be a bilinear form on a finite-dimensional vector space V over a field K. As usual we define the matrix $\boldsymbol{A}=(a_{ij})$ of $\mathscr{B}$ with respect to an ordered basis $(a_1,a_2,\ldots,a_n)$ of V by $a_{ij}=\mathscr{B}(a_i,a_j)$. If $\boldsymbol{B}$ is the matrix of $\mathscr{B}$ with respect to a new basis and $\boldsymbol{X}$ is the transition matrix then $\boldsymbol{B}=\boldsymbol{X}^{\mathrm{T}}\boldsymbol{A}\boldsymbol{X}$ and $\boldsymbol{A}$, $\boldsymbol{B}$ are thus *congruent*. If $\mathscr{B}$ is symmetric or alternating, then explicit normal forms for the congruence classes over various fields are well known, but this is not the case for general asymmetric forms. Recently, Bremser [1] has obtained representatives in the case $n=2$, K finite and $\mathscr{B}$ non-degenerate.

In this paper we derive such normal forms when K is finite and $n=3$, with no restriction on $\mathscr{B}$ or the characteristic of the field. We take an elementary approach which does not require one first to count the number of classes as in [1]. The numbers we obtain, which differ between the odd and even characteristic cases, are easily checked to be in agreement with the counting formula of Waterhouse [5]. We remark finally that we could also deduce our results from the general structure theory of Riehm [3], Scharlau [4] and others, but that is not our purpose here.

In the following, we shall say that $\mathscr{B}$ is *split* if $V=U\oplus W$ with $\dim U=1$ and $\mathscr{B}(x,y)=\mathscr{B}(y,x)=0$ for all $x\in U$, $y\in W$.

* Corresponding author. E-mail: smscorba@reading.ac.uk.

PII S0012-365X(97)00183-0

2. The non-split case

If $a \in V$ let $R_a = \{x \in V \mid \mathscr{B}(a,x) = 0\}$ and $L_a = \{x \in V \mid \mathscr{B}(x,a) = 0\}$. Notice that, if $a \neq 0$, R_a and L_a are the kernels of the non-zero linear maps $\mathscr{B}(a,\quad): V \to K$ and $\mathscr{B}(\quad,a): V \to K$, respectively. Hence, $\dim R_a$, $\dim L_a \geqslant 2$ and we have the following lemma.

Lemma 1. *$\mathscr{B}$ is split if and only if (exactly) one of the following is true*:

$$\exists a \in V - \{0\}\colon R_a = L_a = V, \tag{1}$$

$$\exists a \in V\colon a \notin R_a = L_a (\neq V). \tag{2}$$

Proof. If $\mathscr{B}$ is split then $U = Ka$ for some non-zero $a \in V$ and $W \subset L_a$, $W \subset R_a$. If $R_a = V$ then $\mathscr{B}(a,a) = 0$ which implies $a \in L_a$ and hence $L_a = V$; similarly, $L_a = V$ implies $R_a = V$. If $L_a, R_a \neq V$ then $L_a = R_a = W$ and $a \notin L_a$. Conversely, if (1) is satisfied we take $U = Ka$ and W any complementary subspace; if (2) is satisfied we take $U = Ka$ and $W = L_a$. $\square$

Lemma 2. *If $\mathscr{B}$ is not antisymmetric then there exists a basis of V with respect to which the matrix of $\mathscr{B}$ has the form*

$$A = \begin{pmatrix} \mu & 0 & 0 \\ 0 & \nu & t \\ \alpha & \beta & \lambda \end{pmatrix}, \tag{3}$$

with $\mu \neq 0$.

Proof. Since $\mathscr{B}$ is not antisymmetric, there exists an $a \in V$ with $\mathscr{B}(a,a) = \mu \neq 0$; hence, $\dim R_a = \dim L_a = 2$. But then, $\dim V = 3$ implies $\dim(R_a \cap L_a) \geqslant 1$ and we can select a basis (a,b,c) for V with $b \in R_a \cap L_a$ and $c \in R_a$. With respect to this basis the matrix of $\mathscr{B}$ has the required form. $\square$

Lemma 3. *Assume that with respect to some basis of V, the matrix of $\mathscr{B}$ has the form* (3) (*we do not exclude $\mu = 0$*). *Then $\mathscr{B}$ is split if and only if one of the following is true*:

$$\alpha = 0 \quad or \quad \nu = t = 0 \quad or \quad \left(\frac{\beta - t}{\alpha}\right)^2 \mu + \nu \neq 0.$$

Proof. If $a \in V$, we have $R_a = \{x \in V \mid aAx^{\mathrm{T}} = 0\}$, $L_a = \{x \in V \mid aA^{\mathrm{T}}x^{\mathrm{T}} = 0\}$, having identified V with K^3. Hence, if $a \neq 0$,

$$R_a = L_a \Leftrightarrow \exists \xi \in K^*\colon aA^{\mathrm{T}} = \xi aA.$$

Then by Lemma 1, if $\mathscr{B}$ splits there exists a non-zero $a \in V$ and $\xi \in K^*$ such that $aA^{\mathrm{T}} = \xi aA$. In particular, $\xi aAa^{\mathrm{T}} = aA^{\mathrm{T}}a^{\mathrm{T}} = aAa^{\mathrm{T}}$. Then with the conclusions and notations of Lemma 1, if $a \notin R_a = L_a$ we have $aAa^{\mathrm{T}} \neq 0$ and so $\xi = 1$. On the other hand, if $a \in R_a = L_a = V$, we have $aA^{\mathrm{T}} = aA = 0$ and so we can take $\xi = 1$ in any case. So if $\mathscr{B}$ splits there exists a non-zero $a \in V$ with $aA^{\mathrm{T}} = aA$ and hence $a(A^{\mathrm{T}} - A) = 0$ which implies $(A - A^{\mathrm{T}})a^{\mathrm{T}} = 0$. So suppose $\mathscr{B}$ splits and $\alpha \neq 0$. We have

$$A - A^{\mathrm{T}} = \begin{pmatrix} 0 & 0 & -\alpha \\ 0 & 0 & t-\beta \\ \alpha & \beta - t & 0 \end{pmatrix}$$

and its reduction to echelon form is

$$\begin{pmatrix} 1 & (\beta - t)\alpha^{-1} & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}.$$

Since a is a solution of the homogeneous system $(A - A^{\mathrm{T}})a^{\mathrm{T}} = 0$, it must be a scalar multiple of $((t - \beta)\alpha^{-1}, 1, 0)$. If we are in part (1) of Lemma 1 then $((t - \beta)\alpha^{-1}, 1, 0)A = 0$ and, hence, $((t - \beta)\alpha^{-1}\mu, v, t) = (0, 0, 0)$ which implies $v = t = 0$. If we are in part (2) of Lemma 1 then we must have $\mathscr{B}(a, a) = aAa^{\mathrm{T}} \neq 0$; i.e. $((\beta - t)/\alpha)^2\mu + v \neq 0$.

The converse part of the lemma is clear. If $v = t = \beta = 0$ then manifestly the form splits; if $v = t = 0$ but $\beta \neq 0$, we can subtract a suitable multiple of the second row and column from the first row and column, respectively, to recognize that the form is split. On the other hand, if $((\beta - t)/\alpha)^2\mu + v \neq 0$ we can take $a = ((t - \beta)\alpha^{-1}, 1, 0)$ which satisfies the conditions of part (2) of Lemma 1. □

Lemma 4. *$\mathscr{B}$ is not split if and only if with respect to a suitable basis of V its matrix has one of the following forms*:

$$\begin{pmatrix} \mu & 0 & 0 \\ 0 & 0 & 1 \\ \alpha & 1 & \lambda \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 & 0 \\ 0 & v & 0 \\ \alpha & \alpha\sqrt{-v} & \lambda \end{pmatrix} \quad \text{with} \begin{cases} \alpha \in K^*, \\ \mu, v \in \{1, \varepsilon\}, \\ \lambda \in \{0, 1, \varepsilon\}, \end{cases} \tag{4}$$

where ε is an arbitrary but fixed non-square in K (if of course its characteristic is not two).

Proof. By Lemma 3, the above matrices represent forms which are non-split. If now, the given form is not split then it is not antisymmetric and so by Lemma 2 its matrix can be put into form (3) with $\mu \neq 0$. Then by Lemma 3, $((\beta - t)/\alpha)^2\mu + v = 0$ and $\alpha \neq 0$.

Assume first that $v \neq 0$; then by adding to the third row and column a suitable multiple of the second row and column, respectively, we can assume $t = 0$. The top 2×2 block in the diagonal of A is diagonal and non-singular and is, therefore, congruent to either

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad \text{or} \quad \begin{pmatrix} 1 & 0 \\ 0 & \varepsilon \end{pmatrix}.$$

We can multiply λ by any square s^2 of K by multiplying the third row and column by s and so we can assume that $\lambda \in \{0, 1, \varepsilon\}$. Hence, with respect to a suitable basis, the matrix of the bilinear form is

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & v & 0 \\ \alpha & \beta & \lambda \end{pmatrix} \quad \text{with} \quad \begin{cases} v \in \{1, \varepsilon\}, \quad \alpha \in K^*, \\ \lambda \in \{0, 1, \varepsilon\}, \\ (\beta\alpha^{-1})^2 + v = 0. \end{cases}$$

Hence, $\beta = \pm\alpha\sqrt{-v}$ and we can assume $\beta = \alpha\sqrt{-v}$ since we can multiply by -1 the second row and column. Notice that if $\operatorname{char} K \neq 2$ exactly one of the two possibilities $v = 1$ and $v = \varepsilon$ makes sense, depending on whether -1 is a square or not in K; and if $\operatorname{char} K = 2$ there is only the possibility $v = 1$ anyhow.

It remains to examine the case $v = 0$. In this case $((t - \beta)\alpha^{-1})^2\mu = 0$ and since $\mu \neq 0$ we have $t = \beta$; and $\beta \neq 0$ since the form is not split. Then we can multiply the second row and column by β^{-1} and the first row and column by a suitable element of K^* to obtain the required form. □

Proposition 1. *If* $\operatorname{char} K \neq 2$ *then there are exactly three equivalence classes of non-split bilinear forms and they are represented by the following matrices*:

$$\begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix}, \quad \begin{pmatrix} \varepsilon & 0 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix}. \tag{5}$$

Proof. From Lemma 4, we know that the classes in question are represented by the matrices (4). We have

$$\begin{pmatrix} \alpha & -\alpha/\sqrt{-v} & -1 \\ \alpha & -\alpha/\sqrt{-v} & 0 \\ 1/(2\alpha) & 1/(2\alpha\sqrt{-v}) & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & v & 0 \\ \alpha & \alpha\sqrt{-v} & \lambda \end{pmatrix}$$
$$\times \begin{pmatrix} \alpha & \alpha & 1/(2\alpha) \\ -\alpha/\sqrt{-v} & -\alpha/\sqrt{-v} & 1/(2\alpha\sqrt{-v}) \\ -1 & 0 & 0 \end{pmatrix}$$
$$= \begin{pmatrix} \lambda & 0 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix}$$

and

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & \alpha & 0 \\ 0 & -\lambda/(2\alpha) & 1/\alpha \end{pmatrix} \begin{pmatrix} \mu & 0 & 0 \\ 0 & 0 & 1 \\ \alpha & 1 & \lambda \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & \alpha & -\lambda/(2\alpha) \\ 0 & 0 & 1/\alpha \end{pmatrix} = \begin{pmatrix} \mu & 0 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix}.$$

So the only possibilities are the classes represented by (5). These are not congruent to each other since their determinants are 0, -1 and $-\varepsilon$, respectively. □

Lemma 5. *Let α, β be distinct non-zero elements of a finite field K of characteristic 2. Then the irreducibility of $X^2 + \alpha X + 1$, $X^2 + \beta X + 1$ over K implies the reducibility of $X^2 + (\alpha\beta/(\alpha + \beta))X + 1$ over K.*

Proof. First, notice that the additive endomorphism $\varphi(x) = x^2 + x$ of K has kernel $\boldsymbol{F}_2$ and, hence, image of index 2 in K. But then $1/\alpha^2$, $1/\beta^2 \notin \operatorname{Im}\varphi$ implies $(1/\alpha^2)+(1/\beta^2) \in \operatorname{Im}\varphi$. On the other hand, $X^2 + X + \gamma$ is reducible over K if and only if $\gamma \in \operatorname{Im}\varphi$. So the irreducibility of $X^2 + X + 1/\alpha^2$ and $X^2 + X + 1/\beta^2$ implies the reducibility of $X^2 + X + ((\alpha + \beta)/(\alpha\beta))^2$. Now, the lemma follows from the observation that, over K, $X^2 + \alpha X + 1$ is reducible if and only if $X^2 + X + 1/a^2$ is. □

Proposition 2. *If* $\operatorname{char} K = 2$ *then there are three classes of inequivalent, non-split bilinear forms, represented by the following matrices*:

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 1 & 1 & 0 \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ \alpha & 1 & 1 \end{pmatrix},$$

where $X^2 + \alpha X + 1$ is an arbitrary but fixed irreducible polynomial of degree two over K.

Proof. It is immediate from Lemma 3 that these matrices represent forms which are not split.

Lemma 4 implies that the non-split forms are represented by the following matrices:

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ \alpha & 1 & \lambda \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ \alpha & \alpha & \lambda \end{pmatrix} \quad \text{with} \begin{cases} \alpha \in K^*, \\ \lambda \in \{0, 1\}. \end{cases} \tag{6}$$

Notice, however, that

$$\begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & \alpha & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ \alpha & 1 & 1 \end{pmatrix} \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & \alpha \\ 1 & 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ \alpha & \alpha & 1 \end{pmatrix}$$

and, hence, we need only consider $\lambda = 0$ for the second type of (6), and multiplying the third row and column of this by $1/\alpha$ it reduces to

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 1 & 1 & 0 \end{pmatrix}.$$

On the other hand, if $\lambda = 0$ in the first of matrices (6) we can multiply the second and third rows and columns by α and $1/\alpha$, respectively, to obtain

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix}.$$

Hence, it remains to show that in

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ \alpha & 1 & 1 \end{pmatrix}$$

we can select α so that $X^2 + \alpha X + 1$ is the fixed irreducible polynomial. If $X^2 + \alpha X + 1$ is reducible over K then there exists an r with $r^2 + \alpha r + 1 = 0$ and, hence,

$$\begin{pmatrix} 1 & r & 0 \\ 0 & \alpha & 0 \\ r/\alpha & r^2/\alpha & 1/\alpha \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ \alpha & 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & r/\alpha \\ r & \alpha & r^2/\alpha \\ 0 & 0 & 1/\alpha \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix}.$$

So we need only consider matrices

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ \alpha & 1 & 1 \end{pmatrix}$$

with $X^2 + \alpha X + 1$ irreducible over K. On the other hand, if $X^2 + \alpha X + 1$ and $X^2 + \beta X + 1$ are distinct and irreducible over K then, by Lemma 5, $X^2 + (\alpha\beta/(\alpha + \beta))X + 1$ is reducible and hence the equation $x^2 + (\alpha\beta/(\alpha + \beta))x + 1 = 0$ has a solution in K. But then also $s^2 + \beta s + 1 + \beta^2/\alpha^2 = 0$ has a solution $s = (\alpha + \beta)/(\alpha x)$. Therefore,

$$\begin{pmatrix} 1 & \alpha s/\beta & 0 \\ 0 & \alpha/\beta & 0 \\ s & 0 & \beta/\alpha \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ \alpha & 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & s \\ \alpha s/\beta & \alpha/\beta & 0 \\ 0 & 0 & \beta/\alpha \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ \beta & 1 & 1 \end{pmatrix}.$$

It remains to show that the three matrices in the statement of the proposition are not congruent to each other. The first matrix is not congruent to the other two since it has determinant 0 and the others do not. So we must show that the second and third matrices are not congruent. We proceed indirectly, assuming that there exists $\boldsymbol{X} = (x_{ij})$ with

$$\boldsymbol{X}^{\mathrm{T}} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix} \boldsymbol{X} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ \alpha & 1 & 1 \end{pmatrix} \quad \text{where} \quad \begin{cases} \det \boldsymbol{X} \neq 0 \text{ and} \\ X^2 + \alpha X + 1 \\ \text{is irreducible over } K. \end{cases}$$

Let us call (a_{ij}) the matrix on the left-hand side of the above equality; comparing entries we have $a_{22} = x_{12}^2 + x_{32}x_{12} = x_{12}(x_{12} + x_{32}) = 0$ and, hence, $x_{12} = 0$ or $x_{12} = x_{32}$. Also,

$$a_{21} + a_{12} = x_{32}x_{11} + x_{31}x_{12} = 0, \tag{7}$$

$$a_{31} + a_{13} = x_{33}x_{11} + x_{31}x_{13} = \alpha, \tag{8}$$

$$a_{32} + a_{23} = x_{33}x_{12} + x_{32}x_{13} = 0. \tag{9}$$

If $x_{12} \neq 0$ then $x_{12} = x_{32}$, and (7), (9) imply $x_{11} = x_{31}$, $x_{13} = x_{33}$, respectively; hence, $\det X = 0$, a contradiction. So $x_{12} = 0$; if $x_{32} \neq 0$ then (7) implies $x_{11} = 0$ and hence $a_{11} = 0$, a contradiction. Therefore, $x_{12} = x_{32} = 0$ and $x_{11} \neq 0$. Next, we have $a_{12} = x_{31}x_{22} = 0$ and $a_{23} = x_{22}x_{33} = 1$ which imply $x_{22} \neq 0$ and $x_{31} = 0$. Now, $x_{31} = 0$ implies $a_{11} = x_{11}^2 = 1$ which implies $x_{11} = 1$. But then (8) becomes $x_{33} = \alpha$. Hence, $a_{33} = x_{13}^2 + \alpha x_{13} = 1$ contradicting the irreducibility of $X^2 + \alpha X + 1$. □

3. The split case

Now, we examine bilinear forms that split. We shall use the following notation:

$$\mathscr{S} = \{(a_{ij}) \in M_3(K) \mid a_{12} = a_{13} = a_{21} = a_{31} = 0\}.$$

Lemma 6. *If $X^{\mathrm{T}}AX = B$ with X non-singular and A, $B \in \mathscr{S}$ are non-symmetric, then there exists a non-singular $Y \in \mathscr{S}$ with $Y^{\mathrm{T}}AY = B$; furthermore, if μ, ν, y are the top left entries of A, B, Y, respectively, then $\nu = y^2\mu$.*

Proof. If $A, B \in \mathscr{S}$ then

$$A - A^{\mathrm{T}} = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & -\beta \\ 0 & \beta & 0 \end{pmatrix} \quad \text{and} \quad B - B^{\mathrm{T}} = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & -\gamma \\ 0 & \gamma & 0 \end{pmatrix}.$$

Suppose now that A, B are not symmetric (i.e. $\beta, \gamma \neq 0$) and $X^{\mathrm{T}}AX = B$ with $X = (x_{ij})$ non-singular. Then $X^{\mathrm{T}}(A - A^{\mathrm{T}})X = B - B^{\mathrm{T}}$. Comparing first rows we have

$$-x_{21}x_{32} + x_{31}x_{22} = 0 \quad \text{and} \quad -x_{21}x_{33} + x_{31}x_{23} = 0. \tag{10}$$

So the minors of position $(1,2)$ and $(1,3)$ in X are zero. Since X is non-singular, the minor

$$\begin{vmatrix} x_{22} & x_{23} \\ x_{32} & x_{33} \end{vmatrix}$$

of position $(1,1)$ is not zero which forces the homogeneous system (10) to have only the trivial solution $x_{21}=x_{31}=0$. This also implies $x_{11}\neq 0$ since $\det X\neq 0$. But then:

$$X^{\mathrm{T}}AX=\begin{pmatrix} x_{11} & 0 & 0\\ x_{12} & * & *\\ x_{13} & * & * \end{pmatrix}\begin{pmatrix} \mu & 0 & 0\\ 0 & * & *\\ 0 & * & * \end{pmatrix}\begin{pmatrix} x_{11} & x_{12} & x_{13}\\ 0 & * & *\\ 0 & * & * \end{pmatrix}$$

$$=\left(\begin{array}{c|cc} \mu x_{11}^2 & \mu x_{11}x_{12} & \mu x_{11}x_{13}\\ \hline \mu x_{11}x_{12} & & \\ & \multicolumn{2}{c}{T} \\ \mu x_{11}x_{13} & & \end{array}\right)=\begin{pmatrix} \nu & 0 & 0\\ 0 & * & *\\ 0 & * & * \end{pmatrix}.$$

If $\mu\neq 0$ then $x_{12}=x_{13}=0$ and the proof is complete. If $\mu=0$ the block T does not depend on x_{12},x_{13} and, hence, we can use the matrix

$$Y=\begin{pmatrix} x_{11} & 0 & 0\\ 0 & x_{22} & x_{23}\\ 0 & x_{32} & x_{33} \end{pmatrix}$$

instead of X to obtain the same result: $Y^{\mathrm{T}}AY=X^{\mathrm{T}}AX$. $\square$

Now, it is clear how to find a complete set of representatives for the congruence classes of matrices which represent bilinear forms that split. First, consider matrices of the form

$$\left(\begin{array}{c|cc} \mu & 0 & 0\\ \hline 0 & & \\ & \multicolumn{2}{c}{A_0} \\ 0 & & \end{array}\right)\quad \text{with } \mu\in\{0,1,\varepsilon\}. \tag{11}$$

This is symmetric if and only if A_0 is symmetric. On the other hand, by Lemma 6, two matrices A,A' of type (11) with non-symmetric A_0,A_0' are congruent if and only if $\mu=\mu'$ and A_0,A_0' are congruent.

So in order to find the required representatives we must write down representatives for the symmetric forms and then add to the list all matrices (11) with A_0 ranging over a complete set of representatives of the non-symmetric 2×2 forms.

In the case where K is a finite field we can obtain the 3×3 symmetric representatives from Theorems IV.10 and IV.11 in Newman [2]. As regards the 2×2 non-symmetric representatives for the case where $\mathscr{B}$ is non-degenerate we can obtain them from Theorems 2 and 3 in Bremser [1]. In both instances, the representatives are different for $\operatorname{char} K \neq 2$ and $\operatorname{char} K = 2$. The 2×2 representatives from [1] are

$\operatorname{char} K \neq 2$	$\operatorname{char} K = 2$
$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$, $\begin{pmatrix} \varepsilon & 0 \\ 2\varepsilon & \varepsilon \end{pmatrix}$, $\begin{pmatrix} 1 & 0 \\ \beta & 1 \end{pmatrix}$, $\begin{pmatrix} 1 & 0 \\ \beta & \varepsilon \end{pmatrix}$	$\begin{pmatrix} 1 & 0 \\ \beta & 1 \end{pmatrix}$

where ε is an arbitrary but fixed non-square in K^* and β runs over a complete set of coset representatives of $\{1, -1\}$ in K^*.

It remains to find the 2×2 representatives of the non-symmetric degenerate bilinear forms. Let $\mathscr{D}$ be such a form on the two-dimensional space U. Since $\mathscr{D}$ is not symmetric it is not the zero form. If $\mathscr{D}(x,x) = 0$ for every $x \in U$ then its matrix is of the form

$$\begin{pmatrix} 0 & -\alpha \\ \alpha & 0 \end{pmatrix} \quad \text{with } \alpha \neq 0,$$

contradicting the degeneracy of $\mathscr{D}$. So there exists a $v \in U$ with $\mathscr{D}(v,v) = \mu \neq 0$. Then $v \notin R_v = \{x \in U \mid \mathscr{D}(v,x) = 0\}$ and we can select a basis (v,u) of U with $u \in R_v$; with respect to this basis the matrix of $\mathscr{D}$ is

$$\begin{pmatrix} \mu & 0 \\ \alpha & \nu \end{pmatrix}.$$

Since $\mathscr{D}$ is degenerate we must have $\nu = 0$; however, $\alpha \neq 0$ since $\mathscr{D}$ is not symmetric. But then the matrix is

$$\begin{pmatrix} \mu & 0 \\ \alpha & 0 \end{pmatrix} \quad \text{with } \alpha, \mu \neq 0$$

and, hence,

$$\begin{pmatrix} 1 & -\mu/\alpha \\ 0 & 1/\alpha \end{pmatrix} \begin{pmatrix} \mu & 0 \\ \alpha & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ -\mu/\alpha & 1/\alpha \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}.$$

So there is only one such $\mathscr{D}$ and it is represented by

$$\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}.$$

Collating all this information we have the following comprehensive lists.

Theorem. *Let V be a three-dimensional vector space over the finite field K. Every bilinear form on V is represented by one and only one of the following matrices*:

Case 1: $\operatorname{char} K \neq 2$.

Symmetric	Non-symmetric	
	Split	Non-split
$\begin{pmatrix}0&0&0\\0&0&0\\0&0&0\end{pmatrix}$ $\begin{pmatrix}1&0&0\\0&0&0\\0&0&0\end{pmatrix}$ $\begin{pmatrix}\varepsilon&0&0\\0&0&0\\0&0&0\end{pmatrix}$ $\begin{pmatrix}1&0&0\\0&1&0\\0&0&0\end{pmatrix}$ $\begin{pmatrix}1&0&0\\0&\varepsilon&0\\0&0&0\end{pmatrix}$ $\begin{pmatrix}1&0&0\\0&1&0\\0&0&1\end{pmatrix}$ $\begin{pmatrix}1&0&0\\0&1&0\\0&0&\varepsilon\end{pmatrix}$	$\begin{pmatrix}\mu&0&0\\0&0&1\\0&-1&0\end{pmatrix}$ $\begin{pmatrix}\mu&0&0\\0&0&0\\0&1&0\end{pmatrix}$ $\begin{pmatrix}\mu&0&0\\0&\varepsilon&0\\0&2\varepsilon&\varepsilon\end{pmatrix}$ $\begin{pmatrix}\mu&0&0\\0&1&0\\0&\beta&1\end{pmatrix}$ $\begin{pmatrix}\mu&0&0\\0&1&0\\0&\beta&\varepsilon\end{pmatrix}$	$\begin{pmatrix}0&0&0\\0&0&1\\1&1&0\end{pmatrix}$ $\begin{pmatrix}1&0&0\\0&0&1\\1&1&0\end{pmatrix}$ $\begin{pmatrix}\varepsilon&0&0\\0&0&1\\1&1&0\end{pmatrix}$

where $\mu \in \{0,1,\varepsilon\}$, with ε an arbitrary but fixed non-square in K^*, and β runs over a complete set of coset representatives of $\{1,-1\}$ in K^*. Their total number is $3|K|+16$.

Case 2: $\operatorname{char} K = 2$.

Symmetric	Non-symmetric	
	Split	Non-split
$\begin{pmatrix}0&0&0\\0&0&0\\0&0&0\end{pmatrix}$ $\begin{pmatrix}1&0&0\\0&0&0\\0&0&0\end{pmatrix}$ $\begin{pmatrix}1&0&0\\0&1&0\\0&0&0\end{pmatrix}$ $\begin{pmatrix}1&0&0\\0&1&0\\0&0&1\end{pmatrix}$ $\begin{pmatrix}0&0&0\\0&0&1\\0&1&0\end{pmatrix}$	$\begin{pmatrix}\mu&0&0\\0&0&0\\0&1&0\end{pmatrix}$ $\begin{pmatrix}\mu&0&0\\0&1&0\\0&\beta&1\end{pmatrix}$	$\begin{pmatrix}1&0&0\\0&1&0\\1&1&0\end{pmatrix}$ $\begin{pmatrix}1&0&0\\0&0&1\\1&1&0\end{pmatrix}$ $\begin{pmatrix}1&0&0\\0&0&1\\\alpha&1&1\end{pmatrix}$

where $\mu \in \{0,1\}$, $\beta \in K^*$ and $X^2+\alpha X+1$ is an arbitrary but fixed irreducible polynomial of degree two over K. Their total number is $2|K|+8$.

References

[1] P.S. Bremser, Congruence classes of matrices in $GL_2(\boldsymbol{F}_q)$, Discrete Math. 118 (1993) 243–249.
[2] M. Newman, Integral Matrices, Academic Press, New York, 1972.
[3] C. Riehm, The equivalence of bilinear forms, J. Algebra 31 (1974) 45–66.
[4] R. Scharlau, Zur Klassifikation von Bilinearformen und von Isometrien über Körpern, Math. Z. 178 (1981) 359–373.
[5] W.C. Waterhouse, The number of congruence classes in $M_n(\boldsymbol{F}_q)$, Finite Fields Appl. 1 (1995) 57–63.