Available online at www.sciencedirect.com

ScienceDirect

Linear Algebra and its Applications 418 (2006) 468–479

LINEAR ALGEBRA AND ITS APPLICATIONS

www.elsevier.com/locate/laa

Generalized inverses of an invertible infinite matrix over a finite field

C.R. Saranya [a], K.C. Sivakumar [b,*]

[a] Department of Mathematics, College of Engineering, Guindy, Chennai 600 025, India

[b] Department of Mathematics, Indian Institute of Technology Madras, Chennai 600 036, India

Received 17 August 2005; accepted 21 February 2006
Available online 21 April 2006
Submitted by M. Neumann

Abstract

In this paper we show that, contrary to finite matrices with entries taken from finite field, an invertible infinite matrix could have generalized inverses that are different from classical inverses.

AMS classification: Primary 15A09

Keywords: Moore–Penrose inverse; Group inverse; Matrices over finite fields; Infinite matrices

1. Introduction

Let A be a finite matrix. Recall that a matrix X is called the Moore–Penrose inverse of A if it satisfies the following Penrose equations:

$$\begin{aligned} &AXA = A; \quad XAX = X, \\ &(AX)^{\mathrm{T}} = AX; \quad (XA)^{\mathrm{T}} = XA. \end{aligned}$$

Such an X will be denoted by $A^{\dagger}$. The group inverse (if it exists) of a finite square matrix A denoted by $A^{\#}$ is the unique solution of the equations

$$AXA = A; \quad XAX = X; \quad XA = AX.$$

[*] Corresponding author.
E-mail address: kcskumar@iitm.ac.in (K.C. Sivakumar).

doi:10.1016/j.laa.2006.02.023

It is well known that the group inverse of A exists iff the range space $R(A)$ of A and the null space $N(A)$ of A are complementary. For specific applications, for example in solving linear system of equations, it is sufficient to look for X satisfying the equation $AXA = A$. Such an X is called a generalized inverse or a g-inverse of A. A generalized inverse X satisfying the equation $XAX = X$ is called a reflexive generalized inverse of A and will be denoted by A_r^- (see for instance [10]). It is well known that, in general for any A there are infinitely many generalized inverses and reflexive generalized inverses [1]. We also refer the reader to the recent books [13,14].

Pearl [9] was perhaps the first to consider the question of existence of various generalized inverses of a matrix (except the group inverse) over an arbitrary field under an involutory automorphism. Specifically, he proved the following result:

Lemma 1.1 [9, Theorem 1]. *Let A be a rectangular matrix over a field. Then $A^\dagger$ exists iff* $\mathrm{rank}(A) = \mathrm{rank}(A^{\mathrm{T}}A) = \mathrm{rank}(AA^{\mathrm{T}})$.

This result also appears to have been independently obtained by Kalman [6, Section 3, p. 116]. Characterizations for the existence of reflexive generalized inverses and normalized generalized inverses were also obtained by Pearl (see for instance, Theorem 4 and Corollary 3 in [9]). Fulton [4,5] studied factorizations for a given matrix A and obtained conditions for the existence of a normalized generalized inverse (any reflexive generalized inverse X satisfying $(AX)^{\mathrm{T}} = AX$) and the Moore–Penrose inverse of A. He also determined the number of various generalized inverses of A by elementary methods. More recently, Wu and Dawson [3,15] applied generalized inverses of matrices over finite fields to cryptology and proposed a key agreement scheme. They also studied generalized inverses of linear transformations over finite fields and obtained characterizations for the existence of various types of generalized inverses [16]. As pointed out by these authors, there are two essential differences between generalized inverses of real or complex matrices and generalized inverses of matrices over finite fields. One is that the Moore–Penrose inverse of a real or complex matrix always exists (and it is unique), whereas, it need not exist for a matrix over a finite field. For example, the matrix $\begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}$ over $\mathbb{F}_2 = \{0, 1\}$ does not have a Moore–Penrose inverse [16]. Another difference is that there are only finitely many generalized inverses, reflexive generalized inverses and normalized generalized inverses for a matrix over a finite field. As mentioned earlier, this is not the case for real or complex matrices. Dai and Zhang [2] obtained further characterizations for the existence of Moore–Penrose inverse. They reduced the problem of constructing Moore–Penrose invertible matrices to that of constructing subspaces of certain type with respect to some classical groups. They also gave an explicit formula for the Moore–Penrose inverse based on a full-rank factorization [2]. We recall some of the important results that these authors obtained for generalized inverses of a finite matrix over a finite field. We will later show that none of these is applicable in the case of infinite matrices (Section 5).

Let $\mathbb{F}_q$ denote a finite field of order q and $\mathbb{F}_q^k$ denote the k-fold cartesian product of $\mathbb{F}_q$. Let $M_{m\times n}$ denote the set of all matrices over $\mathbb{F}_q$ of order $m \times n$.

Lemma 1.2 [16, Theorem 2]. *Let $A \in M_{m\times n}$. Then a reflexive generalized inverse A_r^- satisfies $(AA_r^-)^{\mathrm{T}} = AA_r^-$ iff $N(A^{\mathrm{T}}) = N(AA^{\mathrm{T}})$.*

Lemma 1.3 [16, Theorem 4]. *Let $A \in M_{m\times n}$. Then a reflexive generalized inverse A_r^- satisfies $(A_r^-A)^{\mathrm{T}} = A_r^-A$ iff $N(A) = N(A^{\mathrm{T}}A)$.*

Lemma 1.4 [16, Theorem 6]. *Let A_r^- be a reflexive generalized inverse of $A \in M_{m\times n}$. Then A_r^- is a Moore–Penrose inverse of A iff the following conditions are satisfied*:

(a) $R(A_r^-) = (N(A))^\perp$.
(b) $N(A_r^-) = (R(A))^\perp$.
(c) $A_r^- Ax = x \ \forall x \in (N(A))^\perp$.
(d) $AA_r^- y = y \ \forall y \in R(A)$.

Lemma 1.5 [16, Theorem 7]. *If $A \in M_{m\times n}$ has a Moore–Penrose inverse, then it is unique.*

The concept of group inverse was studied for matrices over integral domains and later over commutative rings by Manjunatha Prasad and others [7,8]. For the sake of completeness, we recall the following result.

Lemma 1.6 [7, Lemma 3]. *If A is a square matrix of* rank 1 *over an integral domain D, then A has a group inverse iff* Tr A, *the trace of A is invertible in D. In this case, the group inverse $A^\# = (\mathrm{Tr}\, A)^{-2}A$.*

For a characterization of the existence of the group inverse of a finite matrix over general commutative rings we refer to Theorem 10 in [8].

This paper deals with generalized inverses of infinite matrices over the finite field $\mathbb{F}_2$. When dealing with multiplication of two infinite matrices A and B suppose that at least one of them has the property that there are only finitely many entries equal to 1 in any row and in any column. Then all infinite sums appearing in AB and BA are only finite sums (namely 0 or 1) over the field $\mathbb{F}_2$. Even with the definition as above, it must be emphasized that matrix multiplication is non-associative. For instance, let A be the infinite matrix all of whose principal diagonal entries and super diagonal entries are 1 and all other entries 0. If e denotes the infinite column vector all of whose entries are 1 then $(e^{\mathrm{T}}A)e = 1$, whereas $e^{\mathrm{T}}(Ae) = 0$. Thus, for an infinite matrix A, we also demand associativity in the first two Penrose equations and rewrite them as

$$(AX)A = A(XA) = A,$$
$$(XA)X = X(AX) = X.$$

We call X as a Moore–Penrose inverse of an infinite matrix A if X satisfies the two equations as above and the last two Penrose equations. Similarly, we call X a group inverse of an infinite matrix A if X satisfies the two equations as above and the commutativity condition. Clearly, if the classical inverse exists then it is also a Moore–Penrose inverse as well as a group inverse.

We will also have ocassion to deal with multiplication of infinite matrices A and B when neither has the property that any row and any column has finitely many non-zero entries. The following definitions will be used, in this connection.

Definition 1.7. Let $\{s_n\} \subset \mathbb{F}_q^\infty$. We say that $s \in \mathbb{F}_q^\infty$ is a limit of $\{s_n\}$ if for every $k \in \mathbb{N}$, there exists n_0 such that $(s_n - s)_i = 0$, $1 \leqslant i \leqslant k$, for all $n \geqslant n_0$, where $(s_n - s)_i$ denotes the ith coordinate of $s_n - s$. In this case, we say that s_n converges to s.

Remark 1.8. It is clear from the definition that if s_n converges to s, then s must be unique. Since the objects of study in this paper are infinite matrices over $\mathbb{F}_2$, we will consider sequences s_n over $\mathbb{F}_2$ and so we have $s_n - s = s_n + s$.

Example 1.9. Let s_n be defined by

$$(s_n)_i = \begin{cases} 1 & \text{if } i = 4, 8, \ldots, 4n, \\ 0 & \text{otherwise} \end{cases}$$

and s be defined by

$$s_i = \begin{cases} 1 & \text{if } i = 4, 8, \ldots, \\ 0 & \text{otherwise.} \end{cases}$$

Then

$$(s_n + s)_i = \begin{cases} 1 & \text{if } i = 4(n+1), 4(n+2), \ldots, \\ 0 & \text{otherwise.} \end{cases}$$

For any given $k \in \mathbb{N}$, choose n_0 such that $n_0 \geqslant k/4$, for instance. Then $(s_n + s)_i = 0, 1 \leqslant i \leqslant k$, for all $n \geqslant n_0$. Thus s_n converges to s.

Definition 1.10. Let $s_n = \sum_{r=1}^{n} a_r$ denote the nth partial sum of the series $\sum_{r=1}^{\infty} a_r$. Then $\sum_{r=1}^{\infty} a_r$ is said to be convergent with sum s, if any one of the following holds:

(i) $\{s_n\}$ converges to s.
(ii) $\{s_{2n}\}$ converges to s and $\{s_{2n-1}\}$ does not converge.
(iii) $\{s_{2n-1}\}$ converges to s and $\{s_{2n}\}$ does not converge.

If any one of the above holds, we write $\sum_{r=1}^{\infty} a_r = s$.

Remark 1.11. Note that if a series $\sum_{r=1}^{\infty} a_r$ is such that $\{s_{2n}\}$ converges to s and $\{s_{2n-1}\}$ converges to $t \neq s$, then by definition, the given series is not convergent.

Example 1.12. Consider the series $\sum_{r=1}^{\infty} e^{4r}$. The sequence of nth partial sums is given by $s_n = e^4 + e^8 + \cdots + e^{4n}$. Let s be defined by

$$s_i = \begin{cases} 1 & \text{if } i = 4, 8, \ldots, \\ 0 & \text{otherwise.} \end{cases}$$

Then $s_n + s$ is given by

$$(s_n + s)_i = \begin{cases} 1 & \text{if } i = 4(n+1), 4(n+2), \ldots, \\ 0 & \text{otherwise.} \end{cases}$$

For any given $k \in \mathbb{N}$, choose n_0 such that $n_0 \geqslant k/4$. Then $(s_n + s)_i = 0, 1 \leqslant i \leqslant k$, for all $n \geqslant n_0$. Thus s_n converges to s ((i) of Definition 1.10 holds) and so we have $\sum_{r=1}^{\infty} e^{4r} = e^4 + e^8 + e^{12} + \cdots$ Note that s_n is the same as that of Example 1.9.

Let A be an infinite matrix over $\mathbb{F}_2$. Let $\sum_{r=1}^{\infty} e^{j_r}$ denote a specific vector in $\mathbb{F}_2^{\infty}$. Note that the infinite series is used only as a short symbol and has no meaning of convergence, as it is. This will prove to be a very convenient notation, as will be evidenced later. (For example let $e \in \mathbb{F}_2^{\infty}$ be the vector all of whose coordinates are 1. Also, let $e^n = (0, 0, \ldots, 1, 0, \ldots)$ with 1 appearing in the nth coordinate. Then we will use the symbol $e^1 + e^2 + e^3 + \cdots$ to denote e.) Then we set

$$A\left(\sum_{r=1}^{\infty} e^{j_r}\right) = \sum_{r=1}^{\infty} A(e^{j_r})$$

provided the series on the right is convergent (according to Definition 1.10). If A, B and C are infinite matrices related by the equation $AB = C$, we prove the same by verifying $AB(e^k) = C(e^k)$, for all k. This in turn, is verified by establishing $A(a^k) = C(e^k)$, where $a^k = B(e^k)$ will be checked as indicated above.

In what follows, an infinite matrix A is said to have a classical inverse if there exists a matrix B such that $AB = BA = I$. Recently, Sivakumar [11,12] showed that an infinite matrix could have classical inverses and also have generalized inverses, thereby establishing that the set of classical inverses is properly contained in the set of generalized inverses, for infinite matrices. These were in response to a recent open problem on the existence and uniqueness of the Moore–Penrose inverse of infinite matrices. In the same spirit, in this paper, we show that for an infinite matrix over a finite field, generalized inverses and classical inverses could simultaneously exist. Results of this type have not been obtained earlier, to the best of our knowledge. It must be emphasized that our results are placed in an analytical framework. Specifically, we use a novel notion of convergence of infinite series of vectors, with entries 0 or 1 (Definition 1.10). This concept seems to be of interest in its own right. Also, we deal with infinite matrices whose entries are taken from $\mathbb{F}_2$, whereas the articles [11,12] deal with real entries. We also demonstrate that generalized inverses of infinite matrices over a finite field (specifically $\mathbb{F}_2$), behave very differently in contrast to the finite matrix case. In particular, in the final section of this article it shown that known results in the finite matrix case fail in a variety of ways, in the infinite matrix case. Thus the present article is in clear contrast with the earlier ones, viz., [11,12].

We organize the paper as follows. We first give an example of an invertible infinite matrix V which has more than one classical inverse (which are automatically Moore–Penrose inverses) in Theorem 2.1. We next show that V also has a Moore–Penrose inverse which is not a classical inverse (Theorem 3.6). Thus it follows that the Moore–Penrose inverse of V is not unique. We then proceed to show that V has a group inverse (Theorem 4.6) which is not a classical inverse and which turns out to be a Moore–Penrose inverse, as well (Theorem 4.7). It might be emphasized that this is not true for finite matrices with entries from a finite field. We close the paper with a section on counterexamples.

2. Existence and non-uniqueness of classical inverse

We first consider the problem of determining a classical inverse of a particular infinite matrix. We do not view infinite matrices as operators on some vector spaces. However, for the sake of ease in proofs we will continue to use the “basis” $\{e^n : n \in \mathbb{N}\}$, where $e^n = (0, 0, \ldots, 1, 0, \ldots)$ with 1 appearing in the nth coordinate. With this notation we consider the infinite matrix V such that $V(e^1) = e^2$ and $V(e^n) = e^{n-1} + e^{n+1}$, $n \geqslant 2$. We also define formally $V(\sum_{r=1}^{\infty} a_r) = \sum_{r=1}^{\infty} V(a_r)$. Our first result shows that V has infinitely many classical inverses. In what follows $\langle x, y\rangle$ will denote the sum $\sum_{i=1}^{\infty} x_i y_i$. Thus, in this notation to show that an infinite matrix M is symmetric we verify that

$$\langle Me^k, e^l\rangle = \langle e^k, Me^l\rangle \quad \text{for all } k, l.$$

Theorem 2.1. *Let U and W be infinite matrices defined over $\mathbb{F}_2$ by $U(e^1) = e^2 + e^4 + e^6 + e^8 + \cdots$; $U(e^2) = e^1$ and $U(e^{n+1}) = e^n + U(e^{n-1}), n \geqslant 2$ and $W(e^1) = e^1 + e^2 + e^3 + e^4 + \cdots$; $W(e^2) = e^1$ and $W(e^{n+1}) = e^n + W(e^{n-1}), n \geqslant 2$. Then $UV = VU = I$ and $WV = VW = I$.*

Proof. We observe that $U(e^{n-1} + e^{n+1}) = e^n$ and $W(e^{n-1} + e^{n+1}) = e^n$, $n \geqslant 2$. We prove by induction on n that $VU(e^{n+1}) = e^{n+1} = UV(e^{n+1})$. For the basis step, we first note that $UV(e^1) = U(e^2) = e^1$. We claim that

$$VU(e^1) = V(e^2 + e^4 + e^6 + e^8 + \cdots) = e^1.$$

We prove this as follows.

Consider the sequence $\{s_n\}$ defined by $s_n = V(e^2 + e^4 + \cdots + e^{2n})$. Then $s_n = e^1 + e^{2n+1}$. If $s = e^1$, then $s_n + s = e^{2n+1}$. It is now clear that s_n converges to s, ((i) of Definition 1.10 holds) as we set out to prove. Also $UV(e^2) = U(e^1 + e^3) = e^2$ and $VU(e^2) = V(e^1) = e^2$.

Suppose that $UV(e^l) = e^l = VU(e^l)$ for all $l \leqslant n$. Consider $VU(e^{n+1}) = V(e^n) + VU(e^{n-1}) = e^{n-1} + e^{n+1} + e^{n-1} = e^{n+1}$. Also $UV(e^{n+1}) = U(e^n + e^{n+2}) = e^{n+1}$. Thus $UV = VU = I$. To prove $WV = VW = I$, it is sufficient to prove that $WV(e^i) = e^i = VW(e^i)$, $i = 1, 2$. The rest would follow as above. Now, $WV(e^1) = W(e^2) = e^1$. We next show that $VW(e^1) = e^1$.

Consider the sequence $\{s_n\}$ defined by $s_n = V(e^1 + e^2 + e^3 + \cdots + e^n)$. Then $s_n = e^1 + e^{n+1}$. If $s = e^1$, then $s_n + s = e^{n+1}$. It then follows that s_n converges to s ((i) of Definition 1.10 holds). Thus, $VW(e^1) = e^1$. Also, $VW(e^2) = V(e^1) = e^2$ and $WV(e^2) = W(e^1) = e^2$. □

3. Existence of Moore–Penrose inverse

The existence of a Moore–Penrose inverse of V is established in a series of lemmas to follow.

Lemma 3.1. *Let Z be the infinite matrix over $\mathbb{F}_2$ defined by*

$$Z(e^1) = e^4 + e^8 + e^{12} + \cdots, \quad Z(e^2) = e^1$$

and

$$Z(e^{n+1}) = e^n + Z(e^{n-1}), \quad n \geqslant 2.$$

Then $ZV = I$, $V(ZV) = V$, $(ZV)Z = Z$, and $(ZV)^{\mathrm{T}} = ZV$. We also have

(i) $VZ(e^{2n}) = e^{2n}$.
(ii) $VZ(e^{2n-1} + e^{2n+1}) = e^{2n-1} + e^{2n+1}$.

Proof. We have $ZV(e^1) = Z(e^2) = e^1$; $ZV(e^2) = Z(e^1 + e^3) = e^2$ and for $n \geqslant 3$, $ZV(e^n) = Z(e^{n-1} + e^{n+1}) = e^n$. Thus $ZV = I$, so that we have the equations $V(ZV) = V$, $(ZV)Z = Z$, and $(ZV)^{\mathrm{T}} = ZV$.

Consider the sequence $\{s_n\}$ defined by $s_n = V(e^4 + e^8 + \cdots + e^{4n})$. Then $s_n = e^3 + e^5 + e^7 + \cdots + e^{4n-1} + e^{4n+1}$. If $s = e^1$, then clearly, s_n does not converge to s. Thus, $VZ(e^1) \neq e^1$, so that $VZ \neq I$. If $t = e^3 + e^5 + e^7 + \cdots$, then $s_n + t = e^{4n+3} + e^{4n+5} + \cdots$ Clearly, s_n converges to t, so that we can write $VZ(e^1) = e^3 + e^5 + \cdots$

It is now routine to verify the identities (i) and (ii), by induction. □

Remark 3.2. Note that as a consequence of Lemma 3.1, we have for all $n \geqslant 2$, $VZ(e^{n-1} + e^{n+1}) = e^{n-1} + e^{n+1}$.

Lemma 3.3. *Let Z be as defined in Lemma 3.1. Then*

(i) $(VZ)V = V$ *and*
(ii) $Z(VZ) = Z$.

Proof. We have

$$(VZ)V(e^1) = VZ(e^2) = e^2$$

and

$$(VZ)V(e^2) = VZ(e^1 + e^3) = V(e^2).$$

For $n \geqslant 3$,

$$(VZ)V(e^n) = VZ(e^{n-1} + e^{n+1}) = e^{n-1} + e^{n+1} = V(e^n).$$

Thus, Z satisfies $(VZ)V = V$, proving (i).

We next establish (ii).

Consider the sequence $\{s_n\}$ defined by $s_n = Z(e^3 + e^5 + \cdots + e^{2n-1})$. Then

$$s_n = \begin{cases} e^4 + e^8 + e^{12} + \cdots + e^{2n-2} & \text{if } n \text{ is odd,} \\ (e^{2n-2} + e^{2n-6} + \cdots + e^6 + e^2) + Z(e^1) & \text{if } n \text{ is even.} \end{cases}$$

If $s = e^4 + e^8 + \cdots$, then for odd values of n, we have $s_n + s = e^{2n+2} + e^{2n+6} + \cdots$ It now follows that, s_n converges to s. For even values of n, $\{s_n\}$ cannot be convergent due to the presence of the terms inside the paranthesis, above. Thus by (iii) of Definition 1.10, we conclude that

$$Z(e^3 + e^5 + \cdots) = e^4 + e^8 + \cdots = Z(e^1).$$

Recall that we have shown $VZ(e^1) = e^3 + e^5 + \cdots$ Thus we have

$$Z(VZ)(e^1) = Z(e^3 + e^5 + e^7 + \cdots) = Z(e^1).$$

Also, $Z(VZ)(e^2) = Z(e^2)$, as $VZ(e^2) = e^2$. Suppose that $Z(VZ)(e^l) = Z(e^l)$, for $l \leqslant n$. Consider

$$\begin{aligned} Z(VZ)(e^n) &= Z(V(e^{n-1} + Z(e^{n-2}))) = ZV(e^{n-1}) + Z(VZ)(e^{n-2}) \\ &= e^{n-1} + Z(e^{n-2}) = Z(e^n), \end{aligned}$$

where we have used the fact that $ZV = I$ and $Z(VZ)(e^{n-2}) = Z(e^{n-2})$, by induction hypothesis. We have thus proved $Z(VZ) = Z$. □

Lemma 3.4. *Let Z be as defined in Lemma 3.1. Then*

$$VZ(e^{2n+1}) = e^1 + VZ(e^1) + e^{2n+1}, \quad n \geqslant 0.$$

Proof. Clearly, the above is satisfied for $n = 0$. Suppose that it is true for all $l \leqslant n$. Consider

$$\begin{aligned} VZ(e^{2n+3}) &= V(e^{2n+2} + Z(e^{2n+1})) = e^{2n+1} + e^{2n+3} + VZ(e^{2n+1}) \\ &= e^{2n+1} + e^{2n+3} + e^1 + VZ(e^1) + e^{2n+1} = e^1 + VZ(e^1) + e^{2n+3} \end{aligned}$$

proving the induction step. □

Lemma 3.5. *Let Z be as defined in Lemma 3.1. Then $(VZ)^{\mathrm{T}} = VZ$.*

Proof. When k and l are both even, then $VZ(e^k) = e^k$ and $VZ(e^l) = e^l$, by Lemma 3.1. In this case, we clearly have $\langle VZ(e^k), e^l\rangle = \langle e^k, VZ(e^l)\rangle$. If $k = 2r$ and $l = 2s + 1$, then it follows that

$$\langle VZ(e^k), e^l\rangle = 0 = \langle e^k, VS(e^l)\rangle.$$

The case when l is odd and k is even is similar.

Finally, if $k = 2r + 1$ and $l = 2s + 1$, then it can be shown that

$$\langle VZ(e^k), e^l\rangle = 1 + \delta_{rs} = \langle e^k, VZ(e^l)\rangle,$$

where δ_{rs} is the Kronecker delta. □

Theorem 3.6. *Let Z be as defined in Lemma 3.1. Then Z is not a classical inverse of V nor a group inverse of V, but Z is a Moore–Penrose inverse of V.*

Proof. From Lemma 3.1, $ZV = I$ and $VZ \neq I$. Thus Z is not a classical inverse nor a group inverse of V. It is also shown in Lemma 3.1 that $V(ZV) = V$, $(ZV)Z = Z$ and $(ZV)^{\mathrm{T}} = ZV$. Lemma 3.3 establishes that $(VZ)V = V$ and $Z(VZ) = Z$. Lemma 3.5 establishes that $(ZV)^{\mathrm{T}} = ZV$. Thus Z is a Moore–Penrose inverse of V. □

4. Existence of group inverse

Again, the existence of a group inverse of V is established in a series of lemmas.

Lemma 4.1. *Let Y be the infinite matrix defined by*

$$Y(e^1) = e^4 + e^8 + e^{12} + \cdots,$$
$$Y(e^2) = e^3 + e^5 + e^7 + \cdots,$$
$$Y(e^{2n}) = \begin{cases} e^{2n+1} + e^{2n+3} + e^{2n+5} + \cdots & \text{if } n \text{ is odd,} \\ e^1 + e^3 + \cdots + e^{2n-1} & \text{if } n \text{ is even} \end{cases}$$

for $n \geqslant 2$ and

$$Y(e^{2n+1}) = e^{2n} + Y(e^{2n-1}) \quad \text{for } n \geqslant 1.$$

Then for $n \geqslant 1$

$$VY(e^{2n}) = e^{2n} = YV(e^{2n}).$$

Proof. Let $n \geqslant 1$ be odd. Then $VY(e^{2n}) = V(e^{2n+1} + e^{2n+3} + \cdots)$. We show that $V(e^{2n+1} + e^{2n+3} + \cdots) = e^{2n}$. Consider the sequence $\{s_l\}$ defined by $s_l = V(e^{2n+3} + e^{2n+5} + \cdots + e^{2n+l})$. Then $s_l = e^{2n+2} + e^{2n+l+1}$. If $s = e^{2n+2}$, then $s_l + s = e^{2n+l+1}$. It now follows that, $V(e^{2n+3} + e^{2n+5} + \cdots) = e^{2n+2}$. If n is even, then

$$\begin{aligned} VY(e^{2n}) &= V(e^1 + e^3 + \cdots + e^{2n-1}) \\ &= e^2 + e^2 + e^4 + e^4 + \cdots + e^{2n-2} + e^{2n-2} + e^{2n} = e^{2n}. \end{aligned}$$

Also

$$YV(e^2) = Y(e^1 + e^3) = e^2.$$

For $n \geqslant 1$, consider

$$\begin{aligned} YV(e^{2n}) &= Y(e^{2n-1} + e^{2n+1}) = Y(e^{2n-1}) + Y(e^{2n+1}) \\ &= Y(e^{2n-1}) + e^{2n} + Y(e^{2n-1}) = e^{2n}. \qquad \square \end{aligned}$$

Lemma 4.2. *Let Y be as defined in Lemma 4.1. Then for $n \geqslant 1$*

$$VY(e^{2n+1}) = e^1 + Y(e^2) + e^{2n+1} = YV(e^{2n+1}).$$

Proof. We prove the first equation by induction on n. First note that

$$e^1 + Y(e^2) + e^{2n+1} = e^1 + e^3 + e^5 + \cdots + e^{2n-1} + e^{2n+3} + \cdots$$

Consider the sequence $\{s_n\}$ defined by $s_n = V(e^4 + e^8 + \cdots + e^{4n})$. Then $s_n = e^3 + e^5 + e^7 + \cdots + e^{4n+1}$. If $s = Y(e^2) = e^3 + e^7 + e^9 + \cdots$, then we have $s_n + s = e^{4n+3} + e^{4n+5} + \cdots$ It now follows that, s_n converges to s. Thus,

$$\begin{aligned} VY(e^3) &= V(e^2 + Y(e^1)) = e^1 + e^3 + VY(e^1) \\ &= e^1 + e^3 + V(e^4 + e^8 + \ldots) = e^1 + e^3 + Y(e^2). \end{aligned}$$

This establishes the basis step ($n = 1$). It is now routine to verify the induction step and is omitted. This proves the first equality. The second equality is similarly proved. □

Remark 4.3. From Lemmas 4.1 and 4.2, we have $YV = VY$.

Lemma 4.4. *Let Y be as defined in Lemma 4.1. Then for all k*

$$V(YV)(e^k) = (VY)V(e^k) = V(e^k).$$

Proof. The proof follows by employing induction. □

Lemma 4.5. *Let Y be as defined in Lemma 4.1. Then for all k*

$$Y(VY)(e^k) = (YV)Y(e^k) = Y(e^k).$$

Proof. We prove the equations for even values and odd values of k, in that order. The proof is by induction on k. For the basis step $k = 2$ we have $(VY)(e^2) = e^2$, so that $Y(VY)(e^2) = Y(e^2)$. Also, as was shown in Lemma 4.1, $V(e^{2n+3} + e^{2n+5} + \cdots) = e^{2n+2}$. Thus, $V(e^3 + e^5 + \cdots) = e^2$. So

$$(YV)Y(e^2) = (YV)(e^3 + e^5 + \cdots) = Y(V(e^3 + e^5 + \cdots)) = Y(e^2).$$

Now, assume that

$$Y(VY)(e^{2l}) = (YV)Y(e^{2l}) = Y(e^{2l}) \quad \text{for all } l \leqslant n.$$

Consider $Y(VY)(e^{2(n+1)}) = Y(VY)(e^{2n+2}) = Y(e^{2n+2})$, by Lemma 4.1. Also, $(YV)Y(e^{2n+2}) = YV(u)$, where

$$u = Y(e^{2n+2}) = \begin{cases} e^1 + e^3 + \cdots + e^{2n+1} & \text{if } n \text{ is odd,} \\ e^{2n+3} + e^{2n+5} + e^{2n+7} + \cdots & \text{if } n \text{ is even.} \end{cases}$$

So

$$(YV)Y(e^{2n+2}) = \begin{cases} Y(V(e^1 + e^3 + \cdots + e^{2n+1})) & \text{if } n \text{ is odd,} \\ Y(V(e^{2n+3} + e^{2n+5} + e^{2n+7} + \cdots)) & \text{if } n \text{ is even.} \end{cases}$$

Again, $V(e^{2n+3} + e^{2n+5} + e^{2n+7} + \cdots) = e^{2n+2}$ and $V(e^1 + e^3 + \cdots + e^{2n+1}) = e^{2n+2}$, so that $Y(V(e^1 + e^3 + \cdots + e^{2n+1})) = Y(e^{2n+2})$. Thus $(YV)Y(e^{2n+2}) = Y(e^{2n+2})$. This completes the proof for even k.

Next, we take the case of odd k. We first show by induction on n that

$$(YV)Y(e^{2n+1}) = Y(e^{2n+1}).$$

Consider $s_n = (YV)(e^4 + e^8 + \cdots + e^{4n}) = e^4 + e^8 + \cdots + e^{4n}$. If $s = e^4 + e^8 + \cdots$, then $s_n + s = e^{4(n+1)} + e^{4(n+2)} + \cdots$ Thus s_n converges to s and so we have

$$(YV)Y(e^1) = (YV)(e^4 + e^8 + e^{12} + \cdots) = Y(e^1),$$

which provides the basis step ($n = 0$) for induction. Suppose that for all k with $1 \leqslant k \leqslant n$, $(YV)Y(e^{2k+1}) = Y(e^{2k+1})$. Consider

$$\begin{aligned} (YV)Y(e^{2(n+1)+1}) &= (YV)Y(e^{2n+3}) = (YV)(e^{2n+2} + Y(e^{2n+1})) \\ &= YV(e^{2n+2}) + (YV)Y(e^{2n+1}) = e^{2n+2} + Y(e^{2n+1}) \\ &= Y(e^{2n+3}) = Y(e^{2(n+1)+1}). \end{aligned}$$

Next, let $s_n = Y(e^3 + e^5 + \cdots + e^{2n-1})$. Then

$$s_n = \begin{cases} e^4 + e^8 + \cdots + e^{2n-4} + Y(e^{2n-1}) & \text{if } n \text{ is odd,} \\ e^4 + e^8 + \cdots + e^{2n-2} & \text{if } n \text{ is even.} \end{cases}$$

If $s = Y(e^1) = e^4 + e^8 + \cdots$, then it follows that s_n converges to s, whenever n is even. Since $Y(e^{2n-1})$ can be shown to be equal to $e^2 + e^6 + \cdots + e^{2n-2} + e^{2n+2} + e^{2n+6} + \cdots$, it follows that $\{s_n\}$ does not converge when n is odd. It now follows from (ii) of Definition 1.10, that $\{s_n\}$ converges to s. Thus, $Y^2(e^2) = Y(Y(e^2)) = Y(e^3 + e^5 + \cdots) = Y(e^1)$, so that $Y(e^1) + Y^2(e^2) = 0$. Hence, for $n \geqslant 1$

$$Y(VY)(e^{2n+1}) = Y(e^1 + Y(e^2) + e^{2n+1}) = Y(e^1) + Y^2(e^2) + Y(e^{2n+1}) = Y(e^{2n+1})$$

completing the proof for odd values of k. □

Theorem 4.6. *Let Y be as in Lemma 4.1. Then Y is a group inverse of V but not a classical inverse of V.*

Proof. By Remark 4.3, $YV = VY$. By Lemma 4.4

$$V(YV) = (VY)V = V$$

and by Lemma 4.5

$$Y(VY) = (YV)Y = Y.$$

Thus Y is a group inverse of V. Since $VY(e^1) = YV(e^1) = Y(e^2) \neq e^1$, we conclude that Y is not a classical inverse of V. □

Recall that Z (as defined in Lemma 3.1) is a Moore–Penrose inverse but not a group inverse of V. Interestingly, the infinite matrix Y defined in Lemma 4.1 turns out to be a Moore–Penrose inverse of V, as we show next.

Theorem 4.7. *Let Y be as defined in Lemma 4.1. Then Y is a Moore–Penrose inverse of V.*

Proof. Clearly, it is sufficient to show that YV is symmetric. However, this is similar to Lemma 3.5. □

Remark 4.8. It is an interesting open question to determine if V has a group invese which is not a Moore–Penrose inverse.

5. Counterexamples

In this section we show by examples that none of the results for generalized inverses of finite matrices over finite fields mentioned in the introduction is applicable for infinite matrices.

Example 5.1. Let Z be as defined in Lemma 3.1 and Y be as defined in Lemma 4.1. Then Y and Z both are Moore–Penrose inverses of V. Thus Lemma 1.5 does not hold.

Example 5.2. Let x^0 denote the vector $e^2 + e^6 + e^{10} + \cdots$ and $s_n = V(e^2 + e^6 + \cdots + e^{4n-2}) = e^1 + e^3 + \cdots + e^{4n-1}$. Clearly, s_n does not converge to zero so that $V(x^0) \neq 0$. Thus, $x^0 \notin N(V)$. If $t_n = V(s_n)$, then $t_n = e^{4n}$, so that t_n converges to 0. In other words, $V^2(x^0) = 0$, so that $x^0 \in N(V^2)$. Since V is symmetric, we conclude that Lemma 1.2 does not hold.

Example 5.3. By the definition of Z, we have $e^1 = Z(e^2) \in R(Z)$. Clearly, $N(V) = \{x : x = 0 \text{ or } x = e^1 + e^3 + e^5 + \cdots\}$. However, by setting $v^0 = e^1 + e^3 + \cdots$, we have $\langle v^0, e^1\rangle = \langle e^1, e^1 + e^3 + \cdots\rangle = 1$, so that $e^1 \notin (N(V))^{\perp}$. Thus (a) of Lemma 1.4 does not hold.

Example 5.4. We have shown that $Y(e^3 + e^5 + \cdots) = Y(e^1)$, (proof of Lemma 3.5) so that $Y(e^1 + e^3 + \cdots) = 0$. Thus $w^0 = e^1 + e^3 + \cdots \in N(Y)$. Now, if y^0 denotes the vector $e^2 + e^4 + \cdots$ then it can be verified that $V(y^0) = e^1$ so that $e^1 \in R(V)$. However, $\langle w^0, e^1\rangle = 1$, so that $w^0 \notin (R(V))^{\perp}$. Thus (b) of Lemma 1.4 does not hold.

Example 5.5. Recall that $N(V) = \{x : x = 0 \text{ or } x = e^1 + e^3 + e^5 + \cdots\}$. Let $u^0 = e^1 + e^3$. Then $u^0 \in (N(V))^{\perp}$. However,

$$YV(u^0) = Y(e^2 + e^2 + e^4) = Y(e^4) = e^3 + Y(e^2) = e^5 + e^7 + \cdots \neq u^0.$$

Thus (c) of Lemma 1.4 does not hold.

Example 5.6. By Example 5.4 we have $e^1 \in R(V)$. However, as we have established earlier (proof of Lemma 3.1), $VZ(e^1) \neq e^1$. Thus (d) of Lemma 1.4 does not hold.

Remark 5.7. We mention in the passing that the examples given above can be used to show that none of the characterizations for the existence of reflexive generalized inverses and normalized generalized inverses obtained by Pearl [9, Theorem 4 and Corollary 3] hold. We omit the details.

Acknowledgements

The authors thank a referee for suggestions that have improved the readability of the article. They thank Professor P. Veeramani, Department of Mathematics, Indian Institute of Technology Madras for several suggestions. The first author thanks Indian Institute of Technology Madras for the financial support from the Summer Fellowship Programme 2005.

References

[1] A. Ben-Israel, T.N.E. Greville, Generalized Inverses: Theory and Applications, second ed., Springer-Verlag, New York, 2003.
[2] Z.D. Dai, Y. Zhang, Partition, construction and enumeration of $M–P$ invertible matrices over finite fields, Finite Fields Appl. 7 (2001) 428–440.
[3] E. Dawson, C.K. Wu, Key agreement scheme based on generalized inverses of matrices, Elect. Lett. 33 (14) (1997) 1210–1211.
[4] J.D. Fulton, Generalized inverses of matrices over a finite field, Discrete Math. 21 (1978) 23–29.
[5] J.D. Fulton, Generalized inverses of matrices over fields of characteristic two, Linear Algebra Appl. 28 (1979) 69–76.
[6] R.E. Kalman, Algebraic aspects of the generalized inverse of a rectangular matrix, in: M.Z. Nashed (Ed.), Generalized Inverses and Applications, Academic Press, New York, 1976, pp. 111–124.
[7] K. Manjunatha Prasad, K.P.S. Bhaskara Rao, R.B. Bapat, Generalized inverses over integral domains II: Group inverses and Drazin inverses, Linear Algebra Appl. 146 (1991) 31–47.
[8] K. Manjunatha Prasad, Generalized inverses of matrices over commutative rings, Linear Algebra Appl. 211 (1994) 35–52.
[9] M.H. Pearl, Generalized inverses of matrices with entries taken from an arbitrary field, Linear Algebra Appl. 1 (1968) 571–587.
[10] C.A. Rohde, Some results on generalized inverses, SIAM Rev. 8 (1960) 201–205.
[11] K.C. Sivakumar, Moore–Penrose inverse of an invertible infinite matrix, Linear and Multilinear Algebra 54 (2006) 71–77.
[12] K.C. Sivakumar, Generalized inverses of an invertible infinite matrix, Linear and Multilinear Algebra 54 (2) (2006) 113–122.
[13] G. Wang, Y. Wei, S. Qiao, Generalized Inverses: Theory and Computations, Science Press, Beijing/New York, 2004.
[14] M. Wei, Supremum and Stability of Weighted Pseudoinverses and Weighted Least Squares Problems: Analysis and Computations, Nova Science Publishers, New York, 2001.
[15] C.K. Wu, E. Dawson, Generalized inverses in public key cryptodesign, IEE Proc.-Comp. Digit. Techn. 145 (5) (1998) 23–29.
[16] C.K. Wu, E. Dawson, Existence of generalized inverses of linear transformations over finite fields, Finite Fields Appl. 4 (1998) 307–315.