FINITE FIELDS AND THEIR APPLICATIONS **4,** 307–315 (1998)
ARTICLE NO. FF980215

Existence of Generalized Inverse of Linear Transformations over Finite Fields

Chuan-Kun Wu*

School of Computing and Information Technology, University of Western Sydney (Nepean),
P.O. Box 10, Kingswood, New South Wales 2747, Australia
E-mail: c.wu@uws.edu.au

and

Ed Dawson

Information Security Research Centre, Queensland University of Technology, G.P.O. Box 2434,
Brisbane, Queensland 4001, Australia
E-mail: dawson@fit.qut.edu.au

Communicated by Zhe-Xian Wan

Received October 2, 1996; revised January 28, 1998

Relationships between the orthogonal direct sum decomposition of a vector space over a finite field and the existence of the generalized inverses of a linear transformation over the finite field are analyzed. Necessary and sufficient conditions for judging the existence of the generalized inverses of a linear transformation over a finite field are presented. © 1998 Academic Press

Key Words: generalized inverse; finite field; orthogonal direct sum decomposition.

1. INTRODUCTION

It is known that linear transformations can usually be represented by matrices. The study of generalized inverses of linear transformations can to some extent be converted to the study of matrices. Since the 1970s the theory of generalized inverse of matrices has been systematically developed [1], but

* On leave from Xidian University, Xian 710071, P.R. China. Work was done while the author was visiting Queensland University of Technology.

1071-5797/98 $25.00

most results were obtained over the field of real numbers. With the development of digital communications and computer science, algebraic methodology over finite fields has been more and more extensively exploited. For the essential difference between the field of real numbers and finite fields, some properties of matrices over the field of real numbers cannot be analogized over finite fields. This paper will present a study of generalized inverses over finite fields. Sufficient and necessary conditions for judging the existence of generalized inverse of linear transformations over finite fields are given.

2. PRELIMINARIES

Let p be a prime, $q = p^m$ with $m \geq 1$. Denote by F_q the finite field with q elements. Let $M_{m\times n}$ be the set of all matrices over F_q of order $m \times n$. When $m = n$ all matrices in $M_{n\times n}$ are square. We denote by I_n the identity matrix of order $n \times n$, i.e., all ones on its main diagonal and all zeros elsewhere. It is known that any $A \in M_{m\times n}$ corresponds uniquely to a linear mapping Γ_A from F_q^n to F_q^m given by

$$\Gamma_A(x) = Ax, \qquad \forall x \in F_q^n. \tag{1}$$

In addition A^T, the transposed matrix of A, corresponds uniquely to a linear mapping Γ_{A^T} from F_q^m to F_q^n given by

$$\Gamma_{A^T}(y) = A^T y = (y^T A)^T, \qquad \forall x \in F_q^m. \tag{2}$$

Conversely, let Γ_A be a linear mapping from F_q^n to F_q^m; then there must exist an unique matrix $A \in M_{m\times n}$ such that Eq. (1) holds for every $x \in F_q^n$. This means that we can always use A and A^T to describe the mappings of (1) and (2).

Definition 1. Let $A \in M_{m\times n}$. A matrix $B \in M_{n\times m}$ is called the *generalized inverse* of A if

$$ABA = A \tag{3}$$

is satisfied. This is denoted $B = A_g^-$. Such a matrix B is called a *reflexive generalized inverse* of A if the equation

$$BAB = B \tag{4}$$

is satisfied as well. This is denoted $B = A_r^-$. A reflexive generalized inverse A_r^- of A is called a *Moore–Penrose* (*M-P*) *generalized inverse* if it also satisfies the following two properties:

$$(A_r^- A)^T = A_r^- A, \tag{5}$$

$$(AA_r^-)^T = AA_r^-. \tag{6}$$

An M-P generalized inverse of A is usually denoted by A^+.

Definition 2. In the forthcoming discussion we shall use the following abbreviations:

Rank(A):	the rank of matrix A.
$\|A\|$:	determinant of matrix A.
Im(A):	image vector space of A (or Γ_A).
Ker(A):	kernel vector space of A (or Γ_A).
dim(V):	dimension of vector space V.

Definition 3. Let $V \subset F_q^n$, $x = (x_1, \dots, x_n)$ and $y = (y_1, \dots, y_n)$ be two vectors of F_q^n. Then

$$\prec x, y \succ \; = x^T y = y^T x = \sum_{i=1}^{n} x_i y_i \qquad (\text{mod } p)$$

is called the *inner product* of x and y, and $V^\perp = \{y \in F_q^n\colon \prec x, y \succ = 0$ holds for every $x \in V\}$ is called the *orthogonal vector space* of V. It should be noted that all additions here are over the finite field F_q.

Definition 4. Let V be a vector subspace of F_q^n. Then F_q^n is said to be able to be decomposed into the *direct orthogonal sum* of V, denoted

$$F_q^n = V \oplus V^\perp,$$

if for any $x \in F_q^n$, there exists a unique $x_1 \in V$ and a unique $x_2 \in V^\perp$ such that $x = x_1 + x_2$. In this case $V^\perp$ is called the *orthogonal complement* of V.

3. EXISTENCE OF GENERALIZED INVERSES

The following lemma shows the existence of a generalized inverse and a reflexive generalized inverse of an arbitrary matrix over F_q as we have in the case of real-number field.

Lemma 1. *For any matrix over an arbitrary field, there exists a reflexive generalized inverse matrix.*

Over the real-number field, there always exists an M-P generalized inverse for an arbitrary matrix. However, this is not the case over finite fields. For example the matrix $A = \left[\begin{smallmatrix} 1 & 1 \\ 0 & 0 \end{smallmatrix}\right]$ over the binary field has only four reflexive generalized inverses, namely $\left[\begin{smallmatrix} 1 & 0 \\ 0 & 0 \end{smallmatrix}\right]$, $\left[\begin{smallmatrix} 1 & 1 \\ 0 & 0 \end{smallmatrix}\right]$, $\left[\begin{smallmatrix} 0 & 0 \\ 1 & 0 \end{smallmatrix}\right]$, and $\left[\begin{smallmatrix} 0 & 0 \\ 1 & 1 \end{smallmatrix}\right]$. It is easy to check that only $B = \left[\begin{smallmatrix} 1 & 0 \\ 0 & 0 \end{smallmatrix}\right]$ satisfies that AB is symmetric and none satisfies that BA is symmetric as well. In the following we discuss the circumstances in which there exists a reflexive generalized inverse which satisfies (5) and/or (6). The following three well-known lemmas will be used in this paper.

LEMMA 2. *Let V be a vector subspace of F_q^n. Then F_q^n can be decomposed into the orthogonal direct sum of V if and only if $V \cap V^{\perp} = \{\mathbf{0}\}$.*

LEMMA 3. *Let $A \in M_{m\times n}$, A_r^- be a reflexive generalized inverse of A. Then we have*

$$\mathrm{Ker}(A_r^- A) = \mathrm{Ker}(A), \tag{7}$$

$$\mathrm{Im}(AA_r^-) = \mathrm{Im}(A), \tag{8}$$

$$\mathrm{Rank}\,(A) = \mathrm{Rank}\,(A_r^-) = \mathrm{Rank}(A_r^- A) = \mathrm{Rank}\,(AA_r^-). \tag{9}$$

Notice that (5) and (6) mean that $A_r^- A$ and AA_r^- are symmetric, respectively. We next describe further when a matrix is symmetric.

LEMMA 4. *Let $A \in M_{n\times n}$. Then A is symmetric, i.e., $A^T = A$, if and only if for any $x, y \in F_q^n$ we have*

$$\prec Ax, y \succ = \prec x, Ay \succ.$$

LEMMA 5. *Let $A \in M_{n\times n}$ and $A^2 = A$. Then A is symmetric if and only if*

$$(\mathrm{Ker}\,(A))^{\perp} = \mathrm{Im}\,(A).$$

Proof. Necessity: For $x \in \mathrm{Im}\,(A)$ and $y \in \mathrm{Ker}\,(A)$, since A is symmetric, by Lemma 4 we have

$$\prec Ax, y \succ = \prec x, Ay \succ = \prec x, \mathbf{0} \succ = 0.$$

Thus $\mathrm{Im}\,(A) \subseteq (\mathrm{Ker}\,(A))^{\perp}$. But $\dim(\mathrm{Ker}\,(A)) + \dim(\mathrm{Im}\,(A)) = n$, so $(\mathrm{Ker}\,(A))^{\perp} = \mathrm{Im}\,(A)$.

Sufficiency: Suppose we have $A^2 = A$ and $(\mathrm{Ker}\,(A))^{\perp} = \mathrm{Im}\,(A)$. Let $x_1, x_2 \in F_q^n$. Then they can be written as

$$x_1 = Ax_1 + (I_n - A)x_1 \qquad \text{and} \qquad x_2 = Ax_2 + (I_n - A)\,x_2.$$

Note that $(I_n - A)x_i \in \operatorname{Ker}(A) = (\operatorname{Im}(A))^{\perp}$, $i = 1, 2$. We then have

$$\prec Ax_1, x_2 \succ = \prec Ax_1, Ax_2 + (I_n - A)x_2 \succ = \prec Ax_1, Ax_2 \succ.$$

In the same way it can be shown that $\prec x_1, Ax_2 \succ = \prec Ax_1, Ax_2 \succ$. Thus $\prec Ax_1, x_2 \succ = \prec x_1, Ax_2 \succ$. By Lemma 4 we know that A is symmetric. ■

THEOREM 1. *Let $A \in M_{m\times n}$. Then a necessary and sufficient condition for the existence of a reflexive generalized inverse A_r^- of A which satisfies Eq.* (5) *is that F_q^n has the following orthogonal direct sum decomposition*:

$$F_q^n = \operatorname{Ker}(A) \oplus (\operatorname{Ker}(A))^{\perp}. \tag{11}$$

Proof. Necessity: Let A_r^- be a reflexive generalized inverse which satisfies Eq. (5). Then by Lemma 5 we have

$$(\operatorname{Ker}(A_r^- A))^{\perp} = \operatorname{Im}(A_r^- A).$$

For any $x \in \operatorname{Ker}(A_r^- A) \cap \operatorname{Im}(A_r^- A)$, since $x \in \operatorname{Im}(A_r^- A)$, there exists $y \in F_q^n$ such that $x = A_r^- Ay$. Thus we have

$$A_r^- Ax = A_r^- AA_r^- Ay = A_r^- Ay = x.$$

On the other hand, $x \in \operatorname{Ker}(A_r^- A)$ implies that $A_r^- Ax = \mathbf{0}$, i.e., $x = \mathbf{0}$. Therefore $\operatorname{Ker}(A_r^- A) \cap \operatorname{Im}(A_r^- A) = \{\mathbf{0}\}$ and hence $F_q^n = \operatorname{Ker}(A_r^- A) + \operatorname{Im}(A_r^- A) = \operatorname{Ker}(A_r^- A) + (\operatorname{Ker}(A_r^- A))^{\perp}$. By Lemma 3 we then have Eq. (11).

Sufficiency: Assume the validity of Eq. (11). Denote by $M = (\operatorname{Ker}(A))^{\perp}$, $N = \operatorname{Ker}(A)$. Then we can write

$$S = \{Ax : x \in F_q^n\} = \{Ax : x \in M\}.$$

For any $y \in S$, there must exist an $x \in M$ such that $y = Ax$. Moreover the existence of x is unique, as otherwise we would have $Ax_1 = Ax_2$ for some $x_1, x_2 \in M$ and consequently $x_1 - x_2 \in \operatorname{Ker}(A) \cap \operatorname{Ker}(A))^{\perp}$. By the assumption this leads to a contradiction of Lemma 2. Since S is a vector subspace of F_2^m, we denote by T its complement (not necessary orthogonal) subspace; i.e., T is a subspace of F_2^m such that $S \cap T = \{\mathbf{0}\}$, and any $y \in F_2^m$ can uniquely be written as $y_1 + y_2$, where $y_1 \in S$ and $y_2 \in T$. Now define a mapping Γ_B from F_2^m to F_2^n as follows: for an arbitrary $y = y_1 + y_2 \in F_2^m$, where $y_1 = Ax \in S$ with $x \in M$ and $y_2 \in T$, $\Gamma_B(y) = x$. The linearity of Γ_B is shown as follows: Let $y = y_1 + y_2$ and $z = z_1 + z_2$ be two arbitrary vectors of F_2^m, where $y_1 = Ax_1$, $z_1 = Ax_2$, and $y_2, z_2 \in T$. By definition we have $\Gamma_B(y + z) = x_1 + x_2 = \Gamma_B(y) + \Gamma_B(z)$. Thus Γ_B corresponds uniquely to a matrix $B \in M_{n\times m}$ such that for every $y = y_1 + y_2 \in F_q^m$, $By = x$ for some $x \in M$ such that $y_1 = Ax$. For any $x \in F_q^n$ this can be written as $x = x_M + x_N$, where $x_M \in M$ and $x_N \in N$. Thus

$$ABAx = ABAx_M = Ax_M = Ax.$$

Thus we get $ABA = A$. For any $y = y_1 + y_2 \in F_q^m$, where $y_1 = Ax \in S$ and $y_2 \in T$, we have $BABy = BAx = x = BY$. This shows that B is a reflexive generalized inverse of A. By the initial assumption and $\operatorname{Ker}(A) = \operatorname{Ker}(BA)$ from Lemma 3 we have

$$F_q^n = \operatorname{Ker}(BA) \oplus (\operatorname{Ker}(BA))^{\perp} = \operatorname{Ker}(BA) \oplus \operatorname{Im}(BA).$$

Notice that $(BA)^2 = BA$; by Lemma 5 we then have $(BA)^T = BA$. ■

An alternative of the above condition is as follows:

THEOREM 2. *Let $A \in M_{m \times n}$. Then a necessary and sufficient condition for the existence of a reflexive generalized inverse of A which satisfies* (5) *is that for any $x \in F_q^m$, $A^T x = 0$ if and only if $AA^T x = 0$.*

Proof. By Theorem 1, a necessary and sufficient condition for the existence of a reflexive generalized inverse of A satisfying (5) is

$$F_q^n = \operatorname{Ker}(A) \oplus (\operatorname{Ker}(A))^{\perp}.$$

It is known that the preceding decomposition is equivalent to

$$\operatorname{Rank}(A) = \operatorname{Rank}(AA^T),$$

and the conclusion follows. ■

THEOREM 3. *Let $A \in M_{m \times n}$. Then a necessary and sufficient condition for the existence of a reflexive generalized inverse A_r^- of A which satisfies Eq.* (6) *is that F_q^m has the following orthogonal direct sum decomposition*:

$$F_q^m = \operatorname{Im}(A) \oplus (\operatorname{Im}(A))^{\perp}. \tag{12}$$

Proof. Necessity: Let A_r^- be a reflexive generalized inverse of A satisfying Eq. (6). Notice that the matrix A is a reflexive generalized inverse of A_r^- satisfying Eq. (5). By Theorem 1 we have

$$F_q^m = \operatorname{Ker}(A_r^-) \oplus (\operatorname{Ker}(A_r^-))^{\perp}.$$

For any $y \in \mathrm{Ker}(A_r^-)$ and $Ax \in \mathrm{Im}(A)$, since $(AA_r^-)^T = AA_r^-$, we have

$$\prec Ax, y \succ = \prec AA_r^- Ax, y \succ = \prec Ax, AA_r^- y \succ = \prec Ax, \mathbf{0} \succ = 0.$$

Thus $\mathrm{Ker}(A_r^-) \subseteq (\mathrm{Im}(A))^\perp$. Notice that $\dim(\mathrm{Ker}(A_r^-)) + \dim(\mathrm{Im}(A)) = m$. This implies that $\mathrm{Ker}(A_r^-) = (\mathrm{Im}(A))^\perp$ and we then have Eq. (12).

Sufficiency: Assume the validity of Eq. (12). Denote by $S = \mathrm{Im}(A)$ and $T = (\mathrm{Im}(A))^\perp$. Any $y \in F_q^m$ can uniquely be written as $y = y_S + y_T$, where $y_S \in S$ and $y_T \in T$. Define a mapping Γ_B from F_q^m to F_q^n which satisfies $\Gamma_B(y_S + y_T) = x$, where $y_S = Ax \in S$. Similar to the proof of Theorem 1, it can be proven that Γ_B is a linear mapping corresponding uniquely to a matrix $B \in M_{n\times m}$. Moreover B is a reflexive generalized inverse of A and $\mathrm{Im}(AB) = \{ABy : y \in F_q^m\} = \{ABy : y \in S\}$. For any $y \in T$, by definition we have $By = \mathbf{0}$, so $y \in \mathrm{Ker}(B)$. But it is noticed that $\dim(T) = \dim(\mathrm{Ker}(B))$. Thus $T = \mathrm{Ker}(B) = \mathrm{Ker}(AB)$ and consequently by Lemma 3 we have $\mathrm{Ker}(AB) = (\mathrm{Im}(AB))^\perp$. By Lemma 5 and the fact that $(AB)^2 = AB$, we have $(AB)^T = AB$. ■

Likewise we have another alternative of Theorem 3.

THEOREM 4. *Let $A \in M_{m\times n}$. Then a necessary and sufficient condition for the existence of a reflexive generalized inverse of A which satisfies* (6) *is that for any $y \in F_q^n$, $Ay = 0$ if and only if $A^T Ay = 0$.*

Proof. Similar to the proof of Theorem 2. ■

If there exists an M-P generalized inverse of A, by Theorems 1 and 3 we know that the orthogonal direct sum decompositions (11) and (12) are both true simultaneously. It might be asked whether the converse is true as well; i.e., if decompositions (11) and (12) both hold simultaneously for some matrix $A \in M_{m\times n}$, does there exist a reflective generalized inverse of A which satisfies (5) and (6) simultaneously? The following theorem gives a positive answer.

THEOREM 5. *Let $A \in M_{m\times n}$. Then a necessary and sufficient condition for the existence of an M-P generalized inverse of A is that both Eqs.* (11) *and* (12) *hold simultaneously.*

Proof. Necessity is obvious from Theorems 1 and 3. Now the sufficiency is proved as follows. Denote by $M = (\mathrm{Ker}(A))^\perp$, $N = \mathrm{Ker}(A)$, $S = \mathrm{Im}(A)$, and $T = \mathrm{Im}(A))^\perp$. Then $\{Ax : x \in F_q^n\} = \{Ax : x \in M\}$. Define a mapping $\Gamma_B : F_q^m \to F_q^n$ such that for any $y = y_S + y_T$, where $y_S = Ax \in S$ and $y_T \in T$, $\Gamma_B(y) = x$. Then Γ_B is linear and corresponds uniquely to a matrix $B \in M_{n\times m}$. It is easy to check that

1. for any $x \in M$ we have $BAx = x$, and
2. for any $y \in S$ we have $ABy = y$.

By a deduction similar to that of Theorems 1 and 3 it can be proved that the constructed matrix B is indeed an M-P generalized inverse of A. ■

COROLLARY 1. *Let $A \in M_{m \times n}$. We have*

1. *A necessary and sufficient condition for the existence of a reflexive generalized inverse of A satisfying* (5) *is that* $\text{Rank}(A) = \text{Rank}(AA^T)$.

2. *A necessary and sufficient condition for the existence of a reflexive generalized inverse of A satisfying* (6) *is that* $\text{Rank}(A) = \text{Rank}(A^TA)$.

3. *A necessary and sufficient condition for the existence of an M-P generalized inverse of A is that* $\text{Rank}(A) = \text{Rank}(AA^T) = \text{Rank}(A^TA)$.

LEMMA 6. *Let A_r^- be a reflexive generalized inverse of $A \in M_{m \times n}$. Then AA_r^- is symmetric if and only if*

$$(\text{Ker}(A_r^-))^\perp = \text{Im}(A). \tag{13}$$

Proof. Necessity: Assume that AA_r^- is symmetric, i.e., $(AA_r^-)^T = AA_r^-$. Then for any $x \in \text{Ker}(A_r^-)$, $A_r^- x = \mathbf{0}$; and for any $y \in \text{Im}(A)$, there must exist a z such that $y = Az$. Thus $AA_r^- y = AA_r^- Az = Az = y$. Therefore

$$\prec x, y \succ = \prec x, AA_r^- y \succ = \prec AA_r^- x, y \succ = \prec \mathbf{0}, y \succ = 0.$$

This implies that $(\text{Ker}(A_r^-))^\perp \subseteq \text{Im}(A)$. By $\dim((\text{Ker}(A_r^-))^{\perp}) = \dim(\text{Im}(A))$ we have $(\text{Ker}(A_r^-))^\perp = \text{Im}(A)$.

Sufficiency: Assume $(\text{Ker}(A_r^-))^\perp = \text{Im}(A)$. Then by Lemma 3 it follows that $(\text{Ker}(AA_r^-))^\perp = \text{Im}(AA_r^-)$. Since $(AA_r^-)^2 = AA_r^-$, by Lemma 5 we have $(AA_r^-)^T = AA_r^-$. ■

LEMMA 7. *Let $A \in M_{m\times n}$, A_r^- be a reflexive generalized inverse of A. Then $A_r^- A$ is symmetric if and only if*

$$(\text{Ker}(A))^\perp = \text{Im}(A_r^-). \tag{14}$$

Proof. Similar to the proof of Lemma 6. ■

By Lemmas 6 and 7 we have

THEOREM 6. *Let $A \in M_{m\times n}$, A_r^- be a reflexive generalized inverse of A. Then A_r^- is an M-P generalized inverse of A if and only if the following conditions hold*:

1. $\text{Im}(A_r^-) = (\text{Ker}(A))^\perp$;
2. $\text{Ker}(A_r^-) = (\text{Im}(A))^\perp$;
3. *For any* $x \in (\text{Ker}(A))^\perp$, $A_r^- Ax = x$;
4. *For any* $y \in \text{Im}(A)$, $AA_r^- y = y$.

THEOREM 7. Let $A \in M_{m \times n}$. *If there exists an M-P generalized inverse of A, then the generalized inverse must be unique.*

4. CONCLUDING REMARKS

It is shown that the existence of generalized inverses of a linear transformation depends on the orthogonal direct sum decomposition. Necessary and sufficient conditions are presented for the existence of generalized inverses over finite fields. It should be noted that the theory of generalized inverses over finite fields can be a useful tool for cryptographic design. Based on the large number of generalized inverses of a matrix, a public key cryptosystem was proposed in [2]. We have recently designed a key agreement scheme based on the theory of generalized inverses of matrices over finite fields [3]. It is anticipated that further applications of the theory of generalized inverses of matrices over finite fields are possible.

ACKNOWLEDGMENT

The authors are grateful to the anonymous referees for their valuable comments and rectifications.

REFERENCES

1. A. Ben-Israel and T. N. E. Greville, "Generalized Inverses: Theory and Applications," Wiley, New York, 1974.
2. C. K. Wu, A public-key cryptosystem based on generalized inverse of matrices, *J. China Inst. Comm.* **14** (1993), 99–104.
3. E. Dawson and C. K. Wu, A key agreement scheme based on generalized inverses of matrices, *Electron. Lett.* **33** (1997), 1210–1211.