# GENERALIZED INVERSES OF MATRICES OVER A FINITE FIELD 

John D. FULTON<br>Clemson University, Dept of Mathematical Sciences, College of Sciences, Clemson, SC 2963i. U.S.A.

Received 5 April 1976
Revised 24 January 1977
For a given $m \times n$ matrix $A$ of rank $r$ over a finite field $F$, the number of generalized invers as, of reflexive generalized inverses, of normalized generalized inverses, and of pseudoinverses of A are derermined by elementary methods. The more difficult problem of determining which $m \times n$ matrices $A$ of rank $r$ over $F$ have normalized generalized inverses and which have pseudoinverses is solved. Moreover, the number of such matrices which possess normalized generalized inverses and the number which pcssess pseudoinverses are found.

## 1. Introdaction

Moore [ 8,9 ] generalized the notion of the inverse of an $n \times n$ matrix to include generalized inverses of $m \times n$ matrices of arbitrary rank $r$ over the real and the complex fields. Penrose [11] applied generalized inverses of matrices to solutions of simultaneous linear equations. Rohde [12,13] distinguished four different generalized inverses of a given $m \times n$ matrix $A$ of rank $r$ over the complex fielo (see Section 2). Pearl [10] considered the existence of the various generalized inverses of a given $m \times n$ matrix of rank : cyer an arbitrary field $F$ under an arbitrary involutory automorphism $-: F \rightarrow F$. Kina [7] 1 is found, for a given $\boldsymbol{m} \times \boldsymbol{n}$ matrix of rank $r$ over a finite field, the number oi reflexive generalized inverses of $A$.

## 2. Notation and preliminaries

Let $F$ be a field with an involutory automorphism -. Let $M_{n, m}(F)$ de note the set of all $n \times m$ matrices over $F$. If $A=\left(a_{i j}\right) \in M_{n, m}(F)$, then $A^{*}=\left(a_{i j}^{*}\right) \in M_{m, n}(F)$, where $a_{i j}^{*}=\bar{a}_{i i}$.

Definition 2.1. Let $A \in M_{m . n}(F)$ and $A=\left(a_{i j}\right)$. Any $X$ in $G(m, n, F)=$ $\left\{X \in M_{n, m}(F): A X A=A\right\}$ will be called a generrized inverse of $A$ and will be denoted by $A^{g}=X$. Any $X$ in $R(m, n, F)=\{X \in G(m, n, F): X A X=X\}$ will be called a reflexive generalized inverse of $A$ and will be denoted by $A^{\prime}-X$. Any $X$
in $N(m, n, F)=\left\{X \in R(m, n, F):(A X)^{*}=A X\right\}$ will be called a normalized generalized inverse of $A$ and will be denoted by $A^{n}=X$. Any $X$ in $P(m, n, F)=$ $\left\{X \in N(m, n, F):(X A)^{*}=X A\right\}$ will be called a pseudoinverse of $A$ and will be denoted by $A \dagger=X$.

GF $\left(q^{2}\right)$ will denote a finite field of cardinality $q^{2}$, where $q=p^{y}, p$ a prime, $y$ a positive integer. The symbol - will denote an involutory field automorphism of GF $\left(q^{2}\right)$ given by $\bar{a}=a^{q}$. Then GF $(q)$ is the fixed subfield of GF $\left(q^{2}\right)$ relative to the automorphism -. If $q$ is odd and $g$ is any generator of the multiplicative group of $\operatorname{GF}(a)$, let $w=g^{(q+1) / 2}$. Then $\operatorname{GF}\left(q^{2}\right)=\{c+d w: c, d \in \operatorname{GF}(q)\}$ and $\overline{c+d w}=$ $c+d w^{q}=c-d w$. If $q$ is even, let $w$ denote any primitive element of GF $\left(q^{2}\right)$. Then GF $\left(q^{2}\right)=\{c+d w: c, d \in \operatorname{GF}(q)\}$, and if $a=c+d w$, then $\bar{a}=c+d w^{q}$ and $a \bar{a}=$ $c^{L}+\left(w+w^{q}\right) c d+w^{q+1} d^{2} \in$ ( $\mathrm{BF}(q)$.
$\mathscr{V}_{c}\left(q^{i}\right)$ will denote the vector space of $c$-tuples $\chi=\left(x_{1}, x_{2}, \ldots, x_{c}\right)$ over GF $\left(q^{i}\right)$, $i=1,2$. If $h$ is a Hermitian scalar product on $\mathscr{V}_{c}\left(q^{2}\right) \times \mathscr{V}_{c}\left(q^{2}\right)$ and if $\mathscr{T}_{3}$ is any ordered basis for $\mathscr{V}_{c}\left(q^{2}\right)$, then there exist elements $h_{i j}$ in GF $\left(q^{2}\right)$ such that $h(\chi, \chi)=\sum_{i}^{c} \sum_{j}^{c} h_{i j} x_{i} \bar{x}_{j}=\chi H \chi^{*}$, where $H=\left(h_{i j}\right)$ is the $c \times c$ Hermitian matrix of the Hermitian form on $\mathscr{V}_{c}\left(q^{2}\right)$ relative to $\mathscr{B}$ defined by $h$ and where * represents the conjugate, transpose.

If $h$ is a Hermitian scalar product of rank $k$ on $\mathscr{V}_{n}\left(q^{2}\right) \times \mathscr{V}_{n}\left(q^{2}\right)$, it may be seen in the text by Jacobson [6, p.153], for example that there exists an ordered basis $\left(\nu_{1}, \ldots, \nu_{k}, \zeta_{1}, \ldots, \zeta_{n-k}\right)$ of $\mathscr{V}_{n}\left(q^{2}\right)$ such that the matrix of $h$ relative to this basis is the diagonal matrix $D=D\left[b_{1}, \ldots, b_{k}, 0, \ldots, 0\right]$, where $0 \neq b_{i}=h\left(\nu_{i}, \nu_{i}\right), i=$ $1, \ldots, k$.

Carlitz and I 'ges [1] use a theorem by Dickson [2, p.46] to show that if $q^{2}$ is odd, there exi asis $\left(\omega_{1}, \ldots, \omega_{k}, \zeta_{1}, \ldots, \zeta_{n-k}\right)$ of $\mathscr{V}_{n}\left(q^{2}\right)$ such that ,ie matrix of $h$ relative to cus basis is

$$
\left[\begin{array}{cc}
I_{k} & 0 \\
0 & 0
\end{array}\right]
$$

where $I_{k}$ is the $k \times k$ identity matrix.
Suppose $\boldsymbol{q}^{2}$ is even. Since each $b_{i}$ in the matrix $D$ above is a Hermitian element of $\operatorname{GF}\left(q^{2}\right)$, choose element $c_{i} \in \operatorname{GF}(q)$ such that $c_{i}^{2}=b_{i} \in \operatorname{GF}(q)$. Then $c_{i} \bar{c}_{i}=b_{i}$. Hence, there exists an ordered basis $\left(\omega_{1}, \ldots, \omega_{k}, \zeta_{1}, \ldots, \zeta_{n-\mathrm{r}}\right)$ such that the matrix of $h$ relative to this basis is

$$
\left[\begin{array}{ll}
I_{h} & 0 \\
0 & 0
\end{array}\right] .
$$

If $\mathscr{S}$ is a subspace of $\mathscr{V}=\mathscr{V}_{c}\left(q^{2}\right)$, subspace $\mathcal{S}^{\mathscr{L}}=\{\chi \in \mathscr{V}: h(\chi, \sigma)=0$ for all $\sigma \in \mathscr{Y}\}$. The radical of subspace $\mathscr{S}$ is the subspace $\mathrm{R} \mathfrak{I} \mathscr{P}=\mathscr{P} \cap \mathscr{S}^{\perp}$. A subspace $\mathscr{S}$ of $\mathscr{V}$ is said to be nonisotropic, isotropic, or totally isotropic according as $\operatorname{Rad}(\mathscr{Y})$ is $\{0\}$, is not $\{0\}, \sim$ is $\mathscr{P}$, respectively. The Hermitian scalar product $h$ is said to be
nondegenerate, or be of full rank if Rad $\mathscr{V}:=\{0\}$. St bspaces $\mathscr{S}_{1}$ and $\mathscr{S}_{2}$ of $\mathscr{O}$ are said to $\mathbf{d e} h$-equivalent if and only if there exists a linear isomorphism $U$ of $\mathscr{S}_{1}$ onto $\mathscr{S}_{2}$ such that $h(\chi, \eta)=h(U(\chi), U(\eta))$ fo ${ }^{*}$ all $\chi, \eta \in \mathscr{C}_{1}$. Also, if $U$ defines an $h$-equivalence of $\mathscr{V}$, then $U$ is said to be a unitary transformation on $\mathscr{V}$.

Throughout this paper, $|\mathscr{F}|$ will denote the cardinality of the set $\mathscr{P}$, and $\rho(A)$ will denote the rank of matrix $A$.

## 3. The generalized inverses of a given matrix

We shall prove the following theorem:
Theorem 3.1. Let $A \in M_{m, n}(G F(q))$ of $\operatorname{rank} r=\rho(A)$. Theri

$$
\begin{align*}
|G(m, n, \mathrm{GF}(q))| & =q^{n m-r^{2}}  \tag{1}\\
|R(m, n \cdot \mathrm{GF}(g))| & =q^{r(m+n-2 r)} . \tag{2}
\end{align*}
$$

Let $A \in M_{m, n}\left(G F\left(q^{2}\right)\right)$ of rank $r=\rho(A)$. Then

$$
\begin{align*}
& \left|N\left(m, n, \operatorname{GF}\left(q^{2}\right)\right)\right|=\left\{\begin{array}{cc}
q^{2 r(n-r)} & \text { if } r=\rho\left(A^{*} A\right), \\
0 & \text { if } r>\rho\left(A^{*} A\right) .
\end{array}\right.  \tag{3}\\
& \left|P\left(m, n, \operatorname{GF}\left(q^{2}\right)\right)\right|= \begin{cases}1 & \text { if } r=\rho\left(A^{*} A\right)=\rho\left(A A^{*}\right), \\
0 & \text { otherwise. } .\end{cases} \tag{4}
\end{align*}
$$

Proof. (4) follows from [8] and [10, Theorem 1]. (2) is clear from [7]. We consider (1). For $A$, there exist two nonsingular matrices $P$ and $Q$ over GF $(q)$ such that

$$
P A Q=\left(\begin{array}{ll}
I_{r} & 0 \\
0 & 0
\end{array}\right)=K_{r},
$$

where $I_{r}$ denotes the $r \times r$ identity matrix. Let $X \in G(m, n, \mathrm{GF}(q))$ and let

$$
Y=Q^{-1} X P^{-1}=\left(\begin{array}{ll}
Y_{1} & Y_{2} \\
Y_{3} & Y_{4}
\end{array}\right)
$$

From $A X A=A$, we obtain $K_{r} Y K_{r}=K_{r}$ and $Y_{1}=I_{r}$. We see that $Y_{2}, Y_{3}$, and $Y_{s}$ are arbitrary. Thus, we find that $|G(m, n, G F(q))|=q^{m n-r^{2}}$ since $Y_{2}$ is $r \times(m-r)$ $Y_{3}$ is $(n-r) \times r$, and $Y_{4}$ is $(n-r) \times(m-r)$.

Consider (3). If $r>\rho\left(A^{*} A\right)$, then $\left|N\left(m, n, G F\left(q^{2}\right)\right)\right|=0$ by [10. Corollary 1]. W'e suppose $\rho\left(A^{*} A\right)=r=\rho(A)$. For $A$, there exist nonsingular matrices $P$ in $M_{m, m}\left(\mathrm{GF}\left(q^{2}\right)\right)$ and $O$ in $M_{n, n}\left(\mathrm{GF}\left(q^{2}\right)\right)$ such that $P A O=K_{r}$. Let Xe $N\left(m, n, \mathrm{GF}\left(q^{2}\right)\right)$ and let

$$
Y=Q^{-i} X P^{-1}=\left(\begin{array}{ll}
Y_{1} & Y_{2} \\
Y_{3} & Y_{4}
\end{array}\right)
$$

Then we can obtain that $K_{r} Y K_{r}=K_{n} Y_{1}=I_{n} Y_{4}=Y_{3} Y_{2}$ and $P F^{*}\left(K_{r} Y\right)^{*}\left(P P^{*}\right)^{-1}=$ $K, Y$, By letting

$$
\left(P P^{*}\right)^{-1}=\left(\begin{array}{ll}
B_{1} & B_{2} \\
B_{3} & B_{4}
\end{array}\right)
$$

we show with little difficilty that $Y_{2}^{*} B_{1}=B_{3}$. We show that $B_{1}$ is nonsingular (see [10, pp. $5 / 4-575]$ ). Thus, we have $Y_{2}=\left(B_{3} B_{1}^{-1}\right)^{*} . Y_{3} \in M_{r, n-r}\left(G F\left(q^{2}\right)\right)$ is arbitrary, and, herce, we infer that $\left|N\left(m, n, \operatorname{GF}\left(q^{2}\right)\right)\right|=q^{2 r(n-r)}$. This proves the theorem.

Thus, as has been indicatcd by Pearl [10], the methods of Section 3 are field independent and certainly free of the theory of Hermitian forms. However, as will be seen in Section 4, the more difficult problem of determining which matrices over GF ( $q^{2}$ ) have normalized generalized inverses and which have pseudionverses will be resolved by methods peculiar to finite fislds. Our methods invoke the classical theory of Hermitian forms over Gr $\left(q^{2}\right)$.

## 4. Matrices $A$ such that $A^{n}$ and $A \dagger$ exist

Pearl [10, Theorem 1] proved that $A \in M_{m, n}\left(G F\left(q^{2}\right)\right)$ with $r=\rho(A)$ has a normalized generalized inverse if and only if $r=\rho\left(A^{*} A\right)$ and has a pseudoinverse if and only if $r=\rho\left(A^{*} A\right)=\rho\left(A A^{*}\right)$. We let $\mathscr{A}\left(m, n, r, q^{2}\right)=\left\{A \in M_{m, n}(G F\right.$ $\left.\left.\left(q^{2}\right)\right): r=\rho\left(A_{i}\right)=\rho\left(A^{*} A\right)\right\} \quad$ and $\quad$ let $\quad \mathscr{B}\left(m, n, r, q^{2}\right)=\left\{A \in \mathscr{A}\left(\neq n, n, r, q^{2}\right): r=\right.$ $\left.\rho\left(A A^{*}\right)\right\}$.

We require in this section the cardinality (see [14, p. 33], for example)

$$
\begin{equation*}
\left|U_{k}\left(q^{2}\right)\right|=: q^{\left(k^{2}-k\right) / 2} \prod_{i=1}^{k}\left(q^{i}-(-1)^{i}\right) \tag{5}
\end{equation*}
$$

of $\mathscr{U}_{k}\left(q^{2}\right)$, the unitary subgioup of the $g \in$ neral linear group in $M_{r, k}\left(G F\left(q^{2}\right)\right)$. Also, we require the widely known caillinality

$$
\begin{equation*}
\left|\mathscr{S}\left(r, k, q^{2}\right)\right|=\prod_{i=0}^{r-1}\left(q^{2 k}-q^{2 i}\right) \tag{6}
\end{equation*}
$$

of $\mathscr{P}\left(r, k, q^{2}\right)=\left\{A \in M_{r, k}\left(\operatorname{GF}\left(q^{2}\right)\right): r=p(A)\right\}$.
Our method of characterizing and enumerating the rank $r$ matrices $A \in$ ${ }_{n, n}\left(\mathrm{GF}\left(q^{2}\right)\right)$ such that $A^{n}$ or $A \dagger$ exist involves the sGations in $M_{\text {m, }}\left(\mathrm{GF}\left(q^{2}\right)\right)$ to $\therefore T=I_{r}$.

Lemma 4.1. If $\mathscr{G}\left(m, r, q^{2}\right)=\left\{T \in M_{m, r}\left(G F\left(q^{2}\right)\right): T^{*} T=I_{r}\right\}$, then

$$
\begin{equation*}
\left|\mathscr{T}\left(m, r, q^{2}\right)\right|=\left|U_{m}\left(q^{2}\right)\right| /\left|U_{m-r}\left(q^{2}\right)\right| \tag{7}
\end{equation*}
$$

where for $k=m$ or $k=m-r,\left|U_{k}\left(q^{2}\right)\right|$ is given by (5).

Proof. Let $T=\left[\tau_{1}, \tau_{2}, \ldots, \tau_{r}\right] \in \mathscr{T}\left(m, r, q^{2}\right)$ and let $\mathscr{C}$ denote column space. FGT $\mathcal{q}=V_{m}\left(q^{2}\right)$, let $h$ be a nondegenerate Hermitian scalar pressuct on $\mathscr{V} \times \mathscr{V}$ such that the rnatrix of $h$ relative to the ordered basis of elementary $m \times 1$ unit vectors ( $\varepsilon_{1}, \ldots, s_{2}$ ) of $\mathscr{V}$ is $I_{m}$. Let $\left.\mathscr{W}=<\varepsilon_{1}, \ldots, \varepsilon_{r}\right\rangle$ and consider the linear transformation $L: W \rightarrow \mathscr{G}(T)$ such that $L\left(\varepsilon_{i}\right)=\tau_{i}, i=1, \ldots, r$. Then $L$ is an $h$ equivalence of $\mathscr{W}$ onto $\mathscr{C} \mathscr{P}(T)$. Since $W^{\perp}=(\mathscr{C} \mathscr{P}(T))^{\perp}=\{0\}$, each of $\mathscr{W}$ and $\mathscr{C} \mathscr{S}(T)$ is nonisotropi: and Witt's theorem [6, p. 162] applies. Hence, $L$ can be extended to an element $U_{0}$ of the unitary group on $\mathscr{V}$. Consider the unitary group on $\mathscr{V}$ as $\mathscr{U _ { m }}\left(q^{2}\right)$, the group of unitary matrices of the unitary transformations on $\mathscr{V}$ relative to the ordere 1 basis $\left(\varepsilon_{1}, \varepsilon_{2}, \ldots, \varepsilon_{m}\right)$. Let $\mathscr{L}=\left\{U \in \mathscr{U}_{m}\left(q^{2}\right): U\right.$ exten's $\left.L\right\}$. Also, the identity linear transformation $I: \mathscr{W} \rightarrow \mathscr{W}$ such that $I\left(\varepsilon_{i}\right)=\varepsilon_{i}, i=1, \ldots, r$, is an $h$-equivalence of $W$ and, thus, can be extended to an element of $\|_{m}\left(q^{2}\right)$. If we let $\mathscr{I}$ denote the subgroup $\left\{U_{\varepsilon} \mathscr{U}_{m}\left(q^{2}\right): U\right.$ extends $\left.I\right\}$ of $\mathscr{U}_{m}\left(q^{2}\right)$, it is immediate that $\Phi$ is isomorphic to $\mathscr{U}_{m \ldots}\left(q^{2}\right)$ and that $\mathscr{L}=U_{0} \mathscr{L}$, the coset of $\mathscr{L}$ in $U_{m}\left(q^{2}\right)$ which contains $U_{0}$. Hence, $|\mathscr{L}|=\left|U_{0} \mathscr{I}\right|=|\mathscr{I}|=\left|U_{m-r}\left(q^{2}\right)\right|$. Therefore, $\left|\mathscr{T}\left(m, r, q^{2}\right)\right|$ is given by (7), and the proof is complete.

Theorem 4.2. Let $A \in M_{m, n}\left(\operatorname{GF}\left(i^{2}\right)\right)$ have $\rho(A)=r$. Then $A \in \mathscr{A}\left(m, n r, q^{2}\right)$ if and only if $A=T S$, where $T$ is $m \times r$ such that $T^{*} T=I_{r}$ and where $S$ s $r \times n$ with $\rho(S)=r$. Moreover,

$$
\begin{equation*}
\left|\mathscr{A}\left(m, n, r, q^{2}\right)\right|=\left|\mathscr{S}\left(r, n, q^{2}\right)\right|\left|\mathscr{T}\left(m, r, q^{2}\right)\right| /\left|थ_{r}\left(q^{2}\right)\right| \tag{8}
\end{equation*}
$$

where $\left|\mathscr{P}\left(r, n, q^{2}\right)\right|$ is given by (6), $\left|\mathscr{T}\left(m, r, q^{2}\right)\right|$ is given by (7), ana $\left|Q_{r}\left(q^{2}\right)\right|$ is given by (5).

Proof. Let $A \in M_{m, n}\left(G F\left(q^{2}\right)\right)$ have rank $r$. Then $A=R S_{1}$, where $R$ is $m \times r$ and $S_{1}$ is $r \times n$ such that $\rho(R)=\rho\left(S_{1}\right)=r$ (see [3]). Now $\rho\left(A^{*} A\right)=r$ if and only if $\rho\left(R^{*} R\right)=r$. Again, for $\mathscr{V}=\mathscr{V}_{m}\left(q^{2}\right)$, let $h$ be a nundegenerate Hermitian scalar product on $\mathscr{V} \times \mathscr{V}$ such that the matrix of $h$ : ative to the ordered basis of elementary $m \times 1$ unit vectors $\left(\varepsilon_{1}, \ldots, \varepsilon_{m}\right)$ of $\mathscr{V} ; i_{n}$. From Section $2, \rho\left(R^{*} R\right)=r$ if and only if there exists an ordered basis $\left(\tau_{1}, i_{2}, \ldots, \tau_{r}\right)$ of $\mathscr{C} \mathscr{S}(R)$ such that $h\left(\tau_{i}, \tau_{j}\right)=\delta_{i j}$, the Kronecker delta, ancu, tius, if anci only if there exists a nonsingular matrix $\operatorname{MeM}_{r, r}\left(\mathbf{G F}\left(q^{2}\right)\right)$ such that if $\left[\tau_{1}, \tau_{2}, \ldots, \tau_{r}\right]=R M=T$, then $T^{*} T=I_{r}$. Thus, $r=\rho\left(A^{*} A\right)=\rho(A)$ if and orly if $A=R S_{1}=T M^{-1} S_{1}=T S$, where $T$ and $S$ satisfy the statement of Theorem 4.2

Among the $\left|\mathscr{T}\left(m, r, q^{2}\right)\right| \mid \mathcal{F}\left(r: z, q^{-} \|\right.$pairs of matrices $(T, S)$ in $\mathscr{T}\left(m, r, q^{2}\right) \times$ $\mathscr{P}\left(r, n, q^{2}\right)$, the same matrix $A=T S$ in $\mathscr{A}\left(m, n, r, q^{2}\right)$ may be repeated many times. In fact, for $\left(T_{1}, S_{1}\right),\left(T_{2}, S_{2}\right.$ in $\mathscr{T}\left(m, r, q^{2}\right) \times \mathscr{F}\left(r, n, q^{2}\right), T_{1} S_{1}=T_{2} S_{2}$ if and only if $T_{2}=T_{1}\left(S_{1} S_{2}^{i}\right)$, where $I_{r}=T_{2}^{*} T_{2}=\left(S_{1} S_{2}^{i}\right)^{*} T_{1}^{*} T_{1}\left(S_{1} S_{2}^{i}\right)=\left(S_{1} S_{2}^{i}\right) *\left(S_{1} S_{2}^{i}\right)$ and where $S_{2}^{i}$ is any right inverse for $S_{2}$. Hence $T_{1} S_{1}=T_{2} S_{2}$ if and only if $S_{1} S_{2}^{i} \in \mathcal{U}_{r}\left(q^{2}\right)$. On the other hand, if $T_{1} \in \mathscr{T}\left(m, r, q^{2}\right)$ and $U \in \varkappa_{r}\left(q^{2}\right)$, so does $T_{2}=T_{1} U \in \mathscr{T}\left(m, r, q^{2}\right)$. This, $\mathscr{A}\left(m, n, r, q^{2}\right) \mid$ is given by (8). Hence, Theorem 4.2 has been pioved.

We remark here that if $\mathscr{G}\left(r, n, q^{2}\right)=\left\{G \in M_{r, n}\left(G F\left(q^{2}\right)\right): G G^{*}=I_{r}\right\}$, then $\left|G\left(r, n, q^{2}\right)\right|=\mid \mathscr{T}\left(n, r, q^{2}\right)_{i}$, given by (7).

Theorem 4.3. Let $A \in M_{m, n}(G F(q))$ have $\rho(A)=r$. Then $A \in \mathscr{B}\left(m, n, r, q^{2}\right)$ if and only if $A=T N G$, where $T \in \mathscr{T}\left(m, r, q^{2}\right), \quad N \in \mathscr{S}\left(r, r, q^{2}\right)$, and $G \in \mathscr{G}\left(r, n, q^{2}\right)$. Moreover,

$$
\begin{equation*}
\left|\mathscr{B}\left(m, n, r, q^{2}\right)\right|=\left.\left|\mathscr{T}\left(m, r, q^{2}\right)\right|\left|\mathscr{S}\left(r, r, q^{2}\right)\right|\left|\mathscr{T}\left(n, r, q^{2}\right)\right|| | \mathscr{U}_{r}\left(q_{1}^{2}\right)\right|^{2} \tag{9}
\end{equation*}
$$

wher: each of $\mathscr{T}\left(m, r, q^{2}\right)$ and $\mathscr{T}\left(n, r, q^{2}\right)$ is given by (7), where $\mathscr{S}\left(r, r, q^{2}\right)$ is given by (6), and where $U_{r}\left(q^{2}\right)$ is given by (5).

Proof. Let $A=T S \in \mathscr{A}\left(m, n, r, q^{2}\right)$, where $T \in \mathscr{S}\left(i m, r, q^{2}\right)$ and $S \in \mathscr{P}\left(r, n, q^{2}\right)$. Then $r=\rho\left(A A^{*}\right)$ if anc oniy if $r=\rho\left(S S^{*}\right)$ if and only if there exists an $r \times r$ nonsinguiar matrix $N_{1}$ such that if $\dot{v}=N_{1} S$, then $G G^{*}=I_{r}$. Hence, $\rho\left(A A^{*}\right)=r$ if nd only if $A=T N G$, where each of $T, N=N_{1}^{-1}$; and $G$ satisfies the statement or Theorem 4.3.

Consider the list of

$$
\left|\mathscr{T}\left(m, r, q^{2}\right)\right|\left|\mathscr{P}\left(r, r, q^{2}\right)\right|\left|\mathscr{T}\left(n, r, q^{2}\right)\right| /\left|U_{r}\left(q^{2}\right)\right|
$$

$m \times n$ matrices $A=T N G$, each belonging to $\mathscr{B}\left(m, n, r, q^{2}\right)$, where $T \in \mathscr{T}\left(m, r, q^{2}\right)$, $N \in \mathscr{S}\left(r, r, q^{2}\right)$, and $G \in \mathscr{G}\left(r, n, q^{2}\right)$ and where if $T_{1} N_{1} G_{1}$ and $T_{2} N_{2} G_{2}$ are in the ist, then $T_{1} \neq T_{2} U$ for any $U \in \mathscr{Q} i_{r}\left(q^{2}\right)$. Now $T_{1} N_{1} G_{1}=T_{2} N_{2} G_{2}$ in the list if and only if $T_{2}=T_{1}\left(N_{1} G_{1} G_{2}^{i} N_{2}^{-1}\right)$, where $G_{2}^{i}$ is any right inverse for $G_{2}$ and where $U=N_{1} G_{1} G_{2}^{i} N_{2}^{-1} \in \mathscr{U}_{r}\left(q^{2}\right)$. That is, $T_{1} N_{1} G_{1}=T_{2} N_{2} F_{2}$ if and only if $T_{1}=T_{2}$ and, thus, $N_{1} G_{1}=N_{2} G_{2}$. But $N_{1} G_{1}=N_{2} G_{2}$ if and only if $G_{2}=\left(N_{2}^{-1} N_{1}\right) G_{1}$, where $I_{r}=G_{2} G_{2}^{*}=\left(N_{2}^{-1} N_{1}\right) G_{1} G_{1}^{*}\left(N_{2}^{-1} N_{1}\right)^{*}=\left(N_{2}^{-1} N_{1}\right)\left(N_{2}^{-1} N_{1}\right)^{*}$. Hence each $A \in$ $\mathscr{B}\left(m, n, r, q^{2}\right)$ occurs precisely $\left|U_{r}\left(q^{2}\right)\right|$ times in the list. Therefore, $\left|\mathscr{B}\left(m, n, r, q^{2}\right)\right|$ is given by (9). The proof is complete.

The problem of finding the number $m \times n$ matrices $X$ over GF $\left(q^{2}\right)$ which satisfy the matrix equation $X A X^{*}=B$, for given Hermitian matrives $A$ and $B$ has received much attention $[1,4,5,15]$, and in the latter three papers, the number solutions $X$ of rank $r$ is given. We did not appeal to these papers, however, and referred to develop methods of vur own.

We assumed in this section that the involutory automernem - on $\operatorname{GF}\left(q^{2}\right)$ was not the identity (see Section 2). However, if - is the ilentity automorphism of GF $\left(q^{2}\right)$ (GF ( $q$ ) could be used as well in this case, ant if $q$ is odd the methods ard enumerations of this section need no alterthon $[6, p$. 162]. On the other hand, if - is the identity and $q$ is ever, Witt's thecren must be reformulaicd [ $6, p$. 162], and special methods must be devised to find $\left|\mathscr{A}\left(m, n, r, q^{2}\right)\right|$ and Pim, $n \cdot q^{3}!$ Th $=$ case where the involutory autom whis in $\cdots$ of $G F\left(q^{2}\right)$, $q$ even, * a tomorphism will be considered in ab il er paper by the aubor.

## References

[1] L. Carlitz and J.H. Hodges, Representations by Hermitian forms in a finite fie'd, Duke Math. J. 22 (1965) 393-406.
[2] L. Dickson, Linear Groups With an Exposition of the Galois Theory, (Leipzig; Reprinted by Dover, New York, 1958).
[3] J.S. Frame, Matrix functions and applications, IEEE Spectrum 1 (1964) 208-220.
[4] J.D. Fulton, Representations by Hermitian forms in a finite field of characte istic two, Can. J. Math. (to appear).
[5] J.H. Hodges, An Hermitian matrix e fuation over a finite field Duke Math. J. 33 (1966) 123-130.
[6] N. Jacobson, Lectures in Abstract Algebra, Vol. II, (Van Nostrand, New York, 1953).
[7] J.B. Kim, On singular matrices, J. Korean Math. Soc. 3 (1966) 1-2.
[8] E.H. Moore, On the reciprocal of the general algebraic matrix (abstract). Bull. Am. Matt. So:26 (1920) 394-395.
[9] S.H. Moore, General analysis, Part I, Mem. Am. Prlos. Soc. 1 (1935).
[10] M.H. Peatı, Generalized inverses of matrices with entries taken from an arbitrary field, :inear Algebra and Appl. 1 (1968) 571-587.
[11] R. Pearuse, A generalized inverse for marices, Pruc. Cambridge Philos. Soc. 51 (1955) 4061 -413.
[12] C.A. Rohde, Generalized inverses of partitioned matrices, J. Soc. Irdust. Appl. Math. 13 (1965) 1033-1035.
[13] C.A. Rohde, Some results on generalized inverses, SIAM Rev. 8 (1966) 2 J1-205.
[14] G.E. Wall, On the conjugacy classes in the unitary, symplectic and orthogonal groups, J. Austral. Math. Soc 3 (1963) 1-62.
[15] Z. Wan and B. Yang, Studies in finite geometries and the construction of i icomplete block designs, III: some "anzahl" theorems in unitary geometry over finite fields and their applizations, Acta Math. Sinica 15 (1965) 533-544 (Chinese Math.-Acta 7 (1955) 252-264).

