Designs, Codes and Cryptography, 13, 313–330 (1998)


# Quasideterminant Characterization of MDS Group Codes over Abelian Groups

A. A. ZAIN*
*Dept. of Electrical Engineering, Indian Institute of Technology, Delhi, Hauz Khas, New Delhi 110 016, India*

B. SUNDAR RAJAN bsrajan@ee.iitd.ernet.in
*Dept. of Electrical Engineering, Indian Institute of Technology, Delhi, Hauz Khas, New Delhi 110 016, India*

**Communicated by:** A. Blokhuis

*Received February 10, 1995; Revised January 2, 1996; Accepted July 10, 1996*

**Abstract.** A group code defined over a group $G$ is a subset of $G^n$ which forms a group under componentwise group operation. The well known matrix characterization of MDS (Maximum Distance Separable) linear codes over finite fields is generalized to MDS group codes over abelian groups, using the notion of quasideterminants defined for matrices over non-commutative rings.

**Keywords:** group codes, maximum distance separable codes, quasideterminants, non-commutative rings.

## I. Introduction

An $(n, k)$ linear code over the finite field $GF(q)$ is a $k$-dimensional subspace of the $n$-dimensional vector space $GF(q)^n$. The minimum Hamming distance, $d_{\min}$, of a linear code satisfies the inequality, $d_{\min} \leq n - k + 1$, known as the Singleton bound [9]. A code that satisfies the Singleton bound with equality is called a Maximum Distance Separable (MDS) code. It is well known [7, Chapter 11, Theorem 8] that linear MDS codes over finite fields can be characterized in terms of the square submatrices of its generator matrix. To be precise "An $(n, k)$ code $C$ over $GF(q)$ with generator matrix $[I|A]$ where $A$ is a $k \times (n-k)$ matrix over $GF(q)$ is MDS if and only if every square submatrix formed from any $i$ rows and any $i$ columns, for any $i = 1, 2, \ldots, \min\{k, n-k\}$ of $A$ is nonsingular." We generalize this result to the general case of group codes over abelian groups. A group code over a group $G$ is a subgroup of the $n$-fold direct sum of $G$, under componentwise operation. The Singleton bound holds for nonlinear codes and hence for group codes.

The motivation for the study of group codes arises because of their importance as a basic ingredient for Geometrically Uniform codes which include several important known classes of signal space codes [2]. Moreover, the additive groups of finite fields and integer residue rings are groups, respectively elementary abelian groups and cyclic groups. So, every linear code over a finite field is a group code over its additive group and similarly for linear codes

---

* Part of this correspondence appears in Proceedings of Fourth International Workshop on Algebraic and Combinatorial Coding Theory (ACCT-IV), Novgorod, Russia, September, 11–17, 1994, pp. 194–197.

*Table I.* Codewords of a (4,2,3) MDS group code over $C_2 \oplus C_2 \equiv \{e, x\} \oplus \{e, y\}$.

| | | | |
|---|---|---|---|
| $(e\ e\ e\ e)$ | $(x\ e\ xy\ xy)$ | $(y\ e\ y\ y)$ | $(xy\ e\ x\ x)$ |
| $(e\ x\ xy\ y)$ | $(x\ x\ e\ x)$ | $(y\ x\ x\ e)$ | $(xy\ x\ y\ xy)$ |
| $(e\ y\ y\ x)$ | $(x\ y\ x\ y)$ | $(y\ y\ e\ xy)$ | $(xy\ y\ xy\ e)$ |
| $(e\ xy\ x\ xy)$ | $(x\ xy\ y\ e)$ | $(y\ xy\ xy\ x)$ | $(xy\ xy\ e\ y)$ |

over integer residue rings. But, not every group code over an elementary abelian group can be made a linear code over a finite field by imposing a multiplicative structure on the elementary abelian group. This is illustrated by the code given in Table I, which is a MDS group code over the direct sum group of two cyclic groups each of order 2. This motivates the study of group codes, especially MDS group codes.

The Hamming distance properties of group codes, in particular, MDS group codes have been dealt with and several nonexistence results have been obtained [3].

Throughout the paper, we restrict our consideration to systematic group codes since the logic of the Singleton bound [9] leads to the simple characterization "A group code over $G$ of size $|G|^k$ is MDS only if the restriction of the code to any $k$ coordinates is $G^k$." This means group codes which are not equivalent to a systematic group code can not be MDS.

The content of this paper has been organized as follows: The matrix description of group codes over $G$ is given in Section 2. Definitions and basic relations concerning determinants of matrices over non-commutative rings are discussed in Section 3. Section 4 contains the main result, i.e., quasideterminant characterization of MDS group codes over $G$. Section 5 contains a detailed discussion of an example. Some concluding remarks are given in Section 5.

The following notations/conventions are used throughout the paper.

| | |
|---|---|
| $G$ | a finite abelian group |
| $\oplus$ | group operation in $G$ |
| $e$ | identity element of $G$ |
| $End(G)$ | the ring of endomorphisms of $G$ |
| $\Psi_I$ | Identity mapping from $G$ to $G$ |
| $\Psi_e$ | Mapping from $G$ to $G$ that maps all the elements to $e$ |
| $G^n$ | the $n$-fold direct product of $G$ |
| $C_M$ | the cyclic group with $M$ elements |
| $C_p^m$ | an elementary abelian group of type $(1, 1, \ldots, 1)$ ($m$ times) |
| $R$ | a non-commutative ring with identity |
| $Z_M$ | the residue class integer ring modulo $M$ |
| $GF(p^m)$ | the finite field with $p^m$ elements |
| $\|A\|_{ij}$ | $i, j$-th quasideterminant of the matrix $A$ (Definition 3 in Section 3) |
| $A^{ij}$ | the matrix obtained from $A$ by deleting the $i$-th row and the $j$-th column |
| $\equiv$ | is isomorphic to |
| $I \setminus J$ | The set of elements of $I$ excluding those that are in $J$ |

## II. Matrix Description of Group Codes

DEFINITION 1: *[1] A systematic $(n, k)$ group code over an abelian group $G$ is a subgroup of $G^n$ with order $|G|^k$ described by n-k homomorphisms $\phi_l$, $l = 1, 2, \ldots, n-k$, of $G^k$ onto $G$. Its codewords are of the form $(x_1, \ldots, x_k, x_{k+1}, \ldots, x_n)$ where*

$$x_{k+l} = \phi_l(x_1, \ldots, x_k) = \bigoplus_{j=1}^{k} \phi_l(e, \ldots, e, x_j, e, \ldots, e), \quad l = 1, 2, \ldots, n-k, \tag{1}$$

*and e is the identity element of $G$.*

Every codeword of a $(k+s, k)$ group code over $G$ is of the form

$$\begin{aligned}(x_1, x_2, \ldots, x_k, x_{k+1}, x_{k+2}, \ldots, x_{k+s}) &= (x_1, x_2, \ldots, x_k, \phi_1(x_1, \ldots, x_k), \\ &\quad \phi_2(x_1, \ldots, x_k), \ldots, \phi_s(x_1, \ldots, x_k)) \\ &= (x_1, x_2, \ldots, x_k, \psi_{11}(x_1) \oplus \cdots \oplus \\ &\quad \psi_{k1}(x_k), \ldots, \psi_{1s}(x_1) \oplus \cdots \oplus \psi_{ks}(x_k))\end{aligned} \tag{2}$$

where $x_i \in G, i = 1, 2, \ldots, k, \quad \psi_{jl} \in End(G), j = 1, 2, \ldots, k, 1 \leq l \leq s$. The homomorphism $\phi_l$ is said to decompose in terms of elements of $End(G)$ and is written as

$$\phi_l = \psi_{1l}\psi_{2l}\cdots\psi_{kl}, \quad 1 \leq l \leq s.$$

DEFINITION 2: *For a $(k+s, k)$ group code $L$ over $G$, defined by the homomorphisms $\{\phi_1, \phi_2, \ldots, \phi_s\}$, the $k \times s$ matrix over $End(G)$, denoted by $\Psi$,*

$$\Psi = \begin{bmatrix} \psi_{11} & \psi_{12} & \cdots & \psi_{1s} \\ \psi_{21} & \psi_{22} & \cdots & \psi_{2s} \\ \vdots & \vdots & \ldots & \vdots \\ \psi_{k1} & \psi_{k2} & \cdots & \psi_{ks} \end{bmatrix} \tag{3}$$

*where $\phi_l = \psi_{1l}\psi_{2l}\cdots\psi_{kl}$, for $l = 1, 2, \ldots, s$, is called the associated matrix of the code $L$.*

Every matrix of the form (3) defines a $(k+s, k)$ group code over $G$. Moreover, this matrix when operates on an element $(x_1, x_2, \ldots, x_k) \in G^k$ (information vector) gives the check vector $(x_{k+1}, x_{k+2}, \ldots, x_{k+s})$ as given below:

$$[x_{k+1}x_{k+2}\cdots x_{k+s}] = [x_1 x_2 \cdots x_k]\Psi$$

or

$$[x_{k+1}x_{k+2}\cdots x_{k+s}]^{tr} = \Psi^{tr}[x_1 x_2 \cdots x_k]^{tr},$$

where,

$$x_{k+l} = \psi_{1l}(x_1) \oplus \psi_{2l}(x_2) \oplus \cdots \psi_{kl}(x_k) \quad l = 1, 2, \ldots, s.$$

The generator matrix denoted by $\Lambda$, which when operates on an information vector gives the corresponding codeword, is given by

$$\Lambda = \left[\begin{array}{cccc|cccc} \psi_I & \psi_e & \cdots & \psi_e & \psi_{11} & \psi_{12} & \cdots & \psi_{1s} \\ \psi_e & \psi_I & \cdots & \psi_e & \psi_{21} & \psi_{22} & \cdots & \psi_{2s} \\ \vdots & \vdots & \dots & \vdots & \vdots & \vdots & \dots & \vdots \\ \psi_e & \psi_e & \cdots & \psi_I & \psi_{k1} & \psi_{k2} & \cdots & \psi_{ks} \end{array}\right] \tag{4}$$

The associated matrix $\Psi$ in (3) is over $End(G)$ which is a non-commutative ring. In the case of linear codes over $GF(p^m)$ the associated matrix $\Psi$ is also over $GF(p^m)$. In the case of codes over $C_M$ the associated matrix is over $Z_M$, a commutative ring. In general for group codes over $G$ the associated matrix is over a non-commutative ring and the conventional notions like determinant and singularity of the matrices do not carry over directly. The counterpart of these notions for matrices over a non-commutative ring is discussed in detail in [4,5] and the notions and properties required for our purposes are discussed in the next section.

## III. Determinants of Matrices Over Non-Commutative Rings

Let $R$ be a non-commutative ring with identity and

$$A = (a_{ij}), i, j \in I = \{1, 2, \dots, n\},$$

be a $n \times n$ matrix over $R$.

DEFINITION 3: *[4] [5] For any $n \times n$ matrix $A$ over $R$, the $n^2$ quasideterminants, denoted by $|A|_{ij}$, are defined by induction as follows: For $n = 1, |A|_{11} = a_{11}$. Suppose that quasideterminants for all matrices of order less than n are already defined. Let$A^{\alpha\beta}$ be the $(n-1) \times (n-1)$ matrix obtained from $A$ by deleting the $\alpha$-th row and the $\beta$-th column. The quasideterminant with index $pq$ is defined as follows*

$$|A|_{pq} = a_{pq} - \sum_{i \neq p, j \neq q} a_{pj} |A^{pq}|_{ij}^{-1} a_{iq}$$

For example, for a $2 \times 2$ matrix $A = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix}$ the four quasideterminants are

$$\begin{aligned} |A|_{11} &= a_{11} - a_{12} a_{22}^{-1} a_{21}; \\ |A|_{12} &= a_{12} - a_{11} a_{21}^{-1} a_{22}; \\ |A|_{21} &= a_{21} - a_{22} a_{12}^{-1} a_{11}; \\ |A|_{22} &= a_{22} - a_{21} a_{11}^{-1} a_{12}; \end{aligned}$$

For $P$ and $Q$ subsets of $I$ with $|P| = |Q|$, let $A^{P,Q}$ be the submatrix of the matrix $A$ obtained by deleting the rows with indices $p \in P$, and the columns with indices $q \in Q$, and also let $A_{P,Q} = A^{I\setminus P, I\setminus Q}$, and $P_i = P \cup \{i\}$ and $Q_j = Q \cup \{j\}$. Construct the matrix

$$B = (b_{kl}), k \in I\setminus P, l \in I\setminus Q, \ where\ b_{kl} = |A_{P_k,Q_l}|_{kl}.$$

The following Theorem, known as the Sylvester identity is proved in [4]:

THEOREM 1 [4]: *For* $k \in I\setminus P, l \in I\setminus Q$,

$$|A|_{kl} = |B|_{kl} \tag{5}$$

*From the Sylvester identity it follows that a quasideterminant of an* $n \times n$ *matrix* $A$ *is expressed either via a quasideterminant of a* $2\times 2$ *matrix consisting of four quasideterminants of* $(n-1)\times(n-1)$ *submatrices of* $A$ *or via a quasideterminant of an* $(n-1)\times(n-1)$ *matrix consisting of* $(n-1)^2$ *quasideterminants of* $2\times 2$ *submatrices of* $A$.

DEFINITION 4: *[5] For* $A^{L,M}$ *where* $|L| = |M| = k$, $p \notin L, q \notin M$, *the quasideterminant* $|A^{L,M}|_{pq}$ *is said to be a k-quasiminor of* $A$.

The following relations, obtained in [5, corollary 1.3.3],

$$|A|_{ij}|A^{il}|_{pj}^{-1} = -|A|_{il}|A^{ij}|_{pl}^{-1} \ for\ \ l \neq j, p \neq i \tag{6}$$

$$|A^{kj}|_{iq}^{-1}|A|_{ij} = -|A^{ij}|_{kq}|^{-1}|A|_{kj} \ for\ \ i \neq k, q \neq j \tag{7}$$

and the following two lemmas will be used to prove the main result of this paper, Theorem 2 in the next section.

LEMMA 1: *Let* $A = (a_{ij})$ *be an* $n\times n$ *matrix over* $R$ *such that all square smaller submatrices of orders* $1, 2, \ldots, (n-1)$, *are invertible. If one of the quasideterminants of* $A$ *is invertible then its all other quasideterminants are also invertible.*

*Proof.* Given as Appendix 1. ■

LEMMA 2: *Let* $A = (a_{ij})$ *be an invertible* $n \times n$ *matrix over* $R$ *such that all smaller square submatrices are invertible. Then all its* $n^2$ *quasideterminants are invertible.*

*Proof.* Given as Appendix 2. ■

## IV. Quasideterminant Characterization

The main result, i.e., Theorem 2, which characterizes MDS group codes over abelian groups in terms of quasideterminants of the square submatrices of the associated matrix of the code, is obtained in this section.

LEMMA 3: *A $(k+s, k)$ group code L over G, defined by the homomorphisms $\{\phi_1, \phi_2, \ldots, \phi_s\}$, is MDS iff every square submatrix of its associated matrix of the form*

$$\Psi_h = \begin{bmatrix} \psi_{i_1 j_1} & \psi_{i_1 j_2} & \cdots & \psi_{i_1 j_h} \\ \psi_{i_2 j_1} & \psi_{i_2 j_2} & \cdots & \psi_{i_2 j_h} \\ \vdots & \vdots & \cdots & \vdots \\ \psi_{i_h j_1} & \psi_{i_h j_2} & \cdots & \psi_{i_h j_h} \end{bmatrix} \tag{8}$$

*for $1 \leq i_k, j_k \leq h$, $k = 1, 2, \ldots, h$, and $h = 1, 2, \ldots, \min\{s, k\}$, represents an automorphism of $G^h$.*

*Proof.* Let the associated matrix of $L$ be $\Psi$ as given in (3). Suppose all $h \times h$ submatrices, $h = 1, 2, \ldots, \min\{s, k\}$, of $\Psi$ are automorphisms of $G^h$. Let

$$\underline{\mu} = (\mu_1, \mu_2, \ldots, \mu_k, \mu_{k+1}, \ldots, \mu_{k+s})$$

be a codeword in $L$. We have

$$\mu_{k+t} = \psi_{1t}(\mu_1) \oplus \psi_{2t}(\mu_2) \oplus \cdots \oplus \psi_{kt}(\mu_k) \quad t = 1, 2, \ldots, s.$$

Suppose in $\{\mu_1, \mu_2, \ldots, \mu_k\}$, only $h$ elements are nonzero, those with indices $j_1, j_2, \ldots, j_h$. Then the following equations hold:

$$\mu_{k+t} = \psi_{j_1 t}(\mu_{j_1}) \oplus \psi_{j_2 t}(\mu_{j_2}) \oplus \cdots \oplus \psi_{j_h t}(\mu_{j_h}) \quad t = 1, 2, \ldots, s.$$

Suppose $h$ of the $\mu_{k+t}$, with indices $k + i_1, k + i_2, \ldots, k + i_h$ are zeros. Then, we have

$$\mu_{k+t} = e = \psi_{j_1 t}(\mu_{j_1}) \oplus \psi_{j_2 t}(\mu_{j_2}) \oplus \cdots \oplus \psi_{j_h t}(\mu_{j_h}) \quad t = i_1, i_2, \ldots, i_h.$$

But since every $h \times h$ of the form (8) represents an automorphism of $G^h$, the set of equations above imply $\mu_{j_1} = \mu_{j_2} = \cdots = \mu_{j_h} = e$, which is not true. Hence the weight of $\underline{\mu}$ is at least $h + s - h + 1 = s + 1$. Therefore $L$ is MDS.

To prove the converse, let $L$ be MDS and $L'$ be the group code consisting of the codewords $(x_1, \ldots, x_{k+s})$ in $L$ satisfying $x_i = 0$ for $i \in \{1, 2, \ldots, k\} \backslash \{j_1, j_2, \ldots, j_h\}$. Then let $L^*$ denote the group code obtained from $L'$ by dropping all the components except the components with indices $\{j_1, j_2, \ldots, j_h, k + i_1, k + i_2, \ldots, k + i_h\}$ i.e., $L^*$ is a $(2h, h)$ group code. Let the associated matrix of $L^*$ be denoted by $\Delta_h$.$L^*$ is also MDS and hence the minimum distance of $L^*$ is $h + 1$. Consider the following matrix equation

$$\Lambda_h[\gamma_1 \;\; \gamma_2 \;\; \cdots \;\; \gamma_h]^{tr} = [e \;\; e \;\; \cdots \;\; e]^{tr},$$

where $[\gamma_1 \;\; \gamma_2 \;\; \cdots \;\; \gamma_h] \in G^h$. If a non-all $e$ vector $[\gamma_1 \;\; \gamma_2 \;\; \cdots \;\; \gamma_h]$ exists satisfying the above matrix equation, then the vector $\underline{\gamma} = [\gamma_1, \gamma_2, \ldots, \gamma_h, e, e, \ldots, e]$, of length $2h$, is a codeword of $L^*$. But the weight of $\underline{\gamma}$ is $\leq h$. Since $L^*$ is MDS it follows that $\underline{\gamma}$ is an all $e$ vector which means $\Delta_h$ represents an automorphism of $G^h$. ■

The following corollary is an immediate consequence of Lemma 3.

COROLLARY 1: *In an MDS group code over $G$, symbols of any $k$ locations can be taken as information symbols and the rest as check symbols.*

From lemma 3 it follows that a necessary condition for the associated matrix to represent a MDS group code is that all smaller square submatrices of $\Psi$ are invertible.

THEOREM 2: *A $(k+s,k)$ group code $L$ over $G$, defined by (3), is MDS iff for every square submatrix of its associated matrix of the form*

$$\Psi_{h\times h} = \begin{bmatrix} \psi_{i_1 j_1} & \psi_{i_1 j_2} & \cdots & \psi_{i_1 j_h} \\ \psi_{i_2 j_1} & \psi_{i_2 j_2} & \cdots & \psi_{i_2 j_h} \\ \vdots & \vdots & \dots & \vdots \\ \psi_{i_h j_1} & \psi_{i_h j_2} & \cdots & \psi_{i_h j_h} \end{bmatrix} \tag{9}$$

*for $1 \le i_r, j_r \le h$, $r = 1, 2, \dots, h$, and $h = 1, 2, \dots, \min\{s, k\}$, one of its quasideterminants is an automorphism of $G$.*

*Proof.* From Lemma 3, it is sufficient to prove the following: Every $h \times h$ submatrix of the associated matrix of the code represents an automorphism of $G^h$, $h = 1, 2, \dots, \min\{s, k\}$, if and only if one of its $h^2$ quasideterminants is an automorphism of $G$.

The proof is by induction on $h$.

For $h = 1$ this is clear, since the quasideterminant of $\Psi_h$ is its one entry.

For $h = 2$, consider a $2 \times 2$ submatrix of $\Psi$ of the form $\Psi_{2\times 2} = \begin{bmatrix} \psi_{i_1 j_1} & \psi_{i_1 j_2} \\ \psi_{i_2 j_1} & \psi_{i_2 j_2} \end{bmatrix}$, whose entries are invertible, i.e., automorphisms of $G$. For this matrix the four quasideterminants exist and are given by:

$$\begin{aligned} |\Psi|_{i_1 j_1} &= \psi_{i_1 j_1} - \psi_{i_1 j_2}\psi^{-1}_{i_2 j_2}\psi_{i_2 j_1}; \\ |\Psi|_{i_1 j_2} &= \psi_{i_1 j_2} - \psi_{i_1 j_1}\psi^{-1}_{i_2 j_1}\psi_{i_2 j_2}; \\ |\Psi|_{i_2 j_1} &= \psi_{i_2 j_1} - \psi_{i_2 j_2}\psi^{-1}_{i_1 j_2}\psi_{i_1 j_1}; \\ |\Psi|_{i_2 j_2} &= \psi_{i_2 j_2} - \psi_{i_2 j_1}\psi^{-1}_{i_1 j_1}\psi_{i_1 j_2}; \end{aligned}$$

Let $|\Psi|_{i_2 j_2}$ be an automorphism of $G$. We shall show that $\Psi_{2\times 2}$ represents an automorphism of $G^2$. Let

$$\begin{bmatrix} \psi_{i_1 j_1} & \psi_{i_1 j_2} \\ \psi_{i_2 j_1} & \psi_{i_2 j_2} \end{bmatrix} \begin{bmatrix} x_{i_1} \\ x_{i_2} \end{bmatrix} = \begin{bmatrix} e \\ e \end{bmatrix}.$$

By applying the following elementary row operations

$$R_1 \to \psi^{-1}_{i_1 j_1} R_1;\ R_2 \to \psi^{-1}_{i_2 j_1} R_2;\ R_2 \to R_2 - R_1;\ R_2 \to \psi_{i_2 j_1} R_2,$$

on $\Psi_{2\times 2}$, where $R_i$, $i = 1, 2$, denotes the $i$-th row, we obtain

$$\begin{bmatrix} 1 & \psi^{-1}_{i_1 j_1}\psi_{i_1 j_2} \\ 0 & |\Psi_{2\times 2}|_{22} \end{bmatrix}$$

which is row equivalent to $\Psi_{2\times 2}$. Hence we have

$$\begin{bmatrix} 1 & \psi_{i_1 j_1}^{-1}\psi_{i_1 j_2} \\ 0 & |\Psi_{2\times 2}|_{22} \end{bmatrix} \begin{bmatrix} x_{i_1} \\ x_{i_2} \end{bmatrix} = \begin{bmatrix} e \\ e \end{bmatrix},$$

which means $|\Psi_{2\times 2}|_{22}(x_{i_2}) = e$, i.e., $x_{i_2} = e$, and using this in $x_{i_1} \oplus \psi_{i_1 j_1}^{-1}\psi_{i_1 j_2}(x_{i_2}) = e$ gives $x_{i_1} = e$. Hence the invertibility of $|\Psi_{2\times 2}|_{22}$ implies the invertibility of $\Psi_{2\times 2}$.

Conversely, let $\Psi_{2\times 2}$ be invertible and all its entries are also invertible. Then by Lemma (2) all the four quasideterminants of $\Psi_{2\times 2}$ are invertible.

Now assuming that for all square submatrices of orders $1, 2, \ldots, (h-1)$, of $\Psi_{h\times h}$, every one of them is invertible iff one of its quasideterminants is invertible, we shall show that $\Psi_{h\times h}$ is invertible iff one of its quasideterminants is invertible.

Let the $h \times h$ matrix under consideration be

$$\Psi_{h\times h} = \begin{bmatrix} \psi_{11} & \psi_{12} & \cdots & \psi_{1h} \\ \psi_{21} & \psi_{22} & \cdots & \psi_{2h} \\ \vdots & \vdots & \ldots & \vdots \\ \psi_{h1} & \psi_{h2} & \cdots & \psi_{hh} \end{bmatrix}$$

(To avoid clumsiness in the notation this matrix is assumed without loss of generality, instead of the matrix in the statement of the theorem.)

Let $|\Psi_{h\times h}|_{hh}$ be invertible.

By successive applications of the same elementary row operations given in the proof of Lemma 2, on $\Psi_{h\times h}$, we will obtain the matrix given below which is row equivalent to $\Psi_{h\times h}$:

$$\begin{bmatrix} 1 & \psi_{11}^{-1}\psi_{12} & \psi_{11}^{-1}\psi_{13} & & \psi_{11}^{-1}\psi_{1(h-1)} & \psi_{11}^{-1}\psi_{1h} \\ 0 & 1 & |\Psi_{P_2Q_2}|_{22}^{-1}|\Psi_{P_2Q_3}|_{23} & & |\Psi_{P_2Q_2}|_{22}^{-1}|\Psi_{P_2Q_{h-1}}|_{2(h-1)} & |\Psi_{P_2Q_2}|_{22}^{-1}|\Psi_{P_2Q_h}|_{2h} \\ 0 & 0 & 1 & & |\Psi_{P_3^{(1)}Q_3^{(1)}}|_{33}^{-1}|\Psi_{P_3^{(1)}Q_{h-1}^{(1)}}|_{3(h-1)}^{-1} & |\Psi_{P_3^{(1)}Q_3^{(1)}}|_{33}^{-1}|\Psi_{P_3^{(1)}Q_h^{(1)}}|_{3h} \\ \vdots & \vdots & \vdots & \cdots & \vdots & \vdots \\ 0 & 0 & 0 & & 1 & |\Psi_{P_{h-1}^{(h-3)}Q_{h-1}^{(h-3)}}|_{(h-1)(h-1)}^{-1}|\Psi_{P_{h-1}^{(h-3)}Q_h^{(h-3)}}|_{(h-1)h} \\ 0 & 0 & 0 & & 0 & |\Psi_{P_h^{(h-2)}Q_h^{(h-2)}}|_{hh} \end{bmatrix} \quad (10)$$

where the sets $P^{(1)}, P^{(2)}, \ldots, P^{(h-2)}, Q^{(1)}, Q^{(2)}, \ldots, Q^{(h-2)}$ are same as given in the proof of Lemma 2. In view of this row equivalence the solution of the system of equations

$$\Psi_{h\times h}\begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_h \end{bmatrix} = \begin{bmatrix} e \\ e \\ \vdots \\ e \end{bmatrix} \tag{11}$$

is also the solution of the system of equations given by

$$\left[\begin{matrix} 1 & \psi_{11}^{-1}\psi_{12} & \psi_{11}^{-1}\psi_{13} & \cdots & \psi_{11}^{-1}\psi_{1(h-1)} \\ 0 & 1 & |\Psi_{P_2Q_2}|_{22}^{-1}|\Psi_{P_2Q_3}|_{23} & \cdots & |\Psi_{P_2Q_2}|_{22}^{-1}|\Psi_{P_2Q_{h-1}}|_{2(h-1)} \\ 0 & 0 & 1 & \cdots & |\Psi_{P_3^{(1)}Q_3^{(1)}}|_{33}^{-1}|\Psi_{P_3^{(1)}Q_{h-1}^{(1)}}|_{3(h-1)}^{-1} \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \\ 0 & 0 & 0 & \cdots & 0 \end{matrix}\right.$$

$$\left.\begin{matrix} \psi_{11}^{-1}\psi_{1h} \\ |\Psi_{P_2Q_2}|_{22}^{-1}|\Psi_{P_2Q_h}|_{2h} \\ |\Psi_{P_3^{(1)}Q_3^{(1)}}|_{33}^{-1}|\Psi_{P_3^{(1)}Q_h^{(1)}}|_{3h} \\ \vdots \\ |\Psi_{P_{h-1}^{(h-3)}Q_{h-1}^{(h-3)}}|_{(h-1)(h-1)}^{-1}|\Psi_{P_{h-1}^{(h-3)}Q_h^{(h-3)}}|_{(h-1)h} \\ |\Psi_{P_h^{(h-2)}Q_h^{(h-2)}}|_{hh} \end{matrix}\right]\begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_h \end{bmatrix} = \begin{bmatrix} e \\ e \\ \vdots \\ e \end{bmatrix} \tag{12}$$

Since the $(h, h)$-th entry of the matrix given in (12) is $|\Psi_{h\times h}|_{hh}$, we have

$$|\Psi_{h\times h}|_{hh}(x_h) = e$$

which means $x_h = e$, since $|\Psi_{h\times h}|_{hh}$ is invertible.

Next by back substitution one can obtain $x_1 = x_2 = \cdots = x_{h-1} = x_h = e$, which means $\Psi_{h\times h}$ is invertible or equivalently it represents an automorphism of $G^h$.

Conversely, given that $\Psi_{h\times h}$ and all its square submatrices are invertible, from Lemma 2 it follows that all its $h^2$ quasideterminants are invertible.

This completes the proof. ■

## V. Example

For the purpose of illustration let us consider the length 6 MDS group code over $C_2 \oplus C_2 = \{0, 1\} \oplus \{0, 1\} = \{00, 10, 01, 11\} = \{e, x, y, xy\}$. consisting of 64 codewords listed in Table II. There are only 6 automorphisms of $C_2 \oplus C_2$ listed below along with their inverses for quick reference.

| | | | | | | |
|---|---|---|---|---|---|---|
| Automorphism | $\begin{bmatrix}1&0\\0&1\end{bmatrix}$ | $\begin{bmatrix}0&1\\1&0\end{bmatrix}$ | $\begin{bmatrix}1&1\\1&0\end{bmatrix}$ | $\begin{bmatrix}0&1\\1&1\end{bmatrix}$ | $\begin{bmatrix}1&1\\0&1\end{bmatrix}$ | $\begin{bmatrix}1&0\\1&1\end{bmatrix}$ |
| Inverse | $\begin{bmatrix}1&0\\0&1\end{bmatrix}$ | $\begin{bmatrix}0&1\\1&0\end{bmatrix}$ | $\begin{bmatrix}0&1\\1&1\end{bmatrix}$ | $\begin{bmatrix}1&1\\1&0\end{bmatrix}$ | $\begin{bmatrix}1&1\\0&1\end{bmatrix}$ | $\begin{bmatrix}1&0\\1&1\end{bmatrix}$ |

The associated matrix of this code is

$$A_{3\times 3} = \begin{bmatrix}\psi_{11} & \psi_{12} & \psi_{13}\\ \psi_{21} & \psi_{22} & \psi_{23}\\ \psi_{31} & \psi_{32} & \psi_{33}\end{bmatrix} = \begin{bmatrix}\begin{bmatrix}1&1\\0&1\end{bmatrix} & \begin{bmatrix}0&1\\1&1\end{bmatrix} & \begin{bmatrix}1&0\\0&1\end{bmatrix}\\ \begin{bmatrix}0&1\\1&0\end{bmatrix} & \begin{bmatrix}1&0\\0&1\end{bmatrix} & \begin{bmatrix}1&0\\0&1\end{bmatrix}\\ \begin{bmatrix}1&1\\0&1\end{bmatrix} & \begin{bmatrix}1&0\\0&1\end{bmatrix} & \begin{bmatrix}0&1\\1&1\end{bmatrix}\end{bmatrix}$$

Using the Sylvester Identity a quasideterminant of $A_{3\times 3}$ will be written as quasideterminant of $2 \times 2$ matrix of the following submatrices:

| | |
|---|---|
| $A_{\{1,2\}\{1,2\}} = \begin{bmatrix}\begin{bmatrix}1&1\\0&1\end{bmatrix} & \begin{bmatrix}0&1\\1&1\end{bmatrix}\\ \begin{bmatrix}0&1\\1&0\end{bmatrix} & \begin{bmatrix}1&0\\0&1\end{bmatrix}\end{bmatrix}$ | $A_{\{1,2\}\{1,3\}} = \begin{bmatrix}\begin{bmatrix}1&1\\0&1\end{bmatrix} & \begin{bmatrix}1&0\\0&1\end{bmatrix}\\ \begin{bmatrix}0&1\\1&0\end{bmatrix} & \begin{bmatrix}1&0\\0&1\end{bmatrix}\end{bmatrix}$ |
| $b_{22} = \lvert A_{\{1,2\}\{1,2\}}\rvert_{22} = \begin{bmatrix}0&1\\1&1\end{bmatrix}$ | $b_{23} = \lvert A_{\{1,2\}\{1,3\}}\rvert_{23} = \begin{bmatrix}1&1\\1&0\end{bmatrix}$ |

$$A_{\{1,3\}\{1,2\}} = \begin{bmatrix} \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} & \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix} \\ \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} & \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \end{bmatrix} \quad A_{\{1,3\}\{1,3\}} = \begin{bmatrix} \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} & \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \\ \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} & \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix} \end{bmatrix}$$

$$b_{32} = |A_{\{1,3\}\{1,2\}}|_{32} = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} \qquad b_{33} = |A_{\{1,3\}\{1,3\}}|_{33} = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}$$

We have

$$B = \begin{bmatrix} b_{22} & b_{23} \\ b_{32} & b_{33} \end{bmatrix}$$

and

$$|A|_{22} = |B|_{22} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

$$|A|_{23} = |B|_{23} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

$$|A|_{32} = |B|_{32} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

$$|A|_{33} = |B|_{33} = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}$$

## VI. Discussion

When specialized to group codes over elementary abelian groups, say $C_p^m$, the associated matrix becomes a matrix over a matrix ring over the finite field $GF(p)$. The structure of these matrix rings is well studied [8]. The associated matrix still remains a matrix over a non-commutative ring. Imposing a multiplicative structure on $C_p^m$ and making it the field $GF(p^m)$, the associated matrix becomes a matrix over $GF(p^m)$, and Theorem 2 reduces to the well known characterization of MDS codes over finite fields [7, Chapter 11, Theorem 8].

When specialized to group codes over cyclic groups $C_M$, the associated matrix becomes a matrix over a commutative ring $Z_M$, and Theorem 2 reduces to a simple form, i.e., a group code over $C_M$ is MDS iff all square submatrices of its associated matrices have determinant a unit in $Z_M$.

*Table 2.* Listing of codewords of Example in Section 5.

| | | | |
|---|---|---|---|
| (e,e,e,e,e,e) | (x,e,e,x,y,x) | (y,e,e,xy,x,xy) | (xy,e,e,y,xy,y) |
| (e,e,x,x,x,y) | (x,e,x,e,xy,xy) | (y,e,x,y,e,x) | (xy,e,x,xy,y,e) |
| (e,e,y,y,y,xy) | (x,e,y,xy,e,y) | (y,e,y,x,xy,e) | (xy,e,y,e,x,x) |
| (e,e,xy,xy,xy,x) | (x,e,xy,y,x,e) | (y,e,xy,e,y,y) | (xy,e,xy,x,e,xy) |
| (e,x,e,y,x,x) | (x,x,e,xy,xy,e) | (y,x,e,x,e,y) | (xy,x,e,e,y,xy) |
| (e,x,x,xy,e,xy) | (x,x,x,y,y,y) | (y,x,x,e,x,e) | (xy,x,x,x,xy,x) |
| (e,x,y,e,xy,y) | (x,x,y,x,x,xy) | (y,x,y,xy,y,x) | (xy,x,y,y,e,e) |
| (e,x,xy,x,y,e) | (x,x,xy,e,e,x) | (y,x,xy,y,xy,xy) | (xy,x,xy,xy,x,y) |
| (e,y,e,xy,y,y) | (x,y,e,y,e,xy) | (y,y,e,e,xy,x) | (xy,y,e,x,x,e) |
| (e,y,x,y,xy,e) | (x,y,x,xy,x,x) | (y,y,x,x,y,xy) | (xy,y,x,e,e,y) |
| (e,y,y,x,e,x) | (x,y,y,e,y,e) | (y,y,y,y,x,y) | (xy,y,y,xy,xy,xy) |
| (e,y,xy,e,x,xy) | (x,y,xy,x,xy,y) | (y,y,xy,xy,e,e) | (xy,y,xy,y,y,x) |
| (e,xy,e,x,xy,xy) | (x,xy,e,e,x,y) | (y,xy,e,y,y,e) | (xy,xy,e,xy,e,x) |
| (e,xy,x,e,y,x) | (x,xy,x,x,e,e) | (y,xy,x,xy,xy,y) | (xy,xy,x,y,x,xy) |
| (e,xy,y,xy,x,e) | (x,xy,y,y,xy,x) | (y,xy,y,e,e,xy) | (xy,xy,y,x,y,y) |
| (e,xy,xy,y,e,y) | (x,xy,xy,xy,y,xy) | (y,xy,xy,x,x,x) | (xy,xy,xy,e,xy,e) |

Theorem 2 does not extend to group codes over nonabelian groups since the set of endomorphisms of a nonabelian group form a near-ring [6] which is more general than a non-commutative ring. It would be interesting to develop the counterpart of the notion of quasideterminant, to matrices over near-rings and extend Theorem 2 to group codes over nonabelian groups.

## Appendix 1

**Proof of Lemma 1:** The proof is by induction on $n$ the order of the matrix $A$. For $n = 1$, the lemma 1 is true. For $n = 2$, we have $A_{2\times 2} = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix}$ where the entries are invertible. Without loss of generality let $|A_{2\times 2}|_{22}$ be invertible. In eq. (6), putting $i = j = 2$ and $p = l = 1$, we obtain the following relation

$$|A_{2\times 2}|_{22} = -|A_{2\times 2}|_{21} a_{11}^{-1} a_{12}$$

from which we conclude that $|A_{2\times 2}|_{21}$ is invertible. In eq. (7) if we put $i = j = 2$ and $k = q = 1$, we obtain

$$|A_{2\times 2}|_{22} = -a_{21} a_{11}^{-1} |A_{2\times 2}|_{12}$$

from which we conclude that $|A_{2\times 2}|_{12}$ is invertible. By putting $i = 1$, $j = 2$, $p = 2$, $l = 1$, in eq. (6) we obtain

$$|A_{2\times 2}|_{12} = -|A_{2\times 2}|_{11} a_{21}^{-1} a_{22}$$

from which it follows that $|A|_{11}$ is invertible.

Induction Hypothesis: The lemma is true for $(n-1)$.

Without loss of generality let the quasideterminant $|A|_{nn}$ of $A$ be invertible. By putting $i = j = n, p = 1, l = 1, 2, \ldots, (n-1)$, in eq. (6), we obtain the following (n-1) relations:

$$\begin{aligned}
|A|_{nn} &= -|A|_{n1}|A^{nn}|_{11}^{-1}|A^{n1}|_{1n} \\
|A|_{nn} &= -|A|_{n2}|A^{nn}|_{12}^{-1}|A^{n2}|_{1n} \\
\cdots &= \cdots \\
\cdots &= \cdots \\
|A|_{nn} &= -|A|_{n(n-1)}|A^{nn}|_{1(n-1)}^{-1}|A^{n(n-1)}|_{1n}
\end{aligned}$$

From the above set of equations it follows that $|A|_{nl}$, for $l = 1, 2, \ldots, (n-1)$ are invertible. By putting $i = j = n$, $q = 1, k = 1, 2, \ldots, (n-1)$, in eq. (7), we obtain the following $(n-1)$ relations:

$$\begin{aligned}
|A|_{nn} &= -|A^{1n}|_{n1}|A^{nn}|_{11}^{-1}|A|_{1n} \\
|A|_{nn} &= -|A^{2n}|_{n1}|A^{nn}|_{21}^{-1}|A|_{2n} \\
\cdots &= \cdots \\
\cdots &= \cdots \\
|A|_{nn} &= -|A^{(n-1)n}|_{n1}|A^{nn}|_{(n-1)1}^{-1}|A|_{(n-1)n}
\end{aligned}$$

From these relations it follows that $|A|_{kn}$ is invertible for $k = 1, 2, \ldots, (n-1)$.

In the same manner, using eq. (6), one can check that

$|A|_{(n-1)l}, l = 1, 2, \ldots, (n-1)$ are invertible by putting $j = n,\ i = (n-1),\ p = 1,\ l = 1, 2, \ldots, (n-1)$,

$|A|_{(n-2)l}, l = 1, 2, \ldots, (n-1)$ are invertible by putting $j = n,\ i = (n-2),\ p = 1,\ l = 1, 2, \ldots, (n-1)$,

$\vdots$

$|A|_{1l}, l = 1, 2, \ldots, (n-1)$ are invertible by putting $j = n,\ i = 1,\ p = 1,\ l = 1, 2, \ldots, (n-1)$,

So, we conclude that all the quasideterminants of $A$ are invertible.

This completes the proof. ∎

## Appendix 2

**Proof of Lemma 2:** By Lemma 1 it is sufficient to show that one of the $n^2$ quasideterminants of $A$ is invertible. Without loss of generality we will show that $|A|_{nn}$ is invertible.

The proof is by induction on n the order of the matrix $A$. For $n = 1$, the lemma 2 is true.

For $n = 2$, let

$$ {}_{2\times 2} = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} $$

where all the entries are invertible. Since $A_{2\times 2}$ is invertible, there exists

$$ B_{2\times 2} = \begin{bmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{bmatrix}, $$

such that $AB = BA = I_{2\times 2}$, where $I_{2\times 2}$ is the $2 \times 2$ identity matrix, i.e., $\begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix}$ $\begin{bmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ or

$$ \begin{aligned} a_{11}b_{11} \ &+ \ a_{12}b_{21} = 1 \\ a_{21}b_{11} \ &+ \ a_{22}b_{21} = 0 \\ a_{11}b_{12} \ &+ \ a_{12}b_{22} = 0 \\ a_{21}b_{12} \ &+ \ a_{22}b_{22} = 1 \end{aligned} $$

The last two equations in two unknowns $b_{12}$ and $b_{22}$ can be written in matrix form

$$ \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} \begin{bmatrix} b_{12} \\ b_{22} \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \end{bmatrix} $$

Now we apply elementary row operations

$$ R_1 \to a_{11}^{-1} R_1;\ R_2 \to a_{21}^{-1} R_2;\ R_2 \to R_2 - R_1;\ R_2 \to a_{21} R_2, $$

where $R_i$, $i = 1, 2$, denote the $i$-th row, on $A_{2\times 2}$, (which is valid since all the entries of $A_{2\times 2}$ are invertible), to obtain

$$ \begin{bmatrix} 1 & a_{11}^{-1}a_{12} \\ 0 & |A_{2\times 2}|_{22} \end{bmatrix} $$

which is row equivalent to $A_{2\times 2}$ [10]. Hence, we have

$$ \begin{bmatrix} 1 & a_{11}^{-1}a_{12} \\ 0 & |A_{2\times 2}|_{22} \end{bmatrix} \begin{bmatrix} b_{12} \\ b_{22} \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \end{bmatrix} $$

i.e. $|A_{2\times 2}|_{22} b_{22} = 1$. Similarly, by using $BA = I_{2\times 2}$, one can obtain, $b_{22}|A_{2\times 2}|_{22} = 1$. Hence, $b_{22} = |A_{2\times 2}|_{22}^{-1}$, i.e., $|A_{2\times 2}|_{22}$ is invertible. Then by Lemma 1, $|A_{2\times 2}|_{11}$, $|A_{2\times 2}|_{12}$, $|A_{2\times 2}|_{21}$ are also invertible.

Induction hypothesis: Let all square submatrices of order $1, 2, \ldots, (n-1)$ of $A$ have invertible quasideterminants.

Now we will show that the induction hypothesis is true for $A_{n\times n}$.

Let $A_{n\times n}$ be invertible, whose all smaller submatrices are also invertible, i.e., all the quasideterminants of the smaller submatrices are invertible. Since $A_{n\times n}$ is invertible there exist $B_{n\times n}$ such that $A_{n\times n}B_{n\times n} = B_{n\times n}A_{n\times n} = I_{n\times n}$.

From $A_{n\times n}B_{n\times n} = I_{n\times n}$ we have,

$$\begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \cdots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{bmatrix} \begin{bmatrix} b_{1n} \\ b_{2n} \\ \vdots \\ b_{nn} \end{bmatrix} = \begin{bmatrix} 0 \\ \vdots \\ 0 \\ 1 \end{bmatrix} \tag{A2.1}$$

By applying the following elementary operations

$R_i \to a_{i1}^{-1}R_i \;\; i = 1, 2, \ldots, n;\; R_i \to R_i - R_1 \;\; i = 2, \ldots, n;\; R_i \to a_{i1}R_i \;\; i = 2, \ldots, n,$

on $A_{n\times n}$, we obtain

$$\begin{bmatrix} 1 & a_{11}^{-1}a_{12} & \cdots & a_{11}^{-1}a_{1(n-1)} & a_{11}^{-1}a_{1n} \\ 0 & |A_{P_2Q_2}|_{22} & \cdots & |A_{P_2Q_{(n-1)}}|_{2(n-1)} & |A_{P_2Q_n}|_{2n} \\ \vdots & \vdots & \cdots & \vdots & \vdots \\ 0 & |A_{P_{(n-1)}Q_2}|_{(n-1)2} & \cdots & |A_{P_{(n-1)(n-1)}}|_{(n-1)(n-1)} & |A_{P_{(n-1)}Q_n}|_{(n-1)n} \\ 0 & |A_{P_nQ_2}|_{n2} & \cdots & |A_{P_nQ_{(n-1)}}|_{n(n-1)} & |A_{P_nQ_n}|_{nn} \end{bmatrix} \tag{A2.2}$$

In matrix (A2.2), for $i, j \geq 2$, the $(i, j)$-th entry can be written as

$$|A_{P_iQ_j}|_{ij}$$

which is the quasideterminant of index $ij$ of a $2 \times 2$ submatrix of $A$ having rows with indices $\{1, i\} = P \cup \{i\}$ where $P = \{1\}$ and columns with indices $\{1, j\} = Q \cup \{j\}$ where $Q = \{1\}$.

From the induction hypothesis, the quasideterminants of all $2\times 2$ submatrices are invertible and hence for $i, j \geq 2$, all the entries in matrix (A2.2) are invertible. So, we can apply the same elementary row operations on the $(n-1) \times (n-1)$ submatrix of the matrix (A2.2) and obtain the matrix given below:

$$\left[\begin{matrix} 1 & a_{11}^{-1}a_{12} & a_{11}^{-1}a_{13} \\ 0 & 1 & |A_{P_2Q_2}|_{22}^{-1}|A_{P_2Q_3}|_{23} \\ 0 & 0 & |A_{P_3Q_3}|_{33} - |A_{P_3Q_2}|_{32}|A_{P_2Q_2}|_{22}^{-1}|A_{P_2Q_3}|_{23} \\ \vdots & \vdots & \vdots \\ 0 & 0 & |A_{P_{(n-1)}Q_3}|_{(n-1)3} - |A_{P_{(n-1)}Q_2}|_{(n-1)2}|A_{P_2Q_2}|_{22}^{-1}|A_{P_2Q_3}|_{23} \\ 0 & 0 & |A_{P_nQ_3}|_{n3} - |A_{P_nQ_2}|_{n2}|A_{P_2Q_2}|_{22}^{-1}|A_{P_2Q_3}|_{23} \end{matrix}\right. \quad \cdots$$

$$\cdots \quad \begin{matrix} a_{11}^{-1}a_{1(n-1)} \\ |A_{P_2Q_2}|_{22}^{-1}|A_{P_2Q_{(n-1)}}|_{2(n-1)} \\ |A_{P_3Q_{(n-1)}}|_{3(n-1)} - |A_{P_3Q_2}|_{32}|A_{P_2Q_2}|_{22}^{-1}|A_{P_2Q_{(n-1)}}|_{2(n-1)} \\ \vdots \\ |A_{P_{(n-1)}Q_{(n-1)}}|_{(n-1)(n-1)} - |A_{P_{(n-1)}Q_2}|_{(n-1)2}|A_{P_2Q_2}|_{22}^{-1}|A_{P_2Q(n-1)}|_{2(n-1)} \\ |A_{P_nQ_{(n-1)}}|_{n(n-1)} - |A_{P_nQ_2}|_{n2}|A_{P_2Q_2}|_{22}^{-1}|A_{P_2Q_{(n-1)}}|_{2(n-1)} \end{matrix}$$

$$\left. \begin{matrix} a_{11}^{-1}a_{1n} \\ |A_{P_2Q_2}|_{22}^{-1}|A_{P_2Q_n}|_{2n} \\ |A_{P_3Q_n}|_{3n} - |A_{P_3Q_2}|_{32}|A_{P_2Q_2}|_{22}^{-1}|A_{P_2Q_n}|_{2n} \\ \vdots \\ |A_{P_{(n-1)}Q_n}|_{(n-1)n} - |A_{P_{(n-1)}Q_2}|_{(n-1)2}|A_{P_2Q_2}|_{22}^{-1}|A_{P_2Q_n}|_{2n} \\ |A_{P_nQ_n}|_{nn} - |A_{P_nQ_2}|_{n2}|A_{P_2Q_2}|_{22}^{-1}|A_{P_2Q_n}|_{2n} \end{matrix} \right] \tag{A2.3}$$

In matrix (A2.3), for $i, j \geq 3$, the $(i, j)$-th entry is

$$|A_{P_iQ_j}|_{ij} - |A_{P_iQ_2}|_{i2}|A_{P_2Q_2}|_{22}^{-1}|A_{P_2Q_j}|_{2j}$$

which is the quasideterminant of index $ij$ of the following $2 \times 2$ matrix

$$\begin{bmatrix} |A_{P_2Q_2}|_{22} & |A_{P_2Q_j}|_{2j} \\ |A_{P_iQ_2}|_{i2} & |A_{P_iQ_j}|_{ij} \end{bmatrix}$$

Hence for $i, j \geq 3$, the $(i, j)$-th entry can be recogized as the quasideterminant of index $ij$ of a $3 \times 3$ submatrix of $A$ having rows with indices $\{1, 2, i\}$ and columns with indices $\{1, 2, j\}$ written in terms of a quasideterminant of the $2 \times 2$ matrix consisting of quasideterminants of $2 \times 2$ submatrice of the $3 \times 3$ submatrix, i. e., for $i, j \geq 3$, the $(i, j)$-th entry can be written as

$$|A_{P_i^{(1)}Q_j^{(1)}}|_{ij}$$

where $P^{(1)} = Q^{(1)} = \{1, 2\}$; $P_i^{(1)} = P^{(1)} \cup \{i\}$ and $Q_i^{(1)} = Q^{(1)} \cup \{j\}$.

Hence matrix (A2.3) can be written as

$$\left[ \begin{matrix} 1 & a_{11}^{-1}a_{12} & a_{11}^{-1}a_{13} \\ 0 & 1 & |A_{P_2Q_2}|_{22}^{-1}|A_{P_2Q_3}|_{23} \\ 0 & 0 & |A_{P_3^{(1)}Q_3^{(1)}}|_{33} \\ \vdots & \vdots & \vdots \\ 0 & 0 & |A_{P_{(n-1)}^{(1)}Q_3^{(1)}}|_{(n-1)3} \\ 0 & 0 & |A_{P_n^{(1)}Q_3^{(1)}}|_{n3} \end{matrix} \right. \quad \cdots$$

$$\cdots \quad \left. \begin{matrix} a_{11}^{-1}a_{1(n-1)} & a_{11}^{-1}a_{1n} \\ |A_{P_2Q_2}|_{22}^{-1}|A_{P_2Q_{(n-1)}}|_{2(n-1)} & |A_{P_2Q_2}|_{22}^{-1}|A_{P_2Q_n}|_{2n} \\ |A_{P_3^{(1)}Q_{(n-1)}^{(1)}}|_{3(n-1)} & |A_{P_3^{(1)}Q_n^{(1)}}|_{3n} \\ \vdots & \vdots \\ |A_{P_{(n-1)}^{(1)}Q_{(n-1)}^{(1)}}|_{(n-1)(n-1)} & |A_{P_{(n-1)}^{(1)}Q_n^{(1)}}|_{(n-1)n} \\ |A_{P_n^{(1)}Q_{(n-1)}^{(1)}}|_{n(n-1)} & |A_{P_n^{(1)}Q_n^{(1)}}|_{nn} \end{matrix} \right] \tag{A2.4}$$

Since all the quasideterminants of all smaller submatrices of $A$ are invertible (by the induction hypothesis), we can apply the elementary operations in sequence and obtain the upper triangular matrix given below:

$$A = \begin{bmatrix} 1 & a_{11}^{-1}a_{12} & a_{11}^{-1}a_{13} & \cdots & a_{11}^{-1}a_{1(n-1)} & a_{11}^{-1}a_{1n} \\ 0 & 1 & |A_{P_2Q_2}|_{22}^{-1}|A_{P_2Q_3}|_{23} & \cdots & |A_{P_2Q_2}|_{22}^{-1}|A_{P_2Q_{(n-1)}}|_{2(n-1)} & |A_{P_2Q_2}|_{22}^{-1}|A_{P_2Q_n}|_{2n} \\ 0 & 0 & 1 & \cdots & |A_{P_3^{(1)}Q_3^{(1)}}|_{33}^{-1}|A_{P_3^{(1)}Q_{(n-1)}^{(1)}}|_{3(n-1)} & |A_{P_3^{(1)}Q_3^{(1)}}|_{33}^{-1}|A_{P_3^{(1)}Q_n^{(1)}}|_{3n} \\ \vdots & \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & |A_{P_{(n-1)}^{(n-3)}Q_{(n-1)}^{(n-3)}}|_{(n-1)(n-1)}^{-1}|A_{P_{(n-1)}^{(n-3)}Q_n^{(n-3)}}|_{(n-1)n} \\ 0 & 0 & 0 & \cdots & 0 & |A_{P_n^{(n-2)}Q_n^{(n-2)}}|_{nn} \end{bmatrix} \tag{A2.5}$$

where the sets $P^{(1)}, P^{(2)}, \ldots, P^{(n-2)}, Q^{(1)}, Q^{(2)}, \ldots, Q^{(n-2)}$ are defined as follows:

$$\begin{aligned} P^{(1)} &= Q^{(1)} &&= \{1, 2\} \\ P^{(2)} &= Q^{(2)} &&= \{1, 2, 3\} \\ &\vdots && \vdots \\ P^{(n-3)} &= Q^{(n-3)} &&= \{1, 2, \ldots, n-3, n-2\} \\ P^{(n-2)} &= Q^{(n-2)} &&= \{1, 2, \ldots, n-2, n-1\} \end{aligned}$$

(The matrix (A2.5) has been obtained from $A$ by elementary row operations. So matrix (A2.5) and $A$ are row equivalent [10].)
We have $P_n^{(n-2)} = P^{(n-2)} \cup \{n\} = I$; $Q_n^{(n-2)} = P^{(n-2)} \cup \{n\} = I$, and

$$|A_{P_n^{(n-2)}Q_n^{(n-2)}}|_{nn} = |A|_{nn}.$$

So, the syatem of equations (A2.1) can be written as

$$A' \begin{bmatrix} b_{1n} \\ b_{2n} \\ \vdots \\ b_{nn} \end{bmatrix} = \begin{bmatrix} 0 \\ \vdots \\ 0 \\ 1 \end{bmatrix}$$

which implies that

$$|A|_{nn} b_{nn} = 1$$

Similarly, starting from $B_{n\times n}A_{n\times n} = I_{n\times n}$, we can obtain

$$b_{nn}|A|_{nn} = 1$$

Hence $b_{nn} = |A|_{nn}^{-1}$, i.e., $|A|_{nn}$ is invertible. From Lemma 1, it follows that all other quasideterminants are also invertible.
This completes the proof. ■

## Acknowledgments

The authors gratefully acknowledge the anonymous reviewer for his detailed review which helped to improve the clarity of the paper and correct a mistake in Theorem 2. They would also like to express their appreciation to Mr. L. Venkata Subramaniam for preparing the Latex version of the paper.

## References

1. E. Biglieri and M. Elia, Construction of linear block codes over groups, *IEEE International Symposium on Information Theory*, San Antonio, Texas (1993).
2. G. D. Forney, Jr., Geometrically uniform codes, *IEEE Transactions on Information Theory*, Vol. IT-37, No. 5 (1991) pp. 1241–1260.
3. G. D. Forney, Jr., On the Hamming distance property of group codes, *IEEE Transactions Information Theory*, Vol. IT-38, No. 6 (1992) pp. 1797–1801.
4. I. M. Gel’fand and V. S. Retakh, Determinants of matrices over noncommutative rings, *Funktsional’nyi Analiz i Ego Prilozheniya*, Vol. 25, No. 2 (April–June 1991) pp. 13–25.
5. I. M. Gel’fand and V. S. Retakh, A theory of noncommutative determinants and characteristic functions of graphs, *Funktsional’nyi Analiz i Ego Prilozheniya*, Vol. 26, No. 4 (Oct.–Dec.) pp. 1–20.
6. James R. Clay, *Near Rings, Geneses and Applications*, Oxford University Press (1992).
7. F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error Correcting Codes*, North-Holland (1977).
8. B. R. McDonald, *Finite Rings with Identity*, Marcel Dekker, New York (1974).
9. Singleton, Maximum distance q-ary codes, *IEEE Transactions on Information Theory*, Vol. IT-10 (1964) pp. 116–118.
10. T. W. Hungerford, *Algebra*, Chapter VII, Springer-Verlag (1989).