An Algorithm for Constructing Random Inverses of Non-Square Matrices Across Arbitrary Fields

Farshid Haidary Makouí 1, Aaron Gulliver 1, and Mohammad Dakhilalian 1

1Affiliation not available

October 31, 2023

Abstract

In the realm of linear algebra, the notion of matrix inversion plays a crucial role. While the inversion of square matrices is well-known and results in a unique inverse, however, the non-square inverse matrix is not unique and in fact, the number of inverses for a non-square matrix can be as vast as $q^m(n-m)$, where $q$ signifies the order of the underlying field. In this paper, we embark on a journey to construct these elusive inverse matrices, harnessing the power of arbitrary fields. Arbitrary fields, including prime fields, finite fields, real fields, and complex fields. These fields find practical applications that are essential to contemporary technology. I have written 5 MATLAB programs that able to construct random inverses in different fields based on the given algorithm.
An Algorithm for Constructing Random Inverses of Non-Square Matrices Across Arbitrary Fields

Farshid Haidary Makoui\textsuperscript{1}, T. Aaron Gulliver\textsuperscript{1}, and Mohammad Dakhilalian\textsuperscript{2}

\textsuperscript{1}Department of Electrical and Computer Engineering, University of Victoria, Victoria, B.C., Canada. email: makoui@uvic.ca, agullive@ece.uvic.ca
\textsuperscript{2}Department of Electrical and Computer Engineering, Isfahan University of Technology, Isfahan, Iran. email: mdalian@iut.ac.ir

Abstract

This paper delves deeper into the comprehensive exploration of random matrix theory and its applications. This paper introduces a novel method that extends the concept of generalized random inverse non-square matrices, broadening the scope to encompass a variety of mathematical fields. Prime fields, denoted as $GF(p)$, and finite fields, represented by $GF(p^i)$, form a crucial part of this expansion. Additionally, it delves into the real field and also considers the complex field.

Keywords: Finite Fields, Generalized Inverse Matrix, Post Quantum

1 Introduction

In the realm of linear algebra, the notion of matrix inversion plays a crucial role. While the inversion of square matrices is well-known and results in a unique inverse, however, the non-square inverse matrice is not unique and in fact, the number of inverses for a non-square matrix can be as vast as $q^{m(n-m)}$, where $q$ signifies the order of the underlying field. In this paper, we embark on a journey to construct these elusive inverse matrices, harnessing the power of arbitrary fields. Arbitrary fields, including prime fields, finite fields, real fields, and complex fields, offer a rich mathematical background that extends far beyond conventional numerical domains. These fields find practical applications that are essential
to contemporary technology. Finite fields, also known as Galois fields (GFs), are fundamental mathematical structures that find extensive applications in various domains, including cryptography, signal processing, error correction, and data transmission [1] [2]. These fields, characterized by their finite set of elements and algebraic operations, have emerged as essential tools in modern science and technology. In cryptography, finite fields play an important role, forming the basis of secure communication protocols and encryption algorithms. The utilization of finite fields in cryptographic systems ensures the confidentiality and integrity of sensitive information. Notably, techniques like elliptic curve cryptography [3] [4], and the implementation of the Advanced Encryption Standard (AES) heavily rely on arithmetic operations within finite fields to provide robust security [5] [6]. In signal processing and coding theory, finite fields offer powerful tools for data transmission and error correction. Matrices defined over finite fields enable the sharing of secret keys and secure data exchange over insecure channels, making them essential in various cryptosystems. Moreover, finite fields are instrumental in the development of error-correcting codes, including Reed-Solomon and BCH codes, ensuring reliable data transmission and storage [7–9]. In [10], matrix inversion and $GF(256)$ are employed to enhance digital image encryption, thereby improving both the security and speed of encrypting digital images. It was shown in [11] that a matrix over a finite field can be used to share the secret key, known as the seed, over an insecure channel.

Complex inverse matrices find applications across science, engineering, and mathematics. They are essential in quantum mechanics for solving linear equations governing quantum behavior [12]. In wireless communications, they aid in channel equalization and beamforming [13], while in digital signal processing, they enable filtering, equalization, and spectral analysis [14]. In electrical engineering, complex inverse matrices are employed to solve intricate circuit equations, perform impedance matching, and analyze electromagnetic fields [15]. These matrices also play a pivotal role in control systems, facilitating modeling and control of dynamic systems, including electrical circuits and mechanical setups [16]. Furthermore, complex matrices describe the behavior of optical components like lenses in optical systems [17]. They are valuable in multivariate statistics, particularly in techniques such as Principal Component Analysis (PCA) and Factor Analysis [18]. Complex inverse matrices contribute significantly to computer graphics by enabling transformations and rendering in 3D graphics [19]. In the realm of medical imaging, they are employed for image reconstruction, benefiting techniques like Magnetic Resonance Imaging (MRI) and tomography [20]. Lastly, these matrices hold a fundamental position in the emerging field of quantum computing, where they are integral to quantum gates and algorithms [21].
The next section proposes a method for random matrix inversion in the context of binary arithmetic as the initial focus. Subsequent sections will expand upon this concept, delving into the realm of random matrix inversion in an arbitrary fields beyond binary arithmetic. This sequential approach allows for a gradual exploration of the topic, starting with a foundation in binary arithmetic before extending to broader fields.

2 Random Inverse of the Non-Square Matrix in Binary Arithmetic

Let $B$ a full rank non-square matrix with dimensions $m \times n$ where $m < n$, such that

$$B_{m \times n} = \begin{pmatrix} b_1 & B_1 & b_2 & B_2 & \ldots & b_y & B_x & b_{y+1} \end{pmatrix},$$  \hspace{1cm} (1)

where $B_1, B_2, \ldots, B_x$ are the matrices with $m$ rows and $n_1, n_2, \ldots, n_x$ columns, respectively, such that $n_1 + n_2 + \ldots + n_x = n - m$. Also $b_1, b_2, \ldots, b_{y+1}$ are the column vectors with $m$ rows, where $y + 1 = m$.

The either of $B_i \ (i = 1, \ldots, x)$ and $b_j \ (j = 1, \ldots, y + 1)$ can be null matrix $B$ or null vector $b$.

A full-rank matrix $B$ must include a minimum of $m$ linearly independent column vectors $b_j \ (j = 1, \ldots, y + 1)$. For example the following matrix $B$ is a full rank matrix with $\text{rank} = 5$

$$B_{5 \times 9} = \begin{pmatrix} 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 & 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix},$$

$$= \begin{pmatrix} b_1 & b_2 & b_3 & B_3 & b_4 & b_5 \end{pmatrix},$$

where $B_1, B_2$ and $B_4$ are null matrices.
Let’s consider matrix $A$ is the inverse of $B$ matrix, therefore $B_{m \times n}A_{n \times m} = I_{m \times m}$. 

$$A_{n \times m} = \begin{pmatrix} a_1 \\ A_1 \\ a_2 \\ A_2 \\ \vdots \\ a_y \\ A_x \\ a_{y+1} \end{pmatrix}, \quad (2)$$

where $A_1, A_2, \ldots, A_x$, are the matrices with $n_1, n_2, \ldots, n_x$ rows, respectively, such that $n_1 + n_2 + \ldots + n_x = n - m$. Also $a_1, a_2, \ldots, a_{y+1}$, are the row vectors with $m$ columns, where $y + 1 = m$.

Hence the matrix $A$ is the inverse of matrix $B$, then the product of $B$ and $A$ will result in the identity matrix.

$$BA = \begin{pmatrix} b_1 & B_1 & b_2 & B_2 & \ldots & b_y & B_x & b_{y+1} \end{pmatrix} \times \begin{pmatrix} a_1 \\ A_1 \\ a_2 \\ A_2 \\ \vdots \\ a_y \\ A_x \\ a_{y+1} \end{pmatrix} = I_m, \quad (3)$$

$$\sum_{i=1}^{x} B_i A_i + \sum_{j=1}^{y+1} b_j a_j = I_m \quad (4)$$

A random pseudo-inverse matrix $A$ can be generated by randomly selecting $A_1, A_2, \ldots, A_x$ and constructing the corresponding row matrix variables $a_1, a_2, \ldots, a_{y+1}$.
Let define $A_a$ and $B_b$ such that

\[(A_a)_{m \times m} = \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_{y+1} \end{pmatrix}, (B_b)_{m \times m} = \begin{pmatrix} b_1 & b_2 & \ldots & b_{y+1} \end{pmatrix} \]  

(5)

Therefore,

\[\sum_{i=1}^{x} B_i A_i + B_b A_a = I_m \]  

(6)

\[B_b A_a = I_m + \sum_{i=1}^{x} B_i A_i \]

\[A_a = (B_b)^{-1} (I_m + \sum_{i=1}^{x} B_i A_i) \]  

(7)

Hence, the columns of the binary matrix $B_b$ are linearly independent, resulting in a determinant of 1. Therefore, matrix $B_b$ is a non-singular matrix. Consequently, by selecting random matrices $A_i$, matrix $A_a$ can be constructed as outlined in equation (3.5).

For example, let’s consider matrix $B$ with dimensions $m=5$ and $n=9$, such that

\[B_{5 \times 9} = \begin{pmatrix} 0 & 1 & 0 & 1 & 1 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{pmatrix} \]

\[= \begin{pmatrix} b_1 & b_2 & b_3 & B_3 & b_4 & b_5 \end{pmatrix} \]

Therefore, matrix $A_{9 \times 5}$ would be such

\[A_{9 \times 5} = \begin{pmatrix} a_1 \\ a_2 \\ a_3 \\ A_3 \\ a_4 \\ a_5 \end{pmatrix} \]
where $A_3$ can be randomly selected

$$A_3 = \begin{pmatrix} 0 & 1 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 0 \end{pmatrix}.$$

Given matrices $B_3$ and $(B_b)_{m \times m}$

$$B_3 = \begin{pmatrix} 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}, (B_b)_{5 \times 5} = \begin{pmatrix} 0 & 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 \end{pmatrix},$$

the inverse of $(B_b)_{m \times m}$ would be as follows:

$$(B_b)^{-1} = \begin{pmatrix} 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 \end{pmatrix}.$$ 

Therefore, matrix $A_a$ can be constructed as:

$$A_a = (B_b)^{-1}(I_5 + B_3A_3)$$

where

$$A_a = \begin{pmatrix} 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 \end{pmatrix} \times \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix} + \begin{pmatrix} 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \times \begin{pmatrix} 0 & 1 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 0 \end{pmatrix}.$$
$A_a = \begin{pmatrix} 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 \end{pmatrix} \times \begin{pmatrix} 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 \end{pmatrix}$

$(A_a)_{5 \times 5} = \begin{pmatrix} a_1 \\ a_2 \\ a_3 \\ a_4 \\ a_5 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 & 1 \end{pmatrix}$.

Having matrices $A_3$ and $A_a$, the inverse matrix $A$ can be constructed such that:

$A_{9 \times 5} = \begin{pmatrix} a_1 \\ a_2 \\ a_3 \\ a_4 \\ a_5 \\ A_3 \\ A_3 \\ A_3 \\ A_3 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 & 1 \end{pmatrix}$

where $B_{(5 \times 9)} \times A_{(9 \times 5)} = I_5$.

### 3 Random Inverse of the Non-Square Matrix in Arbitrary Fields

This section demonstrates that the presented method can also be applied to construct random inverses on an arbitrary field. Let $B$ be a full rank non-square matrix where all its elements are from the field $(b_{ij} \in F_q)$, with dimensions $m \times n$ ($m < n$). $A$ is another matrix with elements from the field $(a_{ij} \in F_q)$, having dimensions $n \times m$, and it satisfies the equation $BA = I_m$. 

7
\[
\begin{pmatrix}
b_{1,1} & b_{1,2} & b_{1,3} & \cdots & b_{1,n} \\
b_{2,1} & b_{2,2} & b_{2,3} & \cdots & b_{2,n} \\
b_{3,1} & b_{3,2} & b_{3,3} & \cdots & b_{3,n} \\
\vdots & \vdots & \vdots & \ddots & \vdots \\
b_{m,1} & b_{m,2} & b_{m,3} & \cdots & b_{m,n}
\end{pmatrix}
\begin{pmatrix}
a_{1,1} & a_{1,2} & a_{1,3} & \cdots & a_{1,m} \\
a_{2,1} & a_{2,2} & a_{2,3} & \cdots & a_{2,m} \\
a_{3,1} & a_{3,2} & a_{3,3} & \cdots & a_{3,m} \\
\vdots & \vdots & \vdots & \ddots & \vdots \\
a_{n,1} & a_{n,2} & a_{n,3} & \cdots & a_{n,m}
\end{pmatrix} = I_m.
\tag{8}
\]

This result a linear equation system with \(m^2\) equations and \(mn\) variables \((a_{ij})\),

\[
\begin{align*}
b_{1,1}a_{1,1} + b_{1,2}a_{2,1} + \ldots + b_{1,n}a_{n,1} &= 1 \\
b_{1,1}a_{1,2} + b_{1,2}a_{2,2} + \ldots + b_{1,n}a_{n,2} &= 0 \\
b_{1,1}a_{1,3} + b_{1,2}a_{2,3} + \ldots + b_{1,n}a_{n,3} &= 0 \\
\vdots & \\
b_{m,1}a_{1,m} + b_{m,2}a_{2,m} + \ldots + b_{m,n}a_{n,m} &= 1
\end{align*}
\]

Thus, there would be \(q^{mn-m^2} = q^{m(n-m)}\) solutions available for matrix \(A\) on \(F_q\).

For infinite filed, such as real fileld, there would be unlimited solutions.

Let write the matrix \(BA = I_m\) in equation (3.3) with the following format as mentioned on previous section,

\[
\begin{pmatrix}
a_1 \\
A_1 \\
a_2 \\
A_2 \\
\vdots \\
a_y \\
A_y \\
a_{y+1}
\end{pmatrix} = I_m,
\]

where

\[
(A_a)_{m \times m} = \begin{pmatrix}
a_1 \\
a_2 \\
\vdots \\
a_{y+1}
\end{pmatrix},
(B_b)_{m \times m} = \begin{pmatrix}
b_1 & b_2 & \cdots & b_{y+1}
\end{pmatrix},
\]
and therefore,

$$A_a = (B_b)^{-1}(I_{m \times m} + \sum_{i=1}^{x} B_i A_i)$$

Where $A_i$ matrices $(i = 1, \ldots, x)$ and their corresponding $a_1, a_2, \ldots, a_{y+1}$ can be selected randomly. This enables constructing the total $q^{m(n-m)}$ available inverse matrices on $F_q$. As mentioned, the columns of the binary matrix $B_b$ are linearly independent, resulting in a non-zero determinant value, confirming the non-singularity of the $B_b$ matrix.

## 4 Finite Field Random Inverse

A finite field is a mathematical structure used in various areas of mathematics, computer science, and cryptography. Finite fields have a finite number of elements, which means it is a set of numbers with addition and multiplication operations that satisfy specific properties. It also known as a Galois field that denoted as $GF(p)$ or $GF(p^i)$, where $p$ is a prime number and $r$ is a positive integer.

The $GF(p)$ also called prime field that is explain in next section. In a finite field $GF(p^i)$, the elements are polynomials of degree less than $r$ with coefficients in $GF(p)$. Addition and multiplication of polynomials are performed modulo an irreducible polynomial of degree $r$.

It was shown in [22] that, the elements of $GF(2^4)$ with irreducible polynomial $x^4+x+1$ would be $x^0 = 1, x^1, x^2, x^3, \ldots$ that can be presented as polynomial with degree less than 4, such

$$
\begin{align*}
  x^4 &= x + 1 \\
  x^5 &= x^2 + x \\
  x^6 &= x^3 + x^2 \\
  x^7 &= x^3 + x + 1 \\
  x^8 &= x^2 + 1 \\
  x^9 &= x^3 + x \\
  x^{10} &= x^2 + x + 1 \\
  x^{11} &= x^3 + x^2 + x \\
  x^{12} &= x^3 + x^2 + x + 1 \\
  x^{13} &= x^3 + x^2 + 1 \\
  x^{14} &= x^3 + 1 \\
  x^{15} &= x^4 + x = 1
\end{align*}
$$

Hence, the irreducible polynomial $x^4+x+1$ is primitive, as it exhibits a 4-stage binary Linear Feedback Shift Register (LFSR) with a minimum cycle length of $2^4 - 1$ periods,
Table 1: Multiplication table of $GF(2^4)$ with Irreducible Polynomial $x^4 + x + 1$

<table>
<thead>
<tr>
<th>×</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>A</th>
<th>B</th>
<th>C</th>
<th>D</th>
<th>E</th>
<th>F</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>6</td>
<td>7</td>
<td>8</td>
<td>9</td>
<td>a</td>
<td>b</td>
<td>c</td>
<td>d</td>
<td>e</td>
<td>f</td>
</tr>
<tr>
<td>2</td>
<td>0</td>
<td>2</td>
<td>4</td>
<td>6</td>
<td>8</td>
<td>a</td>
<td>c</td>
<td>e</td>
<td>3</td>
<td>1</td>
<td>7</td>
<td>5</td>
<td>b</td>
<td>9</td>
<td>f</td>
<td>d</td>
</tr>
<tr>
<td>3</td>
<td>0</td>
<td>3</td>
<td>6</td>
<td>5</td>
<td>c</td>
<td>f</td>
<td>a</td>
<td>9</td>
<td>b</td>
<td>8</td>
<td>d</td>
<td>e</td>
<td>7</td>
<td>4</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>4</td>
<td>0</td>
<td>4</td>
<td>8</td>
<td>c</td>
<td>3</td>
<td>7</td>
<td>b</td>
<td>f</td>
<td>6</td>
<td>2</td>
<td>e</td>
<td>a</td>
<td>5</td>
<td>1</td>
<td>d</td>
<td>9</td>
</tr>
<tr>
<td>5</td>
<td>0</td>
<td>5</td>
<td>a</td>
<td>f</td>
<td>7</td>
<td>2</td>
<td>d</td>
<td>8</td>
<td>e</td>
<td>b</td>
<td>4</td>
<td>1</td>
<td>9</td>
<td>c</td>
<td>3</td>
<td>6</td>
</tr>
<tr>
<td>6</td>
<td>0</td>
<td>6</td>
<td>c</td>
<td>a</td>
<td>b</td>
<td>d</td>
<td>7</td>
<td>1</td>
<td>5</td>
<td>3</td>
<td>9</td>
<td>f</td>
<td>e</td>
<td>8</td>
<td>2</td>
<td>4</td>
</tr>
<tr>
<td>7</td>
<td>0</td>
<td>7</td>
<td>e</td>
<td>9</td>
<td>f</td>
<td>8</td>
<td>1</td>
<td>6</td>
<td>d</td>
<td>a</td>
<td>3</td>
<td>4</td>
<td>2</td>
<td>5</td>
<td>c</td>
<td>b</td>
</tr>
<tr>
<td>8</td>
<td>0</td>
<td>8</td>
<td>3</td>
<td>b</td>
<td>6</td>
<td>e</td>
<td>5</td>
<td>d</td>
<td>c</td>
<td>4</td>
<td>f</td>
<td>7</td>
<td>a</td>
<td>2</td>
<td>9</td>
<td>1</td>
</tr>
<tr>
<td>9</td>
<td>0</td>
<td>9</td>
<td>1</td>
<td>8</td>
<td>2</td>
<td>b</td>
<td>3</td>
<td>a</td>
<td>4</td>
<td>d</td>
<td>5</td>
<td>c</td>
<td>6</td>
<td>f</td>
<td>7</td>
<td>e</td>
</tr>
<tr>
<td>A</td>
<td>0</td>
<td>a</td>
<td>7</td>
<td>d</td>
<td>e</td>
<td>4</td>
<td>9</td>
<td>3</td>
<td>f</td>
<td>5</td>
<td>8</td>
<td>2</td>
<td>1</td>
<td>b</td>
<td>6</td>
<td>c</td>
</tr>
<tr>
<td>B</td>
<td>0</td>
<td>b</td>
<td>5</td>
<td>e</td>
<td>a</td>
<td>1</td>
<td>f</td>
<td>4</td>
<td>7</td>
<td>c</td>
<td>2</td>
<td>9</td>
<td>d</td>
<td>6</td>
<td>8</td>
<td>3</td>
</tr>
<tr>
<td>C</td>
<td>0</td>
<td>c</td>
<td>b</td>
<td>7</td>
<td>5</td>
<td>9</td>
<td>e</td>
<td>2</td>
<td>a</td>
<td>6</td>
<td>1</td>
<td>d</td>
<td>f</td>
<td>3</td>
<td>4</td>
<td>8</td>
</tr>
<tr>
<td>D</td>
<td>0</td>
<td>d</td>
<td>9</td>
<td>4</td>
<td>1</td>
<td>c</td>
<td>8</td>
<td>5</td>
<td>2</td>
<td>f</td>
<td>b</td>
<td>6</td>
<td>3</td>
<td>e</td>
<td>a</td>
<td>7</td>
</tr>
<tr>
<td>E</td>
<td>0</td>
<td>e</td>
<td>f</td>
<td>1</td>
<td>d</td>
<td>3</td>
<td>2</td>
<td>c</td>
<td>9</td>
<td>7</td>
<td>6</td>
<td>8</td>
<td>4</td>
<td>a</td>
<td>b</td>
<td>5</td>
</tr>
<tr>
<td>F</td>
<td>0</td>
<td>f</td>
<td>d</td>
<td>2</td>
<td>9</td>
<td>6</td>
<td>4</td>
<td>b</td>
<td>1</td>
<td>e</td>
<td>c</td>
<td>3</td>
<td>8</td>
<td>7</td>
<td>5</td>
<td>a</td>
</tr>
</tbody>
</table>

where $x^{15}$ cycles back to $x^0$ denoting a value of 1.

Table 3.1 illustrates the results of multiplication operations among the finite elements of $GF(2^4)$.

Let's consider the finite field $GF(2^4)$, where matrix $B$ is given, such

$$B_{4 \times 7} = \begin{pmatrix} 2 & 1 & 3 & 8 & 5 & A & 8 \\ D & 2 & E & C & 3 & 1 & 6 \\ C & 1 & 4 & 8 & 6 & F \\ E & 7 & 0 & 2 & E & 0 & C \end{pmatrix} = \begin{pmatrix} b_1 & B_1 & b_2 & b_3 & B_3 & b_4 \end{pmatrix}$$

so there is no $B_2, B_1, B_3$ and $B_b$ are

$$B_1 = \begin{pmatrix} 1 \\ 2 \\ 1 \\ 7 \end{pmatrix}, \ B_3 = \begin{pmatrix} 5 & A \\ 3 & 1 \\ 8 & 6 \\ E & 0 \end{pmatrix}, \ B_b = \begin{pmatrix} 2 & 3 & 8 & 8 \\ D & E & C & 6 \\ C & 1 & 4 & F \\ E & 0 & 2 & C \end{pmatrix}.$$
Therefore \((B_b)^{-1}\) can be constructed

\[
(B_b)^{-1} = \begin{pmatrix} 9 & C & C & 7 \\ B & 3 & E & F \\ 1 & 4 & E & 9 \\ 4 & 1 & 2 & 1 \end{pmatrix}.
\]

Now by random selection of \(A_1, A_3\)

\[
A_1 = \begin{pmatrix} 5 & 4 & 5 & 2 \end{pmatrix}, \quad A_3 = \begin{pmatrix} F & 9 & B & 9 \\ 0 & 9 & D & 5 \end{pmatrix},
\]

the \(A_a\) can be constructed as

\[
A_a = (B_b)^{-1}(I_4 + B_1A_1 + B_3A_3),
\]

\[
A_a = \begin{pmatrix} 9 & C & C & 7 \\ B & 3 & E & F \\ 1 & 4 & E & 9 \\ 4 & 1 & 2 & 1 \end{pmatrix} \times \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} + \begin{pmatrix} 5 & 4 & 5 & 2 \\ A & 8 & A & 4 \\ 5 & 4 & 5 & 2 \\ 8 & F & 8 & E \end{pmatrix} + \begin{pmatrix} 6 & E & A & F \\ 2 & 1 & 3 & D \\ 1 & 7 & F & 9 \\ 5 & 7 & 8 & 7 \end{pmatrix},
\]

\[
A_a = \begin{pmatrix} 9 & C & C & 7 \\ B & 3 & E & F \\ 1 & 4 & E & 9 \\ 4 & 1 & 2 & 1 \end{pmatrix} \times \begin{pmatrix} 2 & A & F & D \\ 8 & 8 & 9 & 9 \\ 4 & 3 & B & B \\ D & 8 & 0 & 8 \end{pmatrix},
\]

\[
A_a = \begin{pmatrix} a_1 \\ a_2 \\ a_3 \\ a_4 \end{pmatrix} = \begin{pmatrix} B & 5 & 5 & 9 \\ 4 & 9 & 3 & 7 \\ 6 & 9 & 5 & 3 \\ 5 & 8 & 5 & 5 \end{pmatrix},
\]

and therefore matrix \(A\) can constructed as follows:

\[
A_{7 \times 4} = \begin{pmatrix} a_1 \\ A_1 \\ a_2 \\ a_3 \\ A_3 \\ a_4 \end{pmatrix} = \begin{pmatrix} B & 5 & 5 & 9 \\ 5 & 4 & 5 & 2 \\ 4 & 9 & 3 & 7 \\ 6 & 9 & 5 & 3 \\ F & 9 & B & 9 \\ 0 & 9 & D & 5 \\ 5 & 8 & 5 & 5 \end{pmatrix}.
\]
where $B_{(4 \times 7)} \times A_{(7 \times 4)} = I_4$ in $GF(2^4)$

\[
\begin{pmatrix}
2 & 1 & 3 & 8 & 5 & A & 8 \\
D & 2 & E & C & 3 & 1 & 6 \\
C & 1 & 1 & 4 & 8 & 6 & F \\
E & 7 & 0 & 2 & E & 0 & C
\end{pmatrix}
\times
\begin{pmatrix}
B & 5 & 5 & 9 \\
5 & 4 & 5 & 2 \\
4 & 9 & 3 & 7 \\
6 & 9 & 5 & 3 \\
F & 9 & B & 9 \\
0 & 9 & D & 5 \\
5 & 8 & 5 & 5
\end{pmatrix}
= I_4.
\]

### 4.1 Prime Field Random Inverse

As mentioned on previous section, the a finite field $GF(p)$ also called prime field. In a prime field $GF(p)$, the elements are integers modulo $p$ where $p$ is a prime number. The addition and multiplication operations are performed modulo $p$. For example, in the prime field $GF(7)$, the elements are $(0, 1, 2, 3, 4, 5, 6)$, and arithmetic is done modulo 7. So, for instance, $3 + 5 = 1$ in $GF(7)$ as $(3 + 5) mod(7) = 1$.

As per the equations (3), (5), (4), and (6):

\[
\sum_{i=1}^{x} B_iA_i + B_aA_a = I_m.
\]

In this study, both finite fields and prime fields are extensively employed. It’s important to note that the operation denoted as ‘+’ in the context of a finite field functions as a bitwise XOR operation. This operation follows the rules of arithmetic in binary representation. However, when working within a prime field, the ‘+’ and ‘-’ operations take on distinct roles. In this context, ‘+’ and ‘-’ are not bitwise XOR operations but rather traditional addition and subtraction. The crucial distinction arises when introducing modulo (p), where ‘p’ represents the prime number defining the field. These modulo operations are fundamental for ensuring calculations remain within the bounds of the prime field.

Therefore, for a prime field using modulo $p$

\[
B_aA_a = I_m - \sum_{i=1}^{x} (B_iA_i) mod(p), \quad (9)
\]

\[
A_a = (B_b)^{-1}(I_m - \sum_{i=1}^{x} (B_iA_i) mod(p)) \quad (10)
\]
Now, let's consider the prime field $GF(7)$, where matrix $B$ is given, such as
\[
B_{3 \times 6} = \begin{pmatrix}
3 & 5 & 2 & 4 & 1 & 2 \\
1 & 2 & 6 & 2 & 5 & 6 \\
4 & 3 & 3 & 4 & 5 & 5
\end{pmatrix} = \begin{pmatrix} B_1 & b_2 & b_3 & b_4 & B_4 \end{pmatrix}
\]

Here, $B_1, B_4, B_b$, and $(B_b)^{-1}$ are defined as:
\[
B_1 = \begin{pmatrix} 3 & 5 \\ 1 & 2 \\ 4 & 3 \end{pmatrix}, B_4 = \begin{pmatrix} 2 \\ 6 \\ 5 \end{pmatrix}, B_b = \begin{pmatrix} 2 & 4 & 1 \\ 6 & 2 & 5 \\ 3 & 1 & 5 \end{pmatrix}, (B_b)^{-1} = \begin{pmatrix} 2 & 5 & 3 \\ 1 & 0 & 4 \\ 0 & 4 & 6 \end{pmatrix}.
\]

By randomly selecting matrices $A_1$ and $A_4$ as
\[
A_1 = \begin{pmatrix} 1 & 6 & 6 \\ 1 & 6 & 2 \end{pmatrix}, A_4 = \begin{pmatrix} 1 & 6 & 1 \end{pmatrix},
\]

the $A_a$ can be constructed as follows:

\[
A_a = (B_b)^{-1}(I_3 - B_1A_1 - B_4A_4),
\]

which yields

\[
A_a = \begin{pmatrix} 2 & 5 & 3 \\ 1 & 0 & 4 \\ 0 & 4 & 6 \end{pmatrix} \times \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} - \begin{pmatrix} 1 & 6 & 0 \\ 3 & 4 & 3 \\ 0 & 0 & 2 \end{pmatrix} - \begin{pmatrix} 2 & 5 & 2 \\ 6 & 1 & 6 \\ 5 & 2 & 5 \end{pmatrix}
\]

\[
A_a = \begin{pmatrix} 2 & 5 & 3 \\ 1 & 0 & 4 \\ 0 & 4 & 6 \end{pmatrix} \times \begin{pmatrix} -2 & -11 & -2 \\ -9 & -4 & -9 \\ -5 & -2 & -6 \end{pmatrix} \quad mod(7)
\]

\[
A_a = \begin{pmatrix} 2 & 5 & 3 \\ 1 & 0 & 4 \\ 0 & 4 & 6 \end{pmatrix} \times \begin{pmatrix} 5 & 3 & 5 \\ 5 & 3 & 5 \\ 2 & 5 & 1 \end{pmatrix}
\]

resulting in

\[
A_a = \begin{pmatrix} a_2 \\ a_3 \\ a_4 \end{pmatrix} = \begin{pmatrix} 6 & 1 & 3 \\ 6 & 2 & 2 \\ 4 & 0 & 5 \end{pmatrix},
\]
thus, the matrix $A$ can constructed as

$$A_{6\times3} = \begin{pmatrix} A_1 \\ a_2 \\ a_3 \\ a_4 \\ A_4 \end{pmatrix} = \begin{pmatrix} 1 & 6 & 6 \\ 1 & 6 & 2 \\ 6 & 1 & 3 \\ 6 & 2 & 2 \\ 4 & 0 & 5 \\ 1 & 6 & 1 \end{pmatrix},$$

where $B_{(3\times6)} \times A_{(6\times3)} = I_3$ in prime field $GF(7)$.

## 5 Complex Random Inverse Matrices

Complex numbers consist of two components: the real part, which entirely resides on the real number line, and the imaginary part, which represents the magnitude of the number’s deviation from the real part. The concept of complex numbers is essential for various mathematical operations involving quantities with both real and imaginary components.

In a complex number of the form $a + bi$, where $a$ and $b$ are real numbers:

- $a$: is the real part.
- $bi$: is the imaginary part.

The imaginary part of a complex number involves the imaginary unit $i$, defined as the square root of $-1$. For example, in the complex number $3 + 4i$, the real part is 3, and the imaginary part is $4i$.

As specified by equations (3), (5), (4), and (6):

$$\sum_{i=1}^{x} B_i A_i + B_b A_a = I_m.$$  

Therefore, for a complex random inverse matrices:

$$B_b A_a = I_m - \sum_{i=1}^{x} (B_i A_i), \quad \text{(11)}$$

$$A_a = (B_b)^{-1}(I_m - \sum_{i=1}^{x} (B_i A_i)). \quad \text{(12)}$$
Now, let’s consider the complex matrix $B_{3 \times 5}$ provided below:

\[
\begin{pmatrix}
46.0504 + 70.7762i & 37.8806 + 48.5372i & 48.9987 + 43.2619i & 94.7195 + 51.0426i \\
94.2528 + 52.9646i & 40.1540 + 61.8018i & 71.8969 + 11.0150i & 12.0771 + 42.6998i \\
62.8343 + 65.2427i & 32.1394 + 50.2087i & 19.3064 + 91.6550i & 13.9920 + 2.9286i & 43.8656 + 27.5350i
\end{pmatrix}
\]

\[= \begin{pmatrix} B_1 & b_2 & b_3 & b_4 \end{pmatrix} \]

Here, $B_1$ and $B_b$ are defined as:

\[
B_1 = \begin{pmatrix}
46.0504 + 70.7762i & 37.8806 + 48.5372i & 48.9987 + 43.2619i & 94.7195 + 51.0426i \\
94.2528 + 52.9646i & 40.1540 + 61.8018i & 71.8969 + 11.0150i & 12.0771 + 42.6998i \\
62.8343 + 65.2427i & 32.1394 + 50.2087i & 19.3064 + 91.6550i & 13.9920 + 2.9286i & 43.8656 + 27.5350i
\end{pmatrix},
\]

\[
B_b = \begin{pmatrix}
37.8806 + 48.5372i & 48.9987 + 43.2619i & 94.7195 + 51.0426i \\
71.8969 + 11.0150i & 12.0771 + 42.6998i & 63.0943 + 96.3703i \\
19.3064 + 91.6550i & 13.9920 + 2.9286i & 43.8656 + 27.5350i
\end{pmatrix}.
\]

Thus, the $(B_b)^{-1}$ can constructed such

\[
(B_b)^{-1} = \begin{pmatrix}
0.0025 - 0.0035i & 0.0024 + 0.0064i & -0.0036 - 0.0077i \\
0.0216 - 0.0281i & 0.0000 + 0.0219i & -0.0206 + 0.0168i \\
-0.0106 + 0.0105i & 0.0032 - 0.0169i & 0.0146 - 0.0023i
\end{pmatrix}.
\]

By randomly selecting matrices $A_1$ as

\[
A_1 = \begin{pmatrix}
0.7434 + 0.5976i & 0.1693 + 0.1271i & 0.6074 + 0.4992i \\
0.1168 + 0.4257i & 0.9301 + 0.0815i & 0.4689 + 0.0585i
\end{pmatrix},
\]

the $A_a$ can be constructed as follows:

\[
A_a = (B_b)^{-1}(I_3 - B_1A_1),
\]

resulting in

\[
A_a = \begin{pmatrix}
an_2 \\
n_3 \\
n_4
\end{pmatrix} = \begin{pmatrix}
-0.4652 - 0.5131i & -0.5037 - 0.0087i & -0.5138 - 0.2573i \\
1.4248 - 1.5911i & -0.6536 - 0.1757i & 0.8439 - 0.9126i \\
-1.2214 - 0.0303i & -0.3543 - 0.1799i & -1.0996 - 0.0862i
\end{pmatrix},
\]
thus, the matrix $A$ can constructed as

$$A_{5 \times 3} = \begin{pmatrix} A_1 \\ a_2 \\ a_3 \\ a_4 \end{pmatrix} = \begin{pmatrix} 0.7434 + 0.5976i & 0.1693 + 0.1271i & 0.6074 + 0.4992i \\ 0.1168 + 0.4257i & 0.9301 + 0.0815i & 0.4689 + 0.0585i \\ -0.4652 - 0.5131i & -0.5037 - 0.0087i & -0.5138 - 0.2573i \\ 1.4248 - 1.5911i & -0.6536 - 0.1757i & 0.8439 - 0.9126i \\ -1.2214 - 0.0303i & -0.3543 - 0.1799i & -1.0996 - 0.0862i \end{pmatrix}.$$  

where $B_{(3 \times 5)} \times A_{(5 \times 3)} = I_3$.

### 6  Real Number Inverse Matrix

Real numbers are used extensively in various branches of mathematics, physics, engineering, and many other fields to represent quantities, measurements, and values in the real world. They constitute fundamental concept in mathematics and form the basis of our everyday numerical system. This comprehensive set of numbers encompasses a wide range of values, including integers, fractions, decimals, and irrational numbers. In the context of constructing a random inverse matrix for a non-square matrix with real-number elements, equations (3), (5), (4), and (6), as well as (11), and the subsequent equation (12), can be effectively applied

$$A_a = (B_b)^{-1}(I_m - \sum_{i=1}^{x}(B_i A_i)).$$

### 7  Conclusion

This paper introduces a novel method for constructing generalized random inverses of full-rank non-square matrices across diverse mathematical domains.

It was shown that, within arbitrary fields, there exist $q^m(n - m)$ random matrices that can be effectively employed for non-square full-rank matrices with dimensions $m \times n$, where $n > m$. Additionally, the paper introduces a pioneering approach for constructing a random inverse matrix denoted as matrix $A$. This matrix comprises two components, $A_i$ and $A_a$ matrices. The method involves the random selection of $A_i$ matrices, which consist of a total of $n - m$ rows, and the matrix $A_a$, which incorporates the remaining $m$ rows constructed from the randomized $A_i$ matrices.

The paper underscores the versatility of this method by illustrating its applicability across diverse fields, including binary, real, prime fields, finite fields, and complex fields.
References


