Generating Large Non-Singular Matrices over an Arbitrary Field with Blocks of Full Rank

James Xiao Yongxin Zhou*

June 27, 2002

Abstract

This note describes a technique for generating large non-singular matrices with blocks of full rank. While this may be of independent interest, our motivation arises in the white-box implementation of cryptographic algorithms with S-boxes.

1 Introduction and Notation

This note describes a technique for generating large non-singular matrices with blocks of full rank. One motivation is the following. For ciphers such as AES[4], DES[5], and CAST[6] involving linear transformations and substitution boxes (S-boxes), white-box cryptographic implementations[7] attempt to hide linear transformations in the non-linear S-box lookups by blocking the matrices for the linear transformations, and then non-linearly encoding the matrix operations by converting the blocks into substitution boxes (S-boxes) with arbitrary bijective input and output encodings. Security considerations dictate that the matrices be hard to discover from the S-boxes. A bijective S-box leaks no information if its input and output codings are unknown and arbitrary, whereas a lossy S-box leaks information: distinct encoded inputs map to the same encoded output, reducing the search space for encodings. This in turn means that blocks of reduced rank should be avoided.

We now introduce our notation. Let ${}^{n}_{m}M$ denote an $n \times m$ matrix M over field F;[1] ${}^{n}M$ is short for ${}^{n}_{n}M$. ${}^{n}\mathbf{I}$ denotes an $n \times n$ identity matrix. ${}^{n}_{m}\mathbf{0}$ denotes an $n \times m$ zero matrix; ${}^{n}\mathbf{0}$ is short for ${}^{n}_{n}\mathbf{0}$. As usual, $m_{i,j}$ denotes the matrix M element in *row* i and *column* j.

A matrix may be *blocked* into submatrices. For example,

$$\begin{pmatrix} {}^{b}_{a}A & {}^{b}_{c}B \\ {}^{d}_{a}C & {}^{d}_{c}D \end{pmatrix}$$

*yongxin.zhou@cloakware.com

[1] We refer to this as m inputs (columns) and n outputs (rows), because multiplying ${}^{n}_{m}M\,{}^{m}_{1}X$ yields a vector ${}^{n}_{1}Y$.

is a blocked matrix with blocks A, B, C, D, each of which is itself a matrix. Horizontally adjacent blocks must have the same number of rows, and vertically adjacent blocks must have the same number of columns.

Where a matrix ${}^n_m M$ is blocked, and all of the blocks are square and have the same dimensions $p \times p$ with $p|m$ and $p|n$, we use the notation ${}^n_m M[{}^p B]$ to denote an $n \times m$ matrix M with $\frac{mn}{p^2}$ blocks. Here $B_{i,j}$ denotes the block in row i and column j of blocks.

For convenience we give the following definition:

Definition 1.1 *If all the blocks $B_{i,j}$ in a block matrix ${}^n_m M[{}^p B]$ are invertible, matrix M is called an (m, n, p)* block invertible matrix*. Furthermore, if $m = n$, and M is invertible then M is called an (m, p)* block invertible square matrix*.*

In this note we describe a way to create a block invertible square matrix ${}^n_n M[{}^p B]$ for p and n natural numbers where $p|n$ and $p > 1$. One known technique involves the Kronecker product, or tensor product of matrices[2]. If we can find an invertible matrix ${}^p A$ such that all entries $a_{i,j}$ are not 0 in field F, its tensor product $A \otimes B$ with another invertible matrix ${}^p B$ is a (p^2, p) block invertible square matrix. However, this approach fails for cases where the matrix A does not exist — for example, when constructing $(2^t, 2)$ block invertible matrices over GF(2). We provide a method of constructing block invertible matrices over any field.

2 Preliminary Result

First we prove the following result.

Lemma 2.1 *Let p and r be two integers with $p > 1$ and $p \geq r \geq 0$. Then there exists a matrix ${}^p A$ such that*

$$T = \begin{pmatrix} {}^r\mathbf{I} & \\ & {}^{p-r}\mathbf{0} \end{pmatrix} + A$$

is an invertible matrix over field F.

Proof: We construct a matrix ${}^p A$ such that T is invertible, where

$$T = \begin{pmatrix} {}^r\mathbf{I} & {}^{p-r}\mathbf{0} \\ {}^{p-r}\mathbf{0} & {}^{p-r}\mathbf{0} \end{pmatrix} + A \ .$$

Case 1: If r is even, define

$$A = \begin{pmatrix} 0 & 1 & & & & & & \\ 1 & 1 & & & & & & \\ & & 0 & 1 & & & & \\ & & 1 & 1 & & & & \\ & & & & \cdots & \cdots & & \\ & & & & & 0 & 1 & \\ & & & & & 1 & 1 & \\ & & & & & & & {}^{p-r}\mathbf{I} \end{pmatrix}$$

with the $\frac{r}{2}$ invertible matrix $\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$ on the diagonal. Therefore A is invertible. Since

$$ {}^{2}\mathbf{I} + \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} $$

has a determinant of 1, T is invertible as each diagonal block is invertible:

$$ T = \begin{pmatrix} {}^{2}\mathbf{I} & & & & \\ & {}^{2}\mathbf{I} & & & \\ & & \cdots & \cdots & \\ & & & {}^{2}\mathbf{I} & \\ & & & & {}^{p-r}\mathbf{0} \end{pmatrix} + \begin{pmatrix} 0 & 1 & & & & & & & \\ 1 & 1 & & & & & & & \\ & & 0 & 1 & & & & & \\ & & 1 & 1 & & & & & \\ & & & & \cdots & \cdots & & & \\ & & & & & & 0 & 1 & \\ & & & & & & 1 & 1 & \\ & & & & & & & & {}^{p-r}\mathbf{I} \end{pmatrix} $$

$$ = \begin{pmatrix} 1 & 1 & & & & & & & \\ 1 & 2 & & & & & & & \\ & & 1 & 1 & & & & & \\ & & 1 & 2 & & & & & \\ & & & & \cdots & \cdots & & & \\ & & & & & & 1 & 1 & \\ & & & & & & 1 & 2 & \\ & & & & & & & & {}^{p-r}\mathbf{I} \end{pmatrix}. $$

Case 2: r is odd. For $r = 1$, A can be defined as

$$ A = \begin{pmatrix} 1 & 1 & \\ 1 & 0 & \\ & & {}^{p-2}\mathbf{I} \end{pmatrix} $$

Since $p > 1$, we have $p - 2 \geq 0$. Note that A is invertible, and

$$ T = \begin{pmatrix} 1 & 0 & \\ 0 & 0 & \\ & & {}^{p-2}\mathbf{0} \end{pmatrix} + A = \begin{pmatrix} 0 & 1 & \\ 1 & 0 & \\ & & {}^{p-2}\mathbf{I} \end{pmatrix} $$

is also invertible.

For r odd and $r > 1$, let $r = 2n + 3$ where $n \geq 0$. Now define A to be

$$A = \begin{pmatrix} 1 & 1 & 1 & & & & \\ 1 & 1 & 0 & & & & \\ 1 & 0 & 0 & & & & \\ & & & 0 & 1 & & \\ & & & 1 & 1 & & \\ & & & \cdots & \cdots & & \\ & & & & 0 & 1 & \\ & & & & 1 & 1 & \\ & & & & & & {}^{p-2n}\mathbf{I} \end{pmatrix}$$

Note that

$${}^{3}\mathbf{I} + \begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 0 \\ 1 & 0 & 1 \end{pmatrix}$$

which is invertible; and using the same argument as above, both A and T are invertible. ■

3 Constructing a block invertible square matrix

Before proceeding, we recall an elementary result used in the proof of our main result.

Lemma 3.1 From Paley and Weichsel[3]: *For a given square matrix ${}^{n}M$ of rank $r \leq n$ over field F, there exist invertible matrices ${}^{n}P$ and ${}^{n}Q$ such that*

$$M = P \begin{pmatrix} {}^{r}\mathbf{I} & \\ & {}^{n-r}\mathbf{0} \end{pmatrix} Q.$$

Theorem 3.2 (Main result) *For any field F, and for any positive integers n and p such that $n \geq p$ and $p|n$, there exists an (n, p) block invertible square matrix.*

Proof: We construct the matrix inductively. For the first step we find an invertible square matrix ${}^{p}M$ over F. Note that there are infinitely many $p \times p$ invertible matrices over infinite field F and there are

$$\prod_{i=0}^{p-1} (q^p - q^i)$$

invertible matrices over finite field F of order q[1]. These facts grant us a variety of choices of ${}^{p}M$. This ${}^{p}M$ is a (p, p) block invertible square matrix.

Now suppose we have found a (t, p) block invertible square matrix M with $t \geq p$ and $p|t$. The third step is to construct a $(t + p, p)$ block invertible square matrix.

It is not hard to see that there exists a (p,t,p) block invertible matrix X and a (t,p,p) block invertible matrix Y. In fact X and Y can be constructed from M because M is a (t,p) block invertible square matrix.

Let ${}^pW$ be a matrix over F. Observing the following matrix equation:

$$\begin{pmatrix} M & 0 \\ X & W \end{pmatrix} \cdot \begin{pmatrix} I & M^{-1}Y \\ 0 & I \end{pmatrix} = \begin{pmatrix} M & Y \\ X & XM^{-1}Y + W \end{pmatrix}$$

we claim that if we can find a $p \times p$ invertible matrix W such that $XM^{-1}Y + W$ is invertible, then matrix

$$N = \begin{pmatrix} M & Y \\ X & XM^{-1}Y + W \end{pmatrix}$$

is a $(t+p,p)$ invertible square matrix. In fact, if W is invertible, the left-side of the matrix equation implies N is invertible. Following the assumptions that M, X, Y, and $XM^{-1}Y + W$ are (t,p), (p,t,p), (t,p,p) and (p,p) block invertible matrices, respectively, by definition, N is a block invertible square matrix. Such a matrix W can be constructed in the following way.

¿From Lemma 3.1, for the $p \times p$ square matrix $XM^{-1}Y$, there exist two invertible matrices ${}^pP$ and ${}^pQ$ such that

$$P(XM^{-1}Y)Q = \begin{pmatrix} {}^r\mathbf{I} & {}^{p-r}\mathbf{0} \\ {}_{p-r}\mathbf{0} & {}^{p-r}_{p-r}\mathbf{0} \end{pmatrix}$$

where r is the rank of $XM^{-1}Y$. By Lemma 2.1, an invertible matrix ${}^pA$ exists such that

$$\begin{pmatrix} {}^r\mathbf{I} & {}^{p-r}\mathbf{0} \\ {}_{p-r}\mathbf{0} & {}^{p-r}_{p-r}\mathbf{0} \end{pmatrix} + A$$

is invertible. Now we can define W as $W = P^{-1}AQ^{-1}$. Then the matrix

$$XM^{-1}Y + W = P^{-1}(P(XM^{-1}Y)Q + A)Q^{-1} = P^{-1}(\begin{pmatrix} {}^r\mathbf{I} & {}^{p-r}\mathbf{0} \\ {}_{p-r}\mathbf{0} & {}^{p-r}_{p-r}\mathbf{0} \end{pmatrix} + A)Q^{-1}$$

is invertible, completing our construction. ∎

4 Example

In the following example, for $F = \mathrm{GF}(2)$, we construct an $(n,2)$ block invertible square matrix for any even number $n > 0$. All blocks mentioned below are of dimension 2×2.

Since any invertible 2×2 matrix is a $(2,2)$ block invertible square matrix, we can safely assume that we already have a $(t,2)$ block invertible square matrix ${}^tM$ for $t \geq 2$. We construct a $(t+2,2)$ block invertible square matrix ${}^{t+2}M'$ as follows.

1. Use a row of blocks of matrix M to create a matrix ${}^2_tX$.
2. Use a column of blocks of matrix M to create a matrix ${}^t_2Y$.
3. Get invertible matrices ${}^2P$ and ${}^2Q$ such that $P(XM^{-1}Y)Q = \begin{pmatrix} {}^r\mathbf{I} & \\ & {}_{2-r}\mathbf{0} \end{pmatrix}$.
4. Define matrix ${}^2A$ as follows:
   (a) if $r = 0$, $A = {}^2\mathbf{I}$;
   (b) if $r = 1$, $A = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$;
   (c) if $r = 2$, $A = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$.
5. Then $\begin{pmatrix} M & Y \\ X & XM^{-1}Y + P^{-1}AQ^{-1} \end{pmatrix}$ is a $(t+2, 2)$ block invertible matrix.

Repeat for $(n-2)/2$ steps to obtain an $(n, 2)$ block invertible square matrix.

Acknowledgements

The original question in this note was proposed to the authors by Stanley Chow and Harold Johnson. The authors thank Paul Van Oorschot and Harold Johnson for their valuable comments on the draft of this note.

References

[1] Leonard E. Dickson, *Linear Groups, with an Exposition of Galois Field Theory*, p.77. Dover Publication, New York, 1958.

[2] N. Jacobson, *Basic Algebra I*, Freeman and Worth, 1985.

[3] H. Paley, P.M. Weichsel, *Elements of Abstract and Linear Algebra*, p.422, Holt, Rinehart, and Winston, 1972.

[4] Joan Daemen, Vincent Rijmen, *The Design of Rijndael: AES – The Advanced Encryption Standard*, Springer, 2001.

[5] FIPS 46, *Data encryption standard*, Federal Information Processing Standards Publication 46, U.S. Department of Commerce, National Bureau of Standards, 1977.

[6] C. Adams, *Constructing Symmetric Ciphers Using the CAST Design Procedure*, Designs, Codes and Cryptography, vol.12 no.3 (1997), pp.283-316.

[7] S. Chow, P. Eisen, H. Johnson, P.C. van Oorschot, *White-Box Cryptography and an AES Implementation*. TO APPEAR IN: Record of the 9th Annual Workshop on Selected Areas in Cryptography (SAC 2002), August 15-16, 2002.