Some Classes of Invertible Matrices in *GF*(2)

James S. Plank* Adam L. Buchsbaum‡

Technical Report UT-CS-07-599
Department of Electrical Engineering and Computer Science
University of Tennessee

August 16, 2007

The home for this paper is `http://www.cs.utk.edu/~plank/plank/papers/CS-07-599.html`. Please visit that link for up-to-date information about the publication status of this and related papers.

Abstract

Invertible matrices in $GF(2)$ are important for constructing MDS erasure codes. This paper proves that certain classes of matrices in $GF(2)$ are invertible, plus some additional properties about invertible matrices.

1 Introduction

We are concerned with the question of whether certain matrices in *GF*(2) are invertible. This question is important when designing erasure codes for storage applications. If an erasure code is composed solely of exclusive-or operations [1, 2, 3, 4, 5, 8, 9], then it may be represented as a matrix-vector product in *GF*(2). The act of decoding transforms an original *distribution matrix* into a square decoding matrix that must be inverted. The process is described for general $GF(2^w)$ by Plank [7] and is first used in *GF*(2) by Blomer et al. [2].

As such, a fundamental part of defining MDS erasure codes is to construct distribution matrices that result in invertible decoding matrices. This paper does not delve into erasures codes, but instead proves that certain classes of matrices in *GF*(2) are invertible. It also proves some properties of invertible matrices.

2 Nomenclature

In *GF*(2), each element is either 0 or 1; addition is the binary *exclusive-or* operator (denoted $\oplus$), and multiplication is the binary *and* operator.

When we refer to a matrix M^w, that means that M^w is a square matrix in *GF*(2) with w rows and columns. Other information about the matrix is included in the subscripts. We refer to the element in row r and column c of M^w as $M^w[r, c]$. These are zero-indexed, so the top-left element of M^w is $M^w[0, 0]$, and the bottom-right element of M^w is $M^w[w-1, w-1]$.

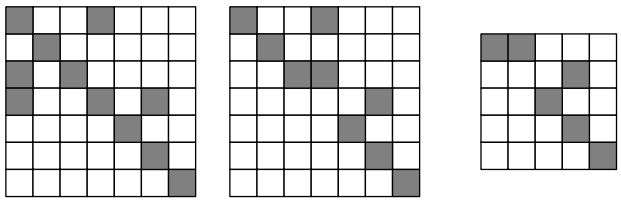
We perform arithmetic of row and column indices in M^w over the commutative ring $\mathbb{Z}/w\mathbb{Z}$. We denote the quantity x modulo w by $\overline{x}_w$. In particular, because $\overline{x+w}_w = \overline{x}_w$, we have $\overline{-1}_w = \overline{w-1}_w$. When context disambiguates, we drop the extra notation; e.g., $\overline{-1}_w = w-1$.

*Department of Electrical Engineering and Computer Science, University of Tennessee, Knoxville, TN 37996, `plank@cs.utk.edu`.
‡ AT&T Labs-Research, Shannon Laboratory, 180 Park Avenue, Florham Park, NJ 07932 , `alb@research.att.com`.

2.1 Invertibility

One way to test whether a square matrix M is invertible is to perform Gaussian Elimination on it until it is in upper triangular form. Then M is invertible if and only if the result is unit upper triangular. (Basic facts about invertibility of matrices under simple operations are available in many textbooks, e.g., Lancaster and Tismenetsky [6].)

We define steps of Gaussian Elimination as follows. Let c be the leftmost column with at least two 1's in some M^w; let r be the topmost row such that $M^w[r, c] = 1$ and $M^w[r, c'] = 0$ for $0 \leq c' < c$. Then one *step of Gaussian Elimination* or *Elimination Step* replaces every row $r' \neq r$ such that $M^w[r', c] = 1$ with the sum of rows r and r'. An example is in Figure 1. The first step of Gaussian Elimination for the matrix in Figure 1(a) replaces row 2 with the sum of rows 0 and 2, and row 3 with the sum of rows 0 and 3. The resulting matrix is in Figure 1(b).



(a) (b) (c)

Figure 1: One step of Gaussian Elimination, and deleting rows and columns that are upper-triangular.

When the leftmost ℓ columns of a matrix M^w have zeros below the main diagonal—i.e., $M[i, j] = 0$ for $0 \leq i < \ell$ and $i < j < w$—we say the leftmost ℓ columns are *in upper triangular form* or are *upper triangular*; if in addition $M^w[i, i] = 1$ for $0 \leq i < \ell$, we say the leftmost ℓ columns are *in unit upper triangular form* or are *unit upper triangular*. Assume the leftmost ℓ columns of M^w are unit upper triangular, and construct matrix $M^{w'}$, where $w' = w - \ell$, by deleting the leftmost ℓ columns and top ℓ rows of M^w. Then M^w is invertible iff $M^{w'}$ is invertible. For example, since the leftmost two columns of the matrix in Figure 1(b) are in unit upper triangular form, we may delete the leftmost two columns and the top two rows to produce the matrix in Figure 1(c). This matrix is not invertible; therefore, the matrices in Figures 1(a) and 1(b) are also not invertible.

There are other simple operations that preserve invertibility. The first are what we call *row shifting* and *column shifting*. There are four variants. Each takes an original matrix M^w and constructs a new matrix M^w_* as follows:

- Shifting up by r rows: $M^w_*[i, j] = M^w[\overline{i + r}_w, j]$, for $0 \leq i, j < w$.
- Shifting down by r rows: $M^w_*[i, j] = M^w[\overline{i - r}_w, j]$, for $0 \leq i, j < w$.
- Shifting left by c columns: $M^w_*[i, j] = M^w[i, \overline{j + c}_w]$, for $0 \leq i, j < w$.
- Shifting right by c columns: $M^w_*[i, j] = M^w[i, \overline{j - c}_w]$, for $0 \leq i, j < w$.

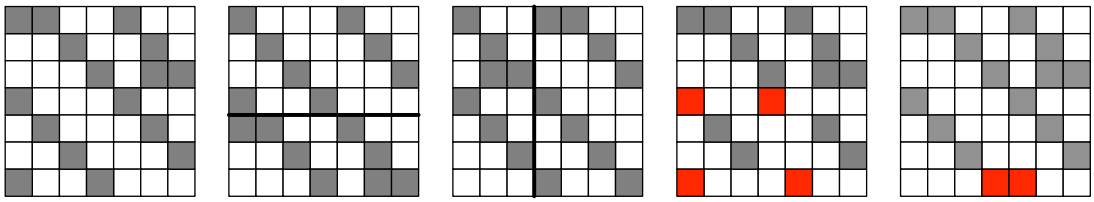
Obviously, shifting M^w up by r rows is equivalent to shifting it down by $w - r$ rows, and shifting M^w left by r columns is equivalent to shifting it right by $w - r$ columns. Swapping rows and columns preserves invertibility, and substituting any row with the sum of it and another row also preserves invertibility. Examples are in Figure 2.

We denote by I^w (rsp., $I^w_{\rightarrow c}$) the $w \times w$ identity matrix (rsp., shifted c columns to the right) and by 0^w the $w \times w$ matrix of all zeros. Finally, we say a matrix class $\mathcal{M}$ is *invertible* iff all matrices in $\mathcal{M}$ are invertible.

3 The Matrix Classes $D^w_{d,s}$ and $S^w_{d,s}$

We now define two classes of matrices: $D^w_{d,s}$ and $S^w_{d,s}$. In both: $w > 2$, $0 < d < w$, and $0 < s < w$. The letters are short for "different" and "same". We define $D^w_{d,s,0}$ to be the *base element* of $D^w_{d,s}$. We construct $D^w_{d,s,0}$ as follows:

- Start with $D^w_{d,s,0} = I^w + I^w_{\rightarrow d}$.

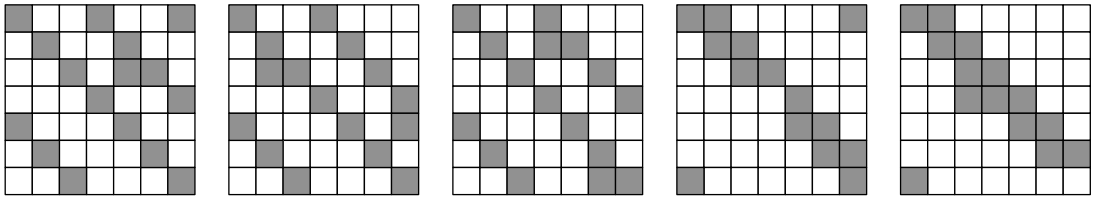


(a) (b) (c) (d) (e)

Figure 2: Operations that preserve invertibility. (a) is the original matrix. (b) shifts (a) up by three rows, or down by four rows. (c) shifts (a) left by four rows, or right by three rows. (d) swaps rows 3 and 6. (e) replaces row 6 with the sum of rows 3 and 6.

- Set $D^w_{d,s,0}[0, w-1] = D^w_{d,s,0}[0, w-1] \oplus 1$.
- Set $D^w_{d,s,0}[s, \overline{d+s-1}_w] = D^w_{d,s,0}[s, \overline{d+s-1}_w] \oplus 1$.

There are w elements of $D^w_{d,s}$, denoted $D^w_{d,s,0}, \ldots, D^w_{d,s,w-1}$. $D^w_{d,s,i}$ is equal to $D^w_{d,s,0}$ shifted i rows down and i columns to the right. Therefore, all elements of $D^w_{d,s}$ have the same invertibility. Figure 3 gives various examples. The intuition is that elements of $D^w_{d,s}$ are composed of two diagonals that differ by d columns. There are two extra bits flipped in the matrix, which are s rows apart and adjacent to **different** diagonals.



$D^7_{3,2,0}$ $D^7_{3,2,2}$ $D^7_{3,2,6}$ $D^7_{1,3,0}$ $D^7_{1,3,3}$

Figure 3: Various examples of matrices in $D^w_{d,s}$.

The definition of $S^w_{d,s}$ is similar, except the two extra bits that are flipped are adjacent to the **same** diagonal. As with $D^w_{d,s}$, we define a *base element* $S^w_{d,s,0}$ as follows:

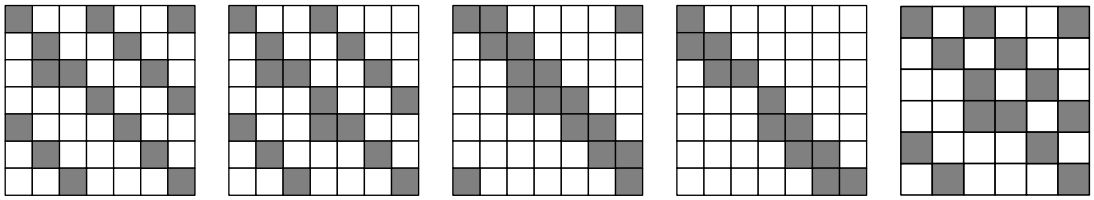
- Start with $S^w_{d,s,0} = I^w + I^w_{\rightarrow d}$.
- Set $S^w_{d,s,0}[0, w-1] = S^w_{d,s,0}[0, w-1] \oplus 1$.
- Set $S^w_{d,s,0}[s, \overline{s-1}_w] = S^w_{d,s,0}[s, \overline{s-1}_w] \oplus 1$.

As with $D^w_{d,s}$, there are w elements of $S^w_{d,s}$, denoted $S^w_{d,s,0}, \ldots, S^w_{d,s,w-1}$. $S^w_{d,s,i}$ is equal to $S^w_{d,s,0}$ shifted i rows down and i columns to the right. Note that when w is even, there are only $w/2$ distinct elements of $S^w_{d,s}$, because $S^w_{d,s,i}$ is equal to $S^w_{d,s,\overline{i+\frac{w}{2}}_w}$. We give examples of $S^w_{d,s}$ in Figure 4.

4 Simple Relationships on $D^w_{d,s}$ and $S^w_{d,s}$ that Preserve Invertibility

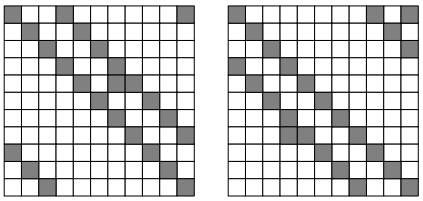
We use the following relationships on $D^w_{d,s}$ and $S^w_{d,s}$.

Lemma 1 *$D^w_{d,s}$ is invertible iff $D^w_{w-d,w-s}$ is invertible.*



$S^7_{3,2,0}$ $S^7_{3,2,2}$ $S^7_{1,3,0}$ $S^7_{6,3,0}$ $S^6_{2,3,0} = S^6_{2,3,3}$

Figure 4: Various examples of matrices in $S^w_{d,s}$.



$D^{11}_{3,4,0}$ $D^{11}_{8,7,0}$

Figure 5: $D^{11}_{8,7,0}$ is constructed from $D^{11}_{3,4,0}$ by shifting it four rows up and $(4+3)$ rows to the left.

Proof: $D^w_{w-d,w-s,0}$ can be derived by shifting $D^w_{d,s,0}$ s rows up and $s+d$ columns left. □

Figure 5 demonstrates Lemma 1.

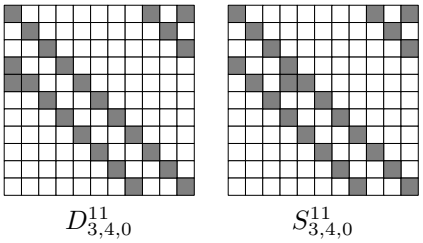
Lemma 2 *$S^w_{d,s}$ is invertible iff $S^w_{d,w-s}$ is invertible.*

Proof: $S^w_{d,s,w-s}$ is identical to $S^w_{d,w-s,0}$. □

Lemma 3 *For $s > 1$, $D^w_{d,s}$ is invertible iff $S^w_{d,s}$ is invertible.*

Proof: $S^w_{d,s,0}$ can be constructed from $D^w_{d,s,0}$ by substituting row s with row s plus row $(s-1)$. □

Figure 6 demonstrates Lemma 3.

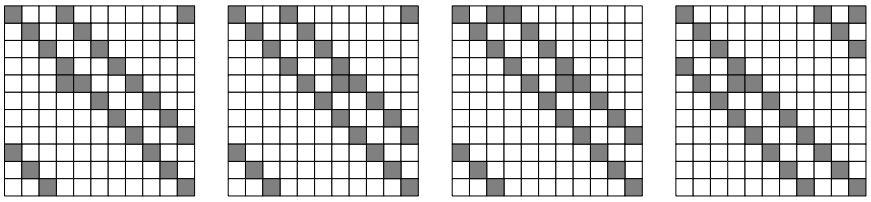


$D^{11}_{3,4,0}$ $S^{11}_{3,4,0}$

Figure 6: $S^{11}_{3,4,0}$ is constructed from $D^{11}_{3,4,0}$ by substituting row 4 with row 4 plus row 3.

Lemma 4 *For $0 < s < w-1$, $S^w_{d,s}$ is invertible iff $S^w_{w-d,s}$ is invertible.*

Proof: $S^w_{w-d,s,0}$ can be constructed from $S^w_{d,s,0}$ by first substituting row s with row s plus row $(s-1)$ and row 0 with row 0 plus row $w-1$, and then shifting the result d columns to the left. □



(a) $S^{11}_{3,4,0}$ (b) (c) (d) $S^{11}_{8,4,0}$

Figure 7: (b) is created by substituting row 4 with row 4 plus row 3. (c) is created by substituting row 0 with row 0 plus row 10. (d) is created by shifting left three columns.

Lemma 4 is demonstrated by Figure 7, where each step of converting $S^{11}_{3,4,0}$ to $S^{11}_{8,4,0}$ is shown.

The constraints on s in Lemmas 3 and 4 are due to the following. When $s = 1$, adding rows 0 and 1 does not have the desired effect of moving row s's one from one diagonal to the other, because row 0 has three ones. When $s = w-1$, adding rows 0 and $w - 1$ has the same problem.

For convenience in the sequel, we consider invertibility to be an equivalence relation, so two matrices or matrix classes are *equivalent* iff they are both invertible or both not invertible.

5 Our Target Class of Matrices, $\mathcal{L}$, and the Grand Liberation Theorem

We define the class $\mathcal{L}$ to be the union of all $D^w_{d,s}$ such that:

- $w > 1$ is odd.
- *GCD*$(d, w) = 1$.
- If d is even, $s = w - \frac{d}{2}$.
- If d is odd, $s = \frac{w-d}{2}$.

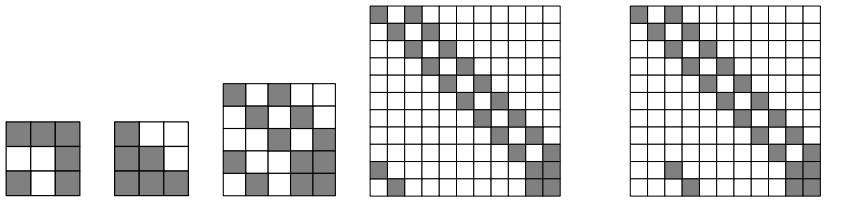
Theorem 5 (The Grand Liberation Theorem) *All matrices in $\mathcal{L}$ are invertible.*

The rest of this paper proves the theorem. After demonstrating a few special cases, which include $D^{\,3}_{1,1}$, the proof proceeds as follows:

1. We prove by induction that $D^w_{2,w-1}$ is invertible for all odd w.
2. For $d > 2$, we first show that for any odd d there exists some even d' such that $D^w_{d,\frac{w-d}{2}}$ is equivalent to $D^w_{d',w-\frac{d'}{2}}$. Hence we restrict our attention to even $d > 2$.
3. We show that for any even $d > 2$, $D^w_{d,w-\frac{d}{2}}$ is equivalent to $S^w_{d,\frac{d}{2}}$.
4. We show that the derived $S^w_{d,\frac{d}{2}}$ is equivalent to some $S^{w'}_{d',\frac{w'}{2}}$ with $2 < w' < w$, w' even, and *GCD*$(w', d') = 1$.
5. We show that any $S^w_{d,\frac{w}{2}}$ with even $w > 2$ and *GCD*$(w, d) = 1$ is equivalent to some $D^{w'}_{d',s'} \in \mathcal{L}$ such that $w' < w$.
6. A second inductive argument completes the proof, as we can iterate Steps 2–5 until $w' = 3$ or $d' = 2$ in Step 5.

5.1 Step 1: Base Cases for the Global Induction

First, there are only two $D^3_{d,s} \in \mathcal{L}$: $D^3_{1,1}$ and $D^3_{2,2}$. Their base elements are shown in Figure 8(a) and (b). It is easy to verify that they are invertible. Additionally, Figure 8(c) shows $D^5_{2,4,4}$, which will be used below. It is also easy to verify that it is invertible.



(a) $D^3_{1,1,0}$ (b) $D^3_{2,2,0}$ (c) $D^5_{2,4,4}$ (d) $D^{11}_{2,10,10}$ (e) $D^{11}_{2,10,10}$ after two steps of Gaussian Elimination.

Figure 8: Base cases for the inductive proof.

We now prove that $D^w_{2,w-1}$ is invertible for all odd w. We have already shown in Figure 8 that this is true for $w = 3$ and $w = 5$. Let $w > 5$ be odd, and assume by induction that $D^{w'}_{2,w'-1}$ is invertible for odd $1 < w' < w$. Consider $D^w_{2,w-1,w-1}$. An example is $D^{11}_{2,10,10}$, depicted in Figure 8(d). This matrix has a very specific format: All elements of I and $I_{\rightarrow 2}$ are set to one, as are $D^w_{2,w-1,w-1}[w-1][w-2]$ and $D^w_{2,w-1,w-1}[w-2][w-1]$.

Now, perform two steps of Gaussian Elimination. This will set $D^w_{2,w-1,w-1}[w-2,0]$ and $D^w_{2,w-1,w-1}[w-1,1]$ to zero, and $D^w_{2,w-1,w-1}[w-2,2]$ and $D^w_{2,w-1,w-1}[w-1,3]$ to one. Figure 8(e) demonstrates for $w = 11$. The resulting matrix's first two columns are unit upper triangular, so the first two rows and columns may be deleted. This yields $D^{w-2}_{2,w-3,w-3}$, which is of the form $D^{w'}_{2,w'-1,w'-1}$ for some odd $1 < w' < w$. By induction, $D^{w'}_{2,w'-1,w'-1}$ is invertible. Therefore, $D^w_{2,w-1}$ is invertible for all odd $w > 1$.

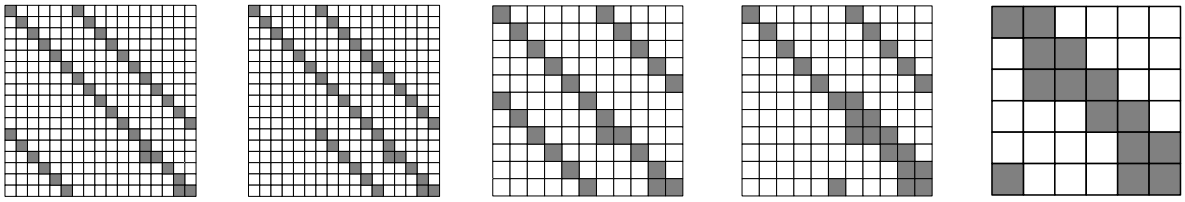
5.2 Steps 2–4: Reducing the Problem to $S^w_{d,\frac{w}{2}}$ for w Even, $GCD(w,d) = 1$

Now consider any $D^w_{d,\frac{w-d}{2}} \in \mathcal{L}$ such that d is odd. By Lemma 1, this is equivalent to $D^w_{w-d,w-\frac{w-d}{2}}$. Since $w - d$ is an even number, $D^w_{w-d,w-\frac{w-d}{2}} \in \mathcal{L}$. Therefore, every element $D^w_{d,s} \in \mathcal{L}$ for which d is odd has a corresponding element $D^w_{d',s'} \in \mathcal{L}$ for which d' is even. Thus we need only prove that the elements $D^w_{d,w-\frac{d}{2}} \in \mathcal{L}$ with even d are invertible. We proved above that $D^w_{2,w-1}$ is invertible, so we now prove that $D^w_{d,w-\frac{d}{2}}$ is invertible for even $d > 2$.

Therefore, consider $D^w_{d,w-\frac{d}{2}}$ such that $d > 2$ is even, $w > 3$ is odd, and $GCD(w,d) = 1$. Since $d > 2$, it follows that $w - \frac{w-1}{2} = \frac{w-1}{2} \leq w - \frac{d}{2} \leq w - 2$. Since $w > 3$, the smallest value that $w - \frac{d}{2}$ may be is $\frac{5-1}{2} = 2$. Therefore, by Lemma 3, $D^w_{d,w-\frac{d}{2}}$ is equivalent to $S^w_{d,w-\frac{d}{2}}$, which by Lemma 2 is equivalent to $S^w_{d,w-(w-\frac{d}{2})} = S^w_{d,\frac{d}{2}}$.

So now consider $S^w_{d,\frac{d}{2},w-\frac{d}{2}-1}$. An example is $S^{17}_{6,3,13}$, depicted in Figure 9(a). Suppose $w > 2d$. (w will not equal $2d$, because $GCD(w,d) = 1$.) Perform d steps of Gaussian Elimination on $S^w_{d,\frac{d}{2},w-\frac{d}{2}-1}$. This moves the ones in rows $w - d$ through $w - 1$ from columns 0 through $d - 1$ to columns d through $2d - 1$. In our example of $S^{17}_{6,3,13}$, six steps of Gaussian Elimination are shown in Figure 9(b). Therefore, when we delete the first d rows and columns of the resulting matrix, we are left with $S^{w-d}_{d,\frac{d}{2},w-d-\frac{d}{2}-1}$. Note: $w - d$ is odd; $w - d > d$; and since $GCD(w,d) = 1$, $GCD(w - d, d) = 1$. Our example continues in Figure 9(c), where we delete the first six rows and columns of Figure 9(b) to get $S^{11}_{6,3,7}$.

Iterate this process until it yields $S^w_{d,\frac{d}{2},w-\frac{d}{2}-1}$ for $d < w < 2d$. We now perform $(w - d)$ steps of Gaussian Elimination. This moves the leftmost ones in rows $(w - d)$ through $(2(w - d) - 1)$ over d columns to the right. When we delete the first $w - d$ rows and columns, we are left with $S^d_{d-(w-d),\frac{d}{2},\frac{d}{2}-1} = S^d_{2d-w,\frac{d}{2},\frac{d}{2}-1}$. Since $GCD(w,d) = 1$, $GCD(d, 2d - w) = 1$ as well.



(a) $S^{17}_{6,3,13}$ (b) Six Elimination Steps (c) $S^{11}_{6,3,7}$ (d) Five Elimination Steps (e) $S^{6}_{1,3,2}$

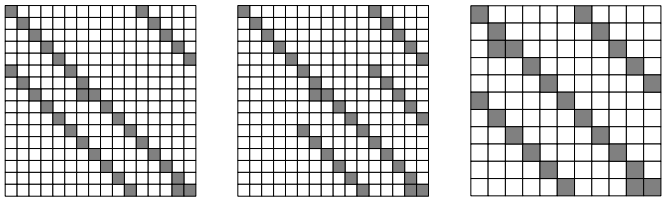
Figure 9: An example of converting $S^{\,w}d, \frac{d}{2}$ to $S^{d}_{x,\frac{d}{2}}$ for $w = 17$ and $d = 6$.

Figure 9(d) shows $11 - 6 = 5$ steps of Gaussian Elimination of $S^{11}_{6,3,7}$, and Figure 9(e) shows that $S^{6}_{1,3,2}$ results when we delete the first five rows and columns from Figure 9(d).

We have thus reduced the original problem to the following: Given $S^{\,w'}_{d',\frac{w'}{2}}$ with even $w' > 2$ and $GCD(w', d') = 1$, determine whether $S^{w'}_{d',\frac{w'}{2}}$ invertible. We address this in the next section.

5.3 Steps 5–6: Proving that $S^{w}_{d,\frac{w}{2}}$ is Invertible for w Even, $GCD(w, d) = 1$

Since $w > 2$, it follows that $1 < \frac{w}{2} < w - 1$. Therefore, by Lemma 4, $S^{w}_{d,\frac{w}{2}}$ is equivalent to $S^{w}_{w-d,\frac{w}{2}}$, so we may assume that $d > \frac{w}{2}$. We're going to break this proof into two cases. The first is when $d > \frac{w}{2} + 1$. Consider $S^{w}_{d,\frac{w}{2},\frac{w}{2}-1}$. An example of this is $S^{16}_{11,8,7}$ displayed in Figure 10(a). We perform $w-d$ steps of Gaussian Elimination on $S^{\,w}_{d,\frac{w}{2},\frac{w}{2}-1}$. Since $d > \frac{w}{2} + 1$, we know that $w - d < \frac{w}{2} - 1$, so the $w - d$ steps of Gaussian Elimination simply move the leftmost ones in rows $(w - d)$ through $(2(w - d) - 1)$ over d columns to the right. Deleting the first $w - d$ rows and columns from the matrix, we are left with $S^{d}_{2d-w,\frac{w}{2},d-\frac{w}{2}-1}$. These steps are shown in Figures 10(b) and (c), as $S^{16}_{11,8,7}$ is converted into into $S^{11}_{6,8,2}$.



(a) $S^{16}_{11,8,7}$ (b) 5 Elimination Steps (c) $S^{11}_{6,8,2}$

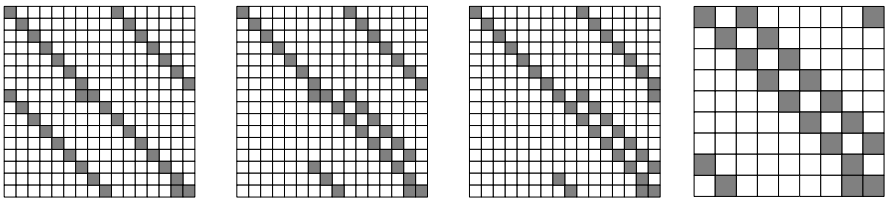
Figure 10: An example of converting $S^{\,w}d, \frac{w}{2}$ to $S^{d}_{2d-w,\frac{w}{2}}$ for $w = 16$ and $d = 11$.

As before, since $GCD(w, d) = 1$, we know that $GCD(2d - w, d) = 1$. That w is even implies that $2d - w$ is also even. Moreover, since $d > \frac{w}{2} + 1$, we know that $2d - w > 1$. Therefore, by Lemma 3, $S^{d}_{2d-w,\frac{w}{2}}$ is equivalent to $D^{d}_{2d-w,\frac{w}{2}}$. Finally:

$$\begin{aligned} d - \frac{2d - w}{2} &= \frac{2d - 2d + w}{2} \\ &= \frac{w}{2}. \end{aligned}$$

Therefore, $D^d_{2d-w,\frac{w}{2}} = D^d_{2d-w,d-\frac{2d-w}{2}}$, which is an element of $\mathcal{L}$. By induction, $D^d_{2d-w,d-\frac{2d-w}{2}}$ is invertible, implying that $S^w_{d,\frac{w}{2}}$ is invertible.

The second case is for $S^w_{d,\frac{w}{2}}$ when $d = \frac{w}{2}+1$ and $GCD(w, \frac{w}{2}+1) = 1$. An example is $S^{16}_{9,8,7}$ shown in Figure 11(a). Again, we will perform $w-d$ elimination steps. We will do this in two parts, however. In the first part, we perform $w-d-1$ elimination steps. This moves the leftmost ones in rows $(w-d)$ through $(2(w-d)-2)$ over d columns to the right. This is pictured in Figure 11(b). The last elimination step replaces two rows of the matrix, because row $(w-d)$ has an extra one adjacent to the diagonal. Therefore, both rows $(w-d)$ and $(2(w-d)-1)$ move their leftmost ones into the column $(w-1)$. This is pictured in Figure 11(c).



(a) $S^{16}_{9,8,7}$ (b) 6 Elimination Steps (c) 1 More (d) $S^9_{2,8,0}$

Figure 11: An example of converting $S^w d, \frac{w}{2}$ to $S^d 2, d-1$ when $d = \frac{w}{2}+1$ for $w = 16$.

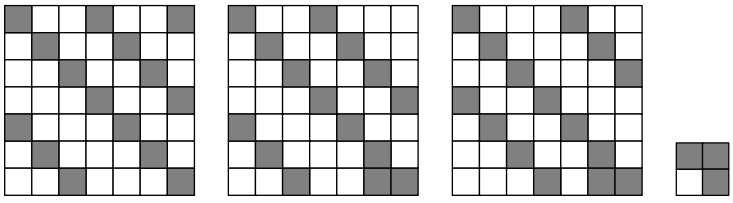
When the first $w-d$ rows and columns are deleted from the matrix, we are left with $S^{\,d}_{2d-w,\frac{w}{2},0}$. Since $d = \frac{w}{2}+1$, this is equal to $S^d_{2,d-1,0}$ (shown as $S^9_{2,8,0}$ in Figure 11(d)). That $w > 2$ is even implies that $d = \frac{w}{2}+1 > 2$ is odd, so $d-1 > 1$; thus by Lemma 3, $S^d_{2,d-1}$ is equivalent to $D^d_{2,d-1}$, which we proved invertible in Section 5.1. Therefore $S^w_{d,\frac{w}{2}}$ is invertible. Q.E.D.

6 The Class $\mathcal{O}$ and the Little Liberation Theorem

We now define a third class of matrices, O^w_d such that $w > d \geq 1$. We define $O^w_{d,0}$ to be the *base element* of O^w_d and construct $O^w_{d,0}$ as follows:

- Start with $O^w_d = I^w + I^w_{\rightarrow d}$.
- Set $O^w_{d,0}[0, w-1] = O^w_{d,0}[0, w-1] \oplus 1$.

Thus, $O^w_{d,0}$ is similar to $D^w_{d,s,0}$ and $S^w_{d,s,0}$, except it only has one extra one in it, in the top-right corner. There are w elements of O^w_d, denoted $O^w_{d,0}, \ldots, O^w_{d,w-1}$. $O^w_{d,i}$ is equal to $O^w_{d,0}$ shifted i rows down and i columns to the right. Therefore, all elements of O^w_d are equivalent. We show some examples of matrices in O^w_d in Figure 12.



(a) $O^7_{3,0}$ (b) $O^7_{3,6}$ (c) $O^7_{4,6}$ (d) $O^2_{1,1}$

Figure 12: Examples of matrices in O^w_d.

We start with a simple lemma:

Lemma 6 *O_d^w is invertible iff O_{w-d}^w is invertible.*

Proof: $O_{w-d,w-1}^w$ can be derived by replacing row $w-1$ of $O_{d,w-1}^w$ with the sum of rows $w-1$ and $w-2$, and shifting the resulting matrix d columns to the left. An example is in Figure 12, where $O_{4,6}^7$ may be obtained by replacing row 6 of $O_{3,6}^7$ with the sum of rows 5 and 6, and shifting the result three columns to the left. □

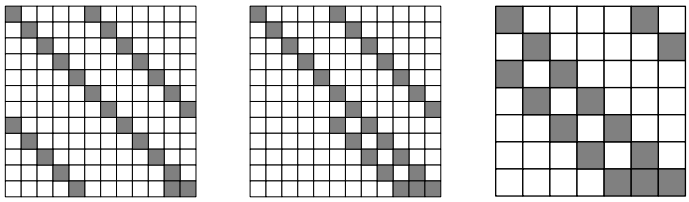
Define $\mathcal{O}$ to be the union of all O_d^w such that $GCD(w,d) = 1$.

Theorem 7 (The Little Liberation Theorem) *All matrices in $\mathcal{O}$ are invertible.*

Proof: This proof is far simpler than that of the Grand Liberation Theorem. It, too, is inductive. We start with the base case O_1^2, an element of which is pictured in Figure 12(d). This matrix is already in unit upper triangular form and is therefore invertible.

Now, consider $O_d^w \in \mathcal{O}$ and suppose by induction that $O_{d'}^{w'} \in \mathcal{O}$ is invertible for all $1 \leq d' < w' < w$. By Lemma 6 and the hypothesis that $GCD(w,d) = 1$, we may assume that $d < \frac{w}{2}$, or else we consider O_{w-d}^w in lieu of O_d^w. Performing d elimination steps on $O_{d,w-1}^w$ moves the leftmost ones in rows $w-d$ through $w-1$ over d columns to the right. Since $d < \frac{w}{2}$, these ones will not be moved to the diagonal, nor will the one at $O_{d,w-1}^w[w-1, w-2]$ be affected. Therefore deleting the leftmost d columns, which are now unit upper triangular, and top d rows leaves $O_{d,w-d-1}^{w-d}$. Since $GCD(w,d) = 1$, $GCD(w-d,d) = 1$, and therefore $O_{d,w-d-1}^{w-d} \in \mathcal{O}$. By induction, O_d^{w-d} is invertible; therefore O_d^w is invertible. □

An example is depicted in Figure 13 where $O_{5,11}^{12}$ is converted to $O_{5,6}^7$ by five elimination steps.



(a) $O_{5,11}^{12}$ (b) Five elimination steps (c) $O_{5,6}^7$

Figure 13: An example of converting $O_{d,w-1}^w$ to $O_{d,w-d-1}^{w-d}$.

7 Some Trivial Properties of Matrices in $GF(2)$

The following two lemmas are likely folklore, but we include them for completeness.

Lemma 8 *If some matrix M^w has precisely w ones, then M^w is invertible iff it is a permutation matrix.*

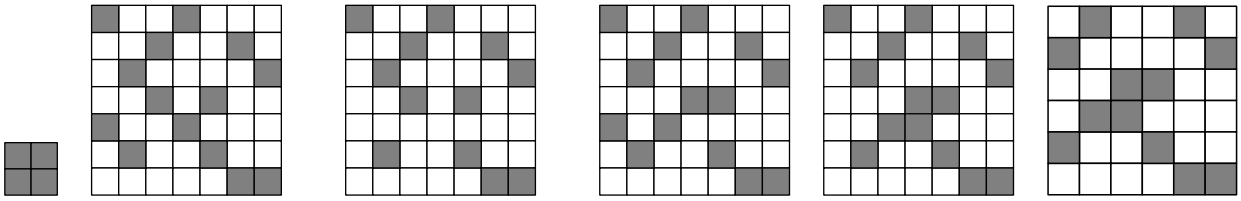
Proof: Any permutation matrix is invertible. Conversely, if M^w has precisely w ones but is not a permutation matrix, then some row or column contains all zeros, in which case M^w is not invertible. □

Lemma 9 *Let M_1^w and M_2^w be permutation matrices. The sum $M_1^w + M_2^w$ is not invertible.*

Proof: Let $M^w = M_1^w + M_2^w$. Suppose there exist r and c such that $M_1^w[r,c] = M_2^w[r,c] = 1$. Then row r of M^w contains all zeros, so M^w is not invertible. Thus, we assume there are no such r and c; in this case, M has precisely two ones in each row and column. We prove by induction that such matrices are not invertible.

The base case is shown in Figure 14(a), which depicts the only M^2 with two ones in each row and column. This matrix is clearly not invertible.

Now, let matrix M^w for some $w > 2$ have exactly two ones in each row and column. Let rows r_1 and r_2 be the two rows that have ones in column zero, and let $c_1, c_2 > 0$ be such that $M^w[r_1, c_1] = M^w[r_2, c_2] = 1$. Swap row r_1 with row 0, and perform one elimination step. This will set $M^w[r_2, 0] = 0$ and $M^w[r_2, c_1] = M^w[r_2, c_1] \oplus 1$. If $c_1 = c_2$, then all of row r_2's elements become zero, so M^w is not invertible. If $c_1 \neq c_2$, then deleting the first row and column leaves a matrix M^{w-1} with exactly two ones in each row and column. By induction, this new matrix in not invertible; therefore M^w is also not invertible. □



(a) M^2. (b) M^7, $c_1 = c_2 = 3$. (c) After one elimination step, Row 4 is all zeros. (d) M^7, $c_1 = 3, c_2 = 2$. (e) After one elimination step. (f) M^6.

Figure 14: Matrices with two ones in each row and column.

We show examples of the elimination step in Figure 14(b)-(f). In Figure 14(b), the elimination step, depicted in Figure 14(c) turns row 4 into all zeros. In Figure 14(d), the elimination step of the matrix M^7 results in Figure 14(e), which is equivalent to a matrix M^6 (Figure 14(f)).

8 A Final Theorem on the Invertibility of a Type of $(k+2)w \times kw$ Matrix

Let row r of some matrix M^w contain precisely one one—we call such a row an *identity row*—and let the one be in column c. By cofactor expansion, deleting row r and column c yields an equivalent matrix M^{w-1}.

The remaining theorem concerns a $(k+2) \times k$ block matrix $\mathcal{A}$, structured as follows and pictured in Figure 15:

- Each block is $w \times w$.
- Block $\mathcal{A}[i, i] = I^w$ for $0 \leq i < k$.
- Blocks $\mathcal{A}[i, j] = \mathcal{A}[j, i] = 0^w$ for $0 \leq i < j < k$.
- Block $\mathcal{A}[k, j] = I^w$ for $0 \leq j < k$.
- Block $\mathcal{A}[k+1, j] = X_j$ for $0 \leq j < k$ and some given X_j.

Consider the class $\mathcal{A}^*$ of $\binom{k+2}{2}$ block matrices induced by deleting any two rows of blocks from $\mathcal{A}$.

Theorem 10 *All matrices in $\mathcal{A}^*$ are invertible iff (1) every X_i is invertible, and (2) for $0 \leq i < j < k$, $X_i + X_j$ is invertible.*

Proof: Let $A \in \mathcal{A}^*$. There are four cases.

Case 1: A is composed of the first k rows of blocks of $\mathcal{A}$, which form I^{kw}.

Case 2: A is composed of row k and any $k-1$ of the first k rows of blocks of $\mathcal{A}$. Now, A has $(k-1)w$ identity rows. Deleting these rows and their associated columns yields I^w.

Case 3: A is composed of row $k+1$ and any $k-1$ of the first k rows of blocks of $\mathcal{A}$; let i be the omitted row of blocks from the first k. Again, A has $(k-1)w$ identity rows, which we can delete with their associated columns to yield X_i, so A is equivalent to X_i.

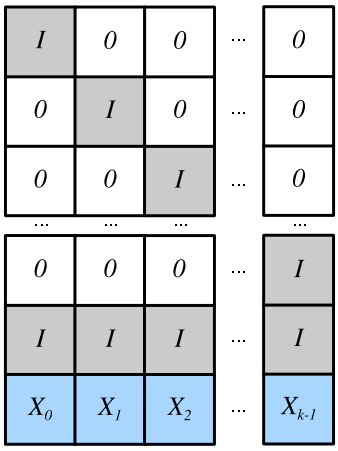


Figure 15: The $(k+2) \times k$ block matrix $\mathcal{A}$ of $w \times w$ matrices over *GF*(2).

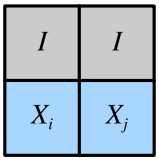


Figure 16: The $2w \times 2w$ matrix that results when $w(k-2)$ identity rows are deleted from A in Case 4.

Case 4: A is composed of rows k, $k+1$, and any $k-2$ of the first k rows of blocks of $\mathcal{A}$; let i and j be the omitted rows of blocks from the first k. Now A has $(k-2)w$ identity rows, which we can delete with their associated columns to yield the matrix pictured in Figure 16.

Now, perform w elimination steps on this matrix. For each r and c such that $X_i[r,c] = 1$, the elimination step for column c will replace row $w+r$ with the sum of rows $w+r$ and c. This will set $X_i[r,c] = 0$ and $X_j[r,c] = X_j[r,c] \oplus 1$. After the elimination steps, the leftmost w columns will be upper triangular, and deleting them leaves $X_i + X_j$. Therefore, A is equivalent to $X_i + X_j$. □

9 Acknowledgements

This material is based upon work supported by the National Science Foundation under grants CNS-0437508 and CNS-0615221.

References

[1] M. Blaum, J. Brady, J. Bruck, and J. Menon. EVENODD: An efficient scheme for tolerating double disk failures in RAID architectures. *IEEE Transactions on Computing*, 44(2):192– 202, February 1995.

[2] J. Blomer, M. Kalfane, M. Karpinski, R. Karp, M. Luby, and D. Zuckerman. An XOR-based erasure-resilient coding scheme. Technical Report TR-95-048, International Computer Science Institute, August 1995.

[3] P. Corbett, B. English, A. Goel, T. Grcanac, S. Kleiman, J. Leong, and S. Sankar. Row diagonal parity for double disk failure correction. In *4th Usenix Conference on File and Storage Technologies*, San Francisco, CA, March 2004.

[4] J. L. Hafner. WEAVER Codes: Highly fault tolerant erasure codes for storage systems. In *FAST-2005: 4th Usenix Conference on File and Storage Technologies*, pages 211–224, San Francisco, December 2005.

[5] J. L. Hafner. HoVer erasure codes for disk arrays. In *DSN-2006: The International Conference on Dependable Systems and Networks*, Philadelphia, June 2006. IEEE.

[6] P. Lancaster and M. Tismenetsky. *The Theory of Matrices*. Computer Science and Applied Mathematics. Academic Press, San Diego, CA, second edition, 1985.

[7] J. S. Plank. A tutorial on Reed-Solomon coding for fault-tolerance in RAID-like systems. *Software – Practice & Experience*, 27(9):995–1012, September 1997.

[8] J. S. Plank and L. Xu. Optimizing Cauchy Reed-Solomon codes for fault-tolerant network storage applications. In *NCA-06: 5th IEEE International Symposium on Network Computing Applications*, Cambridge, MA, July 2006.

[9] J. J. Wylie and R. Swaminathan. Determining fault tolerance of XOR-based erasure codes efficiently. In *DSN-2007: The International Conference on Dependable Systems and Networks*, Edinburgh, Scotland, June 2007. IEEE.