All or nothing at all*

Paolo D'Arco
Dipartimento di Informatica
Università degli Studi di Salerno
84084 Fisciano (SA), Italy

Navid Nasr Esfahani
David R. Cheriton School of Computer Science
University of Waterloo
Waterloo, Ontario N2L 3G1, Canada

Douglas R. Stinson†
David R. Cheriton School of Computer Science
University of Waterloo
Waterloo, Ontario N2L 3G1, Canada

Submitted: Aug 11, 2016; Accepted: Oct 5, 2016; Published: Oct 14, 2016
Mathematics Subject Classifications: 05B05, 05B10, 05B20, 94A60

Abstract

We continue a study of unconditionally secure all-or-nothing transforms (AONT) begun by Stinson (2001). An AONT is a bijective mapping that constructs s outputs from s inputs. We consider the security of t inputs, when $s-t$ outputs are known. Previous work concerned the case $t = 1$; here we consider the problem for general t, focussing on the case $t = 2$. We investigate constructions of binary matrices for which the desired properties hold with the maximum probability. Upper bounds on these probabilities are obtained via a quadratic programming approach, while lower bounds can be obtained from combinatorial constructions based on symmetric BIBDs and cyclotomy. We also report some results on exhaustive searches and random constructions for small values of s.

1 Introduction

Rivest defined all-or-nothing transforms in [10] in the setting of computational security. Stinson considered unconditionally secure all-or-nothing transforms in [12]. Here we extend some of the results in [12] by considering more general types of unconditionally secure all-or-nothing transforms.

Let X be a finite set, called an *alphabet*. Let s be a positive integer, and suppose that $\phi : X^s \to X^s$. We will think of ϕ as a function that maps an input s-tuple, say

*We have "borrowed" the title of this paper from the classic song of the same name written by Altman and Lawrence in 1939. It was recorded by Frank Sinatra and the Harry James Orchestra in 1939, and became a huge hit in 1943.

†D. Stinson's research is supported by NSERC discovery grant 203114-11.

$\mathbf{x} = (x_1, \ldots, x_s)$, to an output s-tuple, say $\mathbf{y} = (y_1, \ldots, y_s)$, where $x_i, y_i \in X$ for $1 \leqslant i \leqslant s$. Informally, the function ϕ is an unconditionally secure *all-or-nothing transform* provided that the following properties are satisfied:

1. ϕ is a bijection.
2. If any $s-1$ of the s output values $y_1, \ldots, y_s$ are fixed, then the value of any one input value x_i ($1 \leqslant i \leqslant s$) is completely undetermined, in an information-theoretic sense.

We will denote such a function as an (s, v)-AONT, where $v = |X|$.

The above definition can be rephrased in terms of the entropy function, H, as follows. Let $X_1, \ldots, X_s, Y_1, \ldots, Y_s$ be random variables taking on values in the finite set X. (The variables $X_1, \ldots, X_s$ need not be independent, or uniformly distributed.) Then these $2s$ random variables define an AONT provided that the following conditions are satisfied:

1. $\mathsf{H}(Y_1, \ldots, Y_s \mid X_1, \ldots, X_s) = 0$.
2. $\mathsf{H}(X_1, \ldots, X_s \mid Y_1, \ldots, Y_s) = 0$.
3. $\mathsf{H}(X_i \mid Y_1, \ldots, Y_{j-1}, Y_{j+1}, \ldots, Y_s) = \mathsf{H}(X_i)$ for all i and j such that $1 \leqslant i \leqslant s$ and $1 \leqslant j \leqslant s$.

Rivest [10] defined AONT to provide a mode of operation for block ciphers that would require the decryption of all blocks of an encrypted message in order to determine any specific single block of plaintext. He called it the "package transform". The method is very simple and elegant. Suppose we are given s blocks of plaintext, $(x_1, \ldots, x_s)$. First, we apply an AONT, computing $(y_1, \ldots, y_s) = \phi(x_1, \ldots, x_s)$. Then we encrypt $(y_1, \ldots, y_s)$ using a block cipher. At the receiver's end, the ciphertext is decrypted, and then the inverse transform ϕ^{-1} is applied to restore the s plaintext blocks. Note that the transform ϕ is not secret. Extensions of this technique are studied in [1, 5].

All-or-nothing transforms have turned out to have numerous applications in cryptography and security. Here are some representative examples:

- exposure-resilient functions [2]
- network coding [3, 6]
- secure data transfer [14]
- anti-jamming techniques [9]
- secure distributed cloud storage [8, 11]
- query anonymization for location-based services [15].

We note that the above definition of an unconditionally secure AONT does not say anything regarding partial information that might be revealed about more than one of the s input values. For example, it does not rule out the possibility of determining the exclusive-or of two input values, given some relatively small number of output values. This motivates the following more general definition. Let $1 \leqslant t \leqslant s$. We will say that ϕ is a *t-all-or-nothing transform* (or *t-AONT*) provided that the following properties are satisfied:

1. ϕ is a bijection.

2. If any $s-t$ of the s output values $y_1, \ldots, y_s$ are fixed, then any t of the input values x_i $(1 \leqslant i \leqslant s)$ are completely undetermined, in an information-theoretic sense.

We will denote such a function as a (t, s, v)-AONT, where $v = |X|$. Note that the original definition corresponds to a 1-all-or-nothing transform.

This definition can also be rephrased in terms of the entropy function. As before, let $X_1, \ldots, X_s, Y_1, \ldots, Y_s$ be random variables taking on values in the finite set X. These $2s$ random variables define a t-AONT provided that the following conditions are satisfied:

1. $\mathsf{H}(Y_1, \ldots, Y_s \mid X_1, \ldots, X_s) = 0$.

2. $\mathsf{H}(X_1, \ldots, X_s \mid Y_1, \ldots, Y_s) = 0$.

3. For all $\mathcal{X} \subseteq \{X_1, \ldots, X_s\}$ with $|\mathcal{X}| = t$, and for all $\mathcal{Y} \subseteq \{Y_1, \ldots, Y_s\}$ with $|\mathcal{Y}| = t$, it holds that
$$\mathsf{H}(\mathcal{X} \mid \{Y_1, \ldots, Y_s\} \setminus \mathcal{Y}) = \mathsf{H}(\mathcal{X}). \tag{1}$$

Note that the first two conditions are just saying that the associated function ϕ is a bijection.

1.1 Organization of the Paper

The rest of this paper is organized as follows. In Section 2, we give our basic result that characterizes linear AONT in terms of matrices having invertible submatrices. We also give a construction using Cauchy matrices over a finite field $\mathbb{F}_q$, which is applicable provided that $q \geqslant 2s$. It turns out that it is impossible to construct linear AONT over $\mathbb{F}_2$, so an interesting question is how "close" one can get to an AONT in this setting. In Section 3, we give some preliminary results and analyze one infinite class of matrices. In Section 4, we derive an upper bound on the maximum number of invertible 2 by 2 submatrices of an invertible s by s $0-1$ matrix (this is relevant for the study of 2-AONT). We use a method based on quadratic programming to prove our bound. In Section 5, we discuss five construction methods for invertible s by s $0-1$ matrices containing a large number of invertible 2 by 2 submatrices. The five methods are:

1. exhaustive search,

2. a random construction,

3. a recursive construction,

4. a construction using symmetric balanced incomplete block designs (SBIBDs), and

5. a construction based on cyclotomy.

We achieve our best asymptotic results from SBIBDs, where we have an infinite class of examples that are close to the upper bound derived in the previous section. In Section 6, we turn to arbitrary (i.e., linear or nonlinear) AONT, and describe some connections with orthogonal arrays. Finally, Section 7 is a brief summary.

2 Linear AONT

We are mainly going to consider linear transforms. Let $\mathbb{F}_q$ be a finite field of order q. An AONT with alphabet $\mathbb{F}_q$ is *linear* if each y_i is an $\mathbb{F}_q$-linear function of $x_1, \ldots, x_s$. Then, we can write $\mathbf{y} = \phi(\mathbf{x}) = \mathbf{x}M^{-1}$ and $\mathbf{x} = \phi^{-1}(\mathbf{y}) = \mathbf{y}M$, where M is an invertible s by s matrix with entries from $\mathbb{F}_q$.

We will also be interested in functions that satisfy the condition (1) for certain (but not necessarily all) pairs $\mathcal{X}, \mathcal{Y}$. This will be particularly relevant in the case where ϕ is a binary linear transform. More specifically, suppose $q = 2^r$ for some $r \geqslant 1$ and M is defined over the subfield $\mathbb{F}_2$ (so M is a $0-1$ matrix). This could be desirable from an efficiency point of view, because the only operations required to compute the transform are exclusive-ors of bitstrings. However, it turns out that there are no nontrivial 1-AONT (a fact that was already observed in [12]). So it is a reasonable and interesting problem to study how close we can get to an AONT in this setting. We will give a precise answer to this question for $t = 1$ in Theorem 8; much of the rest of this paper will study the corresponding problem when $t = 2$.

For $I, J \subseteq \{1, \ldots, s\}$, define $M(I, J)$ to be the $|I|$ by $|J|$ submatrix of M induced by the *columns* in I and the *rows* in J. The following lemma characterizes linear all-or-nothing transforms in terms of properties of the matrix M. This lemma can be considered to be a generalization of [12, Theorem 2.1].

Lemma 1. *Suppose that q is a prime power and M is an invertible s by s matrix with entries from $\mathbb{F}_q$. Let $\mathcal{X} \subseteq \{X_1, \ldots, X_s\}$, $|\mathcal{X}| = t$, and let $\mathcal{Y} \subseteq \{Y_1, \ldots, Y_s\}$, $|\mathcal{Y}| = t$. Then the function $\phi(\mathbf{x}) = \mathbf{x}M^{-1}$ satisfies (1) with respect to $\mathcal{X}$ and $\mathcal{Y}$ if and only if the submatrix $M(I, J)$ is invertible, where $I = \{i : X_i \in \mathcal{X}\}$ and $J = \{j : Y_j \in \mathcal{Y}\}$.*

Proof. Let $\mathbf{x}' = (x_i : i \in I)$. We have $\mathbf{x}' = \mathbf{y}M(I, \{1, \ldots, s\})$. Now assume that y_j is fixed for all $j \in J$. Then we can write $\mathbf{x}' = \mathbf{y}'M(I, J) + \mathbf{c}$, where $\mathbf{y}' = (y_j : j \in J)$ and $\mathbf{c}$ is a vector of constants. If $M(I, J)$ is invertible, then $\mathbf{x}'$ is completely undetermined, in the sense that $\mathbf{x}'$ takes on all values in $(\mathbb{F}_q)^t$ as $\mathbf{y}'$ varies over $(\mathbb{F}_q)^t$. On the other hand, if $M(I, J)$ is not invertible, then $\mathbf{x}'$ can take on only $(\mathbb{F}_q)^{t'}$ possible values, where $\mathsf{rank}(M(I, J)) = t' < t$. $\square$

An s by s *Cauchy matrix* can be defined over $\mathbb{F}_q$ if $q \geqslant 2s$. Let $a_1, \ldots, a_s, b_1, \ldots, b_s$ be distinct elements of $\mathbb{F}_q$. Let $c_{ij} = 1/(a_i - b_j)$, for $1 \leqslant i \leqslant s$ and $1 \leqslant j \leqslant s$. Then $C = (c_{ij})$ is the Cauchy matrix defined by the sequence $a_1, \ldots, a_s, b_1, \ldots, b_s$. The most important property of a Cauchy matrix C is that any square submatrix of C (including C itself) is invertible over $\mathbb{F}_q$.

Cauchy matrices were briefly mentioned in [12] as a possible method of constructing AONT. However, they are particularly relevant in light of the stronger definitions we are now investigating. To be specific, Cauchy matrices immediately yield the strongest possible all-or-nothing transforms, as stated in the following theorem.

Theorem 2. *Suppose q is a prime power and $q \geqslant 2s$. Then there is a linear transform that is simultaneously a (t, s, q)-AONT for all t such that $1 \leqslant t \leqslant s$.*

3 Linear transforms over $\mathbb{F}_2$

Remark 3. In the remainder of the paper, when we discuss invertibility of a matrix, we mean invertibility over $\mathbb{F}_2$.

There is no Cauchy matrix over $\mathbb{F}_2$ if $s > 1$. In fact, it is easy to see that there is no linear $(1, s, 2)$-AONT if $s > 1$. This is because every entry of M must equal 1 (in order that the 1 by 1 submatrices of M are invertible). But then M itself is not invertible. This motivates trying to determine how close we can get to a $(1, s, 2)$-AONT, or more generally, to a $(t, s, 2)$-AONT, for a given t, $1 \leqslant t \leqslant s$.

For future reference, we record the 2 by 2 invertible $0-1$ matrices.

Fact 4. *A 2 by 2 $0-1$ matrix is invertible if and only if it is one of the following six matrices:*

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

We first consider an example.

Example 5. Define a 3 by 3 matrix:

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

It is clear that seven of the nine 1 by 1 submatrices of M are invertible (namely, the "1" entries). There are nine 2 by 2 submatrices of M and seven of them are seen to be invertible, from Fact 4. The only non-invertible 2 by 2 submatrices are $M(\{1,3\},\{1,2\})$ and $M(\{1,2\},\{1,3\})$. Finally, M itself is invertible.

It seems natural to quantify the "closeness" of M to an all-or-nothing transform by considering the ratio of invertible square submatrices to the total number of square submatrices (of a given size t). Therefore, for an s by s invertible $0-1$ matrix M and for

$1 \leqslant t \leqslant s$, we define

$$N_t(M) = \text{number of invertible } t \text{ by } t \text{ submatrices of } M$$

and

$$R_t(M) = \frac{N_t(M)}{\binom{s}{t}^2}.$$

We refer to $R_t(M)$ as the *t-density* of the matrix M. For $1 \leqslant t \leqslant s$, we also define

$$R_t(s) = \max\{R_t(M) : M \text{ is an } s \text{ by } s \text{ invertible } 0-1 \text{ matrix}\}.$$

$R_t(s)$ denotes the maximum t-density of any s by s invertible $0-1$ matrix.

For the matrix M from Example 5, we have $R_1(M) = 7/9$ and $R_2(M) = 7/9$.

Lemma 6. *Suppose $M = J_s - I_s$, where I_s denotes the s by s identity matrix and J_s denotes the s by s matrix in which every entry is equal to one. Then M is invertible over $\mathbb{F}_2$ if and only if s is even.*

Proof. If s is even, then it is easy to check that $M^{-1} = M$. If s is odd, then observe that the sum of all the columns of M yields the zero-vector, so we have a dependence relation among the columns of M. □

Lemma 7. *Suppose M is an s by s $0-1$ matrix having at most $s-1$ zero entries. Then M is invertible over $\mathbb{F}_2$ if and only if the zero entries occur in $s-1$ different rows and in $s-1$ different columns.*

Proof. If M has at most $s-2$ zero entries, then there must exist at least two columns of M that do not contain a zero entry. These two columns are identical, so they are linearly dependent.

Now, suppose that M has exactly $s-1$ zero entries. If there are at least two zero entries in a specific column of M, then there must exist at least two columns of M that do not contain a zero entry, and therefore M is not invertible. A similar conclusion holds if there exist at least two zero entries in a specific row of M. Therefore we can restrict our attention to the case where the zero entries occur in $s-1$ different rows and in $s-1$ different columns. We will show that M is invertible in this case.

By permuting rows and columns if necessary (which does not affect invertibility), we can assume that $M = (m_{ij})$ has the form

$$M = \begin{pmatrix} 1 & 1 & 1 & 1 & \dots & 1 \\ 1 & 0 & 1 & 1 & \dots & 1 \\ 1 & 1 & 0 & 1 & \dots & 1 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & 1 & 1 & 1 & \dots & 0 \end{pmatrix}. \tag{2}$$

It is easy to see that the s by s matrix M is invertible by verifying the following formula for M^{-1}:

$$M^{-1} = \begin{pmatrix} a & \mathbf{1}^T \\ \mathbf{1} & I \end{pmatrix},$$

where $\mathbf{1}$ is a column vector consisting of $s-1$ ones, I is an $s-1$ by $s-1$ identity matrix, and $a = s \bmod 2$.

$\square$

The following result is an immediate corollary of Lemma 7.

Theorem 8. *For all $s \geqslant 1$, we have $R_1(s) = 1 - \frac{s-1}{s^2}$.*

Remark 9. It was shown in [12] that $R_1(s) \geqslant 1 - \frac{1}{s}$ when s is even. This was based on using the matrix $J_s - I_s$ as a transform. Theorem 8 is a slight improvement, and it holds for all values of s.

Example 10. Consider the 4 by 4 matrix given by (2):

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

Here, we can verify using Lemmas 6 and 7 that $R_1(M) = 13/16$, $R_2(M) = 24/36 = 2/3$ and $R_3(M) = 9/16$.

In fact, it is possible to compute all the values $R_t(M)$ for the s by s matrix M given in (2). There are $\binom{s}{t}^2$ submatrices N of M of dimensions t by t. From the structure of M, and from Lemmas 6 and 7, we see that a t by t submatrix N is invertible if and only if one of the following conditions holds:

1. N contains $t-1$ zero entries, or
2. t is even and N contains t zero entries.

If we can count the number of submatrices of this form, then we can compute $R_t(M)$. But this is not hard to do.

Lemma 11. *The s by s matrix M given in (2) has exactly $\binom{s-1}{t-1}(1 + (s-t+1)(s-t))$ submatrices that contain exactly $t-1$ zero entries.*

Lemma 12. *The s by s matrix M given in (2) has exactly $\binom{s-1}{t}$ submatrices that contain exactly t zero entries.*

So we now obtain the following.

Theorem 13. *Let M be the s by s matrix given in (2) and let $1 \leqslant t \leqslant s-1$. If t is odd, then*

$$N_t(M) = \binom{s-1}{t-1}(1 + (s-t+1)(s-t)).$$

If t is even, then

$$N_t(M) = \binom{s-1}{t} + \binom{s-1}{t-1}(1 + (s-t+1)(s-t)).$$

Theorem 13 also provides (constructive) lower bounds on $R_t(s)$ for all values of $t \leqslant s$. We do not claim that these bounds are necessarily good asymptotic bounds, however. Even for $t = 2$, we get $R_2(M) \to 0$ as $s \to \infty$, since $\binom{s-1}{t-1}(1 + (s - t + 1)(s - t)) \in \Theta(s^3)$ and $\binom{s}{t}^2 \in \Theta(s^4)$. This suggests looking for constructions which will yield constant lower bounds on $R_2(s)$. On the other side, we would also like to find good upper bounds on $R_2(s)$.

4 Upper Bounds for $R_2(s)$

We first establish an easy upper bound for $R_2(s)$. This bound is a consequence of the following lemma.

Lemma 14. *Any 2 by s $0-1$ matrix contains at most $s^2/3$ invertible 2 by 2 submatrices.*

Proof. Let N be any 2 by s $0-1$ matrix. Consider the 2 by 1 submatrices of N. Suppose there are a_0 occurrences of $\begin{pmatrix} 0 \\ 0 \end{pmatrix}$, a_1 occurrences of $\begin{pmatrix} 0 \\ 1 \end{pmatrix}$, a_2 occurrences of $\begin{pmatrix} 1 \\ 0 \end{pmatrix}$, and a_3 occurrences of $\begin{pmatrix} 1 \\ 1 \end{pmatrix}$. Of course $a_0 + a_1 + a_2 + a_3 = s$. From Fact 4, the number of invertible 2 by 2 submatrices in N is easily seen to be $a_1a_2 + a_1a_3 + a_2a_3$. This expression is maximized when $a_0 = 0$, $a_1 = a_2 = a_3 = s/3$, yielding $3(s/3)^2 = s^2/3$ invertible 2 by 2 submatrices. □

Theorem 15. *For any $s \geqslant 2$, it holds that*

$$R_2(s) \leqslant \frac{2s}{3(s-1)}.$$

Proof. From Lemma 14, in any two rows of M there are at most $s^2/3$ invertible 2 by 2 submatrices. Now, in the entire matrix M, there are $\binom{s}{2}$ ways to choose two rows, and there are $\binom{s}{2}^2$ submatrices of order 2. This immediately yields

$$R_2(s) \leqslant \frac{\binom{s}{2}(s^2/3)}{\binom{s}{2}^2} = \frac{2s}{3(s-1)}.$$ □

Example 16. When $s = 3$, we only get the trivial upper bound $R_2(3) \leqslant 1$ from Theorem 15. Consider the matrix

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

It is clear from the proof of Theorem 15 that all nine 2 by 2 submatrices of M are invertible, and M is the only 3 by 3 matrix with this property. However, M is not itself invertible, so we can conclude that $R_2(3) \leqslant 8/9$. Example 5 shows that $R_2(3) \geqslant 7/9$.

In fact, we can show that $R_2(3) = 7/9$. Suppose that $R_2(3) = 8/9$. If M is any matrix with $R_2(M) = 8/9$, then two pairs of rows each contain three invertible 2 by 2 submatrices. It then follows from Fact 4 that each row contains exactly two ones. So the nullspace of M contains $(1, 1, 1)$ and M is not invertible. Thus $R_2(3) = 7/9$.

Example 17. When $s = 4$, we get $R_2(4) \leqslant 8/9$ from Theorem 15. Consider the matrix $M = J_4 - I_4$. M is invertible from Lemma 6. It is easy to check that 30 of the 2 by 2 submatrices of M are invertible. Therefore, $R_2(4) \geqslant 5/6$.

We can in fact show that $R_2(4) = 5/6$, as follows. Suppose $R_2(4) > 5/6$. Then there is a 4 by 4 0-1 matrix having at least 31 invertible 2 by 2 submatrices. Hence, some pair of rows must contain more than five such submatrices, in violation of Lemma 14.

We next present a generalization of Theorem 15 that leads to an improved upper bound on $R_2(s)$. The proof of Theorem 15 was based on upper-bounding the number of invertible 2 by 2 submatrices in any two rows of an s by s matrix M. Here we instead determine an upper bound on the number of invertible 2 by 2 submatrices in any four rows of M. (It turns out that considering three rows at a time yields the same bound as Theorem 15, so we skip directly to an analysis of four rows at a time.)

Label the non-zero vectors in $\{0, 1\}^4$ in lexicographic order as follows: $b_0 = (0, 0, 0, 0)$, $b_1 = (0, 0, 0, 1)$, $b_2 = (0, 0, 1, 0)$, $b_3 = (0, 0, 1, 1)$, $\ldots$, $b_{15} = (1, 1, 1, 1)$. For $1 \leqslant i, j \leqslant 15$, define c_{ij} to be the number of invertible 2 by 2 submatrices in the 4 by 2 matrix $\left(\begin{array}{c|c} b_i^T & b_j^T \end{array} \right)$. Let $C = (c_{ij})$; note that C is a 15 by 15 symmetric matrix with zero diagonal such that every off-diagonal element is a positive integer. This matrix C is straightforward to compute and it is presented in Figure 1.

Now define $\mathbf{z} = (z_1, \ldots, z_{15})$ and consider the following quadratic program $\mathcal{Q}$:

Maximize	$\frac{1}{2}\mathbf{z}C\mathbf{z}^T$
subject to	$\sum_{i=1}^{15} z_i \leqslant 1$ and $z_i \geqslant 0$, for all i, $1 \leqslant i \leqslant 15$.

We have the following result.

Theorem 18. *For any integer $s \geqslant 4$, it holds that*

$$R_2(s) \leqslant \frac{\gamma s}{3(s-1)},$$

where γ denotes the optimal solution to $\mathcal{Q}$.

Proof. Let M be any s by s $0-1$ matrix. Consider any four rows of M, say the first four rows without loss of generality, and denote the resulting 4 by s submatrix by M'. For $0 \leqslant i \leqslant 15$, suppose there are a_i columns of M' that are equal to b_i^T. The number N of 2 by 2 invertible submatrices of M' is equal to $\frac{1}{2}\mathbf{a}C\mathbf{a}^T$, where $\mathbf{a} = (a_1, \ldots, a_{15})$ (we can ignore a_0 because a zero column does not give rise to any invertible submatrices). If we now define $z_i = a_i/s$ for all i, then we obtain

$$N = \frac{1}{2}\mathbf{a}C\mathbf{a}^T = \frac{s^2}{2}\mathbf{z}C\mathbf{z}^T \leqslant \gamma s^2.$$

There are $\binom{s}{4}$ ways to choose four rows from M. The total number of occurrences of invertible 2 by 2 submatrices obtained is at most $\binom{s}{4}\gamma s$. However, each invertible 2 by 2

$$C = \begin{pmatrix} 0 & 1 & 1 & 1 & 1 & 2 & 2 & 1 & 1 & 2 & 2 & 2 & 2 & 3 & 3 \\ 1 & 0 & 1 & 1 & 2 & 1 & 2 & 1 & 2 & 1 & 2 & 2 & 3 & 2 & 3 \\ 1 & 1 & 0 & 2 & 3 & 3 & 2 & 2 & 3 & 3 & 2 & 4 & 5 & 5 & 4 \\ 1 & 1 & 2 & 0 & 1 & 1 & 2 & 1 & 2 & 2 & 3 & 1 & 2 & 2 & 3 \\ 1 & 2 & 3 & 1 & 0 & 3 & 2 & 2 & 3 & 4 & 5 & 3 & 2 & 5 & 4 \\ 2 & 1 & 3 & 1 & 3 & 0 & 2 & 2 & 4 & 3 & 5 & 3 & 5 & 2 & 4 \\ 2 & 2 & 2 & 2 & 2 & 2 & 0 & 3 & 5 & 5 & 5 & 5 & 5 & 5 & 3 \\ 1 & 1 & 2 & 1 & 2 & 2 & 3 & 0 & 1 & 1 & 2 & 1 & 2 & 2 & 3 \\ 1 & 2 & 3 & 2 & 3 & 4 & 5 & 1 & 0 & 3 & 2 & 3 & 2 & 5 & 4 \\ 2 & 1 & 3 & 2 & 4 & 3 & 5 & 1 & 3 & 0 & 2 & 3 & 5 & 2 & 4 \\ 2 & 2 & 2 & 3 & 5 & 5 & 5 & 2 & 2 & 2 & 0 & 5 & 5 & 5 & 3 \\ 2 & 2 & 4 & 1 & 3 & 3 & 5 & 1 & 3 & 3 & 5 & 0 & 2 & 2 & 4 \\ 2 & 3 & 5 & 2 & 2 & 5 & 5 & 2 & 2 & 5 & 5 & 2 & 0 & 5 & 3 \\ 3 & 2 & 5 & 2 & 5 & 2 & 5 & 2 & 5 & 2 & 5 & 2 & 5 & 0 & 3 \\ 3 & 3 & 4 & 3 & 4 & 4 & 3 & 3 & 4 & 4 & 3 & 4 & 3 & 3 & 0 \end{pmatrix}.$$

Figure 1: The objective function C for the quadratic program

submatrix is included in exactly $\binom{s-2}{2}$ sets of four rows, so the total number of invertible 2 by 2 submatrices is at most

$$\frac{\binom{s}{4}\gamma s^2}{\binom{s-2}{2}}.$$

The total number of 2 by 2 submatrices is $\binom{s}{2}^2$, so we obtain the upper bound

$$R_2(s) \leqslant \frac{\binom{s}{4}\gamma s^2}{\binom{s-2}{2}\binom{s}{2}^2} = \frac{\gamma s}{3(s-1)}. \tag{3}$$

□

In general, it can be difficult to find (global) optimal solutions for quadratic programs. We were able to solve our quadratic program $\mathcal{Q}$ using the BARON software [13] on the NEOS server (`http://www.neos-server.org/neos/`). The result is that $\gamma = 15/8$ and an optimal solution is given by $z_7 = z_{11} = z_{13} = z_{14} = 1/4$, $z_i = 0$ if $i \notin \{7, 11, 13, 14\}$. It is interesting to observe that this solution corresponds to the given set of four rows containing only columns consisting of three 1's and one 0. In fact, when $s = 4$, this provides an alternative proof of Example 17.

Applying Theorem 18, we immediately obtain the following improved upper bound.

Corollary 19. *For any $s \geqslant 4$, it holds that*

$$R_2(s) \leqslant \frac{5s}{8(s-1)}.$$

This upper bound is asymptotically equal to 5/8, which is a definite improvement over the asymptotic upper bound of 2/3 obtained from Theorem 15.

It is of course possible to generalize this approach, by considering ρ rows at a time. The coefficient matrix C will have $2^\rho - 1$ rows and columns. If γ_ρ denotes the solution to the related quadratic program, then we obtain the following generalization of Theorem 18.

Theorem 20. *For any integers $s \geqslant \rho \geqslant 2$, it holds that*

$$R_2(s) \leqslant \frac{4\gamma_\rho}{\rho(\rho-1)} \times \frac{s}{s-1}. \tag{4}$$

Proof. The equation (3) becomes the following:

$$R_2(s) \leqslant \frac{\binom{s}{\rho}\gamma_\rho s^2}{\binom{s-2}{\rho-2}\binom{s}{2}^2} = \frac{4\gamma_\rho}{\rho(\rho-1)} \times \frac{s}{s-1}. \qquad \square$$

The difficulty in obtaining improved bounds using this approach is that the optimal solutions γ_ρ of the quadratic programs are hard to compute.

5 Constructions

In the next subsections, we consider five possible construction methods for AONT with good 2-density. The first is exhaustive search. The second is based on choosing each entry independently at random with an appropriate probability. The third technique is a recursive technique. The fourth method is based on using incidence matrices of symmetric BIBDs. Our fifth and last approach makes use of classical results concerning cyclotomy and cyclotomic numbers.

5.1 Exhaustive Searches

We used an exhaustive search in order to find an invertible $s \times s$ matrix with the maximum possible number of invertible 2×2 submatrices, for $4 \leqslant s \leqslant 8$. The algorithm consists of s nested loops, each iterating over the possible values in a given row of the matrix. There are 2^s possibilities for any given row. However, any permutation of rows and columns does not affect either the nonsingularity of the matrix or the number of invertible 2×2 submatrices. Therefore, the search algorithm only generated matrices in which each row has at least as many 1's as the row immediately above it. Also, if two rows have the same number of 1's, the row having the smaller representation as a binary number would appear higher. These two rules enabled us to search only a $1/s!$ fraction of the search domain. Finally, we partially restricted column permutations by fixing all the 1's in the first row to occur in the rightmost positions. This also sped up the search process.

The computations for $4 \leqslant s \leqslant 8$ were executed on one node on the Cheriton School of Computer Science server, `linux.cs.uwaterloo.ca`, which has a 64 bit AMD CPU, having a 2.6 GHz clock rate. For $s = 9$, we attempted to use the same algorithm distributed over 256 processors on `grex.westgrid.ca`. But the search was not finished by the end of the 96 hour time limit. However, it did find a solution with 783 invertible 2×2 submatrices, which is presented in Example 40.

5.2 Random Constructions

We investigate the expected number of invertible 2 by 2 submatrices in a random s by s $0-1$ matrix M. Suppose every entry of M is chosen to be a 1 with probability ϵ, independent of the values of all other entries. Using Fact 4, it is easy to see that a specified 2 by 2 submatrix is invertible with probability

$$4\epsilon^3(1-\epsilon) + 2\epsilon^2(1-\epsilon)^2 = 2\epsilon^2(1-\epsilon)(2\epsilon+1-\epsilon) = 2\epsilon^2(1-\epsilon^2).$$

This function is maximized by choosing $\epsilon = \sqrt{1/2}$. The expected number of invertible 2 by 2 submatrices in M is $\frac{1}{2}\binom{s}{2}^2$ (leading to an expected 2-density of .5). Unfortunately, this does not immediately yield an AONT because it seems difficult to ensure that the constructed matrix is itself invertible. However, this random construction proves to be a useful method to obtain good small examples.

5.3 Recursive Constructions

We now investigate the possibility of constructing "good" AONT recursively. Specifically, we analyze a type of doubling construction in a particular case. We begin with the $(2, 4, 2)$-AONT from Example 17. Recall that this AONT arises from the matrix $J_4 - I_4$ and it achieves the optimal result $R_2(4) = 5/6$. We might try to use this matrix to construct a $(2, 8, 2)$-AONT. There are various ways in which we could try to do this; we present one method which leads to a reasonably good outcome. Consider the matrix

$$M = \left(\begin{array}{c|c} J_4 - I_4 & J_4 - I_4 \\ \hline J_4 - I_4 & J_4 \end{array}\right).$$

We first need to show that M is invertible. We show that $\det(M) = 1$ as follows. Consider a matrix of the form

$$M = \left(\begin{array}{c|c} A & B \\ \hline C & D \end{array}\right),$$

where A, B, C, D are square submatrices and $CD = DC$. In this case, it is known that $\det(M) = \det(AD - BC)$.

In our construction, we have $CD = DC = 3J_4 = J_4$, so this formula can be applied. We have $A = B = C = J_4 - I_4$ and it is easy to check that $BC = I_4$, $AD = J_4$. Therefore $AD - BC = J_4 - I_4$ and $\det(M) = \det(AD - BC) = \det(J_4 - I_4) = 1$.

Next, we proceed to compute the number of 2 by 2 invertible submatrices of M. We do this by looking at pairs of rows of M, say row i and row j, and computing the relevant numbers a_0, a_1, a_2, a_3 in each case (where we are using the notation from the proof of Lemma 14). We tabulate the results in Table 1.

Table 1: 2 by 2 invertible submatrices of M

i, j	a_0, a_1, a_2, a_3	# invertible submatrices
$1 \leqslant i < j \leqslant 4$	$a_1 = 2, a_2 = 2, a_3 = 4$	20
$5 \leqslant i < j \leqslant 8$	$a_1 = 1, a_2 = 1, a_3 = 6$	13
$1 \leqslant i \leqslant 4, 5 \leqslant j \leqslant 8, j \neq i + 4$	$a_1 = 2, a_2 = 1, a_3 = 5$	17
$1 \leqslant i \leqslant 4, j = i + 4$	$a_0 = 1, a_1 = 1, a_3 = 6$	6

The number of occurrences of the four cases enumerated in Table 1 is (respectively) $6, 6, 12$ and 4. Therefore,

$$N_2(M) = 6 \times 20 + 6 \times 13 + 12 \times 17 + 4 \times 6 = 426.$$

Finally, we compute

$$R_2(M) = \frac{426}{\binom{8}{2}^2} = \frac{426}{784} = .5434.$$

Summarizing, we have the following.

Theorem 21. *$N_2(8) \geqslant 426$ and $R_2(8) \geqslant .5434$.*

It is interesting to note that this recursive construction yields a better result than the direct constructions considered previously. For example, if $M = J_8 - I_8$, then we only get that $N_2 \geqslant 364$. Also, Theorem 13 (with $s = 8$, $t = 2$) only yields $N_2 \geqslant 322$.

5.4 Constructions from Symmetric BIBDs

We next give a construction which potentially achieves similar behaviour as the random construction, using symmetric balanced incomplete block designs (SBIBDs). A (v, k, λ)-*balanced incomplete block design* (BIBD) is a pair $(X, \mathcal{A})$, where X is a set of v *points* and $\mathcal{A}$ is a collection of k-subsets of X called *blocks*, such that every pair of points occurs in exactly λ blocks. Denote $b = |\mathcal{A}|$; it is well-known that $b = \lambda v(v-1)/(k(k-1))$. It is also the case that every point occurs in exactly $r = bk/v = \lambda(v-1)/(k-1)$ blocks. A BIBD is *symmetric* if $v = b$. Equivalently, this condition can be expressed as $r = k$ or $\lambda(v-1) = k(k-1)$.

Suppose $(X, \mathcal{A})$ is a (v, k, λ)-BIBD. Denote $X = \{x_i : 1 \leqslant i \leqslant v\}$ and $\mathcal{A} = \{A_j : 1 \leqslant j \leqslant b\}$. The *incidence matrix* of $(X, \mathcal{A})$ is the v by b $0-1$ matrix $M = (m_{ij})$ where $m_{ij} = 1$ if $x_i \in A_j$, and $m_{ij} = 0$ if $x_i \notin A_j$.

Lemma 22. *Suppose M is the incidence matrix of a symmetric (v, k, λ)-BIBD. Then M is invertible over $\mathbb{F}_2$ if and only if k is odd and λ is even.*

Proof. It is well-known (see, e.g., [4]) that $\det(M)$ is an integer and

$$(\det(M))^2 = k^2(k-\lambda)^{v-1}.$$

Reducing modulo 2, we see that $\det(M) \equiv 1 \bmod 2$ if and only if k is odd and λ is even. $\square$

Theorem 23. *Suppose M is the incidence matrix of a symmetric (v, k, λ)-BIBD where k is odd and λ is even. Then*

$$R_2(M) = \frac{k^2 - \lambda^2}{\binom{v}{2}}. \tag{5}$$

Proof. First, since k is odd and λ is even, M is invertible over $\mathbb{F}_2$ by Lemma 22. Consider two rows of M and define a_0, a_1, a_2, a_3 as in the proof of Theorem 15. Using the fact that M is the incidence matrix of a symmetric (v, k, λ)-BIBD, it is not hard to see that $a_0 = v - 2k + \lambda$, $a_1 = a_2 = k - \lambda$ and $a_3 = \lambda$. Then we can compute

$$a_1a_2 + a_1a_3 + a_2a_3 = 2\lambda(k - \lambda) + (k - \lambda)^2 = k^2 - \lambda^2.$$

From this, we have $N_2(M) = \binom{v}{2}(k^2 - \lambda^2)$ and (5) is easily derived. $\square$

Let's try to figure out the best result that we could possibly obtain from Theorem 23. Suppose $k \approx cv$. Then from the equation $\lambda(v - 1) = k(k - 1)$, we see that $\lambda \approx c^2v$. Substituting into (5), we get $R_2(M) \approx 2(c^2 - c^4)$. Now we of course have $0 \leqslant c \leqslant 1$, and the function $2(c^2 - c^4)$ is maximized when $c = \sqrt{1/2}$. In this case, we would get $R_2(M) \approx 1/2$, more-or-less matching the random construction from Section 5.2. We have also guaranteed that the matrix M is invertible. Of course, we would require a suitable SBIBD in order to get close to this bound.

We consider some examples to illustrate the application of Theorem 23.

Example 24. It is known [4] that there is a $(31, 21, 14)$-SBIBD. Noting that 21 is odd and 14 is even, the incidence matrix of this design is invertible over $\mathbb{F}_2$ by Lemma 22. Observe that $21/31$ is quite close to $\sqrt{1/2}$, so we expect a good result. Applying Theorem 23, we get

$$R_2(M) = \frac{21^2 - 14^2}{\binom{31}{2}} = \frac{49}{93} \approx .5269.$$

Example 25. There also exists $(40, 27, 18)$-SBIBD (see [4]). Noting that 27 is odd and 18 is even, the incidence matrix of this design is invertible over $\mathbb{F}_2$ by Lemma 22. Applying Theorem 23, we get

$$R_2(M) = \frac{27^2 - 18^2}{\binom{40}{2}} = \frac{27}{52} \approx .5192.$$

Example 26. A $(4m - 1, 2m - 1, m - 1)$-SBIBD is called a *Hadamard design*. If m is odd, then $\lambda = m - 1$ is even. Certainly $k = 2m - 1$ is odd, so the incidence matrix M is invertible, by Lemma 22. These SBIBDs are known to exist for infinitely many (odd) values of m, e.g., whenever $4m - 1 \equiv 3 \bmod 8$ is a prime or a prime power (see [4]). From the incidence matrix of such a BIBD, we obtain

$$R_2(M) = \frac{(2m - 1)^2 - (m - 1)^2}{\binom{4m-1}{2}} \approx 3/8.$$

Example 27. Here we make use of a classic result based on difference sets. Suppose $q = 4t^2 + 9$ is prime and t is odd. In this situation, it was shown by E. Lehmer that the quartic residues modulo q, together with 0, form a difference set which generates a $(q, (q + 3)/4, (q + 3)/16)$-SBIBD (e.g., see [4, p. 116]). If we complement this design (i.e., we replace all 0's by 1's and all 1's by 0's in the incidence matrix), the result is a $(q, 3(q - 1)/4, 3(3q - 7)/16)$-SBIBD. This SBIBD will have k odd and λ even, so its incidence matrix M is invertible, by Lemma 22. The first example is obtained when $t = 5$, yielding

$$R_2(109) \geqslant \frac{329}{654}.$$

Asymptotically, from (5), we obtain

$$R_2(M) \approx \frac{63}{128}$$

if there exist sufficiently large q of the desired form. However, it is a famous unsolved conjecture that there exist infinitely many primes of the form $x^2 + 9$, so we are not in a position to claim that this asymptotic result holds.

The following theorem generalizes Example 25.

Theorem 28. *Suppose m is a positive integer and $s = (3^{m+1} - 1)/2$. Then*

$$R_2(s) \geqslant \frac{40 \times 3^{2m-3}}{(3^{m+1} - 1)(3^m - 1)}.$$

Proof. The points and hyperplanes of the m-dimensional projective geometry over $\mathbb{F}_3$ yield a

$$\left(\frac{3^{m+1} - 1}{2}, \frac{3^m - 1}{2}, \frac{3^{m-1} - 1}{2}\right)\text{-SBIBD.}$$

If we complement this design, we get a

$$\left(\frac{3^{m+1} - 1}{2}, 3^m, 2 \times 3^{m-1}\right)\text{-SBIBD.}$$

This design has k odd and λ even, so we can apply Theorem 23. The result is that

$$R_2\left(\frac{3^{m+1} - 1}{2}\right) \geqslant \frac{(3^m)^2 - (2 \times 3^{m-1})^2}{\binom{\frac{3^{m+1}-1}{2}}{2}} = \frac{40 \times 3^{2m-3}}{(3^{m+1} - 1)(3^m - 1)}. \qquad \square$$

Let's examine the asymptotic behaviour of the result proven in Theorem 28. The SBIBD has $k \approx 2v/3$ and $\lambda \approx 4v/9$. It then follows from (5) that

$$R_2(M) = \frac{k^2 - \lambda^2}{\binom{v}{2}} \approx 2\left(\left(\frac{2}{3}\right)^2 - \left(\frac{4}{9}\right)^2\right) = \frac{40}{81}.$$

Therefore, we obtain the following corollary.

Corollary 29. *It holds that* $\limsup_{s\to\infty} R_2(s) \geqslant \frac{40}{81}$.

We note that $40/81 \approx .494$. So there is a gap between our upper and lower asymptotic bounds on 2-density, which are respectively .625 (from Corollary 19) and .494 (and of course the lower bound only has been proven to hold within a certain infinite class of examples).

5.5 Constructions using Cyclotomy

We now look at constructions using cyclotomy. Let $p = 4f+1$ be prime, where f is even, and let $\nu \in \mathbb{F}_p{}^*$ be a primitive element. Let $C_0 = \{\nu^{4i} : 0 \leqslant i \leqslant f-1\}$; this is the unique subgroup of $\mathbb{F}_p{}^*$ having order f. The multiplicative cosets of C_0 are $C_j = \nu^j C_0$, for $j = 0,1,2,3$. These cosets are often called *cyclotomic classes*.

We now construct a p by p $0-1$ matrix $M' = (m_{ij})$ from C_0. The rows and columns of M' are indexed by $\mathbb{F}_p$, and $m_{ij} = 1$ if and only if $j - i \in C_0$. Note that the ith row of M' is the incidence vector of $i + C_0$. Finally, define M to be the complement of M' (i.e., replace all 1's by 0's and vice versa).

We will now compute the number of invertible 2 by 2 submatrices of M. Consider rows i_1 and i_2 of M. It is obvious that the number of invertible 2 by 2 submatrices contained in these two rows is the same as the number of invertible 2 by 2 submatrices contained in rows 0 and d, where $d = i_1 - i_2$. We can compute this number if we can determine the number n_d of columns c such that $m_{0c} = m_{dc} = 1$. It is clear that

$$n_d = |C_0 \cap (d + C_0)|.$$

However,

$$|C_0 \cap (d + C_0)| = |d^{-1}C_0 \cap (1 + d^{-1}C_0)|.$$

Now, $d^{-1}C_0 = C_j$, for some j, $0 \leqslant j \leqslant 3$, so

$$n_d = |C_j \cap (1 + C_j)|$$

for this particular value of j. This quantity is a *cyclotomic number of order* 4 and is denoted by (j,j).

We will make use of the following theorem from [7].

Theorem 30. *[7, Theorem 1] Suppose* $p = 4f+1$ *is prime and* f *is even. Let* $\nu \in \mathbb{F}_q$ *be a primitive element. Let* $p = \alpha^2 + \beta^2$, *where* $\alpha \equiv 1 \bmod 4$ *and* $\nu^f \equiv \alpha/\beta \bmod p$. *Then the cyclotomic numbers* (j,j) $(0 \leqslant j \leqslant 3)$, *are as follows:*

$$\begin{aligned}
(0,0) = A_0 &= \frac{p-11-6\alpha}{16} = \frac{4f-10-6\alpha}{16}\\
(1,1) = A_1 &= \frac{p-3+2\alpha-4\beta}{16} = \frac{4f-2+2\alpha-4\beta}{16}\\
(2,2) = A_2 &= \frac{p-3+2\alpha}{16} = \frac{4f-2+2\alpha}{16}\\
(3,3) = A_3 &= \frac{p-3+2\alpha+4\beta}{16} = \frac{4f-2+2\alpha+4\beta}{16}.
\end{aligned}$$

Remark 31. A prime $p \equiv 1 \bmod 4$ can be expressed as the sum of two squares in a unique manner. If $p = \alpha^2 + \beta^2$, then one of α, β is odd and the other is even. So without loss of generality we can take α to be odd and β to be even. In this way, α and β are determined up to their signs. The condition $\alpha \equiv 1 \bmod 4$ now determines α uniquely, and, similarly, $\nu^f \equiv \alpha/\beta \bmod p$ determines β uniquely.

Now we can compute the number of 2 by 2 submatrices contained in rows i_1 and i_2 of M. Again we define a_0, a_1, a_2, a_3 as in the proof of Theorem 15. Recalling that M is the complement of M', we have

$$a_1 = a_2 = f - (j, j)$$

and

$$a_3 = p - 2f + (j, j) = 2f + 1 + (j, j),$$

where $(i_1 - i_2)^{-1}C_0 = C_j$. Thus we obtain

$$a_1a_2 + a_1a_3 + a_2a_3 = 5f^2 + 2f - (j, j)(4f + 2 + (j, j)).$$

As we consider all $\binom{p}{2}$ pairs $\{i_1, i_2\}$ with $i_1 \neq i_2$, we see that (j, j) takes on each of the four possible values A_i $(1 \leqslant i \leqslant 4)$ one quarter of the time. Therefore the total number of invertible 2 by 2 submatrices in M is

$$\begin{aligned} &\binom{p}{2} \sum_{i=0}^{3} \left(\frac{5f^2 + 2f - A_i(4f + 2 + A_i)}{4} \right) \\ = \ &\binom{p}{2} \frac{252f^2 + 168f + 25 - 3\alpha^2 - 2\beta^2 - 6\alpha}{64}, \end{aligned}$$

where the last line is obtained by applying the formulas given in Theorem 30.

Example 32. Suppose $p = 17 = 4 \times 4 + 1$. Then $\nu = 3$ is a primitive element. Since $17 = 1^2 + 4^2$, we have $\alpha = 1$ and $\beta \in \{4, 13\}$. We compute $3^4 \equiv 13 \bmod 17$. Since $1/4 \equiv 13 \bmod 17$, we have $\beta = 4$. The cyclotomic classes are

$$\begin{aligned} C_0 &= \{1, 13, 16, 4\} \\ C_1 &= \{3, 5, 14, 12\} \\ C_2 &= \{9, 15, 8, 2\} \\ C_3 &= \{10, 11, 7, 6\}. \end{aligned}$$

The cyclotomic numbers can now be computed from Theorem 30; they are

$$\begin{aligned} (0, 0) = A_0 &= \frac{17 - 11 - 6}{16} = 0 \\ (1, 1) = A_1 &= \frac{17 - 3 + 2 - 4 \times 4}{16} = 0 \\ (2, 2) = A_2 &= \frac{17 - 3 + 2}{16} = 1 \\ (3, 3) = A_3 &= \frac{17 - 3 + 2 + 4 \times 4}{16} = 2. \end{aligned}$$

The total number of invertible 2 by 2 submatrices in M is 9962.

Table 2: Examples from Cyclotomy

p	f	α	β	$N_2(M)$	$R_2(M)$
17	3	1	4	9962	.53860
97	5	9	-4	10831020	.49962
193	5	-7	12	170314008	.49613
241	7	-15	4	414228390	.49527
401	3	1	-20	3177945050	.49408
433	5	17	-12	4320175230	.49388
449	3	-7	20	4995836216	.49388

It remains to consider the invertibility of the matrices M constructed above. The matrices in question are cyclic. Suppose a p by p cyclic $0-1$ matrix M has as its initial row the vector $(m_0, \ldots, m_{p-1})$. We associate with this vector the polynomial

$$m(x) = \sum_{i=0}^{p-1} m_i x^i \in \mathbb{Z}_2[x].$$

It is easy to see that M is invertible if and only if $\gcd(m(x), x^p - 1) = 1$. In this case, the inverse $m^{-1}(x)$ of $m(x)$ is defined in the quotient ring $\mathbb{Z}_2[x]/(x^p - 1)$. The cyclic matrix whose first row is determined by $m^{-1}(x)$ will in fact be the inverse of M. Therefore, to determine the invertibility of M, we just need to do a gcd computation.

Example 33. Let $p = 17$. From Example 32, we have $C_0 = \{1, 13, 16, 4\}$. The first row of M is

1 0 1 1 0 1 1 1 1 1 1 1 1 0 1 1 0,

which corresponds to the polynomial

$$m(x) = 1 + x^2 + x^3 + x^5 + x^6 + x^7 + x^8 + x^9 + x^{10} + x^{11} + x^{12} + x^{14} + x^{15}.$$

The inverse of $m(x)$ is

$$m^{-1}(x) = 1 + x + x^3 + x^4 + x^5 + x^6 + x^7 + x^{10} + x^{11} + x^{12} + x^{13} + x^{14} + x^{16}.$$

By Dirichlet's Theorem, there are an infinite number of primes $p \equiv 1 \bmod 8$. However, we do not have a theoretical criterion to determine if a given matrix M in this class of examples is invertible. Therefore, we cannot prove that there are an infinite number of examples of this type. However, by computing gcds, as described above, we determined all the invertible matrices M of order less than 500 that can be constructed by this method. Some data about these matrices is presented in Table 2. Another observation is that, if this is in fact an infinite class, then it can be shown that the density of these examples approaches $63/128 \approx .492$ as f approaches infinity.

Table 3: Values and Bounds on $N_2(s)$ for small s

s	$N_2(s)$	justification
2	$N_2(2) = 1$	Fact 4
3	$N_2(3) = 7$	Example 16
4	$N_2(4) = 30$	Example 17
5	$N_2(5) = 70$	exhaustive search (Example 36)
6	$N_2(6) = 150$	exhaustive search (Example 37)
7	$N_2(7) = 287$	exhaustive search (Example 38)
8	$N_2(8) = 485$	exhaustive search (Example 39)
9	$N_2(9) \geqslant 783$	Example 40
10	$N_2(10) \geqslant 1194$	Example 41
11	$N_2(11) \geqslant 1744$	Example 42
12	$N_2(12) \geqslant 2448$	Example 43

5.6 Values and Bounds on $N_2(s)$ for Small s

We summarize our upper and lower bounds on $N_2(s)$ for $s \leqslant 12$ in Table 3. For the cases $s = 5, 6, 7, 8$, we have exact values of $N_2(s)$ that are obtained from exhaustive computer searches For $s = 9$, our lower bound is obtained from a partial (uncompleted) exhaustive search. For $s = 10, 11, 12$, the lower bounds come from randomly constructed matrices. All of these matrices are presented in Appendix A.

6 General Transforms

In this section, we examine general (i.e., linear or nonlinear) AONT over an arbitrary alphabet, extending some results from [12] in a straightforward manner.

Let A be an N by k array whose entries are elements chosen from an alphabet X of order v. We will refer to A as an (N, k, v)-*array*. Suppose the columns of A are labelled by the elements in the set $C = \{1, \ldots, k\}$. Let $D \subseteq C$, and define A_D to be the array obtained from A by deleting all the columns $c \notin D$. We say that A is *unbiased* with respect to D if the rows of A_D contain every $|D|$-tuple of elements of X exactly $N/v^{|D|}$ times.

The following result characterizes (t, s, v)-AONT in terms of arrays that are unbiased with respect to certain subsets of columns.

Theorem 34. *A (t, s, v)-AONT is equivalent to a $(v^s, 2s, v)$-array that is unbiased with respect to the following subsets of columns:*

1. $\{1, \ldots, s\}$,
2. $\{s + 1, \ldots, 2s\}$, *and*

3. $I \cup \{s+1, \ldots, 2s\} \setminus J$, for all $I \subseteq \{1, \ldots, s\}$ with $|I| = t$ and all $J \subseteq \{s+1, \ldots, 2s\}$ with $|J| = t$.

Proof. Let A be the hypothesized $(v^s, 2s, v)$-array on alphabet X, $|X| = v$. We construct $\phi : X^s \to X^s$ as follows: for each row $(x_1, \ldots, x_{2s})$ of A, define

$$\phi(x_1, \ldots, x_s) = (x_{s+1}, \ldots, x_{2s}).$$

The function ϕ is easily seen to be a (t, s, v)-AONT.

Conversely, suppose ϕ is a (t, s, v)-AONT. Define an array A whose rows consist of all v^s $2s$-tuples $(x_1, \ldots, x_{2s})$, where $\phi(x_1, \ldots, x_s) = (x_{s+1}, \ldots, x_{2s})$. Then A is the desired $(v^s, 2s, v)$-array. □

An OA(s, k, v) (an *orthogonal array*) is a (v^s, k, v)-array that is unbiased with respect to any subset of s columns. The following corollary of Theorem 34 is immediate.

Corollary 35. *If there exists an OA$(s, 2s, v)$, then there exists a (t, s, v)-AONT for all t such that $1 \leqslant t \leqslant s$.*

We note that orthogonal arrays are equivalent to maximum distance separable (i.e., MDS) codes. Hence, it is easy to construct (t, s, v)-AONTs whenever v is a prime power and $2s \leqslant v$ (but we can also do this using Cauchy matrices; see Theorem 2). In the case $v = 2$, it was previously shown in [12, Theorem 3.5] that there is no $(1, s, 2)$-AONT (linear or nonlinear) if $s \geqslant 2$.

7 Summary

We have initiated a study of all-or-nothing transforms where we consider the security of t inputs when $s - t$ outputs are fixed or known. We focussed on the case $t = 2$, for linear transforms defined over $\mathbb{F}_2$. Here one fundamental problem is to determine the maximum 2-density, which we denoted by $R_2(s)$. The asymptotic behavior of $R_2(s)$ is an interesting open question, i.e., what is the value $L = \limsup_{s \to \infty} R_2(s)$? Our results establish that $.494 \leqslant L \leqslant .625$.

It should be possible to adapt the techniques used in this paper to deal with cases where $t > q$, or to analyze tranforms over $\mathbb{F}_q$ for fixed prime powers $q > 2$.

Acknowledgements

D. R. Stinson would like to thank Jeroen van de Graaf for rekindling his interest in AONT. Thanks also to Hugh Williams for providing some relevant number-theoretic information, and to Stephen Vavasis, Yuying Li and Henry Wolkowicz for useful discussions about quadratic programming. Finally, thanks to the referee for helpful comments concerning presentation, and for supplying the formula for M^{-1} in Lemma 7.

Note Added in Proof

In recent work (Y. Zhang, T. Zhang, X. Wang and G. Ge, Invertible binary matrices with maximum number of 2-by-2 invertible submatrices, *Discrete Mathematics* **340** (2017) 201–208) additional results on the topic of this paper are obtained. In particular, it is shown that $\lim_{s\to\infty} R_2(s) = .5$, thus answering the question posed in the Summary.

References

[1] V. Canda and Tran van Trung. A new mode of using all-or-nothing transforms. *ISIT 2002*, p. 296.

[2] R. Canetti, Y. Dodis, S. Halevi, E. Kushilevitz and A. Sahai. Exposure-resilient functions and all-or-nothing transforms. *Lecture Notes in Computer Science* **1807** (2000), 453–469 (EUROCRYPT 2000).

[3] R. G. Cascella, Z. Cao, M. Gerla, B. Crispo and R. Battiti. Weak data secrecy via obfuscation in network coding based content distribution. *Wireless Days, 2008*, pp. 1–5.

[4] C. J. Colbourn and J. H. Dinitz, eds. *The CRC Handbook of Combinatorial Designs, Second Edition*, CRC Press, 2006.

[5] A. Desai. The security of all-or-nothing encryption: protecting against exhaustive key search. *Lecture Notes in Computer Science* **1880** (2000), 359–375 (CRYPTO 2000).

[6] Q. Guo, M. Luo, L. Li and Y. Yang. Secure network coding against wiretapping and Byzantine attacks. *EURASIP Journal on Wireless Communications and Networking* **2010** (2010), article No. 17.

[7] S. A. Katre and A. R. Rajwade. Resolution of the sign ambiguity in the determination of the cyclotomic numbers of order 4 and the corresponding Jacobsthal sum. *Math. Scand.* **60** (1987), 52–62.

[8] J. Liu, H. Wang, M. Xian and K. Huang. A secure and efficient scheme for cloud storage against eavesdropper. *Lecture Notes in Computer Science* **8233** (2013), 75–89 (ICICS 2013).

[9] A. Proano and L. Lazos. Packet-hiding methods for preventing selective jamming attacks. *IEEE Transactions on Dependable and Secure Computing* **9** (2012), 101–114.

[10] R. L. Rivest. All-or-nothing encryption and the package transform. *Lecture Notes in Computer Science* **1267** (1997), 210–218 (Fast Software Encryption 1997).

[11] Y.-J. Song, K.-Y. Park and J.-M. Kang. The method of protecting privacy capable of distributing and storing of data efficiently for cloud computing environment. *Computers, Networks, Systems and Industrial Engineering 2011*, pp. 258–262.

[12] D. R. Stinson. Something about all or nothing (transforms). *Designs, Codes and Cryptography* **22** (2001), 133–138.

[13] M. Tawarmalani and N. V. Sahinidis. A polyhedral branch-and-cut approach to global optimization. *Mathematical Programming* **103** (2005), 225–249.

[14] R. A. Vasudevan, A. Abraham and S. Sanyal. A novel scheme for secured data transfer over computer networks *Journal of Universal Computer Science* **11** (2005), 104–121.

[15] Q. Zhang and L. Lazos. Collusion-resistant query anonymization for location-based services. *2014 IEEE International Conference on Communications*, pp. 768–774.

A Matrices Yielding Good or Exact Lower Bounds for $N_2(M)$

Example 36. An invertible 5 by 5 matrix having 70 invertible 2×2 submatrices:

$$M_{5\times5} = \begin{pmatrix} 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 & 0 \end{pmatrix}.$$

Example 37. An invertible 6 by 6 matrix having 150 invertible 2×2 submatrices:

$$M_{6\times6} = \begin{pmatrix} 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 \end{pmatrix}.$$

Example 38. An invertible 7 by 7 matrix having 287 invertible 2×2 submatrices:

$$M_{7\times7} = \begin{pmatrix} 0 & 0 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 \end{pmatrix}$$

Example 39. An invertible 8 by 8 matrix having 485 invertible 2×2 submatrices:

$$M_{8\times8} = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \end{pmatrix}$$

Example 40. An invertible 9 by 9 matrix having 783 invertible 2×2 submatrices:

$$M_{9\times 9} = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 0 \end{pmatrix}$$

Example 41. An invertible 10 by 10 matrix having 1194 invertible 2×2 submatrices:

$$M_{10\times 10} = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \end{pmatrix}$$

Example 42. An invertible 11 by 11 matrix having 1744 invertible 2×2 submatrices:

$$M_{11\times 11} = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \end{pmatrix}$$

Example 43. An invertible 12 by 12 matrix having 2448 invertible 2×2 submatrices:

$$M_{12\times 12} = \begin{pmatrix} 1&0&1&1&1&1&1&1&1&0&1&0\\ 1&1&1&1&1&0&1&1&1&1&1&0\\ 1&1&1&0&1&0&1&1&0&1&1&1\\ 0&0&1&0&1&1&1&0&1&1&1&1\\ 0&0&1&1&1&1&1&1&0&1&0&1\\ 1&1&0&1&1&0&0&1&1&1&1&1\\ 0&1&1&0&0&1&1&0&1&1&1&1\\ 0&1&0&1&1&1&0&1&1&1&0&1\\ 0&1&1&1&0&1&1&1&1&1&1&0\\ 1&1&1&1&1&1&0&1&0&0&1&1\\ 1&1&1&0&1&1&1&1&1&1&0&1\\ 1&1&0&1&1&1&1&0&1&0&0&1 \end{pmatrix}$$