All or Nothing at All

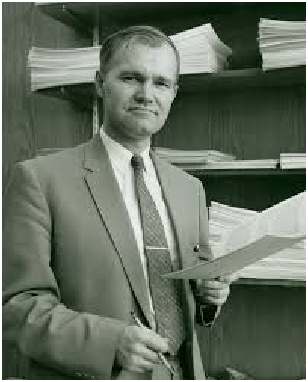
Douglas R. Stinson

David R. Cheriton School of Computer Science
University of Waterloo

29th MCCCC, Charleston, October 18, 2015

This talk is based on joint work with Paolo D'Arco and Navid Nasr Esfahani.

In Memory of Ralph Stanton, 1923–2010



All-or-nothing Transforms

- X is a finite set
- s is a positive integer, and $\phi : X^s \to X^s$.
- 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 $(1 \leq i \leq s)$ is completely undetermined.
- We will denote such a function as an (s, v)-*AONT*, where $v = |X|$.
- The desired property can be expressed as

$$\mathsf{H}(X_i \mid Y_1, \ldots, Y_{j-1}, Y_{j+1}, \ldots, Y_s) = \mathsf{H}(X_i),$$

for all i and j such that $1 \leq i \leq s$ and $1 \leq j \leq s$.

Cryptographic Motivation

- Rivest defined *AONT* in 1997 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.
- 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.

Linear AONT

- Let $\mathbb{F}_q$ be a finite field of order q.
- An (s, q)-*AONT* defined on $\mathbb{F}_q$ is linear if each y_i is an $\mathbb{F}_q$-linear function of $x_1, \ldots, x_s$.

Theorem 1 (Stinson, 2000)

Suppose that q is a prime power and M is an invertible s by s matrix with entries from $\mathbb{F}_q$, such that no entry of M is equal to 0. Then the function $\phi : (\mathbb{F}_q)^s \to (\mathbb{F}_q)^s$ defined by

$$\phi(\mathbf{x}) = \mathbf{x}M^{-1}$$

is a linear (s, q)-AONT.

Example: Hadamard Matrices

- Suppose $p > 2$ is prime, $s \equiv 0 \bmod 4$, and H is a Hadamard matrix of order s.
- H has entries ± 1 and $HH^T = sI_s$.
- Construct M by reducing the entries of H modulo p.
- Then M yields a linear (s, p)-*AONT*.
- If $s = 4$ and $p = 3$, we have

$$H = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & -1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \end{pmatrix} \rightarrow M = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 2 & 2 & 1 \\ 1 & 2 & 1 & 2 \\ 1 & 1 & 2 & 2 \end{pmatrix}$$

Example: Cauchy Matrices

- An s by s Cauchy matrix can be defined over $\mathbb{F}_q$ if $q \geq 2s$.
- Let $a_1, \dots, a_s, b_1, \dots, b_s$ be distinct elements of $\mathbb{F}_q$.
- Let

$$c_{ij} = \frac{1}{a_i - b_j},$$

  for $1 \leq i \leq s$ and $1 \leq j \leq s$.
- Then $C = (c_{ij})$ is the Cauchy matrix defined by the sequence $a_1, \dots, a_s, b_1, \dots, b_s$.
- A Cauchy matrix C is invertible, and all of its entries are non-zero, so C yields an (s, q)-*AONT*.

Example: The Bierbrauer Construction

- Let $q = p^k$ where $q > 2$, p is prime and k is a positive integer.
- Let $\lambda \in \mathbb{F}_q$ be such that $\lambda \notin \{s - 1 \bmod p, s - 2 \bmod p\}$.
- Define $\gamma = (s - 1 - \lambda)^{-1}$; note that $\gamma \neq 0, 1$.
- Let M be the following (symmetric) matrix:

$$M = \begin{pmatrix} 1-\gamma & -\gamma & -\gamma & \dots & -\gamma & \gamma \\ -\gamma & 1-\gamma & -\gamma & \dots & -\gamma & \gamma \\ -\gamma & -\gamma & 1-\gamma & \dots & -\gamma & \gamma \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ -\gamma & -\gamma & -\gamma & \dots & 1-\gamma & \gamma \\ \gamma & \gamma & \gamma & \dots & \gamma & -\gamma \end{pmatrix}.$$

Example: The Bierbrauer Construction (cont.)

- It is straightforward to verify that M is invertible; indeed, we have

$$M^{-1} = \begin{pmatrix} 1 & 0 & 0 & \dots & 0 & 1 \\ 0 & 1 & 0 & \dots & 0 & 1 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & 1 & 1 \\ 1 & 1 & 1 & \dots & 1 & \lambda \end{pmatrix}.$$

- Therefore M yields an (s, q)-*AONT*.
- This *AONT* is also very efficient computationally, since it is sparse (it contains mostly 0 entries).

Binary Transforms

- A transform defined over $\mathbb{F}_2$ is termed a binary transform.
- A binary transform automatically yields a transform over any field $\mathbb{F}_{2^n}$, in which the only computations are exclusive-ors of bitstrings.
- Unfortunately, there is no (linear or nonlinear) $(s, 2)$-*AONT* for any $s \geq 2$!
- This suggests looking for (binary, linear) transforms that are "close to" *AONT*.
- Suppose that s is even, and let $M = J_s - I_s$ (where J_s is the s by s all-1's matrix).

Binary Transforms (cont.)

- For example, when $s = 4$, we have

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

- Then $M^{-1} = M$, where M is considered as a matrix over $\mathbb{F}_2$.
- In this resulting transform, each x_j will depend on all the y_i's except for y_j.
- The density of 1's in the example above is $12/16 = 3/4$.

Generalized AONT

- Let $|X| = v$ and let $1 \leq t \leq s$.
- $\phi : X^s \to X^s$ is a t-all-or-nothing transform 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 $(1 \leq i \leq s)$ are completely undetermined.
- We will denote such a function ϕ as a (t, s, v)-*AONT*.
- The original definition corresponds to a 1-*AONT*.
- Property 2 can be rephrased as follows: 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

$$\mathsf{H}(\mathcal{X} \mid \{Y_1, \ldots, Y_s\} \setminus \mathcal{Y}) = \mathsf{H}(\mathcal{X}). \tag{1}$$

Linear t-AONT

For an s by s matrix M with entries from $\mathbb{F}_q$, and 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.

Theorem 2

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 t by t submatrix $M(I, J)$ is invertible, where $I = \{i : X_i \in \mathcal{X}\}$ and $J = \{j : Y_j \in \mathcal{Y}\}$.

Cauchy Matrices, Again

Any square submatrix of a Cauchy matrix is again a Cauchy matrix, and therefore it (the submatrix) is invertible. So we have the following result.

Theorem 3

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

Binary t-AONT

- We quantify the "closeness" of M to a *t-AONT* by considering the ratio of the number of invertible t by t submatrices to the total number of t by t submatrices.
- For an s by s invertible $0-1$ matrix M and for $1 \leq t \leq s$, 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.
- 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.

Invertible 2 by 2 $0-1$ Matrices

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

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

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

Example

- Define a 3 by 3 matrix:

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

- Seven of the nine 2 by 2 submatrices of M are invertible.
- The only non-invertible 2 by 2 submatrices are $M(\{1,3\},\{1,2\})$ and $M(\{1,2\},\{1,3\})$.
- Both of these submatrices are equal to

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

- Finally, M itself is invertible.
- Therefore, $R_2(M) = 7/9$.
- In fact, this is optimal, so $R_2(3) = 7/9$.

Another Example

- Consider the 4 by 4 matrix $J_4 - I_4$:

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

- 30 of the 36 2 by 2 submatrices of M are invertible.
- Also, M itself is invertible.
- Therefore, $R_2(M) = 5/6$.
- In fact, this is optimal, so $R_2(4) = 5/6$.

An Upper Bound on $R_2(s)$

- Let N be a 2 by s $0-1$ matrix and consider its 2 by 1 submatrices.
- 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 $a_0 + a_1 + a_2 + a_3 = s$.
- The number of invertible 2 by 2 submatrices in N is

$$a_1 a_2 + a_1 a_3 + a_2 a_3.$$

An Upper Bound on $R_2(s)$ (cont.)

- This expression is maximized when

$$a_0 = 0, \quad a_1 = a_2 = a_3 = s/3.$$

- Therefore, the maximum number of invertible 2 by 2 submatrices is

$$3\left(\frac{s}{3}\right)^2 = \frac{s^2}{3}.$$

- We have proven the following result.

Lemma 4

A 2 by s $0-1$ matrix contains $\leq s^2/3$ invertible 2 by 2 submatrices.

An Upper Bound on $R_2(s)$ (cont.)

Theorem 5

For any $s \geq 2$, it holds that

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

Proof.

From Lemma 4, in any two rows of M there are at most $s^2/3$ invertible 2 by 2 submatrices. 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

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

$\square$

An Improved Upper Bound

- We begin by establishing upper bound on the number of invertible 2 by 2 submatrices in any 4 by s $0-1$ matrix.
- Label the non-zero vectors in $\{0,1\}^4$ in lexicographic order as follows:

$$\begin{array}{ccc} b_0 = (0,0,0,0) & b_1 = (0,0,0,1) & b_2 = (0,0,1,0) \\ b_3 = (0,0,1,1) & \dots & b_{15} = (1,1,1,1). \end{array}$$

- For $1 \leq i, j \leq 15$, 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 $C = (c_{ij})$.
- C is a 15 by 15 symmetric matrix with zero diagonal such that every off-diagonal element is a positive integer.

The Matrix C

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

A Quadratic Program

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

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

We were able to solve the quadratic program $\mathcal{Q}$ using the BARON software on the NEOS server

`http://www.neos-server.org/neos/`.

The optimal solution to $\mathcal{Q}$ is $\gamma = 15/8$.

The Improved Bound

- It follows that the number of invertible 2 by 2 submatrices in a 4 by s matrix is at most $15s^2/8$.
- The number of invertible 2 by 2 submatrices in an s by s matrix is at most

$$\frac{\binom{s}{4}}{\binom{s-2}{2}} \times \frac{15s^2}{8} = \frac{5s^3(s-1)}{32}.$$

- Hence,

$$R_2(s) \leq \frac{5s^3(s-1)}{32} \times \frac{1}{\binom{s}{2}^2} = \frac{5s}{8(s-1)}.$$

- Asymptotically, the upper bound on $R_2(s)$ has been improved from $2/3$ to $5/8$.

Symmetric BIBDs

- 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 $b = |\mathcal{A}|$; then $b = \lambda v(v-1)/(k(k-1))$.
- Every point occurs in exactly $r = bk/v = \lambda(v-1)/(k-1)$ blocks.
- A *BIBD* is symmetric if $v = b$.
- Suppose $(X, \mathcal{A})$ is a (v, k, λ)-*BIBD*.
- Denote $X = \{x_i : 1 \leq i \leq v\}$ and $\mathcal{A} = \{A_j : 1 \leq j \leq b\}$.
- 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 $x_i \notin A_j$.

Invertibility of Incidence Matrices of Symmetric BIBDs

Lemma 6

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 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. $\square$

Invertibility of Incidence Matrices of Symmetric BIBDs

Theorem 7

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

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

Proof.

Given any two rows of M, we have $a_3 = \lambda$, $a_1 = a_2 = k - \lambda$. Hence,

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

□

The expression (2) is maximized when $k \approx \frac{v}{\sqrt{2}}$, in which case $R_2(M) \approx 1/2$.

An Infinite Class of Examples from SBIBDs

- The points and hyperplanes of the m-dimensional projective geometry over $\mathbb{F}_3$ yield a $\left(\frac{3^{m+1}-1}{2}, \frac{3^m-1}{2}, \frac{3^{m-1}-1}{2}\right)$-*SBIBD*.
- Complement it to get a $\left(\frac{3^{m+1}-1}{2}, 3^m, 2 \times 3^{m-1}\right)$-*SBIBD*.
- Since k odd and λ even, we can apply Theorem 7.
- Then
$$R_2\left(\frac{3^{m+1}-1}{2}\right) \geq \frac{40 \times 3^{2m-3}}{(3^{m+1}-1)(3^m-1)}.$$

Example

- If we take $m = 2$, then we are starting with a $(13, 4, 1)$-*SBIBD*.
- After complementing, we have a $(13, 9, 6)$-*SBIBD*.
- This yields
$$R_2\left(13\right) \geq \frac{15}{26}.$$
- Asymptotically, this class of examples has
$$R_2(M) \approx \frac{40}{81} \approx .494.$$
- This is the best asymptotic result we have at present.

A Possibly Infinite Class of Examples from SBIBDs

- Suppose $q = 4t^2 + 9$ is prime and t is odd.
- Then the quartic residues modulo q, together with 0, form a difference set which generates a $\left(q, \frac{q+3}{4}, \frac{q+3}{16}\right)$-*SBIBD*.
- Complement this design to get a $\left(q, \frac{3(q-1)}{4}, \frac{3(3q-7)}{16}\right)$-*SBIBD*.
- Since k is odd and λ is even, the incidence matrix M is invertible.
- Unfortunately, it is not known if an infinite number of primes of the desired form exist.
- If there are arbitrarily large primes of this type, we obtain

$$R_2(M) \approx \frac{63}{128} \approx .492.$$

Examples from Cyclotomy

- Let $p = 4f + 1$ be prime, where f is even, and let $\nu \in {\mathbb{F}_p}^*$ be a primitive element.
- Let $C_0 = \{\nu^{4i} : 0 \leq i \leq f - 1\}$; 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.
- 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

$$m_{ij} = 1 \text{ if and only if } j - i \in C_0.$$

- The ith row of M' is the incidence vector of $i + C_0$.
- Finally, define M to be the complement of M'.

Cyclotomic Numbers

Theorem 8

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 denoted (j, j), where $(j, j) = |C_j \cap (1 + C_j)|$ for $0 \leq j \leq 3$, are as follows:

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

Invertible 2 by 2 Submatrices

- Using these results on cyclotomic numbers, we can show that the total number of invertible 2 by 2 submatrices in M is

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

- Asymptotically, we have that the density of these examples approaches $63/128 \approx .492$.
- But are the matrices invertible?
- We can check invertibility by a simple $\gcd$ computation.
- Up to order 500, we get invertible matrices when $p = 17, 97, 193, 241, 401, 433, 449$.

Future Work and Open Problems

- Can we improve the upper bounds on $R_2(s)$ by using appropriate software to solve larger quadratic programs?
- Is there a theoretical criterion to determine the invertibility of the matrices obtained from cyclotomy-based constructions?
- It is easy to show that the expected density of invertible 2 by 2 submatrices in an s by s matrix is 0.5, if every entry is chosen randomly to be a "1" with probability $1/\sqrt{2}$. But what about the invertibility of the s by s matrices?
- Does $\lim_{s\to\infty} R_2(s)$ exist? If so, is $\lim_{s\to\infty} R_2(s) = 0.5$?
- We have determined the optimal density $R_2(s)$ for $s \leq 8$ by exhaustive search. Can we extend the exhaustive search to compute $R_2(9)$?

References

[1] P. D'Arco, N. Esfahani and D. R. Stinson. All or nothing at all. ArXiv report 1510.03655, October 13, 2015. `arxiv.org/abs/1510.03655`.

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

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

Thank You For Your Attention!