Some recent results on all-or-nothing transforms,
or
All or nothing at all

Douglas R. Stinson

David R. Cheriton School of Computer Science
University of Waterloo

Alex Rosa 80, Mikulov, June 27–30, 2017

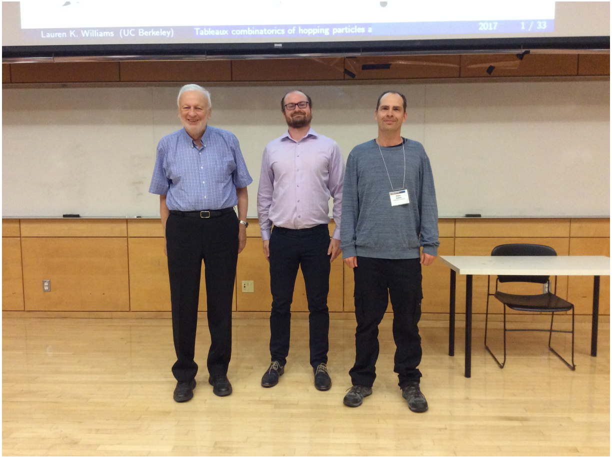
This talk is based on joint work with Paolo D'Arco, Navid Nasr Esfahani and Ian Goldberg.

Congratulations Alex!

Lauren K. Williams (UC Berkeley)
Tableaux combinatorics of hopping particles a

Presentation of the 2012 Euler medal to Alex at CanaDAM

Three ICA Medallists


Lauren K. Williams (UC Berkeley)
Tableaux combinatorics of hopping particles a
2017
1 / 33

Alex Rosa (2012 Euler medal), Padraig Ó Catháin (2015 Kirkman medal) and Peter Dukes (2014 Hall medal)

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 $y_1, \dots, y_s$ 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 $v = |X|$.
- *AONT* were originally defined by Rivest (1997), motivated by an application to cryptography.

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, $s \equiv 0 \mod 4$, and H is a Hadamard matrix of order s.
- $HH^T = sI_s$.
- Construct M by reducing the entries of H modulo p.
- M is invertible modulo p, and therefore M yields a linear (s,p)-*AONT*.

A linear $(4,5)$-AONT:

$$H = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & 1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix} \rightarrow M = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & 4 & 4 \\ 1 & 4 & 1 & 4 \\ 1 & 4 & 4 & 1 \end{pmatrix}.$$

Example: Cauchy Matrices

- An s by s Cauchy matrix can be defined over $\mathbb{F}_q$ if $q \geq 2s$.
- Let $a_1, \ldots, a_s, b_1, \ldots, b_s$ 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 $a_1, \ldots, a_s, b_1, \ldots, b_s$.
- A Cauchy matrix C is invertible, and all of its entries are non-zero, so C yields an (s, q)-*AONT*.

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*.

Linear 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 (D'Arco, Esfahani and Stinson, 2016)

Suppose that q is a prime power and M is an invertible s by s matrix with entries from $\mathbb{F}_q$, such that every t by t submatrix of M is invertible. 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 (t, s, q)-AONT.

Examples

A linear $(2, 5, 5)$-AONT:

$$\begin{pmatrix} 0 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 2 & 3 \\ 1 & 3 & 0 & 1 & 2 \\ 1 & 2 & 3 & 0 & 1 \\ 1 & 1 & 2 & 3 & 0 \end{pmatrix}$$

A linear $(2, 7, 7)$-AONT:

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

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 (D'Arco, Esfahani and Stinson, 2016)

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 $1 \leq t \leq s$.

So the open cases are for $q < 2s$. One particularly interesting question is "how large can s be as a function of q?"

Upper Bound on the Size s

Theorem 4 (Esfahani, Goldberg and Stinson, 2017)

Suppose there is a (t, s, v)-AONT. Then there is an OA(t, s, v).

Proof.

Suppose we represent a (t, s, v)-*AONT* by a v^s by $2s$ array denoted by A. Let R denote the rows of A that contain a fixed $(s-t)$-tuple in the last $s-t$ columns of A. Then $|R| = v^t$. Delete all the rows of A not in R and delete the last s columns of A. The resulting array, A', is an OA(t, s, v). □

Corollary 5

Suppose there is a $(2, s, v)$-AONT. Then $s \leq v + 1$.

Remark: In the linear case, the stronger bound $s \leq v$ can be proven.

Binary AONT with $t = 2$

- When $t = q = 2$, it must be the case that $s \leq 3$.
- $s = 2$ is trivial and $s = 3$ is impossible.
- For $s \geq 3$, this suggests that we consider how “close” to a $(2, s, 2)$-*AONT* we can get.
- We mainly study the linear case.
- For invertible binary s by s matrix M, define

  $$N(M) = \text{number of invertible } 2 \text{ by } 2 \text{ submatrices of } M$$

  and

  $$R(M) = \frac{N(M)}{\binom{s}{2}^2}.$$

- We refer to $R(M)$ as the 2-density of the matrix M.
- We also define

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

- $R(s)$ denotes the maximum 2-density of any invertible binary s by s matrix.

Invertible 2 by 2 Binary Matrices

A 2 by 2 binary 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, $R(M) = 7/9$.
- In fact, this is optimal, so $R(3) = 7/9$.

Another Example

- Consider the following 4 by 4 matrix:

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

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

An Upper Bound on $R(s)$

- 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

$$a_1a_2 + a_1a_3 + a_2a_3.$$

An Upper Bound on $R(s)$ (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 6

A 2 by s binary matrix contains at most $s^2/3$ invertible 2 by 2 submatrices.

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

Theorem 7 (D'Arco, Esfahani and Stinson, 2016)

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

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

Proof.

From Lemma 6, 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

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

□

Improved Upper Bounds

- Using quadratic programming, D'Arco, Esfahani and Stinson (2016) also proved that

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

- Then Zhang, Zhang, Wang and Ge (2016) used a modified quadratic program to show that

$$\limsup_{s\to\infty} R(s) \leq \frac{1}{2}.$$

Lower Bounds from Symmetric BIBDs

- D'Arco, Esfahani and Stinson (2016) suggested using incidence matrices of symmetric BIBDs.
- The incidence matrix of the points and hyperplanes of the m-dimensional projective geometry over $\mathbb{F}_3$ yields 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*.
- This yields

$$R\left(\frac{3^{m+1}-1}{2}\right) \geq \frac{40 \times 3^{2m-3}}{(3^{m+1}-1)(3^m-1)}.$$

- Asymptotically, this class of examples yields

$$\liminf_{s\to\infty} R(s) \geq \frac{40}{81} \approx .494.$$

Lower Bounds from Cyclotomy

- D'Arco, Esfahani and Stinson (2016) also suggested using cyclotomy.
- Suppose $p = 4f + 1$ is prime and f is even.
- Using cyclotomic classes of order 4, we can construct p by p matrices in which the 2-density is (asymptotically) $63/128 \approx .492$.
- Later, Zhang, Zhang, Wang and Ge (2016) used the same technique with cyclotomic classes of order 7 to construct p by p matrices in which the 2-density is (asymptotically) $1200/2401 \approx .49979$.
- These constructions do not necessarily yield invertible matrices. However, Zhang, Zhang, Wang and Ge (2016) observe that it is possible to transform the matrix into an invertible matrix by adjusting the entries on the main diagonal. This does not affect the asymptotic 2-density.

Random Matrices

- D'Arco, Esfahani and Stinson (2016) also suggested using random matrices.
- Consider a binary matrix in which every entry is chosen randomly to be a "1" with probability $1/\sqrt{2}$.
- It is easy to show that the expected 2-density is equal to $1/2$.
- Again, the entries on the main diagonal can be adjusted to get an invertible matrix, without affecting the asymptotic density.
- This works for any order s, so the result is that

$$\lim_{s \to \infty} R(s) = \frac{1}{2}.$$

References

[1] P. D'Arco, N. Nasr Esfahani and D. R. Stinson. All or nothing at all. *Electronic Journal of Combinatorics* **23(4)** (2016), paper #P4.10, 24 pp.

[2] N. Nasr Esfahani, Ian Goldberg and D. R. Stinson. Some results on the existence of t-all-or-nothing transforms over arbitrary alphabets. ArXiv report 1702.06612, Feb. 21, 2017.

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

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

[5] 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.

Thank You For Your Attention!