Some results on the existence of t-all-or-nothing transforms over arbitrary alphabets, or All or nothing at all

Douglas R. Stinson

David R. Cheriton School of Computer Science
University of Waterloo

CanaDAM, Toronto, June 12–15, 2017

In honour of the work of Alex Rosa

This talk is based on joint work with Navid Nasr Esfahani and Ian Goldberg.

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, $s \equiv 0 \bmod 4$, 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 $y_1, \dots, y_s$ 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?"

Reducing the Size s

Theorem 4

If there exists a linear (t, s, q)-AONT with $t < s$, then there exists a linear $(t, s-1, q)$-AONT.

Proof.

Let M be a matrix for a linear (t, s, q)-*AONT*. Consider all the s possible $s-1$ by $s-1$ submatrices formed by deleting the first column and a row of m. We claim that at least one of these s matrices is invertible. For, if they were all noninvertible, then M would be noninvertible, by considering the cofactor expansion with respect the first column of M. $\square$

A linear $(2, q+1, q)$-*AONT* Does Not Exist

From now on, we will focus mainly on the case $t = 2$.

Theorem 5

There is no linear $(2, q+1, q)$-AONT for any prime power q.

Main question: for which prime powers q does there exist a linear $(2, q, q)$-*AONT*?

Computer Searches

We performed an exhaustive search for linear $(2, q, q)$-*AONT* for prime powers $q \leq 11$.

Table: Number of reduced and inequivalent linear $(2, q, q)$-*AONT*

q	reduced $(2, q, q)$-*AONT*	inequivalent $(2, q, q)$-*AONT*
3	2	1
4	3	2
5	38	5
7	13	1
8	0	0
9	0	0
11	21	1

Computer Searches (cont.)

For all odd primes $q \leq 23$, there exists a cyclic $(q-1)$-skew symmetric $(2, q, q)$-*AONT*. These were also found by computer. Here is an example for $q = 11$:

$$\left(\begin{array}{c|cccccccccc}
0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
\hline
1 & 0 & 1 & 4 & 8 & 3 & 5 & 7 & 2 & 6 & 9 \\
1 & 9 & 0 & 1 & 4 & 8 & 3 & 5 & 7 & 2 & 6 \\
1 & 6 & 9 & 0 & 1 & 4 & 8 & 3 & 5 & 7 & 2 \\
1 & 2 & 6 & 9 & 0 & 1 & 4 & 8 & 3 & 5 & 7 \\
1 & 7 & 2 & 6 & 9 & 0 & 1 & 4 & 8 & 3 & 5 \\
1 & 5 & 7 & 2 & 6 & 9 & 0 & 1 & 4 & 8 & 3 \\
1 & 3 & 5 & 7 & 2 & 6 & 9 & 0 & 1 & 4 & 8 \\
1 & 8 & 3 & 5 & 7 & 2 & 6 & 9 & 0 & 1 & 4 \\
1 & 4 & 8 & 3 & 5 & 7 & 2 & 6 & 9 & 0 & 1 \\
1 & 1 & 4 & 8 & 3 & 5 & 7 & 2 & 6 & 9 & 0
\end{array}\right).$$

What is the Pattern?

order			
3		1	
5	1	2	3
7	2 5	3	1 4
11	1 4 8 3	5	7 2 6 9
13	11 3 10 5 4	6	8 7 2 9 1
17	7 1 14 6 3 5 4	8	12 11 13 10 2 15 9
19	8 6 7 13 3 2 17 14	9	4 1 16 15 5 11 12 10
23	7 14 17 2 6 3 4 10 9 1	11	21 13 12 18 19 16 20 5 8 15

Theoretical Results

Theorem 6

Suppose $q = 2^n$ *and* $q - 1$ *is a (Mersenne) prime. Then there exists a linear* $(2, q-1, q)$*-AONT over* $\mathbb{F}_q$*.*

Proof.

Let $\alpha \in \mathbb{F}_q$ be a primitive element and let $M = (m_{r,c})$ be the $q-1$ by $q-1$ Vandermonde matrix in which $m_{r,c} = \alpha^{rc}$, for all r, c, $0 \le r, c \le q-1$. □

Theoretical Results (cont.)

Theorem 7

For any prime power q, there is a q by q matrix defined over $\mathbb{F}_q$ such that any 2 by 2 submatrix is invertible.

Proof.

$M = (m_{r,c})$ be the q by q matrix of entries from $\mathbb{F}_q$ defined by the rule $m_{r,c} = r + c$, where the sum is computed in $\mathbb{F}_q$. □

The above-defined matrix is not invertible if $q > 2$, so this construction does not yield an AONT.

General (Nonlinear or Linear) AONT

Theorem 8

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 9

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

This is slightly weaker than the bound $s \leq v$ that holds in the linear case.

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.

Thank You For Your Attention!