Note 1

February 23,2019

1 Summary

AONT is a type of transform defined in section 1. We classify AONT tranforms into 2 types: linear AONT and nonlinear AONT. To study the existence of (t,s,v) AONT. For fixed q and t, we define

$S(q,t) = \{s : there\ exists\ a\ linear\ (t,s,q)\ AONT\}$,

$s_{max}(q,t) = the\ max\ value\ in\ S(q,t)$.

Then we find the upper bound(necessary condition for existence) and lower bound(construction) for s_{max}. (s_{max} makes sense for linear AONT because the integers in S(q,t) are consecutive. Proof can be seen in **Theorem 5.1**).

1. When studying linear AONT, we mainly use matrix representations for AONT, and we focus on the invertible submatrix of M. I summarized current results of S(q,t) for t=1,t=2 and arbitrary t in section 3 to 5.
2. Orthogonal array is the major tool for studying nonlinear AONT. Existing results include Bush bound and etc. as I summarized in section ?.
3. Computational method is of significant help in the study of AONT. In section , I summarized some computational results.
4. There are certain relationships between resilient function and AONT, which I summarized in section ?.
5. Finally, the last section described the open problem that I'm most interested in now and summarized my thoughts on this problem.

2 Introduction

Definition 2.1. ***General AONT***

Suppose X is a finite field of order q. ϕ is a funtion that maps an input s-tuple to an output s-tuple, i.e. $\phi : X^s \to X^s, \vec{x} = (x_1, x_2, ..., x_s) \mapsto \vec{y} = (y_1, y_2, ..., y_s)$. We call ϕ an (unconditionally secure) (t,s,q)-all-or-nothing transform provided:

1. *ϕ is a bijection.*
2. *If any s-t of the s output values $y_1, y_2, ..., y_s$ are fixed, then the value of any t inputs are completely undetermined (in an information-theoretic sense), i.e. assume z is a t-input of $x_1, x_2, ..., x_s$, then for any $w \in X^t, P(z = w) = \frac{1}{|q^t|}$.*

Lemma 2.1. ***Tool: Unbiased Array(General AONT)***

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

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

Jiayuan Ye, Email:yuan74@mail.ustc.edu.cn
School of Mathematics, University of Science and Technology of China, Hefei, Anhui, 230026, China

Definition 2.2. ***linear AONT***

Suppose X finite field of order q, ϕ is as described above. Then call ϕ a linear AONT if each y_i is an $\mathbb{F}_q$-linear function of $x_1, x_2, ..., x_s$. We can write

$$y = \phi(x) = x \cdot M \text{ and } x = \phi^{-1}(y) = y \cdot M^{-1}$$

where M is an s by s matrix with entries from $\mathbb{F}_q$

Lemma 2.2. ***Tool:Matrix with invertible t×t submatrices(Linear AONT)***

$\mathbb{F}_q$ is a finite field, M is an invertible s by s matrix with entries from $\mathbb{F}_q$. Then M defines a linear (t,s,q)-AONT $\Leftrightarrow$ every t by t submatrix of M is invertible.

3 Linear AONT with t=1

This is fully solved. The following theorem can be directly concluded from **Lemma 2.4**.

Theorem 3.1. *M is an invertible s by s matrix over F_q, such that no entry of M is equal to 0.Then M defines a linear (1,s,q)-AONT.*

Applying the theorem above, We can get the following results:

Result 3.1. ***(Existence)***

1. *S(q,1)={All positive integers}.*

   q>2 is prime power, there exists a linear (1,s,q)-AONT. We can construct such an AONT in many ways including Hadamard matrix, Vandermonde matrix, Cauchy matrix and other computationally-efficient methods. See details in construction

2. *S(2,1)={1,2}*

   q=2, s≥2, then since the matrix in which all entries equal 1 is not invertible, there does not exist a (1,s,2)-AONT.

   Remark: However, we can get quite close. Assume s is even and $M = \begin{pmatrix} 0 & 1 & ... & 1 \\ 1 & 0 & ... & 1 \\ ... & ... & ... & ... \\ 1 & 1 & ... & 0 \end{pmatrix}$*. Then since* $\vec{x} = y \cdot M^{-1} = y \cdot M$*, x_i depends on all the y_j's except for y_i.i.e. if s-1 of outputs are know, assume y_i is unknown, then all x_j's are completely undetermined except x_i.*

Construct 3.2. ***(q>2 prime: Hadamard matrix)***

When s≡0 mod 4 and q>2 is prime, there exists a Hadamard matrix M of order q. Then $MM^T = sI_s (mod\ q) \Rightarrow M^{-1} = q^{-1}M^T$, since M has no zero entry, M defines a linear (1,s,q)-AONT.

Note: The condition above is due to: Hadamard matrix can exist only if s=1,s=2 or s≡0 mod 4.(And it's conjectured that Hadamard matrix exist for all n≡0 mod 4)

Construct 3.3. ***(q>2 prime power, q>s: Vandermonde matrix)***

When q>s+1, take s distinct elements from $\mathbb{F}_q$, say $a_1, a_2, ..., a_s$, then $M = \begin{pmatrix} a_1 & a_1^2 & ... & a_1^s \\ a_2, & a_2^2 & ... & a_2^s \\ ... & ... & ... & ... \\ a_s & a_s^2 & ... & a_s^s \end{pmatrix}$

Construct 3.4. ***(q>2 prime power, q≥2s: Cauchy matrix)***

Since q≥2s, we can take 2s differenet values in $\mathbb{F}_q$, say they are $a_1, ..., a_s, b_1, ..., b_s$. Define M=$(m_{ij})_{s\times s}$, where $m_{ij} = 1/(a_i - b_j)$. Then M defines a (1,s,q)-AONT.

Proof: (1)Since a_i, b_j are distinct, every entry of M is non-zero modular q. (2) det(M)=$\frac{\prod_{1\le i\le j\le n}(x_j-x_i)(y_i-y_j)}{\prod_{1\le i,j\le n}(x_i-y_j)}$*, thus is non-zero modular q. (for calculation details, see this page)*

Jiayuan Ye, Email:yuan74@mail.ustc.edu.cn
School of Mathematics, University of Science and Technology of China, Hefei, Anhui, 230026, China

Construct 3.5. ***(Construction:More Computationally-efficient)***

Suppose $q = p^k$ where p>2 is prime and k is a prime power and s is a positive integer. Then there exists a linear (1,s,q)-AONT.

Pick λ from $\mathbb{F}_q$, s.t. $\lambda \notin \{s-1 \ mod\ p, s-2 \ mod\ p\}$. Define $\gamma = \frac{1}{s-1-\lambda}$,

$$M = \begin{pmatrix} 1-\gamma & -\gamma & ... & -\gamma \\ -\gamma & 1-\gamma & ... & -\gamma \\ ... & ... & ... & ... \\ \gamma & \gamma & ... & -\gamma \end{pmatrix}, M^{-1} = \begin{pmatrix} 1 & 0 & ... & 1 \\ 0 & 1 & ... & 1 \\ ... & ... & ... & ... \\ \lambda & \lambda & ... & \lambda \end{pmatrix}$$

4 Linear AONT with t=2

Result 4.1. $(2, s, 2^n)$ ***Linear AONT***

If $2^n - 1$ is prime and $s \leq q-1$, then there exists a linear $(2, s, 2^q)$ AONT over $\mathbb{F}_q$.

Let $\alpha \in \mathbb{F}_q$ be a primitive element and let M=(m_{ij}) be s by s Vandermonde matrix in which $m_{ij} = \alpha^{ij}$. Since α is primitive, M is invertible. Say M' is a 2 by 2 submatrix of M, and M'=$\begin{pmatrix} \alpha^{ij} & \alpha^{ij'} \\ \alpha^{i'j} & \alpha^{i'j'} \end{pmatrix}$

Then det(M')=0 $\Leftrightarrow ij + i'j' - i'j - ij' \equiv 0 \ mod(q-1)$

$\Leftrightarrow (i-i')(j-j') \equiv 0 \ mod(q-1) \Leftrightarrow \begin{cases} i - i' = 0 \\ j - j' = 0 \end{cases}$

Definition 4.1. ***type μ standard form***

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

There are μ zero diagonal entries, χ is $s-\mu$ by $s-\mu$ matrix.

Theorem 4.1. ***(2,q+1,q) linear AONT doesn't exist***

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

Proof: Take M to be the type μ standard form. Define $(i,j) \sim (i',j') \Leftrightarrow \exists \alpha \in \mathbb{F}_q \setminus \{0\}, s.t. (i,j) = \alpha(i',j')$, then there are q+1 equivlent classes in $\mathbb{F}_q \setminus \{(0,0)\}$.

Let (i,j) run all the columns of 2 rows fixed. Then evevry row contains exactly one zero. Therefore, $\mu = q+1$. M=$\begin{pmatrix} 0 & 1 & 1 & \cdots & 1 \\ 1 & 0 & & & \\ 1 & & 0 & & \\ \vdots & & & \ddots & \\ 1 & & & & 0 \end{pmatrix}$*. Take M' to be the lower right q by q submatrix of M, then each row of M contain each of the q elements in $\mathbb{F}_q$ exactly once. Thus the sum of all rows of M' is zero vector, thus M' is not invertible.*

Lemma 4.2. ***standard μ type of linear (2,q,q)-AONT***

Suppose that M is a matrix for a linear (2,q,q)-AONT in standard form. Then M is of type q or type q-1.

Proof: similar to the previous theorem.

Definition 4.2. ***reduced matrix for linear AONT***

Matrix M is reduced if it's a linear (2,q,q) AONT that satisfies:

1. *the diagonal of M consists of zeros.*
2. *the remaining entries in the first row and first column of M are ones*
3. *the entries in column 3,...,q of row 2 of M are in increasing order.*

Result 4.2. ***Computational results for linear (2,q,q)-AONT***

Result 4.3. ***Summary for (2,s,q) linear AONT***

Jiayuan Ye, Email:yuan74@mail.ustc.edu.cn
School of Mathematics, University of Science and Technology of China, Hefei, Anhui, 230026, China

5 Linear AONT for arbitrary t

Theorem 5.1. ***Existence of linear AONT with recursive s***

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

Proof: We only need to proove there exists a s-1 by s-1 invertible submatrix of M. Applying pegion-pole principle, we can get the result aspired.

Result 5.1. ***Existence of the strongest AONT***

When q≥2s,an s by s Cauchy matrix M can be defined over $\mathbb{F}_q$(For construction, see Construction 3.4).

Since every submatrix of M is a Cauchy matrix, thus is invertible. Cauchy matrix immediately yield the strongest AONT possible, i.e. M is a (t,s,q) AONT for all t≤s.

6 General AONT for arbitrary t

The most popular method for studying this problem is applying $t-(v,k,\lambda)$ orthogonal array.

Definition 6.1. ***orthogonal array***

A $t-(v,k,\lambda)$-OA (t≤k) is a $\lambda v^t \times k$ array whose entries are chosen from a set X with v points s.t. in every subset of t columns of the array, every t-tuple of points of X appears in exactly λ rows.

Theorem 6.1. ***(t,s,v) AONT and t-(v,s,1) OA***

Suppose we represent a (t,s,v)-AONT by a $(v^s, 2s, v)$-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. Dlete all the rows of A not in R and delete the last s columns of A and call the resulting array A'. Within any t columns of A, we see that every t-tuple of symbols occur exactly once, since the rows of A' are determined by fixing s-t outputs of the AONT. This says that A' is an t-(v,s,1)-OA.

Result 6.1. ***Bush Bound***

If there is an t-OA(v,s,1), then

$$s \le \begin{cases} v+t-1 & if\ t=2, or\ if\ v\ is\ even\ and\ 3 \le t \le v \\ v+t-2 & if\ v\ is\ odd\ and\ 3 \le t \le v \\ t+1 & if\ t \ge v \end{cases}$$

Proof: Left to be studied.

Corollary 6.2. ***Results deduced from Bush bound***

- *If there is a (2,s,v) AONT, then s≤v+1*
- *If there is a (3,s,v) AONT and v≥3, then* $s \le \begin{cases} v+1 & v\ is\ even \\ v+2 & v\ is\ odd \end{cases}$
- *If t ≥ v, s∈{t,t+1}*

7 Connection between resilient function and AONT

Definition 7.1. ***Resilient function***

Let |X|=v. An (n,m,t,q)-resilient function is a function $g: X^n \to X^m$ which has the property that, if any t of the n input values are fixed and the remaining n-t input values are chosen independently and uniformly at random, then every output m-tuple occurs with the same probability $1/q^m$

Theorem 7.1. ***AONT and resilient funtion: Linear***

Suppose there is a linear (t,s,q)-AONT. Then there is a linear (s,s-t,t,q) resilient function.

Proof: Suppose that the s by s matrix M over $\mathbb{F}_q$ gives rise to a linear (t,s,q)-AONT. Then, from lemma 3,every t by t submatrix of M is invertible. Construct an s by t matrix M^* by deleting any s-t rows of M. Clearly any t columns of M^* are linearly independent.

Let $\mathscr{C}$ be the code generated by the rows of M^* and let $\mathscr{C}'$ be the dual code(i.e. $\mathscr{C}$ is the parity chaeck matrix of code $\mathscr{C}'$). Then $\mathscr{C}$ has column rank t⇔ code $\mathscr{C}'$ has minimum distance at least t+1.

Jiayuan Ye, Email:yuan74@mail.ustc.edu.cn
School of Mathematics, University of Science and Technology of China, Hefei, Anhui, 230026, China

Let N be a generating matrix for $\mathscr{C}'$, Then the function $f(x) = xN^T$ is a (linear) (s,s-t,t,q) resilient function.

Question: I don't understand why not just choose s-t rows of M to form N. This seems straightforward.

Theorem 7.2. ***AONT and resilient function: General***

Left to be studied.

8 My current focus

1. Is there a similar relationship in non linear AONT transforms as described in **Theorem 5.1**?
2. When t≥ v, according to **Cor 6.2**, s∈{t,t+1}. Then under what circumstances can s take these two values?
3. In the case of (2,s,v) general AONT, can the bound in **Cor 6.2** be strengthened to s≤v, analogous to the linear case?
4. For (3,s,q) AONT, there are already 2 results:
   - When q≥2s, there exists (3,s,q) AONT
   - If there exists (3,s,q) AONT, then s≤ $\begin{cases} q+1 & q \text{ is even} \\ q+2 & q \text{ is odd} \end{cases}$

   What additional results can be proven(especially for (3,q,q) AONT)?

   Question: what if q is not prime power? Can I simply map q to be a subset of a finite field solve this problem?
5. Are there any additional tool for studying general AONT besides OA?

Jiayuan Ye, Email:yuan74@mail.ustc.edu.cn
School of Mathematics, University of Science and Technology of China, Hefei, Anhui, 230026, China