中国科学技术大学

本科大研结题论文

一类特殊变换 AONT 的存在性与构造的研究

作者姓名： 叶嘉沅

学科专业： 信息与计算科学

导师姓名： 张先得 教授

完成时间： 二〇一九年十月二十四日

University of Science and Technology of China

A dissertation for bachelor’s degree

AONT: existence, construction and application

Author: Jiayuan Ye

Speciality: Information and Computing Sciences

Supervisor: Prof. Xian De Zhang

Finished time: October 24, 2019

目录

第一章　中文内容摘要

(t,s,q)-all-or-nothing 变换（简称 AONT）是一个 q 元域上的 s 元组到 s 元组的双射，它能够保证如果已知 s-t 个输出，则任意 t 个输出的值都是完全不能确定的。在这篇文章中的主要问题就是，什么样的情况下 AONT 存在。本文总结了此前的结果，这包括 t=1 时的已被完全确定的存在性结果，t=2 时的构造证明存在性结果，t=2 时的穷举结果（q<29）。本文还单独总结了二元域上 AONT 的存在和构造结果。最后，本文总结了这个问题中还没有解决的可研究问题。

关键词：AONT; 有限域; 正交阵列; 密码学

第二章　简介

设 X 是一个有限集合（也称为字母表），s 为正整数，函数 ϕ 为 X 上的 s 元组上的变换，$\phi : X^i \Leftarrow X^s, x = (x_1, ..., x_s) \mapsto y = (y_1, ..., y_s)$. 如果下列条件满足，我们就称 ϕ 为一个 AONT 变换

1. ϕ 是双射.
2. 若 s 个输出中的 s-t 个值 $y_1, y_2, ..., y_s$ 固定时, 任意 t 个输入是完全不能确定的 (信息论意义下), i.e. 假设 z 是 $x_1, x_2, ..., x_s$ 中的一个长度为 t 的输入, 则 $\forall w \in X^t, P(z = w) = \frac{1}{|q^t|}$.

也可在熵意义下对它做一个新的定义。设 $X_1, ..., X_s, Y_1, ..., Y_s$ 是在有限集合 X 上取值的随机变量。（$X_1, ..., X_s$ 不需要独立，也不需要同分布）则 2s 个随机变量可以确定一个 AONT 变换为 ϕ 为 X 上的 s 元组上的变换 $\phi : X^i \Leftarrow X^s, x = (X_1, ..., X_s) \mapsto y = (Y_1, ..., Y_s)$，如果以下条件满足

1. $H(Y_1, ..., Y_s | X_1, ..., X_s) = 0$
2. $H(X_1, ..., X_s | Y_1, ..., Y_s) = 0$
3. $H(X_{i_1}, ..., X_{i_t} | Y_{j_1}, ..., Y_{j_{s-t}}) = H(X_{i_1}, ..., X_{i_t})$ 对任意 $1 \leqslant i_1 < ... < i_t \leqslant s$ 和 $1 \leqslant j_1 < ... < j_{s-t} \leqslant s$ 都成立

AONT 变换是一类有广泛应用的变换，包括在 package transform, exposure-resilient functions,network coding,secure data transfer,anti-jamming techniques,secure distributed cloud storage,query anonymization for location-based service 等方面的应用。

第三章　AONT 的基本性质以及研究主题

第一节　线性 AONT 基本性质

由于线性 AONT 可以由**矩阵**表示，设 $\phi(x) = x \cdot M^{-1}$, 则可以通过刻画 M 的**矩阵性质**来刻画线性 AONT[1?]：

引理 3.1　设 M 为 (t,s,q) 线性 AONT 的矩阵表示，则 M 为一个 s 阶 $\mathcal{F}_q$ 上方阵，且 M 的所有 t 阶子矩阵均可逆。

证明　不妨设 $y_{t+1}, ..., y_s$ 已知，M_1 是 M 的子矩阵,$M_1 = M\begin{pmatrix} 1 & ... & t \\ 1 & ... & s \end{pmatrix}$。则以 $(x_1, x_2, ..., x_t)$ 为例，设 $M_{1t} = M\begin{pmatrix} 1 & ... & t \\ 1 & ... & t \end{pmatrix}$，则 $(x_1, ..., x_t) = (y_1, ..., y_t) \cdot M_{1t}$。由于 $(x_1, ..., x_t)$ 完全不确定，故 M_{1t} 可逆，同理可证 M 的任意 t 阶子矩阵可逆。　□

线性 AONT 的存在性有归纳关系

引理 3.2　(t,s,q) 线性 AONT 存在，则 (t,s-1,q) 线性 AONT 存在

证明　设 M 为 (t,s,q) 线性 AONT 的矩阵表示，考虑 M 的 $(s-1)\times(s-1)$ 子矩阵，若 $\forall(s-1)\times(s-1)$ 子矩阵均不可逆，则与 M 可逆矛盾。　□

第二节　线性 AONT 研究主题

若定义 S(t,q) 是使线性 AONT 存在的 s，则**引理**3.2的归纳关系，可以直接推出，S(t,q) 有上界 M(t,q)，且对于 $\forall s\ s.t.\ t \leqslant s \leqslant M(t,q)$，(t,s,q) 线性 AONT 均存在。

故线性 AONT 的存在性结果，主要在于对 **M(t,q)** 的研究。主要可分为研究 **M(t,q)** 的上界和下界。

由于 q=2 的广泛应用价值，对于 q=2 的 AONT 的研究也吸引了很多注意。

- **上界**

  要得到上界主要是通过**证明**的方法，证明某个 s 下不存在 (t,s,q)AONT。

- **下界**

  要得到下界主要通过**构造**的方法，构造出某个 s 下具体的 (t,s,q)AONT 来证明下界 ⩾s。

第三节 非线性 AONT 基本性质

非线性 AONT 可以由**阵列**来表示，可以通过**阵列性质**刻画。先将无偏阵列定义阐述如下

定义 3.1 设 A 是 $N \times k$ 阵列，其中的元素是大小为 v 的集合 $\mathcal{X}$ 中的元素，则称 A 为 (N,k,v) **阵列**。设 $D \subseteq \{1, 2, ..., k\}$，定义 A_D 为从 A 中删去所有 D 之外的列后得到的阵列。若 A_D 中，任意 D 元组均出现 $N/v^{|D|}$ 次，则称 A 为相对于 D 的**无偏阵列**

然后自然由非线性 AONT 定义，得到下面的引理（阵列刻画）

引理 3.3 设 A 为一个 (t,s,q)AONT 的阵列表示，则 A 为一个 q^s 行，$2s$ 列的阵列，且它关于以下列集合是**无偏 (unbiased)** 的

- {1,2,...,s}
- {s+1,s+2,...,2s}
- $\mathcal{X} \cup \mathcal{Y}, \mathcal{X} \subseteq \{1, 2, ..., s\}, \mathcal{Y} \subseteq \{s+1, s+2, ..., 2s\}$ and $|\mathcal{X}| = t, |\mathcal{Y}| = s - t$

非线性 AONT 也有一些**归纳关系**

引理 3.4 Product Construction

如果存在 (t,s,m)AONT 和 (t,s,n)AONT，则存在 (t,s,mn)AONT

证明 设 $A = [(a_{i,j})]$ 是 $\mathbb{Z}_n$ 上的 $(n^s, 2s, n)$ 阵列，它对应于一个 (t,s,n)AONT，$B = [(b_{i,j})]$ 是 $\mathbb{Z}_m$ 上的 $(m^s, 2s, m)$ 阵列，它对应于一个 (t,s,m)AONT。则对 $1 \leqslant i \leqslant n^s$ 和 $1 \leqslant j \leqslant m^s$，设

$$H_{i,j} = ((a_{i,1}, b_{j,1}), (a_{i,2}, b_{j,2}), ..., (a_{i,2s}, b_{j,2s}))$$

容易验证由所有 $H_{i,j}$ 行向量构成的阵列，是一个 $\mathbb{Z}_m \times \mathbb{Z}_n$ 上对应于 (t,s,nm)AONT 的正交阵列。 □

第四节 非线性 AONT 研究主题

对于非线性 AONT 的研究在于**构造**，即能否构造出线性结果构造不出的 AONT。

第四章　线性 AONT 下 M(t,q) 的已有研究结果整理

已有的 $M(t,q)$ 结果可以分为上界结果和下界结果，将结果与研究方法整理如下。

- 证明**上界**一般涉及**不存在性**的证明，较为困难，证明方法也不尽相同。基本的思路是，通过所有 t 阶子方阵均可逆，得到对矩阵的一系列约束。然后想办法得到与整体可逆性或者与某一个 t 阶子方阵的可逆性矛盾的结果。
- 证明**下界**主要是通过**构造**。可以先简化矩阵结构然后设计算法进行简单穷举。

下面对结果进行归类和证明

第一节　一般性 M(t,q) 与 t,q 的关系

下面的定理来自[2]，阐述了对**一般性 t,q** 均成立的**下界**结果，这也是我所阅读过的论文中唯一的一般性结果。

定理 4.1　$M(t,q) \geqslant \lfloor q/2 \rfloor$

证明　在[2]中，他们通过 **Cauchy 矩阵**定义了一类强 AONT，即对任意 t，均为 AONT。

1. 首先定义 q 元域上的 s 阶 Cauchy 矩阵。

   q⩾2s 时，可以按照下面的方法构造 $\mathcal{F}_q$ 上的 $s\times s$**Cauchy 矩阵**。设 $a_1,a_2,\cdots,a_s$ 和 $b_1,b_2,\cdots,b_s$ 是 $\mathcal{F}_q$ 上 $2s$ 个互异元素。则令 $c_{ij}=1/(a_i-b_j), 1\leqslant i\leqslant s, 1\leqslant j\leqslant s$。则 $C=(c_{ij})$ 是由 $a_1,a_2,\cdots,a_s,b_1,b_2,\cdots,b_s$ 决定的 Cauchy 矩阵。
2. 然后证明由 Cauchy 矩阵确定的线性变换对任意 t 都是 AONT。由于 Cauchy 矩阵的任意阶子方阵依然是 Cauchy 矩阵，故只需证明 $\forall n$，n 阶 Cauchy 矩阵是可逆的。

   设 D_n 是 n 阶 $Cauchy$ 矩阵,

$$D_n=\begin{pmatrix}\frac{1}{x_1-y_1} & \frac{1}{x1-y2} & \cdots & \frac{1}{x_1-y_n}\\ \frac{1}{x_2-y_1} & \frac{1}{x_2-y_2} & \cdots & \frac{1}{x_2-y_n}\\ \vdots & \vdots & \ddots & \vdots\\ \frac{1}{x_n-y_1} & \frac{1}{x_n-y_2} & \cdots & \frac{1}{x_n-y_n}\end{pmatrix}$$

则第 2,...,n 列减去第一列

$$det(D_n)=\begin{vmatrix} \frac{1}{x_1-y_1} & \frac{1}{x_1-y_2}\frac{y_2-y_1}{x_1-y_1} & \cdots & \frac{1}{x_1-y_n}\frac{y_n-y_1}{x_1-y_1} \\ \frac{1}{x_2-y_1} & \frac{1}{x_2-y_2}\frac{y_2-y_1}{x_2-y_1} & \cdots & \frac{1}{x_2-y_n}\frac{y_n-y_1}{x_2-y_1} \\ \vdots & \vdots & \ddots & \vdots \\ \frac{1}{x_n-y_1} & \frac{1}{x_n-y_2}\frac{y_2-y_1}{x_n-y_1} & \cdots & \frac{1}{x_n-y_n}\frac{y_n-y_1}{x_n-y_1} \end{vmatrix}$$

$$=\frac{\prod_{j=2}^{n}(y_j-y_1)}{\prod_{i=1}^{n}(x_i-y_1)}\begin{vmatrix} 1 & \frac{1}{x_1-y_2} & \cdots & \frac{1}{x_1-y_n} \\ 1 & \frac{1}{x_2-y_2} & \cdots & \frac{1}{x_2-y_n} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & \frac{1}{x_n-y_2} & \cdots & \frac{1}{x_n-y_n} \end{vmatrix}$$

第 2,...,n 行减去第一行

$$=\frac{\prod_{j=2}^{n}(y_1-y_j)}{\prod_{i=1}^{n}(x_i-y_1)}\begin{vmatrix} 1 & \frac{1}{x_1-y_2} & \cdots & \frac{1}{x_1-y_n} \\ 0 & \frac{1}{x_2-y_2}\frac{x_1-x_2}{x_1-y_2} & \cdots & \frac{1}{x_2-y_n}\frac{x_1-x_2}{x_1-y_n} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & \frac{1}{x_n-y_2}\frac{x_1-x_n}{x_1-y_2} & \cdots & \frac{1}{x_n-y_n}\frac{x_1-x_n}{x_1-y_n} \end{vmatrix}$$

$$=\frac{\prod_{j=2}^{n}(y_1-y_j)\prod_{i=2}^{i=n}(x_1-x_i)}{\prod_{i=1}^{n}(x_i-y_1)\prod_{j=2}^{j=n}(x_1-y_j)}\begin{vmatrix} 1 & 1 & \cdots & 1 \\ 0 & \frac{1}{x_2-y_2} & \cdots & \frac{1}{x_2-y_n} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & \frac{1}{x_n-y_2} & \cdots & \frac{1}{x_n-y_n} \end{vmatrix}$$

$$=\frac{\prod_{j=2}^{n}(y_1-y_j)\prod_{i=2}^{i=n}(x_1-x_i)}{\prod_{i=1}^{n}(x_i-y_1)\prod_{j=2}^{j=n}(x_1-y_j)}\begin{vmatrix} \frac{1}{x_2-y_2} & \cdots & \frac{1}{x_2-y_n} \\ \vdots & \ddots & \vdots \\ \frac{1}{x_n-y_2} & \cdots & \frac{1}{x_n-y_n} \end{vmatrix}$$

以此类推归纳可得

$$det(D_n)=\frac{\prod_{1\leqslant i<j\leqslant n}(x_j-x_i)(y_j-y_i)}{\prod_{1\leqslant i,j\leqslant n}(x_i-y_j)}$$

由于 $x_1,x_2,...,x_n,y_1,y_2,...,y_n$ 是不同的元素，所以 $det(D_n)\neq 0$

□

第二节 M(1,q) 与 q 的关系

M(1,q) 在论文[3] 中被完全确定，首先将 M(1,q) 的结果阐述如下。

定理 4.2 $M(1,q)=\begin{cases}2 & q=2\\ Z^{+} & q>2\end{cases}$

然后通过表格将具体构造性结果和不存在性的证明结果整理如下

表 4.1 $M(1,q)$ 上下界结果及构造方法

q	结果	工具
q=2 素数幂	M(1,2)=1	反证法
q>2 素数幂	$M(1,q)=Z^{+}$	$I-\gamma J$(J 为全 1 矩阵)
q>2 素数	$M(1,q)=Z^{+}$	Hadamard 矩阵
q>2 素数幂	$M(1,q)\geqslant q-1$	Vandermonde 矩阵
q>2 素数幂	$M(1,q)\geqslant \lfloor q/2\rfloor$	Cauchy 矩阵

下面的定理由 **引理**3.1直接推出，是研究 (1,s,q) 线性 AONT 的主要工具。

定理 4.3 M 是 F_q 上 $s\times s$ 方阵, 且 M 没有 0 元素. 则 M 定义了一个线性 (1,s,q)-AONT.

定理 4.4 M(1,2)=1

证明 由于 $\mathcal{F}_2$ 上非 0 元素只有 1，故若存在 (1,s,2)AONT 的矩阵表示为全 1 矩阵，显然不可逆，故矛盾。故 M(1,2)=1。 □

注 虽然 $q=2$ 时对 $s>1$ 不存在 $(1,s,2)$AONT，但是可以得到减弱版的与 AONT 性质相当接近的结构。假设 s 为偶数，$M=\begin{pmatrix}0&1&\dots&1\\1&0&\dots&1\\\dots&\dots&\dots&\dots\\1&1&\dots&0\end{pmatrix}$。则有 $M=M^{-1}$，故 $\boldsymbol{x}=y\cdot M^{-1}=y\cdot M$。于是 x_i 的取值依赖于除 y_i 之外的所有 y_j。i.e. 若已知 $s-1$ 个输出，不妨设 y_i 是未知的，则除 x_i 之外的所有 x_j 都是完全随机的。

定理 4.5 (Hadamard matrix) $q>2$ 素数时，$M(1,q)=Z^{+}$

证明 由于线性 AONT 的归纳性质**引理**3.2，只需证明任意大的整数 N，均存在 (1,s,q) 线性 AONT，其中 $s>N$，由于 Hadamard 矩阵可以得到对 $\forall s\equiv 0$ mod 4，均有 (1,s,q) 线性 AONT

当 $s \equiv 0 \mod 4$ 且 $q > 2$ 是素数时, 存在 s 阶 Hadamard 矩阵 M。则 $\boldsymbol{M}\boldsymbol{M}^T = s\boldsymbol{I}_s \mod q$, i.e.$\boldsymbol{M}^{-1} = q^{-1}\boldsymbol{M}^T$。由于 M 没有 0 元素, 故 M 是一个线性 (1,s,q)-AONT. □

注 上面的条件是由 Hadamard 矩阵的存在性导出的。Hadamard 矩阵存在的必要条件是 $s = 1, s = 2$ 或 $s \equiv 0 \mod 4$ 时存在。(同时有未证明但是一般认同的猜想：对 $\forall s \equiv 0 \mod 4$，都存在 s 阶 Hadamard 矩阵。

定理 4.6 (Vandermonde matrix) 若 $q > 2$ 素数幂, 则 $M(1, q) \geqslant q - 1$

证明 只需证明存在 (1,q-1,q) 线性 AONT。由于 $q \geqslant s + 1$, 所以可以从 $\mathbb{F}_q$ 中挑选出 s 个互异非 0 元素，设为 $a_1, a_2, ..., a_s$, 则可以构造 Hadamard 矩阵 $\boldsymbol{M} = \begin{pmatrix} a_1 & a_1^2 & ... & a_1^s \\ a_2, & a_2^2 & ... & a_2^s \\ ... & ... & ... & ... \\ a_s & a_s^2 & ... & a_s^s \end{pmatrix}$。则 M 定义了一个 (1,q-1,q) 线性 AONT □

定理 4.7 (Cauchy matrix) 若 $q > 2$ 素数幂，则 $M(1, q) \geqslant \lfloor q/2 \rfloor$

这是由**定理**4.1直接得到的。

定理 4.8 ($\boldsymbol{I} - \gamma\boldsymbol{J}$) 若 q 为素数幂，且 $q > 2$，则 $M(1, q) = Z^+$

证明 可以通过矩阵 $\boldsymbol{I} - \gamma\boldsymbol{J}$，对任意大的整数 s 构造 (1,s,q) 线性 AONT。

从 $\mathbb{F}_q$ 中选取 λ，s.t.$\lambda \notin \{s - 1 \ mod \ p, s - 2 \ mod \ p\}$. 定义 $\gamma = \frac{1}{s-1-\lambda}$

令 $\boldsymbol{M} = \begin{pmatrix} 1-\gamma & -\gamma & ... & -\gamma \\ -\gamma & 1-\gamma & ... & -\gamma \\ ... & ... & ... & ... \\ \gamma & \gamma & ... & -\gamma \end{pmatrix}$,

则显然 M 无 0 元素，且则容易验证

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

故 M 定义了一个 (1,s,q) 线性 AONT。 □

第三节 M(2,q) 与 q 的关系

对于 t=2 的情况，之前的[4] 与[5] 做了一些深入的研究，包括**上界**与**下界**，首先用表格的方式将结果与研究工具整理如下

表 4.2 $M(2,q)$ 上下界结果及使用工具

结果类别	结果	工具
上界	q 素数幂，$M(2,q) \leqslant q$	q 元域所有元素之和为 0
下界	q 素数幂，$M(2,q) \geqslant \phi(q)$	循环码 (cyclic code)
	q 素数幂，$M(2,q) \geqslant \lfloor q \rfloor$	Cauchy 矩阵
	p 素数，$M(2,p) \geqslant p$	循环码 (cyclic code)
	若 $q=2^n$ 且 $q-1$ 为素数, 则 $M(2,q) \geqslant q-1$	有限域的原根性质
q 定值	$M(2,4)=4$	穷举算法
	$M(2,8)=7$	
	$M(2,9)=8$	

证明上界结果时包含 (2,q+1,q) 线性 AONT 的不存在性的证明，这是为数不多的已有的不存在性的证明，值得借鉴。在构造下界的 AONT 时，利用了多种方法，已有的包括通过转化为循环码，通过简化矩阵结构设计的简单穷举算法等等。

一、不存在性：(2,q+1,q) 线性 AONT

基本的思路是，通过所有 t 阶子方阵均可逆，得到对矩阵的一系列约束。然后想办法得到与整体可逆性或者与某一个 t 阶子方阵的可逆性矛盾的结果。

定理 4.9 q 为素数幂，则 $M(2,q) \leqslant q$

证明 要证 $M(2,q) \leqslant q$ 只需证不存在 $(2,q+1,q)$ 线性 AONT，分为 $q=2$ 和 $q>2$ 两种情况来证明

- 若 q=2，则首先列出所有的 2 阶 $\mathcal{F}_2$ 上可逆矩阵 $\begin{pmatrix}1&1\\1&0\end{pmatrix}\begin{pmatrix}1&1\\0&1\end{pmatrix}\begin{pmatrix}0&1\\1&1\end{pmatrix}\begin{pmatrix}1&0\\1&1\end{pmatrix}\begin{pmatrix}1&0\\0&1\end{pmatrix}\begin{pmatrix}0&1\\1&0\end{pmatrix}$.
  反证设 M 是 (2,3,2) 线性 AONT 的对应矩阵，则 M 的任两行都包含 3 个可逆 2×2 子矩阵。故每行都包含 2 个 1，1 个 0（若 0 多于 1 个则与可逆性矛盾，若没有 0 则另一行必定包含 2 个 0 或 2 个 1 也与可逆性矛盾）。故 $M\cdot(1,1,1)^T=0$ in $\mathcal{F}_2$，与 M 可逆性矛盾。

故不存在 (2,3,2) 线性 AONT

- 若 q>2，反证：假设存在 (2,q+1.q) 线性 AONT，设它相对应的矩阵为 M。考虑 M 的 $2\times(q+1)$ 矩阵，它由 q+1 个二维向量构成。所有二维非零向量共 q^2-1 个，按照线性相关可分为 q+1 个等价类。因此矩阵的两行中，每个等价类出现一次，故矩阵每行都有一个 0 元素。故可以将矩阵归纳为 q+1 standard form。而每个列向量除去第一行元素后，是 q 元域上的 q 个元素各出现一次。故 q>2 时，后 q 行的向量和的每个元素均等于 $\sum_{x\in\mathcal{F}_q} x=0$

□

二、一般 q 的构造：利用循环码

定理 4.10 $M(2,q)\geqslant\phi(q)$

证明 设 $q=p^r$ 是素数幂，α 是 $\mathcal{F}_q$ 上一个原根。构造矩阵 P 是 $\mathcal{F}_q$ 上的 $(q-1)\times(q-1)$ 矩阵，其中 $P(s,t)$ 表示 P 的第 s 行，第 t 列元素。$P(s,s)=0, s=0,1,...,q-2; P(s,t)=\frac{\alpha^s}{\alpha^s-\alpha^t}, s=0,1,...,q-2, t=0,1,...,q-2, s\neq t.$

- 先证明 P 的任意 2×2 子矩阵均可逆。考虑 P 的第 i 行第 j 行和第 i’ 列第 j’ 列构成的子矩阵。其中 $i<j, i'<j'$, 分下面两种情况讨论
  1. 若 $i=i'$(或 $i=j', j=i', j=j'$), 则 $det(P)=-P(i,j')P(i',j)\neq 0$
  2. 其他情况, $det(P')=\frac{\alpha^i}{\alpha^i-\alpha^{i'}}\frac{\alpha^j}{\alpha^j-\alpha^{j'}}-\frac{\alpha^i}{\alpha^i-\alpha^{j'}}\frac{\alpha^j}{\alpha^j-\alpha^{i'}}$。故当且仅当 $(\alpha^i-\alpha^j)(\alpha^{i'}-\alpha^{j'})=0$ 时上式成立。即当且仅当 $i=j$ 且 $i'=j'$ 时成立，与 $i<j, i'<j'$ 矛盾，故 $det(P')\neq 0, P'$ 可逆。
- 再证明 $rank(P)=\Phi(q)$，观察到矩阵 P 是循环的，故可以考虑 P 作为生成矩阵的循环码 (cyclic code)[?]。
  1. 长度为 n 的 $\mathcal{F}_q$ 上的线性码 C 称为循环码，如果 $\forall$ 向量 **c**= $(c_0,c_1,\cdots,c_{n-1})\in C$ 做一次循环移位得到的向量 $(c_{n-1},c_0,\cdots,c_{n-2})$ 也属于 C。
  2. 考虑 $\mathcal{F}_q^n$ 到最高次不超过 n-1 的 $\mathcal{F}_q[x]$ 多项式环 $\mathcal{F}_q/(x^n-1)$ 的同构映射 $\phi:(c_0,c_1,\cdots,c_{n-1})\mapsto c(x)=c_0+c_1x+\cdots+c_{n-1}x^{n-1}$。则由 **c** 生成循环码 C 作为 $\mathcal{F}_q^n$ 的子空间可以同构于 $\mathcal{F}_q[x]/(x^n-1)$ 的生成元是 $gcd(c(x),x^n-1)$ 的理想。故 C 的维数为 $n-deg(gcd(c(x),x^n-1))$
  3. 若 P 为 C 的生成矩阵，则 $rank(P)=dim(C)$
- 构造 P 作为生成矩阵的循环码，其生成多项式为 $f(x)=0+\frac{1}{1-\alpha}x+\frac{1}{1-\alpha^2}x^2+$

$... + \frac{1}{1-\alpha^{q-2}x^{q-2}}$。故 $rank(P) = q - 1 - deg(gcd(f(x), x^{q-1} - 1))$。由于 $x^{q-1} - 1 = (x-1)(x-\alpha)...(x-\alpha^{q-2})$。而 $\Phi(q) = p^{r-1}(p-1) = p^r - p^{r-1}$ 其中 $q = p^r$, 故要证明 $rank(P) = \Phi(q)$ 只需证明 $p^r - 1 - deg(gcd(x^{q-1} - 1, f(x))) = p^r - p^{r-1}$,i.e. 只需证 $deg(gcd(x^{q-1} - 1, f(x))) = p^{r-1} - 1$，i.e. 只需证明 $f(x)$ 在 $\mathcal{F}_q$ 上有 $p^{r-1} - 1$ 个不同的根。

Claim:$\{x \in \mathcal{F}_q | f(x) = 0\} = \{\alpha^p, \alpha^{2p}, ..., \alpha^{(p^{r-1}-1)p}\}$

Proof:

1. 若 $x = 1$, 则 $f(x) = \frac{1}{1-\alpha} + \frac{1}{1-\alpha^2} + ... + \frac{1}{1-\alpha^{q-2}} = -1 \neq 0$
2. 若 $x = \alpha^{kp}, 1 \leqslant k \leqslant p^{r-1} - 1$, 则 $-f(\alpha^{kp}) = 0 - f(\alpha^{kp}) = 1 + \frac{1}{1-\alpha}(1-x) + \frac{1}{1-\alpha^2}(1-x^2) + ... + \frac{1}{1-\alpha^{q-2}}(1-x^{q-2})$. 又因为

$$\frac{1}{1-\alpha^i}(1-(\alpha^{kp})^i) = \frac{1}{1-\alpha^i}(1-(\alpha^i)^{kp}) = 1 + \alpha^i + ... + (\alpha^i)^{kp-1}$$

所以可以将 $-f(\alpha^{kp})$ 展开如下:

$$-f(\alpha^{kp}) = q - 1 + \sum_{j=1}^{kp-1}\sum_{i=1}^{q-2}(\alpha^i)^j = q - 1 + (kp-1)\cdot(-1) = 0$$

故 $\alpha^{kp}, 1 \leqslant k \leqslant p^{r-1} - 1$ 为 f(x) 的根

3. 若 $x = \alpha^{kp+r}, 1 \leqslant r < p$ 且 $1 \leqslant k \leqslant p^{r-1} - 1$，则与 2 同理：$-f(\alpha^{kp+r}) = q - 1 + (kp + r - 1)(-1) = -r \neq 0$

故 $f(x) = 0$ 的解恰为 p^{r-1} 个，$\{x \in \mathcal{F}_q | f(x) = 0\} = \{\alpha^p, \alpha^{2p}, ..., \alpha^{(p^{r-1}-1)p}\}$

□

定理 4.11 若 q 为素数，记 $p = q$, 则 $M(2, p) = p$

由**定理**4.9得 $M(2, p) \leqslant p$。故只需构造出一个 (2,p,p) 线性 AONT 即可。在论文[5] 中给出了利用循环码转化为循环码维数问题的构造性证明。

构造: 令 A=(A(s,t)) 为 $\mathcal{F}_p$ 上的 $p \times p$ 矩阵。A(s,t) 表示 A 第 s 行第 t 列元素。A(s,s)=0 , s=0,1,...,p-1, A(s,1)=1,s=1,2,...,p-1A(s,t)=$(s-t)^{-1}$ for s=0,1,...,p-1,t=1,2,...,p-1,$s \neq t$。则 A 为 (2,p,p) 线性 AONT。

证明 证明分为两步，先证明 A 的所有 2 阶子矩阵均可逆，然后证明 A 可逆。

- 首先证明 A 的 2×2 子方阵均可逆。考虑 A 的第 i,j 行和第 i',j' 列构成的 2×2 子矩阵 A'，其中 i<i',j<j', 考虑下面几种情况

  1. 若 $i = i'$(或 $i = j'$ 或 $j = i'$ 或 $j = j'$)，则 $det(A') = -A(i, j')A(j, i')$≠0

2. 若 i'=0 且 i≠0，则 $det(A') = A(j, j') - A(i, j') \neq 0$
3. 若 i'≠0,i≠i',i≠j',j≠i',j≠j', 则 det(A')=$\frac{1}{i-i'}\frac{1}{j-j'} - \frac{1}{i-j'}\frac{1}{j-i'}$，所以 det(A')=0⇔ $ii' + jj' = ij' + i'j \Leftrightarrow (i-j)(i'-j') = 0 \Leftrightarrow i = j$ 或 $i' = j'$ 由于假设 $i < j$ 且 $i' < j'$,$det(A') \neq 0$。

- 然后证明 A 可逆，可以通过构造辅助矩阵来证明，步骤如下
  1. 构造辅助矩阵 B 为 $\mathcal{F}_p$ 上的 $p \times p$ 矩阵，B(s,t) 为 B 的第 s 行第 t 列元素.$B(s,s) = 0, s = 0, 1, ..., p-1$ 且 $B(s,t) = (s-t)^{-1}, s = 0, 1, ..., p-1, t = 0, 1, ..., p-1, s \neq t$ 由于 B 的每行每列都包含 $\mathcal{F}_p$ 中每个元素恰好一次，故 $rank(B) \leqslant p-1$
  2. 因为 A 的后 p-1 列包含 $\mathcal{F}_p$ 中每个元素恰好一次，所以 A 可通过行变化消成分块对角阵，A 可逆当且仅当 A 的右下方 $(p-1)\times(p-1)$ 子矩阵 A_1(和 B 的右下方 $(p-1)\times(p-1)$ 子矩阵 B_1 相同) 可逆。因此结合上一步，由于 B 的第一行可以通过行高斯消元消为全 0 向量，故只需证明 rank(B)=p-1。
  3. 为了证明 $rank(B) = p-1$, 考虑 B 作为生成矩阵的循环码 (cyclic code)。则 $rank(B)$ =B 作为生成矩阵的循环码的维数。与上一条结论同理，由于 B 的构造显然 B 是循环码的生成矩阵, 考虑 B 的生成多项式 $f(x) = 0 - x - \frac{1}{2}x^2 - \cdots - \frac{1}{p-1}x^{p-1}$。$f(1) = 0, f'(1) \neq 0$。又因为在 $\mathcal{F}_p$ 上，$x^p - 1 = (x-1)^p$，故 $gcd(f(x), x^p - 1) = (x-1)$,degree 为 1, 故 B 的维数是 p-1.

□

最后 q 为素数幂且 q-1 为 Messen 素数时，有特殊的构造性结果

定理 4.12　若 $q = 2^n$ 且 $q-1$ 为素数, 则 $M(2,q) \geqslant q-1$

证明　设 $\alpha \in \mathcal{F}_q$ 是基本元，$M = (m_{r,c})$ 是 $s \times s$ 的 Vandermonde 矩阵，$m_{r,c} = \alpha^{rc}, 0 \leqslant r, c \leqslant s-1$. 则

$$det(M) = \prod_{0 \leqslant i < j \leqslant s-1} (\alpha^j - \alpha^i) \neq 0$$

故 M 可逆。只需证明 M 的任意 2×2 子矩阵都可逆。考虑由 M 的第 i 行,j 行,i' 列,j' 列构成的 2×2 子矩阵，其中 $i \neq j, i' \neq j'$ 则

$$det(M') = \alpha^{ii'+jj'} - \alpha^{ij'+ji'}$$

故 $det(M') = 0 \Leftrightarrow \alpha^{ii'+jj'} = \alpha^{ij'+ji'}$

$$\Leftrightarrow ii' + jj' \equiv ij' + ji' \mod (q-1)$$

$$\Leftrightarrow (i-j)(i'-j') \equiv 0 \mod (q-1)$$

由于 $q-1$ 是素数，故上式

$$\Leftrightarrow i = j \ and \ i' = j'$$

与假设 $i \neq j, i' \neq j'$ 矛盾。 □

三、特殊 q 的构造: 穷举

在之前的不存在性证明中，我们得到了 $M(2,q) \leqslant q$ 的上界 q，但是 q 为素数幂且非素数时，(2,q,q) 线性 AONT 的存在性没有确定。这对于改善上界至关重要:

1. 如果 (2,q,q) 线性 AONT 不存在，则上界可以由 q 改善为 q-1。
2. 如果 (2,q,q) 线性 AONT 存在，则下界可以由 $\phi(q)$ 改善为 q，进一步由于 M(2,q) 上界为 q，便可以完全确定 M(2,q)=q。

论文[4] 中便通过穷举计算了 (2,q,q)，q⩽11 时线性 AONT。

由于 $\mathcal{F}_q$ 上的 s 阶矩阵是一个非常大的空间，当 s 增大时它更是增长得非常快。所以为了提高穷举算法的有效性，有两个方向的研究。一个是对矩阵进行简化和分类，以**减小搜索空间**。另一个是设计低时间复杂度的**穷举算法**。将研究结果整理如下:

1. **简化矩阵和缩小搜索空间**

   为了对所有 2 阶子矩阵均可逆的特殊矩阵进行简化，它们被证明可以通过初等变换约化为 μ standard form

   定理 4.13 设 M 是表示线性 (2,s,q)-AONT 的矩阵。则 M 每行每列至多 1 个 0。通过行列置换和数乘，可以将 M 化为形如 $\begin{pmatrix} 0 & 1 & 1 & \cdots & 1 \\ 1 & \ddots & & & \\ 1 & & 0 & & \\ \vdots & & & & \\ 1 & & & & \end{pmatrix}$ 的矩阵，其中对角线前 μ 个元素为 0。

   于是只需研究这种 u-standard 矩阵，简单分析该形式的矩阵可以得到 (2,q,q)-AONT 存在的一个必要条件。

引理 4.14　若 M 为线性 (2,q,q)-AONT 的 standard form，则 M 的 type 为 q-1 或 q

证明　如果 M 的 type⩽q-2。则 M 的最后两行均为非零元素，构成 q 个线性无关的向量。但是 q 元域上的线性相关等价类 q+1 个，其中两个等价类必含 0 元素，故至多 q-1 个无 0 元素线性无关的向量，矛盾。 □

继续分析后，进一步可以证明不存在 type 为 q-1 的情况。

定理 4.15　对任意素数幂 $q > 2$, 不存在 type 为 q-1 的 (2,q,q) 线性 AONT。

证明　反证，假设存在 type 为 q-1 的 (2,q,q) 线性 AONT 且它的矩阵表示为 M，则

$$M = \begin{pmatrix} 0 & 1 & 1 & \cdots & 1 & 1 \\ 1 & 0 & m_{2,3} & \cdots & m_{2,q-1} & m_{2,q} \\ 1 & m_{3,2} & 0 & \cdots & m_{3,q-1} & m_{3,q} \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 1 & m_{q-1,2} & m_{q-1,3} & \cdots & 0 & m_{q-1,q} \\ 1 & m_{q,2} & m_{q,3} & \cdot & m_{q,q-1} & m_{q,q} \end{pmatrix}$$

其中 $m_{q,q} \neq 0$。由于 M 的每个 2×2 子矩阵均可逆故 $m_{i,j} \neq 0, \forall i \neq j$。将每列都 $\times m_{q,j}^{-1}$ 则得到

$$M_1 = \begin{pmatrix} 0 & 1/m_{q,2} & 1/m_{q,3} & \cdots & 1/m_{q,q-1} & 1/m_{q,q} \\ 1 & 0 & m_{2,3}/m_{q,3} & \cdots & m_{2,q-1}/m_{q,q-1} & m_{2,q}/m_{q,q} \\ 1 & m_{3,2}/m_{q,2} & 0 & \cdots & m_{3,q-1}/m_{q,q-1} & m_{3,q}/m_{q,q} \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 1 & m_{q-1,2}/m_{q,2} & m_{q-1,3}/m_{q,3} & \cdots & 0 & m_{q-1,q}/m_{q,q} \\ 1 & 1 & 1 & \cdots & 1 & 1 \end{pmatrix}$$

由于所有 2×2 子矩阵可逆，故每行的 q 个元素互不相同，而 $q > 2$ 时 $\mathcal{F}_q$ 上所有元素和为 0(模 q 下)。故 M_1 的各列之和为 0 向量 (模 q 下)。故 M_1 不可逆。故 M 不可逆，矛盾。 □

于是得到

推论 4.16　若 M 为线性 (2,q,q)-AONT 的 standard form，则 M 的 type 为 q

通过行列变换，我们可以进一步简化 type 为 q 的 (2,q,q) 线性 AONT 的表示矩阵 M，将其简化为如下定义的 reduced form

定理 4.17 设矩阵 M 是 type 为 q 的 (2,q,q)-AONT 的 standard form，则它可以通过初等变换约化为如下定义的 reduced form

- 对角线元素全为 0
- 第一行，第一列元素除首个元素外全为 1
- 第二行元素按照第 3、4、...、q 列递增

约化为 reduced form 后，我们便可以将它作为我们的搜索空间。

2. **具体穷举算法的设计**

已经确定搜索空间是 reduced form 的情况下，我们可以通过再将 reduced form 按以下形式分为等价类，以降低搜索次数和复杂度。

定义 4.1 若 M 与 M' 是线性 (t,s,q)AONT 的 reduced form，则我们称 M 与 M' 是等价的，当且仅当以下三条中的一条成立

(a) M 与 M' 可通过行置换和列置换互相得到

(b) M 与 M'可以通过左乘和右乘对角矩阵相互得到

(c) $M^T = M'$

引理 4.18 可以通过下面的步骤得到一个 reduced form M 的所有等价 reduced form

(a) 任取 M 的 2 行 r_1, r_2，交换 M 的第 1 行和第 r_1 行，第 2 行和第 r_2 行。然后交换新矩阵的第 1 列和第 r_1 列，第 2 列和第 r_2 列。

(b) 将新矩阵的第 2,...,q 列各乘常数使得第一行变为 (011...1)

(c) 将新矩阵的第 2,...,q 行各乘常数使得第一列变为 $(011...1)^T$

(d) 作第 3 到 q 列的置换，使得 M 的第二行的第 3 到 q 个元素增序排列，记该置换为 π

(e) 将置换 π 同样作用到行上

(f) 将 M 转置然后重复操作 1 到 5

于是，我们的算法如下

3. **穷举的计算结果**

对于 q<11 ,[4] 和[5] 穷举了所有 reduce form，并将它划分为初等变换下的等价类，将结果整理如表格4.3。

下面将部分穷举得到的例子罗列如下：

例 4.1 一个定义在 $\mathcal{F}_4 = \mathbb{Z}_2[x]/(x^2 + x + 1)$ 上的线性 (2,4,4)-AONT：

算法 4.1 Search algorithm for (2,q,q) reduced form

输入:

prime power q;

输出:

$S := \{M \in M_q(\mathcal{F}_q)\ which\ is\ a\ AONT\ reduced\ form\}$;

$W := \{N(A) : A \in S, N(A) \in$

$N^+\ which\ are\ number\ of\ equivalent\ classes\ of\ A\}$;

List and check the search space $\mathcal{X}$ for all reduced forms;
There are $\binom{q-1}{q-2}$ possibilities for second role;
There are $(q-1)!$ possibilities for 3^{rd} to last row.;
However due to uniqueness of elements in $\{m_{i2}, ..., m_{i,q}\}$,i=2,...,q and uniqueness of elements in $\{m_{2j}, ..., m_{qj}\}$,j=2,...,q, the checking space is significantly smaller.;
repeat
    Pick one matrix M from $\mathcal{X}$ and then delete it.;
    Get all equivalent reduced form by 引理4.18,record the number N_M;
    $S = S \cap \{M\}$;
    $W = W \cap \{(M, N_M)\}$
until $\mathcal{X} = \varnothing$;

表 4.3 线性 (2,q,q)-AONT 的 Reduced form 和等价类数量的穷举结果，q⩽ 11 素数幂

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

$$\begin{pmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & x \\ 1 & x & 0 & x+1 \\ 1 & 1 & x & 0 \end{pmatrix}$$

例 4.2 一个定义在 $\mathcal{F}_9 = \mathbb{Z}_3[x]/(x^2+1)$ 上的线性 (2,8,9)-AONT：

$$\begin{pmatrix} 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 2x & x+1 & x+2 & 2x & \\ 1 & 1 & 0 & 2x+1 & x+1 & x+2 & 2 & x \\ 1 & 2x & x & 0 & x+2 & 2 & 2x+1 & x+1 \\ 1 & x+2 & 2 & x & 0 & 1 & 2x & 2x+1 \\ 1 & x+1 & x+2 & 2x & 2x+1 & 0 & 1 & 2 \\ 1 & x+1 & x+2 & 2x & 2x+1 & 0 & 1 & 2 \\ 1 & x & x+1 & 1 & 2 & 2x+1 & 0 & x+2 \\ 1 & 2 & 2x+1 & x+1 & 1 & 2x & x & 0 \end{pmatrix}$$

第五章 非线性 (t,s,q)-AONT 存在性已有研究结果整理

非线性 AONT 的研究还处于初级阶段，结果不多。此前的理论结果大多将非线性 AONT 与 OA 联系，通过 bush bond 得到一些保证存在的必要性条件。另外也有特殊 q 下的一些结果。总的来说，(t,s,v)AONT 的存在性介于 OA(t,s,v) 与 OA(s,2s,v) 存在性之间，可以视为这两者之间的一种组合结构。

第一节 一般性结果

定义 5.1 (t,s,v) 正交阵列 OA(t,s,v) 本文中，若一个 $v^s \times s$ 的阵列，其中任意 t 列中，任意一个 t 元组都恰好出现 v^{s-t} 次，则称该阵列为一个 (t,s,v) 正交阵列，记作 OA(t,s,v)。

结合非线性 AONT 的**定义**3.3，快速得到以下两个推论

推论 5.1 如果存在 (t,s,v)-AONT, 则至少存在一个 OA(t,s,v)。

推论 5.2 如果存在 $OA(s,2s,v)$，则可构造 (t,s,v)-AONT,$\forall 1 \leqslant t \leqslant s$

由**推论**5.1, 可以由 AONT 的存在性推出 OA 的存在性。故可以利用 OA 存在条件[6] 的 bush bond 来推出 (t,s,v)-AONT 存在的必要条件，下面的结果直接由 **Bush Bond** 推出。

定理 5.3 Bush Bond

1. 如果存在 (2,s,q)AONT，则 s⩽q+1
2. 如果存在 (3,s,q)AONT 且 q>2，则 s⩽ $\begin{cases} q+1 & q \text{ is even} \\ q+2 & q \text{ is odd} \end{cases}$
3. 如果存在 (t,s,q)AONT 且 t⩾q，则 s∈{t,t+1}

第二节 特殊结果

一、理论构造证明

定理 5.4 如果存在 OA(2,4,v)，则存在一个 (2,3,v)AONT

证明 设 A 是 $\mathbb{Z}_v$ 上的一个正交阵列 $OA(2,4,v)$，它一共 v_2 行，每行由 $C_{i,j}, i, j \in \mathbb{Z}_v$ 来标定。不失一般性，我们可以假设 $C_{i,j} = (i, j, L_1(i, j), L_2(i, j))$。

对 $i, j \in \mathbb{Z}_v$，可以构造这样的 v^3 个行向量

$$H_{i,j,x} = (L_1(i,j), L_2(i,j), x, j+x, L_1(i,x), L_2(i,x)$$

.

设 H 是这样的 v^3 个行向量构成的 $(v^3, 6, v)$ 阵列，则

Claim:H 是一个 $(2,3,v)$AONT。

Proof: 由**引理**3.3，只需验证其中的三个条件。

1. **引理**3.3中的前两个条件由于 OA 定义显然成立。
2. 假设从前 3 列中选择两列 c_1 列和 c_2 列，从后三列中选择一列 c_3 列。则只需构造一个从上面选择的 3 列构成的行向量到所有 $\mathbb{Z}_v$ 上三元组的双射。由于构造的对称性，不失一般性，我们可以假设 $c_1 = 1, c_2 = 2, c_3 = 4$。对任意 $\mathbb{Z}_v$ 上的三元组 $(a,b,c) \in \mathbb{Z}_v^3$，设 $L_1(i,j) = a, L_2(i,j) = b$ 且 $j + c$。则由 OA 的定义，由前两个等式我们可以唯一确定 i, j，由确定的 (i,j) 和最后一个等式可进一步确定 x，证毕。

□

关于 OA(2,4,n) 的存在性结果在[6] 中有这样的结果。

引理 5.5　当且仅当 $n \neq 2, 6$ 时，存在一个 OA(2,4,n)。

所以结合上面的**定理**5.4和**引理**5.5，可以得到关于 (2,3,n)AONT 和 (1,3,n)AONT 的存在性的一个推论：

推论 5.6　对正整数 $n \neq 2, 6$，存在 (2,3,n)-AONT 和 (1,3,n)-AONT。

二、计算穷举结果

采用最基本的 unbiased array 来刻画 AONT，于是可以通过简单的穷举得到一些结果。以 q=2 为例。

首先，穷举找到所有的（行变换同构意义下）OA(2,3,2) 为 $\begin{bmatrix} 0 & 0 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{bmatrix}$ 和 $\begin{bmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \\ 1 & 1 & 1 \end{bmatrix}$，它们刚好构成了 $\mathcal{F}_2^3$ 上 8 个向量的一个划分。

将输出，即阵列的后 3 列按照二进制大小排序得

$$\left[\begin{array}{c|ccc} & 0 & 0 & 0 \\ A & 0 & 0 & 1 \\ & 0 & 1 & 0 \\ & 0 & 1 & 1 \\ \hline & 1 & 0 & 0 \\ B & 1 & 0 & 1 \\ & 1 & 1 & 0 \\ & 1 & 1 & 1 \end{array}\right]$$

其中 A,B 为上述两个 OA(2,3,2) 的行重排。因此，考虑 A,B 的 OA(2,3,2) 选择和 A，B 的行重排，只需穷举 $2\cdot 4!\cdot 4!$ 种可能。穷举后得到的结果是，不存在这样的 unbiased 阵列。

因此得到

定理 5.7　(2,3,2) 非线性 AONT 不存在。

注　同理还可以穷举其他的 (2,p+1,p) 非线性 AONT 观察是否存在，这是很有意义的问题，因为线性的 (2,p+1,p)-AONT 不存在。

第六章 开放性问题提出

对于任意的 t 和 q，显然 AONT 还有很大的研究空间，关于它的存在性结果，从现有的结果也可以做出一些相应的猜想。在这里我们列出一些猜想，以及还有待解决的问题。

1. 非线性的 (2,q+1,q)-AONT 是否存在?
2. 由之前的穷举结果可以观察到，存在 (2,4,4) 线性 AONT，但是不存在 (2,8,8) 和 (2,9,9) 线性 AONT。于是自然猜测：$q>4$ 且 q 为素数幂（非素数）时，是否不存在 (2,q,q) 线性 AONT?
3. 非线性 AONT 的穷举算法的研究
4. 非线性 AONT 的归纳性质的研究，类似线性 AONT 中 (t,s,q)-AONT 的存在性 $\Leftarrow$(t,s-1,q)-AONT 的存在性
5. 对于其他 t，例如 t=3 的 AONT 的研究（目前只有 Cauchy Matrix 的充分性条件和 Bush bond 的必要性条件）

参 考 文 献

[1] Stinson N N E D R. Computational results on invertible matrices with the maximum number of invertible 2× 2 submatrices. *Australasian Journal of Combinatorics*, 2017, 69(1):130-144.

[2] D'Arco P, Esfahani N N, Stinson D R. All or nothing at all. 2015.

[3] Stinson D R. Something about all or nothing (transforms). *Designs, Codes and Cryptography*, 2001, 22(2):133-138.

[4] Esfahani N N, Goldberg I, Stinson D R. Some results on the existence of t -all-or-nothing transforms over arbitrary alphabets. *IEEE Transactions on Information Theory*, 2018, 64(4):3136-3143. DOI: 10.1109/TIT.2017.2780233.

[5] Wang X, Cui J, Ji L. Linear (2, p, p)-aonts do exist. 2018.

[6] Bose R C, Shrikhande S S, Parker E T. Further results on the construction of mutually orthogonal latin squares and the falsity of euler's conjecture. *Canadian Journal of Mathematics*, 1960, 12:189-203.