Note 2: 结果整理

2019 年 10 月 11 日

1 问题介绍

1.1 线性 AONT

线性 AONT 可以由**矩阵**表示，可以通过**矩阵性质**刻画

Theorem 1.1. *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。*

q 固定时，关于不同 s 的线性 AONT 存在性结果，有一定**归纳关系**。

Lemma 1.2. *(t,s,q) 线性 AONT 存在，则 (t,s-1,q) 线性 AONT 存在*

Proof: 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。

若定义 S(t,q) 是使线性 AONT 存在的 s，则由这一归纳关系，可以直接推出，S(t,q) 有上界 M(t,q)，且对于 $\forall s\ s.t.\ t \le s \le M(t,q)$，(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。

1.2 一般的 AONT

一般的 AONT 可以由**阵列**来表示，可以通过**阵列性质**刻画

Theorem 1.3. *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}*
- $\mathcal{X}\cup\mathcal{Y}, \mathcal{X}\in\{1,2,...,s\}, \mathcal{Y}\in\{s+1,s+2,...,2s\}$ *and* $|\mathcal{X}|=t, |\mathcal{Y}|=s-t$

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

一般的 AONT 也有一些**归纳关系**

Lemma 1.4. ***Product Construction***

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

Proof: 考虑 $\mathcal{Z}_m \times \mathcal{Z}_n$

对于一般 AONT 的研究在于**构造**，即能否构造出线性结果构造不出的 AONT。

2 此前的线性结果

正如之前所说，线性结果主要是对 M(t,q) 的研究，之前的结果有对任意 t 和 q 均成立的一般性结果，也有特殊 t 和 q 情况下通过穷举等方式找到的结果。简要总结如下

2.1 强 AONT（利用 Cauchy Matrix）

在论文All or Nothing at All, Paolo D'Arco et al.中，他们研究了在 $\mathcal{F}_q$ 上的线性 AONT。结果简要叙述如下。

首先定义 q 元域上的 s 阶 Cauchy 矩阵。

Definition 2.1. *An s by s* ***Cauchy matrix*** *can be defined over* $\mathcal{F}_q$ *if* $q \geq 2s$*, Let* $a_1,a_2,\cdots,a_s$ *and* $b_1,b_2,\cdots,b_s$ *be distinct elements of* $\mathcal{F}_q$*. Let* $c_{ij} = 1/(a_i - b_j)$*,for* $1 \leq i \leq s, 1 \leq j \leq s$*. Then* $C = (c_{ij})$ *is the Cauchy matrix defined by the sequence* $a_1, a_2, \cdots, a_s, b_1, b_2, \cdots, b_s$*.*

然后证明 *Cauchy* 矩阵的一个重要性质

Lemma 2.2. ***Any square submatrix of Cauchy Matrix is invertible over*** $\mathcal{F}_q$

Proof:

由于 Cauchy 矩阵的任意阶子方阵依然是 Cauchy 矩阵，故只需证明 n 阶 Cauchy 矩阵是可逆的，$\forall n$。

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

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

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

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

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

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

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

由此，可以得到 M(t,q) 的一个下界

Result 2.3. *q 为任意素数幂时，M(t,q)≥ ⌊q/2⌋*

2.2 (2,s,q) 线性 AONT

此前的论文中，分析了 M(2,q) 与 q 的关系，即需要研究具备所有 2 阶子矩阵均可逆的特殊矩阵。在论文Some results on the existence of t-all-or-nothing transforms over arbitrary alphabets, D.R.Stinson et al.中，为了对这种矩阵进行了简化，作者定义了一种 μ standard form

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

Definition 2.4. 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。

首先，关于 M(2,q) 的**上界**，有以下结果

2.2.1 上界结果

要得到上界主要是通过证明的方法，证明某个 s 下不存在 (2,s,q)AONT。下面是一个对所有素数幂 q 均成立的结果。

Result 2.5. ***There is no linear (2,q+1,q)-AONT for prime power q. Therefore, M(2,q)≤q***

Proof:

1. 若 *q=2*，则 *(2,3,2)* 线性 *AONT* 不存在
2. 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 $\sum_{x\in\mathcal{F}_q} x = 0$

2.2.2 下界结果

而关于 M(2,q) 的**下界**，也有以下结果，主要通过**构造**出某个 s 下具体的 (2,s,q)AONT 来证明下界 ≥s。

Result 2.6. ***M(2,p)≥ p for p prime***

在论文*Linear (2, p, p)-AONTs do Exist, Xin Wang et al.*中给出了构造性证明。

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*。

Proof:

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

- 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 $det(A')=-A(i,j')A(j,i')\neq 0$
  2. 若 $i'=0$ 且 $i\neq 0$，则 $det(A')=A(j,j')-A(i,j')\neq 0$
  3. 若 $i'\neq 0, i\neq i', i\neq j', j\neq i', j\neq j'$, 则 $det(A')=\frac{1}{i-i'}\frac{1}{j-j'}-\frac{1}{i-j'}\frac{1}{j-i'}$，所以 $det(A')=0\Leftrightarrow ii'+jj'=ij'+i'j\Leftrightarrow (i-j)(i'-j')=0\Leftrightarrow i=j$ 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 $rank(B)\leq p-1$
  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。长度为 n 的 $\mathcal{F}_q$ 上的线性码 $\mathcal{C}$ 称为循环码，如果 $\forall$ 向量 $\boldsymbol{c}=(c_0,c_1,\cdots,c_{n-1})\in\mathcal{C}$, 将它做一次循环移位得到的向量 $(c_{n-1},c_0,\cdots,c_{n-2})$ 也属于 $\mathcal{C}$. 在研究 $\mathcal{F}_q$ 上的循环码时，作码文 $\boldsymbol{c}=(c_0,c_1,\cdots,c_{n-1})$ 到最高次不超过 *n-1* 的 $\mathcal{F}_q[x]$ 多项式 $c(x)=c_0+c_1x+\cdots+c_{n-1}x^{n-1}$ 的一一映射。故由 $\boldsymbol{c}$ 生成的循环码 $\mathcal{C}$ 可以视为 $\mathcal{F}_q/(x^n-1)$ 的理想，且它的生成元是 $gcd(c(x),x^n-1)$,$\mathcal{C}$ 的维数为 $n-deg(gcd(c(x),x^n-1))$
  4. 下面证明 $rank(B)=p-1$, 由于 B 的构造显然 B 是循环码的生成矩阵,$f(x)=0-x-\frac{1}{2}x^2-\cdots-\frac{1}{p-1}x^{p-1}$。$f(1)=0, f'(1)\neq 0$。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*.

Result 2.7. ***M(2,q)≥q-1 for q=*2^n 且 *q-1* 为素数**

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

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

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

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

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

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。

Result 2.8. ***M(2,q)***$\geq \phi(q)$ ***for q prime power*** 设 $q=p^r$ 是素数幂，α 是 $\mathcal{F}_q$ 上一个原根。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。

- **构造**: $P(s,s)=0, s=0,1,...,q-2; P(s,t)=\frac{\alpha^s}{\alpha^s-\alpha^t}, s=0,1,...,q-2, t=0,1,...,q-2, s\neq t.$

- 下面证明 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。

- 下面用与构造 $(2,p,p)$ 线性 $AONT$ 时同样的循环码方法，证明 $rank(P)=\Phi(q)$

  1. 观察到矩阵 P 是循环的，生成多项式为 $f(x)=0+\frac{1}{1-\alpha}x+\frac{1}{1-\alpha^2}x^2+...+\frac{1}{1-\alpha^{q-2}x^{q-2}}$，由于 $x^{q-1}-1=(x-1)(x-\alpha)...(x-\alpha^{q-2})$。$\Phi(q)=p^{r-1}(p-1)=p^r-p^{r-1}$, 故只需证明 $deg(gcd(x^{q-1}-1, f(x)))=p^{r-1}-1$，即只需证明 $f(x)$ 在 $\mathcal{F}_q$ 上有 $p^{r-1}-1$ 个不同的根。
  2. ***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 $x=\alpha^{kp}, 1\leq k\leq p^{r-1}-1$, 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:

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

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

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

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

3 M(t,q) 的上界和下界的改善

3.1 M(2,q) 的改善

对 M(2,q) **上界**的改善和**下界**的改善空间，主要存在于 q 为素数幂且非素数时。研究的主题转为 (2,q,q) 线性 AONT 是否存在。如果不存在，则上界可以由 q 改善为 q-1。如果存在，则下界可以由 $\phi(q)$ 改善为 q，进一步由于 **Result 2.5**上界为 q，可以完全确定 M(2,q)=q。

在论文Some results on the existence of t-all-or-nothing transforms over arbitrary alphabets, D.R.Stinson et al.中，有引理描述了了 (2,q,q)-AONT 的一个必要条件如下

Lemma 3.1. 若 ***M*** 为线性 ***(2,q,q)-AONT*** 的 ***standard form***，则 ***M*** 的 ***type*** 为 ***q-1*** 或 ***q***

Proof: 如果 M 的 $type \le q\text{-}2$。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 $q\text{-}1$ 个无 0 元素线性无关的向量，矛盾。

在论文Linear (2, p, p)-AONTs do Exist, Xin Wang et al.中，作者研究了 type 为 q-1 的情形，并证明了这种情形对于素数幂不存在

Result 3.2. 对任意素数幂，不存在 ***type*** 为 ***q-1*** 的 ***(2,q,q)*** 线性 ***AONT***。

Proof: 反证，假设存在 $type$ 为 $q\text{-}1$ 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

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

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。故行元素之和为 0(模 q 下)。故 M_1 不可逆。故 M 不可逆，矛盾。

于是得到

Corollary 3.3. 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，得到如下定义的 reduced form

Definition 3.4. 满足 *(2,q,q)-AONT* 的矩阵 *M* 若满足如下条件，则称其为 *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

简化到这种程度后，论文Some results on the existence of t-all-or-nothing transforms over arbitrary alphabets, D.R.Stinson et al.中便通过穷举计算了 (2,q,q)，q≤11 时线性 AONT 的个数，将其穷举算法和结果列举如下。

***Algorithm* 3.5. 穷举算法**

-

Result 3.6. 计算结果

对于 *q<11*，作者没有通过穷举找到任何 *type* 为 *q-1* 的 *(2,q,q)-AONT*，这也是 ***Result 3.2***的一个验证。穷举了所有 *reduce form* 并找到了等价类后，将结果整理如表格*1*。

可以观察到，q=8 和 9 时，均不存在 (2,q,q)-AONT。于是

Claim: 不存在 (2,q,q) 线性 AONT，若 q>4 且 q 为素数幂（非素数）

在这一节试图对 M(2,q) 的下界进行改善

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

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

表 1: Number of Reduced and Indquivalent linear (2,q,q)-AONT,for prime powers q≤ 11

4 此前的非线性结果

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。

Definition 4.1. ***(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)*。

由 AONT 的定义，快速得到以下引理

Lemma 4.2. *若存在 OA(s,2s,v), 则可构造 (t,s,v)-AONT,*$\forall 1 \leq t \leq s$

Proof:

Lemma 4.3. *若存在一个 (t,s,v)-AONT，则存在一个 OA(t,s,v)*

Proof:

由 Lemma 4.3, 可以通过 OA 存在条件的 bush bond 来推出 (t,s,v)-AONT 存在的必要条件

Result 4.4. ***result from bush bound***

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

集中在 (2,s,q) 的层面，由于线性 AONT 的存在性要求 $s \leq q$ 则自然提出问题是否可以构造非线性的 (2,q+1,q)-AONT，这个问题在 section 5 中进行研究

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

5 非线性 (2,q+1,q)-AONT 的存在性

5.1 q≤ 11 时的穷举结果

采用最基本的 unbiased array 来刻画 AONT

1. q=2

   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 (2,3,2) 非线性 AONT 不存在。

2. q=3

   与上面同理，找到所有的（行变换同构意义下）OA(2,4,3)

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