國 立 交 通 大 學

應用數學系
數學建模與科學計算碩士班

碩 士 論 文

運用程式論證特定群試設計之存在性

The Existence of Certain Pooling Designs by Programming

研 究 生：劉家安
指導老師：翁志文 教授

中 華 民 國 九 十 九 年 六 月

運用程式論證特定群試設計之存在性

The Existence of Certain Pooling Designs by Programming

研　究　生：劉家安　　　　Student：Chia-An Liu

指導教授：翁志文　　　　Advisor：Chih-Wen Weng

國　立　交　通　大　學

應用數學系數學建模與科學計算碩士班

碩　士　論　文

A Thesis

Submitted to Department of Applied Mathematics College of Science,

Institute of Mathematical Modeling and Scientific Computing

National Chiao Tung University

in Partial Fulfillment of the Requirements

for the Degree of

Master

In

Applied Mathematics

June 2010

Hsinchu, Taiwan, Republic of China

中　華　民　國　九　十　九　年　六　月

運用程式論證特定群試設計之存在性

學生：劉家安　　　　　　　　　　　　　指導老師：翁志文 教授

國立交通大學應用數學系數學建模與科學計算碩士班

摘　要

本文先介紹一種特定群試設計方法，討論此設計方法所具有的性質，並提出三個程式，來論證此種設計方法可應用的情況。程式內容包括論證此設計方法的存在性、原根(primitive root)的列表、以及找尋此設計方法存在的最佳情況。

The Existence of Certain Pooling Designs by Programming

Student: Chia-An Liu Advisor: Chih-Wen Weng

Institute of Mathematical Modeling and Scientific Computing

National Chiao Tung University

Abstract

This thesis introduces a certain pooling design first, including the properties it has. Then proposes three programs to identify the existence of this pooling design, list the primitive roots, and optimize the conditions of this pooling design.

誌　謝

感謝我的指導教授翁志文老師。老師面對問題的嚴謹態度，不論在學術研究，或是待人處事的方面，都使我獲益良多。也感謝系上給我如此優良的學習環境，交大予我自由寬廣的學術風氣。他日若有所成，我必定飲水思源。

感謝黃喻培學長和吳欣融學長。若不是你們的承先，也不會有這篇論文的啟後。感謝應數同學們。(女士優先)玉雯、士軒、葉彬、逸軒、以及育生，不管是學習上的磨練切磋，或是生活中的守望相助，你們是最好的依靠。也感謝建模所的學弟妹們。(照座號排)芳竹、啟豪、明虔、淑娟、訓利、玠旼、玉峰、以及芷萱，你們或許不知道幫過我什麼，但我想說，隨心所欲，行善於舉手投足間，才正是幫助之最高境界。

最後感謝父母親長久以來的細心栽培，哥哥的關懷打氣。日常生活中，給我無微不至的照料；求學過程中，給我盡其所能的支持，讓我毫無後顧之憂。也感謝我的女朋友佳玲，是未婚妻了，總能體諒我忙碌的研究生活，同時給我關心與鼓勵。感謝所有在期間幫助過我的人，僅以此論文的呈獻，表達我最誠摯的感激。

家安　謹誌

2010 年 6 月　於新竹交大

Contents

1 Introduction ……………………………………………………………………………..1

2 Our Construction ………………………………………………………………………..1

3 Testing program of our construction ……………………………………………………6

4 Generators of each prime less than 100 …………………………………………………...7

5 The minimal elements set $\mathbb{Z}_m \times F_q$ based on our construction …………………………..11

6 Conclusions and future works ………………………………………………………….14

References ……………………………………………………………………………………14

1. Introduction

A binary matrix M is called *d-disjunct* if any column of M is not covered by the boolean sum of d other columns. We construct $t \times n$ d-disjunct matrices for $(t, n) = ((d+1)m, (d+1)m+1)$, where d is a prime power, $m = 2d-4$, $m = 2d-3$, or $m \geq 2d-1$ [1]. The details of this construction are introduced in the chapter 2.

We proposed an algorithm in each chapter 3 to 5. They have different functions, but the main purpose is the same: to find the existence of the certain pooling designs based on our construction introduced in chapter 2. We also applied some theorems of the Number Theory [2] to certify the correctness of the algorithm. Especially, in chapter 5 we have some new conclusions beyond the thesis [1]. It might be the future work of this research.

2. Our construction

This construction is operated in the sense of finite geometry. Let P be a set of $m \times n$ elements. In this chapter we call an element *point*, and a *n-subset* of P a *line*. Our object is to find a class $\mathcal{B}$ of lines in P such that $|\mathcal{B}| = |P| + 1$, and any two lines in $\mathcal{B}$ have at most one point in common.

Let q be a prime power and $m \geq q$ be an integer. Let $F_q := \{0, a^0, a^1, \cdots, a^{q-2}\}$ denote the finite field of q elements. Let $\mathbb{Z}_m := \{0, 1, \cdots, m-1\}$ be the addition group of integers modulo m. Our construction starts from the elements of $\mathbb{Z}_m \times F_q$ as points. Then we try to properly pick subsets such that any two lines intersect at at most one point. The followings are the foundations of our construction.

Definition 2.1. (Forward Difference Distinct Property)

For $T \subseteq \mathbb{Z}_m \times F_q$, T is said to have the *forward difference distinct property* if the set

$$FD_T := \{(j, y) - (i, x) \mid (i, x), (j, y) \in T \text{ with } i < j\}$$

consists of $\dfrac{|T|(|T|-1)}{2}$ elements.

Lemma 2.2.

Let $T_{m,q} := \{(i, a^i) \mid i \in \mathbb{Z}_m, 0 \leq i \leq q-1\}$. Then $T_{m,q}$ has the *forward difference distinct property* in $\mathbb{Z}_m \times F_q$.

(*pf*)

Given pair $(c,d)\in\mathbb{Z}_m\times F_q$, solve the equation $(c,d)=(j,a^j)-(i,a^i)$, for $0\le i<j\le q-1$. If $c=q-1$, then $i=0$ and $j=q-1$. If $c\ne q-1$, then $a^i=d/(a^c-1)$ and $j=c+i$. In each case the (i,a^i) and (j,a^j) are uniquely determined. It follows that $T_{m,q}$ consists of $\dfrac{|T_{m,q}|(|T_{m,q}|-1)}{2}$ elements. □

We can view $T_{m,q}$ as a line in the plane $\mathbb{Z}_m\times F_q$ as Figure 1 shows.

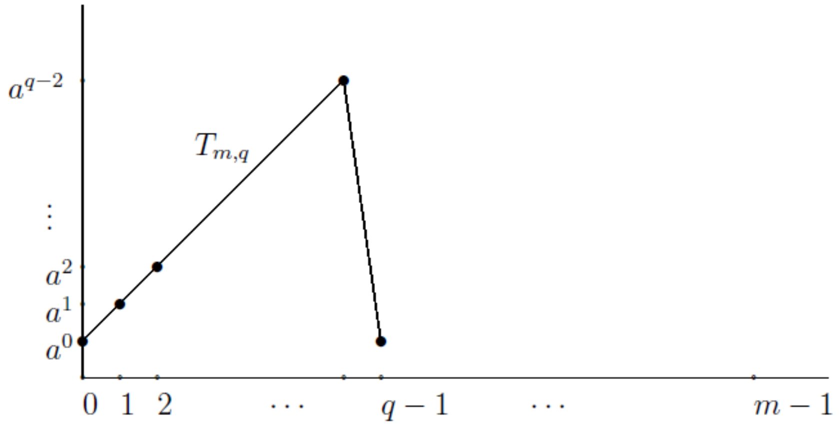

Figure 1: $T_{m,q}$ in $\mathbb{Z}_m\times F_q$

Definition 2.3. (Difference Distinct Property)

For $T\subseteq\mathbb{Z}_m\times F_q$, T is said to have the *difference distinct property* if the set

$$D_T:=\{(j,y)-(i,x)\,|\,(i,x),(j,y)\in T \text{ with } i\ne j\}$$

consists of $|T|(|T|-1)$ elements.

Lemma 2.4.

Let $T_{m,q}:=\{(i,a^i)\,|\,i\in\mathbb{Z}_m, 0\le i\le q-1\}$. If $m\ge 2q-1$, then $T_{m,q}$ has the *difference distinct property* in $\mathbb{Z}_m\times F_q$.

(*pf*)

By Lemma 2.2, we have $|FD_{T_{m,q}}|=|-FD_{T_{m,q}}|=\dfrac{q(q-1)}{2}$. The first coordinate of an element in $FD_{T_{m,q}}$ runs from 1 to $q-1$, and the first coordinate of an element in $-FD_{T_{m,q}}$ runs from

$m+1-q$ to $m-1$. The assumption $m \ge 2q-1$ implies that $FD_{T_{m,q}} \cap (-FD_{T_{m,q}}) = \phi$. □

Lemma 2.5.

The set $T_{m,q}$ has the *difference distinct property* in $\mathbb{Z}_m \times F_q$ for $m = 2q-3$ and $m = 2q-4$.

(*pf*)

By Lemma 2.2, we have $|FD_{T_{m,q}}| = |-FD_{T_{m,q}}| = \dfrac{q(q-1)}{2}$. Given $(c,d) \in FD_{T_{m,q}}$:

(i) If $m = 2q-3$, then $1 \le c \le q-1$ and $q-2 \le -c \le 2q-4$. The repletion of differences can only occur at $c = q-1$ or $c = q-2$. Since $(q-1,0) \in FD_{T_{m,q}}$ and $(q-2,0) \in -FD_{T_{m,q}}$, $(q-2,0) \notin FD_{T_{m,q}}$ and $(q-1,0) \notin -FD_{T_{m,q}}$.

(ii) If $m = 2q-4$, then $1 \le c \le q-1$ and $q-3 \le -c \le 2q-5$. The repletion of differences can only occur at $c = q-1$ or $c = q-2$ or $c = q-3$. Since $(q-1,0) \in FD_{T_{m,q}}$ and $(q-3,0) \in -FD_{T_{m,q}}$, $(q-3,0) \notin FD_{T_{m,q}}$ and $(q-1,0) \notin -FD_{T_{m,q}}$. Now focus on case $c = q-2$. The only two elements of $FD_{T_{m,q}}$ with the first coordinate $q-2$ is $(q-2, a^{q-2}-2)$ and $(q-2, a^{q-1}-a)$, where a is a generator for F_q^*. If $a^{q-2}-2 = a^{q-1}-a$, then $a = -1$, which is a contradiction. □

Lemma 2.6.

Suppose that $T_{m,q}$ has the *difference distinct property*, and $B' = \{u + T_{m,q} \mid u \in \mathbb{Z}_m \times F_q\}$. Then $|L_1 \cap L_2| \le 1$, for $\forall L_1, L_2 \in B', L_1 \ne L_2$.

(*pf*)

Suppose not. Then $\exists L_1, L_2 \in B', L_1 \ne L_2$ such that $|L_1 \cap L_2| \ge 2$. Suppose $L_1 = (u_1,v_1) + T_{m,q}$, $L_2 = (u_2,v_2) + T_{m,q}$ and $p_1, p_2 \in L_1 \cap L_2, p_1 \ne p_2$. Let $p_1 = (u_1,v_1) + (c_1,d_1) = (u_2,v_2) + (c_2,d_2)$, $p_2 = (u_1,v_1) + (c_3,d_3) = (u_2,v_2) + (c_4,d_4)$. Then $(u_1,v_1) - (u_2,v_2) = (c_1,d_1) - (c_2,d_2) = (c_3,d_3)$ $-(c_4,d_4)$, and it is true only when $(c_1,d_1) = (c_3,d_3)$ and $(c_2,d_2) = (c_4,d_4)$. Hence $p_1 = p_2$, which is a contradiction. □

Note that there are *mq* lines and *mq* points in $\mathbb{Z}_m \times F_q$, and a line has $q = |T_{m,q}|$ points with *q* different first coordinates. This is the frame of our work. Now, add more points and lines in B'. Since $(0,x) \notin -FD_{T_{m,q}} \bigcup FD_{T_{m,q}}$, $L \bigcap ((0,x)+L) = \phi$ for any nonzero $x \in F_q$ and $L \in B'$. We add a common point $(i+q,\infty) \in \mathbb{Z}_m \times (F_q \bigcup \{\infty\})$ to each line $L = u + T_{m,q}$ to forms a new set B'' where $i \in \mathbb{Z}_m$ is the first coordinate of u. Note that the points set of B'' becomes $\mathbb{Z}_m \times (F_q \bigcup \{\infty\})$. To show that any two lines in B'' also intersect at at most one point, we prove the following Lemma 2.7 first.

Lemma 2.7.

Suppose that $T_{m,q} \subseteq \mathbb{Z}_m \times F_q$ has the *difference distinct property* in $\mathbb{Z}_m \times F_q$. Let $L_1 = (c,d_1) + T_{m,q}$, $L_2 = (c,d_2) + T_{m,q}$ be two distinct lines in B'. Then $L_1 \bigcap L_2 = \phi$.

(*pf*)
Suppose $(e,f) \in L_1 \bigcap L_2$, then $(e,f) = (c,d_1) + (x_1,y_1) = (c,d_2) + (x_2,y_2)$ for some $(x_1,y_1),(x_2,y_2) \in T_{m,q}$. Thus $e - c = x_1 = x_2$. Since each element in $T_{m,q}$ has distinct first coordinate, we can conclude that $(c,d_1) = (c,d_2)$ and hence $L_1 = L_2$. It is a contradiction. □

Lemma 2.8.

Any two distinct lines in B'' intersect at at most one point.

(*pf*)
It is easy to see that B'' contains exactly one point of the form (c,∞). Let L_1, L_2 be two distinct lines in B'' containing (c_1,∞), (c_2,∞), respectively. If $c_1 \neq c_2$, $L_1 \setminus (c_1,\infty)$ and $L_2 \setminus (c_2,\infty)$ are two distinct lines in B'' and have at most one point in common by Lemma 2.6. If $c_1 = c_2$, the set of the first coordinates of $L_1 \setminus (c_1,\infty)$ and $L_2 \setminus (c_2,\infty)$ must be the same. Thus $L_1 \setminus (c_1,\infty) = (e,f_1) + T_{m,q}$ and $L_2 \setminus (c_2,\infty) = (e,f_2) + T_{m,q}$ for some $e \in \mathbb{Z}_m$, $f_1, f_2 \in F_q$. By Lemma 2.7, $L_1 \setminus (c_1,\infty) \bigcap L_2 \setminus (c_2,\infty) = \phi$, so L_1, L_2 only intersect at (c_1,∞).□

Let $V_i = \{(i,j) \mid j \in F_q \bigcup \{\infty\}\}$ for $0 \le i \le m-1$, and V_i is called the *i-th vertical line*. Let $H = \{(i,\infty) \mid 0 \le i \le q\}$, and H is called the *infinite line*. We add these to B'' and complete our construction.

Lemma 2.9.

Set $B := B'' \bigcup \{H, V_0, V_1, \cdots, V_{m-1}\}$ as the set of lines with underground point set $\mathbb{Z}_m \times (F_q \bigcup \{\infty\})$. Then any two lines in B intersect at at most one point.

(*pf*)

It is easily seen that $V_i \bigcap V_j = \phi$ for $i \neq j$, and $V_i \bigcap H = (i, \infty)$ .It remains to show that $|L \bigcap V_i| \leq 1$ and $|L \bigcap H| \leq 1$ for any $L \in B''$, $1 \leq i \leq m-1$. Since each point in L has distinct first coordinate and contains only one point of the type (c, ∞), the result follows. □

Note that $|\mathbb{Z}_m \times (F_q \bigcup \{\infty\})| = m(q+1)$ and $|B| = m(q+1)+1$, which is our final result.

Theorem 2.10.

Suppose that $T_{m,q} \subseteq \mathbb{Z}_m \times F_q$ has the *difference distinct property*. Let *M* be the incidence matrix of $\mathbb{Z}_m \times (F_q \bigcup \{\infty\})$ and B. Then *M* is a nontrivial *q*-disjunct matrix with $m(q+1)$ rows and constant column weight $(q+1)$.

(*pf*)

Applying Lemma 2.4 and Lemma 2.5 to Theorem 2.10. Corollary 3.11 also follows. □

Corollary 2.11.

Let *M* be the incidence matrix of $\mathbb{Z}_m \times (F_q \bigcup \{\infty\})$ and B where $m = 2q-4$, $2q-3$, or $m \geq 2q-1$. Then *M* is a nontrivial *q*-disjunct matrix with $m(q+1)$ rows and constant column weight $(q+1)$.

Example 2.12. (A construction of 36×37 5-disjunct matrix**)**

Take $q = 5$, $m = 6 = 2q-4$, and $a = 2$ is a generator of 5. Then $T_{6,5} = \{(i, a^i) \mid i \in \mathbb{Z}_6, 0 \leq i \leq 4\} = \{(0,1), (1,2), (2,4), (3,3), (4,1)\}$. We write $T_{6,5} = \{01, 12, 24, 33, 41\}$ for simplifying the notation.

(1) Let $L(u) = (u + T_{6,5}) \bigcup (i+5, \infty)$, where i is the first coordinate of u. Then

$L(00)=\{01,12,24,33,41,5\infty\}$, $L(01)=\{02,13,20,34,42,5\infty\}$, $L(10)=\{11,22,34,43,51,0\infty\}$, $L(11)=\{12,23,35,44,52,0\infty\}$, …, $L(54)=\{50,01,13,22,30,4\infty\}$. There are 30 lines.

(2) Let $V_i=\{(i,j)\mid j\in F_q\cup\{\infty\}\}$ for $0\le i\le 5$. V_i is called the *i-th vertical line.*

$V_0=\{00,01,02,04,03,0\infty\}$, $V_1=\{10,11,12,14,13,1\infty\}$, $V_2=\{20,21,22,24,23,2\infty\}$, $V_3=\{30,31,32,34,33,3\infty\}$, $V_4=\{40,41,42,44,43,4\infty\}$, $V_5=\{50,51,52,54,53,5\infty\}$.

There are 6 lines.

(3) Let $H=\{(i,\infty)\mid 0\le i\le q\}$, and H is called the *infinite line*.
$H=\{0\infty,1\infty,2\infty,3\infty,4\infty,5\infty\}$. There is 1 line.

The above (1), (2), and (3) are the 37 lines based on out construction. □

3. Testing program of our construction

An important work after the construction of a type of pooling design is to know what properties it has. Here we provides a way to verify the existence of *difference distinct property*. The existence of this property can make sure the construction in chapter 2 can be applied into the pooling design.

Algorithm 3.1.

Step 1: Input (*q,a,m*), where *q* is a prime power, *a* is a generator of *q*, and *m*>*q* is an integer.

Step 2: Construct the $T_{m,q}$ matrix of order $q\times 2$ by

$$(T_{m,q})_{(i+1)-\text{th row}}=(i,a^i)\in\mathbb{Z}_m\times F_q, i=1,2,\cdots,q-1.$$

Step 3: Construct another "checking matrix" of size $q(q-1)\times 4$. The 4 components of each row is minuend term, subtrahend term, and the results.

Step 4: Check the repetition of each row after the construction of the checking matrix.

Example 3.2.

Input $(q,a,m)=(7,3,12)$, then construct $T_{m,q}$ matrix:

Tmq =

0 1 - term 1

1	3	- term 2
2	2	- term 3
3	6	- term 4
4	4	- term 5
5	5	- term 6
6	1	- term 7

The $T_{m,q}$ matrix is a 7×2 matrix. Now construct the "checking matrix" of size 42×4, in which each row stores the minuend term, subtrahend term, and the results in $\mathbb{Z}_5\times F_7$. Then, check the repetition of the checking matrix. In this example, it will run out the following results:

ans =

1	7	6	0
7	1	6	0

It means the result of term 1 minus term 7 is $(6,0)$, which equals to the result of term 7 minus term 1. Additionally, since there are some results run out, this case $(q,a,m)=(7,3,12)$ cannot have the *difference distinct property* based on our construction. In fact, it is easy to proved that $m=2q-2$ will not have *difference distinct property* based on our construction.

4. Generators of each prime less than 100

In this chapter we propose an algorithm for finding the all generators of each prime less than 100, and then show the results as a table of generator database. Also showing is the relation between the *Euler's phi function* and the number of generators. Two lemmas are proposed to help the program be faster as finding the generators of large prime.

Algorithm 4.1. (See if *a* is a *generator* of prime *p* or not.)
Input prime *p* and generator *a*
Set *temp=1, count=1*;
while *count*$\leq$*p-2*
    temp=temp$\times$*a (mod p)*;
    if *temp=1*
        break the while loop and try next *a=a+1*;
    end

if *count=p-2*

print *a* and try next *a=a+1*;

end

count=count+1;

end

Table 4.2. (The generators of each prime less than 100.)

Prime p	Generators a	$\phi(p-1)$
3	2	1
5	2,3	2
7	3,5	2
11	2,6,7,8	4
13	2,6,7,11	4
17	3,5,6,7,10,11,12,14	8
19	2,3,10,13,14,15	6
23	5,7,10,11,14,15,17,19,20,21	10
29	2,3,8,10,11,14,15,18,19,21,26,27	12
31	3,11,12,13,17,21,22,24	8
37	2,5,13,15,17,18,19,20,22,24,32,35	12
41	6,7,11,12,13,15,17,19,22,24,26,28,29,30,34,35	16
43	3,5,12,18,19,20,26,28,29,30,33,34	12
47	5,10,11,13,15,19,20,22,23,26,29,30,31,33,35,38,39,40, 41,43,44,45	22
53	2,3,5,8,12,14,18,19,20,21,22,26,27,31,32,33,34,35,39, 41,45,48,50,51	24
59	2,6,8,10,11,13,14,18,23,24,30,31,32,33,34,37,38,39,40, 42,43,44,47,50,52,54,55,56	28
61	2,6,7,10,17,18,26,30,31,35,43,44,51,54,55,59	16
67	2,7,11,12,13,18,20,28,31,32,34,41,44,46,48,50,51,57,61,63	20
71	7,11,13,21,22,28,31,33,35,42,44,47, 52,53,55,56,59,61,62,63,65,67,68,69	24
73	5,11,13,14,15,20,26,28,29,31,33,34,39,40,42,44,45,47, 53,58,59,60,62,68	24
79	3,6,7,28,29,30,34,35,37,39,43,47,48, 53,54,59,60,63,66,68,70,74,75,77	24
83	2,5,6,8,13,14,15,18,19,20,22,24,32,34,35,39,42,43,45,46,47,50, 52,53,54,55,56,57,58,60,62,66,67,71,72,73,74,76,79,80	40
89	3,6,7,13,14,15,19,23,24,26,27,28,29,30,31,33,35,38,41,43,46,48,	40

	51,54,56,58,59,60,61,62,63,65,66,70,74,75,76,82,83,86	
97	5,7,10,13,14,15,17,21,23,26,29,37,38,39,40,41, 56,57,58,59,60,68,71,74,76,80,82,83,84,87,90,92	32

In fact, the number of generators is equal to $\phi(p-1)$, where ϕ is the *Euler's phi function*.

Definition 4.3. (Euler's Phi Function)

The number of integers between 0 and some positive integer *m* that are relatively prime to *m* is an important quantity, so we give this quantity a name:

$$\phi(m) = |\{a \mid 1 \le a \le m, gcd(a,m) = 1\}|.$$

Theorem 4.4. (Euler's Phi Function Formulas**)**

(a) If *p* is a prime and $k \ge 1$, then $\phi(p^k) = p^k - p^{k-1}$.

(b) If $\gcd(m,n) = 1$, then $\phi(mn) = \phi(m)\phi(n)$.

(*pf*)

The verification of the *prime power* formula (a) is easy, so we need to check the formula (b). Here, we did this by using one of the most powerful tools in number theory: COUNTING! Briefly, we are going to find a set contains $\phi(mn)$ elements, and find another set contains $\phi(m)\phi(n)$ elements. Then, show that the two sets contains the same number of elements.

The first set is: $A = \{a \mid 1 \le a \le mn, \text{ and } \gcd(a,mn) = 1\}$.

The second set is: $B = \{(b,c) \mid 1 \le b \le m, \text{ and } \gcd(b,m) = 1, \text{ and } 1 \le c \le n, \text{ and } \gcd(c,n) = 1\}$.

Clearly that *A* has $\phi(mn)$ elements and *B* has $\phi(m)\phi(n)$ elements. Then, find a function *f* from *A* to *B* in the following way:

$$f(a) = (b,c), \text{ if } a \equiv b \pmod{m} \text{ and } a \equiv c \pmod{n}.$$

Now, check that *f* is one-to-one and onto:

(i) Take two numbers a_1 and a_2 from *A*, such that $f(a_1) = f(a_2)$. Then $a_1 \equiv b \equiv a_2$ (mod *m*) and $a_1 \equiv c \equiv a_2 \pmod{n}$. Thus, $a_1 - a_2$ is divisible by both *m* and *n*, in other words, $a_1 \equiv a_2 \pmod{mn}$, which means a_1 and a_2 are the same elements in *A*.

(ii) Clearly that for any given pairs *(b,c)* from *B*, we can always find a integer a, $1 \le a \le mn$, satisfying $a \equiv b \pmod{m}$ and $a \equiv c \pmod{n}$. □

Lemma 4.5. (Euler's Phi Function Summation Formula**)**

Let $d_1, d_2, \cdots, d_r$ be the divisors of *n*. Then $\phi(d_1) + \phi(d_2) + \cdots + \phi(d_r) = n$.

(*pf*)

Let $F(n) = \phi(d_1) + \phi(d_2) + \cdots + \phi(d_r)$, and from *Euler's Phi Function Multiplication Formula* we can get that $F(mn) = F(m)F(n)$ if $\gcd(m,n) = 1$. Check the value of $F(p^k)$ for prime powers: $F(p^k) = \phi(1) + \phi(p) + \phi(p^2) \cdots + \phi(p^k) = 1 + (p-1) + (p^2 - p) + \cdots + (p^k - p^{k-1}) = p^k$.

Now, factor *n* into a product of prime powers, say $n = p_1^{k_1} p_2^{k_2} \cdots p_s^{k_s}$, and compute $F(n)$:

$$F(n)=F(p_1^{k_1}p_2^{k_2}\cdots p_s^{k_s})=F(p_1^{k_1})F(p_2^{k_2})\cdots F(p_s^{k_s})=p_1^{k_1}p_2^{k_2}\cdots p_s^{k_s}=n$$

Hence we verify that $F(n)$ always equals *n*. □

Definition 4.6. (Primitive Root)

(1) $e_p(a)=$ the smallest exponent $e\ge 1$ so that $a^e\equiv 1(\bmod\ p)$, for *p* is prime and $1\le a\le p-1$.

(2) A number *g* with maximum exponent $e_p(g)=p-1$ is called a *primitive root modulo p*.

Note that the *primitive root* in Number Theory is so called the *generator* in this thesis.

Theorem 4.7. (Primitive Root Theorem**)**

There are exactly $\phi(p-1)$ primitive roots modulo *p*.

(*pf*)

We prove it by using one of the most powerful tools in number theory: COUNTING! Define a function: $\psi(d)=$ (the number of $a's$ with $1\le a\le p$ and $e_p(a)=d$). In particular, $\psi(p-1)$ is the number of primitive roots modulo *p*.

Let *n* be any number that dividing $p-1$, say, $p-1=nk$. Then,

$$X^{p-1}-1=X^{nk}-1=(X^n-1)((X^n)^{k-1}+(X^n)^{k-2}+\cdots+X^n+1)$$

and count how many roots these polynomials have modulo *p*.

First, $X^{p-1}-1\equiv 0\ (\bmod\ p)$ has exactly $p-1$ solutions $X=1,2,\cdots,p-1$. On the other hand, $X^n-1\equiv 0\ (\bmod\ p)$ has at most *n* solutions and $(X^n)^{k-1}+(X^n)^{k-2}+\cdots+1\equiv 0\ (\bmod\ p)$ has at most $n(k-1)$ solutions. Hence the only way is $X^n-1\equiv 0\ (\bmod\ p)$ has exactly *n* solutions and $(X^n)^{k-1}+(X^n)^{k-2}+\cdots+1\equiv 0\ (\bmod\ p)$ has at exactly $n(k-1)$ solutions. Now, count the number of solutions to $X^n-1\equiv 0\ (\bmod\ p)$ using another way. Let $d_1,d_2,\cdots,d_r$ be the divisors of *n*. Then the number of solutions to $X^n-1\equiv 0\ (\bmod\ p)$ is equal to $\psi(d_1)+\psi(d_2)+\cdots+\psi(d_r)$, and we have the formula: $\psi(d_1)+\psi(d_2)+\cdots+\psi(d_r)=n$.

(i) As $n=q$ is a prime, $\psi(1)+\psi(q)=q=\phi(1)+\phi(q)$. $\psi(1)=\phi(1)=1$, so $\psi(q)=\phi(q)$.

(ii) As $n=q^2$, $\psi(1)+\psi(q)+\psi(q^2)=q^2=\phi(1)+\phi(q)+\phi(q^2)$. So, $\psi(q^2)=\phi(q^2)$.

(iii) By induction method, $\psi(q^k)=\phi(q^k)$, as $n=q^k$ is a prime power.

(iv) As $n=q_1q_2$ for two different primes q_1,q_2, $\psi(1)+\psi(q_1)+\psi(q_2)+\psi(q_1q_2)=q_1q_2$ $=\phi(1)+\phi(q_1)+\phi(q_2)+\phi(q_1q_2)$. So, $\psi(q_1q_2)=q_1q_2=\phi(q_1q_2)$.

(v) By induction method, assume $\psi(d)=\phi(d)$, for all numbers $d<n$. We may also assume $n=d_1>d_i, i=2,3,\cdots,r$. From $\psi(n)+\psi(d_2)+\cdots+\psi(d_r)=n=\phi(n)+\phi(d_2)+\cdots+\phi(d_r)$, we can get the equality $\psi(n)=\phi(n)$.

Take $n=p-1$, $\psi(p-1)=\phi(p-1)$, which is the desired conclusion. □

We also noticed the following two lemmas from the table so that the performance of program can be enhanced as finding the generators of larger primes.

Lemma 4.8.

For prime $p \equiv 1 \pmod 4$, if *g* were a generator of *p*, then -*g* is also a generator of *p*.

(*pf*)

Suppose not, i.e., *g* is a generator of *p*, but there exists $2 \le b \le (p-2), b \mid (p-1)$, such that $(-g)^b \equiv 1 \pmod p$.

(i) if *b* were even, then $g^b \equiv (-g)^b \equiv 1 \pmod p$, which is clearly a contradiction.

(ii) if *b* were odd: $4 \mid (p-1)$ implies that $2b \mid (p-1)$ and $2b < (p-1)$, and hence $g^{2b} \equiv (-g)^{2b} \equiv 1 \pmod p$, which is a contradiction. □

Lemma 4.9.

For prime $p \equiv 3 \pmod 4$, if *g* were a generator of *p*, then -*g* is not a generator of *p*.

(*pf*)

Clearly that $\frac{p-1}{2}$ is odd and $g^{\frac{p-1}{2}} \equiv (-1) \pmod p$. Hence $(-g)^{\frac{p-1}{2}} \equiv 1 \pmod p$. □

Note that *g* and (-*g*) may both not be the generators of *p*. For example, 7 and 12 are both not the generators of prime 19.

5. The minimal elements set $\mathbb{Z}_m \times F_q$ based on our construction

After finding the generators of each prime less than 100, we are interested in the minimal $\mathbb{Z}_m \times F_q$ that can make $T_{m,q}$ have the *difference distinct property* based on our construction. In this chapter we introduce an algorithm first, and then get the conclusion that the minimal size of $\mathbb{Z}_m$ corresponding to the F_q can be less than $m = 2q-4$, which is one lower bound that we proposed in our paper.

Recall the Algorithm 3.1 in the previous chapter. In the algorithm we input (q, a, m), where *q* is a prime power, *a* is a generator of *q*, and *m* is the size of the addition group $\mathbb{Z}_m$. The results shows the repetition between the differences of every two terms.

Algorithm 5.1. (Find the minimal $\mathbb{Z}_m$ corresponding to the prime *q* and generator *a*)

Input prime q and generator a

for int m from $q+1$ to $2q-5$

do Alorithm 3.1 with the input (q, a, m);

if there are results run out

try the next $m+1$;

else (there are no results run out)

output (q, a, m);

break the for loop;

end

Table 5.2 (The minimal $\mathbb{Z}_m$ corresponding to every generator of each prime less than 100.)

Prime q	**Generators a**															
	Corresponding minimal $\mathbb{Z}_m \times F_q$ based on our construction															
5	**2**	**3**	$(m,q)=(5,6)$ is the only case for $m=q+1$													
	6	6														
7	**3**	**5**														
	10	10														
11	**2**	**6**	**7**	**8**	Note that the minimal $\mathbb{Z}_m$ is less that $2q-4$.											
	15	15	16	16												
13	**2**	**6**	**7**	**11**												
	20	18	20	18												
17	**3**	**5**	**6**	**7**	**10**	**11**	**12**	**14**								
	26	27	26	27	28	27	28	27								
19	**2**	**3**	**10**	**13**	**14**	**15**										
	30	31	30	31	30	30										
23	**5**	**7**	**10**	**11**	**14**	**15**	**17**	**19**	**20**	**21**						
	36	37	37	38	36	38	37	37	38	38						
29	**2**	**3**	**8**	**10**	**11**	**14**	**15**	**18**	**19**	**21**	**26**	**27**				
	45	44	47	44	47	46	45	48	44	48	44	46				
31	**3**	**11**	**12**	**13**	**17**	**21**	**22**	**24**								
	52	52	50	50	52	52	48	48								
37	**2**	**5**	**13**	**15**	**17**	**18**	**19**	**20**	**22**	**24**	**32**	**35**				
	59	62	63	62	63	63	59	63	62	63	62	63				
41	**6**	**7**	**11**	**12**	**13**	**15**	**17**	**19**	**22**	**24**	**26**	**28**	**29**	**30**	**34**	**35**
	66	66	68	68	66	68	68	66	74	68	66	74	68	66	73	73
43	**3**	**5**	**12**	**18**	**19**	**20**	**26**	**28**	**29**	**30**	**33**	**34**				
	72	74	72	72	73	73	74	73	72	74	74	73				

47	**5**	**10**	**11**	**13**	**15**	**19**	**20**	**22**	**23**	**26**	**29**	**30**	**31**	**33**	**35**	**38**
	81	79	74	81	79	81	76	79	80	77	81	74	79	79	80	77
	39	**40**	**41**	**43**	**44**	**45**										
	78	76	78	80	79	80										
53	**2**	**3**	**5**	**8**	**12**	**14**	**18**	**19**	**20**	**21**	**22**	**26**	**27**	**31**	**32**	**33**
	91	88	90	90	92	92	88	92	90	90	87	87	91	92	90	92
	34	**35**	**39**	**41**	**45**	**48**	**50**	**51**								
	92	96	92	87	92	90	96	87								

59	**2**	**6**	**8**	**10**	**11**	**13**	**14**	**18**	**23**	**24**	**30**	**31**	**32**	**33**
	100	99	104	99	102	101	102	101	101	96	100	97	96	98
	34	**37**	**38**	**39**	**40**	**42**	**43**	**44**	**47**	**50**	**52**	**54**	**55**	**56**
	98	104	102	103	97	97	102	95	98	101	97	98	95	103
61	**2**	**6**	**7**	**10**	**17**	**18**	**26**	**30**	**31**	**35**	**43**	**44**	**51**	**54**
	103	104	105	104	107	107	107	105	103	105	101	101	104	107
	55	**59**												
	104	105												
67	**2**	**7**	**11**	**12**	**13**	**18**	**20**	**28**	**31**	**32**	**34**	**41**	**44**	**46**
	115	118	115	117	117	110	118	117	117	114	115	110	114	115
	48	**50**	**51**	**57**	**61**	**63**								
	118	118	115	118	115	118								
71	**7**	**11**	**13**	**21**	**22**	**28**	**31**	**33**	**35**	**42**	**44**	**47**	**52**	**53**
	125	125	125	118	124	126	122	126	126	124	118	119	121	124
	55	**56**	**59**	**61**	**62**	**63**	**65**	**67**	**68**	**69**				
	122	121	124	125	126	126	124	124	119	126				
73	**5**	**11**	**13**	**14**	**15**	**20**	**26**	**28**	**29**	**31**	**33**	**34**	**39**	**40**
	120	128	123	126	126	128	123	122	124	123	123	125	126	129
	42	**44**	**45**	**47**	**53**	**58**	**59**	**60**	**62**	**68**				
	129	120	123	126	130	125	123	122	130	124				
79	**3**	**6**	**7**	**28**	**29**	**30**	**34**	**35**	**37**	**39**	**43**	**47**	**48**	**53**
	144	141	139	139	133	133	139	143	133	134	141	133	139	144
	54	**59**	**60**	**63**	**66**	**68**	**70**	**74**	**75**	**77**				
	133	138	133	138	141	141	143	138	138	134				
83	**2**	**5**	**6**	**8**	**13**	**14**	**15**	**18**	**19**	**20**	**22**	**24**	**32**	**34**
	144	138	140	144	148	140	141	141	144	147	146	144	148	146
	35	**39**	**42**	**43**	**45**	**46**	**47**	**50**	**52**	**53**	**54**	**55**	**56**	**57**
	144	142	144	136	144	143	144	138	144	144	147	147	136	140
	58	**60**	**62**	**66**	**67**	**71**	**72**	**73**	**74**	**76**	**79**	**80**		

	151	141	144	142	140	139	141	151	143	139	144	147		
89	**3**	**6**	**7**	**13**	**14**	**15**	**19**	**23**	**24**	**26**	**27**	**28**	**29**	**30**
	152	154	154	159	155	154	156	158	156	156	156	156	157	152
	31	**33**	**35**	**38**	**41**	**43**	**46**	**48**	**51**	**54**	**56**	**58**	**59**	**60**
	158	156	156	154	157	157	154	159	154	151	148	155	157	154
	61	**62**	**63**	**65**	**66**	**70**	**74**	**75**	**76**	**82**	**83**	**86**		
	151	148	154	154	155	155	153	156	157	154	153	157		
97	**5**	**7**	**10**	**13**	**14**	**15**	**17**	**21**	**23**	**26**	**29**	**37**	**38**	**39**
	168	166	175	172	166	172	169	169	170	166	167	169	170	168
	40	**41**	**56**	**57**	**58**	**59**	**60**	**68**	**71**	**74**	**76**	**80**	**82**	**83**
	169	172	166	172	167	170	161	175	172	170	161	172	172	170
	84	**87**	**90**	**92**										
	172	167	170	167										

We can give the table a brief conclusion that we find the minimal size of $\mathbb{Z}_m$ can be less than $2q-4$ for every prime $p \geq 11$. In additionally, the distance between minimal size of $\mathbb{Z}_m$ and $2q$ gets longer as the prime gets larger.

You may also notice that $(m,q)=(5,6)$ is the only case for $m=q+1$. In fact, it is the Example 2.12 which is introduced to fit our construction in chapter 2.

6. Conclusions and future works

We applied our construction to implement a certain pooling design. In this thesis we also tried to find ways to improve the properties of this construction. Through the programming, it shows that $\mathbb{Z}_m$ can be less than $2q-4$ for every prime $p \geq 11$, and this result is better than the results we proposed on the original paper [1].

The bound of $\mathbb{Z}_m$ might be lower if we keep running the program in chapter 5 through every generators. However, due to the complexity and lacking of memories, so far we have not get the results. Improving the algorithm and mathematical deduction will be the following challenge of this research.

References

[1] Yu-pei Huang, Hsin-jung Wu, and Chih-wen Weng, *d*-disjunct Matrices with constant column weight *d+1*, March, 2010.

[2] Joseph H. Silverman, A friendly introduction to number theory, 2nd Ed., ch20, pp125-134, Prentice-Hall, 2004.

[3] Ding-Zhu Du and Frank K Hwang, Pooling designs and nonadaptive group testing, World Scientific, 2006.