中華民國 第 50 屆中小學科學展覽會

作品說明書

國中組　數學科

第一名

030421

密碼鎖-拉丁超立方體的完美控制情形

學校名稱：國立南科國際實驗高級中學(國中)

作者：	指導老師：
國二 尤怡方	曾智偉
國二 余珍華	許淑芬
國二 李敏辰	
國一 陳佑瑄	

關鍵詞：Cartesian　product、拉丁超立方體、延伸樹

得獎感言

對於這一次的得獎，我們感到難以言盡的喜悅，因為我們過程中經歷了無數次的挑戰與瓶頸，常常有山窮水盡的感覺，曾經幾度想要放棄。但在智偉老師的指導與我們組員努力下，總算「柳暗花明又一村」，找到了新的方法或研究方向。此外我們遇到瓶頸後，總是去尋找資料、問老師，或是去從我們已知的部分尋找特別的地方以把我們的研究推進下去。像是我們一直找不到四維的切確公式時，我們曾經有想過：「做到這裡就夠了」，但是在導師的督促和秉持「好還要更好」的精神，我們在努力地尋找一點的可能性時，發現了完美控制情形，所以才能有現在如此輝煌的結果。我們所獲的的榮耀，不應只侷限於我們而已，我們要感謝我們的指導老師－志偉老師與淑芬老師，在研究過程中給予我們協助與指正。

摘要

有個密碼鎖由 D 個旋鈕組成，每個旋鈕有 N 種不同的號碼，由於構造缺點若 D 個旋鈕中僅有*1*個號碼錯誤仍能打開密碼鎖，問最少嘗試多少組號碼才能保證一定能打開這個鎖？這個問題等同於在 N 元 D 維超立方中找一組點集，點集中的點各自向其 D 維度畫出延伸線，若超立方中的所有點都至少被*1*條延伸線所涵蓋，要求重複涵蓋的次數總和要最少。

*43*屆的科展中已經討論過*3*個旋鈕的情況，我們接著分析*4*個旋鈕的情況。在討論中發現 $D=4$時並沒有型如 $D=3$時保證打開的最小次數公式，我們給出上下限的公式。但 $D=N+1$ 且 N 是任意質數時卻很特別，恰可利用拉丁超立方挑出*1*組點集，其所有延伸線涵蓋的點都沒有重複，稱為完美控制，而保證打開鎖的最小次數是 N^{N-1}。

壹、 研究動機

在學校看到上屆學長的科展海報，很好奇的去搜尋資料後，發現這個問題和很多領域有關，像是「忘記旅行箱密碼的故事」、「工廠製作密碼鎖的原理」、「千禧蟲」等。我們覺得高維度超立方體很有趣，對於密碼鎖的瑕疵問題能轉換成超立方體問題也覺得很新鮮，起初老師讓我們看影片「不可能的三角形」去體會視覺誤差的情況，然後由紙上3維立方體各線條間交叉關係讓我們去想像4維的圖形在紙上表現時的關係。另外在找資料時還看到有關超立方體內探尋漢彌頓路徑、Euler的36軍官及還有2元超立方體[參考資料一]等問題，老師也提到4維可想成是3維再結合1維度的結果，和國1學的實數線變成2維的平面很相似，這些都讓我們覺得十分想去了解，尤其是一開始老師問我們「會不會畫4維超立方的模型呢？」引起我們很大的興趣，最後我們決定把這個國際奧林匹克競賽的題目從3個旋鈕8個號碼延伸下去，看能不能對於更多旋鈕的情況有所發展。

貳、 研究目的

一、 分析4個旋鈕上各有 N 個號碼的數學模型(N^4 問題)，求保證開鎖的最小次數或上下限。

二、 4個旋鈕上各有3個號碼時(3^4 問題)，找到保證能打開鎖的最少號碼組合，並證明其是完美控制的情況。

三、 5個旋鈕上各有4個號碼時(4^5 問題)，找到保證能打開鎖的最少號碼組合，並證明其是完美控制的情況。

四、 當 N 是質數，在 $N+1$ 個旋鈕上各有 N 個號碼時(N^{N+1} 問題)，找到保證打開的最少號碼組合，並證明其是完美控制情況，最小次數是 N^{N-1} 。

參、 研究設備及器材

紙、筆、 *Excel* 、網際網路、多向連結方塊、智高積木

肆、 研究過程與方法

一、前言

(一)文獻探討

1988年國際奧林匹克數學競賽中東德提供1個預選題如下：1個密碼鎖由3個旋鈕，每個旋鈕有8個位置(號碼)組成，由於構造上的缺點只要旋鈕中有2個正確便能打開這個鎖。問最少要嘗試多少組合才能保證打開這個鎖？這問題的答案出奇之小是32組號碼。後來在43屆的全國科展中曾被推廣為3個旋鈕其上有 n 個位置的 $n\times n\times n$ 密碼鎖問題，討論出保證能開鎖的最少號碼組合次數的公式如下：

n是偶數時：$(\frac{n}{2})^2+(\frac{n}{2})^2$　　[參考資料三 P.5]

n是奇數時：$(\frac{n+1}{2})^2+(\frac{n-1}{2})^2$ .....(一.1式)

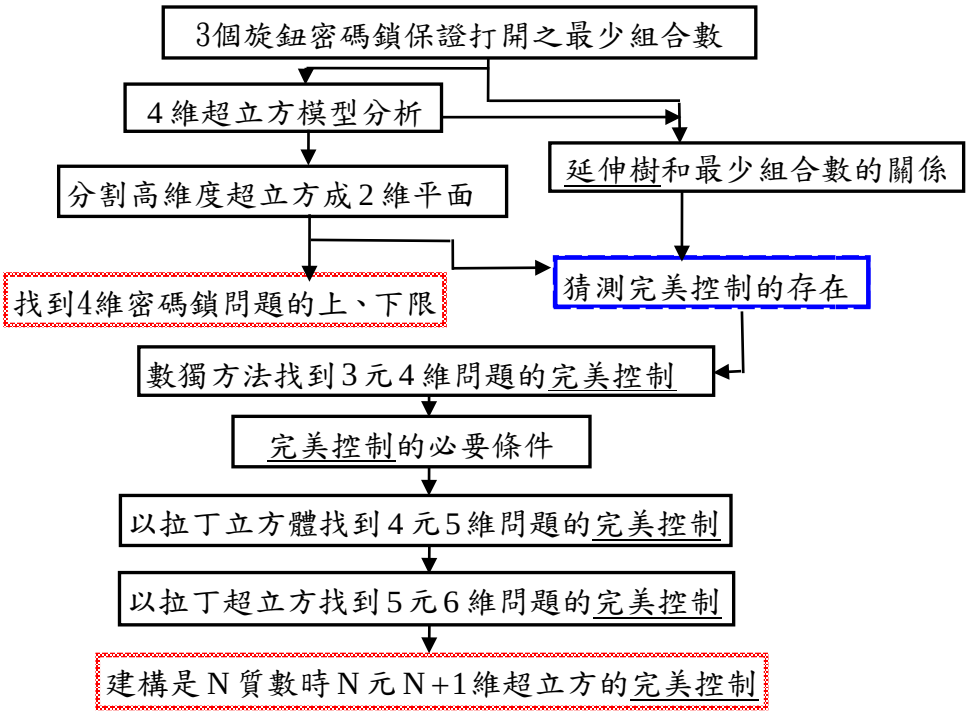
其後在48屆全國科展中有篇文章「超立方Qn的最小控制」，主要是談論如下：在2^n超立方中取1個點集，點集中的點及其有邊相連(只有1維座標不同)的點都聯集起來，若聯集的結果是整個超立方，便稱這個點集是1個控制集，點數最小的控制集其點數稱為控制數。文章討論出$n=2^p-1$時用nim(拈)遊戲選的任2控制點不會控制同1個點，此時控制數是2^{n-p}，但n是其它數時沒有找到公式只可以確定上限。文章中還提及1個控制點可以控制本身及跟自己有邊相連的點，就像是一個警衛可以看守自己這個點還有它眼力可達的點，我們覺得這個概念可以用於43屆密碼鎖科展中，於是試著結合2篇科展文章將其再推廣。

(二)名詞與符號定義

於本文中我們會重複使用到幾個概念，為了表達上的方便我們首先定義下列名詞：

1. 延伸樹：　1個點及超立方中與此點僅有1維座標相異之點的聯集。
2. 控制集：　1點集若其內各點之延伸樹的聯集等於整個超立方，稱此點集是個控制集，其內的點稱為控制點。
3. 完美控制：　1組控制集其控制點之延伸樹間沒有交集的情況。

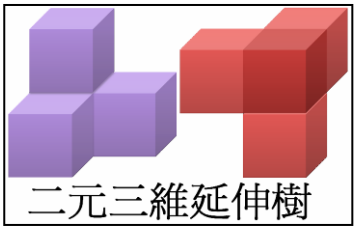
(三)研究流程圖



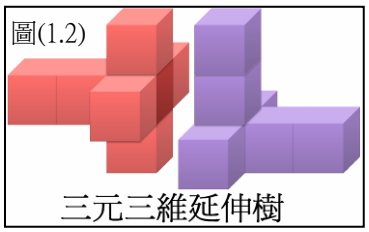
二、4個旋鈕上各有N個號碼時保證開鎖的最小次數上下限

(一)分析3維的模型結構來推演4維的情況

由警衛看守 2^n 超立方觀點可知缺陷密碼鎖問題可轉變成超立方體中延伸樹的涵蓋與重疊問題，於是我們從延伸樹著手來分析。2元3維立方體中的每個延伸樹涵蓋了4個點圖(1.1)，顯而易見的若所選的2點其延伸樹之間沒有重疊，則這2個點就形成1組控制集。



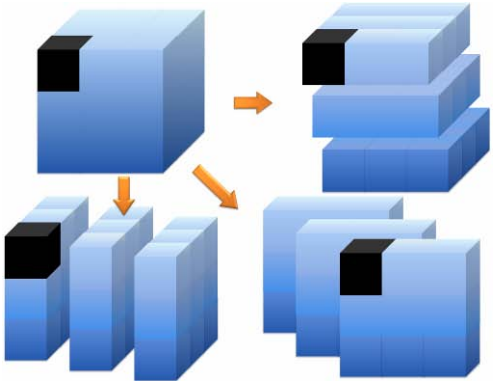
圖(1.1)



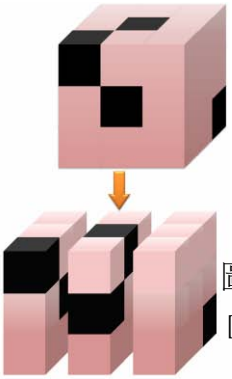
把3元3維的立方體由3個不同方向分割成9個2維平面觀察，發現任1個點會出現在3個不同的2維平面中，由*(一.1式)*知3元3維的最小控制集其點數是5，這5點在所有平面上共出現15次，由鴿籠原理得知某個平面上的控制點數會大於1，延伸樹會重疊。又每個延伸樹可涵蓋7個點(圖1.2)，$5\times 7-27=8$──有8次重疊。

n 元3維的立方體中，每個延伸樹涵蓋 $3\times(n-1)+1=3n-2$ 個點。若延伸樹間不重疊，n^3 必定是 $3n-2$ 的倍數。我們用 *Excel* 來計算時在小於1000的正整數中只有1和2滿足上述要求，因此猜想完美控制的情況會存在但很稀少。

3元3維的立方體可以切割成九個平面，1個控制點會出現在不同的3個2維平面上。



3元3維的最小可行解數為5，某些平面會出現2個控制點。



圖(1.3)
[參考文獻二 p.12]

【小結論1】n 元3維的立方體中，n =1和2時才能挑出延伸樹不重疊的控制集。

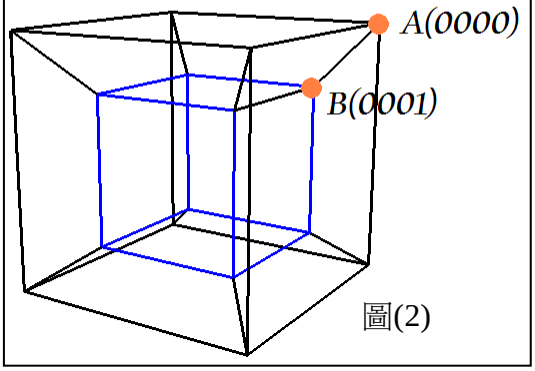
證明：若 $(3n-2)\mid n^3$ 且 $(3n-2)\mid(3n-2)^3$，則 $(3n-2)\mid[27n^3-(3n-2)^3]$，

$(3n-2)\mid(54n^2-36n+8)$，$(3n-2)\mid[(54n^2-36n+8)-6(3n-2)^2]$，最後得到

$(3n-2)\mid 8$ ，$3n-2$ 必定是8的因數，因此 n 的正整數解只有1或2。

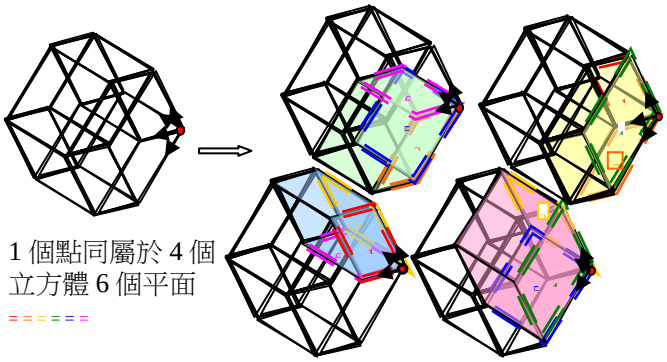
3維立方體中的點都有3個方向要延伸， 4維中的點都該有4個方向延伸，其中任選3個方向可組成一個立方體。同一個維度上的2點其坐標只有1維數字不同，且可各自屬於2個相異而不相交的3維立方體，如圖(2) 中 A(0000) 屬於外層的立方體， B(0001) 屬於內層的立方體。選定某3維立方上的點A可發現它的延伸樹只能涵蓋另1個3維立方上的1個點B如圖(4) ，同時平面外的點其延伸樹最多只能涵蓋此平面中的1個點。

一個 2 元 4 維的超立方體有 8 個立方體、16 個平面、24 條邊、32 個點。



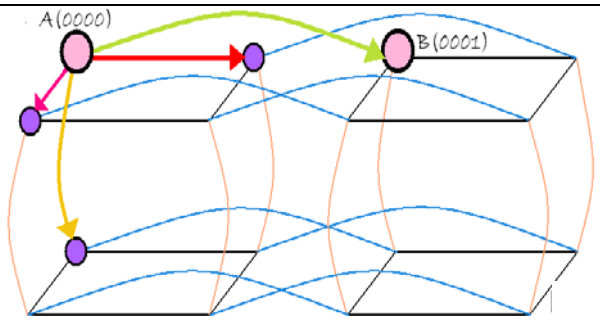
圖(2)

2元4維時，1個延伸樹涵蓋了5個點，故需要4個控制點以上才能蓋滿超立方 2^4 點，因此延伸樹間最少重疊了 $4\times5-2^4=4$ 次。



1 個點同屬於 4 個立方體 6 個平面

圖(3)



圖(4) 右立方體中的所有點，只有B點能被點A的延伸樹涵蓋。[參考文獻一 p.3]

$n=3$時由 *Cartesian prodcut* $3^4=3\times3\times(3\times3)$ 得知1個3元4維的超立方可視為9個3×3的平面，若將其分割成9個平面如表(一)，利用2維平面外的點最多只和此平面上的1個點有邊相連通的特性，可畫出選定之點其4個方向上的延伸線以構成延伸樹，表(一)中9個黑格其延伸樹恰好蓋滿 3^4 超立方，故這9點成為一組控制集。

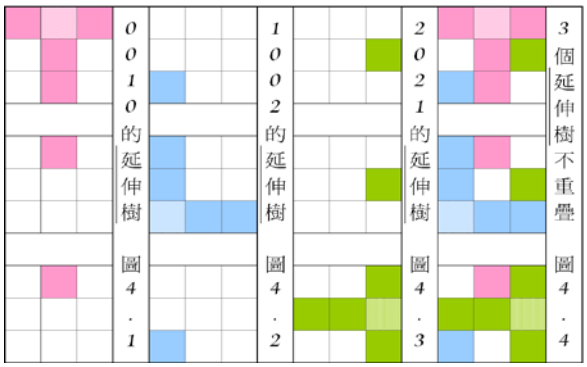
x1	x2	x3	x4					
0000	0010	0020	1000	1010	1020	2000	2010	2020
0001	0011	0021	1001	1011	1021	2001	2011	2021
0002	0012	0022	1002	1012	1022	2002	2012	2022
0100	0110	0120	1100	1110	1120	2100	2110	2120
0101	0111	0121	1101	1111	1121	2101	2111	2121
0102	0112	0122	1102	1112	1122	2102	2112	2122
0200	0210	0220	1200	1210	1220	2200	2210	2220
0201	0211	0221	1201	1211	1221	2201	2211	2221
0202	0212	0222	1202	1212	1222	2202	2212	2222

四個顏色代表四個不同的維度

表(一)，一個三元四維的超立方體

(二)利用數獨遊戲的方法讓4維圖形中的延伸樹減少重疊

由表(一)看出要減少延伸樹的重疊，關鍵是像數獨遊戲般在不同行、列之中挑選控制點。點(0010)的延伸樹在 x_3 方向只能涵蓋(1010)和(2010)兩點，在 x_4 方向只能涵蓋(0110)和(0210)兩點。右圖(5)可以看到(0010)　(1002),(2021)3個點中任2點在各自的平面上的行列位置都不相同，其延伸樹用不同的顏色標示便可發現彼此沒有重疊。



圖(5)

進一步觀察，如果1個格子看作是1個2維平面，表(一)中9個控制點其 (x_1, x_2) 座標是 (0,0) ~ (2,2) 如表(二.1)中的黑色數字，剛好是整數0 ~ 8的10進位換成3進位的2元數， x_3, x_4 各自成1個拉丁方陣，且 (x_3, x_4) 形成1個正交拉丁方陣(表二.2)。

0010	1002	2021
0122	1111	2100
0201	1220	2212

9個平面的控制點 (表二.1)

→

10	02	21
22	11	00
01	20	12

X3 X4正交拉丁方陣 (表二.2)

=

1	0	2
2	1	0
0	2	1

X3 拉丁方陣 (表二.3)

+

0	2	1
2	1	0
1	0	2

X4 拉丁方陣 (表二.4)

表(二)

3^4 超立方中任1點其延伸樹可涵蓋 $2\times4+1=9$ 個點，若延伸樹不重疊則要蓋滿超立方需 $81\div9=9$ 個延伸樹，表(一)中的控制集有9個控制點故是最小控制集，延伸樹間沒重疊。

(三)推測4維問題中不存在型如3維時的最小控制集點數公式，故推論上下限

2元3維和3元4維都可挑出延伸樹不重疊的控制集，而2元3維的最小控制集點數是2，觀察 $2=1^2+1^2$ 符合一.1式的要求，$2=2^{2-1}$ 也符合 n^{n-1} 型態，3元4維的最小控制集點數是9，分析一下9這個整數會符合什麼樣的公式，由於

$9=1+8=2+7=3+6=4+5=3\times3$，我們發現 $9=1+8$ 符合 $9=1^3+2^3$，而 $9=3^2$ 符合 n^{n-1}，只有這2個式子其型態和3維時公式類似也和 3^4 中的3與4兩數字相關，故猜測若4維有類似3維時型態的簡單公式應該如下:

$$\begin{cases} (\frac{n}{2})^3+(\frac{n}{2})^3 & ,n\text{是偶數時} \\ (\frac{n+1}{2})^3+(\frac{n\text{-}1}{2})^3 & ,n\text{是奇數時} \end{cases} \quad \text{.....(二.1式)}$$

或　n^{n-1}　.....(二.2式)

依*(二.1式)*，則 $n=4$ 時最小控制集點數是 $(\frac{4}{2})^3+(\frac{4}{2})^3=16$ ，但4元4維中每個控制點其延伸樹可以涵蓋 $3\times4+1=13$ 個點，16個控制點則涵蓋 $13\times16<4^4$ ，沒蓋滿 4^4 ，故最小控制集點數不可能是16，可知*(一.2式)*不合。

依*(二.2式)*，則 $n=4$ 時最小控制集點數為 4^3 ，由*(一.1式)*知道1個4元3維的立方體只需要8個控制點，再由 *Cartesian prodcut* $4^4=(4\times4\times4)\times4$ ，4元4維超立方體等於是由4個4元3維的立方體所組成，所需的最小控制集點數不會超過 $4\times8=32$ ，並不是*(二.2式)*預測的64，故*(二.2式)*也是不合的。4維情況下我們沒找到合理的公式，不過由 $N^4=N^3\times N$ ，把N元4維超立方看做N個 N^3 立方體再加上*(一.1式)*，可以推論4維密碼鎖的最小控制集點數的1個明顯上限公式：

【小結論*2*】*4*維問題中的最小控制集點數上限

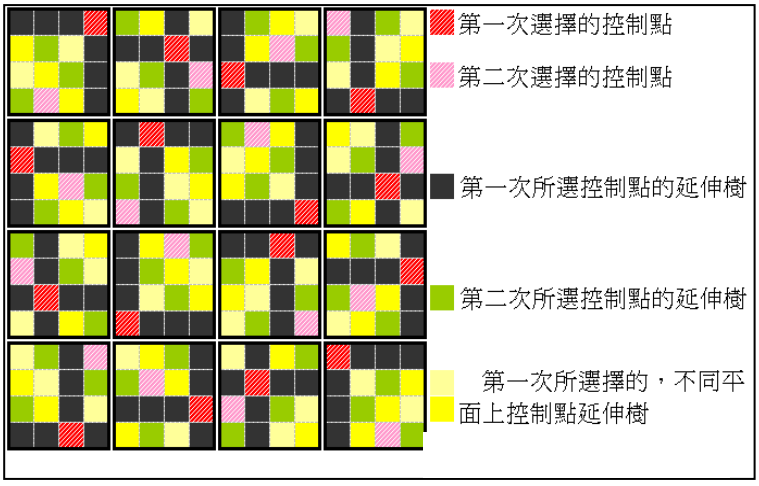
N是偶數時：$[(\frac{N}{2})^2+(\frac{N}{2})^2]\times N$

N是奇數時：$[(\frac{N+1}{N})^2+(\frac{N-1}{N})^2]\times N$ .....(二.3 式)

3元4維存在延伸樹都不重疊的完美控制。那4元4維的密碼鎖問題是否也存在完美控制？4元4維中的*1*點其延伸樹共涵蓋13個點，若每個延伸樹彼此不重疊則它們的聯集必為是13的倍數，但 4^4 不是13的倍數，所以不可能出現完美控制的情形。

進一步把 4^4 分割成16個 4^2 平面分析，在選擇控制點時先選出16個延伸樹都不重疊的控制點，發現每個2維平面上都剩下3個沒被涵蓋到的點，我們思考如何讓一個控制點其延伸樹扣除掉重疊後，其可以涵蓋的效應可以達到最大，但目前我們只能讓第二次所選的控制點其延伸樹的有效涵蓋數為3。

圖(6) 4元4維的2維分割圖及1組控制集



右圖(6)中4元4維中所選的控制集其延伸樹會出現重疊，我們由*(二.3式)*算出其上限點數是32，而這組找出來的控制集點數也是32，我們試過的方法都無法用少於32個控制點去涵蓋整個超立方，雖是如此但我們仍無法證明這就是一組最小控制集。

4元4維中的每個延伸樹的涵蓋點數是13， $20\times13<4^4$ ， $21\times13>4^4$ ，由延伸樹和超

立方體總點數的關係來看，控制點數不能小於21，是目前我們所知的下限。

由於n元4維的密碼鎖問題中有n^4個點需要被涵蓋，每個延伸樹都能涵蓋$4n-3$個點，若是延伸樹不重疊，只需$\frac{n^4}{4n-3}$個控制點，這時$4n-3$必須是n^4的因數；若$4n-3=n^1$，則$n=1$；$4n-3=n^2$則$n=1$或3；$4n-3=n^3$則$n=1$。

【小結論*3*】n元4維的超立方中，$n=1$和*3*時才能挑出延伸樹不重疊的控制集。

$n=2$時$\frac{n^4}{4n-3}>3$，由*(*二*.3*式*)*得知2^4密碼鎖問題最小控制集點數上限是4，故2^4最小控制集其點數＝4，因延伸樹能涵蓋5點，$4\times5>2^4$這也是1組非完美控制的最小控制集。

【小結論*4*】4維問題中的最小控制集數的下限：

$$\text{最小控制集點數}\geq\frac{n^4}{4n-3}\quad\text{.....(二.4式)}$$

(四) N元N+1維滿足完美控制的必要條件

留意到2元3維和3元4維都有完美控制，4元4維卻沒有，那什麼條件下能出現完美控制呢？

N元D維中每個點其延伸樹可涵蓋$(N-1)\times D+1$個點，因此$(N-1)\times D+1$為N^D的因數是完美控制的必要條件，寫成$(N-1)\times D+1=N^K$，K是正整數。由2元3維和3元*4*維的例子我們猜，當$D=N+1$，也就是$K=2$時，滿足必要條件，這時$(N-1)\times D+1=(N+1)\times(N-1)+1=N^2$。

【小結論*5*】N元$N+1$維時滿足完美控制的必要條件，此時最小控制集點數為：

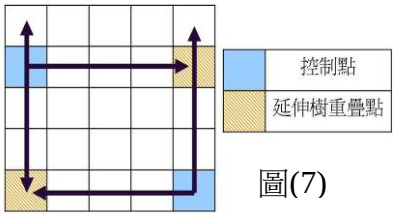
$$\frac{N^D}{(N-1)\times D+1}=N^{N-1}\quad\text{.....(二.5式)}$$

三、 *4*元*5*維的完美控制

在上一節中預測了N元$N+1$維時可能有完美控制，首先討論$N=4$的情形，我們仍需先找出1組涵蓋整個4^5超立方的控制集，再去證明它是1組完美控制。

(一)完美控制則任*1*平面上最多能有1個控制點

兩個控制點出現在同一平面上則其延伸樹必會重疊

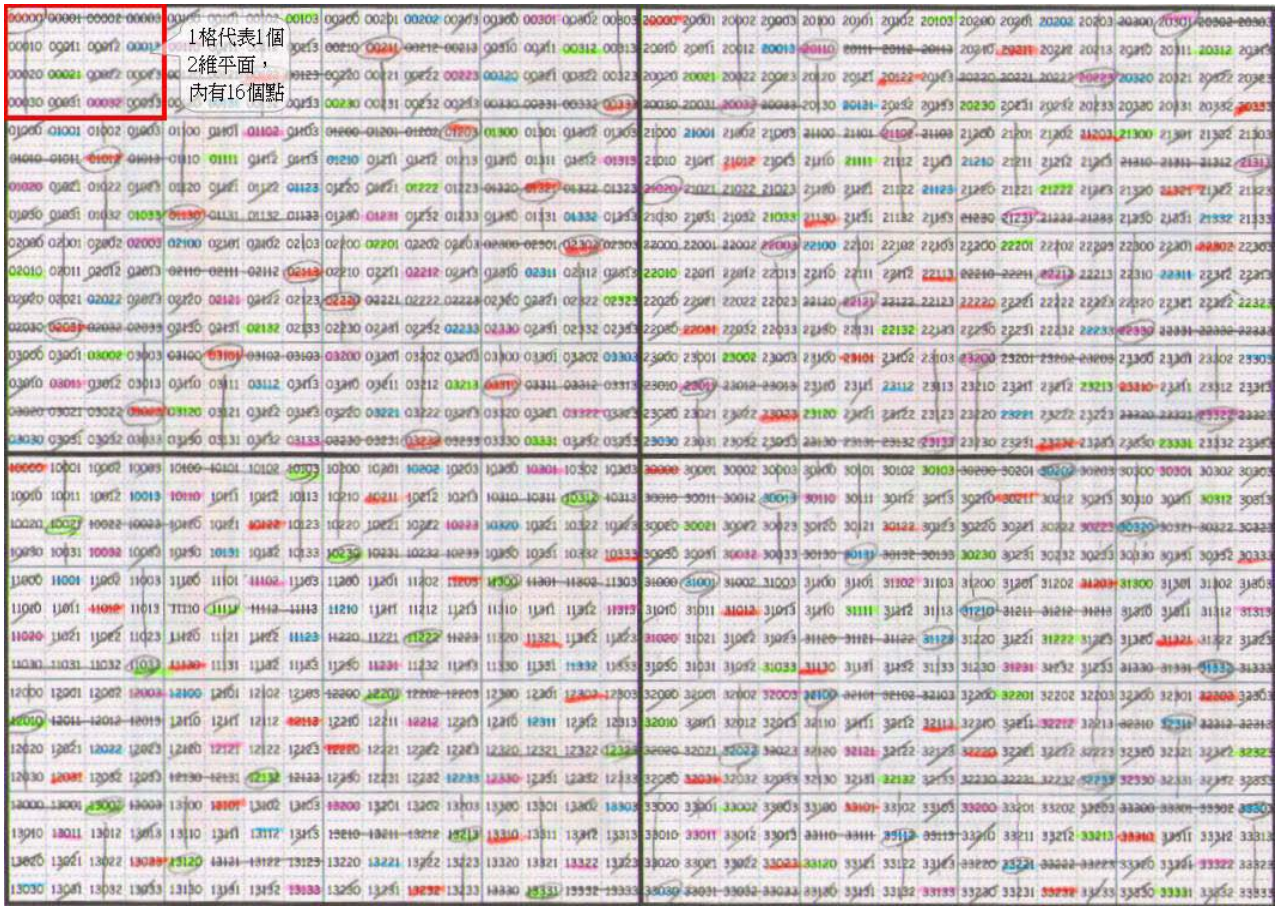


圖(7)

如右圖(7)，反之所有平面上最多只有1控制點時則延伸樹不重疊，故完美控制時所有平面上不能超過1個控制點。

(二)用拉丁超立方和正交拉丁方陣挑選完美控制的控制集

在3元4維中使用數獨的方法找到的控制集是完美控制，我們也把4元5維分割成64個2維平面如下圖(8)，再借用「不同行、列」的想法挑出1組64個點。



圖(8)　圈起64個點及其延伸樹

上圖*(8)*中挑出的64個點其座標列出如表*(*四*)(*五*)(*六*)(*七*)*。表*(*四*)*中每1格代表1個圖*(8)*中的2維平面，將其編為0 ~ 63號，同1格中的16個點它們前3維座標都相同所以把這64個平面命名為 $(x_1, x_2, x_3) = (0,0,0) \sim (3,3,3)$ 如同表*(*五*)*所示，這64個3元數也正好是表*(*四*)*中的數由10進位轉成4進位的結果。

編號*0~63*個格子代表*64*個*2*維平面

	0	*4*	*8*	*12*	*16*	*20*	*24*	*28*	*32*	*36*	*40*	*44*	*48*	*52*	*56*	*60*	表四
	1	*5*	*9*	*13*	*17*	*21*	*25*	*29*	*33*	*37*	*41*	*45*	*49*	*53*	*57*	*61*	
	2	*6*	*10*	*14*	*18*	*22*	*26*	*30*	*34*	*38*	*42*	*46*	*50*	*54*	*58*	*62*	
	3	*7*	*11*	*15*	*19*	*23*	*27*	*31*	*35*	*39*	*43*	*47*	*51*	*55*	*59*	*63*	
x1	*000*	*010*	*020*	*030*	*100*	*110*	*120*	*130*	*200*	*210*	*220*	*230*	*300*	*310*	*320*	*330*	表五
x2	*001*	*011*	*021*	*031*	*101*	*111*	*121*	*131*	*201*	*211*	*221*	*231*	*301*	*311*	*321*	*331*	
x3	*002*	*012*	*022*	*032*	*102*	*112*	*122*	*132*	*202*	*212*	*222*	*232*	*302*	*312*	*322*	*332*	
	003	*013*	*023*	*033*	*103*	*113*	*123*	*133*	*203*	*213*	*223*	*233*	*303*	*313*	*323*	*333*	

這64個點其(x_4, x_5)座標如表(六)，把x_4, x_5的數字分開來看，這2×64個數字剛好形成2個4階拉丁立方體，同時(x_4, x_5)在相同的平面中形成4階的正交拉丁方陣。把表(五)和表(六)合成表(七)就是這64個點的5維座標。

X4和x5在各平面上結合成4階正交拉丁方陣

x4 x5																	
	00	12	31	23	21	33	10	02	32	20	03	11	13	01	22	30	表六
	22	30	13	01	03	11	32	20	10	02	21	33	31	23	00	12	
	11	03	20	32	30	22	01	13	23	31	12	00	02	10	33	21	
	33	21	02	10	12	00	23	31	01	13	30	22	20	32	11	03	

合成5維座標

00000	01012	02031	03023	10021	11033	12010	13002	20032	21020	22003	23011	30013	31001	32022	33030	表七
00122	01130	02113	03101	10103	11111	12132	13120	20110	21102	22121	23133	30131	31123	32100	33112	
00211	01203	02220	03232	10230	11222	12201	13213	20223	21231	22212	23200	30202	31210	32233	33221	
00333	01321	02302	03310	10312	11300	12323	13331	20301	21313	22330	23322	30320	31332	32311	33303	

檢查這64個點的延伸樹後發現恰可涵蓋4元5維的超立方體，所以這是一組控制集，接下來我們要證明所選控制集是完美控制。

(三)控制點出現在平面上的總次數，證明任1平面都恰有1個控制點

4元5維超立方可由10個方向分割成2維平面，每個方向都分割出64個平面，故整個超立方包含了640個平面。5維超立方中任1個點會出現在10個平面上，故64個控制點恰在所有平面上共出現640次。

若是640個平面上都出現控制點，由鴿籠原理，得到所有平面上恰有1個控制點，因此延伸樹間不重疊。我們把640個平面分成3類5種情況討論：

	沒有(x_4, x_5)	有(x_4, x_5)的其中1個	有(x_4, x_5)
選取維度	1、x_1, x_2, x_3	2、x_1, x_2, x_4 和 x_1, x_2, x_5 3、x_1, x_3, x_4 和 x_1, x_3, x_5 4、x_2, x_3, x_4 和 x_2, x_3, x_5	x_1, x_4, x_5 5、x_2, x_4, x_5 x_3, x_4, x_5

1. x_1, x_2, x_3 方向的64個平面

圖(8)中所挑的64個控制點其(x_1, x_2, x_3)座標恰如表(五)所示，也就是這64個控制點分別自出現在表(五)中所示的64個平面，故$(x_1, x_2, x_3) = (0,0,0) \sim (3,3,3)$這64個2維平面上都有控制點出現。

2. 換掉x_3，考慮x_1, x_2, x_4和x_1, x_2, x_5方向的2組64個平面

	00	11	22	33	10	11	12	13	20	21	22	23	30	31	32	33	
x1	00	11	22	33	10	11	12	13	20	21	22	23	30	31	32	33	表
x2	00	11	22	33	10	11	12	13	20	21	22	23	30	31	32	33	八
	00	11	22	33	10	11	12	13	20	21	22	23	30	31	32	33	

每一縱行的數字都相同，每一橫列間的數字都不相同

圖(8)中所挑的64個控制點其中 (x_1, x_2) 兩維度座標如上表(八)所示，因 x_4 在同1方向上的數字都不同，故把 x_4 填入表(八)後形成下表（九），其64格各自出現000～333的相異3元數，數字皆不重複，這說明了這個切割方向上64個2維平面都出現了控制點。相同的表（十）中的64個數字所代表的平面也都出現了控制點。

x1	000	011	023	032	102	113	121	130	203	212	220	231	301	310	322	333	
x2	002	013	021	030	100	111	123	132	201	210	222	233	303	312	320	331	表
x4	001	010	022	033	103	112	120	131	202	213	221	230	300	311	323	332	九
	003	012	020	031	101	110	122	133	200	211	223	232	302	313	321	330	
x1	000	012	021	033	101	113	120	132	202	210	223	231	303	311	322	330	
x2	002	010	023	031	103	111	122	130	200	212	221	233	301	313	320	332	表
x5	001	013	020	032	100	112	121	133	203	211	222	230	302	310	323	331	十
	003	011	022	030	102	110	123	131	201	213	220	232	300	312	321	333	

3. 換掉 x_2 ，考慮 x_1, x_3, x_4 和 x_1, x_3, x_5 方向的2組64個平面

	00	00	00	00	10	10	10	10	20	20	20	20	30	30	30	30	
x1	01	01	01	01	11	11	11	11	21	21	21	21	31	31	31	31	表
x3	02	02	02	02	12	12	12	12	22	22	22	22	32	32	32	32	十一
	03	03	03	03	13	13	13	13	23	23	23	23	33	33	33	33	

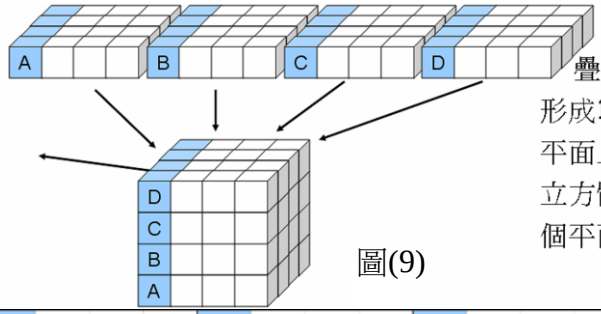
x_4, x_5 皆是同1維度4個數字各自相異的拉丁立方體，分別填入表(十一)後形成下表（十二）、（十三），兩組中64個3元數各自相異。故這2組64個平面上都有控制點出現。

x1	000	001	003	002	102	103	101	100	203	202	200	201	301	300	302	303	
x3	012	013	011	010	110	111	113	112	211	210	212	213	313	312	310	311	表
x4	021	020	022	023	123	122	120	121	222	223	221	220	320	321	323	322	十二
	033	032	030	031	131	130	132	133	230	231	233	232	332	333	331	330	
x1	000	002	001	003	101	103	100	102	202	200	203	201	303	301	302	300	
x3	012	010	013	011	113	111	112	110	210	212	211	213	311	313	310	312	表
x5	021	023	020	022	120	122	121	123	223	221	222	220	322	320	323	321	十三
	033	031	032	030	132	130	133	131	231	233	230	232	330	332	331	333	

4. 換掉 x_1 ，考慮 x_2, x_3, x_4 和 x_2, x_3, x_5 方向2組64個平面

A	B	C	D
00	00	00	00
01	01	01	01
02	02	02	02
03	03	03	03

表十五



圖(9)

疊合4個平面就形成1個立方體，4平面上的4縱行在立方體中也組成1個平面。

	A				B				C				D				
x2	00	10	20	30	00	10	20	30	00	10	20	30	00	10	20	30	表十四
x3	01	11	21	31	01	11	21	31	01	11	21	31	01	11	21	31	
	02	12	22	32	02	12	22	32	02	12	22	32	02	12	22	32	
	03	13	23	33	03	13	23	33	03	13	23	33	03	13	23	33	

表(七)中的 (x_2, x_3) 如表(十四)，將4個平面疊成1個立方體，藍底的4個縱行疊合成1個直立的4×4平面如圖(9)。這個4階方陣中的 (x_2, x_3) 如表(十五)。表(十五)的型態和表(十一)是相同的，所以把 x_4 和 x_5 各自加到表(十五)後在這個直立平面上的16個3位元數也都不重複，圖(9)中藍色位置填出的結果就是000～333如下表(十六)、(十七)，這2組64個平面都有控制點出現其上。

x2	000	101	203	302	002	103	201	300	003	102	200	301	001	100	202	303	表十六
x3	012	113	211	310	010	111	213	312	011	110	212	313	013	112	210	311	
x4	021	120	222	323	023	122	220	321	022	123	221	320	020	121	223	322	
	033	132	230	331	031	130	232	333	030	131	233	332	032	133	231	330	
x2	000	102	201	303	001	103	200	302	002	100	203	301	003	101	202	300	表十七
x3	012	110	213	311	013	111	212	310	010	112	211	313	011	113	210	312	
x5	021	123	220	322	020	122	221	323	023	121	222	320	022	120	223	321	
	033	131	232	330	032	130	233	331	031	133	230	332	030	132	231	333	

5. 同時換上 x_4, x_5，考慮 x_1, x_4, x_5、x_2, x_4, x_5 和 x_3, x_4, x_5 方向3組64個平面

x_4, x_5 在各平面上皆呈正交拉丁方陣，在每平面上16個2元數皆不相同故2元數前方放上1位數字後其3位元數也不會重複如下表。

x1 x4 x5	000	012	031	023	121	133	110	102	232	220	203	211	313	301	322	330	表十八
	022	030	013	001	103	111	132	120	210	202	221	233	331	323	300	312	
	011	003	020	032	130	122	101	113	223	231	212	200	302	310	333	321	
	033	021	002	010	112	100	123	131	201	213	230	222	320	332	311	303	
x2 x4 x5	000	112	231	323	021	133	210	302	032	120	203	311	013	201	322	430	表十九
	022	130	213	301	003	111	232	320	010	102	221	333	031	223	300	412	
	011	103	220	332	030	122	201	313	023	131	212	300	002	210	333	421	
	033	121	202	310	012	100	223	331	001	113	230	322	020	232	311	403	
x3 x4 x5	000	012	031	023	021	033	010	002	032	020	003	011	013	001	022	030	表二十
	122	130	113	101	103	111	132	120	110	102	121	133	131	123	100	112	
	211	203	220	232	230	222	201	213	223	231	212	200	202	210	233	221	
	333	321	302	310	312	300	323	331	301	313	330	322	320	332	311	303	

這說明這3組64個平面上也都出現了控制點

由以上10個方向來觀察，利用拉丁超立方體及正交拉丁方陣的特性讓我們證明了在這10組各64個平面上都出現控制點，所以640個平面都恰只有1個控制點，因此延伸樹間皆不重疊。

(四)控制集點數及延伸樹涵蓋點數乘積證明是完美控制

*1*控制點其延伸樹都能涵蓋16個點，圖*(8)*中64個點的延伸樹最多能涵蓋$16\times 64=4^5$個點，由於其延伸樹都不重疊故共涵蓋了4^5個點，故此64點形成控制集且是完美控制，也解決了4旋鈕5號碼的最小保證開鎖問題。

四、建造拉丁超立方體，構造*5*元*6*維的解

在3元4維及4元5維中發現，完美控制的控制點其最後2維數字上分別呈現拉丁方陣和拉丁立方體，而前面維度的數字呈現10進位數字轉換成3及4進位的結果，所以我們依這2個線索去構造5元6維*5*元*6*維的解。

由*(二.5式)*知5元6維完美控制需要挑5^4個控制點。6維超立方中每個點都是6元座標數，任1點所在的15個平面其名稱恰由6元數中任4個數組合表示。

(一)用*10*進位轉換成*5*進位定出*625*個控制點的前*4*維座標

令$S=\{\ s\mid s$是$0\le s\le 624$的整數$\ \}$，把s換算成5進位數的*4*元數：

令
$$\begin{aligned} x_1(s)&=\text{int}(s\div 125)\\ x_2(s)&=\text{mod}[\text{int}(s\div 25),5]\\ x_3(s)&=\text{mod}[\text{int}(s\div 5),5]\\ x_4(s)&=\text{mod}[s,5]\end{aligned}$$
，int( )是取整數，mod[,5]是指取5進位的同餘數。

相異的10進位數換算成5進位數時也相異，故 $x_1x_2x_3x_4$ 組成的4位元數不會重複。

(二)建構2個拉丁超立方體做為最後2維座標

考慮2維拉丁方陣的特性，其同一方向上各位置的數都要不同，我們可以用 x 和 y 的關係建立拉丁方陣

y \ x	0	1	2
0	$P(x,y)\equiv x+\alpha y \bmod n$		
1			
2			

當x相同時，除非y也相同，不然$p(x,y)$不會相同，這個方法可以建立一個拉丁超立方陣。

在 y 相同時，只有在 $x=x'$ 時 $P(x,y)=P(x',y)$ ，這個方法可以建立1個拉丁方陣[參考文獻四*p.28*]。擴展這個想法到高維度中，我們再令：

$$x_5(s)\equiv x_1+x_2+x_3+x_4 \bmod 5$$
$$x_6(s)\equiv x_1+2x_2+3x_3+4x_4 \bmod 5 \quad ,$$

可知 $x_1(s)\times 5^3+x_2(s)\times 5^2+x_3(s)\times 5^1+x_4(s)=s$ .....(四.1式)

在0 ~ 624中取2數p和q若 $x_a(p)=x_a(q), x_b(p)=x_b(q), x_c(p)=x_c(q), x_d(p)\neq x_d(q)$ 這裏的指標 a,b,c,d 是4個介於1到4的相異整數， 則

$$x_5(p)-x_5(q)\equiv[x_a(p)-x_a(q)+x_b(p)-x_b(q)+x_c(p)-x_c(q)+x_d(p)-x_d(q)]\equiv x_d(p)-x_d(q)\bmod 5$$

故 $x_5(p)-x_5(q)=x_d(p)-x_d(q)+5k$ ， k是整數。又 $x_d(p)-x_d(q)$ 不是5的倍數

$\therefore x_5(p)-x_5(q)\neq 0$ ，這說明了 $x_5(s)$ 是個拉丁超立方體。

同理 $x_6(p)-x_6(q)\equiv d\times[x_d(p)-x_d(q)]\bmod 5=d\times[x_d(p)-x_d(q)]+5h$ ，

$\because \begin{cases} |x_d(p)-x_d(q)| \text{不是5的倍數} \\ (d,5)=1 \quad \text{且} d<5 \end{cases}$ ，$\therefore x_6(p)-x_6(q)\neq 0$ 。說明了 $x_6(s)$ 是個拉丁超立方體。

(三)證明所選的625個控制點都不出現在同一個2維平面上

最後令控制點 $C(s)=(x_1(s),x_2(s),x_3(s),x_4(s),x_5(s),x_6(s))$ ，$\{\ C(s)\mid s\in S\ \}$ 則共選出了625個6維度座標點，很明顯如果編號 $p\neq q$ 則控制點 $C(p)\neq C(q)$ 。

從 S 中選2個編號 p 和 q 比較 $C(p)$ 和 $C(q)$ 的6維度座標，若兩控制點的任4維數字相同代表2個點出現在相同的2維平面上。所以我們要去證明如果 $C(p)$ 和 $C(q)$ 的任4個維度數字相同，則 p 和 q 一定是相同的編號，也就是 $C(p)$ 和 $C(q)$ 是同*1*點。

我們把5元6維的問題分成4類，對這15個方向的所有平面一一檢查：

第*1*類：若$C(p)$和$C(q)$的(x_1,x_2,x_3,x_4)座標相同，

$x_1(p)=x_1(q),x_2(p)=x_2(q),x_3(p)=x_3(q),x_4(p)=x_4(q)$，由*(*四*.1*式*)*可得知

$$p=x_1(p)\times5^3+x_2(p)\times5^2+x_3(p)\times5^1+x_4(p)$$
$$=\mathrm{q}=x_1(q)\times5^3+x_2(q)\times5^2+x_3(q)\times5^1+x_4(q)$$ 。

因此$C(p)$和$C(q)$的(x_1,x_2,x_3,x_4)相同時，則$p=\mathrm{q}$，$C(p)=\mathrm{C(q)}$。

第*2*類：若$C(p)$和$C(q)$的(x_a,x_b,x_c,x_5)座標相同，

$x_a(p)=x_a(q),x_b(p)=x_b(q),x_c(p)=x_c(q),x_5(p)=x_5(q)$。因為

$$\because x_5(p)=x_5(q)$$
$$\therefore x_1(p)+x_2(p)+x_3(p)+x_4(p)\equiv x_1(q)+x_2(q)+x_3(q)+x_4(q)\bmod5$$
$$\Rightarrow x_d(p)\equiv x_d(q)\bmod5$$
$$\Rightarrow x_d(p)-x_d(q)=5\mathrm{k},\mathrm{k}\text{是整數}$$
$$\because \left|x_d(p)-x_d(q)\right|<5$$
$$\therefore \mathrm{k}=0 \quad 。$$
$$\Rightarrow x_d(p)=x_d(q)$$

由*(*四*.1*式*)*得到編號$p=q$。因此點$C(p)$和$C(q)$的(x_a,x_b,x_c,x_5)相同時，則$C(p)=\mathrm{C(q)}$。

第*3*類：假設$C(p)$和$C(q)$的(x_a,x_b,x_c,x_6)座標相同，

$x_a(p)=x_a(q),x_b(p)=x_b(q),x_c(p)=x_c(q),x_6(p)=x_6(q)$，

$$\because x_6(p)=x_6(q)$$
$$\therefore x_1(p)+2x_2(p)+3x_3(p)+4x_4(p)\equiv x_1(q)+2x_2(q)+3x_3(q)+4x_4(q)\bmod5,$$
$$\Rightarrow dx_d(p)\equiv dx_d(q)\bmod5$$
$$\Rightarrow d[x_d(p)-x_d(q)]=5k$$
$$\because \begin{cases}\left|x_d(p)-x_d(q)\right|<5\\ d<5\end{cases} 。$$
$$\therefore x_d(p)=x_d(q)$$

由*(*四*.1*式*)*得到編號$p=q$。因此點$C(p)$和$C(q)$的(x_a,x_b,x_c,x_6)若相同，可得$C(p)=\mathrm{C(q)}$。

第*4*類：假設$C(p)$和$C(q)$的(x_a,x_b,x_5,x_6)座標相同，

$x_a(p)=x_a(q),x_b(p)=x_b(q),x_5(p)=x_5(q),x_6(p)=x_6(q)$，

$$\because x_5(p)=x_5(q),x_6(p)=x_6(q)$$
$$\therefore \begin{cases}x_c(p)+x_d(p)\equiv x_c(q)+x_d(q)\bmod5\\ cx_c(p)+dx_d(p)\equiv cx_c(q)+dx_d(q)\bmod5\end{cases}$$，k、h是整數。
$$\Rightarrow \begin{cases}(c-d)(x_d(p)-x_d(q))\equiv0\bmod5\\ (d-c)(x_c(p)-x_c(q))\equiv0\bmod5\end{cases}$$
$$\Rightarrow \begin{cases}(c-d)[x_d(p)-x_d(q)]=5k\\ (d-c)[x_c(p)-x_c(q)]=5h\end{cases}$$

$$\because \begin{cases} (c-d)\neq 0 \\ |x_d(p)-x_d(q)|<5 \end{cases}$$ ，再由(四.1式)我們得到 $p=q$ 。

$$\therefore x_d(p)=x_d(q), x_c(p)=x_c(q)$$

因此點 $C(p)$ 和 $C(q)$ 的 (x_a, x_b, x_5, x_6) 若相同，它們必為同1控制點。

我們證明了所選的625個點中，任意2個不同控制點都不會出現在同一個2維平面上，所以延伸樹也不會重疊。每棵延伸樹所涵蓋點數是 $6\times 4+1=25$，所選的625個點的延伸樹總共涵蓋了 $25\times 625=5^6$ 個點，因延伸樹不重疊所以這 5^6 個點也相異，因此證明了這625個點蓋滿整個超立方所以是5元6維密碼鎖最小控制集也是完美控制。

五、 當N是質數，構造N元N+1維的完美控制情形

雖然在4元5維和5元6維中都挑出完美控制的控制集，但挑選的方法是不同，4元5維的拉丁立方和正交拉丁方陣比5元6維中的拉丁超立方還要難構造出來，原因是5是質數而4*4*是合數。我們把 $N=5$ 的情況推廣到一般的質數。

當 n 是質數時，

令 $S=\{\ s \mid s$是$0\le s\le n^{n-1}-1$的整數 $\}$，把 s 換算成 n-1位元的 n 進位數，令

$x_1(s)=\text{int}(s\div n^{n-2})$

$x_2(s)=\text{mod}[\text{int}(s\div n^{n-3}), n]$

$x_3(s)=\text{mod}[\text{int}(s\div n^{n-4}), n]$ 。

....

....

$x_{n-1}(s)=\text{mod}[s, n]$

接著再建構2個拉丁超立方

令 $x_n(s)\equiv x_1+x_2+x_3+...+x_{n-1} \bmod n$

$x_{n+1}(s)\equiv x_1+2x_2+3x_3+...+(n-1)x_{n-1} \bmod n$

故 $x_1(s)\times n^{n-2}+x_2(s)\times n^{n-3}+x_3(s)\times n^{n-4}+...+x_{n-1}(s)=s$ .....(五.1式)

定義控制點 $C(s)=(x_1(s), x_2(s), x_3(s),..., x_{n+1}(s))$ ，很明顯如果 $p\neq q$ 則 $C(p)\neq C(q)$ 。

我們要證明若是 $C(p)$ 和 $C(q)$ 的任意 $n-1$ 個維度相同，這兩點必為相同的控制點。

我們分成4類把 C_{n-1}^{n+1} 個方向的平面一一檢查：

第1類：若 $C(p)$ 和 $C(q)$ 的前 $n-1$ 維度相同，

$x_1(p)=x_1(q), x_2(p)=x_2(q), x_3(p)=x_3(q),...x_{n-1}(p)=x_{n-1}(q)$ ，由(五.1式)得 $p=q$ 。因此點 $C(p)$ 和 $C(q)$ 的 $(x_1, x_2, x_3,...x_{n-1})$ 若相同，推得 $C(p)$ 和 $C(q)$ 必為同點。

第2類：若$C(p)$和$C(q)$的$(x_{i_1}, x_{i_2}, x_{i_3}....x_{i_{n-2}}, x_n)$相同，

$x_{i_1}(p)=x_{i_1}(q), x_{i_2}(p)=x_{i_2}(q),...x_{i_{n-2}}(p)=x_{i_{n-2}}(q)$，且$x_n(p)=x_n(q)$，其中

$i_j \in \{1,2,3...n-1\}$，且當$j \neq k$時，指標$i_j \neq i_k$。

$\because x_n(p)=x_n(q)$

$\therefore x_1(p)+x_2(p)+x_3(p)...+x_{n-1}(p)=x_1(q)+x_2(q)+x_3(q)...+x_{n-1}(q)+nK$

$\Rightarrow x_{i_{n-1}}(p)=x_{i_{n-1}}(q)+nK$ ，由(五.1式)得$p=q$。故點$C(p)$和$C(q)$的$(x_{i_1}, x_{i_2}, x_{i_3}....x_{i_{n-2}}, x_n)$若相同，必為同1點。

$\because |x_{i_{n-1}}(p)-x_{i_{n-1}}(q)|<n \Rightarrow K=0$

$\therefore x_{i_{n-1}}(p)=x_{i_{n-1}}(q)$

第3類：若$C(p)$和$C(q)$的$(x_{i_1}, x_{i_2}, x_{i_3}....x_{i_{n-2}}, x_{n+1})$相同，

$x_{i_1}(p)=x_{i_1}(q), x_{i_2}(p)=x_{i_2}(q),...x_{i_{n-2}}(p)=x_{i_{n-2}}(q)$，且$x_{n+1}(p)=x_{n+1}(q)$，其中

$i_j \in \{1,2,3...n-1\}$，且當$j \neq k$時，指標$i_j \neq i_k$。。

$\because x_{n+1}(p)=x_{n+1}(q)$

$\therefore x_1(p)+2x_2(p)+3x_3(p)...+(n-1)x_{n-1}(p)$

$=x_1(q)+2x_2(q)+3x_3(q)...(n-1)x_{n-1}(q)+nK$ ， K是整數，

$\Rightarrow i_{n-1}\times x_{i_{n-1}}(p)=i_{n-1}\times x_{i_{n-1}}(q)+nK$

$\Rightarrow i_{n-1}\times[x_{i_{n-1}}(p)-x_{i_{n-1}}(q)]=nK$

$\because \begin{cases} i_{n-1}<n \\ |x_{i_{n-1}}(p)-x_{i_{n-1}}(q)|<n \end{cases} \Rightarrow K=0$ ，由(五.1式)得到$p=q$。因此點$C(p)$和$C(q)$的

$\therefore x_{i_{n-1}}(p)-x_{i_{n-1}}(q)=0$

$(x_{i_1}, x_{i_2}, x_{i_3}....x_{i_{n-2}}, x_{n+1})$若相同，必為同點。

第4類：若$C(p)$和$C(q)$的$(x_{i_1}, x_{i_2}, x_{i_3}....x_{i_{n-3}}, x_n, x_{n+1})$相同，

$x_{i_1}(p)=x_{i_1}(q), x_{i_2}(p)=x_{i_2}(q),...x_{i_{n-3}}(p)=x_{i_{n-3}}(q), x_n(p)=x_n(q), x_{n+1}(p)=x_{n+1}(q)$，其中$n-3$個指標$i_j \in \{1,2,3...n-1\}$，當$j \neq k$時，指標$i_j \neq i_k$。由

$$\begin{cases} x_{i_{n-2}}(p)+x_{i_{n-1}}(p) \equiv x_{i_{n-2}}(q)+x_{i_{n-1}}(q) \bmod n \\ i_{n-2}\cdot x_{i_{n-2}}(p)+i_{n-1}\cdot x_{i_{n-1}}(p) \equiv i_{n-2}\cdot x_{i_{n-2}}(q)+i_{n-1}\cdot x_{i_{n-1}}(q) \bmod n \end{cases}$$

$$\therefore \begin{cases} (i_{n-2}-i_{n-1})\times[x_{i_{n-1}}(p)-x_{i_{n-1}}(q)] \equiv 0 \bmod n \\ (i_{n-1}-i_{n-2})\times[x_{i_{n-2}}(p)-x_{i_{n-2}}(q)] \equiv 0 \bmod n \end{cases} ,$$

$$\Rightarrow \begin{cases} (i_{n-2}-i_{n-1})\times[x_{i_{n-1}}(p)-x_{i_{n-1}}(q)] \equiv nK \\ (i_{n-1}-i_{n-2})\times[x_{i_{n-2}}(p)-x_{i_{n-2}}(q)] \equiv nH \end{cases}$$

K、H是某個整數

因為 n 是質數所以 $(i_{n-1}-i_{n-2})$ 和 $x_{i_{n-1}}(p)-x_{i_{n-1}}(q)$ 的其中之一應是 n 的倍數，但

$$\because \begin{cases} i_{n-1}-i_{n-2}\neq 0 \\ \left| x_{i_{n-1}}(p)-x_{i_{n-1}}(q) \right| <5 \end{cases} \Rightarrow K=0$$

$$\therefore \begin{cases} x_{i_{n-1}}(p)=x_{i_{n-1}}(q) \\ x_{i_{n-2}}(p)=x_{i_{n-2}}(q) \end{cases}$$

，最後我們由*(五.1式)*得到 $p=q$ ，因此點 $C(p)$ 和 $C(q)$ 的 $(x_{i_1},x_{i_2},x_{i_3}....x_{i_{n-3}},x_n,x_{n+1})$ 若相同，必為同1點。

所以所有相異控制點都不在相同的*2*維平面上，故延伸樹不重疊，而每個延伸樹涵蓋的點數是 $(n+1)(n-1)+1=n^2$ ，所選的 n^{n-1} 個延伸樹總共涵蓋了 $n^{n-1}\times n^2=n^{n+1}$ 個點，因此我們證明了這 n^{n-1} 個點集是 n 元 $n+1$ 維密碼鎖的最小控制集，且是完美控制的情況。

伍、研究結果

一、瑕疵密碼鎖保證打開問題可以對應於超立方體中的控制集問題。 N 是質數時，旋鈕數 $D=N+1$ 且旋鈕上有 N 個號碼的情況時可用拉丁超立方找出 N^{N+1} 中延伸樹不重疊的控制集，稱為「完美控制」，這時最小控制集點數是 N^{N-1} 。

二、在 N 不是質數的時候， 4^5 問題的完美控制也可被找到，此時最小控制集點數是*64*。

三、 N^4 問題中，在 $N=1$ 或 3 以外都沒有完美控制； 2^4 問題的最小控制集數是 4 ， 4^4 問題的最小控制集數介於 $21\sim 32$ 之間； N^4 問題給出

上限公式：

$$\begin{cases} \text{N是偶數時：}[(\frac{\text{N}}{2})^2+(\frac{\text{N}}{2})^2]\times \text{N} \\ \text{N是奇數時：}[(\frac{\text{N}+1}{\text{N}})^2+(\frac{\text{N}-1}{\text{N}})^2]\times \text{N} \end{cases} \quad .....(\text{二.3 式})$$

下限公式：$\frac{n^4}{4n-3}$ .....(二.4 式)。

四、 N^D 超立方中完美控制的必要條件為 $\frac{N^D}{(N-1)\times D+1}=N^K, K$ 是正整數；當 $D=N+1$ 時最小控制集點數 $N^K=N^{N-1}$ ，延伸樹涵蓋點數 $(N-1)\times \text{D}+1=N^2$ 。

五、*Cartesian prodcut* 可以把 N^D 超立方分割成較小維度的集合以適合分析，而拉丁超立方的方法也可把 N^{N+1} 也以分割成不重疊的 N^{N-1} 個集合。

陸、 討論

一、在2維平面中畫3維立方體時，我們自小已經學會辨認哪些線條是真的有交點哪些是視覺上的誤差，但在2維平面上畫4維的圖形時線條交錯的誤差辨認起來就麻煩多了，所以把維度高的超立體切割成2維平面是個很好的分析方法。要把4維超立方切成表(一)這個想法我們想了很久，靈感是我們能把3維切成2維平面當然也能把4維分割成2維平面，老師說就是善用 *Cartesian prodcut* 的概念。有了這個想法，高維度的超立方體就不會那麼抽象了，我們也才能夠在高維度的問題中找到分析的起點，發現了3^4問題中的完美控制。

二、拉丁方陣的概念很簡單，但是要用數字或函數去表達一個拉丁方陣就不是那麼容易了，就好像數獨遊戲，規則很容易了解但解法卻不是很好用文字表達，所以本篇報告我們用了很多圖形來表達我們要說明的概念，但即使用了圖形，仍然需要使用「同餘數」來寫出我們要選的控制點，在N^{N+1}所使用的拉丁超立方挑選最小控制集時，也受限於係數與N的互質關係；當試圖把結果推向N是質數以外的情況，很明顯的並不成功，因為各項係數除了要和N互質之外，係數兩兩相減也要和N互質，假設說N是合數而它質因數分解後最小的質因數是α，我們最多只能找到$\alpha-1$個正整數它們兩兩相減後和α互質。因此我們需要用別的方法來建造當N不是質數時的拉丁超立方才能用來解決我們的題目。$N=4$時我們用*2*維平面模型去找到可以用的拉丁超立方，但它就很不容易找到而且也不是後來N是質數時的那種型的函數。

三、在4維度的問題中，我們提到4維度沒有像3維那樣型態的公式，主要也是受限於我們對3次方程式的認識，我們說明沒有像3維類型的公式，還沒能力進一步的證明這類公式不存在，所以只能找到4維問題的最小控制集的上下限。在3維時我們證明完美控制只在$N=1$或2時發生，但高次方的多項式函數的因式問題我們不太會證明，在討論1.6式時只知道$N=1$及$N=D-1$會使得$(N-1)\times D+1$是N^D的因數，如果能證明除了上面以外沒有其它正整數解，等於說明了只有在$N=1$和D-1時，D維超立方密碼鎖才會有完美控制的情況。

四、在N是質數時證明完美控制的過程中，沒有提及最後2維度的超立方體要在各平面中形成正交拉丁方陣，其實它們仍形成正交拉丁方陣，只是在我們的問題中證明的過程不需要強調正交的特性。但是在$N=4$時所用的證明方法卻需要借助正交的特性才好說明。

柒、結論、心得與展望

一、 N是質數或$N=4$時可構造並證明N元$N+1$維的密碼鎖問題會出現完美控制的情況。

二、延伸樹不重疊必須要每個2維平面都只能有1個控制點。我們能由數獨遊戲中發現，建構拉丁方陣的方法可以在每個2維平面挑選1個控制點，經由鴿籠原理，我們把各控制點在所有2維平面中出現的次數加總，除以2維平面的總數，得到所有的2維平面恰有1個控制點，也就是達成延伸樹之間不重疊。最後由每個控制點延伸樹能涵蓋的數目，乘上控制點數來證明所選的是個完美控制的控制集。

三、在 N 是質數時建構2個 N 元 $N+1$ 維拉丁超立方的方法我們已經找到了，所以能證明到其完美控制，但是除了已經有做出 $N=4$ 的例子， N 不是質數時的一般性的拉丁超立方體我們還不會建構，若是能成功建構質數以外的拉丁超立方體，我們就能直接證明任意 N 元 $N+1$ 維的完美控制情況，這也是我們將來的目標。

四、完美控制下的延伸樹彼此不重疊，也就是說我們找到了用拉丁超立方的方法把 N 元 $N+1$ 維超立方體分割成 N^{N-1} 個彼此互斥的部份，而每一部份都由1個樞紐點(控制點)相連。在看參考資料時也看到一些在超立方體上討論漢彌頓迴圈的問題，主要是在討論「在某些節點或邊不能相通時如何在超立方體中找到一個路徑把所有點都連接」，這個讓人覺得很有挑戰性，所以我們也希望能再朝漢彌頓迴圈再去研究。

五、我們討論的密碼鎖問題是指*1*個維度錯誤仍能打開的情況，那如果條件改成*2*個維度錯誤仍能打開呢?如果仍以「完美控制」的角度切入時目前只發現 2^6 問題中有完美控制的情況，而其它的情況還沒有進一步的了解。

六、4維問題中我們尚無法找到一個最小控制集公式，但可以由*Cartesian prodcut* 來理解3維和4維的關係，所以得到最小控制集數的上限公式*(二.3式)*，又從延伸樹的有效涵蓋的觀念中得到最小控制集數的上限公式*(二.4式)*。只是上、下限公式之間的範圍還很大並不優秀，我們應該再學習寫電腦程式去找到一些4維度的問題的控制集，來再把4維度的問題解決得更好。相同的方法我們也可對其它維度做出上、下限的控制集點數公式，但仍因為沒有把範圍逼近的很好故公式並沒有列出。

七、 在做這份科展時老師一直讓我們練習去發現問題的特性、實驗一些例子後去驗證我們的猜想、再去構思想證明的現象如何用數學的方法組織和列式、找到數學的工具來證明我們的推測。每一個小節進行中遇到困難時我們就要回來想一想這個步驟，最後我們找到了一部份我們想知的答案也學到很多思考的方法、表達的方法、證明的寫法。我們發現數學不只是計算，反而感受到了數學和許多現實世界中問題是如此有關連。

捌、參考資料及其它

一、李佳晉、藍唯倫、徐書強、鄭博升/ 超立方體*Qn*之最小控制/ 第四十八屆全國中小學科

學展覽

二、蘇銓閔、吳宗翰、陳慶瑜、許祖兒/ 正方體密碼解 /四十九屆台南縣中小學科學展覽

三、陳冠儒、翁翠微、伍蕙萱、陳冠霖/ 密碼鎖/ 第四十三屆全國中小學科學展覽

四、*Jerzy Wojdyo/ Latin Squares, Cubes and Hypercubes/ Southeast Missouri State University March 31, 200*

【評語】030421

從一國際奧林匹克數學競賽題目出發，研究號碼鎖，涉及不少組合及鴿籠原理等知識，作品有相當的創意及挑戰性，但皆能仔細的處理，討論的範圍還涵蓋 4 維，且知將 4 維想成 3 維再結合 1 維的結果。作品中對所謂控制集及完美控制，討論完整，值得肯定。