

中華民國第四十三屆中小學科學展覽會參展作品專輯

國中組

數學科

科別：數學科

組別：國中組

作品名稱：密碼鎖

關鍵詞：二次函數、配方法

編號：030410

學校名稱：

台北市私立復興國民中學

作者姓名：

陳冠儒、翁翠微、伍蕙萱、陳冠霖

指導老師：

陳俊佑



摘要

一個有 3 個旋鈕，每個位置的號碼數分別是 a 、 b 、 c 的密碼鎖，如果有兩個位置的數字正確就能打開，最少需要猜多少次才能保證打開這個鎖。我們的研究，依照鎖三個位置的號碼數分成： $a = b = c = n$ 、 $a = b < c$ ， $a = b > c$ 和 $a > b > c$ 四個部份。前兩部份的研究已經找到最少次數開鎖的方法，後兩部份則是給了一個演算法可求出開鎖次數的上界。

壹、研究動機

有一次出國時，由於忘記行李箱上鎖的密碼，只好一個一個慢慢試，試了近一千次後終於打開了。那時突發奇想：如果只要兩個位置對了就可打開的話，那就只要試一百次。回到學校問老師有沒有更快的方法。老師說其實只要五十次就可以了。而且跟國中數學第四冊第一章，二次函數的最大值和最小值有關。我們覺得很好奇，就決定對此問題作進一步研究。

貳、研究目的

一個有 3 個旋鈕的密碼鎖各位置的號碼數分別是 a 、 b 、 c ，如果有兩個位置的數字正確就能打開，研究下面的問題

- 一、 $a = b = c = 10$ ，如何 50 次就能打開。
- 二、 $a = b = c = n$ 時，最少嘗試次數是多少，及如何在最少次可以打開。
- 三、 $a = b < c$ 時，最少嘗試次數是多少，如何在最少次可以打開。
- 四、 $a = b > c$ 時，最少嘗試次數是多少，如何在最少次可以打開。
- 五、 $a > b > c$ 時，最少嘗試次數是多少，如何在最少次可以打開。

參、文獻探討

1988 年國際奧林匹克數學競賽，東德提供了一題預選題題目如下：一個保險櫃上的鎖由三個旋鈕組成，每個旋鈕有 8 種不同的位置(號碼)。由於保險櫃構造上的缺點，三個旋鈕中只要有兩個在正確位置時，櫃門即被打開。問至少嘗試多少次組合，才能保證門一定被打開(假定不知道“正確的組合”)，一種試 32 次可以打開的解為 (1,1,1), (1,2,4), (1,3,3), (1,4,2), (2,1,2), (2,2,1), (2,3,4), (2,4,3), (3,1,3), (3,2,2), (3,3,1), (3,4,4), (4,1,4), (4,2,3), (4,3,2), (4,4,1); (5,5,5), (5,6,8), (5,7,7), (5,8,6), (6,5,6), (6,6,5), (6,7,8), (6,8,7), (7,5,7), (7,6,6), (7,7,5), (7,8,8), (8,5,8), (8,6,7), (8,7,6), (8,8,5)。文章中並且證明如果只試 31 次，無法保證必能打開。

肆、研究器材

正方體積木、方格紙、C++ 語言

伍、符號定義

- 一、若有一個密碼鎖，所有三個旋鈕，每個位置的號碼分別為 $1 \sim a$ 、 $1 \sim b$ 、 $1 \sim c$ ， a, b, c 為正整數。我們用 $a \times b \times c$ 代表這一個鎖，則這個鎖所有可能號碼組合 $L = \{ (x, y, z) \mid 1 \leq x \leq a, 1 \leq y \leq b, 1 \leq z \leq c; x, y, z \in N \}$ 。也因為如此，這個鎖也可看成一個邊長分別 a, b, c 之長方體被切割成 $a \times b \times c$ 個單位正方體，每一個單位正方體的座標為 (x, y, z) ，恰對應了一種密碼鎖可能的號碼，其中 $1 \leq x \leq a, 1 \leq y \leq b, 1 \leq z \leq c; x, y, z \in N$ ，則 $a \times b \times c$ 也用來代表 L 這個集合。
- 二、當我們試了某個號碼，不失一般性的假設試的號碼為 $(1,1,1)$ ，若原先的密碼為 $(1,1,t)$ 、 $(1,t,1)$ 或 $(t,1,1)$ ，都是可被打開的。從 L 的幾何圖形來看，當成先把座標 $(1,1,1)$ 的正方體塗成黑格，再從 $(1,1,1)$ 這個黑格往 X 、 Y 、 Z 三個方向各延伸出一條線段，這三條線所覆蓋的正方體的座標恰是猜 $(1,1,1)$ 可以打的開號碼。我們的目標就是找出放若干個黑格，使得這些黑格及延伸的直線可完全覆蓋大長方體。
- 三、 S 是一個 $a \times b \times c$ 的子集合， S 中每個元素所對應的正方體及其延伸的直線可完全覆蓋 $a \times b \times c$ 的長方體，則說 S 是我們要找的解。而我們只要試完 S 裡面所有的號碼組

合，也就是試 $|S|$ 次，就保證可開 $a \times b \times c$ 這個鎖。要求 $a \times b \times c$ 的最快開鎖，亦即求最小的解集合。我們定義函數 $f(a, b, c) = \min\{|S|\}$

四、除了用積木幫忙找解之外，我們也利用方格紙幫我們研究。找 $a \times b \times c$ 的解是畫出 c 個 $a \times b$ 的長方形共有 c 層。此時的原則如下：若 $a = b$ ，則畫 c 個邊長 a 的正方形；若 a 、 b 、 c 三數皆不相同，則取三者最小的為 c 。此時的黑格改用「○」標記，「×」則用來標記該格已經被某個黑格(「○」)所延伸的直線所覆蓋。但一個格子若是與某一「○」同一層，而被水平的縱向或橫向延伸的直線覆蓋時，為了板面乾淨可讀，我們通常不加以標記。

陸、研究過程及結果

我們的研究共分四個部份，第一個部份是先解決三個位置都相同，即 $a = b = c = n$ 的情況；再研究 $a = b < c$ 的情況和 $a = b > c$ 的情況；最後探討三個位置數量皆不同的情況。

一、密碼鎖三個位置數字一樣的情況 ($a = b = c = n$)

$$\text{定理 1. } f(n, n, n) = \begin{cases} \left(\frac{n}{2}\right)^2 + \left(\frac{n}{2}\right)^2 = \frac{n^2}{2} & n \text{ 是偶數} \\ \left(\frac{n+1}{2}\right)^2 + \left(\frac{n-1}{2}\right)^2 = \frac{n^2+1}{2} & n \text{ 是奇數} \end{cases}$$

(一) 解的構造

1. 三叉體

在文獻中所給定的解可以分成兩部份，一部份的數字都是介於 1 到 4 之間，另一部份的數字都是介於 5 到 8 之間，把這兩部份的解及

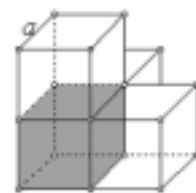


圖 1

其所覆蓋的部份來看，分別都是一個邊長為 4 的**三叉體**。這裡所謂**邊長為 a 的三叉體**是指一個由四個邊長 a 的正方體所組成的立體物件，如圖 1，三個方向上的截面積都是 a^2 ，也就是每一個方向各有 a^2 條直線。而陰影的部份是一個邊長為 a 的正方體。



圖 2

再把兩個邊長為 a 的三叉體如圖 2 所示那樣拼起來，就可以得到一

個邊長為 $2a$ 正方體。因此只要對每一個三叉體求解，也就可以對正方體求解。

1. 三叉體的解

欲覆蓋如圖 1 的三叉體的的所有的小正方體，我們先證明至少放 a^2 個黑格，才能達到，再給一種方法，使得只放 a^2 個黑格就可以達成目的。

因為每個黑格可在三個方向各有一條延伸線，截面為 a^2 的三叉體需要 $3a^2$ 條延伸線來覆蓋，故至少需 $\frac{3a^2}{3} = a^2$ 個黑格。

因為要覆蓋邊長 a 的三叉體，故在三個方向投影均要有 a^2 個。考慮陰影部份的正方體，它的邊長為 a ，若有 a^2 個黑格，則每層恰可有 a 個。如此可用如圖 3 的方式構造解。第一層黑格放在對角線，每往上一層，黑格子的位置就往右移一格；若原本已在最右邊，則移到最左邊，如此， a^2 個黑格確實可覆蓋截面積為 a^2 的三叉體。對應的號碼為： $\{(1,1,1)、(2,2,1)、(3,3,1)、\dots、(a,a,1)；(2,1,2)、(3,2,2)、(4,3,2)、\dots、(a, a-1, 2)、(1, a, 2)；\dots、(a,1,a)、(1,2,a)、(2,3,a)、\dots、(a-2, a-1, a)、(a-1, a, a)\}$ 。如此就能在三個方向都有 a^2 條延伸線，也就能覆蓋邊長 a 的三叉體。

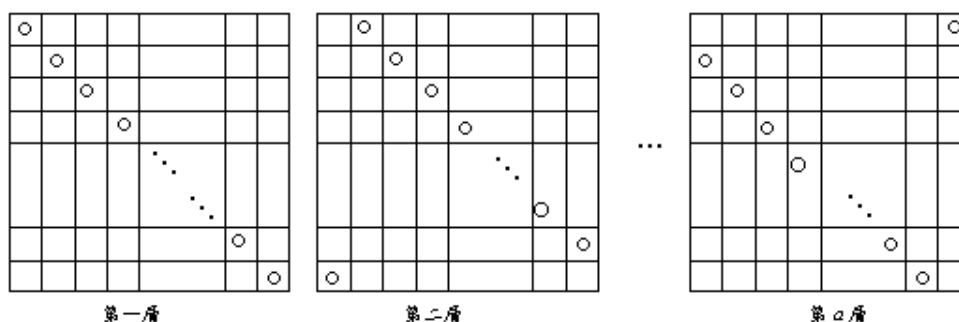


圖 3

2. 正方體的解

從圖 2 知道，邊長為 n 的正方體的解，可以是兩個邊長分別為 a 和 b 的三叉體的解的聯集，其中 $a+b=n$ 。此時解的元素個數為 a^2+b^2 。要注意的是第二個三叉體的解的編排，可以從仿照第一個三叉體的編排方式。但因為第一個三叉體是位於右下角，第二個三叉體是位於左上角，第二個三叉體的號碼需經過轉換， (i, j, k) 會對應到 $(n+1-i, n+1-j, n+1-k)$ 。

若要求正方體解集合的元素個數最少，等於是在 $a+b=n$ 的條件下，求 a^2+b^2 之最小值，此時可應用國中課程第四冊所介紹的二次函數配方法求得。

已知 $a+b=n \Rightarrow b=n-a$ ，

$$a^2 + b^2 = a^2 + (n-a)^2 = a^2 + n^2 - 2na + a^2 = 2a^2 - 2na + n^2 = 2\left(a - \frac{n}{2}\right)^2 + \frac{n^2}{2}$$

當 n 為偶數， $a = \frac{n}{2}$ ， $a^2 + b^2$ 有最小值 $\frac{n^2}{2}$ 。

當 n 為奇數， $a = \frac{n+1}{2}$ 或 $\frac{n-1}{2}$ ， $a^2 + b^2$ 之最小值為 $\left(\frac{n+1}{2}\right)^2 + \left(\frac{n-1}{2}\right)^2 = \frac{n^2 + 1}{2}$ 。

1. 50 次開 $10 \times 10 \times 10$ 的鎖

回到最一開始的問題，現在我們知道要開 $10 \times 10 \times 10$ 的鎖，試 $5^2 + 5^2 = 50$ 次是可以成功的，其中一組可行的號碼如下：

(1,1,1)、(2,2,1)、(3,3,1)、(4,4,1)、(5,5,1)、(1,2,2)、(2,3,2)、(3,4,2)、(4,5,2)、(5,1,2)、
(1,3,3)、(2,4,3)、(3,5,3)、(4,1,3)、(5,2,3)、(1,4,4)、(2,5,4)、(3,1,4)、(4,2,4)、(5,3,4)、
(1,5,5)、(2,1,5)、(3,2,5)、(4,3,5)、(5,4,5)；和
(10,10,10)、(9,9,10)、(8,8,10)、(7,7,10)、(6,6,10)、(10,9,9)、(9,8,9)、(8,7,9)、(7,6,9)、
(6,10,9)、(10,8,8)、(9,7,8)、(8,6,8)、(7,10,8)、(6,9,8)、(10,7,7)、(9,6,7)、(8,10,7)、(7,9,7)、
(6,8,7)、(10,6,6)、(9,10,6)、(8,9,6)、(7,8,6)、(6,7,6)。

(二) 證明解是最佳化

依照 n 的奇偶數，我們分別證明解元素的個數不可能更少。

1. n 是偶數的情況

設 $n = 2k$ ，要證明 $f(n, n, n) = \frac{n^2}{2} = 2k^2$ ，等於要說明如果只用 $\frac{n^2}{2} - 1 = 2k^2 - 1$ 個黑格，不可能覆蓋邊長 n 的正方體。

(1) 任一大小為 $2k^2 - 1$ 之 L 的子集合 S ，考慮 S 中元素的分佈： $\left\lfloor \frac{2k^2 - 1}{2k} \right\rfloor = k$

$- 1$ ，黑格數最少的那一層，最多只有 $k - 1$ 個黑格，且該層至少會剩下 $(k + 1)^2$ 個正方體需別層上下覆蓋。

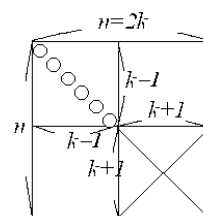


圖 4

- (1) 設黑格數最少的是第一層。這一層和邊長 n 的正方體就被分成：A、B、C、D 四區，如圖 4 和圖 5 所示。A 區是邊長 $(k-1) \times (k-1) \times 2k$ 的長方體，它的第一層擺了 $(k-1)$ 個「○」，D 區是 $(k+1) \times (k+1) \times 2k$ 的長方體，這區在某些層共有 $(k+1)^2$ 個黑格，去上下覆蓋第一層的 D 區；而不管這 $(k+1)^2$ 個黑格怎樣分佈，D 區都完全被覆蓋了。這時還剩下 $k^2 - 3k - 1$ 個黑格。

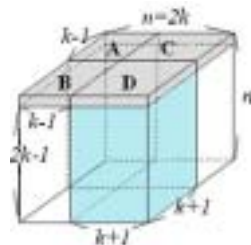


圖 5

- (2) 若在 D 區的 $(k+1)^2$ 黑格能覆蓋 B 區和 C 區的 $k+1$ 層時，所以 B 區還有 $(k-1)(k-2)$ 個直排，C 區至少還有 $(k-1)(k-2)$ 個橫排尚未被覆蓋。
- (3) 能在 B 區蓋住一排直排，也在 C 區蓋住一排橫排；如果在 B 區放一個黑格，則能蓋住 B 區的 $\frac{2k-1}{k+1}$ 個直排，但完全蓋不到 C 區；對稱的來說，黑格放在 C 區的效果跟放在 B 區是一樣的。因此，不管在哪邊放一個黑格最多在 B 區和 C 區共蓋到 2 排，只剩 $k^2 - 3k - 1$ 個黑格是沒法蓋完 B 區和 C 區的。

2. n 是奇數的情況

設 $n = 2k + 1$ 。要證明 $f(n, n, n) = \frac{n^2 + 1}{2} = 2k^2 + 2k + 1$ ，等於需要證明如果只有 $\frac{n^2 + 1}{2} - 1 = 2k^2 + 2k$ 個黑格，不可能覆蓋邊長 n 的正方體。

- (1) 任一大小為 $2k^2 + 2k$ 之 L 的子集合 S ，考慮 S 的分佈： $\left\lfloor \frac{2k^2 + 2k}{2k + 1} \right\rfloor = k$ ，最少的一層最多只有 k 個黑格，該層至少會剩下 $(k+1)^2$ 個正方體需要別層上下覆蓋。

- (2) 這一層和邊長 n 的正方體就被分成：A、B、C、D 四區，

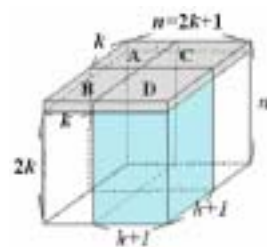


圖 7

如圖 6 和圖 7 所示。其中 A 區是邊長 $k \times k \times (2k + 1)$ 的長方體，它的第一層擺了 k 個「○」，D 區是一個 $(k + 1) \times (k + 1) \times (2k + 1)$ 的長方體，在這區某些層有某些層共有 $(k + 1)^2$ 個黑格，去上下覆蓋第一層的 D 區；而不管這 $(k + 1)^2$ 個黑格怎樣分佈，D 區都完全被覆蓋了。這時還剩下 $k^2 - k - 1$ 個黑格。

(3) 若在 D 區的 $(k + 1)^2$ 黑格有效覆蓋 B 區和 C 區時，B 區仍至少還有 $k \times (k - 1)$ 個直排、C 區也至少還有 $k \times (k - 1)$ 個橫排尚未被覆蓋。

(4) 這時在 A 區放一個黑格能在 B 區蓋住一排直排、也在 C 區蓋住一排橫排；如果在 B 區放一個黑格，則能蓋住 B 區的 $\frac{2k}{k+1}$ 個直排，但完全蓋不到 C 區；對稱的來說，黑格放在 C 區的效果跟放在 B 區是一樣的。因此，不管在哪邊放一個黑格最多在 B 區和 C 區共蓋到 2 排，只剩下 $k^2 - k - 1$ 個黑格是沒法蓋完 B 區和 C 區的。

二、密碼鎖三個位置數字為 $a = b < c$ 的情況

對於這個部份的研究，我們是先對 $(3,3,4) \sim (3,3,8)$ 及 $(4,4,5) \sim (4,4,8)$ 幾個例子去找解，對結果有了一些猜想，最後也證明了猜想是對的。設 $a = b = n$ ， $c = n + k$ ； n 、 k 皆為正整數，則這個結果是這樣的：

定理 2 $f(n, n, n + k) = \min \{s^2 + t^2 + sk \mid s + t = n; t \geq s \geq 0; s, t \in \mathbb{Z}, k \in \mathbb{N}\}.$

當 $k \geq 2n - 2$ ，也就是當 $c \geq 3a - 2$ 時， $f(a, a, c) = a^2$ 。

我們先用 $n=6$ 的例子來說明這個定理。

一個邊長 6 的正方體，是由兩個邊長分別為 s 、 t 的三叉體所組成，則數對 (s, t) 的可能有 3 種： $(3,3)$ 、 $(2,4)$ 、 $(1,5)$ 。表 1 就是對這三種可能，隨著 k 的增加，把 $s^2 + t^2 + sk$ 的值算出來。有底色的部份就是三種可能中較小的，也就是我們所定義的 $f(n, n, n+k)$ ，廣義來說 $(0,6)$ 也可以看成第 4 種，只是 $(0,6)$ 的這一組，不管 k 的值是多少， $s^2 + t^2 + sk$ 的值都是 36。也就是當 k 大於等於 10 時，我們只要試完前兩碼的 36 種可能就好。

	$n=6$		
	$(s, t)=(3,3)$	$(s, t)=(2,4)$	$(s, t)=(1,5)$
$k=0$	$3^2+3^2=18$	$2^2+4^2=20$	$1^2+5^2=26$
$k=1$	$18+3=21$	$20+2=22$	$26+1=27$
$k=2$	$21+3=24$	$22+2=24$	$27+1=28$
$k=3$	$24+3=27$	$24+2=26$	$28+1=29$
$k=4$		$26+2=28$	$29+1=30$
$k=5$		$28+2=30$	$30+1=31$
$k=6$		$30+2=32$	$31+1=32$
$k=7$		$32+2=34$	$32+1=33$
$k=8$			$33+1=34$
$k=9$			$34+1=35$
$k=10$			$35+1=36$
$k=11$			36

表 1

這個例子，可以約略的看出我們如何構造解。因此我們先說明如何構造解 S ，再說明解 S 的大小不可再減少，也就是證明定理 2 是對的。



圖 8

(一) 構造解

從定理 1 我們知道，當 $s+t=n$ ，一個 $n \times n \times n$ 的正方體，可由兩個邊長分別為 s 、 t 的三叉體組合而成（這邊我們假設 $s \geq t$ ），而這個正方體往某一方向多了 k 層變成 $n \times n \times (n+k)$ 的長方體。原先兩個三叉體的黑格的延伸線也會延長。如圖 8 所展現的是兩個邊長分別為 3 的三叉體的組合，往 Z 方向延伸一層後，可以看到共有 18 條線也跟著延伸而一層。留下尚未覆蓋的部分，每一層只需再放 3 個黑格，就可以覆蓋因為延伸而剩下的空格。一般的情況就是一層只需 s 個黑格，故 k 層只需 $s \times k$ 個黑格，即可覆蓋 $n \times n \times (n+k)$ 之長方體。

(二) 證明解個數不會更少

設 $n \times n \times (n+k)$ 之解為 S , $f(n, n, n+k) = |S| = m$ 。

1. 設第一層有最少的黑格，有 s 個。令 $t = n - s$ ，則該層至少有一邊長為 t 之正方形，也就是有 t^2 個正方體需靠別層上下覆蓋。如圖 9。

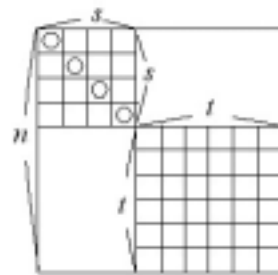


圖 9

2. D 區為 $t \times t \times (n+k)$ 之長方體，已完全被覆蓋。現計算還需放幾個黑格，使得 B、C 各層(第 2 至 $n+k$ 層)得可完全被覆蓋。B、C 兩區未覆蓋的正方體數為 $2st(n+k-1) - 2st^2 = 2st(s+k-1)$ 。每多猜測一次，也就是多放一個黑格在 A 區，至多能在 B、C 兩區多覆蓋 $2t$ 個或 $s+t-1$ 個正方體，但因 $t > s (s \leq \frac{n}{2} \leq t)$ ，故多猜測一次至多能再有效會多蓋 $2t$ 個正方體，可推得至少要再猜 $\frac{2st(s+k-1)}{2t} = s(s+k-1)$ 次。由 1、2 知， $|S| \geq s + t^2 + s^2 + sk - s = s^2 + t^2 + sk$ 。如此就證完定理 2。

3. 將 $t = n - s$ 代入上式可得

$$|S| \geq s^2 + (n-s)^2 + sk = 2s^2 - s(2n-k) + n^2$$

(也就是當 k 固定時， $|S|$ 的最小值時也是 s 的二次函數)，配方後得

$$= 2\left(s - \frac{(2n-k)}{4}\right)^2 + \frac{4n^2 + 4nk - k^2}{8}$$

4. 為了得到函數的最小值，且 s 是正整數，因此 s 是最接近 $\frac{2n-k}{4}$ 的整數。這也是為什麼當 $k=2n-2$ 時， s 取 0 或 1 得到的函數值是一樣，都是 n^2 。而當 $k \leq 2n-2$ 時，因為 s 必需是正整數的原因，所以取 $s=0$ ，會得到 $|S| = n^2$ 。
5. 完整的結果如下頁的表 2。

	$n = 2m$		$n = 2m + 1$	
	s	$ S $	s	$ S $
$k = 0$	$\frac{4m}{4} = m$	$2m^2$	$\frac{4m+2}{4} \Rightarrow \begin{cases} m+1 \\ m \end{cases}$	$2m^2 + 2m + 1$
$k = 1$	$\frac{4m-1}{4} \Rightarrow a = m$	$2m^2 + m$	$\frac{4m+1}{4} \Rightarrow m$	$2m^2 + 3m + 1$
$k = 2$	$\frac{4m-2}{4} \Rightarrow \begin{cases} m \\ m-1 \end{cases}$	$2m^2 + 2m$	$\frac{4m}{4} \Rightarrow m$	$2m^2 + 4m + 1$
$k = 3$	$\frac{4m-3}{4} \Rightarrow m-1$	$2m^2 + 3m - 1$	$\frac{4m-1}{4} \Rightarrow m$	$2m^2 + 5m + 1$
$k = 4$	$\frac{4m-4}{4} \Rightarrow m-1$	$2m^2 + 4m - 2$	$\frac{4m-2}{4} \Rightarrow \begin{cases} m \\ m-1 \end{cases}$	$2m^2 + 6m + 1$
$k = 5$	$\frac{4m-5}{4} \Rightarrow m-1$	$2m^2 + 5m - 3$	$\frac{4m-3}{4} \Rightarrow m-1$	$2m^2 + 7m$
$k = 6$	$\frac{4m-6}{4} \Rightarrow \begin{cases} m-1 \\ m-2 \end{cases}$	$2m^2 + 6m - 4$	$\frac{4m-4}{4} \Rightarrow m-1$	$2m^2 + 8m - 1$
$k = 7$	$\frac{4m-7}{4} \Rightarrow m-2$	$2m^2 + 7m - 6$	$\frac{4m-5}{4} \Rightarrow m-1$	$2m^2 + 9m - 2$
$k = 8$	$\frac{4m-8}{4} \Rightarrow m-2$	$2m^2 + 8m - 8$	$\frac{4m-6}{4} \Rightarrow \begin{cases} m-1 \\ m-2 \end{cases}$	$2m^2 + 10m - 3$
$k = 9$	$\frac{4m-9}{4} \Rightarrow m-2$	$2m^2 + 9m - 10$	$\frac{4m-7}{4} \Rightarrow m-2$	$2m^2 + 11m - 5$
$k = 10$	$\frac{4m-10}{4} \Rightarrow \begin{cases} m-2 \\ m-3 \end{cases}$	$2m^2 + 10m - 12$	$\frac{4m-8}{4} \Rightarrow m-2$	$2m^2 + 12m - 6$
$\mathbb{N}$	$\mathbb{N}$	$\mathbb{N}$	$\mathbb{N}$	$\mathbb{N}$
$k = 2n-5$	$5/4 \Rightarrow s = 1$	$4m^2 - 3$	$5/4 \Rightarrow s = 1$	$4m^2 + 4m - 2$
$k = 2n-4$	$4/4 \Rightarrow s = 1$	$4m^2 - 2$	$4/4 \Rightarrow s = 1$	$4m^2 + 4m - 1$
$k = 2n-3$	$3/4 \Rightarrow s = 1$	$4m^2 - 1$	$3/4 \Rightarrow s = 1$	$4m^2 + 4m$
$k = 2n-2$	$2/4 \Rightarrow s = 0, 1$	$4m^2 = n^2$	$2/4 \Rightarrow s = 0, 1$	$4m^2 + 4m + 1 = n^2$
$k = 2n-1$	$1/4 \Rightarrow s = 0$	$4m^2 = n^2$	$1/4 \Rightarrow s = 0$	$4m^2 + 4m + 1 = n^2$

表 2

三、密碼鎖三個位置數字為 $a = b = n > c$ 的情況

(一) $c = 2$ 的情況：

當 $n \geq 2$, $f(n, n, 2) = 2(n - 1)$

證明：只猜 $2n - 3$ 次不保證能開 $n \times n \times 2$ 的鎖。

任意大小為 $2n - 3$ 之 L 的子集合 S ，因

$$\left\lfloor \frac{2n-3}{2} \right\rfloor = n-2, \text{ 也就是說較少那層最多只有 } n-2$$

個黑格，如圖 10，則這一層還有 4 格需另一層覆蓋。此時只剩下 $n - 5$ 個黑格可放在第二層，這 $n - 5$ 個黑格可縱向(或橫向)覆蓋 $n - 5$ 行(或列)，這時還有 3 行(或列)需要覆蓋，考慮第一層 $n - 2$ 個黑格的上下覆蓋，及第二層的橫向覆蓋 $n - 5$ 個，總共最多還蓋不滿 2 行，故用 $n - 5$ 個蓋不滿 $(n - 2) \times (n - 2)$ 的正方形。如此證明了也就是 $f(n, n, 2) > 2n - 3$ 。

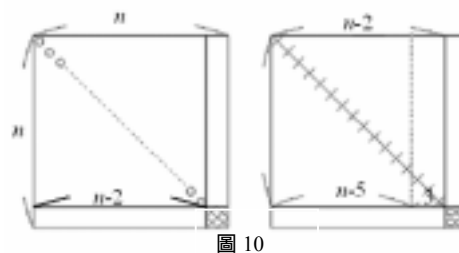


圖 10

(二) $c = 3$ 的情況：

$f(4, 4, 3) = 8$ ，因為試 8 次可以開 $4 \times 4 \times 3$ 的鎖，所以只需要證明只猜 7 次不一定能打開 $4 \times 4 \times 3$ 鎖。

若只有 7 個黑格，因為 $\left\lceil \frac{7}{3} \right\rceil = 3$ ，最少那一層只有兩個，如圖 11。設第一層放了兩個以後，剩下四格時用上下覆蓋，此時還有 $7 - 2 - 4 = 1$ 個黑格，還有兩層各有一個 2×2 的正方形，但只剩下一個黑格，必有一層不夠蓋。



圖 11

$f(5, 5, 3) = 10$ ，先證明只有 9 個黑格不行覆蓋 $5 \times 5 \times 3$ 的長方體。

因為 $\left\lceil \frac{9}{3} \right\rceil = 3$ ，九個黑格分 3 層，最少的一層最多只有三個黑格，如圖 12，這一層還剩 4 格要另外兩層上下覆蓋。此時還有 $9 - 3 - 4 = 2$ 個黑格。蓋完一層後只剩 2 個黑格，另 2 層剩下各六格未被蓋。因 1 個黑格最多再蓋 4 格，所以 2 個黑格無法完全覆蓋。我們也可以看到，如果再有 3 個黑格是可以蓋完的，也因此找到 10 個元素的解。

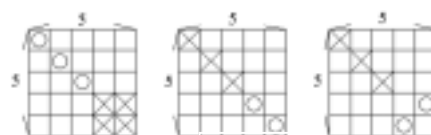


圖 12

$f(n, n, 3) = 3n - 6$ ，我們只證明 $3n - 7$ 個黑格不行覆蓋 $n \times n \times 3$ 的長方體。

若一大小為 $3n - 7$ 的集合 S ，因 $\left\lfloor \frac{3n-7}{3} \right\rfloor = n-3$ ，黑格較少的那層最多只有 $n - 3$ 個黑格，

如圖 13。這層至少還有 9 格需另兩層上下覆蓋。

第二、三層未被覆蓋的是一個邊長 $n - 7$ 、但一對

角線已被覆蓋的正方形。黑格還剩下 $3n - 7 - (n -$

$3) - 9 = 2n - 13$ 個。

這兩層中分 $2n - 3$ 個黑格分到較少的那層只有 $\left\lfloor \frac{2n-13}{2} \right\rfloor = n - 7$ 個黑格。這 $n - 7$ 個黑格

蓋完後還會剩下一個邊長 4 的正方形，這個正方形中還有 12 個空格需要靠第三層由上

面覆蓋。 $(2n - 13) - (n - 7) = n - 6$ 。當 $n = 18$ 時，第二層是一定不會被蓋滿。當 $n = 19$

時，蓋滿第二層之後還剩下 $n - 18$ 個黑格，卻要蓋滿一個邊長 $n - 6$ 的正方形，很明顯

的，這是不可能的事。也就是 $f(n, n, 3) > 3n - 7$ 。

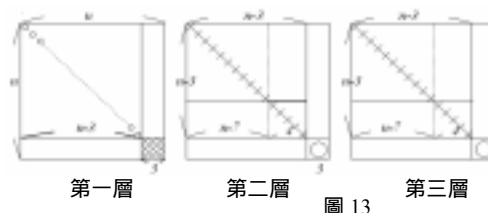


圖 13

(三) $c = 4, 5$ 的情況

這部份的研究，我們是利用方格紙幫助我們找解，並且去證明我們找到的解是最佳情

況。我們只把結果列出來表(三)中。其中一個跟後來研究比較有關的結果是： $f(n+1, n+1,$

$k) = f(n, n, k) + k$

若 $f(n, n, k) = m$ ，表示 m 個黑格就可以覆蓋 $n \times n \times k$ 的長方體，如圖 14

這樣在 $n \times n \times k$ 的長方體外面再放一個 k 個黑格組成的 $1 \times 1 \times k$ 的長方

柱，如此 $(n+1)^2 \times k$ 的長方體完全被覆蓋了。

所以 $(n+1) \times (n+1) \times k$ 的解，至多只要 $f(n, n, k) + k$ 個就好了。



圖 14

再拿其它結果跟 $c = 2$ 、 $c = 3$ 的結果相比較後，發現了一件很特別的事：

當 $n = 2$ ， $f(n, n, 2) = 2(n - 1)$ ；當 $n = 6$ ， $f(n, n, 3) = 3(n - 2)$ ；

當 $n = 12$ ， $f(n, n, 4) = 4(n - 3)$ ；當 $n = 20$ ， $f(n, n, 5) = 5(n - 4)$

因此我們猜想，當 $n = m = c(c - 1)$ 時， $f(n, n, c) = c(n - c + 1)$ 。而比較困難的事情是，我

們把 n 從 c 到 m 遞增的過程中， $f(n, n, c)$ 是如何變化的。

(四) $c = 6$ 的情況

如果我們的猜想正確，那對於 $c = 6$ 的情況，對於 n 的值，就必需從 7 開始找解一直到 30，這是很大的工程。所以我們一邊進行，另一邊就回頭去檢視 $c = 4$ 和 $c = 5$ 的結果。去看看黑格的分布有沒有什麼特別之處，後來發現最佳解的情形下，黑格都是成區塊狀的出現。後來我們想出了**區塊分割法**，可以幫著我們很快的找到黑格數的上界。

(五) 區塊分割法

使用這個方法找到開鎖的解並不能確定是最佳解，但已經對嘗試的次數給一個上界。也就是我們知道最佳解不會超過我們所給的值。

1. 區塊分割法的意義

我們把長方體切成 c 層，每一層都是邊長 n 的正方形。如圖 15, y941 把這邊長為 n 的正方形切成 s 個小正方形(區塊)，設這些小正方形的邊長分別是 $x_1, x_2, \dots, x_s$ ， $x_i \in N$ 。

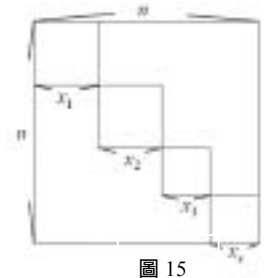


圖 15

一個邊長 x_i 的區塊如完全靠上下覆蓋，則需要 x_i^2 個黑格。我們只需要照著轉格的方式排列，在每一層都放置 x_i 個黑格。除了這 x_i 層之外的 $c - x_i$ 層，各層在這邊長 x_i 的區塊都不需要有黑格，而在其它的正方形都有跟邊長一樣數量的黑格，也就是需要 $n - x_i$ 個黑格，那就可以完全覆蓋這些層。

如此，每一層在一個區塊可以缺席一次，故我們計算在 $x_1, x_2, \dots, x_{s-1}$ 這幾個區塊中，累計的缺席的層數 $t = c - x_1 + c - x_2 + \dots + c - x_{s-1}$ ，也是最後一個區塊 x_s 中，有 t 層必需各層都有 x_s 個黑格。

已知 $x_1 + x_2 + x_3 + \dots + x_{s-1} + x_s = n$ ，並假設 $x_1 \geq x_2 \geq x_3 \geq \dots \geq x_s$ ，若

$c - x_1 + c - x_2 + \dots + c - x_{s-1} \leq c$ 。則定義

$$\bar{f}(n, n, c) = \min \{ x_1^2 + x_2^2 + \dots + x_{s-1}^2 + t x_s \mid x_1 + x_2 + x_3 + \dots + x_{s-1} + x_s = n, \quad x_1 \geq x_2 \geq x_3 \geq \dots \geq x_s, \quad t = c - x_1 + c - x_2 + \dots + c - x_{s-1}, \quad x_i \in N \}.$$

2. 一些相關的發現

(1) 若正整數 $x_1 + x_2 + x_3 + \dots + x_{s-1} + x_s = n$, 且 $|x_i - x_j| \leq 1$, 我們說 **n 被 s 等分**。

也就說如果 n 被 s 等分 , 則每一個 x_i 不是等於 $\left\lfloor \frac{n}{s} \right\rfloor$, 就是等於 $\left\lceil \frac{n}{s} \right\rceil$ 。

而當 n 被 s 等分成 $x_1, x_2 \dots x_s$ 時 , $x_1^2 + x_2^2 + \dots + x_s^2$ 之值有最小。證明如下：先驗證下面三件事情：

$$x_i - x_j > 1, \quad x_i^2 + x_j^2 > (x_i - 1)^2 + (x_j + 1)^2,$$

$$x_i - x_j = 1, \quad x_i^2 + x_j^2 = (x_i - 1)^2 + (x_j + 1)^2,$$

$$x_i - x_j < 1, \quad x_i^2 + x_j^2 < (x_i - 1)^2 + (x_j + 1)^2.$$

這也就是說 , 如果 $x_1, x_2 \dots x_s$ 中有兩數 x_i 和 x_j 的差大於 1 的話 , 我們就把其中較大的數減去 1、較小的數加上 1 , 使其總和仍然是 n , 但所有 s 個數的平方和會減小。重覆這樣的動作直到任意兩數的差都不大於 1 為止。如此就得到平方和最小的情況 , 恰好 n 被 s 等分。

(2) 若 $a = tc$ ($t \in \mathbb{N}$) , 則我們說 $a \times a \times c$ 是第 t 個分段點 , 而 $tc \times tc \times c$ 到

$(tc + c) \times (tc + c) \times c$ 叫第 t 個區段。已經知道 , 在第 t 分段點做區塊分割時是 **$(t+1)$ 等分的**。如表 3 就是 $c = 10$ 的例子。

a		a		c	區塊數	區塊分割
10	$\times$	10	$\times$	10	2	$5^2 + 5^2$
20	$\times$	20	$\times$	10	3	$7^2 + 7^2 + 6^2$
30	$\times$	30	$\times$	10	4	$8^2 + 8^2 + 7^2 + 7^2$
40	$\times$	40	$\times$	10	5	$8^2 + 8^2 + 8^2 + 8^2 + 8^2$
50	$\times$	50	$\times$	10	6	$9^2 + 9^2 + 8^2 + 8^2 + 8^2 + 8^2$
60	$\times$	60	$\times$	10	7	$9^2 + 9^2 + 9^2 + 9^2 + 8^2 + 8^2 + 8^2$
70	$\times$	70	$\times$	10	8	$9^2 + 9^2 + 9^2 + 9^2 + 9^2 + 8^2 + 8^2$
80	$\times$	80	$\times$	10	9	$9^2 + 9^2 + 9^2 + 9^2 + 9^2 + 9^2 + 9^2 + 9^2 + 8^2$
90	$\times$	90	$\times$	10	10	$9^2 + 9^2 + 9^2 + 9^2 + 9^2 + 9^2 + 9^2 + 9^2 + 9^2 + 9^2$

表 3

我們說第 t 個分段點會被 $t+1$ 等分，是因為它不能被 t 等分，這樣會被分成 t 個邊長 c 的區塊，如此所需的黑格數 tc^2 ，會比原先的 $(t+1)\left\lceil\frac{tc}{t+1}\right\rceil^2$ 還來得大。也不能被 $t+2$ 等分，若分成 $t+2$ 個區塊，缺席的總層數會超過 c 層，這時就不只 x_{t+2} 的係數是 c ，還有其它更多區塊不能只用邊長的平方計算，而都要去乘上長方體的高 c ，如此一來，所需的黑格數會比分成 $t+1$ 塊來的多。

(3) 而對於第 t 區段之間的 a ，也就是 $tc < a < (t+1)c$ 時， $a \times a \times c$ 做區塊分割時也是分成 $t+2$ 區塊，而前 t 塊的邊長 $x_1, x_2 \dots x_{t+1}$ ，這些數彼此的差也都不大於 1， x_{t+2} 則是介於 1 到 $\left\lceil\frac{n}{t+1}\right\rceil$ 的整數。第 t 個分段點可以看出來，在每一個區段之間， $\bar{f}(n+1, n+1, c) - \bar{f}(n, n, c)$ 是相當有規律的。利用這個規律，可以很容易用程式把 $\bar{f}(n, n, c)$ 的值算出來。這個規律我們透過下面表 4 這個例子來說明。

a		a		c	區塊數	區塊分割	黑格數	差	
10	×	10	×	10	2	$5^2 + 5^2$	50		
11	×	11	×	10	2	$5^2 + 5^2 + 10 \times 1$	60	10	2 次 10
12	×	12	×	10	2	$5^2 + 5^2 + 10 \times 2$ $6^2 + 5^2 + 9 \times 1$	70	10	
13	×	13	×	10	2	$6^2 + 5^2 + 9 \times 2$	79	9	2 次 9
14	×	14	×	10	2	$6^2 + 5^2 + 9 \times 3$ $6^2 + 6^2 + 8 \times 2$	88	9	
15	×	15	×	10	2	$6^2 + 6^2 + 8 \times 3$	96	8	
16	×	16	×	10	2	$6^2 + 6^2 + 8 \times 4$	104	8	
17	×	17	×	10	2	$6^2 + 6^2 + 8 \times 5$	112	8	4 次 8
18	×	18	×	10	2	$6^2 + 6^2 + 8 \times 6$ $7^2 + 6^2 + 7 \times 5$	120	8	
19	×	19	×	10	2	$7^2 + 6^2 + 7 \times 6$	127	7	
20	×	20	×	10	3	$7^2 + 6^2 + 7 \times 7$	134	7	

表 4

在每一區段的最一開始， $\overline{f}(n+1, n+1, c) - \overline{f}(n, n, c)$ 都會是 10，如此加 10 出現 2 次，這個 $2 = 2 \times 6 - 10$ (5 平方要變成 6 平方)，再來因為也是 5 進位成 6，所以是增加 2 次 9，再來是第一個 6 平方進位成 7 平方，所以會加 4 次 8。

一般來說，從第 t 個分斷點開始增加的數由 c 遞減，每次減 1。而同樣數字重覆的次數是： c 有 $2 \times (x_t + 1) - c$ 次；接下來如果都是要讓 x_t 進位成 $x_t + 1$ 次，則都是 2 次；一直到第一個要從 $x_t + 1$ 進位成 $x_t + 2$ ，才會是 4 次；之後的 $x_t + 1$ 進位成 $x_t + 2$ ，又會到 2 次。如此完成一個區段。

(4) 我們將計算 $\overline{f}(n, n, c)$ 所需要的程式附在附錄中。

四、密碼鎖三個位置數字為 $a > b > c$ 的情況

1.D 區的黑格數：

我們是把 $a \times b \times c$ 的長方體分成 c 層，每一層都是 $a \times b$ 的長方體。設第一層有最少的黑格，只有 x 個黑格 ($0 < x < b$)，則第一層還有 $(a - x)(b - x)$ 個正方體需要上下覆蓋，也就是在 D 區至少要有 $(a - x)(b - x)$ 個黑格。如圖 16 這些黑格如果平均分配到 $b - x$ 層，每層有 $a - x$ 個。

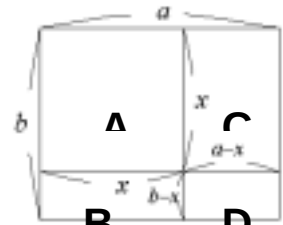


圖 16

2.A 區的黑格數

(1) 照前一段，則共有 $c - (b - x)$ 層在 D 區是沒有黑格(包括第一層)，這些層在 A 區都要 x 個黑格，共需 $(c + x - b)x$ 個黑格。因為至少有第一層在 D 區是沒有黑格，且 $b > c$ ，因此我們知道 $0 < (c + x - b) < x$ 。

(2) D 區有黑格的層數是 $b - x$ 層，考慮這些層在 A 區的情況。因為 A 區有 x 個黑格的已經有 $(c + x - b)$ 層了，這些在 A 區的黑格至少能形一個邊長 $(c + x - b)$ 的正方形，如此 $b - x$ 層中，每層只需要 $x - (c + x - b)$ 個黑格。因此需要 $(b - x)(b - c)$ 個黑格。

3. 黑格總數

把這三類加起來得到黑格數有 $2x^2 - (a + 3b - 2c)x + b(a + b - c)$ 。.....(1)

這又是一個二次函數。當 x 是在 $0 \leq x \leq b$ 這範圍中離 $\frac{a+3b-2c}{4}$ 最近的整數時，黑格數有最少。我們只要把給定的 a 、 b 、 c 代進去算出 x ，再把 x 代到(1)的二次函數中，就可以知道需要嘗試的次數了。

(1) 而當 $x = b$ 時，此時 $\frac{a+3b-2c}{4} \geq b - \frac{1}{2}$ ，即 $a \geq b + 2c - 2$ ，時，函數值會等於 bc 。這跟 $b = c$ 的情況， $a \geq 3c - 2$ 時只要試 c^2 次就好的結果是一致的。

(2) 但當 $a = b$ 時，這個方法得到的黑格數會比用區塊分割法得到的黑格數還多，但我們仍然不太清楚是什麼原因。

柒、討論及未來展望

一、文獻中有證明 $8 \times 8 \times 8$ 的鎖只試 31 個號碼不保證一定能打開，其證明方式在 $n > 13$ 時就不能使用。因此我們才會想出了另一個方法去證明。其中最重要的部份是證明黑格都是落在 A 區或是 D 區。

(一) 一個想法是，當擺上第一層的黑格及 D 區的 $(k+1)^2$ 個黑格後，尚未被覆蓋的正方體：A 區至少還剩下 $(k-1) \times (k-2) \times (2k-1)$ 個、B 區和 C 區都至少還剩下 $(k-1) \times (k+1) \times (k-2)$ 個。其它的黑格在 A 區有 α 個、B 區有 β 個、C 區有 γ 個。這時去計算，當 $\alpha + \beta + \gamma$ 等於剩下的黑格數時，下面兩個不等式是否能同時成立。

$$\begin{cases} (4k-7)\alpha + (k-1)(\beta+\gamma) \geq (k-1)(k-2)(2k-1) \\ 2(k+1)\alpha + (3k-4)(\beta+\gamma) \geq 2(k+1)(k-1)(k-2) \end{cases}$$

經過計算化簡後，當 n 不大於 20 時是可以用這個方法證明。比文獻中的方法略佳。

(二) 另一個想法是扣掉已經被覆蓋的正方體後，每一個 A 區的黑格可以有效蓋住 A 區 $4k-7$ 個正方體，B 區和 C 區各 $k+1$ 個正方體；每一個在 B 區的黑格可以有效蓋住

A 區 $k - 1$ 個正方體，蓋住 B 區 $3k - 4$ 個正方體。因此黑格在 A 區是較佳的。

二、對於 $a > b > c$ 的情況，另一個方法是先把 $a \times b \times c$ 的長方體切出一塊 $x \times x \times c$ 的長方體(通常 $x > c$)。要覆蓋 $a \times b \times c$ 的長方體可看成先利用第三部份($a = b > c$)的研究結果，算出覆蓋 $x \times x \times c$ 的長方體所需的黑格數 $\overline{f}(x, x, c)$ ，再加每一層在 D 區都需要 $(a - x)$ 個黑格，總共需要 $\overline{f}(x, x, c) + c(a - x)$ 個黑格。但這個方法所需的黑格數比正文所題的方法所需的數目要多 2~5 個。

三、有人想到說，做了這麼大的研究，實際上省了多少時間呢？另一個開鎖的方法是不管號碼數最多的那一個旋鈕，只要把另兩個的所有組合試完就好。我們的結果跟這個方法相比，當 a 、 b 、 c 很接近時，約省了一半的次數；如果三個數不接近時，省的時間就很有限；特別是當 $a > b + 2c - 2$ 時，完全沒辦法省下嘗試的次數。

四、這個題目已經完成，接下去可能發展的題目是：

- (1) m 個旋鈕有 n 個對可以打開，如何用最少次保證打開鎖。這時 m 、 n 都是變數；
- (2) 3 個位置中 2 個位置對時有特別的提示，例如說門的鬆緊不一樣，或是聲音不太一樣，找出最少次數保證能打開鎖的最佳策略。(就像猜一個三位數字，但只有 2A 會給回應，如何猜到數字。)

捌、結論

一個有 3 個旋鈕的密碼鎖，各位置的號碼數分別是 a 、 b 、 c ，如果有兩個位置的數字正確就能打開，則我們知道

- 一、運用轉格的方法，可以找到三叉體的解；再利用三叉體的延長和組合可以求出 $a \times a \times a$ 的正方體及 $a \times a \times c$ 的長方體的解($c > a$)。

- 二、 當 $a = b = c = n$ 時，保證打開鎖最少要嘗試 $\left\lfloor \frac{n}{2} \right\rfloor^2 + \left\lceil \frac{n}{2} \right\rceil^2$ 次。
- 三、 當 $a = b < c$ 時，保證打開鎖最少要試 $\min\{s^2 + t^2 + s(c - a) \mid s+t=a, t \geq s \geq 0, s, t \in \mathbb{Z}\}$ 次：特別當 $c \geq 3a - 2$ 時，只要試 a^2 。
- 四、 當 $a = b > c$ 時，利用區塊分割法能夠算出需要嘗試次數的上界。並且在固定 c 的情況下，隨著 a 遞增的，需要嘗試次數也是呈現規則性的遞增。
- 五、 當 $a > b > c$ 時，令 $x = \left\lfloor \frac{a + 3b - 2c}{4} \right\rfloor$ ，需要嘗試的次數最多只要 $2x^2 - (a + 3b - c)x + b(a + b - c)$ 次。

玖、參考資料

單墀、胡大同 數學奧林匹克第 28、29 屆國際數學競賽預選題 九章出版社
p.42 , p.73~p.75

評語

有趣的問題，很棒的解答，看的出已能掌握投影和極小值的一些概念，分析的手法適切而且恰當，雖然某些情況未能找出完整的解答，卻給出了一個不錯的上界，非常優秀的作品。