密碼的計數

柳柏濂

一. 編碼, 把“水”攪混。

提起密碼, 讓我們立即想起了一個充滿奧妙的世界。“破密”和“保密”就好像矛和盾, 轟炸機和高射砲, 一直貫穿在有形和無形的戰爭中。

我們考察這樣的一種密碼。它的本質是一種字母的代換 (Substitution cipher): 把表達信息通常所用的字母, 用一個密碼本中的特殊字母代替。例如, 一個信息 MISSISSIPPI。如果我們用一個特殊密碼表—把英文 26 個字母按順時針方向排在一個圓周上, 成一個密碼表。把原信息的每一個字母, 用密碼表中該字母按順時針方向走第三個位置所在的字母代替。按這個密碼置換規則, MISSISSIPPI 變成 PLVVLVVLSSL, 這類密碼稱爲 Caesar 碼。

編碼 (encipherment) 就是把“水”攪渾, 把通常字母表達信息用字母表的特殊置換產生密碼, 而解碼 (decipherment), 就是上述置換的逆過程。

現在, 我們採用如下的一種規則: 以一篇用字母撰寫的命令爲例。我們用 A 置換第一個出現的字母, 以及在整篇命令中出現此字母的所有位置, 用 B 置換命令中下一個不同的字母以及出現此字母的所有位置, 如此繼續, 這樣得到的密碼稱爲正規密碼。(normalized cyptogram)。

於是, 按照這一算法, 不論信息 MISSISSIPPI, 還是它的 Caesar 密碼 PLVVLVVLSSL, 都可導出同一個正規密碼 ABCCBCCBDDB。

一般地, 如果 p 是任一個通常的信息, c 是 p 的一個密碼, 則 c 和 p 都有一個正規密碼 N。

我們把一個字 (或正規密碼) 中含有的字母的個數稱爲字 (或正規密碼) 的長度。一個值得探索的問題是: 有多少個不同的長爲 n 的正規密碼字?

讓我們考察一些簡單的情形。

若字的長度是 1, 則它的正規密碼必是 A。

若字的長度是 2, 則它的正規密碼是 AA, AB。

若字的長度是 3, 則所有不同的正規密碼是 AAA, AAB, ABA, ABB, ABC。

若字的長度是 4, 則它的正規密碼是

$$AAAA,\ AAAB,\ AABA,\ ABAA,$$
$$AABB,\ ABAB,\ ABBA,\ AABC,$$
$$ABAC,\ ABCA,\ ABBB,\ ABBC,$$
$$ABCB,\ ABCC,\ ABCD$$

我們看到, 正規密碼只著眼於所含字母的類數和分段的長度與相對位置。

一般地, 設 $b(n)$ 表示長爲 n 的不同正規密碼的個數, 則上述簡單情況給出了如下結果:

$$b(1)=1,\ b(2)=2,\ b(3)=5,\ b(4)=15。$$

那麼, 如何求出 $b(n)$?

我們不妨把問題提得更細一點, 考慮長爲 n 的恰有 k 個不同字母的不同正規密碼, 它的個數爲 $S(n,k)$。從上面討論可知, $S(4,1)=1$, $S(4,2)=7$, $S(4,3)=6$, $S(4,4)=1$。

如果我們在一個有 q 字母的密碼表上, 考慮長爲 n 的正規密碼。把所有長爲 n 的不同正規密碼的個記爲 $b_q(n)$。

顯然,

$$b_q(n)=\sum_{j=1}^{\min(n,q)} S(n,j) \qquad (1)$$

於是, 當 $q\geq n$ 時,

$$b_q(n)=\sum_{j=1}^{n} S(n,j)=b(n) \qquad (2)$$

例如, 用英文表達的一個長爲 n 的句子, $q=26$, 當 $n\leq 26$ 時, 它的不同正規密碼個數是

$$b_{26}(n)=\sum_{j=1}^{n} S(n,j)$$

而當 $n>26$ 時, 它的不同正規密碼個數是

$$b_{26}(n)=\sum_{j=1}^{26} S(n,j)。$$

讀者耐著性子讀到這裡, 誰都會忍不住發問: 究竟 $S(n,k)$ 怎樣求出來?

從 $S(n,k)$ 的上述定義, 當然我們知道了它的實際含義。數學家的任務是通過數學的抽象和技巧把它解出來。然而, 爲了更易於解決問題, 我們可以把它轉化爲一個更容易直接思考的模型。

二. 分組, 一個"平凡"的問題

據說, 美國數學教育專家的一項調查表明, 成年人用到的數學不超過初中二年級教材的內容。然而, 如果隨便留心一下周圍的生活。你幾乎都可以提出一個"平凡"的問題, 它需要數學, 並且令大學生也爲如何去解答它弄得搔首托腮。

"十個學生 (他們的名字當然各不相同), 恰分成三組。有多少不同的分法?"現在, 我就提出這樣一個平凡的問題。

當你動手在紙上, 把鄭一, 吳二, 張三, 李四, 王五, 陳六, 何七, 趙八, 梁九, 劉十···擺弄成三堆的時候, 你會覺得, 這個問題不勝其繁。

讓我們把十個人看作一個長爲十的字, 三個小組看作是三種不同字母。於是, 長爲十的恰會三個不同字母的正規密碼一一對應於十個人的分三組的一種方案。例如

AABCACCBBA $\Longleftrightarrow$

鄭一	吳二	張三	李四	王五	陳六	何七	趙八	梁九	劉十
(1)	(1)	(2)	(3)	(1)	(3)	(3)	(2)	(2)	(1)

(不計較組的標號)

沒想到, 這個平凡的問題竟然就是求 $S(10,3)$, 讓你不覺一驚。然而, 換一個角度看問題, 當你意識到求 $S(n,k)$ 只不過是把"n 個人分成 k 組"這個如此平凡的問題時, 你難道不覺得心中大喜嗎?

就用這個模型, 我們去探索 $S(n,k)$。

顯然, $S(0,0)=1$ (無人, 又不分組)。

約定 $S(n,0)=S(0,k)=0$, $n\neq 0$, $k\neq 0$。

要這種分組能夠進行, 必須且僅須人數不少於組數, 因此

$$S(n,k)>0, \quad n\geq k\geq 1$$
$$S(n,k)=0, \quad n<k。$$

易見 $S(n,1)=1$。

考察 $S(n,2)$。把 n 個人 $(n\geq 2)$ 恰分成兩組, 每個人都可有2種選擇。由乘法原理, n 個人共有 2^n 種選擇, 但這裡可能出現所有人選第一組, 或所有人選第2組的情形, 這就不符合"恰分成兩組"的要求。於是, 應有 (2^n-2) 種選擇。但不計較組的標號, 故應 $S(n,2)=\frac{1}{2}(2^n-2)=2^{n-1}-1$。

用類似方法, 讀者可練習, 求得

$$S(n,3)=\frac{1}{3!}(3^n-3\cdot 2^n+3)$$
$$S(n,n-2)=\binom{n}{3}-3\binom{n}{4}$$
$$S(n,n-1)=\binom{n}{2}$$

現在, 讓我們借助分組模型, 用遞歸的方法, 求 $S(n,k)$ 的表達式。

更直接地, 我們把" n 個人恰分成 k 組"看作"n 個有標號 $1,2,\ldots,n$ 的球放到 k 個無標號的盒子裡, 且無一盒空", 它的方法數便是 $S(n,k)$。

我們著眼於球 n。若球 n 獨佔一盒, 則剩下的 $n-1$ 個球須放 $(k-1)$ 個盒, 放法數 $S(n-1,k-1)$。若球 n 不獨佔一盒 (即球 n 所在盒至少有2個球), 則可這樣操作: 先把其餘的 $n-1$ 個球放 n 個盒, 無一盒空, 方法數 $S(n-1,k)$, 然後, 再把這個球 n, 隨意放一盒, 有 n 種放法, 即共 $nS(n-1,k)$ 種放法, 於是得

$$S(n,k)=S(n-1,k-1)+nS(n-1,k) \tag{3}$$

衆所周知, 電腦最擅長於遞歸運算。因此, 從初值 $S(0,0)=1$, $S(0,1)=0$ 開始, 我們用電腦, 按遞歸關係 (3), 對任一對特定的 (n,k), 不難算出 $S(n,k)$。於是, 可編製出下列一個關於 $S(n,k)$ 的數值表 $(1\leq n\leq 10)$

n \ k	1	2	3	4	5	6	7	8	9	10	$B(n)=\sum_{k=1}^{n} S(n,k)$
1	1										1
2	1	1									2
3	1	3	1								5
4	1	7	6	1							15
5	1	15	25	10	1						52
6	1	31	90	65	15	1					203
7	1	63	301	350	140	21	1				877
8	1	127	966	1701	1050	266	28	1			4140
9	1	255	3025	7770	6951	2646	462	36	1		21147
10	1	511	9330	34105	42525	22827	5880	750	45	1	115975

從表中可見, $S(10,3) = 9330$。怪不得我們試圖拼拼湊湊, 去回答本節開頭的那個“平凡”問題, 顯得如此力不從心了。

至此, 對於 $S(n,k)$, 我們總算有了一個算法, 然而, 對追求完美的數學家來說, 仍然試圖求出 $S(n,k)$ 的顯式來。

一個自然的想法是: 從遞歸關係 (3), 用逐步遞降方法求出 $S(n,k)$ 的顯式。然而, 因爲 (3) 式右邊第二項多乘了一個變係數 n。因此, 要從 (3) 直接導出 $S(n,k)$ 變成不可能。

我們採用組合數學的另一個技巧—相容排斥原理。

先退一步考察“n 個有標號的球放到 k 個有標號的盒中, 無一盒空”的放法。請注意, 這與我們的問題區別僅在於 k 個盒“有標號”還是“無標號”而已。既然盒子多了標號, 因此, 每一個無標號盒的放置可生成 $k!$ 個有標號盒的放置。於是, 它的方法數應是

$$kS(n,k)。 \tag{4}$$

從另一方面考察, 在 k 個有標號的盒子中, 放 n 個有標號的球。若至少 j 個 $(0 \le j \le k)$ 盒是空盒, 它的放法數應是 $\binom{k}{j}(k-j)^n$。這是因爲: 先從 k 個盒中選出 j 個空盒有 $\binom{k}{j}$ 種方法, 剩下的 $(k-j)$ 個盒放 n 個標號球有 $(k-j)^n$ 種放法的緣故。由相容排斥原理, 無空盒的放法應是

$$\sum_{j=0}^{k}(-1)^j\binom{k}{j}(k-j)^n \tag{5}$$

既然 (4), (5) 是同一個量, 便得

$$k!S(n,k)=\sum_{j=0}^{k}(-1)^j\binom{k}{j}(k-j)^n$$

即

$$S(n,k)=\frac{1}{k!}\sum_{j=0}^{k}(-1)^j\binom{k}{j}(k-j)^n \tag{6}$$

於是, 我們得到了 $S(n,k)$ 的顯表達式 (6)。有興趣的讀者可以檢驗一下, (6) 式完全符合遞歸關係 (3) 及它的初值。因此, 可以說, (6) 也是 (3) 式的解。

在數學中, $S(n,k)$ 是一個著名的組合數, 稱爲第 II 類 stirling 數, 而它們的和 $B(n) = \sum_{k=1}^{n} S(n,k)$ 稱爲 Bell 數, 以紀念首先研究這類問題的數學家 J. Stirling (1692-1770) 和 E. T. Bell(1883-1960)。

第 II 類 stirling 數 $S(n,k)$ 和 Bell 數 $B(n)$ 有廣泛的應用。用數學語言來闡述: 把集 $A = \{1,2,\ldots,n\}$ 作 k 部分分拆 $\{S_1,\ldots,S_k\}$ $(\cup_{i=1}^{k} S_i = A, S_i \cap S_j = \phi,$ $i \neq j)$。分拆數就是 $S(n,k)$, 而 A 的所有可能分拆數是 $B(n)$。考慮有限集 X, Y, 其中 $|Z| = n$, $|Y| = k$, 則由 X 到 Y 的滿射 (onto mappings) 個數便是 $k!S(n,k)$。

爲了滿足讀者的好奇心, 我們不能不談一下第 I 類 stirling 數, 雖然它跟本文的題旨無關。

如果我們把 n 個有標號的球, 分放到恰好 k 個無標號的圓周上排列, $(0 \leq k \leq n)$。不同的排列方法數 $s(n,k)$, 便稱爲第 I 類 stirling 數。(有些著作稱爲第 I 類 stirling 數的絕對值)。

用組合方法不難得出 $s(n,0) = 1$, $(n \geq 1)$, $s(n,1) = (n-1)!$ 及遞歸式

$$s(n,k) = s(n-1,k-1) + (n-1)s(n-1,k), \quad k \leq n。$$

令人驚異的是迄今還未能找到第 I 類 stirling 數 $s(n,k)$ 的顯表達式。

三. 動真格, 搬出英文詞典

終於, 我們可以鬆一口氣, 滿懷信心回到密碼問題來。

由 (3) 和 (6), 我們可以計算長爲 n 的恰有 k 個不同字母的不同正規密碼數 $S(n,k)$。再由 (1) 和 (2), 可以確定地回答: 長爲 n 的不同正規密碼個數 $b(n) = B(n)$。

從編碼和語言學的角度, 我們不妨作一點有趣的探索。$S(5,4) = 10$ 告訴我們, 由4個不同字母組成的長度爲5的單詞有10種類型 (正規密碼)。動眞格, 我們搬出英文詞典來。確實, 英文單詞就有這10種類型:

OOZED EVERY TASTE SPOTS
WEEDS NEVER SPOON THERE
SHALL SERVE。

然而, 對於 $S(5,3) = 25$, 我們翻遍英文詞典, 只找到19類由3個不同字母組成的長爲5的單詞, 而其餘6類 $AAABC$, $ABBBC$, $ABCCC$, $AABBC$, $AABCC$, $ABBCC$ 卻寄望於未來語言學家創造新詞時填補這一空白。

如果我們考慮句子, 字與字之間就應留空。對於一些保密性能不高的密碼, 亦希望在傳遞信息的單詞之間保留空白間隔。這就給密碼的計算提出了新的要求。這種留空的限制與我們日常書寫的習慣是基本一致的: 第一、留空的位置不能相鄰 (即僅留一個空格)。第二、首末位置不留空。現在, 我們考慮這種具有留空限制的長爲 n 的正規密碼的計數。

如果僅僅考察一個長爲 n 的句子的留空方法數 f_n。那麼, 只要考慮第 $n-1$ 個位置

是非空, 還是空, 兩種情形。我們就立即得到遞歸式

$$\begin{cases} f_n = f_{n-1} + f_{n-2} \\ f_1 = f_2 = 1 \end{cases} \tag{7}$$

衆所周知, $\{f_n\}$ 是著名的費波那契 (Fibonacci) 數列。當然, 如果更仔細地討論空格的取法。例如, 在長爲 n 的句子中, 取出 r 個 $(0 \le r \le \lfloor (n-1)/2 \rfloor)$ 位置留空的方法數: ($\lfloor m \rfloor$ 表不大於 m 的最大整數) 就可以看作是在一個數列 $1, 2, \ldots, n-2$ 中 (因句子首末位不留空) 取出 r 個互不相鄰的元的方法數, 其結果 (見 [2]) 是

$$\binom{(n-1)-(r-1)}{r} = \binom{n-r-1}{r} \tag{8}$$

對照 (7), 這就恰好驗證了一個關於費波那契數列的結論

$$f_n = \sum_{r=0}^{[(n-1)/2]} \binom{n-r-1}{r} \tag{9}$$

現在, 我們可以著手計算有留空限制的正規密碼的個數。

設 $m_q(n)$ 爲在一個有 q 個字母的碼表上生成的長爲 n 的正規密碼個數, 這裡, 碼 (句子) 的長度意味著字母數與空隔數的總和。

如果考慮有 r 個空隔 $(0 \le r \le \lfloor \frac{n-1}{2} \rfloor)$ 的正規密碼。那麼, 設想把那些空隔去掉, 即讓所有字母向一邊擠緊而不留空白, 便得到一個長爲 $n-r$ 面無空隔的正規密碼。

易見, 某 r 個位置取空隔的長爲 n 的正規密碼集與無空隔的長爲 $n-r$ 的正規密碼集是一一對應的。注意到 (8) 式, 便得

$$m_q(n) = \sum_{r=0}^{\lfloor (n-1)/2 \rfloor} \binom{n-r-1}{r} b_q(n-r)。$$

如果我們所用的字母種類數不加限制。這時記 $m_q(n)$ 爲 $M(n)$ 便得

$$M(n) = \sum_{r=0}^{[(n-1)/2]} \binom{n-r-1}{r} B(n-r) \tag{10}$$

下面給出一個 $M(n)$ 數值表 $(1 \le n \le 10)$

n	1	2	3	4	5	6	7	8	9	10
$M(n)$	1	2	7	25	102	456	2219	11640	65364	390646

試看 $M(4)$ 的25個留空正規密碼

AAAA AAAB AABA AABB AABC
ABAA ABAB ABAC ABBA ABBB
ABBC ABCA ABCB ABCC ABCD
AA A AA B AB A AB B AB C
A AA A AB A BA A BB A BC

四. 更精確, 借助相伴碼

既然, 編碼和解碼都追求精確, 那麼, 我們做碼的計數時, 也應追求更精密的計數。

當寫下一個正規密碼時, 最引起我們注意的是, 同一個字母連續出現的碼段, 我們稱它爲貫 (run)。一個貫所含的位置數稱爲貫的長。一個正規密碼 (本節討論不帶空隔的正規密碼) 由很多貫組成。所有貫長中的最大者, 稱爲此正規密碼的貫長。

我們約定, 正規密碼的長用 n 表示, 所含不同字母個數用 k 表示。所含貫的個數用 d 表示, 而密碼的貫長表爲 ℓ。顯然, $k \le d \le n$, $\lceil \frac{n}{d} \rceil \le \ell \le n$, 這裡 $\lceil m \rceil$ 表不小於 m 的

最小整數。例如, $ABCCBCCBDDB$, 有 $n=11$, $k=4$, $d=8$, $\ell=2$。而所有 $n=5$, $k=3$, $d=3$, $\ell=2$ 的正規密碼是 $AABBC$, $AABCC$, $ABBCC$。

比上一節更精確的一個問題是: 有多少個具有參數 n, k, d, ℓ 的不同的正規密碼?

爲了解決這個問題, 我們引進一個相伴正規密碼 (associated normal cryptogram) 的概念, 簡稱 ANC。如果把一個含 k 個不同字母的正規密碼 NC 的所有字母作不同置換 (更數學化地說: 在 k 個字母的對稱群作用下) 所得的所有密碼, 稱爲 NC 的相伴正規密碼 (ANC)。例如, $ABBAC$ 的 ANC 是 $ABBAC$, $CBBCA$, $BAABC$, $CAACB$, $ACCAB$, $BCCBA$。

爲敍述更簡明, 我們約定下列符號

$C^{(\le\ell)}_{(\le k)}(n,d)$ — 長爲 n, 貫數爲 d, 且不同字母數至多 k 個, 貫長至多 ℓ 的 ANC 個數。

$C^{(\le\ell)}_{(=k)}(n,d)$ — 長爲 n, 貫數爲 d, 不同字母數 k 貫長至多 ℓ 的 ANC 個數。

類似可知 $C^{(=\ell)}_{(=k)}(n,d)$。在上述記號中, 若 D 換爲 C, 則表同類約束條件下, 正規密碼的個數。

下面, 讀者將更多和符號打交道。我們的任務是求 $D^{(\le\ell)}_{(=k)}(n,d)$ 或 $D^{(\le\ell)}_{(\le k)}(n,d)$。由 ANC 定義, 易知

$$D^{(\le\ell)}_{(=k)}(n,d)=\frac{1}{k!}C^{(\le\ell)}_{(=k)}(n,d) \qquad (11)$$

我們先求 $C^{(\le\ell)}_{(\le k)}(n,d)$。

令 $P^{(\le\ell)}_{n,d}$ 表正整數 n 分爲 d 部分, 且每部分不大於 ℓ 的分拆個數。也即方程 $x_1+x_2+\cdots+x_d=n$, $1\le x_i\le\ell$, $\lceil\frac{n}{d}\rceil\le\ell\le n$, $1\le d\le n$ 的解 $(x_1,x_2,\ldots x_d)$ 的個數。於是

$$C^{(\le\ell)}_{(\le k)}(n,d)=k(k-1)^{d-1}P^{(\le\ell)}_{n,d} \qquad (12)$$

這是因爲 n 分拆爲 d 部分後, 在第一段 (貫) 有 k 種可能的字母選擇, 其餘 $d-1$ 段各有 $(k-1)$ 種可能的字母選擇。現在, 只須求 $P^{(\le\ell)}_{n,d}$。

運用生成函數的技巧 (見 [4]), $P^{(\le\ell)}_{n,d}$ 是 $(t+t^2+\cdots+t^\ell)^d$ 展式中 t^n 項係數。

$$\begin{aligned}
&(t+t^2+\cdots+d^\ell)^d=t^d(1-t^\ell)^d(1-t)^{-d}\\
&=t^d\sum_{r\ge0}(-1)^r\binom{d}{r}t^{\ell r}\sum_{r\ge0}\binom{d+r-1}{d-1}t^r\\
&=t^d\sum_{n=d}^{\infty}\Big[\sum_{j\ge0}(-1)^j\binom{d}{j}\\
&\quad\cdot\binom{d+(n-d-\ell j)-1}{d-1}\Big]t^{n-d}\\
&=\sum_{n=d}^{\infty}\sum_{j\ge0}(-1)^d\binom{d}{j}\binom{n-\ell j-1}{d-1}t^n。
\end{aligned}$$

注意到 $j\le d$ 且 $d-1\le n-\ell j-1$, 即 $j\le\min\{d,(n-d)/\ell\}$。於是

$$P^{(\le\ell)}_{n,d}=\sum_{j=0}^{\min(d,\lfloor(n-d)/l\rfloor)}(-1)^j\binom{d}{j}\cdot\binom{n-\ell j-1}{d-1} \qquad (13)$$

由 (12), (13), 便得

$$C^{(\le\ell)}_{(\le k)}(n,d)=k(k-1)^{d-1}\sum_{j=0}^{\min(d,\lfloor(n-d)/\ell\rfloor)}\cdot(-1)^j\binom{d}{j}\binom{n-\ell j-1}{d-1}, \qquad (14)$$

由 (11), 我們的目標仍需求 $C^{(\le\ell)}_{(=k)}(n,d)$。注意到

$$C^{(\le\ell)}_{(\le k)}(n,d)=\sum_{i=1}^{k}\binom{k}{i}C^{(\le\ell)}_{(=i)}(n,d) \quad (15)$$

運用二項式反演技巧 (見 [5]) 即

$$a_n=\sum_{r=1}^{n}\binom{n}{r}b_r \Leftrightarrow b_n=\sum_{r=1}^{n}(-1)^{n-r}\binom{n}{r}a_r$$

由 (15) 得

$$\begin{aligned}&C^{(\le\ell)}_{(=k)}(n,d)\\&=\sum_{i=1}^{k}(-1)^{k-i}\binom{k}{i}C^{(\le\ell)}_{(\le i)}(n,d)\\&=P^{(\le\ell)}_{n,d}\sum_{i=1}^{k}(-1)^{k-i}\binom{k}{i}i(i-1)^{d-1}\\&=P^{(\le\ell)}_{n,d}\sum_{i=2}^{k}(-1)^{k-i}\binom{k}{i}i(i-1)^{d-1} \quad (16)\end{aligned}$$

由 (11) 便得

$$\begin{aligned}&D^{(\le\ell)}_{(=k)}(n,d)\\&=P^{(\le\ell)}_{n,d}\frac{1}{k!}\sum_{i=2}^{k}(-1)^{k-i}\binom{k}{i}i(i-1)^{d-1}\\&=\frac{1}{k!}\sum_{i=2}^{k}(-1)^{k-i}\binom{k}{i}i(i-1)^{d-1}\\&\quad\cdot\sum_{j=0}^{\min(d,\lfloor(n-d)/\ell\rfloor)}(-1)^{j}\binom{d}{j}\\&\quad\cdot\binom{n-\ell j-1}{d-1} \quad (17)\end{aligned}$$

對於另外的正規密碼, 顯然

$$\begin{aligned}D^{(=\ell)}_{(=k)}(n,d)&=D^{(\le\ell)}_{(=k)}(n,d)\\&\quad-D^{(\le\ell-1)}_{(=k)}(n,d) \quad (18)\end{aligned}$$

$$D^{(\le\ell)}_{(\le k)}(n,d)=\sum_{j=1}^{k}D^{(\le\ell)}_{(=j)}(n,d) \quad (19)$$

回想起第一, 三節的結果, 我們可以檢驗

$$\sum_{i=k}^{n}D^{(\le n)}_{(=k)}(n,i)=S(n,k)$$

$$\sum_{i=k}^{n}\sum_{j=1}^{n}D^{(\le n)}_{(=j)}(n,i)=\sum_{j=1}^{n}S(n,j)=B(n)。$$

還可以得到關於 $C^{(\le\ell)}_{(\le k)}(n,d)$ 的下列遞歸關係

$$\begin{aligned}C^{(\le\ell)}_{(\le k)}(n,d)&=(k-1)\sum_{j=1}^{k}C^{(\le\ell)}_{(\le k)}(n-j,d-1),\\&\quad 1\le\ell<n \quad (20)\end{aligned}$$

$$\begin{aligned}C^{(\le\ell)}_{(\le k)}(n,d)&=\binom{n-1}{d-1}k(k-1)^{d-1},\\&\quad \ell=n \quad (21)\end{aligned}$$

上述兩式可以如下證明: 設一個相伴正規密碼的最後一個貫是 R 且 R 的長度是 j, $1\le j\le\ell$, $1\le\ell\le n$。刪去 R, 便得一個帶參數 $n-j$, $d-1$, $(\le k)$, $(\le\ell)$ 的相伴正規密碼, 這類密碼的個數是 $C^{(\le\ell)}_{(\le k)}(n-j,d-1)$ 注意到恢復 R 的方法有 $k-1$ 種。對 j 求和由 1 到 ℓ, $1\le\ell\le n-1$, 便得 (20)。若 $\ell=n$, n 的恰有 d 部分的有序分拆數是 $\binom{n-1}{d-1}$。而放 k 類字母在 d 部分的方法數是 $k(k-1)^{d-1}$, 便得 (21) 式。

下面試驗證我們的結果。由 (17) 式,

$$\begin{aligned}D^{(\le2)}_{(=3)}(5,4)&=\frac{1}{3!}\sum_{i=2}^{3}(-1)^{3-i}\binom{3}{i}i(i-1)^{4-i}\\&\quad\cdot(-1)^{0}\binom{4}{0}\binom{5-0-1}{4-1}\\&=12\end{aligned}$$

符合條件的所有正規密碼是: $AABAC$, $AABCA$, $AABCB$, $ABAAC$, $ABACC$, $ABBAC$, $ABBCB$, $ABCAA$, $ABCBB$, $ABCCA$, $ABCCB$。

類似地, $D^{(\le 2)}_{(=2)}(5,4) = 4$, 它們是 $AABAB$, $BAABA$, $ABAAB$, $BABAA$,

$$D^{(\le 2)}_{(=1)}(5,4) = 0$$
$$D^{(\le 1)}_{(=3)}(5,4) = 0$$

由 (18) $D^{(=2)}_{(=3)}(5,4) = D^{(\le 2)}_{(=3)}(5,4) - D^{(\le 1)}_{(=3)}(5,4) = 12 - 0 = 12$ 由 (19)

$$\begin{aligned} D^{(\le 2)}_{(\le 3)}(5,4) &= \sum_{j=1}^{3} D^{(\le 2)}_{(j=2)}(5,4) \\ &= D^{(\le 2)}_{(=1)}(5,4) + D^{(\le 2)}_{(=2)}(5,4) \\ &\quad + D^{(\le 2)}_{(=3)}(5,4) \\ &= 0 + 4 + 12 = 16 \end{aligned}$$

最後, 我們也可以考慮有空隔的帶參數 n, k, d, ℓ 的正規密碼的計數, 沿用上述記號, 把 M 代替 C 表示增加如第三節的有空隔制的計數, 用類似方法可得

$$\begin{aligned} M^{(\le \ell)}_{(=k)}(n,d) = &\sum_{r=0}^{\lfloor (n-1)/2 \rfloor} \binom{n-r-1}{r} D^{(\le \ell)}_{(=k)} \\ &\cdot D^{(\le \ell)}_{(=k)}(n,d) \end{aligned}$$

參考文獻

1. S. W. Golomb, On the Enumeration of Cryptograms, Mathematics magazine 53, No. 4 (1980), 219-221.
2. 柳柏濂, 欄柵前面的思考—不含定距元素的組合問題, 數學傳播, 第二十一卷第一期, 29-34。
3. Liu Bolian, A Note on the Enumeration of Cryptograms, Menemui Mat. 13(1991), 57-63.
4. 柳柏濂, 別瞧不起它, 那個中學教材中的式子, 數學傳播, 第二十一卷第四期。
5. 柳柏濂, 阿凡提巧拆金環與完備分拆, 數學傳播, 第二十一卷第三期, 73-79。

—本文作者任教於中國華南師範大學數學系和廣東職業技術師範學院計算機系—