Folosindu-se calculatorul electronic *ABM*-650 și procedeele descrise la un exemplu de 100 grupuri cifrate ($m = 100$) se încearcă 50 trigrafuri ($k' = 50$) și se obțin 10 000 probe pentru examinare.

Acestea dau 280 monturi și 320 (a, b, c). Se obțin 20 monturi cauzale. Se elimină cazurile unde Δ sau Δ' este 0 sau 13 (mod 26 și se încearcă un număr suficient de trigrafuri.

Timpul pentru încercările a 10 000 probe a fost evaluat la aproximativ 30 minute, la acest calculator de mare viteză.

BIBLIOGRAFIE

1. L. Levine: Variabile Matrix Substitution in Algebraic Cryptography — The American Mathematical, Monthly" vol. 65/1958 pag. 170—179
2. J. Levine: Sorne elementary cryptogranalysis of Algebraic Cryprography — The American Mathematical Monthly" vol. 60/1961 pag. 411—418.
3. J. Levine: Some Applications of High-Speed Computers to the case $n = 2$ of Algebraic Cryptography „Mathemativs of Computation" 15 (1961), pag. 254—260.
4. Gr. C. Moisil: Introducere în algebră, vol. I, pag. 32—34
5. C. Popovici: Aritmetica și teoria numerelor pag. 93—96; 99—101, 116—122.
6. Gantmaher: Teoria matricilor.

FUNCȚII CARE REALIZEAZĂ CORESPONDENȚA BIUNIVOCĂ ÎNTRE MULȚIMEA NUMERELOR NATURALE ȘI MULȚIMEA PERECHILOR ORDONATE DE NUMERE NATURALE

ȘTEFAN N. BERȚI

Corespondența biunivocă care există între mulțimea numerelor naturale și mulțimea perechilor ordonate de numere naturale (între N și N^2) se stabilește de obicei prin indicarea acestei corespondențe, fără a explicita funcțiile (directă și inversă) care realizează această corespondență. Astfel se așează toate perechile de numere naturale într-un tablou dreptunghiular infinit:

1,1	1,2	1,3	1,4	. . .
2,1	2,2	2,3	2,4	. . .
3,1	3,2	3,3	3,4	. . .
4,1	4,2	4,3	4,4	. . .
.	.	.	.	
.	.	.	.	
.	.	.	.	

și la fiecare din aceste perechi de numere naturale se pune în corespondență cîte un număr natural, fie prin metoda diagonală:

1	2	4	7	. . .
3	5	8	12	. . .
6	9	13	18	. . .
10	14	19	25	. . .
.	.	.		
.	.	.		
.	.	.		

fie prin metoda fîșiilor dreptunghiulare

1	2	5	10	. . .
4	3	6	11	. . .
9	8	7	12	. . .
16	15	14	13	. . .
.	.	.	.	
.	.	.	.	

fie printr-o altă metodă. Astfel se pune problema găsirii unor funcții:

$$n(s, t) \qquad (N^2 \longrightarrow N)$$

$$s(n),\ t(n) \qquad (N \longrightarrow N)$$

cu proprietățile:

a) $n(s, t) \neq n(s', t')$

pentru orice:

$$(s, t),\ (s', t') \in N^2,\ (s, t) \neq (s', t');$$

b) $n(s, t) = k$

pentru orice $k \in N$ are o soluție (unică)

$$(s, t) \in N^2;$$

c) $n[(s\,k),\ t\,(k)] = k$

pentru $k \in N$;

d) $s(n(k, l)) = k,\ \ t(n(k,l)) = l$

pentru $(k, l) \in N^2$.

Prin metoda diagonală:

(1) $1 \leftrightarrow (1,1),\ 2 \leftrightarrow (1,2),\ 3 \leftrightarrow (2,1),\ 4 \leftrightarrow (1,3),\ 5 \leftrightarrow (2,2), \ldots$

sau prin metoda *fîșiilor dreptunghice*:

(2) $1 \leftrightarrow (1,1),\ 2 \leftrightarrow (1,2),\ 3 \leftrightarrow (2,2), 4 \leftrightarrow (2,1),\ 5 \leftrightarrow (1,3), \ldots$

se realizează cîte o corespondență biunivocă între N și N^2. (Există și alte corespondențe, dar cele de mai sus sînt mai uzuale.)

În această lucrare vom cerceta forma explicită a funcțiilor care realizează aceste corespondențe biunivoce.

Prin $[a]$ vom nota partea întreagă a numărului real a, adică cel mai mare număr întreg care nu depășește numărul a.

Metoda diagonală. Pe a l-a diagonală se află următoarele l perechi de numere naturale:

$$(1, l),\ (2, l-1),\ (3, l-2), \ldots, (s, t), \ldots,\ (l,\ 1)$$

unde $s + t = l + 1$. Astfel pe cele $l - 1$ diagonale precedente se află:

$$1 + 2 + 3 + \ldots + (l-1) = \frac{(l-1)\,l}{2}$$

perechi de numere naturale, deci notînd cu $n_1(s, t)$ numărul natural care corespunde perechii ordonate (s, t) de numere naturale, vom avea :

$$n_1(1, l) = \frac{(l-1)\,l}{2} + 1.$$

Pentru $s + t = l + 1$, adică $l = s + t - 1$ vom avea :

$$n_1(s, t) = \frac{(l-1)\,l}{2} + s = \frac{(s+t-2)\,(s+t-1)}{2} + s.$$

Dacă perechea corespunzătoare numărului natural n se află pe diagonala $\lambda = \lambda(n)$, atunci

$$\frac{(\lambda-1)\cdot\lambda}{2} + 1 \leqslant n \leqslant \frac{\lambda(\lambda+1)}{2}.$$

Cazurile extreme corespund la :

$$\lambda = \frac{1+\sqrt{8n-7}}{2} \text{ și } \lambda = \frac{-1+\sqrt{8n+1}}{2}.$$

Pentru orice număr natural n are loc inegalitatea :

$$\frac{1+\sqrt{8n-7}}{2} > \frac{-1+\sqrt{8n+1}}{2}.$$

Astfel, diagonala $\lambda = \lambda(n)$ pe care se află perechea corespunzătoare numărului n, este dată de formula :

$$\lambda(n) = \left[\frac{1+\sqrt{8n-7}}{2}\right].$$

Perechea (s, t) se află pe diagonala $s + t - 1$, prin urmare pentru a afla funcțiile $s_1(n)$, $t_1(n)$ care dau perechea :

$$(s_1, t_1)$$

de numere naturale care corespund numărului natural n, trebuie rezolvat sistemul de ecuații :

$$\begin{cases}(s_1 + t_1 - 2)\,(s_1 + t_1 - 1) + 2s_1 = 2n \\ s_1 + t_1 = \lambda(n) + 1.\end{cases}$$

Vom avea :

$$\lambda(\lambda - 1) + 2s_1 = 2n$$

de unde

$$s_1(n) = n - \frac{\lambda(\lambda-1)}{2} = \frac{2n - \left[\frac{1+\sqrt{8n-7}}{2}\right]^2 + \left[\frac{1+\sqrt{8n-7}}{2}\right]}{2}$$

$$t_1(n) = \lambda + 1 - s_1 = \frac{\left[\frac{1+\sqrt{8n-7}}{2}\right]^2 + \left[\frac{-1+\sqrt{8n-7}}{2}\right] - 2n + 2}{2}.$$

Metoda fîșiilor dreptunghice. Pe fîșia l se află perechea de numere :

$$(1, l),\ (2, l), \ldots,\ (l-1, l),\ (l, l),\ (l, l-1), \ldots,\ (l, 2),\ (l, 1)$$

în număr de $2(l-1) + 1 = 2l - 1$. Astfel perechii $(1, l)$ din această fîșie îi corespunde numărul natural

$$n_2(1, l) = 1 + \sum_{k=1}^{l-1}(2k-1) = (l-1)^2 + 1.$$

Dacă $s \leqslant t$, atunci faptul că (s, t) se află pe fîșia l, corespunde la $t = l$, și în acest caz numărul natural care corespunde perechii (s, t) de numere naturale, este dat de formula :

$$n_2(s, t) = (l-1)^2 + s = (t-1)^2 + s.$$

Dacă $s > t$, atunci faptul că (s, t) se află pe fîșia l, corespunde la $s = l$ și în acest caz :

$$n_2(s, t) = (l-1)^2 + l + (l-t) =$$
$$= s^2 - 2s + 1 + s + s - t = s^2 - t + 1.$$

Astfel,

$$n_2(s, t) = \begin{cases}(t-1)^2 + s & \text{pentru } s \leqslant t \\ s^2 - t + 1 & \text{pentru } s > t.\end{cases}$$

Dacă perechea corespunzătoare numărului natural n :

$$(s_2(n), t_2(n))$$

se află pe fîșia $\mu = \mu(n)$, atunci

$$(\mu-1)^2 + 1 \leqslant n \leqslant \mu^2.$$

Cazurile extreme corespund la :

$$\mu = 1 + \sqrt{n-1} \text{ și } \mu = \sqrt{n}.$$

Pentru orice număr natural n are loc inegalitatea :

$$1 + \sqrt{n-1} \leqslant \sqrt{n} \qquad (\text{cînd } n = 1).$$

Astfel

$$\mu(n) = \begin{cases}1 + [\sqrt{n}] & \text{dacă } [\sqrt{n}] < \sqrt{n} \\ \sqrt{n} & \text{dacă } [\sqrt{n}] = \sqrt{n}.\end{cases}$$

Perechea (s_2, t_2) se află pe fîșia :

$$\mu = \max(s_2, t_2) = \frac{1}{2}(s_2 + t_2 + |s_2 - t_2|).$$

Pentru a afla funcțiile $s_2(n)$ și $t_2(n)$ vom avea de rezolvat sistemul de ecuații :

$$\begin{cases}n_2(s_2, t_2) = n \\ s_2 + t_2 + |s_2 - t_2| = 2\mu(n).\end{cases}$$

Dacă : $[\sqrt{n}] = \sqrt{n}$, atunci

$$s_2(n) = \sqrt{n} \text{ şi } t_2(n) = 1.$$

Fie acuma $[\sqrt{n}] < \sqrt{n}$. În acest caz : $\mu(n) = 1 + [\sqrt{n}]$ şi astfel sistemul de mai sus devine :

$$\begin{cases} n_2(s_2, t_2) = n \\ s_2 + t_2 + |s_2 - t_2| = 2 + 2\ [\sqrt{n}]. \end{cases}$$

Dacă $s_2 \leqslant t_2$, atunci vom avea sistemul :

$$\begin{cases} (t_2 - 1)^2 + s_2 = n \\ t_2 = 1 + [\sqrt{n}] \end{cases}$$

cu soluţia :

$$s_2(n) = n - [\sqrt{n}]^2 \; t_2(n) = 1 + [\sqrt{n}].$$

Astfel, condiţia $s_2 \leqslant t_2$ revine la

$$n - [\sqrt{n}]^2 \leqslant 1 + [\sqrt{n}]$$

adică :

$$s_2(n) = n - [\sqrt{n}]^2$$

$t_2(n) = 1 + [\sqrt{n}]$ pentru $n \leqslant [\sqrt{n}]^2 + [\sqrt{n}] + 1$ şi $[\sqrt{n}] < n$.

Dacă $s_2 > t_2$, atunci vom avea sistemul :

$$\begin{cases} s_2^2 - t_2 + 1 = n \\ s_2 = 1 + [\sqrt{n}] \end{cases}$$

cu soluţia

$$s_2(n) = 1 + [\sqrt{n}], \quad t_2(n) = (1 + [\sqrt{n}])^2 - n + 1.$$

Condiţia $s_2 > t_2$ revine deci la

$$n > [\sqrt{n}]^2 + [\sqrt{n}] + 1,$$

adică :

$$s_2(n) = 1 + [\sqrt{n}]$$

$t_2(n) = (1 + [\sqrt{n}])^2 - n + 1$ pentru $n > [\sqrt{n}]^2 + [\sqrt{n}] + 1$ şi $[\sqrt{n}] < \sqrt{n}$.

ŞIRURI DE TRAPEZE ÎNSCRISE ÎN CONICE*

III

E. CARAMAN

Soluţia analitică a teoremelor prof. D. Pompeiu şi T. Lalescu

Se consideră pentagonul $ABCDE$, format din trapezele $ABCD$ şi $BCDE$, cu bazele în rapoartele reale $AD/BC = k_1$ şi $BE/CD = k_2$, egale în teorema lui Pompeiu, diferite în teorema lui Lalescu). Prin vîrfurile acestui pentagon trece o conică.

* Continuare din G. M. – A nr. 9/1965 şi nr. 8/1966