Egy ortogonális latin négyzetekkel kapcsolatos problémáról

Knuth Előd

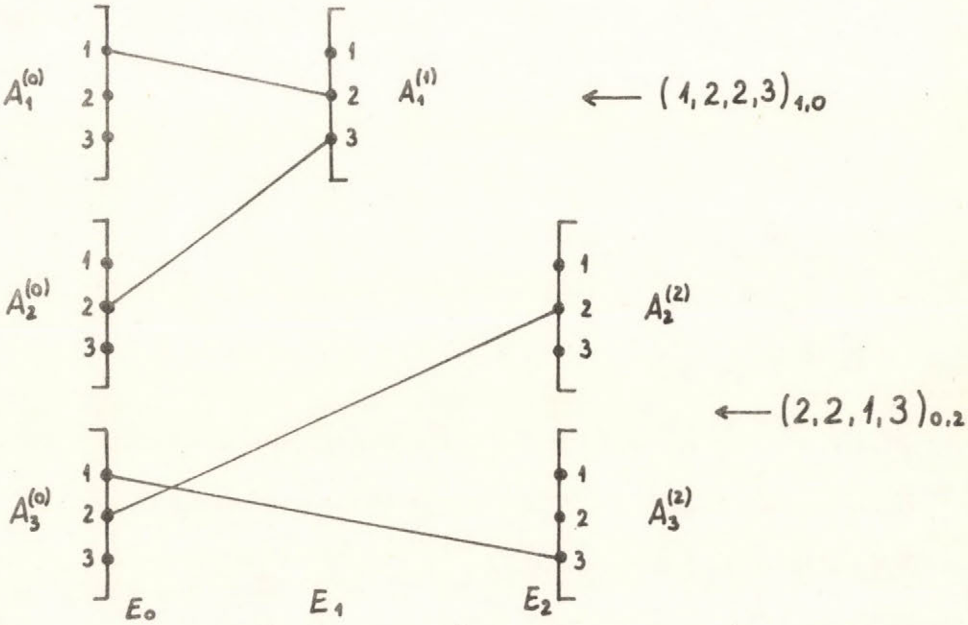
I. Az alapprobléma

Telefonközpontok tervezésénél merült fel a következő probléma:

Adva van $l+1$ db. "egység" - jelölje ezeket $E_o,\ldots E_l$. Minden egységen belül n db "alegység" - jelölje ezeket $A_i^{(k)}$ $k=0,\ldots$; $i=1,\ldots m$. Az egyes alegységek pedig n db. (1-től n-ig sorszámozott) csatlakozási pontot tartalmaznak.

Bizonyos csatlakozási pontok között összeköttetést létesitünk. Ha valamelyik összekötés egy k-sorszámu csatlakozási pontot egy j-sorszámuval köt össze, nevezzük (k,j) összekötésnek. A továbbiakban minden összekötés egyik (és csak egyik) végpontja E_o-hoz fog tartozni, ezért feltehetjük, hogy (k,j) rendezett pár és első eleme az E_o-beli alegység csatlakozási pontjának sorszáma.

Ha az E_o, E_s egységek közti (k_1, j_1), (k_2,j_2) összekötések egy-egy végpontja E_o-ban ill. E_s-ben egy alegységbe esik, akkor nevezzük ezt $(k_1, j_1, k_2, j_2)_{o,s}$ ill. $(k_1, j_1, k_2, j_2)_{s,o}$ összekötéspárnak:



$(k_1, j_1, k_2, j_2)_{u,v}$ és $(k_2, j_2, k_1, j_1)_{u,v}$ között nyilvánvalóan nem teszünk különbséget.

A feladat ezekután a következő:

Konstruálandó az összeköttetéseknek egy rendszere, mely kielégiti az alábbi feltételeket:

1/ E_o minden alegysége E_s minden alegységével össze van kötve egyszeresen $(s=1,2,\ldots l)$, ezen kivül más összekötések nincsenek.

Ez a feltétel az összekötések rendszerének egy egyszerü és szemléletes ábrázolására nyujt lehetőséget:

Készitsünk egy nxn-es négyzet alaku táblázatot, és p-edik sorának r-edik helyére irjuk be az $A_p^{(o)}$, $A_r^{(s)}$ alegységek összekötésének fent definiált (k,j) számpárját. Az 1/ feltétel szerint ekkor a négyzet minden helyére pontosan egy számpár kerül.

Ezt a táblázatot s minden megengedett értékére elkészithetjük. Az összekötések teljes rendszerét igy egy rendezett párokat tartalmazó n x nl-es (azaz l négyzetből álló) mátrixszal reprezentálhatjuk.

2/ Minden csatlakozópontból indul ki összekötés, és minden alegységből minden lehetséges sorszámhoz megy legalább egy összekötés.

Eddigiekből következik, hogy E_o minden csatlakozópontjából pontosan l db összekötés indul ki - minden egységhez egy - E_s, s $\neq$ o, csatlakozópontjaiból pedig mindig csak egyetlen. Továbbá E_o minden alegységéből minden lehetséges sorszámhoz l db összekötés megy, - minden egységhez pontosan egy - E_s, s $\neq$ o, alegységeiből pedig minden lehetséges sorszámhoz egyetlen összekötés megy.

A fent definiált mátrixra ez azt jelenti, hogy annak minden négyzetében minden sorban és minden oszlopban, a beirt számpár bármelyik elemében az 1,2,...n számok egy permutációja szerepel. Másszóval a mátrix minden négyzete a beirt számpár mindkét elemében latin négyzet.

3/ Ha (k_1, j_1) és (k_2, j_2) az E_o egységet ugyanazon egységgel kötik össze, akkor $(k_1, j_1) \neq (k_2, j_2)$.

Ez a feltétel biztositja, hogy bármely összekötés egyértelmüen meghatározza az általa összekötött alegységeket. /Az adott egységeken belül./

Nyilvánvaló, hogy igy a matrix minden négyzete minden lehetséges számpárt tartalmazni fog, mégpedig pontosan egyszer. Másszóval a matrix minden négyzete ortogonális latin-négyzet.

4/ Ugyanazon k_1, j_1, k_2, j_2 értékekhez nem létezik két $(k_1, j_1, k_2, j_2)_{u,v}$ összekötéspár, még különböző u, v értékek mellett sem.

Ez a feltétel nyilvánvalóan azt biztositja, hogy bármely összekötéspár egyértelmüen meghatározza az összekötéseiben szereplő alegységeket, és még az ezeket tartalmazó egységeket is.

Definició szerint egy összekötéspár összekötéseit jellemző számpárok az s-edik négyzetben $(k_1, j_1, k_2, j_2)_{s,o}$

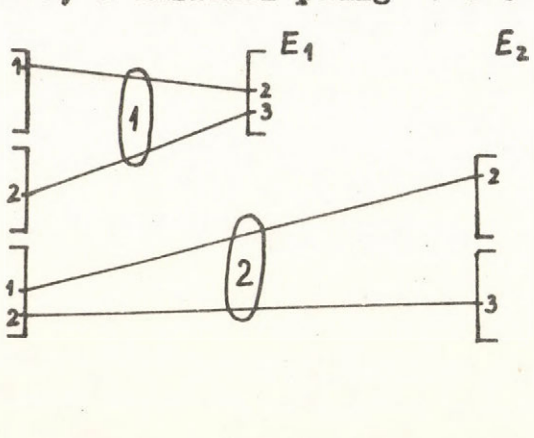
esetén egy sorba $(k_1, j_2, k_2, j_2)_{o,s}$ esetén pedig egy oszlopba kerülnek. Nevezzük a négyzetek sorait és oszlopait közös néven vonalaknak. Mátrixunkra a 4/ feltétel ekkor nyilvánvalóan azt jelenti, hogy nincs két egyvonalba eső számpárja. /Ld. pl. az utolsó oldalon szereplő példákat./

Világos másrészt, hogy minden, az itt leirt tulajdonságokkal rendelkező matrix egyértelmüen meghatározza az összeköttéseknek egy az 1/ - 4/ feltételeket kielégitő rendszerét.

II. További kérdések

Gyakorlatban a 4/ feltétel csak ritkán elégithető ki. A probléma ezért a 4/ feltétel bizonyos gyengitései mellett is vizsgálandó.

a/ Megengedjük, hogy legyen két olyan összeköttés pár, amelyben k_1, j_1, k_2, j_2 azonos, ha az egyiknél $u = 0$, a másiknál pedig $v = 0$ (2. ábra).



Ortogonális latin négyzetekre való átfogalmazásunkban ez azt jelenti, hogy soroknak csak sorokkal, oszlopoknak csak oszlopokkal kell kielégiteni a korábban mondott feltételt.

b/ Tovább gyengithetjük a 4/ feltételt, ha csak azt követeljük, hogy ne legyen két olyan összekötéspár, melyben k_1, j_1, k_2, j_2 megegyezik és mindkettőnél $v = 0$.

Másszóval két összekötéspár csatlakozópont-sorszámai csak akkor nem lehetnek azonosak, ha mindkettő az E_0 egységből indul ki. /Pl. a 2. ábrán az 1 összekötéspár./

/Megjegyzés: annak ellenére, hogy b/ esetén látszólag sokkal gyengébb feltételt kell kielégiteni, az eddigi eredmények alapján valószinünek látjuk, hogy nem jelent komolyabb könnyitést a/-hoz képest./

III. Néhány a problémával kapcsolatos megjegyzés

Mindezek után a következő problémákat vethetjük fel:

I. Adott n és l -hez konstruálandó l db nxn-es ortogonális latin négyzet úgy, hogy semelyik két különböző vonalnak ne legyen egynél több közös eleme.

II. Az előbbi, de csak azt követeljük meg, hogy két sornak vagy két oszlopnak ne legyen egynél több közös eleme.

III. Csak azt követeljük meg, hogy két oszlopnak ne legyen egynél több közös eleme.

Meg fogjuk mutatni, hogy

A/ Az I. feltétel esetén l legfeljebb $\left[\frac{n-1}{2}\right]$, a II. III. feltételek esetén pedig legfeljebb n-1 lehet.

B/ Amennyiben n primszám, ez a határ mindig el is érhető, pl. a következő konstrukciókkal:

I. esetén: $\boxed{a_{ik}^{(j)} = \left(i+k,\ 2ji+(2j-1)k\right)}$ $(mod\ p)$

ahol $a_{ik}^{(j)}$ a j-edik négyzet i-edik sorának k-adik helyére irt elempárt jelenti. /A zárójelbe irt számok moduló p értendők/.

II. és III. esetén pedig:

$$\boxed{a_{ik}^{(j)} = \left(i+k,\ ji+(p-j)k\right)} \quad (mod\ p)$$

$(n=p)$

IV. A kimondott állitások bizonyitása

A/ Tekintsük pl. az (1,1) elemet. Ez minden négyzetben pontosan egyszer fordul elő. Minden alkalommal n-1 elemmel van egy sorban és n-1-el egy oszlopban. Az I. feltétel esetén ezen $2l(n-1)$ elem között azonosak nem szerepelhetnek. Számuk igy legfeljebb azon elemek száma, amelyek az (1,1) elemmel egyáltalán egy sorba vagy oszlopba kerülhetnek. Ezek száma $(n-1)^2$ (azon elemek, melyek az 1 számot nem tartalmazzák.) Az I. feltétel esetén tehát:

$$2l(n-1) \leq (n-1)^2 \qquad \text{azaz} \qquad l \leq \frac{n-1}{2}$$

és ha feltesszük, hogy l egész szám, akkor

$$l \leq \left[\frac{n-1}{2}\right] \qquad \text{-t nyerjük.}$$

A III. feltétel esetén csak az (1,1)-el egy oszlopba eső elemek jönnek számitásba. Ezek száma (n-1). Igy

$$l(n-1) \leq (n-1)^2 \qquad \text{tehát} \qquad l \leq n-1$$

Tekintettel arra, hogy a II. feltétel a III. feltételt magában foglalja, az előbb mondottak erre az esetre is vonatkoznak.

B/ Megmutatjuk, hogy n = primszám esetén a bemutatott konstrukciók valóban kielégitik az előirt feltételeket.

Tekintettel arra, hogy mindegyik konstrukció

$$b_{ij} = (i+j,\ ui+vj)$$ alaku,

ahol $0 \not\equiv U \not\equiv V \not\equiv 0$ (mod p), először megmutatjuk, hogy $\{b_{ij}\}_{i,j=1}^{p}$ ortogonális latin négyzet.

Triviális, hogy $\{b_{ij}\}_1^p$ mindkét indexében latin négyzet, azt kell csak belátni, hogy $b_{i_1 j_1} = b_{i_2 j_2}$ esetén $i_1 \equiv i_2,\ j_1 \equiv j_2$.

Ezt pedig egyszerü számolással nyerhetjük:

ha

$$\begin{aligned} i_1 + j_1 &\equiv i_2 + j_2 \\ ui_1 + vj_1 &\equiv ui_2 + vj_2 \end{aligned} \qquad (\mathrm{mod}\ p)$$

akkor

$$i_1 - i_2 \equiv j_2 - j_1$$

$$u(i_1 - i_2) + v(j_1 - j_2) \equiv 0\ , \quad \text{igy} \quad (u-v)(i_1 - i_2) \equiv 0$$

tekintettel arra, hogy $u \not\equiv v$ (mod p) ebből $i_1 \equiv i_2$ adódik. Tekintsük most az I. feltételhez tartozó konstrukciót:

$$a_{ij}^{k} \equiv (i+j,\ 2ki + (2k-1)j) \qquad \mathrm{mod}\ p$$

Tegyük fel, hogy $a^{k_1}_{i_1 j_1} = a^{k_2}_{i_2 j_2}$ ahol $k_1 \neq k_2$

Vezessük be az alábbi rövid jelöléseket:

$$A_1 = \{a^{k_1}_{i j_1}\}_{i \neq i_1} \qquad A_2 = \{a^{k_1}_{i_1 j}\}_{j \neq j_1}$$

$$B_1 = \{a^{k_2}_{i j_2}\}_{i \neq i_2} \qquad B_2 = \{a^{k_2}_{i_2 j}\}_{j \neq j_2}$$

Ekkor az I. feltétel nyilvánvalóan a következővel ekvivalens:

$$(A_1 \cup A_2) \cap (B_1 \cup B_2) = \phi$$

Szimmetria okokból ehhez elegendő belátni, hogy

a/ $A_1 \cap B_1 = \phi$

és b/ $A_1 \cap B_2 = \phi$ teljesülnek.

a/ Tegyük fel, hogy léteznek olyan i_3, i_4 indexek, melyekre

$i_3 \neq i_1$, $i_4 \neq i_2 \pmod p$ és $a^{k_1}_{i_3 j_1} = a^{k_2}_{i_4 j_2}$

A definició szerint ekkor:

$$\left.\begin{aligned} i_1 + j_1 &\equiv i_2 + j_2 \\ 2k_1 i_1 + (2k_1 - 1) j_1 &\equiv 2k_2 i_2 + (2k_2 - 1) j_2 \\ i_3 + j_1 &\equiv i_4 + j_2 \\ 2k_1 i_3 + (2k_1 - 1) j_1 &\equiv 2k_2 i_4 + (2k_2 - 1) j_2 \end{aligned}\right\} \pmod p$$

Ezekből átrendezésekkel a következő kongruenciát nyerhetjük:

$$2(k_1 - k_2)(i_1 - i_3) \equiv 0 \pmod p$$

Ez pedig feltételeink és p prim volta miatt lehetetlen.

b/ Tegyük fel, hogy léteznek olyan i_3, j_3 indexek, melyekre $i_3 \not\equiv i_1$, $j_3 \not\equiv j_1$ $(mod\, p)$ és $a_{i_3 j_1}^{k_1} = a_{i_2 j_3}^{k_2}$

Ekkor

$$\left.\begin{aligned} i_1 + j_1 &\equiv i_2 + j_2 \\ 2k_1 i_1 + (2k_1 - 1)j_1 &\equiv 2k_2 i_2 + (2k_2 - 1)j_2 \\ i_3 + j_1 &\equiv i_2 + j_3 \\ 2k_1 i_3 + (2k_1 - 1)j_1 &\equiv 2k_2 i_2 + (2k_2 - 1)j_3 \end{aligned}\right\} \quad (mod\, p)$$

Ebből a következő nyerhető:

$$[2(k_1 - k_2) + 1](i_1 - i_3) \equiv 0 \qquad (mod\, p)$$

Tekintettel arra, hogy $i_1 \not\equiv i_3$ és $1 \leq k_1, k_2 \leq \frac{p-1}{2}$ ez lehetetlen.

Tekintsük most a II. feltételhez tartozó konstrukciót:

$$a_{ij}^{k} \equiv (i+j,\ ki + (p-k)j) \qquad (mod\, p)$$

Tegyük fel most is, hogy $a_{i_1 j_1}^{k_1} = a_{i_2 j_2}^{k_2}$ ahol $k_1 \not\equiv k_2$

Előbbi jelöléseinkkel most a következőt kell belátni:

$$(A_1 \cap B_1) \cup (A_2 \cap B_2) = \phi$$

A szimmetria miatt elég $A_1 \cap B_1 = \Phi$ -t bebizonyitani. Tegyük fel, hogy léteznek olyan i_3, i_4 indexek, melyekre $i_1 \not\equiv i_3$, $i_2 \not\equiv i_4 \pmod p$ és $a_{i_3 j_1}^{k_1} = a_{i_4 j_2}^{k_2}$

Definiciónk szerint ekkor:

$$\left.\begin{aligned} i_1 + j_1 &\equiv i_2 + j_2 \\ k_1 i_1 + (p-k_1) j_1 &\equiv k_2 i_2 + (p-k_2) j_2 \\ i_3 + j_1 &\equiv i_4 + j_2 \\ k_1 i_3 + (p-k_1) j_1 &\equiv k_2 i_4 + (p-k_2) j_2 \end{aligned}\right\} \pmod p$$

Az előbbiekhez hasonlóan ebből azonban $(k_1 - k_2)(i_1 - i_3) = 0$ következne, ami lehetetlen.

Ezzel azt is beláttuk, hogy e konstrukció a III. feltételt is kielégiti, hiszen az ennél gyengébb kikötéseket tartalmaz.

V. Néhány példa:

n = 7-re az I. sz. feltétel mellett:

11	22	33	44	55	66	77
23	34	45	56	67	71	12
35	46	57	61	72	13	24
47	51	62	73	14	25	26
52	63	74	15	26	37	41
64	75	16	27	31	42	53
76	17	21	32	43	54	65

11	24	37	43	56	62	75
25	31	44	57	63	76	12
32	45	51	64	77	13	26
46	52	65	71	14	27	33
53	66	72	15	21	34	47
67	73	16	22	35	41	54
74	17	23	36	42	55	61

11	26	34	42	57	65	73
27	35	43	51	66	74	12
36	44	52	67	75	13	21
45	53	61	76	14	22	37
54	62	77	15	23	31	46
63	71	16	24	32	47	55
72	17	25	33	41	56	64

n=5-re a II. feltétellel:

11	22	33	44	55
25	31	42	53	14
34	45	51	12	23
43	54	15	21	32
52	13	24	35	41

11	23	35	42	54
24	31	43	55	12
32	44	51	13	25
45	52	14	21	33
53	15	22	34	41

11	24	32	45	53
23	31	44	52	15
35	43	51	14	22
42	55	13	21	34
54	12	25	33	41

11	25	34	43	52
22	31	45	54	13
33	42	51	15	24
44	53	12	21	35
55	14	23	32	41

Irodalom:

[1] R.C. Bose and S.S. Shrikande: On the falsity of Euler's conjecture about the non existence. of two orthogonal Latin squeres of order 4k+2 Proc. Mat. Acad. Sci. USA. 1959. p. 734.

[2] R.C.Bose and S.S. shrikande: Mutually orthogonal Latin squares. Transactions of the Amer. Math. Soc. 1960. p.191.

[3] D.M.Johson, A.L.Dulmage, N.S.Mendelsohn: Orthomorhism of groups and orthogonal Latin squares. Canadian Journ. of.Math. 1961. p.356.

[4] E.T.Parker: Ortogonal latin squares. Proc.Mat.Acad.Sci.USA. 1959. p. 859.

[5] J.Singer: A class of groups associated with Latin squares. Amer.Math.Monthly.1960.p.235.

[6] K.Yamamoto: Generation principles of Latin squares. Rep.Stat.Appl.Res.Union.Sap.Sci.Eng.1961.p.73.

[7] R.C.Bose, I.M.Chakravarti; D.E.Knuth: On methods of constructing sets of mutually orthogonal Latin squares using a computer I-II. Technometics 1960. p. 507.1961.p.111.

Summary

On a problem of orthogonal Latin squares.

The paper translates a problem concerning the design of telephone exchanges into the language of orthogonal Latin squares. In general, inequalities are deduced for the problem, on the other hand a construction process is given in certain special cases /in case of prime order/.