数理解析研究所講究録
204巻 1974年 8-21

8

Socio-Combinatorics

by Konrad Jacobs
in Erlangen

Everybody knows the marriage theorem of Ph. Hall [3] and W. Maak [7] (see aslo Halmos-Vaughan [4], Maak [8], Jacobs [5]) as an example of a combinatorial theorem which allows of a completely elementary proof and has a sociological interpretation. It is the purpose of the present article to bring three more theorems of the same character to the attention of the reader: V. Strehls theorem on unreliable coalitions, K. Arrows dictatorship theorem, and the friendship theorem of Erdös-Rényi-Sós. It is to be admitted that Arrows dictatorship theorem is the only one among these four which originally stems from sociological investigations. In all other cases the sociological interpretation was only given after the theorem had been found in the course of combinatorial investigations. The coming of "marriage theorem" goes back to Weyl [10], and "friendship" seems to have been mentioned first by Wilf [11].

We will outline an unpublished proof of V. Strehl for his theorem, Kirman-Sondermanns [6] proof of the dictatorship theorem (although this is not the shortest proof; for this see Blau, J. H. [12]), and Wilfs [11] proof of the friendship theorem. All proofs are quite elementary and suggest themselves (as well as the theorems, of course) strongly for

being included in lectures for a wider audience like those published in the Selecta Mathematica series of the Springer-Verlag.

§1. Unreliable coalitions.

Let X be a finite set, to be interpreted as the voting body of some parliament. Nonempty subsets C of X are called coalitions accordingly. A voting function on the set of all coalitions is a ± 1-valued function v such that

$$v(C \cup D) = v(C) \quad (C \cap D = \phi, \quad v(C) = v(D)).$$

A voting function is called linear if there are rationally independent reals $c(x)$ $(x \in X)$ such that

$$v(C) = 1 \quad \text{iff} \quad \sum_{s \in C} c(x) \geq 0.$$

It can be shown that in all cases where the power $|X|$ of X is ≤ 4 every voting function is linear. For $|X| \geq 5$ there are nonlinear voting functions.

There are obviously only the following two ways in which the values $v(E)$, $v(F)$ of 2 coalitions E, F can uniquely determine $v(C)$:

1) C is the disjoint union of E and F, and $v(E)=v(F)$. We have then

$$v(C) = v(E) = v(F).$$

2) C and E are disjoint with union F, and $v(E)=-v(F)$. We have then

$$v(C) = v(F)$$

(because otherwise $v(C)=v(E)=-v(F)$, which is impossible). E and F can exchange their places in either 1) or 2), of course. In both cases we call the set $\{E, F\}$ a derivation of C.

Definition 1.1. A coalition is called unreliable (for v) if it has no derivation.

Unreliability of C thus means: however you split C, the two parts do not vote in the same way; and no matter what you add to C, its vote is the vote of the union.

There are, of course, some trivial cases. Take e.g. a linear v with all $c(x)>0$. Then the only unreliable coalitions are the singletons. Or take a linear v with $c(x)>0$ except for one $x=x_0$, where $|c(x_0)| > \sum_{x\neq x_0} c(x)$. Then again the singletons $\neq x_0$ and X are the only unreliable coalitions. The reader is invited to invent more complicated examples on the same line.

Consider now the coalitions as vectors in R^X via their indicator functions. The above examples suggest that there are always at least $|X|$ linearly independent unreliable coalitions. There are counterexamples showing that this is

not generally true for $|X| \geq 7$. But there is one easy result, which is a small particle in a large bulk of unpublished investigations of V. Strehl running under the headline "fluctuation theory".

Theorem 1.2. If v is linear, then every coalition is a linear combination of unreliable coalitions, i.e. there are $|X|$ linearly independent unreliable coalitions.

In order to prove this, one has only to realize two things

1) passing from C to a derivation $\{E, F\}$ implies a representation of 1_C as a (rational) linear combination of 1_E and 1_F.

2) If E and F constitute a derivation of C, then

$$\left|\sum_{x \in C} c(x)\right| > \left|\sum_{y \in E} c(y)\right|, \left|\sum_{z \in F} c(z)\right|$$

(exercise). Running through successive derivations one builds a binary "tree" which ends up in unreliable coalitions after a finite number of steps.

§2. The dictatorship theorem.

Let again X be a finite set which is to be interpreted as the set of the individuals in a society. Let A be a finite set of "alternatives" and put $|A|=n$. Every indi-

vidual $x \in X$ chooses one of the $n!$ possible total strict orderings of A as its individual preference order in A. Write

$$a \underset{f(x)}{<} b$$

if, for such a choice having been made by all individuals, x prefers b to a. Let C denote the set of all $(n!)^{|X|}$ possible systems f of individual preference orders.

Definition 2.1. A mapping s of C into the set of all $n!$ possible preference orders in A is called a social choice if it obeys the following two rules:

1) Unanimity: If $a \underset{f(x)}{<} b$ for all $x \in X$, then also $a \underset{s(f)}{<} b$.

2) Independence: Let f, g, a, b be such that $a \underset{f(x)}{<} b$ iff $a \underset{g(x)}{<} b$. Then

$$a \underset{s(f)}{<} b \text{ iff } a \underset{s(g)}{<} b.$$

Definition 2.2. A family $\phi \neq F \subseteq X$ is said

1) to win over its complement for s if

$$a \underset{f(x)}{<} b \quad (x \in F), \quad b \underset{f(x)}{<} a \quad (x \notin F)$$

imply $a \underset{s(f)}{<} b$ for every $f \in C$, $a, b \in A$.

2) to rule (for s) if $a \underset{f(x)}{<} b$ $(x \in F)$ implies $a \underset{f(x)}{<} b$ for all $f \in C$, $a, b \in A$ (no matter what the $x \notin F$ do

about a and b).

A ruling singleton is called a dictator (for the given s).

Arrows famous result is

Theorem 2.3. For $n \geq 3$, and every social choice there is exactly one dictator.

The proof outlined here is due to Kirman-Sondermann[6].

The first step is a proof that, for any social choice s, the system of all families winning over their complements is the same for all couples $a \neq b$ in A. One does it by first replacing a, then b by some other alternative in A. Thus we can, for the rest of the proof, limit ourselves to, say, three fixed elements a, b, c of A.

The next step consists in proving that the system of all families winning over their complements forms an ultrafilter. Let us outline how it is shown that e.g. the intersection $E \cap F$ of two such families is again such a family:

For $x \in F \cap G$ we choose $a \underset{f(x)}{<} b \underset{f(x)}{<} c$.

For $x \in F \setminus G$ we choose $b \underset{f(x)}{<} c \underset{f(x)}{<} a$.

For $x \in G \setminus F$ we choose $c \underset{f(x)}{<} a \underset{f(x)}{<} b$.

For $x \notin F \cup G$ we choose $c \underset{f(x)}{<} b \underset{f(x)}{<} a$.

Now we see that for $x \in F=(F \cap G) \cup (F \setminus G)$ we have $b_{f(x)} < c$, and for $x \notin F$ we have $c < b_{f(x)}$. As F wins over its complements, we have $b_{s(f)} < c$.

Similarly we have for $x \in G=(F \cap G) \cup (G \setminus F)$ $a_{f(x)} < b$ and for $x \notin G$ we have $b_{f(x)} < a$. As G wins over its complement, we have $a_{s(f)} < b$. By transitivity, $a_{s(f)} < c$ follows. But for $x \in F \cap G$ we have $a_{f(x)} < c$, and for $x \notin F \cap G$ we have $c < a_{f(x)}$, thus showing that also $F \cap G$ wins over its complement. By similar arguments the other ultrafilter properties are verified.

In the third step of the proof we show that the ruling families form an ultrafilter, more precisely: Let F be a winning family and $a_{f(x)} < b$ $(x \in F)$. Then $\{x \mid a_{f(x)} < b\} \supseteq F$, hence belongs also to the aforementioned ultrafilter, i.e. is winning, and $a_{s(f)} < b$ follows, i.e. F rules.

The last step in the proof consists in realizing that an ultrafilter contains exactly one singleton. In our case, this is the dictator.

One can establish an ultrafilter theorem of the above type also for infinite X, and for so-called "weak orderings" (Fishburn [2]). In this more general situation one can prove the converse statement that every ultrafilter in X is induced by some social choice s.

The proofs clearly show that it is mainly the axiom of

independence ("forgetfulness") which is responsible for the existence of a dictator. But no analogous theory avoiding dictatorship reasonably is known to me.

§3. Friendship.

Let X be a finite set (of persons) and $\sim$ a non-reflexive non-transitive symmetric binary relation in X which we call "friendship". Let us assume the following

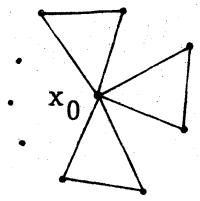
Friendship Axiom. For any $x,y \in X$ with $x \neq y$ there is exactly one

$$z = F(x, y) \in X$$

such that $x \sim z$, $y \sim z$, i.e. any two different persons have exactly one common friend.

This axiom is e.g. fulfilled in the following

Example 3.1. X has an odd number $2n+1$ of elements, and there is one x_0 which is the friend of everybody (a "politician") while the rest of $2n$ persons can be partitioned into n couples of friends. We may picture this situation as follows



The friendship theorem 3.2 below states that this example represents the general case.

Theorem 3.2. If the friendship axiom holds, then there is exactly one "politician" x_0, $|X|$ = odd = $2n+1$, and the remaining $2n$ persons can be divided into n couples of friends.

We outline the simple proof given by Wilf [11] in 1971. The friendship axiom strongly suggests the use of the theory of projective planes. Actually, if we denote for every x by $\ell(x)$ the set of all friends of x, i.e. $\ell(x)=\{y|x\sim y\}$, and call the $\ell(x)$ "lines", $\ell(x)$ being the line determined by x, then the friendship axiom reads as the following well-known axiom for the projective plane:

Axiom I: Any two different lines intersect in exactly one point: $x\neq y$ implies $\ell(x)\cap\ell(y)=\{F(x,y)\}$.

It also reads as

Axiom II. Through any two different points x, y there is exactly one line, namely $\ell(F(x,y))$.

For the projective plane there is still the

Axiom III. There are four different points, no three of them lying on the same line.

This axiom III can be derived from the

Assumption: There is no "politician", i.e. for any $x\in X$ there is at least one $y\neq x$ such that $y\notin\ell(x)$.

We omit the derivation of axiom III from this assumption as well as the derivation of theorem 3.2 from the existence of a "politician" and concentrate upon leading the assumption

to a contradiction.

Under the assumption, we have X as a finite projective plane with the lines $\ell(x)$. Well-known elementary statements about finite projective planes (see e.g. Ryser [9]) show that there is a natural number m such that

$$|X| = m^2 + m + 1$$

and this is also the number of different lines. m is the number of points on every line as well as the number of lines through one point, and we have $m>1$ in our case. Let us number $X=\{x_1,\ldots,x_{m^2+m+1}\}$ and likewise $\{\ell(x)\,|\,x\in X\}=\{\ell(x_1),\ldots,\ell(x_{m^2+m+1})\}$ and let us consider the incidence matrix

$$A = (a_{jk})_{j,k=1,\ldots,m^2+m+1}$$

where

$$a_{jk} = \begin{cases} 1 & \text{if } x_j \in \ell(x_k) \\ 0 & \text{otherwise} \end{cases} .$$

Since $x \neq x$, we have $a_{jj}=0$ $(j=1,\ldots,m^2+m+1)$ and hence trace $(A) = 0$. On the other hand A is a real symmetric mapping and can be put into diagonal form by a procedure which doesn't change the trace. In order to compute the diagonal form, i.e. the eigenvalues and eigenvectors of A, we first do the same with $A^2=B$. This matrix has the easy-to-handle form

$$B = \begin{bmatrix} m+1 & 1 & 1 & \cdots & 1 \\ 1 & m+1 & 1 & \cdots & 1 \\ 1 & 1 & m+1 & \cdots & 1 \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & 1 & 1 & \cdots & m+1 \end{bmatrix}.$$

In fact the diagonal elements count the number of coincidences of $x \in \ell(y)$ and $y \in \ell(x)$ for a fixed x if y runs. The non-diagonal elements count the number of coincidences of

$$x \in \ell(z) \quad \text{and} \quad z \in \ell(y)$$

for fixed $x \neq y$ (it happens exactly once, namely for $z=F(x,y)$).

Now it is easy to see that B has the following eigenvalues and eigenvectors:

1) $(m+1)+(m^2+m)=(m+1)^2$ is a simple eigenvalue for the eigenvector $(1,\ldots,1)$.
2) m is a (m^2+m)-fold eigenvalue for the eigenvectors

$$\begin{array}{ccccccccc} (1, & -1, & 0, & 0, & \ldots & , & 0) \\ (0, & 1, & -1, & 0, & \ldots & , & 0) \\ (0, & 0, & 1, & -1, & \ldots & , & 0) \\ \vdots & & & & & & \\ (0, & 0, & 0, & 0, & \ldots & 1, & -1) \end{array}$$

It is immediately visible that these m^2+m+1 eigenvectors of $B=A^2$ form an orthogonal base of $\mathbb{R}^{m^2+m+1}$. Hence they are also the eigenvectors of A, for the eigenvalues $m+1$, $\pm\sqrt{m},\ldots,\pm\sqrt{m}$ and A may be orthogonally transformed into the shape

$$\begin{bmatrix} m+1 & & & & 0 \\ & \pm\sqrt{m} & & & \\ & & \pm\sqrt{m} & & \\ & & & \ddots & \\ 0 & & & & \pm\sqrt{m} \end{bmatrix}.$$

The trace still being 0, we obtain

$$0 = m + 1 + (\mu_1 - \mu_2)\sqrt{m}$$

where μ_1 is the multiplicity of eigenvalue $+\sqrt{m}$, and μ_2 is the multiplicity of eigenvalue $-\sqrt{m}$. Clearly

$$\mu_1 + \mu_2 = m^2 + m$$

and thus we arrive at

$$\mu_2 = \frac{1}{2}(m^2 + m + \sqrt{m} + \frac{1}{\sqrt{m}}).$$

This, with μ_2 an integer, now easily leads to a contradiction, because then

$$a = \sqrt{m} + \frac{1}{\sqrt{m}} = \frac{m+1}{\sqrt{m}}$$

also is an integer, hence $\sqrt{m}=\frac{u}{v}$ with relatively prime integers $u>0$, v, and we get $v^2m=u^2$ showing $m=u^2$ hence $au=u^2+1$ which has no integer solution a for $u>1$ (the latter being a consequence of $m>1$). Having thus arrived at a contradiction, our assumption is false and a "politician" exists. This proves the friendship theorem 3.2.

Bibliography

[1] Erdös, P., A. Rényi, and V.T. Sős, On a problem in graph theory, Stud. Sci. Math. Hung. Acad. 1, 215-235(1966).

[2] Fishburn, P.C., Utility theory for decision making, New York (Wiley) 1970.

[3] Hall, Ph., On representatives of subsets, J. London Math. Soc. 10, 26-29(1935).

[4] Halmos, P.R., and H. Vaughan, The marriage problem, Amer. J. Math. 72, 214-215(1950).

[5] Jacobs, K., Selecta Mathematica I, Berlin-Göttingen-Heidelberg (Springerverlag) 1968.

[6] Kirman and Sondermann, J. Econ. Theory, 1972.

[7] Maak, W., Eine neue Definition der fastperiodischen Funktionen, Abh. Math. Sem. Univ. Hamburg 11, 240-244(1935).

[8] Maak, W., Fastperiodische Funktionen, 2. Aufl., Berlin-Heidelberg-New York (Springerverlag) 1967.

[9] Ryser, H.J., Combinatorial Mathematics, New York (Wiley) 1963.

[10] Weyl, H., Almost periodic invariant vector sets in a metric vector space, Amer. J. Math. 71, 178-205(1949).

[11] Wilf, H., The friendship theorem, Comb. Math. and its applications, Symp. Oxford 1969, ed. Welsh, Academic Press 1971.

[12] Blau, J.H., A direct proof of Arrow's theorem, Econometrica 40, 61-67(1972).