A theorem on choice functions

KONINKL. NEDERL. AKADEMIE VAN WETENSCHAPPEN – AMSTERDAM
Reprinted from Proceedings, Series A, **60**, No. 4 and Indag. Math., **19**, No. 4, 1957

MATHEMATICS

A THEOREM ON CHOICE FUNCTIONS

BY

N. G. DE BRUIJN

(Communicated by Prof. H. D. KLOOSTERMAN at the meeting of March 30, 1957)

Let M be an infinite set, and let its cardinal number be denoted by $|M| = \mathbf{m}$. Let, for each element $\mu \in M$, a non-empty set A_μ be given. For our purpose it is immaterial whether A_μ's with different μ's have or do not have intersections.

A function f that attaches to every $\mu \in M$ an element of A_μ (so $f(\mu) \in A_\mu$ for all $\mu \in M$) will be called a *choice function*. Two choice functions f_1, f_2 are different if there is a $\mu \in M$ such that $f_1(\mu) \neq f_2(\mu)$. If there are three different choice functions, however, there need not be a μ such that the three values at μ are mutually different. It certainly will not be the case if all A_μ's have just two elements.

Denote the collection of all choice functions by F. For several purposes it is of some importance to have a large subcollection of choice functions which are *independent*, in the following sense: if we take any finite number of elements $f_1, \ldots, f_k$ from the collection, then there is a $\mu \in M$ such that $f_1(\mu), \ldots, f_k(\mu)$ are mutually different. From what we just remarked it is clear that it will be necessary that the order $|A_\mu|$ of A_μ is unbounded if μ runs through M.

We shall impose a slightly stronger condition: we shall assume that the $|A_\mu|$'s are not essentially bounded, i.e. we assume that for every positive integer n there are still $\mathbf{m}$ μ's such that $|A_\mu| > n$. Under this condition we can show that there is a collection of $2^{\mathbf{m}}$ independent choice functions. In many cases this number is equal to the number of all choice functions: if $|A_\mu| \leqslant 2^{\mathbf{m}}$ for all $\mu \in M$, then the total number of choice functions is $(2^{\mathbf{m}})^{\mathbf{m}} = 2^{\mathbf{m}}$ (assuming that $|A_\mu| \geqslant 2$ for $\mathbf{m}$ values of μ).

Theorem. If $|A_\mu|$ is not essentially bounded, then there is an $F^* \subset F$, with $|F^*| = 2^{\mathbf{m}}$, such that the elements of F^* are independent.

Proof. We first show that M can be divided into a countable number of disjoint subsets $M_0, M_1, M_2, \ldots$, such that

$$|M_j| = \mathbf{m} \qquad (j = 0, 1, 2, \ldots),$$
$$|A_\mu| \geqslant 2^j \qquad (\mu \in M_j,\ j = 0, 1, 2, \ldots).$$

This can be done as follows. Let M^i $(i = 0, 1, 2, \ldots)$ denote the set of all μ's with $|A_\mu| \geqslant 2^i$, and put $M^\infty = \bigcap_{i=0}^\infty M^i$. We distinguish two cases. (i) If $|M^\infty| = \mathbf{m}$, then we divide M^∞ into a countable number of disjoint subsets $M_0^\infty, M_1^\infty, \ldots$, each having power $\mathbf{m}$, and we take $M_j = M_j^\infty$ $(j = 1, 2, \ldots)$, $M_0 = M_0^\infty \cup (M \setminus M^\infty)$. (ii) If $|M^\infty| < \mathbf{m}$, then we take $M_0 = M^\infty \cup (M^0 \setminus M^{i_1})$, where i_1 is an integer > 0 with the property that $M^0 \setminus M^{i_1}$ has power $\mathbf{m}$. Next we take $M_1 = M^{i_1} \setminus M^{i_2}$, where i_2 is an integer $> i_1$ such that $M^{i_1} \setminus M^{i_2}$ has power $\mathbf{m}$. We take $M_2 = M^{i_2} \setminus M^{i_3}$, where $i_3 > i_2$, such that $|M_3| = \mathbf{m}$, etc. In both cases it is obvious that the M_j's have the required properties.

Let X be any set with cardinal number $\mathbf{m}$. It is well known that the cartesian products

$$X^2 = X \times X,\ X^3 = X \times X \times X,\ X^4, X^5, \ldots$$

all have cardinal number $\mathbf{m}$. So for $j = 1, 2, 3, \ldots,$ M_j can be mapped one-to-one onto X^j, and there is no objection against assuming that $M_j = X^j$ $(j = 1, 2, \ldots)$.

Let T be a set of two elements, and put $T \times T = T^2$, $T \times T \times T = T^3$, etc. If $j = 1, 2, \ldots,$ $\mu \in M_j$, then T^j can be embedded into A_μ. Our construction of F will only use choice functions whose value at μ is taken from T^j.

The set M_0 is unimportant. For each $\mu \in M_0$ we choose an element $a_\mu \in A_\mu$, and we take $f^*(\mu) = a_\mu$ $(\mu \in M_0)$ for all $f^* \in F^*$. The independence will come from the M_j's with $j > 0$. There is no harm in omitting M_0 entirely.

The problem has thus been reduced to the following case:

$$M = X \cup X^2 \cup X^3 \cup \ldots, \tag{1}$$

and $A_\mu = T^j$ if $\mu \in X^j$ $(j = 1, 2, \ldots)$. The elements of X^j can be described as j-tuples $(x_1, \ldots, x_j)$ $(x_1 \in X, \ldots, x_j \in X)$; the elements of T^j are j-tuples $(t_1, \ldots, t_j)$ $(t_1 \in T, \ldots, t_j \in T)$.

Let F_0 denote the set of all mappings f of X into T. There are $2^{\mathbf{m}}$ such f's. For every $f \in F_0$ we shall define its continuation f^* as a choice function on M. If $f \in F_0$, $j = 1, 2, \ldots,$ we simply define f^* on X^j by

$$f^*((x_1, \ldots, x_j)) = (f(x_1), \ldots, f(x_j)); \tag{2}$$

the right-hand-side is an element of T^j. Obviously $f^*(\mu) = f(\mu)$ if $\mu \in X$. By this extension procedure we have mapped F_0 one-to-one into F, for if f_1 and f_2 are different on X, then their extensions to M are different, because $X \subset M$. Our collection F^* will now be defined as the set of all f^*, if f runs through F_0.

It is not difficult to show that the elements of F^* are independent. Let k be any positive integer, and take k distinct elements of F^*. These can be represented as $f_1^*, \ldots, f_k^*$, where $f_1, \ldots, f_k$ are k distinct elements of F.

If $1 \leqslant p < q \leqslant k$, then f_p and f_q are different. That is to say, there is an element $x_{pq} \in X$ such that $f_p(x_{pq}) \neq f_q(x_{pq})$. Now take $j = \frac{1}{2}k(k-1)$, and in X^j consider the point

$$\mu = (x_{12}, x_{13}, \ldots, x_{1k}, x_{23}, \ldots, x_{2k}, \ldots, x_{k-1,k}). \tag{3}$$

At this point the functions $f_1^*, \ldots, f_k^*$ all have different values. In order to show that $f_p^*(\mu) \neq f_q^*(\mu)$, we just look at the place corresponding to the entry x_{pq} in (3). At that place, $f_p^*(\mu)$ has $f_p(x_{pq})$ (according to (2)), whereas $f_q^*(\mu)$ has $f_q(x_{pq})$. So the points $f_p^*(\mu)$ and $f_q^*(\mu)$ differ in one coordinate, whence they are different points of T^j. This completes the proof.

Remarks. 1. It is not difficult to show that the collection F^*, constructed above, even has the property that its elements are independent in a somewhat stronger sense. For any finite number of distinct elements $f_1^*, \ldots, f_k^*$ of F^* we can state that there are $\mathbf{m}$ μ's such that (for each of these μ's) the k elements $f_1^*(\mu), \ldots, f_k^*(\mu)$ are mutually different. This can be proved as follows: instead of (3) we consider the point

$$(x_0, x_{12}, \ldots, x_{k-1,k}) \in T^{j+1},$$

where x_0 is an arbitrary element of X. For every choice of x_0 this is a point where the $f_1^*, \ldots, f_k^*$ have different values. And there are $\mathbf{m}$ possibilities for x_0.

2. Prof. J. de Groot mentioned to me that the following special case was known to him: If S is an infinite set, with $|S|=\mathbf{m}$, then there is a collection of $2^{\mathbf{m}}$ subsets S_α (α runs through some index set I of power $2^{\mathbf{m}}$), with the following property. If k is any positive integer, and $\alpha_1, \ldots, \alpha_k$ are distinct elements of I, then the difference

(4) $$S_{\alpha_1} \setminus \bigcup_{i=2}^{k} S_{\alpha_i}$$

has power $\mathbf{m}$. This can be derived from our theorem in the following way. Divide S into $\mathbf{m}$ countable disjoint subsets $S^{(\mu)}$ (μ runs through an index set M of power $\mathbf{m}$). For every $\mu \in M$ we put $A_\mu = S^{(\mu)}$. A choice function f_α (defined on M, with $f_\alpha(\mu) \in A_\mu$) now defines a subset S_α of S, viz. the set $\{f_\alpha(\mu) \mid \mu \in M\}$. Taking our collection F^*, we get $2^{\mathbf{m}}$ subsets of S. These evidently satisfy the condition that (4) has power $\mathbf{m}$, as for $\mathbf{m}$ μ's $f_{\alpha_1}(\mu)$ is different from $f_{\alpha_2}(\mu), \ldots, f_{\alpha_k}(\mu)$.

3. The part of our proof that starts from the special case (1), is independent of the axiom of choice. Therefore, in many special cases a set of $2^{\mathbf{m}}$ independent choice functions can be effectively constructed. For example, if M is the set of all positive integers, and if $A_\mu = \{1, 2, \ldots, \mu\}$ ($\mu \in M$), then it is not difficult to give an explicit construction. That is, we can define a collection $\{f_\alpha\}$, where α runs through the collection of all subsets of the set of all positive integers, such that (i) the f_α's are independent, and (ii) if μ is a given integer, then we can evaluate a number n, such that, for every α, the value of $f_\alpha(\mu)$ can be evaluated when the intersection of α and the set $\{1, 2, \ldots, n\}$ is known.

4. In some algebraic systems the theorem can be used for the construction of large subsets whose elements are independent in some algebraic sense. In a subsequent paper we shall show that the group Σ_M of all permutations of an infinite set M contains a free subgroup of order $2^{|M|}$. And, more generally, if we have $2^{|M|}$ groups, each of which can be embedded into Σ_M, then their free product can be embedded into Σ_M. The same thing holds for their direct product.

University of Amsterdam