ON EQUATIONS WITH SETS AS UNKNOWNS

By Paul Erdös and S. Ulam

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF COLORADO, BOULDER

Communicated May 27, 1968

We shall present here a number of results in set theory concerning the decompositions of a set E in various ways as sum (union) of its subsets. These results have connection with problems on countably additive measure functions in abstract sets, but they may also bear on the problems of the axiomatics of set theory and generally on foundations of set theory itself. Some of these results employ the continuum hypothesis or the generalized continuum hypothesis. The several problems which will be presented also put these hypotheses in a certain limelight.

The impossibility of defining a countably additive measure for *all* subsets of a set of power of continuum (a measure which would vanish for subsets consisting of any single point) was first established with the use of the continuum hypothesis by Banach and Kuratowski.[1] Very shortly afterwards, one of us showed the impossibility of such a measure for subsets of a set of power $\aleph_1$ without the use of any hypothesis.[2] The same result was shown there to hold for sets of higher powers, in fact, for all the accessible alephs. More recently, these results have been extended to a large class of inaccessibles as well. These results show that this "problem of measure" is closely related to fundamental problems concerning the role of axioms of set theory. Recent developments have further clarified these relations. Important results have been obtained by Scott, Solovay, Martin, and others. The proofs of these relations make use of the methods introduced by Paul Cohen in proving the independence of the continuum hypothesis.

Both the results of Banach and Kuratowski and the stronger result of Ulam are obtained by exhibiting purely combinatorial schemata of decompositions of abstract sets with certain properties: $B\cdot$ and $K\cdot$ show a countable sequence of decompositions of a set of power of the continuum, each into countably many disjoint subsets so that, no matter how one takes a finite number of sets from each of these decompositions, the intersection of all these finite unions contains, at most, countably many points. Sierpinski[3] generalized the $B\cdot$ and $K\cdot$ schema in the following way. There exists a sequence of decompositions into aleph disjoint sets, each so that if one is selected from any countably many of these (not necessarily all), the union of the selected sets gives the whole of the space, except perhaps for countably many points. Decompositions given by $U\cdot$ show, without the use of the continuum hypothesis, the following phenomenon. A set E of power $\aleph_1$ can be decomposed countably many times into $\aleph_1$ disjoint sets in the following way:

A "matrix" of sets can be constructed such that we have countably many rows and noncountably many columns. Sets in each row are disjoint. The union of sets in any column gives the whole set E except for possibly countably many points. As is easy to see, the existence of such a decomposition (a sequence of decompositions, properly speaking) contradicts the possibility of defining a countably additive real-valued measure function.

In this paper we shall show various modifications of such constructions. In particular, we strengthen the result of Sierpinski. One can decompose E in the nth row into 2^{n+1} disjoint sets with the above property. It is clear that the impossibility of a measure function follows because if the measure for these sets existed, we could select a set of power less than $1/2^n$ and their union would have to measure less than 1. This is a contradiction, since the complement is countable. This construction uses the continuum hypothesis. Whether one can do it by using a weaker hypothesis remains an open problem. Should the number of sets in each row be finite and fixed, we show that one does not need the continuum hypothesis for this property to hold (but of course one does not get the impossibility of a measure function from such a "matrix"). We shall introduce a special symbol for decompositions of sets in such "matrix" patterns.

Finally, we would like to say that all the results and problems in this paper form only a special aspect of a more general problem which we formulate rather vaguely here: Given a class of Boolean relationships to be satisfied by unknown sets, all subsets of a given set, one wants to find or "construct" sets satisfying such relations, which may be countable or noncountable in number. We hope to attack this more general question in a paper to be published in the future.

THEOREM 1. *The real line (and in fact every set of power* c*) can be decomposed in infinitely many ways as the union of* k *disjoint sets*

$$S = \bigcup_{l=1}^{k} A_l^{(n)}, \quad n = 1,2,\ldots$$

so that

$$\left|S - \bigcup_{n=1}^{\infty} \cdot A_{l_n}^{(n)}\right| < k \tag{1}$$

for every choice of the sets $A_{l_n}^{(n)}$, $1 \leq l_n \leq k$.

We prove Theorem 1 without the axion of choice. Consider all sets of $k-1$ disjoint rational intervals and write them in a sequence $\{I_n^{(k-1)}\}$, $n = 1,2\ldots$. The first $k-1$ sets $A_l^{(n)}$, $1 \leq l \leq k-1$, of the nth row of our decomposition matrix are the $k-1$ intervals of $I_n^{(k-1)}$. $A_k^{(n)}$ is the complement of the union of the intervals in $I_n^{(k-1)}$. Now let

$$\bigcup_{n=1}^{\infty} A_{l_n}^{(n)} = F$$

be a typical family of sets, one from each row. To prove (1) it suffices to show that if $x_1, x_2, \ldots x_k$ are any k real numbers, we must have $x_i \in F$ for at least one i, $1 \leq i \leq k$. To see this, observe that there is a set of $k-1$ rational intervals, say $I_n^{(k-1)}$, which separates $x_1, x_2, \ldots x_k$. But then every $A_l^{(n)}$, $1 \leq l \leq k$ contains exactly one of the x_i or $x_i \in F$ for at least one i, as stated. This completes the proof of Theorem 1.

It is easy to see that (1) fails to hold with $k-1$ instead of k, but we leave this to the reader.

THEOREM 2. *Let* $|S| \geq \aleph_0$, $2 \leq k_1 \leq k_2 \leq, \ldots, k_n \to \infty$ *and let*

$$S = \bigcup_{l=1}^{k_n} A_l^{(n)}, \quad n = 1,2,\ldots$$

be a decomposition of S *into* k_n *disjoint sets. Then there is always an* l_n, $1 \leq l_n \leq k_n$, $n = 1,2, \ldots$ *so that*

$$\left|S - \bigcup_{n=1}^{\infty} A_{l_n}^{(n)}\right| \geq \aleph_0. \tag{2}$$

To prove Theorem 2 we will define elements x_u, $1 \leq u \leq \infty$ of S (the x_u's are not necessarily all different, but there are infinitely many different ones among them) and sets $A_{l_n}^{(n)}$ so that

$$x_u \not\in A_{l_n}^{(n)}, \quad 1 \leq u < \infty, 1 \leq n < \infty, 1 \leq l_n \leq k_n \tag{3}$$

(3) will clearly imply Theorem 2.

We construct the x_n and the sets $A_{l_n}^{(n)}$ by induction with respect to n. Assume first that $2 = k_1 = ,\ldots = k_t < k_{t+1}$. Consider the 2^t sets

$$\bigcap_{n=1}^{t} A_l^{(n)} \quad l = 1 \text{ or } 2.$$

The union of these sets is S, thus at least one of them is infinite, say

$$\left|\bigcap_{n=1}^{t} A_{\epsilon_n}^{(n)}\right| = \aleph_0, \ (\epsilon_n = 1 \text{ or } 2).$$

Let x be an arbitrary element of $\bigcap_{i=1}^{t} A_{\epsilon_n}^{(n)}$, put $x = x_1 = \ldots = x_t$ and $A_{l_n}^{(n)} = A_{3-\epsilon_n}^{(n)}$ for $n = 1,2,\ldots t$. Clearly the complement of $\bigcup_{n=1}^{\infty} A_{l_n}^{(n)} = \bigcup_{n=1}^{\infty} A_{3-\epsilon_n}^{(n)}$ (which equals $\bigcap_{n=1}^{t} A_{\epsilon_n}^{(n)}$) is infinite.

Now assume that we have already succeeded in choosing elements $x_1, x_2, \ldots x_u$ and sets $A_{l_n}^{(n)}$, $1 \leq n \leq u$ having the following properties:

$$\left|S - \bigcup_{n=1}^{u} A_{l_n}^{(n)}\right| \geq \aleph_0, \qquad S_u = S - \bigcup_{n=1}^{u} A_{l_n}^{(n)} \tag{4}$$

$$x_s \not\in A_{l_n}^{(n)}, \quad 1 \leq s \leq u; 1 \leq n \leq u \tag{5}$$

and finally there are at most $k_u - 2$ distinct elements among the x_i, $1 \leq i \leq u$. Now we construct x_{u+1} and $A_{l_{u+1}}^{(u+1)}$ so that (4) and (5) remain satisfied and so that there are at most $k_u - 2$ distinct elements among the $x, \ldots x_u, x_{u+1}$.

Assume first that $k_{u+1} = k_u$. Then there are at least two sets $A_{l_1}^{(u+1)}$ and $A_{l_2}^{(u+1)}$ which do not contain any of the elements $x_1, \ldots x_u$ (this follows from the fact that there are at most $k_u - 2$ distinct x's and the $A_l^{(u+1)}$'s are disjoint). At least one of these, say $A_{l_1}^{(u+1)}$, has an infinite complement in S_u (i.e., infinitely many elements of S_u do not belong to $A_{l_1}^{(u+1)}$). Put $A_{l_1}^{(u+1)} = A_{l_{u+1}}^{(u+1)}$ and clearly (4) and (5) are satisfied.

Assume next that $k_{u+1} > k_u$. Then there are at least three sets $A_{l_1}^{(u+1)}$,

$A_{l_1}{}^{(u+1)}$, $A_{l_2}{}^{(u+1)}$ which do not contain any of the x_i, $1 \leq i \leq u$. At least one of the sets, say $A_{l_1}{}^{(u+1)}$, has an infinite complement in S_u; we choose an arbitrary element x_{u+1} from this complement and put $A_{l_1}{}^{(u+1)} = A_{l_{u+1}}{}^{(u+1)}$. x_{u+1} is clearly different from $x_1, x_2, \ldots x_u$, and (4) and (5) are again satisfied. Thus we have constructed the infinite sequence $x_1, x_2, \ldots$ and the sets $A_{l_u}{}^{(u)}$. (3) is clearly satisfied and it is clear from our construction that there are infinitely many distinct elements among the x's, thus (2) is satisfied and Theorem 2 is proved.

Now we would like to state the following question which we cannot solve.

PROBLEM I. *Let $\aleph_0 < |S| \leq c$. Let $2 \leq k_1 \leq k_2 \leq \ldots, k_n \to \infty$, be any sequence of integers. Does there exist for every n a decomposition*

$$S = \bigcup_{l=1}^{k_n} A_l{}^{(n)}$$

into disjoint sets so that for every $1 \leq l_n \leq k_n$

$$\left|S - \bigcup_{n=1}^{\infty} A_{l_n}{}^{(n)}\right| \leq \aleph_0 \quad ?$$

If $c = \aleph_1$, we will see that the answer to our problem is affirmative; in fact very much more is true. But if we do not assume that $c = \aleph_1$, we cannot solve this question even if we assume that $|S| = \aleph_1$ and let our sequence k_n tend to infinity very slowly. If $|S| = c$ and $k_n > 2^n$ as stated in the introduction, we cannot expect a positive solution without some assumption on the power of the continuum since this would imply that there is no real-valued completely additive measure on the subsets of the reals where points measure 0.

It seems very likely that if we do not make some assumption about the power of the continuum, then we cannot obtain a solution to Problem I. It may even be possible to show that if Problem I has a solution for a fixed sequence $k_n \to \infty$, then a solution exists for every such sequence.

It will be convenient to introduce the symbol $m \to (p, q, r, s)$, which means that a set S of power m can be decomposed into the union of p disjoint sets in q ways:

$$S = \bigcup_{1 \leq \alpha \leq \omega_q} A_\alpha{}^{(\beta)}, \quad 1 \leq \beta \leq \omega_p$$

so that if we choose any one of the sets $A_{\alpha_i}{}^{(\beta_i)}$ for r different β_i, then

$$\left|S - \bigcup_i A_{\alpha_i}{}^{(\beta_i)}\right| < s, \tag{6}$$

$m \not\to (p, q, r, s)$ means that such a decomposition is impossible. Sierpinski proved[3] that

$$c \to (\aleph_1, \aleph_0, \aleph_0, \aleph_1) \tag{7}$$

is equivalent to the continuum hypothesis. Sierpinski's result implies that if we assume $c = \aleph_1$, the answer to Problem I is affirmative. We generalized this and proved other results on our symbol, but do not give these proofs since Hajnal observed that all our results follow from previous results of Erdös, Hajnal, and Milner,[4] and Erdös, Hajnal, and Rado.[5] We studied the following symbol extensively:

$$\binom{m}{q} \rightarrow \begin{pmatrix} s & s \\ r & r \end{pmatrix}. \tag{8}$$

The meaning of (8) is as follows: Let $|S_1| = m$, $|S_2| = q$; we split the pairs (x,y), $x \in S_1$, $y \in S_2$ into two classes. Then there is always a $U \subset S_1$, $V \subset S_2$, $|u| = s$, $|V| = r$ so that all the pairs (x,y), $x \in U$, $y \in V$ are in the same class. $\binom{m}{q} \not\rightarrow \begin{pmatrix} s & s \\ r & r \end{pmatrix}$ means that there is a division of the pairs into two classes for which such sets U and V do not exist.

It is easy to see that

$$\binom{m}{q} \rightarrow \begin{pmatrix} s & s \\ r & r \end{pmatrix} \tag{9}$$

is equivalent to

$$m \not\rightarrow (2, q, r, s). \tag{10}$$

First we show that (9) implies (10). Let $|S_1| = m$, $|S_2| = q$. Let $x \in S_1$, $\beta \in S_2$, $1 \leq \beta \leq \omega_q$. The pair (x,β) is in class I if $x \in A_1^{(\beta)}$ and in class II if $x \in A_2^{(\beta)}$. (9) implies that (6) is not always satisfied, hence (10) is proved.

Next we show that (10) implies (9). In fact we show that if (9) does not hold, then $m \rightarrow (2,q,r,s)$. Consider then a splitting of the pairs (x,β) into two classes so that if $U \subset S_1$, $V \subset S_2$, $|U| = s$, $(V) = s$, then there is always a pair (x_1,y_1) in class I and a pair (x_2,y_2) in class II where $x_1 \in U$, $x_2 \in U$; $y_1 \in V$, $y_2 \in V$.

Now we put x in $A_1^{(\beta)}$ if (x,β) is in class I, and in $A_2^{(\beta)}$ if (x,β) is in class II. Now we show that (6) is satisfied. Since $p = 2$ in (6), $\alpha_i = 1$ or $= 2$. Without loss of generality we can assume that for r values of i, $\alpha_i = 1$. But then if (6) is not satisfied, we would have

$$\left|S - \bigcup_i A_1^{(\beta_i)}\right| \geq s, \tag{11}$$

where β_i runs through a set of ordinals V of power r. (11) means that there is a set $U \subset S_1$, $|U| \geq s$ so that all the pairs (x,β_i), $\beta_i \in V$ are in class II, which contradicts our assumption that (9) is false; hence (6) and thus $m \rightarrow (2,q,r,s)$ is proved. Hence (10) implies (9) and thus the proof of the equivalence of (9) and (10) is complete.

Theorem 48 of Erdös-Rado states that

$$\binom{\aleph_1}{\aleph_0} \rightarrow \begin{pmatrix} \aleph_1 & \aleph_1 \\ \aleph_0 & \aleph_0 \end{pmatrix},$$

thus clearly

$$\binom{\aleph_1}{\aleph_0} \rightarrow \begin{pmatrix} \aleph_0 & \aleph_0 \\ \aleph_0 & \aleph_0 \end{pmatrix},$$

which by the equivalence of (9) and (10) implies

$$\aleph_1 \to (2, \aleph_0, \aleph_0, \aleph_0). \tag{12}$$

Perhaps

$$\aleph_2 \to (2, \aleph_r, \aleph_1, \aleph_1),$$

but this is undoubtedly very difficult since it is equivalent to one of the most difficult unsolved problems of Erdös-Hajnal-Rado (problem 12),

$$\begin{pmatrix}\aleph_2\\ \aleph_1\end{pmatrix} \to \begin{pmatrix}\aleph_1 & \aleph_1\\ \aleph_1 & \aleph_1\end{pmatrix}. \tag{13}$$

Perhaps $\aleph_1 \to (2, \aleph_2, \aleph_0, \aleph_1)$, but this is also very difficult, since (see problem 12)

$$\begin{pmatrix}\aleph_1\\ \aleph_2\end{pmatrix} \to \begin{pmatrix}\aleph_1 & \aleph_1\\ \aleph_0 & \aleph_0\end{pmatrix} \tag{14}$$

is also unsolved; (13) would imply (14), but (14) also seems very hard.

On the other hand, it follows from Theorem 33 of Erdös-Hajnal-Rado that

$$\aleph_2 \to (2, \aleph_1, \aleph_0, \aleph_1).$$

We will not discuss $m \to (2,q,r,s)$ further, but refer to reference 5.

We state another result which generalizes Sierpinski's result: Assume that $2^{\aleph_\kappa} = \aleph_{\kappa+1}$, then

$$\aleph_{\kappa+1} \to (\aleph_{\kappa+1}, \aleph_{\kappa+1}, \aleph_\kappa, \aleph_{\kappa+1}). \tag{15}$$

(15) follows from Lemma 14.1 of Erdös-Hajnal-Milner.[4] A slightly weakened form of this lemma is stated as follows:

Assume that $2^{\aleph_\kappa} = \aleph_{\kappa+1}$, $|S_1| = |S_2| = \aleph_{\kappa+1}$. The pairs (x,y), $x \in S$, $y \in S_2$ can be split into $\aleph_{\kappa+1}$ classes so that whenever $U \subset S_1$, $V \subset S_2$, $|U| = \aleph_{\kappa+1}$, $|V| = \aleph_\kappa$, there is an $x \in V$ so that every class is represented by the pairs (x,y), $y \in U$.

Now we deduce (15) from this lemma. The elements of S_1 are denoted by $\{x_\gamma\}$, $1 \leq \gamma \leq \omega_{\kappa+1}$, those of S_2 by $\{\beta\}$ $1 \leq \beta \leq \omega_{\kappa+1}$, and the classes into which the pairs are split are denoted by $\{\alpha\}$, $1 \leq \alpha \leq \omega_{\kappa+1}$.

We put $x_\gamma \in A_\gamma^{(\beta)}$ if the pair (x_γ,β) is in class α. A simple argument using Lemma 14.1 shows that (6) is satisfied with $r = \aleph_\kappa$, $s = \aleph_{\kappa+1}$, which proves (15).

Perhaps $\aleph_{\kappa+1} \to (\aleph_{\kappa+1}, \aleph_{\kappa+2}, \aleph_\kappa, \aleph_{\kappa+1})$ also holds, but as we already stated we could not even prove

$$\aleph_1 \to (2, \aleph_2, \aleph_0, \aleph_1).$$

Finally we state a trivial result. Let $m < \aleph_\kappa$ and assume $2^m < \aleph_{\kappa+1}$. Then $\aleph_{\kappa+1} \to (2, m, m, \aleph_{\kappa+1})$. In fact, the following stronger result holds. Let $|S| = \aleph_{\kappa+1}$. Put

$$S = A_1^{(\beta)} \cup A_2^{(\beta)}, \quad 1 \leq \beta \leq \omega_m.$$

Then for some $\beta_i = 1$ or $\beta_i = 2$, $\bigcup_\beta A_{\beta_i}^{(\beta)}$ has a complement of power $\aleph_{\kappa+1}$. We leave the simple proof to the reader.

[1] Banach and Kuratowski, *Fund. Math.*, **15** (1935).

[2] Ulam, S., "Uber die Masstheorie in der Allgemeinen Mengenlehre," *Fund. Math.*, **16** (1936).

[3] Sierpinski, W., *Hypothèse du Continu* (New York: Chelsea Publishing Company, 1956), 2d ed., pp. 53–55.

[4] Erdös, P., A. Hajnal, and E. Milner, "On the complete subgraphs of graphs defined by systems of sets," *Acta Math. Acad. Sci. Hung.*, **17**, 159–229 (1965).

[5] Erdös, P., A. Hajnal, and R. Rado, "Partition relations for cardinal numbers," *Acta Math. Acad. Sci. Hung.*, **16**, 93–196 (1965); see also the earlier paper by Erdös, P., and R. Rado, "A partition calculus in set theory," *Bull. Am. Math. Soc.*, **62**, 427–489 (1956).