ON IRREDUNDANT SETS OF POSTULATES*

BY

ALONZO CHURCH

1. **Definitions.** We shall say that the postulate A is weaker than the postulate B if B implies A and A does not imply B. This is a definition of the relative strength of two postulates in an absolute sense, as distinguished from their relative strength in the presence of other postulates.

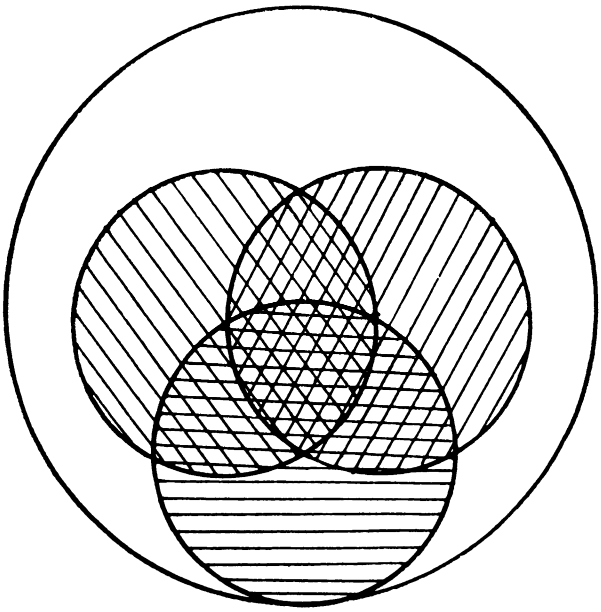

Fig. 1

The postulate A_1 can be weakened with respect to the set $A_1, A_2, A_3, \cdots, A_n$ if there exists a postulate, A_1', weaker than A_1, such that the logical product $A_1' A_2 A_3 \cdots A_n$ implies A_1. Under this definition we say that a postulate can be weakened with respect to a set of postulates, of which it is one, only when it can be replaced in the set by a weaker postulate in such a way that none of the implications of the set as a whole is lost.

A set of postulates is *irredundant* if the postulates are independent and no one of them can be weakened with respect to the set.

* Presented to the Society, December 30, 1924.

2. The relation of irredundance to complete independence.* If we represent the set of all possible mathematical systems by the set of all points in the interior of a circle, we may represent a postulate by a curve which divides the interior of the circle into two regions, which represent, one the set of systems which satisfy the postulate, and one the set of those which do not. We may distinguish between these two regions by shading the one within which the postulate is false and leaving the other unshaded. It is then clear that, if the postulate A is weaker than the postulate B the shaded area corresponding to A in the diagram will lie entirely within that corresponding to B.

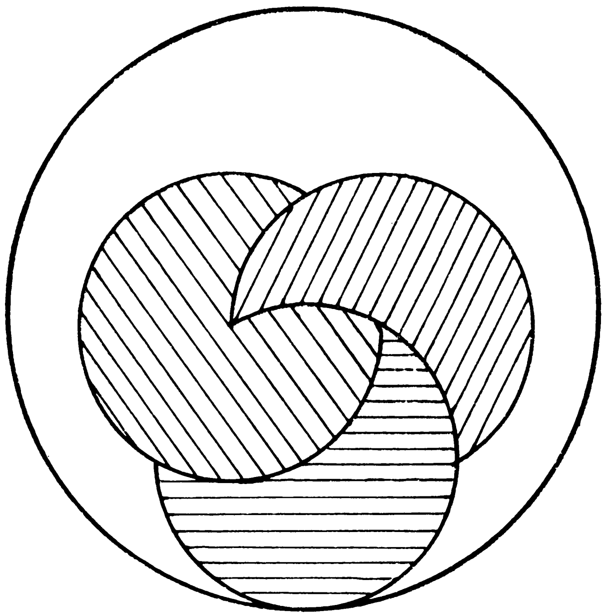

Fig. 2

In this way we may represent a set of three completely independent postulates as shown in Figure 1. The postulates are completely independent because, as is easily verified from the figure, systems exist which satisfy some of the postulates and fail to satisfy the others in any arbitrarily assigned manner. This corresponds to the fact that the three small circles which represent the postulates divide the interior of the large circle into 2^3, or 8, regions.

* The notion of complete independence is due to E. H. Moore. See *Introduction to a Form of General Analysis, New Haven Colloquium*, 1906, p. 82. For a discussion of the significance of this notion, see E. V. Huntington, *A new set of postulates for betweenness, with proof of complete independence*, these Transactions, vol. 26 (1924), p. 277.

If this set is to be made irredundant, the postulates must be weakened until no two of the shaded regions overlap; for so long as two of the shaded regions do overlap, it is possible to shrink one of them without reducing the total shaded area. The weakened set of postulates is represented in Figure 2. On the other hand, if a set of postulates which are not completely independent are to be made so, it may be necessary to strengthen one or more of them.* In particular, if the set is irredundant, all but one of the postulates, at least, must be strengthened.

A set of n completely independent postulates divides the set of all possible systems into 2^n parts, represented in a diagram by regions, the greatest number possible. The division effected by an irredundant set of n postulates, if the set is consistent, is a division into $n+1$ parts, the least number which is possible if the postulates are to be consistent and independent. In general, an irredundant set of postulates is as far removed as possible from a completely independent set.†

3. **A criterion for irredundance.** In the diagram just described the relation of implication between postulates is represented by the relation of inclusion between regions. Thus, if A implies B, the shaded area corresponding to A contains that corresponding to B, and if the negative of A implies B, the unshaded area corresponding to A contains the shaded one corresponding to B. The observations made in the preceding section, therefore, suggest the following theorem:

A necessary and sufficient condition that the postulate A_1 *cannot be weakened with respect to the set* $A_1, A_2, A_3, \cdots, A_n$ *is that the negative of* A_1 *imply each of the postulates* $A_2, A_3, \cdots, A_n$.

The condition is necessary. For let B stand for the logical product $A_2 A_3 \cdots A_n$, and suppose that *not*-A_1 does not imply B. Then *not*-B does not imply A_1, and, therefore, A_1 *or not*-B does not imply A_1. The postulate A_1 *or not*-B is, therefore, weaker than A_1, and can be substituted for A_1 in the set $A_1, A_2, A_3, \cdots, A_n$, without loss of any of the implications of the set.

The condition is sufficient. For suppose that *not*-A_1 implies B, but that there exists a postulate A_1', weaker than A_1, such that the logical product

* For an interesting example of this, see J. S. Taylor, *Complete existential theory of Bernstein's set of four postulates for Boolean algebras*, Annals of Mathematics, ser. 2, vol. 19 (1917), p. 68, and the footnote on that page.

† The idea of a set of mutually prime postulates as defined by H. M. Sheffer is similar to that of an irredundant set as here defined. The two ideas are not, however, the same, because mutual primeness implies complete independence in the sense of E. H. Moore. See an abstract of a paper by H. M. Sheffer, *Mutually prime postulates*, Bulletin of the American Mathematical Society, vol. 22 (1916), p. 287. See also *The General Theory of Notational Relativity*, a privately circulated paper.

$A_1'B$ implies A_1. Then since *not*-A_1 implies B, it follows that *not*-B implies A_1; but $A_1'B$ implies A_1, and, by the law of excluded middle, B or *not*-B; therefore A_1' implies A_1, contrary to the hypothesis that A_1' was weaker than A_1.

The validity of this theorem depends on the validity of certain postulates of logic on which it is based, among which, as we have just seen, is the law of excluded middle. The conception with which we began, that a postulate divides the set of all possible mathematical systems into two parts, also depends, of course, on this law.

From the theorem which has just been proved follows as a corollary

A necessary and sufficient condition that a set of postulates be irredundant is that the postulates be independent and that the negatives of every two be contradictory.

Thus if the independent postulates A, B, C are to be irredundant, we must have *not*-A incompatible with *not*-B, *not*-A incompatible with *not*-C, and *not*-B incompatible with *not*-C.

There is a mechanical method by which any set of independent postulates can be made irredundant. If A, B, C, D are independent postulates, the set A, B', C', D' is an equivalent set which is irredundant, if B' is the proposition *if A then B*, and C' is the proposition *if A and B then C*, and D' the proposition *if A and B and C then D*. This method is open to the objection that it is likely to lead to postulates very complicated in form, and that, in general, the hypothesis of a postulate obtained in this way will be concerned with elements which are not mentioned in the conclusion. For example, if we applied this method to Peano's postulates for the system of positive integers*, we should obtain as our second postulate the following; "If 1 is a number, then every number has a unique successor."

The question arises to what extent it is possible to obtain irredundant sets of postulates which are not open to this objection. As a partial answer to this question, we shall give two examples of such sets of postulates.

4. **A simple example of an irredundant set.** The following set of postulates describes a system of a finite number of elements, which we call numbers, arranged in cyclic order. The undefined terms are *number* and *successor*. The postulates are the following:

1. There is a set of numbers, not null, such that every number in the set has a successor which is in the set.

2. In every proper part P, not null, of the set of all numbers there is a number none of whose successors is in P.

---

* Rivista di Matematica, vol. 1 (1891), pp. 87–102. See also below.

The negatives of these two postulates are

Not-1. There is no set of numbers, other than the null set, such that every number in the set has a successor which is in the set.

Not-2. In some proper part P, not null, of the set of all numbers every number has a successor which is in P.

Since these two statements are plainly contradictory, it will follow, as soon as we give independence examples, that the set of postulates 1 and 2 is irredundant.

An independence example for the first postulate is a system of a finite number of elements arranged in linear order. An independence example for the second postulate is the system of positive integers.

In the case of each example, when we have verified that it fails to satisfy the postulate for which it is given as an independence proof, we need not afterwards verify that it satisfies the other postulate, because we know that the negatives of the two postulates are contradictory. This corresponds to the fact that if a set of postulates satisfy the condition of the preceding section, that is, if the negatives of every two be contradictory, then a postulate of the set can fail to be independent only if its negative be self-contradictory in the system of logic on which the postulates are based.

From postulate 1 above follows the existence of at least one number. From postulate 2 it follows that the set whose existence is required by postulate 1 is the set of all numbers, and, therefore, that every number has a successor.

If a is any number, every number can be reached from a by proceeding from number to successor a finite number of times, for if A is the set of all numbers which can be so reached from a, it is true that every number in A has a successor in A, and therefore, by postulate 2, that A is the set of all numbers. If any number is successor of itself, it follows from postulate 2 that it is the only number, and in this case we have a cycle which contains just one element. In any other case we can find distinct numbers, a and b, such that b is a successor of a. Then there are one or more routes by which a can be reached from b in a finite number of steps from number to successor. And it follows from postulate 2 that any arbitrarily chosen one of these routes must contain every number. The set of all numbers is, therefore, finite, and can be arranged in a cycle in such a way that every number is a successor of the number which next precedes it in the cycle.

Finally, there is no number a which has two successors, b and c. For, if there were, we could find a finite route from b to c, and this route would not contain a, because every finite route from b to a contains all numbers. Similarly there would be a finite route from c to b which did not contain a, and the set P of all numbers which were in either of these routes would have the property that every number in it had a successor in it. But P would not contain a, and would, therefore, violate postulate 2.

We have, therefore, shown that postulates 1 and 2 uniquely determine a system of a finite number of elements arranged in cyclic order.

5. **An irredundant set of postulates for the system of positive and negative integers.*** The following postulates, which deal with a set of undefined elements, *numbers*, and an undefined relation, *successor* among them, describe the system of positive and negative integers:

1. There is a set of numbers, S, not null, such that every number in S has a successor which is in S.

2. If the set of all numbers is such a set S, it is not the only such set.

3. If such sets S exist, one of them has the property that every number in the set is successor of some number in the set.

4. In every proper part P, not null, of the set of all numbers, either some number has no successor which is in P, or some number is successor of no number in P.

The negatives of these postulates are:

Not-1. There is no set of numbers S, other than the null set, such that every number in S has a successor which is in S.

Not-2. The set of all numbers is an S and the only S.

Not-3. Sets S exist, but no one of them has the property that every number in the set is successor of some number in the set.

Not-4. There is a proper part P, not null, of the set of all numbers, such that every number in P has a successor in P and is successor of some number in P.

Of these four statements every two are contradictory. This is evident at once, except in the case of *not*-2 and *not*-3. In order to see that *not*-2 and *not*-3 are contradictory, we observe that if the set of all numbers, N, were an S and the only S, then every number in N would be successor of some number in N, because if the number a in N were successor of no number in N we could, by omitting a from N, obtain an S not the set of all numbers.

Independence examples are as follows. For postulate 1, a system of a finite number of elements arranged in linear order; for postulate 2, a finite

* For a set of independent postulates for the system of positive and negative integers, see A. Padoa, *Un nouveau système irréductible de postulats pour l'algèbre,* Deuxième Congrès International des Mathématiciens, Paris, 1900, pp. 249–256, and *Numeri interi relativi,* Rivista di Matematica, vol. 7 (1901), pp. 73–84. This set is, however, not categorical, because it is satisfied by the set of integers reduced modulo m, where m is any odd integer.

cycle; for postulate 3, the system of positive integers; for postulate 4, a system of two sets of a finite number of elements each, no element common to the two sets, and each set arranged separately in cyclic order. As pointed out in the preceding section, it is sufficient to see, in the case of the first example, that it satisfies *not*-1, because every system which satisfies *not*-1 must also satisfy postulates 2, 3, and 4; and similarly in the case of each of the other examples.

The set of postulates 1, 2, 3, 4 is, therefore, irredundant.

6. **A proof that the foregoing set of postulates is categorical.** We shall prove that the postulates given above uniquely determine the system of positive and negative integers. In order to do this, we shall show that the set of all numbers, as defined by these postulates, can be divided into two parts which have in common one and only one number, *a*, of which one satisfies Peano's postulates for the system of positive integers* when "1" is replaced in them by "*a*", and the other satisfies Peano's postulates when "1" is replaced in them by "*a*" and "successor" by "predecessor".

Peano's postulates are as follows:

1. 1 is a number.

2. Every number has a unique successor.

3. If *a* and *b* are numbers, and if their successors are equal, then *a* and *b* are equal.

4. 1 is not the successor of any number.

5. If *S* is a class of numbers which contains 1, and the class of all successors of numbers in *S* is contained in *S*, then every number is contained in *S*.

If not imperative, it is at least desirable that the proposed proof should be made without the use of the notion of finite cardinal number, although this necessitates an argument somewhat longer than might otherwise be given.

THEOREM 1. *There exists a number.* (Postulate 1 of § 5.)

THEOREM 2. *Every number has a successor.*

For it follows from postulate 4 that the set whose existence is required by postulate 3 is the set of all numbers.

DEFINITION. If the number *a* is successor of the number *b*, then *b* is *predecessor* of *a*.

THEOREM 3. *Every number has a predecessor.* (Postulates 1, 3, 4.)

THEOREM 4. *No number is successor of itself.*

For if *a* were successor of itself, then *a* would be the only number, by postulate 4. But in that case postulate 2 would be violated.

* Loc. cit. See also Formulaire de Mathématiques, vol. 3 (1901), pp. 39–44.

THEOREM 5. *If the number b is successor of the number a, a is not successor of b.*

For if a were successor of b, a and b would be the only numbers, by postulate 4. But in that case postulate 2 would be violated.

DEFINITION. The set of numbers Q is an *interval* if it contains numbers, a and b, which have, respectively, no predecessor and no successor in Q, and every number other than a has a unique predecessor in Q, and every number other than b has a unique successor in Q, and finally, there is no part of Q, not null, in which every number has a successor. The numbers a and b are the *end numbers* of Q, and Q is *an interval* ab.

THEOREM 6. *The set of numbers obtained by omitting b from an interval ab, if $b \neq a$, is an interval ac, where c is the predecessor of b in ab. The set of numbers obtained by omitting a from an interval ab, if $b \neq a$, is an interval db, where d is the successor of a in ab.*

THEOREM 7. *If intervals ab and bc have the property that no number in either, other than b, has a successor in the other, other than b, then the sum, P, of ab and bc is an interval ac.*

Suppose that in some part T of P, not null, every number had a successor. Then the set R of numbers common to T and bc would have the property that every number in it had a successor in it, for otherwise some number in ab would be successor of some number in bc. But R cannot be null, because, if it were, I would be a part of ab. Therefore there is no part of P in which every number has a successor. Therefore, since it is easily seen that P has the other properties required by the definition, it follows that P is an interval ac.

COROLLARY 1. *If c is a successor of b, and, in the interval ab, c has no successor and no predecessor other than b, then the set of numbers obtained by adding c to ab is an interval ac.*

COROLLARY 2. *If c is a predecessor of a, and, in an interval ab, c has no predecessor and no successor other than a, then the set of numbers obtained by adding c to ab is an interval cb.*

THEOREM 8. *If c is a number of an interval ab, this interval can be divided into intervals, ac and cb, whose sum is ab, and which have only c in common.*

Let P be the set of all numbers, c, in ab of which this is not true. If the theorem is true of any number, d, in ab, it is true also of the predecessor of d in ab (Theorem 6 and Theorem 7, Corollary 1). Therefore, if any number c is contained in P, the successor of c in ab is also contained in P. This is true without exception, since b is not contained in P, because ab can be divided into ab and bb, where bb consists of b alone. Therefore, by the definition of interval, the set P is null.

THEOREM 9. *This division is unique.*

For suppose there were another such division of ab, say a division into $(ac)'$ and $(cb)'$. Let P be the set of all numbers in ac and not in $(ac)'$. Since every number in ac, other than c, has a successor in ac, and every number in $(ac)'$, other than a, has a predecessor in $(ac)'$, it follows that if P contains d it contains also the successor of d in ab. Therefore P is null. And, therefore, every number in ac is contained also in $(ac)'$. By the same reasoning, every number in $(ac)'$ is contained also in ac. Therefore ac and $(ac)'$ are identical. Therefore cb and $(cb)'$ are identical.

DEFINITION. The number d, in ab, different from c, in ab, *precedes* or *follows* c *in* ab according as d is in ac or cb.

THEOREM 10. *If d precedes c in ab, then c follows d in ab; and if c follows d in ab, then d precedes c in ab.*

For by Theorems 7, 8, 9, we have

$$ab = ac+cb = ad+dc+cb = ad+db,$$

where db contains c.

THEOREM 11. *If c_1 precedes c_2 in ab and c_2 precedes c_3 in ab, then c_1 precedes c_3 in ab.*

For we have

$$ab = ac_1+c_1b = ac_1+c_1c_2+c_2b = ac_1+c_1c_2+c_2c_3+c_3b = ac_1+c_1c_3+c_3b,$$

and since $c_1c_3+c_3b = c_1b$, by Theorem 7, it follows that c_1b contains c_3.

THEOREM 12. *In any subset P, not null, of an interval ab there is a first number and a last number.*

Let p stand for any number in P. Then in the set R of all numbers which occur in any interval ap, there is a number, c, which has no successor in the set. This number c is a member of P. For, if it were not, it would be a number, not an end number, in some interval ap, and its successor in ap would be a member of R. And there is no number p, in P, which follows c in ab. For, if there were, c would be contained in ap, and its successor in ap would be a member of R. Finally, if d is any number in P, different from c, d must precede c in ab, for c does not precede d, and it follows at once from the definition that one of the numbers c and d precedes the other in ab. Therefore c is the last number in P.

In the set T of all numbers which occur in every interval ap is a number, e, which has no successor in the set. This number e is a member of P. For, if it were not, it would be a number, not an end number, in every interval ap, and its successor in ab would be in every ap, and would, therefore, be a member of T. And there is no number p, in P, which precedes e in ab. For, if there were, e would not be contained in ap, and would, therefore, not be a member of T. And if d is any number in P, different from e, d must follow e in ab. Therefore e is the first number in P.

THEOREM 13. *If a and b are distinct numbers, there do not exist both an interval ab and an interval ba.*

Suppose both do exist. Then, by postulate 4, $ab + ba$ is the set of all numbers.

Suppose that, apart from a and b, ab and ba have no number in common, and no number in either is successor of any number in the other. Then, by postulate 2, there is some proper part, T, of $ab + ba$ in which every number has a successor. There is a number, c, in $ab + ba$ which is not contained in T. It is possible to choose c distinct from a and b. For, if a is not in T, the predecessor of a in ba is also not in T, and if b is not in T, the predecessor of b in ab is also not in T; and since, by Theorem 5, either ab or ba must contain numbers other than a and b, we can always find a number distinct from a and b and not in T, as required. Let c be so chosen, and suppose that c is in ab. Let d and e be the predecessor and the successor, respectively, of c in ab. Then $eb + ba + ad$ is an interval ed by Theorem 7. But this interval contains a part, T, in which every number has a successor, contrary to the definition of interval.

Suppose that, apart from a and b, ab and ba have no number in common, and that some number in one of them, different from a and b, say c in ab, has a successor in the other different from a and b, say d in ba. Then $ac + da$ is a proper part of the set of all numbers in which every number has a successor and a predecessor, contrary to postulate 4.

Suppose that ab and ba have a number, c, in common, other than a and b. Then $ac + ca$ is a proper part of the set of all numbers in which every number has a successor and a predecessor, contrary to postulate 4.

Therefore, in every case, the supposition that both ab and ba exist leads to a contradiction.

THEOREM 14. *If c is a successor of b, the existence of an interval ab implies the existence of an interval ac.*

The number c has no successor, d, in ab. For, if it had, either d would be the predecessor of b in ab, in which case b, c, and d would be the only numbers, by postulate 4, and postulate 2 would be violated, or, if d were not the predecessor of b, the numbers c and d would constitute an interval cd and c together with db would constitute an interval dc, contrary to the preceding theorem. Now there are numbers in ab of which c is successor, for b is such a number. Let d be the first such number (Theorem 12). Then ad and c together constitute an interval ac, by Theorem 7, Corollary 1.

THEOREM 15. *If c is a predecessor of a, the existence of an interval ab implies the existence of an interval cb.*

This follows by reasoning similar to the preceding, using Theorem 7, Corollary 2, in place of Theorem 7, Corollary 1.

DEFINITION. If a is any number, the *ray* A is the set of all numbers b such that an interval ab exists, and the *ray* A' is the set of all numbers c such that an interval ca exists.

From the theorems which precede, we can infer at once that the ray A contains a, and contains no predecessor of a, that every number in A has a successor in A, and that every number but a in A has a predecessor in A. Similarly, the ray A' contains a, and contains no successor of a, and every number in A' has a predecessor in A', and every number but a in A' has a successor in A'.

THEOREM 16. *The rays A and A' have no number other than a in common.*

For, if they had b, different from a, in common, intervals ab and ba would both exist, contrary to Theorem 13.

THEOREM 17. *If the numbers b and c are successors of the number a, then b and c are the same number.*

For suppose that b and c were distinct. Then, if the ray B did not contain c, $A' + B$ would be a proper part of the set of all numbers of which postulate 4 would not be true. Therefore B contains c, and, for the same reason, C contains b. But neither B nor C contains a. Therefore $B + C$ is a proper part of the set of all numbers in which every number has a successor and a predecessor, contrary to postulate 4.

THEOREM 18. *If the number a is successor of the numbers b and c, then b and c are the same number.*

THEOREM 19. *$A + A'$ is the set of all numbers.* (Postulate 4.)

THEOREM 20. *If S is a part of the ray A, such that a is a member of S, and the class of all successors of numbers in S is contained in S, then S contains every number of A.*

For otherwise $S + A'$ would be a proper part of the set of all numbers in which every number had a successor and a predecessor.

THEOREM 21. *If S is a part of the ray A', such that a is a member of S, and the class of all predecessors of numbers in S is contained in S, then S contains every number of A'.*

For otherwise $S + A$ would violate postulate 4.

We have now shown that the set of all numbers can be divided into two parts, A and A', which have a only in common and which satisfy Peano's postulates in the manner described above. Therefore the set of postulates 1, 2, 3, 4 with which we began is categorical.

PRINCETON UNIVERSITY,
PRINCETON, N. J.