REDUCTIO AD ABSURDUM *

(Proof by contradiction)

Y.K. Leong
National University of Singapore

In mathematics, we are concerned with statements about the entities of a certain system. This system is a closed system in the sense that every term has a definite and rigid meaning, and rules for manipulation of these terms always lead us back into the system. To use a crude analogy, a mathematical system is like a chessboard in which the pieces have fixed capabilities and incapabilities, and the transition of one chess position into another is governed by strict rules of movement of the pieces. The whole business of mathematics is to formulate statements about a given mathematical system and to examine which of them are true. The method of establishing or refuting a given statement is condensed into a series of propositions constituting a so-called mathematical "proof". The vehicle by which these propositions are transported to their final conclusion is governed by strict rules of logic.

There is in mathematics a powerful method of proof known as "reductio ad absurdum" (Latin phrase: "reducing to absurdity") or commonly referred to as "proof by contradiction". Its reasoning is based on the fact that given a mathematical statement S, either S is true or else not-S (negation of S) is true. S and not-S cannot be both true. (Of course, in ordinary language, there are statements for which we cannot say whether "it is true" or "it is not true". For instance, "Today is Monday" is a statement which depends on time and place.) "Proof by contradiction" is an indirect proof. Instead of reaching our desired conclusion starting from true premises and using syllogistic arguments, we first assume the truth of the negation of our desired conclusion. As G.H. Hardy puts it, it is like a chess gambit: we are giving away our game. But like a gambit, the successive moves proceed to demolish the pillars on which our mathematical system is built. We finally reach a situation in which contradictions are generated within the system. We could do one of two things: throw away the whole system or throw away the assumption that we started off with. If our system is sound, it is obvious what we should throw away.

One of the classical examples of proof by contradiction is the proof that $\sqrt{2}$ is irrational. First of all, what is meant by "irrational"? An irrational number is, of course, a number which is not rational, and a rational number is one which can be written in the form m/n, where m, n are integers and $n \neq 0$. The proof proceeds as follows. Assume that $\sqrt{2}$ is rational; i.e. $\sqrt{2} = m/n$ where m, n are integers, $n \neq 0$. Since we may cancel off common factors of m and n, we may further assume that m and n do not have non-trivial common factors. We have $2n^2 = m^2$. It follows that 2 divides m^2 and hence m. Let $m = 2m_1$. Then $2n^2 = 4m_1^2$, or $n^2 = 2m_1^2$. This means that 2 divides n^2 and hence n. At this stage, let us sum up the situation: our assumption that $\sqrt{2} = m/n$, where m and n are relatively prime, leads us to the contradiction that m and n have 2 as a common factor. Therefore we conclude that $\sqrt{2}$ is irrational.

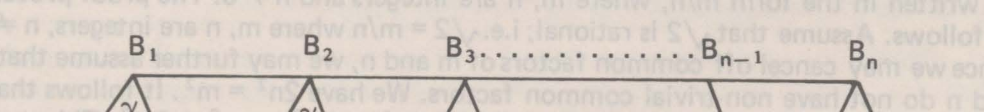
*Text of a talk delivered at Anglo-Chinese Junior College in 1979.

Another old story is Euclid's proof that there are infinitely many primes. A prime is an integer ($\geqslant 2$) whose only positive factors are 1 and itself. Thus the sequence of primes starts off with: 2, 3, 5, 7, 11, 13, 17, 19, 23, ... "Commonsense" may indicate the possibility of going on indefinitely, but anyone who has tried to test whether a large integer is a prime will appreciate the formidable numerical difficulties. There is as yet no way of writing down as large a prime number as we like.

Now for the proof. Suppose that there is a finite number of primes, so that there is one, N say, which is the largest prime. Consider the integer $M = N! + 1$. Either M is prime or it is not. If it is a prime, then $M > N$, contradicting the nature of N. So M cannot be prime. It must be divisible by some prime p say. Now, if we look at M closely, it is not divisible by all the primes from 2 to N inclusive. But p must be one of these. This is again a contradiction. Hence such a prime N cannot exist; and so the number of primes must be infinite.

There is an interesting episode in the history of mathematics in which generations of mathematicians attempted to use the method of proof by contradiction to prove an impossibility. For a long time before the 19th century, there was a belief that Euclid's "Parallel Postulate" could be proved from the rest of his axioms or postulates. An equivalent formulation of the "Parallel Postulate" is: "Through a given point not on a given (straight) line there can be drawn exactly one line parallel to the given line". One of the most well-known efforts to prove this was made by the Italian geometer Saccheri (1667–1733), who, in fact, tried to derive contradictions from the assumption that the Parallel Postulate is false. It was known to him that the Parallel Postulate is equivalent to the statement: "The sum of the angles of any triangle is 2 right angles". He did succeed in showing that the assumption that the angle sum of a triangle is greater than 2 right angles leads to a contradiction. However, his proof that the angle sum of a triangle cannot be less than 2 right angles is erroneous. With hindsight, we know that he could not have succeeded anyway. Since the discovery of non-Euclidean geometry by J. Bolyai (1802–1860) and Lobachevskii (1793–1856) in the 19th century, the Parallel Postulate is known to be independent of the other axioms of Euclid.

We outline the proof by Legendre (1752–1833) that the angle sum of a triangle is less than or equal to 2 right angles, without assuming the validity of the Parallel Postulate. The proof is again one by contradiction.



Let $A_1 B_1 A_2$ be a given triangle. On the line through $A_1 A_2$ produced, construct congruent triangles $A_i B_i A_{i+1}$, $i = 2, 3, \ldots, n$, where $A_1 A_2 = A_2 A_3 = \ldots = A_n A_{n+1}$. Let the angles of triangle $A_1 B_1 A_2$ be α, β, γ (see figure). We wish to show that $\alpha + \beta + \gamma < 2$ right angles. Suppose that $\alpha + \beta + \gamma > 2$ right angles. Then since A_1, A_2, A_3 lie on a straight line, $\alpha + \beta + \gamma_1 = 2$ right angles, where γ_1 = angle $B_1 A_2 B_2$, so that $\alpha + \beta + \gamma_1 < \alpha + \beta + \gamma$, i.e. $\gamma_1 < \gamma$ Then $A_1 A_2 > B_1 B_2$, $A_2 A_3 > B_2 B_3, \ldots$, $A_i A_{i+1} > B_i B_{i+1}, \ldots, A_{n-1} A_n > B_{n-1} B_n$. (Since $A_1, A_2, \ldots, A_{n+1}$ are collinear, we have $A_1 B_1 + B_1 B_2 + \ldots + B_{n-1} B_n + B_n A_{n+1} > A_1 A_{n+1}$, i.e. $A_1 B_1 + (n-1) B_1 B_2 + B_1 A_2 > n A_1 A_2$, i.e. $A_1 B_1 + B_1 A_2 - B_1 B_2 > n(A_1 A_2 - B_1 B_2)$. Now $A_1 A_2 - B_1 B_2 > 0$ and n is arbitrary. If we choose n large enough we get a contradiction (of the axiom of Archimedes).

So far our examples are taken from very classical, if not ancient, mathematics. As a contrast, we give an example of proof by contradiction from mathematics of recent vintage — if one may consider one hundred years ago as recent enough. The subject itself has only been recently introduced to elementary levels of education. We are referring to set theory. We are all aware of the controversy raised by the introduction of sets at the primary school level at the expense of the more traditional topics. Perhaps it may interest you, if not console you, to know that the introduction of infinite sets by the German mathematician Georg Cantor (1845—1918) in 1882 raised an outcry against what were then philosophically unfamiliar and shaky notions like uncountability. Since then the foundations of mathematics appeared to be undermined by the underlying philosophical quicksand. Fortunately for mathematicians the further sinking of the foundations was prevented with concerted and concentrated repairs and reconstruction, and mathematicians continue to make their honest living and you continue to invite them to deliver talks.

To return from the quagmire of historical controversies and intellectual confrontations, let us adopt the attitude and mentality of a bright-eyed naive novice with an open and receptive mind. (As a matter of fact, there is a part of set theory which is known to mathematicians as "Naive set theory".) Let us play with infinite sets as if they were as tangible as toy blocks were to a child. Therefore we assume everybody knows what a set is. Take a set S. If we can count all its elements in a finite number of steps or in a finite interval of time, then we say that S is a finite set. The process of counting involved here is really a mental process rather than an actual physical process. On the other hand, if we cannot perform such a task, then we naturally call S an *infinite* set: for example, the set of integers or the set of prime numbers. The revolutionary break-through which Cantor achieved lies in his audacious attempt to "count" infinite sets.

The most "natural" infinite set to look at, at least to the mathematicians, is the set $N = \{0, 1, 2, \ldots, n \ldots\}$ which is naturally called the set of "natural" numbers. We could ramble off the elements of N one after another, though without coming to an end, in a manner reminiscent of counting, so we call the set N "countable". There are, of course, other infinite sets whose elements could be "counted" off in such a fashion, such as the set of positive even integers $\{2, 4, 6, \ldots\}$. Thus we make the following definition. A set X is said to be *"countable"* if there is a one-to-one mapping from X *onto* N. For example, if $X = \{1, 4, 9, 16, \ldots, n^2, \ldots\}$, the mapping $f\colon X \to N$ defined by $f(n^2) = n-1$, $n = 1, 2, \ldots$, is one-to-one and onto, and so X is countable.

A moment's reflection may give one an uneasy feeling that there are "as many" perfect squares as there are natural numbers. However, counting no longer has its physical meaning and we are beginning to get slightly detached from the world of physical reality. We will rely only on the inflexible rules of logic; physical intuition will fail us. The question to ask is then: "Are there sets which are not countable?" Indeed there are, and lots more of them.

We show that the set of positive real numbers less than 1 is *not countable.* Let $X = \{ x \in \mathbb{R} : 0 < x < 1 \}$. The proof is again one by contradiction. Assume that X is countable. What does that amount to? It means that we can list all the members of X one by one, starting from a real number which we designate the first (or perhaps the zeroth), then a second, a third, and so on, and the listing will exhaust all of X. For this purpose, we will use the decimal representation of real numbers. Any positive real number less than 1 may be written in an infinite decimal form $0 . a_1 a_2 . . . a_n . . .$ where each a_i is one of the numbers 0, 1, . . . , 9. However, there is a slight snag: we must make sure that each member of X is listed exactly once, and there are different-looking decimals which represent the same number, such as $0 \cdot 099 . . . 9 . . .$ and $0 \cdot 10 . . . 0 . . . 0$. This is easily overcome by adopting the rule that we disallow all decimal representations with an infinite chain of 9's.

So if the above list could be drawn up, we could exhibit it in the form:

$$x_1 : 0 \cdot a_{11} a_{12} \ldots a_{1n} \cdots$$
$$x_2 : 0 \cdot a_{21} a_{22} \ldots a_{2n} \cdots$$
$$\vdots$$
$$x_k : 0 \cdot a_{k1} a_{k2} \cdots a_{kn} \cdots$$
$$\vdots$$

We now come to the following contradiction. No matter how the list is made, we can always find a positive real number less than 1 which is not in the list (which is supposed to exhaust the set X). This will then destroy the possibility of the existence of such a list and so X cannot be countable.

Now, how do we create the above contradiction? We define our desired number as follows. Choose a b_1 not equal to a_{11} or 9, a b_2 not equal to a_{22} or 9, and so on, and in general, a b_k not equal to a_{kk} or 9. Bear in mind that each of these b_k are chosen from 0, 1, . . . , 8. Look at the number $b = 0 \cdot b_1 b_2 \ldots b_k \ldots$. It does not have an infinite chain of 9's and is certainly in X. Yet $b \neq x_k$ since it differs from x_k at the kth place of decimal.

The above proof is also called a "diagonal" argument for obvious reasons and is first given by Cantor himself. The implications and repercussions on mathematics were tremendous. Eyes were literally opened towards new horizons. The existence of the so-called "transcendental" numbers was immediately revealed without even giving an inkling as to what one such number could be. This was a disturbing thought to many mathematicians at that time. There have been well-known transcendental numbers like π and e. But the proofs that they are transcendental are difficult. In fact, not too many transcendental numbers were known, especially at that time. And yet here is a proof that claims that multitudes upon multitudes of these creatures abound. The intellectual shock must have been great.

The existence of a mathematical object is sometimes claimed by showing that its non-existence leads to a contradiction. More often than not, such a proof does not actually produce the object. At the end of it, we may not know its value if the object is a number say, nor do we have a procedure or algorithm for finding it. Partly for this reason, some mathematicians, the so-called intuitionists and constructivists, do not find such a proof acceptable. But by and large, the majority of mathematicians are not prepared to renounce the treasury of results obtained by such proofs. A particularly effective application of proof by contradiction is in establishing the non-existence of a mathematical object. This is of course, universally acceptable and is a very powerful weapon in the advancement of mathematics.

ANNOUNCEMENT

The next International Congress of Mathematicians will be held in Warsaw, August 11 – 19, 1982. The Chairman of the Organising Committee is Professor Czeslaw Olech.

The Singapore Mathematical Society will hold an International Mathematical Conference in conjunction with the Department of Mathematics, National University of Singapore at the National University of Singapore on June 1–13 1981.