

The diagonal proof technique

In this course we will among other things consider similarities among the diagonal proofs of Georg Cantor, Kurt Gödel, and Alan Turing, for three key theorems in mathematics, all related to computer science. Diagonal proofs show by contradiction that a claim about numbers (or strings, or propositions, or programs) does not hold, by using the claim to define a set element with properties that violate the claim.

Cantor's theorem holds that the *cardinality* (roughly, size) of the set of real numbers is strictly greater than the cardinality of the set of natural numbers. Gödel showed in 1931 that true assertions in number theory exist that are unprovable within the system of the assertions themselves. Turing showed that a certain problem in computation is algorithmically undecidable, namely the problem of whether a machine of a given description halts on a given input.

The diagonal-proof idea is used to show that there is no 1-to-1 correspondence between two sets; for example, the set of natural numbers (\mathbf{N}) and the set of real numbers (\mathbf{R}). It is a proof by contradiction: It starts with an assumption and then shows that the assumption leads to a contradiction, so the assumption must be dropped.

To show that no bijection exists between two given sets, we can begin by assuming that a bijection *does* exist. For instance, if one of the sets is countable, the assumption can be that the other is countable, and thus has an enumeration listing all elements. Thus, suppose the reals are countable; i.e., there exists an enumeration of reals. Then by the assumption we can list all the reals between 0 and 1 (i.e., all infinite bit sequences with a dot in front) in an infinite series.

The diagonal proof then takes this assumed enumeration and defines a new real, y , whose i^{th} bit is the logical complement ($0 \rightarrow 1, 1 \rightarrow 0$) of the i^{th} bit of the i^{th} element of the supposed enumeration. For every element x of the enumeration, that real y has at least one bit that differs from the bit in the same position of x . Thus y differs from every element in the supposed enumeration, so y can't be in the enumeration. But y is clearly a real, i.e., an infinite bit sequence after a dot. So there can't be such an enumeration. This is the desired contradiction.

It follows that there is no bijection between the reals and the natural numbers. What is diagonal is that the spoiler value, y , is formed by taking bits from the diagonal of the supposed enumeration and flipping them.