Cantor's Little Theorem

Arindama Singh
Department of Mathematics, IIT Madras
email: asingh@iitm.ac.in

Abstract: This article discusses two theorems of Georg Cantor: Cantor's Little Theorem and Cantor's Diagonal Theorem.These results are obtained by generalizing the method of proof ofthe well known Cantor's theorem about the cardinalities of a setand its power set. As an application of these, Gödel's firstincompleteness theorem is proved. Hints are given as to how to derive other deeper results including the existence of Parikh's sentence.

1. Introduction

Each high school student knows what a set is. It was not so before Georg Cantor. He was seriously objected by many well established mathematicians for advocating the notion of *many infinities*. This notion is well recognized now to the point that it forms a basis for modern analysis.

The idea is simple; it says that a set always has less number of elements than its power set. In particular, there are less natural numbers than reals. It is intuitively clear that a finite set has always less number of elements than its power set. For, the power set of a set having n elements has 2^n elements. Taking the set of natural numbers as $\mathbb{N} = \{0, 1, 2, \ldots\}$, we see that the number of elements in any finite set is a natural number. But then the question arises as to how do we talk of the *number of elements* of an infinite set. Well, what is this 'number of elements'? How do we know that there are 10 elements in $\{0, 1, 2, \ldots, 9\}$? Simple, we just *count* them. But then how to count the number of elements in $\mathbb{N}$?

2. Cardinality

Let us look back. What do we mean by counting the elements of a set? Say, how do we count the elements of $\{0, 1, 2, \ldots, 9\}$? It looks odd to ask such a trivial question. But let us put into words whatever that is in our mind.

I would count this way: I put my index finger on 0 and then say 1; next, put my finger on 1 and then say 2, $\cdots$, and finally, put my finger on 9 and say 10. By doing this I have defined a one-one function from the given set onto the set $\{1, 2, \ldots, 10\}$ which sends 0 to 1, 1 to 2, ..., 9 to 10. That is, by counting

we are simply defining a one-one function from a given set onto one set of the form $\{1, 2, 3, \ldots, n\}$. Then we declare that there are n number of elements in the given set. Thus a finite set can be counted this way. That is, a finite set, by definition, is a set from which there is a one-one function onto (even *into* is OK) a set of the form $\{1, 2, 3, \ldots, n\}$.

An infinite set is one which is *not* finite. However, the idea of a function can be used to define an infinite set without using this *not*. You can see easily that if a set is not finite, then there is a one-one function from it to (into or onto) a proper subset of it. Moreover, no finite set satisfies this property. Thus, we define an infinite set as one having this property. Since our counting method fails, we will use the word *cardinality* instead of the number of elements. We would then say that $card\ A = card\ B$ iff there is a one-one function from A onto B. Note that cardinality is only a technical version of the notion of number of elements. However, there is a difference. We do not define what cardinality of a set is. We only know how to talk of the cardinalities of two sets being equal. We can also compare the cardinalities of two sets. We define: $card\ A \leq card\ B$ iff there is a one-one function from A into B. Further, $card\ A < card\ B$ iff $card\ A \leq card\ B$ but $card\ A \neq card\ B$. The fact that $card\ A \leq card\ B$ and $card\ B \leq card\ A$ implies $card\ A = card\ B$ is the well known Cantor-Schröder-Bernstein theorem.

3. Cantor's Theorem

For a set A, let 2^A denote its power set. Cantor's theorem can then be put as $card\ A < card\ 2^A$. A modification of Cantor's original proof is found in almost all text books on Set Theory. It is as follows.

Define a function $f : A \to 2^A$ by $f(x) = \{x\}$. Clearly, f is one-one. Hence $card\ A \leq card\ 2^A$. To show that $card\ A \neq card\ 2^A$, we prove that no one-one function from A to 2^A can be onto. On the contrary, suppose that there is a one-one onto function $g : A \to 2^A$. Let $B = \{x \in A : x \notin g(x)\}$. Since $B \in 2^A$ and g is one-one onto, there is exactly one $y \in A$ such that $g(y) = B$. Is $y \in B$? If $y \in B$, then y must satisfy the defining property of B, and then $y \notin g(y)$. As $g(y) = B$, $y \notin B$. On the other hand, if $y \notin B$, then $y \notin g(y)$, and then y satisfies the defining property of B. Thus, $y \in B$. So, we have shown that $y \in B$ iff $y \notin B$. This is a contradiction. Therefore no one-one function from A to 2^A can be onto.

This is not Cantor's original argument. His argument involves defining a two-variable function which for no values of one of its variables can be equal

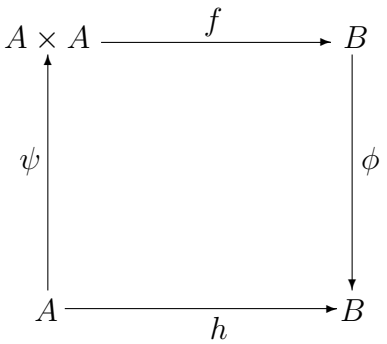
to a well constructed one-variable function. We will abstract his argument to obtain another result. And from that result, we will derive the above theorem. Shortly, we will also see that it is worth doing, for many deep results will follow from this generalization.

4. Cantor's Diagonalization Theorem

To formulate the generalized result, we will introduce some jargons. First, let $\phi : B \to B$ be any function on a set B. ϕ *has a fixed point* iff there is $b \in B$ such that $\phi(b) = b$. Second, let A, B be sets, and $f : A \times A \to B$ be any function. A function $g : A \to B$ *is representable by*f iff there is $a \in A$ such that for all $x \in A$, $g(x) = f(x, a)$. This means that g is representable by f if we can get themap g by evaluating f in its second argument at some point;i.e., $g(\cdot) = f(\cdot, a)$. For different functions $g : A \to B$, the point a can be different so that g is representable by$f$. Can we represent every one-variable function g by a two-variable function f? The following result puts some restrictions on such an f.

Theorem 4.1 [Cantor's Little Theorem] Let A, B be sets and $f : A \times A \to B$ be any function such that all functions $g : A \to B$ are representable by f. Then every function $\phi : B \to B$ has a fixed point.

Proof Suppose that $f : A \times A \to B$ is such a function that all functions $g : A \to B$ are representable by f. Let $\phi : B \to B$ be any function. Define a function $\psi : A \to A \times A$, called *Cantor's diagonalization*, by $\psi(x) = (x, x)$. Let $h = \phi \circ f \circ \psi$; look at the diagram below.



Since the function $h : A \to B$ is representable by f, we have an $a \in A$ such that for all $x \in A$, $h(x) = f(x, a)$. In particular, $h(a) = f(a, a)$. But $h(a) = \phi(f(\psi(a))) = \phi(f(a, a))$. Writing $f(a, a) = b$, we have $\phi(b) = b$. Thus ϕ has a fixed point, namely, b. □

In fact, we have proved a bit more than what is stated in Theorem 4.1. Our construction in the above proof shows the following.

Theorem 4.2 [Cantor's Diagonalization Theorem] Let A, B be sets, and $f : A \times A \to B$, $\phi : B \to B$ be functions. Let $\psi : A \to A \times A$ be the function defined by $\psi(x) = (x, x)$. If ϕ does not have a fixed point, then $h : A \to B$ defined by $h = \phi \circ f \circ \psi$ is not representable by f.

We will refer to the Theorems 4.1-4.2 as CLT, Cantor's Little Theorem and CDT, Cantor's Diagonalization Theorem, respectively. We will now derive Cantor's theorem from CLT. The technique is to choose some particular functions f, g, ϕ, ψ so that the things fall into place.

Theorem 4.3 [Cantor's Theorem] Let A be any set and 2^A be the power set of A. Then $card\ A < card\ 2^A$.

Proof: The map $x \mapsto \{x\}$ is a one-one function from A into 2^A. Hence, $card\ A \leq card\ 2^A$. We show that $card\ A \neq card\ 2^A$. On the contrary, suppose that $card\ A = card\ 2^A$. Then there is a one-one onto function $\alpha : A \to 2^A$. Define a function $f : A \times A \to 2^A$ by

$$f(x, y) = 1 \text{ if } x \in \alpha(y), \text{ and } f(x, y) = 0 \text{ if } x \notin \alpha(y).$$

Let $g : A \to \{0, 1\}$ be any function. This defines a subset of A, namely, $B = \{x \in A : g(x) = 1\}$. Since $\alpha : A \to 2^A$ is onto, there is $z \in A$ such that $\alpha(z) = B$. Now $f(x, z) = g(x)$ for every $x \in A$. Let us verify it. If $x \in B = \alpha(z)$, then $f(x, z) = 1$, and in this case, $g(x) = 1$, by the definition of B. On the other hand, if $x \notin B$ (with $x \in A$), then $x \notin \alpha(z)$, i.e., $f(x, z) = 0$, and in this case, $g(x) = 0$, again by the definition of B. Thus, for every $x \in A$, $g(x) = f(x, z)$. Hence every function $g : A \to \{0, 1\}$ is representable by f. By CLT, every function $\phi : \{0, 1\} \to \{0, 1\}$ has a fixed point. However, the negation function $\neg : \{0, 1\} \to \{0, 1\}$ defined by $\neg(0) = 1, \neg(1) = 0$ has no fixed point. Therefore, $card\ A \neq card\ 2^A$. □

In the following section we prove some more results by using CLT/CDT.

5. Some More Consequences

You have rightly thought that CLT (or CDT) is not just a generalization of Cantor's Theorem; it is a generalization of the proof of Cantor's Theorem. It encapsulates the spirit of Cantor's diagonalization argument employed in the proof of Cantor's Theorem as discussed in Section 2. Thus it should be possible to derive all the results wherever the diagonalization process is used. In this section we derive some such results as corollaries to CDT.

The intended results are from mathematical logic. We will denote by F_1, the set of all first order formulas having one free variable, up to equivalence. F_1 consists of all formulas of the type $P(x), \forall y Q(x,y), \forall x Q(x,y), \exists y Q(x,y)$, $\forall x \exists y(\neg P(x) \wedge Q(y,z))$, etc, having exactly one unquantified variable. Since F_1 is taken up to equivalence, two formulas in F_1 are equal iff they are equivalent as first order formulas. Similarly, F_0 denotes the set of all formulas having no free variables, i.e., all statements, up to equivalence.

We also require the mechanism of Gödel numbering. This scheme assigns a unique natural number to each first order formula in a constructive way. Given a formula P, its Gödel number $\ulcorner P \urcorner$ is a unique natural number from which the formula P can be constructed back. Moreover, each formula is interpreted in the set of natural numbers. Thus formulas in $F_0 \cup F_1$ are taken as properties of natural numbers, or as is commonly said, they are arithmetical predicates. The scheme of Gödel numbering is easily extended to proofs. That is, each proof also has a Gödel number; of course, you have to fix an axiomatic system for the first order logic here, when you talk about proofs. From the Gödel numbering it follows (see [2]) that there exists a function $\delta : \mathbb{N} \to \mathbb{N}$ which satisfies $\delta(\ulcorner P(x) \urcorner) = \ulcorner P(\ulcorner P(x) \urcorner) \urcorner$. In the proof of the following result we make use of this function (also called a diagonalization function) δ.

Theorem 5.1 [Löb's Theorem] For any formula $P(x) \in F_1$, there exists a statement $S \in F_0$ such that $S \equiv P(\ulcorner S \urcorner)$ holds.

Proof Define the function $h : F_1 \to F_0$ by $h = \phi \circ f \circ \psi$, where

$\phi : F_0 \to F_0$ with $\phi(C) = P(\ulcorner C \urcorner)$,

$f : F_1 \times F_1 \to F_0$ with $f(Q(x), R(y)) = R(\ulcorner Q(x) \urcorner)$, and

$\psi : F_1 \to F_1 \times F_1$ with $\psi(P(x)) = (P(x), P(x))$.

Let $\delta : \mathbb{N} \to \mathbb{N}$ be the diagonalization function with $\delta(\ulcorner Q(x) \urcorner) = \ulcorner Q(\ulcorner Q(x) \urcorner) \urcorner$ for any formula $Q(x) \in F_1$. Suppose that ϕ does not have a fixed point. Then by CDT, h is not representable by f. Now,

$$\begin{aligned} g(Q(x)) &= \phi(f(\psi(Q(x)))) = \phi(f(Q(x), Q(x))) = \phi(Q(\ulcorner Q(x) \urcorner)) \\ &= P(\ulcorner Q(\ulcorner Q(x) \urcorner) \urcorner) = P(\delta(\ulcorner Q(x) \urcorner)) = f(Q(x), P(\delta(y))). \end{aligned}$$

This shows that h is representable by f, a contradiction. Therefore, ϕ has a fixed point. Call this fixed point S. Then $S = \phi(S) = P(\ulcorner S \urcorner)$. Since equality in F_1 is simply the equivalence of formulas, $S \equiv P(\ulcorner S \urcorner)$. □

The following result uses the Gödel numbering of proofs.

Theorem 5.2 [Gödel's First Incompleteness Theorem] There is a statement $S \in F_0$ about arithmetic such that S is true iff S is not provable.

Proof Let $P(y, x)$ be the formula denoting "y is the Gödel number of a proof of a statement whose Gödel number is x". This formula is an arithmetical predicate having two free variables; the variables are to take values from $\mathbb{N}$. Let $Q(x) = \forall y \neg P(y, x)$. Now, $Q(x) \in F_1$. By Löb's Theorem, there is a statement $S \in F_0$ such that $S \equiv Q(\ulcorner S \urcorner)$. That is, $S \equiv \forall y \neg P(y, \ulcorner S \urcorner)$ or that $S \equiv \neg \exists y P(y, \ulcorner S \urcorner)$. This says that S is true iff it is not the case that there is a natural number y which is the Gödel number of a proof of S. □

6. Conclusion

No mathematical discourse is complete without raising further problems. To tackle the problems one must master the techniques and there, exercises come of help. Let us have some exercises in the form of applications of CLT/CDT. Your interest may take you to the materials in [1,2,4].

Our first exercise is the Russell's paradox. It says that the set of all sets which are not members of themselves is a member of itself and at the same time, it cannot be a member of itself. It is, of course, not a contradiction since the phrase 'set of all sets which are not members of themselves' may not be meaningful. The exercise is: show that the collection of all sets which are not members of themselves is not a set.

Another well known paradox is the so called Liar's paradox. It says that "This sentence is false" is true iff it is false. A way out is that this particular sentence is meaningless. However, a stronger form of the paradox can be constructed which incorporates meaninglessness into itself. The exercise is: show that there is an English sentence which is neither true, nor false, nor even meaningless.

Using the same technique as explained in this paper, you can also show that there is a (true) statement S in arithmetic whose proof is long but the fact that 'there is a proof of S' has a short proof. This sentence S is called Parikh's sentence. To show this you may start with three arithmetical predicates:

$P(m, x) \equiv$ m is the Gödel number of a proof of a statement whose Gödel number is x

$Q(x) \equiv \exists y P(y, x) \equiv$ the statement whose Gödel number is x

$R_n(x) \equiv \neg \exists m (m < n \wedge P(m, x)) \equiv$ the statement whose Gödel number is x has no proof of length less than n.

Using Löb's Theorem, you conclude the existence of a statement S_n such that $S_n \equiv R_n(\ulcorner S_n \urcorner)$ holds. Since n is arbitrary, you can choose n to be as large as you like. Note that S_n has no proof of length less than n. Though a short proof of "S_n has a proof" can be given. Here is one such: if S_n has no proof, then $R_n(\ulcorner S_n \urcorner)$ is false, and then there is a proof of S_n shorter than n, a contradiction. Thus S_n has a proof. Moreover, this proof is really short! Formalize this argument to prove the existence of Parikh's sentence.

Here are some problems. A Richard sentence is a sentence in English that describes a natural number. Show that there is a Richard sentence which holds for a number m iff it does not hold for m. Is it a paradox or a contradiction? Can you use the same CLT/CDT to prove the existence of non-computable functions? Can the technique be used to prove Recursion Theorem and Rice's Theorem in the theory of computation? Can it be used to prove Baire Category Theorem and Ascoli's Theorem in Topology? What about the Second Incompleteness Theorem of Gödel?

Suggested Reading

1. F.W.Lawvere, Diagonal arguments and cartesian closed categories, In: *Category Theory, Homology Theory and Their Applications*, Springer, pp.134-145, 1996.

2. A.Singh and C.Goswami, *Fundamentals of Logic*, ICPR, New Delhi, 1998