

## Topic 1: Diagonal proofs and uncountable sets

1. Uncountable sets
2. Incompleteness
3. Coinduction

David Keil Theory of Computing 1/101

## How T1 relates to computing

- Our most important result in this course is that some problems are algorithmically unsolvable
- This sets a boundary on the power of computation
- Turing's uncomputability proof is *diagonal*
- Cantor's proof that  $|\mathbb{N}| < |\mathbb{R}|$  and Gödel's proof of limits of logic are also diagonal
- Computation deals with finite, infinite, and uncountable objects or sets
- computation is about sets of strings, languages

David Keil Theory of Computing 1/102

## Languages and countability

- A *string* is a sequence of symbols over a finite alphabet
- The strings are countable, e.g., by numbering them according to bit representation: 0, 1, 01, 10, 11, ...
- A *language* is a set of strings
- A language may be represented as an infinite bit sequence, with a bit in a certain bit location denoting membership in the language: {0, 10, 11, 100} = 10101100...
- Computation operates on strings; models of computation accept sets of strings

## 1. Uncountable sets

- Cardinalities of sets: informally, their sizes
- For infinite sets, we say that two sets have the same cardinality iff there is a *bijection* (1-to-1 correspondence) between their elements
- *Example:*  $\text{Card}(\text{EVEN}) = \text{Card}(\mathbb{N})$   
Proof:  $\text{EVEN}_0 = 0, \text{EVEN}_1 = 2, \text{etc.}$
- *Example:*  $\text{Card}(\mathbb{Q}) = \text{Card}(\mathbb{N})$   
Proof: Zig-zag through a table of rationals

**Theorem: Card  $\mathbb{R}$  > Card  $\mathbb{N}$  (Cantor)****Proof:**

1. Suppose  $\mathbb{R}$  were countable
2. Then the interval  $(0, 1]$  could be enumerated as:
 
$$r_1 = 0 . b_{1,1} b_{1,2} b_{1,3} \dots$$

$$r_2 = 0 . b_{2,1} b_{2,2} b_{2,3} \dots$$

$$\dots$$
3. Now, consider the real number  $s =$ 

$$0 . \neg b_{1,1} \neg b_{2,2} \neg b_{3,3} \dots$$
 That is, for all  $n$ , bit  $n$  is  $\neg b_{n,n}$  (bitwise negation of the diagonal of  $r$ )

**Cantor's thm. (cont'd)**

4. Now, since for every  $i$ , the  $i^{\text{th}}$  bit of  $s$  is different from the  $i^{\text{th}}$  bit of  $r_i$ , so  $s$  differs from every element of  $r$ , so there is no element of sequence  $r$  that matches  $s$
5. Hence  $r$  does not contain  $s$ , which is clearly a real number
6. Hence we have a contradiction and must reject the supposition
7. Hence  $\mathbb{R}$  is not countable

## The proof, illustrated

Supposed enumeration of  $\mathbb{R}$ :

$$r_1 = (\underline{0}, 0, 0, 0, 0, 0, 0, \dots)$$

$$r_2 = (1, \underline{1}, 1, 1, 1, 1, 1, \dots)$$

$$r_3 = (0, 1, \underline{0}, 1, 0, 1, 0, \dots)$$

$$r_4 = (1, 0, 1, \underline{0}, 1, 0, 1, \dots)$$

$$r_5 = (1, 1, 0, 1, \underline{0}, 1, 1, \dots)$$

$$r_6 = (0, 0, 1, 1, 0, \underline{1}, 1, \dots)$$

$$r_7 = (1, 0, 0, 0, 1, 0, \underline{0}, \dots)$$

...

Real number that differs  
with every element in  
enumeration in at least  
one bit:

$$s = (\underline{1}, \underline{0}, \underline{1}, \underline{1}, \underline{1}, \underline{0}, \underline{1}, \dots)$$

## Summary of Cantor's proof

“The proof shows that no matter how a list of real numbers were arranged, a real number could still be defined that would not be in the list”

*T. DiRienzo, J. Bartlett, 2/09*

## A simple diagonal proof

- Let  $\Omega$  be “the set of all sets”
- Hence  $\Omega \in \Omega$
- *Theorem:* “Set of all sets” is a self-contradictory notion
- *Proof:* Consider  $\Omega' = \{ A : A \notin A \}$   
(sets not members of themselves)
- $(\Omega' \in \Omega') \Rightarrow (\Omega' \notin \Omega')$  ,  
 $(\Omega \notin \Omega) \Rightarrow (\Omega \in \Omega)$  , contradictions
- Note role of “Spoiler” instance  $\Omega'$
- We say that  $\Omega, \Omega'$  are *not well founded* (NWF)

## How many functions exist?

- Start with the set of functions  
 $\{ f : \{0\} \rightarrow \{0,1\} \}$
- This is a set of two functions:  
 $\{ \{(0,1)\}, \{(0,0)\} \}$
- The set  $\{ f : \{0, 1\} \rightarrow \{0,1\} \}$  has four elements,  
 $\{ f : \{0, 1, 2\} \rightarrow \{0,1\} \}$  has eight, etc.
- There are  $2^{\mathbb{N}}$  predicates  $f : \mathbb{N} \rightarrow \{0,1\}$
- *Question:* Is this the same as, or more than, the cardinality of the natural numbers?
- Compare with the cardinality of reals

## Can all predicates on $\mathbb{N}$ be computed in Java?

1. Enumerate all Java methods that take an integer parameter and return 0 or 1, as  $J_1, J_2, J_3, \dots$  in a bitwise ordering
2. Consider the predicate  $f: \mathbb{N} \rightarrow \{0,1\}$  s.t.  $f(n) = 1$  if  $J_n(n) = 0$  or  $J_n(n)$  hangs,  $f(n) = 0$  if  $J_n(n) = 1$
3. The predicate  $f$  differs in its behavior from each element of our enumeration of Java methods
4. Hence  $f$  is a predicate not computed by any Java method

## Results

- $\mathbb{N}$  is countable (cardinality  $\aleph_0$ , aleph-null)
- $\mathbb{R}$  is uncountable (cardinality  $\aleph_1$ )
- The set of Java functions is countable using their bit representations
- The set of predicates  $f: \mathbb{N} \rightarrow \{0,1\}$  is uncountable
- There are  $2^{\aleph_0} = \aleph_1$  predicates on  $\mathbb{N}$
- The *sets* of natural numbers are uncountable (see handout)

## 2. Incompleteness

# Gödel's Theorem: Limits of logic and computation

David Keil

*Based on a talk at the Framingham State College  
Math/Computer Science Faculty Seminar, March 27, 2003*

## Overview

- Kurt Gödel, 1931, at age 25, in Vienna, shook up the foundations of mathematical thought as developed in Russell and Whitehead's *Principia Mathematica*
- He showed that no formal axiomatic system of logic could be both *consistent* and *complete*
- Since predicate calculus was proven consistent, Gödel's theorem showed that some truths are unprovable in the system

## General-purpose definitions

- **Consistency:** Attribute of a system in which no false assertion can be proven  
$$\forall p ((\vdash p) \Rightarrow p)$$
- **Completeness:** Attribute of a system in which every true assertion can be proven  
$$\forall p (p \Rightarrow \vdash p)$$
- **Gödel number:** A value that uniquely encodes a logical assertion or sequence of assertions; e.g., a proof

## Intuition of Gödel's proof

- Gödel needed a counter-example to the claim that a system can be both complete and consistent
- He showed that *something like* the following is true but unprovable:  
*“This assertion has no proof”*
- But the assertion actually used has a precise meaning

## Definitions related to theorem

- $Proves(x, y, z)$ : The assertion that the sequence of symbols with Gödel number  $x$  is a valid proof that  $S_y(z)$  is true, where  $S_y$  is the formula with Gödel number  $y$ , and  $z$  is a natural number.
- Let  $G(y)$  be the assertion that  $\neg\exists x Proves(x, y, y)$  i.e.,  $G(y)$  means that what the formula with Gödel number  $y$  asserts about  $y$  is unprovable
- *Example*: Where  $y$  encodes the predicate *even*,  $G(y)$  is the assertion that one cannot prove that the encoding of the predicate *even* is an even number

## Gödel's theorem

“ $\neg\exists x Proves(x, \#(G), \#(G))$ ” is true in predicate calculus, but cannot be proven in the predicate calculus

- *Or*: What  $G$  asserts about predicate  $G$  is true but unprovable
- *Or*: There is no proof that  $G(\#(G))$  is true, but  $G(\#(G))$  is nevertheless true

## Proof of Gödel's theorem

1. Suppose the theorem's claim is false and there exists a proof in predicate calculus that  $\neg \exists x \text{Proves}(x, \#(G), \#(G))$ .
  2. Then the claim is true, by consistency of predicate calculus.
  3. Therefore by its own assertion it is unprovable in predicate calculus.
  4. This contradicts step 1, hence claim holds.
- Note:* The above proof goes outside the formal system of predicate calculus.

## Another way to see the proof

- Think of an infinite truth table, with all formulas on one variable enumerated down the left side and arguments to the formulas as column headers
- There is a *true* in column  $c$  of row  $r$  iff  $f_r(c)$  is true
- Let  $q$  be the Gödel number of the formula that asserts the unprovability of its argument
- Then there must be a *true* in column  $q$  of row  $q$ , because  $f_q(q) = \text{false}$  would say that formula  $q$  is not unprovable, hence provable, hence true, a contradiction
- But if  $f_q(q) = \text{true}$ , then  $f_q(q)$  is both true and (as it claims) unprovable

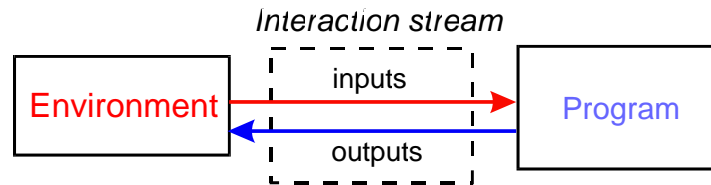
## Incompleteness and computer science

- Using the same *diagonal proof* method, Turing proved a special case of Gödel's theorem
- Given a *computable* function  $f$ , executing an algorithm to compute  $y = f(x)$  proves that  $f(x) = y$
- But for some functions  $f$ , for some  $x$ ,  $y = f(x)$ , but there is no proof that  $f(x) = y$
- This is the same as saying that no algorithm computes  $f$  -- example: the Halting Problem
- Gödel's work in *recursive function theory* matches Turing's results with automata

## Larger significance

- Gödel's theorem was part of a series of results establishing some *limits of knowledge*, that also included
  - Einstein's relativity results
  - Heisenberg's Uncertainty Principle
  - Turing's theorem that some functions are uncomputable
- It marked the failure of Russell's, Whitehead's and Hilbert's effort to reduce mathematics to first-order logic and set theory
- A category of *valid assertions* is established that we cannot *know* are valid

### 3. Streams and coinduction



## Inductively defined sets

- (i) 0 is a natural number;
- (ii) Every  $n \in \mathbb{N}$  has a unique successor,  $n'$ ;
- (iii) i and ii are the only ways to obtain a natural number (Peano)
- Set of expressions using numerals, +, and ( ):
  - $expression \rightarrow$
  - $numeral$  /
  - $numeral + expression$  /
  - $( expression )$
- The definition of such a set may *use* itself
- But such a set does not *contain* itself

## Well-founded sets

- (B. Russell) Let the village hair stylist be the person who cuts the hair of everyone who doesn't cut own hair
- Question: Who cuts the hair-stylist's hair?
- Similar Questions: Is there a set of all sets? If so, does it contain itself? Is there a set of all sets that don't contain themselves?
- In classical (well founded) set theory, it is meaningless to say a set belongs or doesn't belong to itself (Foundation Axiom)

## Streams and non well founded sets

- A non-well-founded set may contain itself, directly or indirectly
- *Example:*  $A = \{ B, C \}; B = \{ A, D \}$
- Every stream of characters is a character, followed by a stream of characters
- Streams contain streams, which contain streams, which contain streams, ...
- *Ex.:* The set of all bit streams  $\{0,1\}^\infty$  consists of any infinite sequence that consists of 0 or 1 followed by a stream

## Streams and coinduction

- *Induction* defines countable sets of finite objects:  $\Sigma^* = \{\lambda\} \cup \{ax \mid a \in \Sigma, x \in \Sigma^*\}$
- *Coinduction*
  - is a dual of induction (recursion), lacking a base case
  - is used to define sets of infinite objects
- The set of streams over an alphabet, expressing ongoing processes such as interaction:

$$\Sigma^\infty = \{ax \mid a \in \Sigma, x \in \Sigma^\infty\}$$

## References (Gödel)

John W. Dawson. *Logical Dilemmas: The Life and Work of Kurt Gödel*. A. K. Peters, 1997.

Gary Flake. *The Computational Beauty of Nature*. MIT Press, 2001, Ch. \_\_\_\_

Kurt Gödel. *On Formally Undecidable Propositions of the Principia Mathematica and Related Systems*. 1931.

Ernest Nagel and James R. Newman. *Gödel's Proof*. New York University Press, 1958.

## References (Coinduction)

Barwise-Moss. *Vicious Circles*, 1996

Finsler, 1920s (NWF sets)

Goldin-Wegner (at [www.engr.uconn.edu/~dgg](http://www.engr.uconn.edu/~dgg))

Peano, 1889 (induction)