Discrete Mathematics: Lecture 6

- Last time:
  - Chap 1.7: Introduction to Proofs
- Today:
  - Chap 1.8: Proof Methods and Strategy
- Note: Assignment 1 due at 9:50am next Wednesday
- Next time:
  - Chap 2.1: Sets
  - Chap 2.2: Set Operations

Review of last time

- Formal proofs versus informal proofs
- Terminology: theorem, proposition, lemma, corollary, conjecture
- Methods of proving theorems
  - Direct proofs
  - Proof by contraposition
  - Proofs by contradiction

Exhaustive Proof and Proof by Cases

- Proof by cases is based on:
  $p_1 \vee p_2 \vee \ldots \vee p_n \rightarrow q \equiv$
  $(p_1 \rightarrow q) \wedge (p_2 \rightarrow q) \wedge \ldots \wedge (p_n \rightarrow q)$
- An exhaustive proof (穷举法) is a special type of proof by cases where each case involves checking a single example
- Example: Prove that $(n+1)^3 \geq 3^n$ if n is a positive integer with $n \leq 4$
- Example: Prove that if n is an integer, then $n^2 \geq n$

Without Loss of Generality (WLOG, 不失一般性)

- WLOG, assume that ... Proof of the case
- Other cases follow by making straightforward changes to the proof
- Example: Show that if x and y are integers and both xy and $x + y$ are even, then both x and y are even.
- Incorrect use of this principle can lead to unfortunate errors

Common Errors with Exhaustive Proof and Proof by Cases

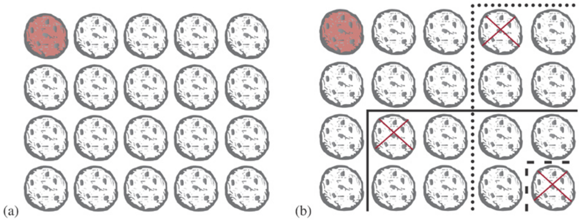
- Draw conclusions from examples
- Example: Every positive integer is the sum of 18 fourth power of integers.
- Miss some cases
- Example: If x is a real number, then x^2 is a positive real number.

Existence Proofs (存在性证明)

- A proof of a proposition of the form $\exists x P(x)$
- A constructive (构造性）) existence proof: finding an element a such that $P(a)$ is true
- A nonconstructive (非构造性) existence proof:
- Example: show that there is a positive integer that can be written as the sum of cubes of two positive integers in two different ways.
  - $1729 = 10^3 + 9^3 = 12^3 + 1^3$
- Example: show that there exist irrational numbers x and y such that x^y is rational.

Chomp: A two-player game

- Cookies placed on a rectangular grid, the top left one poisoned
- Two players take turns making moves; at each move, a player eats a remaining cookie and all cookies to the right and below
- The loser is the player who has to eat the poisoned cookie
- Does one of the players has a winning strategy, that is, wins no matter what the second player does?



Chomp

- We say that a player has a winning strategy (WS) if she has a way to win no matter how the other player plays.
- How to define WS formally?
- We consider a n-round game.
- We say that P1 has a winning strategy if we have $\exists A_1 \forall B_1 \exists A_2 \forall B_2 \ldots \exists A_n \forall B_n win(P1)$
- We say that P2 has a winning strategy if we have $\forall A_1 \exists B_1 \forall A_2 \exists B_2 \ldots \forall A_n \exists B_n win(P2)$
- If there is no tie, then either P1 has a WS or P2 has a WS.

Which player has a winning strategy

- There cannot be a tie in Chomp.
- Thus either P1 has a WS or P2 has a WS.
- We show that P2 cannot have a WS.
- Hence P1 must have a WS.
- Assume to the contrary that P2 has a WS.
- Suppose P1 first chooses the bottom right cookie, then P2 must have a WS against this move.
- Then P1 can omit the first move, and use this strategy of P2 as her WS.
- Thus P1 has a WS, a contradiction to that P2 has a WS.

What's the winning strategy of Player 1

- No one has been able to describe a WS for an arbitrary grid.
- But we can describe WS for square grids or $2 * n$ grids.

Uniqueness Proofs (唯一存在性证明)

- Asserting the existence of a unique element with a certain property
- Two parts of a proof
  - Existence: show that an element x with the desired property exists
  - Uniqueness: show that if $y \neq x$, then y does not have the desired property; or show that if both x and y have the desired property, then $x = y$
- Example: show that if a and b are real numbers and $a \neq 0$, then there is a unique number r such that $ar + b = 0$.

Forward and Backward Reasoning:

- Forward reasoning:
  - used to prove relatively simple results
  - to prove $p \to q$, find a proposition r such that $p \to r$; continue this process, until we reach q
- Backward reasoning:
  - used to prove more complicated results
  - to prove $p \to q$, find a proposition r such that $r \to q$; continue this process, until we reach p
- Example:
  - two players take turns removing 1, 2, or 3 stones at a time from a pile that begins with 15 stones
  - the player who removes the last stone wins the game
  - show that the first player has a winning strategy

Adapting existing proofs

- Often an existing proof can be adapted to prove a new result
- even when this is not the case, some of the ideas used in existing proofs may be helpful
- Example: prove that $\sqrt{3}$ is irrational (无理数) by adapting the proof that $\sqrt{2}$ is irrational

Looking for counterexamples (反例)

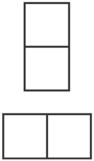
- when confronted with a conjecture, we might try to find a counterexample
- if we cannot find a counterexample, we might again try to prove the statement
- in any case, looking for counterexamples is an extremely important pursuit, which often provides insights into problems
- Example: is it the case that every positive integer is the sum of squares of two integers?
- How about three integers, four integers?

Proof Strategies

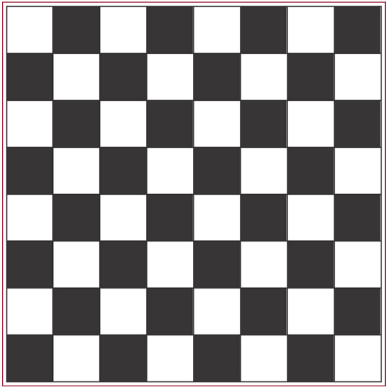
- Mathematics texts formally present theorems and their proofs
- Such presentations do not convey the discovery process in mathematics
- This process begins with exploring concepts and examples, asking questions, formulating conjectures, and attempting to settle these conjectures either by proof or by counterexample
- Conjectures are formulated based on examination of special cases, identification of possible patterns, altering the hypotheses and conclusions of existing theorems, etc.
- We now illustrate through tilings of checkerboards

Tiling terms

- A checkerboard (棋盘) is a rectangle divided into squares of the same size
- A standard checkerboard is a 8*8 checkerboard
- A domino (多米诺骨牌) is a 1*2 rectangular piece
- A board is tiled by dominos when all its squares are covered with no overlapping dominoes and no dominoes overhanging the board



Tilings



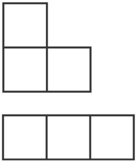
- Can we tile the standard checkerboard using dominos?
- How about removing one corner?
- How about removing two opposite corners?

A proof by contradiction

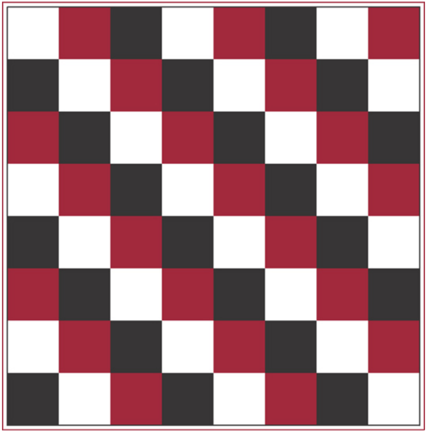
- We color the squares using alternating white and black squares
- Suppose we can use dominoes to cover the board
- Since each domino covers a black square and a white square, there are equal number of black and white squares
- However, the two removed corners have the same color

Tiling with polyominoes (多联骨牌)

- polyominoes: squares that are connected along their edges
- straight and right triominoes
- Can we tile the standard checkerboard using straight triominoes?
- Can we tile the standard checkerboard with a corner removed using straight triominoes?
  adapt the previous proof by contradiction



Tilings



The role of open problems (公开问题)

Many advances in mathematics have been made by people trying to prove famous open problems.

Fermat's last theorem (费马大定理):
The equation $x^n + y^n = z^n$ has no solutions in integers x, y, and z with $xyz \neq 0$ whenever n is an integer with $n > 2$.

- In the 17th century, Fermat jotted on the margin of a book that he had a wondrous proof; however, he never published a proof
- Mathematicians looked for a proof for 3 centuries without success
- In the 1990s, Andrew Wiles found a proof, requiring hundreds of pages of advanced mathematics, and it took him 10 years to find the proof

The $3x + 1$ conjecture

Let $T(x) = x/2$ when x is an even integer, and $T(x) = 3x + 1$ when x is an odd integer. The conjecture states that for all positive integers x, when we repeatedly apply T, we will eventually get 1.

- Example: $x = 13$
- The conjecture has been verified for all integers up to $5.6 \cdot 10^{13}$
- The conjecture has been raised many times and goes by many different names.
- Many mathematicians have been diverted from their work to attack this conjecture.