CS21201 Discrete Structures

Tutorial 3

Proof Techniques

1. The game of Nim is played by two players Alice and Bob. There are two piles with m and n sticks. The moves alternate between Alice and Bob. In each move, the player chooses one non-empty pile, and removes one or more sticks from that pile. The player who fails to make the next move loses (that is, the player who makes the last move wins). Alice makes the first move. Prove the following assertions.

(a) If $m = n$, Bob can always win.

Solution Bob imitates Alice.

(b) If $m \neq n$, Alice can always win.

Solution Alice forces Bob to the situation $m = n$.

2. Let a, b be two positive integers, and $d = \gcd(a,b) = ua + vb$ with $u, v \in \mathbb{Z}$. Prove that u and v can be so chosen that $|u| < \dfrac{b}{d}$ and $|v| \leqslant \dfrac{a}{d}$.

Solution By the extended gcd, we always have a representation of the form $1 = u(\frac{a}{d}) + v(\frac{b}{d})$ for some integers u, v. Write $u = q(\frac{b}{d}) + r$ with $0 \leqslant r < \frac{b}{d}$ (Euclidean division). We then have $1 = \Big(q(\frac{b}{d}) + r\Big)(\frac{a}{d}) + v(\frac{b}{d}) = r(\frac{a}{d}) + s(\frac{b}{d})$, where $s = v + q(\frac{a}{d})$. If $r = 0$, then $s = \frac{d}{b} \leqslant 1 \leqslant \frac{a}{d}$. If $r > 0$, then $|s| = \frac{d}{b}\Big(r(\frac{a}{d}) - 1\Big) < \Big(r(\frac{d}{b})\Big)\frac{a}{d} < \frac{a}{d}$.

3. Prove that $\forall a, b, c \in \mathbb{N}\ \Big[a|(bc) \rightarrow [(a|b) \vee (\gcd(a,c) > 1)]\Big]$.

Solution Assume that $a|(bc)$ and $\gcd(a,c) = 1$. Then, for some integers u, v, we have $1 = ua + vc$. This implies that $b = uab + vbc = (ub)a + v(bc)$ is a multiple of a.

*** 4.** Prove that $\forall a, b, c \in \mathbb{N}\ \Big[(\gcd(a,b) = 1) \rightarrow \exists x \in \mathbb{N}\ [\gcd(a + bx, c) = 1]\Big]$.

Solution Since a and b are coprime, they have different prime factors. Write

$$\begin{aligned} a &= p_1^{e_1} p_2^{e_2} \cdots p_s^{e_s}, \\ b &= q_1^{f_1} q_2^{f_2} \cdots q_t^{f_t}, \end{aligned}$$

with e_i and f_j positive. Now, consider the prime factorization of c

$$c = p_1^{u_1} p_2^{u_2} \cdots p_s^{u_s} q_1^{v_1} q_2^{v_2} \cdots q_t^{v_t} r_1^{w_1} r_2^{w_2} \cdots r_l^{w_l},$$

where u_i and v_j are non-negative, $l \geqslant 0$, and r_k are primes different from all p_i and q_j. Take $x = r_1^{w_1} r_2^{w_2} \cdots r_l^{w_l}$.

5. Let $S \subseteq \mathbb{N}_0 \times \mathbb{N}_0$. It is given that $(0,0) \in S$, and also that whenever $(m,n) \in S$, we have $(m+1, n) \in S$ and $(m, n+1) \in S$. Prove that $S = \mathbb{N}_0 \times \mathbb{N}_0$.

Solution [Proof using well-ordering] Suppose that $S \neq \mathbb{N}_0 \times \mathbb{N}_0$. Then there exists $(a,b) \in \mathbb{N}_0 \times \mathbb{N}_0 - S$. Pick such a pair (a,b) such that a is as small as possible, and b is also as small as possible for the given a. By the well-ordering principle, a and b exist. Since $(0,0) \in S$, we cannot have $a = b = 0$, that is, either a or b is positive (or both are). This means that either $(a-1, b)$ or $(a, b-1)$ is in $\mathbb{N}_0 \times \mathbb{N}_0$. By the choice of a and b, this pair is not in S, so by the given condition, $(a,b) \in S$, a contradiction.

[Proof using induction] Since $(0,0) \in S$ and $(m,0) \in S \rightarrow (m+1, 0) \in S$ for all $m \geqslant 0$, we have $(m,0) \in S$ for all $m \geqslant 0$. Now, take any fixed A. We have $(m,0) \in S$ and $(m,n) \in S \rightarrow (m, n+1) \in S$, so it again follows by induction $(m,n) \in S$ for all $n \geqslant 0$. Since m was chosen arbitrarily in the second induction argument, the result follows.

6. What is wrong with the following proof by induction?

Theorem: All horses are of the same color.

Proof Let there be n horses. We proceed by induction on n. If $n = 1$, there is nothing to prove. So assume that $n > 1$, and that the theorem holds for any group of $n-1$ horses. From the given n horses discard one, say the first one. Then, all the remaining $n-1$ horses are of the same color by the induction hypothesis. Now, put the first horse back, and discard another, say the last one. Then, the first $n-1$ horses have the same color, again by the induction hypothesis. So all the n horses must have the same color as the ones that were not discarded either time.

Solution The argument does not hold for $n = 2$.

7. Let F_n denote the n-th Fibonacci number.

(a) Prove that for all integers m, n with $m \geqslant 1$ and $n \geqslant 0$, we have $F_{m+n} = F_m F_{n+1} + F_{m-1} F_n$.

Solution You may use induction on m or n for $m+n$.

Proof using induction on m: For $m = 1$, we have $F_{n+1} = F_1 F_{n+1} + F_0 F_n$. For $m = 2$, we have $F_{n+2} = F_{n+1} + F_n = F_2 F_{n+1} + F_1 F_n$. So suppose that the statement is true for some m and $m+1$ (and for all n). That is,

$$\begin{aligned} F_{m+n} &= F_m F_{n+1} + F_{m-1} F_n, \\ F_{m+1+n} &= F_{m+1} F_{n+1} + F_m F_n. \end{aligned}$$

Adding these two equations gives

$$F_{m+2+n} = F_{m+1+n} + F_{m+n} = (F_{m+1} + F_m) F_{n+1} + (F_m + F_{m-1}) F_n = F_{m+2} F_{n+1} + F_{m+1} F_n.$$

(b) Let $m, n \in \mathbb{N}$. Prove that if $m|n$, then $F_m|F_n$.

Solution Write $n = qm$. Proceed by induction on q. For $q = 1$, the statement is obviously true. So suppose that $F_m|F_{qm}$. We have $F_{(q+1)m} = F_{m+qm} = F_m F_{qm+1} + F_{m-1} F_{qm}$ by Part (a). Since $F_m F_{qm+1}$ is a multiple of F_m, and $F_{m-1} F_{qm}$ too is a multiple of F_m, it follows that $F_{(q+1)m}$ is a multiple of F_m.

(c) What about the converse of Part (b)?

Solution False. Take $m = 2$ and $n = 3$.

8. Using mathematical induction, prove that $2^n < n! < 2^{n \log_2 n}$ for all $n \geqslant 4$.

Solution [Induction basis] For $n = 4$, we have $2^4 = 16 < 4! = 24 < 2^{4 \log_2 4} = 256$.

[Induction] Suppose that $2^n < n! < 2^{n \log_2 n}$ for some $n \geqslant 4$. We then have

$$(n+1)! = (n+1) \times n! > (n+1) \times 2^n > 2 \times 2^n = 2^{n+1},$$

and

$$(n+1)! = (n+1) \times n! < (n+1) \times 2^{n \log_2 n} = (n+1) \times n^n <= (n+1)^{n+1} = 2^{(n+1) \log_2 (n+1)}.$$

9. The following function takes integer inputs $m, n \geqslant 0$. Determine the value of $g(2, n)$ as a function of n.

```
int g ( int m, int n )
{
   if ( (m == 0) || (n == 0) ) return 1;
   return g(m,n-1) + g(m-1,n);
}
```

Solution We have $g(0, n) = 1$ for all $n \geqslant 0$. For $m = 1$, we have $g(1, 0) = 1$, and $g(1, n) = g(1, n-1) + g(0, n) = g(1, n-1) + 1$ for $n \geqslant 1$. Repeatedly using this identity gives $g(1, n) = 1 + g(1, n-1) = 2 + g(1, n-2) = \cdots = n + g(1, 0) = n + 1$. Finally, we have $g(2, n) = g(1, n) + g(2, n-1) = (n+1) + g(2, n-1) = (n+1) + n + g(2, n-2) = \cdots = (n+1) + n + (n-1) + \cdots + 2 + g(2, 0) = (n+1) + n + (n-1) + \cdots + 2 + 1 = \frac{(n+1)(n+2)}{2}$.

10. Let x be a non-zero real number such that $x + \dfrac{1}{x}$ is an integer. Prove by induction on n that $x^n + \dfrac{1}{x^n}$ is an integer for all $n \geqslant 1$.

Solution [Basis] For $n = 1$, the statement is obvious (it is a part of the hypothesis). For $n = 2$, we use the fact that $\left(x+\frac{1}{x}\right)^2 = x^2+\frac{1}{x^2}+2$ is an integer, so $x^2+\frac{1}{x^2}$ is an integer too.

[Induction] Take $n \geqslant 3$, and assume that $x^{n-1}+\frac{1}{x^{n-1}}$ and $x^{n-2}+\frac{1}{x^{n-2}}$ are integers. But then, we see that

$$x^n+\frac{1}{x^n} = \left(x^n+\frac{1}{x^n}+x^{n-2}+\frac{1}{x^{n-2}}\right)-\left(x^{n-2}+\frac{1}{x^{n-2}}\right) = \left(x^{n-1}+\frac{1}{x^{n-1}}\right)\left(x+\frac{1}{x}\right)-\left(x^{n-2}+\frac{1}{x^{n-2}}\right)$$

is an integer too.

Additional Exercises

11. Prove that $\sqrt{p}$ is irrational for any prime p.

12. Let $n \in \mathbb{N}$. Prove that $\sqrt{n}$ is irrational if and only if n is not a perfect square.

13. Prove the equivalence of the following.

- **(a)** The well-ordering principle of $\mathbb{N}$ (or $\mathbb{N}_0$).
- **(b)** The principle of weak induction.
- **(c)** The principle of the special case of induction.
- **(d)** The principle of strong induction.

14. What is wrong with the following proof by strong induction?

Theorem: $2^n = 1$ for all integers $n \geqslant 0$.

Proof [Basis] For $n = 0$, this is true.

[Induction] Suppose the result holds for $0, 1, 2, \ldots, n-1$. Then, $2^n = 2^1 \times 2^{n-1} = 1 \times 1 = 1$.

15. A finite continued fraction is an expression of the form

$$a_1+\cfrac{1}{a_2+\cfrac{1}{a_3+\cfrac{1}{\ddots+\cfrac{1}{a_n}}}}$$

with $a_1 \in \mathbb{Z}$, and $a_2, a_3, \ldots, a_n \in \mathbb{N}$. Prove that every rational number a/b with $a \in \mathbb{Z}$ and $b \in \mathbb{N}$ has a finite continued fraction.

16. Using the principle of mathematical induction, prove the following statements.

- **(a)** For all $n \geqslant 4$, the n-th Catalan number satisfies $C_n \leqslant 2^{2n-4}$.
- **(b)** The harmonic numbers $H_n = \frac{1}{1}+\frac{1}{2}+\cdots+\frac{1}{n}$ satisfy $\ln(n+1) \leqslant H_n \leqslant \ln n+1$ for all $n \geqslant 1$.

17. Let $T(n)$ denote the number of disk movements performed by the following recursive algorithm for solving the three-peg Tower-of-Hanoi problem.

```
/* Move n disks from Peg A to Peg B using the auxiliary Peg C */
ToH ( n, A, B, C )
{
   if (n == 1) move the only disk from Peg A to Peg B.
   else {
      ToH(n-1,A,C,B);
      Move the largest disk from Peg A to Peg B.
      ToH(n-1,C,B,A);
   }
}
```

(a) Prove that $T(n) = 2^n - 1$.

(b) Prove that no algorithm can solve the problem in less than these many moves.

18. Prove the following assertions about Fibonacci numbers F_n, $n \geqslant 0$.

(a) $\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}^n = \begin{pmatrix} F_{n+1} & F_n \\ F_n & F_{n-1} \end{pmatrix}$ for all $n \geqslant 1$.

(b) $\sum_{i=1}^{n} F_i = F_{n+2} - 1$ for all $n \geqslant 1$.

(c) $\sum_{i=0}^{n-1} F_{2i+1} = F_{2n}$ for all $n \geqslant 1$.

(d) $\sum_{i=1}^{n} F_{2i} = F_{2n+1} - 1$ for all $n \geqslant 1$.

(e) For all $n \geqslant 1$, $\gcd(F_n, F_{n+1}) = \gcd(F_n, F_{n+2}) = \gcd(F_{n+1}, F_{n+2}) = 1$. (That is, any three consecutive Fibonacci numbers are coprime to one another.)

(f) $\gcd(F_m, F_n) = F_{\gcd(m,n)}$ for all $m, n \geqslant 1$.

19. [*Negatively indexed Fibonacci numbers*] For $n \geqslant 1$, inductively define $F_{-n} = F_{-n+2} - F_{-n+1}$. Prove that $F_{-n} = (-1)^{n+1} F_n$ for all $n \geqslant 1$.

20. What does the following function return for integer inputs $m, n \geqslant 0$?

```
int f ( int m, int n )
{
   if ( (m == 0) || (n == 0) ) return 1;
   return f(m,n-1) + f(m-1,n) - 1;
}
```

21. What does the following function return on input n? Also argue that the function terminates for $n \geqslant 1$.

```
int h ( int n )
{
   if (n <= 0) return -1;      /* Error condition */
   if (n % 2 == 1) return 0;   /* n is odd */
   return 1 + h(n*(n+1)/2);    /* n is even */
}
```

22. Consider the following recursive function.

```
int F ( int n, int i, int s, int t )
{
   if (i == n) return s * (n - 1) + 1;
   return F (n, i + 1, s + t, t * n);
}
```

You call `F(n,0,0,1)` from `main()` for a positive integer n. What does the call return as a function of n?

Hard Exercises

**** 23.** [*Frobenius coin problem*] You have coins of two integral denominations $a, b > 1$ with $\gcd(a, b) = 1$. Prove that any integer amount $n \geqslant (a-1)(b-1)$ can be changed by coins of these two denominations.

*** 24.** Let a, b be as in the last exercise. Prove that the amount $(a-1)(b-1) - 1$ cannot be changed by coins of denominations a and b.