CS21201 Discrete Structures
Tutorial 3

Proof Techniques and Induction

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 $1 = \left(q(\frac{b}{d}) + r\right)(\frac{a}{d}) + v(\frac{b}{d}) = r(\frac{a}{d}) + s(\frac{b}{d})$, 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 $|s| = \frac{d}{b}\left(r(\frac{a}{d}) - 1\right) < \left(r(\frac{d}{b})\right)\frac{a}{d} < \frac{a}{d}$.

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

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 $\forall a, b, c \in \mathbb{N} \left[(\gcd(a, b) = 1) \rightarrow \exists x \in \mathbb{N} \left[\gcd(a + bx, c) = 1 \right] \right]$.

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 $m \mid n$, then $F_m \mid F_n$.

Solution Write $n = qm$. Proceed by induction on q. For $q = 1$, the statement is obviously true. So suppose that $F_m \mid F_{qm}$. 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 $\left(x + \dfrac{1}{x}\right)^2 = x^2 + \dfrac{1}{x^2} + 2$ is an integer, so $x^2 + \dfrac{1}{x^2}$ is an integer too.

[Induction] Take $n \geqslant 3$, and assume that $x^{n-1} + \dfrac{1}{x^{n-1}}$ and $x^{n-2} + \dfrac{1}{x^{n-2}}$ 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.

11. All the integers in the sequence 2021, 20821, 208821, 2088821, 20888821, … (with any non-negative number of occurrences of the digit 8 between 20 and 21) are divisible by a common prime p. Find p, and prove the assertion.

Solution The n-th integer in the sequence is $a_n = 208^n21$, where 8^n is the n-fold repetition of the digit 8. We show by induction on n that a_n is divisible by 47 for all $n \geqslant 0$.

[Basis] $a_0 = 2021 = 2025 - 4 = 45^2 - 2^2 = (45 - 2)(45 + 2) = 43 \times 47$.

[Induction] Suppose that a_n is divisible by 47. We have

$$\begin{aligned} a_{n+1} &= 20888\ldots821, \\ a_n &= 2088\ldots821, \\ a_{n+1} - a_n &= 18800\ldots000. \end{aligned}$$

Since $188 = 47 \times 4$, the inductive step is established. (Also note that $a_{n+1} - a_n$ is not divisible by 43.)

12. Let $H_n = \dfrac{1}{1} + \dfrac{1}{2} + \dfrac{1}{3} + \cdots + \dfrac{1}{n}$ denote the n-th harmonic number. By induction on n, prove that $H_n \leqslant 1 + \ln n$ for all $n \geqslant 1$.

Solution [Base] For $n = 1$, we have $H_1 = 1 \leqslant 1 + 0 = 1 + \ln 1$.

[Induction] Take $n \geqslant 1$, and assume that $H_n \leqslant 1 + \ln n$. Then we have

$$\begin{aligned} H_{n+1} &= H_n + \frac{1}{n+1} \\ &\leqslant 1 + \ln n + \frac{1}{n+1} \\ &= 1 + \ln(n+1) + \frac{1}{n+1} + (\ln n - \ln(n+1)) \\ &= 1 + \ln(n+1) + \frac{1}{n+1} + \ln\left(\frac{n}{n+1}\right) \\ &= 1 + \ln(n+1) + \frac{1}{n+1} + \ln\left(1 - \frac{1}{n+1}\right) \\ &= 1 + \ln(n+1) + \frac{1}{n+1} - \frac{1}{n+1} - \frac{1}{2}\left(\frac{1}{n+1}\right)^2 - \frac{1}{3}\left(\frac{1}{n+1}\right)^3 - \frac{1}{4}\left(\frac{1}{n+1}\right)^4 - \cdots \\ &= 1 + \ln(n+1) - \left[\frac{1}{2}\left(\frac{1}{n+1}\right)^2 + \frac{1}{3}\left(\frac{1}{n+1}\right)^3 + \frac{1}{4}\left(\frac{1}{n+1}\right)^4 + \cdots\right] \\ &\leqslant 1 + \ln(n+1). \end{aligned}$$

Since $n \geqslant 1$, we have $0 < \dfrac{1}{n+1} \leqslant \dfrac{1}{2} < 1$, and so we can use the above expansion of $\ln\left(1 - \dfrac{1}{n+1}\right)$.

13. Specify the return value $W(n)$ of the following function as a closed-form expression in its input n (a non-negative integer). Prove your assertion. Assume the availability of a function `binomial(n,k)` that returns the floating-point value of the binomial coefficient $C(n,k) = \binom{n}{k}$. **(5)**

```c
int W ( unsigned int n )
{
    double sum = 0, denominator = 1;
    int k;

    for (k=0; k<=n; ++k) {
        sum += binomial(n+k,k) / denominator;
        denominator *= 2;
    }
    return round(sum);
}
```

Solution We prove by induction on n that for all $n \geqslant 0$, we have

$$W(n) = \sum_{k=0}^{n}\left[\binom{n+k}{k}\frac{1}{2^k}\right] = 2^n.$$

[Basis] For $n = 0$, we have $W(0) = \binom{0}{0} = 1 = 2^0$.

[Induction] Assume that $n \geqslant 0$, and that $W(n) = 2^n$. By Pascal's identity, we have:

$$
\begin{aligned}
W(n+1) &= \sum_{k=0}^{n+1}\left[\binom{n+1+k}{k}\frac{1}{2^k}\right] \\
&= \sum_{k=0}^{n+1}\left[\binom{n+k}{k}+\binom{n+k}{k-1}\right]\frac{1}{2^k} \\
&= \sum_{k=0}^{n}\left[\binom{n+k}{k}\frac{1}{2^k}\right] + \binom{n+n+1}{n+1}\frac{1}{2^{n+1}} + \sum_{k=1}^{n+1}\left[\binom{n+k}{k-1}\frac{1}{2^k}\right]+\binom{n}{-1} \\
&= W(n) + \binom{2n+1}{n+1}\frac{1}{2^{n+1}} + \frac{1}{2}\sum_{k=0}^{n}\left[\binom{n+1+k}{k}\frac{1}{2^k}\right],
\end{aligned}
$$

where the last equality follows from replacing $k-1$ by k in the second sum. Now,

$$\binom{2n+1}{n+1} = \frac{(2n+1)!}{(n+1)!\,n!} = \frac{1}{2}\left[\frac{(2n+2)!}{(n+1)!\,(n+1)!}\right] = \frac{1}{2}\binom{2n+2}{n+1} = \frac{1}{2}\binom{n+1+n+1}{n+1},$$

that is,

$$
\begin{aligned}
W(n+1) &= W(n) + \frac{1}{2}\sum_{k=0}^{n+1}\left[\binom{n+1+k}{k}\frac{1}{2^k}\right] \\
&= W(n) + \frac{1}{2}W(n+1),
\end{aligned}
$$

that is,

$$W(n+1) = 2W(n) = 2^{n+1}.$$

Additional Exercises

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

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

16. 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 generalized form of weak induction.

(d) The principle of strong induction.

17. 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, $2^n = 2^1 \times 2^{n-1} = 1 \times 1 = 1$.

18. 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.

19. 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 $n \geqslant 1$.

20. 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.

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

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

(d) $\displaystyle\sum_{i=1}^{n} F_{2i} = F_{2n+1} - 1$ 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 $m, n \geqslant 1$.

22. [*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 $n \geqslant 1$.

23. 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;
}
```

24. 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 */
}
```

25. 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?