

# Lab00-Proof

CS214-Algorithm and Complexity, Xiaofeng Gao, Spring 2021.

\* If there is any problem, please contact TA Haolin Zhou.

\* Name: Log Creative Student ID: Email: logcreative-lzl@sjtu.edu.cn

1. Prove that for any integer  $n > 2$ , there is a prime  $p$  satisfying  $n < p < n!$ . (Hint: consider a prime factor  $p$  of  $n! - 1$  and prove by contradiction)

**Proof.** Since  $n > 2$ ,

$$n! > n! - 1 > 2n - 1 > 2n - n = n > 2$$

Then there exists a prime factor  $p$  for the positive integer  $n! - 1$ . We consider this prime factor  $p \leq n! - 1 < n!$  and prove it to be the specified prime satisfying  $p > n$  as well.

**Prove by contradiction.** Assume the constructed prime  $p \leq n$ . As  $n! = \prod_{i=1}^n i$  contains all the integer factors less than or equal to  $n$ ,

$$p \mid n!$$

However, it is constructed that

$$p \nmid n! - 1$$

so that

$$p = 1$$

because  $-1 \not\equiv 0 \pmod{p} \Rightarrow n! - 1 \not\equiv n! \pmod{p}$  when  $p > 1$ . This contradicts the fact that  $p$  is a prime and the assumption does not hold.

As a result, The requested prime  $p$  satisfying  $n < p < n!$  is found and the proposition holds.  $\square$

2. Use the minimal counterexample principle to prove that for any integer  $n \geq 7$ , there exists integers  $i_n \geq 0$  and  $j_n \geq 0$ , such that  $n = i_n \times 2 + j_n \times 3$ .

**Proof. Construct the minimal counterexample set.** It is to be proved that  $\emptyset = S \subset A = \{n \in \mathbb{N} \mid n \geq 7\}$  of the numbers  $n \in A$  for which  $\forall i \geq 0, j \geq 0, n \neq i \times 2 + j \times 3$ . **Prove by contradiction.** Assume  $S \neq \emptyset$ , then  $S$  has a least element followed by well-ordering principle. Let  $m \in S$  be the least element.

It is observed that  $7 = 2 \times 2 + 1 \times 3, 8 = 4 \times 2, 9 = 3 \times 3$ , which results in  $m \geq 9$ . Consider the number  $m - 2 \geq 7$ . If  $m - 2 \notin S, \exists i_{m-2}, j_{m-2} \in \mathbb{N}$  such that

$$m - 2 = i_{m-2} \times 2 + j_{m-2} \times 3$$

which leads to

$$m = (i_{m-2} + 1) \times 2 + j_{m-2} \times 3$$

and let  $i_m \leftarrow i_{m-2} + 1, j_m \leftarrow j_{m-2}$  so that  $i_m, j_m \in \mathbb{N}$  are constructed to satisfy  $m = i_m \times 2 + j_m \times 3$ , i.e.,  $m \notin S$ , which could not be true as  $m$  is the element in  $S$  as provided.

Then,  $m - 2 \in S$ . However,  $7 \leq m - 2 < m$  contradicts  $m$  is the least number in  $S$ . So the assumption fails to hold and  $S = \emptyset$ .  $\square$

3. Suppose the function  $f$  be defined on the natural numbers recursively as follows:  $f(0) = 0, f(1) = 1$ , and  $f(n) = 5f(n-1) - 6f(n-2)$ , for  $n \geq 2$ . Use the strong principle of mathematical induction to prove that for all  $n \in \mathbb{N}, f(n) = 3^n - 2^n$ .

**Proof. Prove by strong principle of mathematical induction.** To show that  $n \in \mathbb{N}$ ,  $P(n) : f(n) = 3^n - 2^n$  holds.

**Basic step.** As defined,

$$\begin{aligned} f(0) &= 0 = 3^0 - 2^0 \\ f(1) &= 1 = 3^1 - 2^1 \end{aligned}$$

leads to  $P(0)$  and  $P(1)$  are correct.

**Induction hypothesis.**  $k \geq 2$ , and  $P(n)$  holds for every  $0 \leq n \leq k$ .

**Statements to be shown in induction step.**  $P(k+1)$  holds.

**Proof of induction step.** As it is defined that  $f(n) = 5f(n-1) - 6f(n-2)$  for  $n \geq 2$ ,

$$\begin{aligned} f(k+1) &= 5f(k) - 6f(k-1) \\ &= 5(3^k - 2^k) - 6(3^{k-1} - 2^{k-1}) \\ &= (15 - 6) \times 3^{k-1} - (10 - 6) \times 2^{k-1} \\ &= 3^{k+1} - 2^{k+1} \end{aligned}$$

Therefore,  $P(k+1)$  holds.

By the strong principle of mathematical induction,  $\forall n \in \mathbb{N}$ ,  $f(n) = 3^n - 2^n$ . □

4. An  $n$ -team basketball tournament consists of some set of  $n \geq 2$  teams. Team  $p$  beats team  $q$  iff  $q$  does not beat  $p$ , for all teams  $p \neq q$ . A sequence of distinct teams  $p_1, p_2, \dots, p_k$ , such that team  $p_i$  beats team  $p_{i+1}$  for  $1 \leq i < k$  is called a ranking of these teams. If also team  $p_k$  beats team  $p_1$ , the ranking is called a  $k$ -cycle.

Prove by mathematical induction that in every tournament, either there is a *champion* team that beats every other team, or there is a 3-cycle.

**Proof.**

**Definition 1** (beat). Denote  $p \leftarrow q$  iff  $p$  beats team  $q$ ; denote  $q \rightarrow p$  iff  $q$  does not beat  $p$ .

**Lemma 1** (ranking). There is always a ranking  $p_1, p_2, \dots, p_n$  for  $n$ -team tournament, where  $n \geq 2$ .

**Proof of Lemma 1.** Construct the ranking sequence by **mathematical induction** and inserting. To show that  $n \in \{n \in \mathbb{N} \mid n \geq 2\}$ , it is correct that  $Q(n)$  : there is always a ranking for the  $n$ -team.

**Basic step.** When  $n = 2$ ,

$$\begin{array}{ll} p_1 \leftarrow p_2 & p_1, p_2 \text{ is a ranking} \\ \text{or } p_2 \leftarrow p_1 & p_2, p_1 \text{ is a ranking} \end{array}$$

which shows  $Q(2)$  holds.

**Induction hypothesis.**  $k \geq 3$ ,  $Q(k)$  holds.

**Statements to be shown in induction step.**  $Q(k+1)$  holds.

**Proof of induction step.** Consider inserting  $p_{k+1}$  into the remaining  $k$ -team ranking  $p_1 \leftarrow p_2 \leftarrow \cdots \leftarrow p_k$ . Begin inserting from  $p_1$ , if  $p_{k+1} \leftarrow p_1$ , then  $p_{k+1} \leftarrow p_1 \leftarrow p_2 \leftarrow \cdots \leftarrow p_k$  is the new ranking. Otherwise  $p_1 \leftarrow p_{k+1}$ , compare  $p_2$  with  $p_{k+1}$ , if  $p_{k+1} \leftarrow p_2$ , then  $p_1 \leftarrow p_{k+1} \leftarrow p_2 \leftarrow \cdots \leftarrow p_k$  is the new ranking and so on. The inserting algorithm could be interpreted as follows:

---

**Algorithm 1:** Construct New Ranking by Inserting

---

**Input:** A  $k$ -team ranking  $p_1, p_2, \dots, p_k$ , a new team  $p_{k+1}$

**Output:** New  $(k + 1)$ -team ranking

```

1 if  $p_{k+1} \leftarrow p_1$  then
2   return  $p_{k+1} \leftarrow p_1 \leftarrow p_2 \leftarrow \cdots \leftarrow p_k$ ;
3 for  $i = 2$  to  $k$  do
4   if  $p_{k+1} \leftarrow p_i$  then
5     return  $p_1 \leftarrow \cdots \leftarrow p_{i-1} \leftarrow p_{k+1} \leftarrow p_i \leftarrow \cdots \leftarrow p_k$ ;
6 return  $p_1 \leftarrow p_2 \leftarrow \cdots \leftarrow p_k \leftarrow p_{k+1}$ ;

```

---

By such, we construct the new ranking and  $Q(k + 1)$  holds.

By the principle of mathematical induction, the Lemma 1 holds. □

**Lemma 2** (champion). *If there is a champion team among the ranking  $p_1 \leftarrow p_2 \leftarrow \cdots \leftarrow p_n$ , the champion team must be the head one, namely  $p_1$ .*

**Proof of Lemma 2. Prove by contradiction.** Assume the *champion* team is  $p_i$  other than  $p_1$ , i.e.,  $2 \leq i \leq k$ . Then there always exists a no-beating senario:

$$p_{i-1} \leftarrow p_i$$

which contradicts the definition of beating. The assumption fails to hold and the Lemma 2 is correct. □

Back to the original problem. According to Lemma 1, there always exists a ranking for  $n$ -team tournament:

$$p_1 \leftarrow p_2 \leftarrow \cdots \leftarrow p_n$$

**Case 1: A *champion* team.** If there is a *champion* team, it must be  $p_1$  according to Lemma 2.

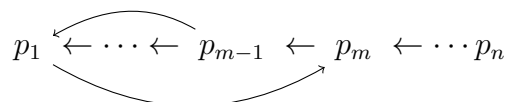
**Case 2: A 3-cycle.** Otherwise, no one could be the champion, which indicates that there exists  $p_m$  such that

$$p_1 \rightarrow p_m$$

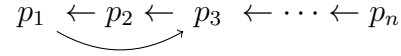
where  $3 \leq m \leq n$  because if  $m = 2$ , the following statements are contradictory:

$$\begin{array}{ll}
 p_1 \rightarrow p_2 & \text{(assumption)} \\
 p_1 \leftarrow p_2 & \text{(ranking)}
 \end{array}$$

By recusively investigating  $p_{m-1}$ , a 3-cycle could be constructed. If  $p_{m-1} \rightarrow p_1$ , then there is a 3-cycle  $p_1, p_{m-1}, p_m$  shown as follows:



Otherwise, investigate  $p_{m-2}$  and attempt to construct the 3-cycle  $p_{m-2}, p_{m-1}, p_1$ . Until  $p_3$  is under investigating and now  $p_1, p_2, p_3$  must be a 3-cycle.

$$p_1 \leftarrow p_2 \leftarrow p_3 \leftarrow \cdots \leftarrow p_n$$


The procedure above could be summarized by the following algorithm.

---

**Algorithm 2:** Construct 3-cycle by Shrinking the Range

---

**Input:** A  $k$ -team ranking  $p_1, p_2, \dots, p_k$ , a winner  $p_m$  that  $p_1 \rightarrow p_m$

**Output:** A 3-cycle

```

1 for  $j = m$  to 3 do
2   if  $p_{j-1} \rightarrow p_1$  then
3     return  $p_1, p_{j-1}, p_j$ ;
4 return  $p_1, p_2, p_3$ ;

```

---

As a result, there must be a 3-cycle in this case.

□

**Remark:** You need to include your .pdf and .tex files in your uploaded .rar or .zip file.