Lecture 3-4: Proof methods

Main points:

- **direct proof / direct calculation**
- **proof by contradiction**: infinitely many primes, irrationality of $\sqrt{2}$, e^n, and π

  implication: the impossibility of sqaring a circle
- **case analysis**: Ramsey number $R(3,3)$, $R(p,q)$ (induction)

  phenomenon: Ramsey theory (mathematical "emergence" phenomenon): sufficiently large population contains structures.
- **variants of induction:** weak and strong induction, simultaneous induction, structure induction (important for analyzing non-number discrete structures)

1 direct proofs

Ex: prove if a is an even number, then a^2 is also an even number.

2 proof by contradiction

Ex: prove if a^2 is even, then a is even.
classical simple examples:
(1) $\sqrt{2}$ is not a rational number.
(2) infinitely many primes.

2.1 The irrationality of e and more

Let's consider e. Recall by Calculus we have

$$e^x = \sum_{i=0}^{\infty} \frac{x^i}{i!} = 1 + x + \frac{x^2}{2!} + \frac{x^3}{3!} + \cdots \tag{1}$$

We will prove that: $e, e^2, e^3, \ldots$ are all irrational numbers!

2.1.1 Warm up: e is irrational

We know that e has some approximate value between 2 and 3. But is it a rational number? It seems it is not. But how to prove it rigourously?

Theorem 1. *e is a irrational number.*

Proof. We again use proof by contradiction. Assume for the sake of a contradiction that $e = p/q \in \mathbb{Q}$. Since e is not an integer (why?), we have $q \neq 1$, hence, $q \geq 2$. By $e = p/q$, we have

$$\frac{p}{q} = 1 + 1 + \frac{1}{2!} + \frac{1}{3!} + \cdots$$

Let's multiply both sides by $q!$. We will get

$$(q-1)!p = k + q! \sum_{n \geq q+1} \frac{1}{n!}$$

for some integer $k \in \mathbb{Z}$. This implies $q! \sum_{n \geq q+1} \frac{1}{n!}$ is also an integer. However, if we write it down, we have

$$\begin{aligned} q! \sum_{n \geq q+1} \frac{1}{n!} &= \frac{1}{q+1} + \frac{1}{(q+1)(q+2)} + \frac{1}{(q+1)(q+2)(q+3)} + ... \\ &< \frac{1}{q+1} + \frac{1}{(q+1)(q+2)} + \frac{1}{(q+2)(q+3)} + \frac{1}{(q+3)(q+4)} + ... \\ &= \frac{1}{q+1} + \frac{1}{q+1} - \frac{1}{q+2} + \frac{1}{q+2} - \frac{1}{q+3} + \frac{1}{q+3} - \frac{1}{q+4} + ... \\ &= \frac{2}{q+1} \leq \frac{2}{3} < 1. \end{aligned}$$

This is a contradiction. □

2.1.2 Many (but simple) lemmas

Next, let's do a larger project. Let's start with a series of simpler observations, whose proofs are left as homework (you can use direct proof method to prove all of these).

Lemma 2. $\sum_{i=k+1}^{\infty} \frac{k! x^i}{i!} \leq x^k e^x$.

Lemma 3. *If $a > b$, then $(a-b)! \mid \frac{a!}{b!}$.*

Now, let's consider the following function. For some very large prime number p, consider the function

$$f(x) = x^{p-1}(x-n)^p, \tag{2}$$

which is a polynomial of variable x. Note that the highest degree is $2p-1$, and lowest degree $p-1$. So, let's write down the expansion of f,

$$f(x) = \sum_{p-1 \leq k \leq 2p-1} c_k x^k, \tag{3}$$

for some coefficients c_k.

We can give the following properties of c_k and f.

Lemma 4. *(1) c_k are integers;*

(2) $|c_{p-1}| = n^p$

(3) $\sum_{p-1\le k\le 2p-1} |c_k| = (n+1)^p$.

(4) For every $0 \le j \le p-1$, $f^{(j)}(n) = 0$.

Proof is left as homework.

We need some final preparation work. We use the following notation to simplify the formulas. Write

$$E(x,m) = \sum_{i=0}^{m} \frac{x^i}{i!} = 1 + x + \frac{x^2}{2!} + \cdots + \frac{x^m}{m!}, \tag{4}$$

which is simply the first m terms of e^x. For example, we can write $e^x = E(x,\infty)$. With this notaion, given any two parameters $k \ge p$, we can write,

$$e^x = E(x,k-p) + E(x,k) - E(x,k-p) + E(x,\infty) - E(x,k). \tag{5}$$

Lemma 5. $\sum_{p-1\le k\le 2p-1} c_k k! \Big(E(n,k) - E(n,k-p)\Big) = 0$.

This looks very complicated, but it is only some simple direct calculation, which is to say, we are still using the "direct proof" method.

Proof. By Lemma 4-(4), we have $\sum_{j=0}^{p-1} f^{(j)}(n) = 0$. We can expand this as follows, by (3),

$$f^{(j)}(x) = \sum_{p-1\le k\le 2p-1} c_k \frac{k!}{(k-j)!} x^{k-j}.$$

Hence,

$$\begin{aligned}
0 = \sum_{j=0}^{p-1} f^{(j)}(n) &= \sum_{j=0}^{p-1} \Big(\sum_{p-1\le k\le 2p-1} c_k \frac{k!}{(k-j)!} n^{k-j} \Big) \\
&= \sum_{p-1\le k\le 2p-1} c_k \cdot k! \cdot \Big(\sum_{j=0}^{p-1} \frac{n^{k-j}}{(k-j)!} \Big) \\
&= \sum_{p-1\le k\le 2p-1} c_k \cdot k! \cdot \Big(\sum_{i=k-p+1}^{k} \frac{n^i}{i!} \Big) \\
&= \sum_{p-1\le k\le 2p-1} c_k \cdot k! \cdot \Big(E(n,k) - E(n,k-p) \Big).
\end{aligned}$$

□

2.1.3 A big theorem

Theorem 6. *e^n is irrational for every integer $n \ge 1$.*

Proof of Theorem 6. Write $C = \sum_{p-1\le k\le 2p-1} c_k k!$, since c_k are all integers, and $k \ge p-1$, we know that C is also an integer, and furthermore,

$$(p-1)! \mid C. \tag{6}$$

Let's consider $C \cdot e^n$. Using (5), and apply Lemma 5, we can expand it as follows,

$$\begin{aligned} C \cdot e^n &= \sum_{p-1 \le k \le 2p-1} c_k k! \Big(E(n, k-p) + E(n,k) - E(n,k-p) + E(n,\infty) - E(n,k). \Big) \\ &= \sum_{p-1 \le k \le 2p-1} c_k k! E(n,k-p) + \sum_{p-1 \le k \le 2p-1} c_k k! \Big(E(n,\infty) - E(n,k). \Big) \\ &= X + Y, \end{aligned}$$

where X and Y denote the first and the second terms in the sum, respectively.

Firstly, let's consider X. Expand it, we have

$$X = \sum_{p-1 \le k \le 2p-1} c_k k! \sum_{i=0}^{k-p} \frac{n^i}{i!} = \sum_{p-1 \le k \le 2p-1} c_k \sum_{i=0}^{k-p} \frac{k!}{i!} n^i$$

By Lemma 3, we know that $(k-i)! \mid \frac{k!}{i!}$. Since $0 \le i \le k-p$, we have $k - i \ge p$. This implies that

$$p! \mid \frac{k!}{i!} \Longrightarrow p! \mid X. \tag{7}$$

In particular, X is an integer.

Next, let's consider Y. Again, expand it, and apply Lemma 2 and Lemma 4, we have

$$\begin{aligned} |Y| = \left| \sum_{p-1 \le k \le 2p-1} c_k k! \sum_{i=k+1}^{\infty} \frac{n^i}{i!} \right| &\le \sum_{p-1 \le k \le 2p-1} |c_k| \cdot \left| \sum_{i=k+1}^{\infty} \frac{k! n^i}{i!} \right| \\ &\le \sum_{p-1 \le k \le 2p-1} |c_k| \cdot n^k e^n \\ &\le e^n n^{2p-1} \sum_{p-1 \le k \le 2p-1} |c_k| \\ &\le e^n n^{2p-1} (n+1)^p \end{aligned} \tag{8}$$

Now, let's use the proof of contradiction method. Assume for the sake of a contradiction that e^n is a rational number. So, there are integers r, s such that $e^n = r/s$. By the equation $Ce^n = X + Y$, we have

$$s(Ce^n - X) = rC - sX = sY.$$

We will show that, if we choose p large enough, on the one hand we will have

$$\left| \frac{rC - sX}{(p-1)!} \right| \ge 1 \tag{9}$$

and on the other hand we will have

$$\left| \frac{sY}{(p-1)!} \right| < 1 \tag{10}$$

which is a contradiction.

We prove (9) first. We have that $s(C \cdot e^n - X) = rC - sX$ is an integer, and because $(p-1)! \mid C$ and $p! \mid X$, we have

$$(p-1)! \mid (rC - sX)$$

At this point, it might be possible that $rC - sX$ is 0. We show it is not by applying Fermat little theorem. Since

$$C = \sum_{p-1 \le k \le 2p-1} c_k k! = c_{p-1}(p-1)! + c_p p! + c_{p+1}(p+1)! + ...c_{2p-1}(2p-1)!,$$

by Lemma 4 and Fermat little theorem, we have (note we need p to be a prime number for applying Fermat little theorem)

$$C \equiv c_{p-1}(p-1)! \equiv n^p(p-1)! \equiv n(p-1)! \not\equiv 0 \mod p!$$

Hence, because $p! \mid X$, we have

$$rC - sX \equiv rn(p-1)! - 0 \equiv rn(p-1)! \not\equiv 0 \mod p!$$

for sufficiently large $p > rn$. This implies $rC - sX \neq 0$, as desired. Since $rC - sX$ is a none-zero integer that is divisible by $(p-1)!$, we have proved (9).

Next, we prove (10). This follows from (8). Indeed,

$$\left|\frac{sY}{(p-1)!}\right| \le \left|\frac{se^n n^{2p-1}(n+1)^p}{(p-1)!}\right| \to 0, \qquad as\ p \to \infty.$$

Hence, if we choose p to be sufficiently large, (10) holds. □

Discussion: (1) We have proved a very general result that $e, e^2, e^3, e^4, \ldots$ are all irrational numbers! Let's recall what tools we have used?

Firstly, we used some very simple Calculus (e.g., Taylor expansion of e^x, derivatives of f, etc).

Secondly, we used properties of binomial coefficients $\binom{a}{b}$, in particular, the fact that it is an integer.

Thirdly, we used Fermat little theorem (to prove some integer is non-zero, which is a typical application of Fermat little theorem), though, recall that we also deduced Fermat little theorem from binomial theorem which follows from binomial coefficients.

Hence, to sum up,

simple calculus + simple properties of $\binom{a}{b} \implies e, e^2, e^3, e^4, \ldots$ **are all irrational!**

Isn't this amazing?!

(2) One may ask, sure, this seems cool. But it seems the result is irrelevant. Afterall, why do we care that $e, e^2, e^3, e^4, \ldots$ are all irrational numbers?

The answer is at least two-fold.

One, the result is beautiful, and beauty and the appreciation of beauty is itself very worth doing, and is one of the finest test and demonstration of human intelligence.

Two, one can in fact further develop the method we saw and prove that e is in fact a transcendental number (i.e., it is not a root of any integer polynomial equation like $x^{23} + 5x^{18} - 30076x^5 + 53492 = 0$), and going further, using the relation between $e^{i\pi} = -1$, one can further prove that π is also a transcendental number, and this solves one of the oldest three geometric problems: you cannot square a circle, i.e., using ruler-and-compass construction, one can not draw a square with the same area of a circle. Note here, that how **analysis (calculus)** and **discrete math (bonomial coefficients)** are used to solve a **geometric** problem.

2.2 Case analysis

Definition 7. *Ramsey number $R(p, q)$ is defined to be the smallest number of people, such that either there are p people who all are all friends, or there are q people who are all strangers.*

For example, take $p = 99$ and $q = 203$. The question we are asking is really: is it true that when the number of people are sufficiently large, then there must be either 99 friends, or 203 strangers? Without rigorous thinking, it's not clear. In other words, no matter how many people there are, there aren't 99 friends, and there are't 203 strangers. Ramsey said (proved) that this is not the case.

Remark: one can think of this as some mathematical "emergence" phenomenon: once the group of people are large enough, some "structue" will appear.

We start with a simple example.

Ex: Prove $R(3, 3) \leq 6$ by case analysis.

Theorem 8. $R(p, q) \leq \binom{p+q-2}{p-1}$.

Note that binomial coefficient again appears!

Proof. This is a simple corollary of the recursive inequality:

$$R(p, q) \leq R(p - 1, q) + R(p, q - 1).$$

(**Alert:** explain it if time allows, or left as homework)

Recall the simple identity for binomial coefficients $\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}$ (do you know how to prove it?). Set $n = p + q - 2, k = p - 1$, we have

$$\begin{aligned} f(p, q) &= \binom{p+q-2}{p-1} \\ &= \binom{p+q-3}{p-1} + \binom{p+q-3}{p-2} \\ &= \binom{p+(q-1)-2}{p-1} + \binom{(p-1)+q-2}{(p-1)-1} \\ &= f(p, q-1) + f(p-1, q). \end{aligned}$$

Since $R(p, q)$ and $f(p, q)$ satisfy the same inequality and $f(p, q)$ satisfies it with equality, we would have $R(p, q) \leq f(p, q)$ if the have the same starting point. Indeed, we have (think for yourself why $R(p, 2) = p$ and $R(2, q) = q$)

$$R(p, 2) = p = f(p, 2), \quad R(2, q) = q = f(2, q).$$

Note that we are secretly using *induction* here. □

Discussion: One may again ask why we care about this seeming pointless small game of thinking about some large population so that it must have some structure (either a group of friends or a group of strangers)? It turns out, surprisingly, that Ramsey numbers appear in many places in mathematics and computer science, including in the design and analysis

of many algorithms. Hence, determining the value of $R(p,q)$ is one of the most important problems in discrete mathematics! However, even to prove better upper and lower bounds is already extremely difficult. For example, if we take $p = q$ in Theorem 8, we get

$$R(p,p) = \binom{2p-2}{p-1} \approx \frac{2^{2p-2}}{\sqrt{2p-2}} \approx \frac{4^p}{\sqrt{p}}.$$

It is only in the past few years that we have really improved this bound [2, 3]! **Read this news report [1] if you are interested.**

2.3 weak and strong induction

The standard induction we use is often simply called induction, which is sometimes called weak induction, to compare with the strong induction. The weak and strong is to indicate the hypothesis is weak or strong, strong means a stronger (more) assumption.

For weak induction, what we do is: assume induction hypothesis is true for $n-1$, and prove it for n.

For strong induction, for example, assume induction hypothesis is true for all $1 \leq m \leq n$, and prove it for $n+1$.

Important: for strong induction, we should verify sufficiently many bases cases, otherwise we may reach a wrong conclusion!

check the Chinese lecture notes.

3 simultaneous induction

Let F_n denote the Fibonacci sequence: $1, 1, 2, 3, 5, 8, 13, ...$, i.e., $F_n = F_{n-1} + F_{n-2}$.

Show that

$$F_n^2 + F_{n-1}^2 = F_{2n-1}. \tag{11}$$

It's natural to try induction. So, let's first rewrite the equation as $F_{2n-1} = F_n^2 + F_{n-1}^2$, and assume it is true for n, and try to prove it is true for $n+1$. We have

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

By induction hypothesis, we have $F_{2n-1} = F_n^2 + F_{n-1}^2$. So, we can plug into the above sum. But what about F_{2n}? We don't know anything about it. Furthermore, the goal (11) we want to prove is about the odd terms F_{2n-1}, it does not concern the even terms F_{2n} at all.

What to do next?

Let's assume the claim is true, and see what we can deduce from it. So, we should have

$$F_{2n} = F_{2(n+1)-1} - F_{2n-1} = (F_{n+1}^2 + F_n^2) - (F_n^2 + F_{n-1}^2) = F_{n+1}^2 - F_{n-1}^2. \tag{12}$$

So, instead of proving (11), let's try to prove (11) and (12). This seems a stupid thing to do, because now we are trying to prove more things, so it must be harder. However, the thing is that we will also have more (and necessary) knowledge when we do the induction. So, it's worth to try to prove (11) and (12) *simultanesouly* via induction. This is called *simultaneous induction*.

Proof. sketch:

- check base cases for both
- induction hypothesis, assume both are true for some n
- prove both are true for $n + 1$

□

4 structure induction

We are familiar with induction when natural numbers are involed. However, in computer science, there are many problems where we have to analysis and prove properties about other structures consisting of other symbols of objects. When these objects are constructed in some controlled way, we may still use induction to help our analysis or poofs, thus the *structure induction*.

Example: prove every BSP (balanced strings of parentheses) has equal numbers of left and right parentheses. See [4, chapter 8]

References

[1] A very big small leap forward in graph theory. `https://www.quantamagazine.org/after-nearly-a-century-a-new-limit-for-patterns-in-graphs-20230502/`.

[2] Marcelo Campos, Simon Griffiths, Robert Morris, and Julian Sahasrabudhe. An exponential improvement for diagonal ramsey. *arXiv preprint arXiv:2303.09521*, 2023.

[3] Parth Gupta, Ndiame Ndiaye, Sergey Norin, and Louis Wei. Optimizing the cgms upper bound on ramsey numbers. *arXiv preprint arXiv:2407.19026*, 2024.

[4] Harry Lewis and Rachel Zax. *Essential discrete mathematics for computer science*. Princeton University Press, 2019.