Discrete Mathematics Recitation Class

Tianyu Qiu

University of Michigan - Shanghai Jiaotong University

Joint Institute

Summer Term 2019

Contents

Principle of Induction (P120-P121)

Let $P(n)$ be a property, $n_0 \in \mathbb{N}$. we can show $P(n)$ holds for all $n \in \mathbb{N}(n \geqslant n_0, n \in \mathbb{N})$ using the following argument structure:

1. Show that $P(0)(P(n_0))$ holds.
2. Show that for arbitrary $n \in \mathbb{N}(n \geqslant n_0, n \in \mathbb{N})$, $P(n) \Rightarrow P(n+1)$.

It then follows, by the Principle of Induction, that for all $n \in \mathbb{N}(n \geqslant n_0, n \in \mathbb{N})$, $P(n)$ holds.

Link between induction and the well-orderedness of $(\mathbb{N}, \leqslant)$ (P124)

Recall: Well-order guarantees the existence of least element (correspondingly, the initial value n_0 in induction) for every non-empty subsets in a linear order.

The Correctness of Principle of Induction (proof by contradiction)

1. Show that $P(n_0)$ holds.
2. Suppose that $\{n \in \mathbb{N} | n \geqslant n_0 \wedge \neg P(n)\}$ is non-empty and let n' be the least element of this set.
3. Let $m \geqslant n_0$ be such that $n' = m + 1$.
4. Show that the fact that $P(m)$ holds implies that $P(n')$ holds, thus obtaining a contradiction.

Examples of Induction (P125)

Theorem

Let $(L, \preceq)$ be a lattice. If $X \subseteq L$ is finite with $|X| \geqslant 2$, then X has a least upper bound.

Proof.

$P(n)$: Every $X \subseteq L$ with $|X| = n$ has a l.u.b..

1. $P(2)$ holds by definition of lattice.
2. (Proof by Contradiction) Suppose that $m > 2$ is least such that there exists

$$X = \{x_1, x_2, \cdots, x_m\} \subseteq L$$

and X does not have a l.u.b. Since m is least, $X' = \{x_1, x_2, \cdots, x_{m-1}\}$ has a l.u.b. y. And since $(L, \preceq)$ is a lattice, $y \vee x_m$ exists. Moreover, $y \vee x_m$ is the l.u.b. for X, which is a contradiction.

Strong Induction (P126)

An argument by strong induction that shows that a property $A(n)$ holds for all $n \in \mathbb{N}$ with $n \geqslant n_0$ proceeds as follows:

1. Show that $A(n_0)$ holds.
2. Show that for all $n \geqslant n_0$, if for all $n_0 \leqslant k \leqslant n$, $A(k)$ holds, then $A(n+1)$ holds
3. Conclude that for all $n \in \mathbb{N}$ with $n \geq n_0$, $A(n)$ holds.

Theorem

For all $n \in \mathbb{N}$ with $n \geqslant 2$, n is either prime or the product of primes.

Recursive Definitions (P128)

A definition in the following form is called a recursive definition:
Define a function $f : \mathbb{N} \to \mathbb{N}$ by specifying:

1. The value of $f(0)$ and maybe some other initial values of f such as $f(1)$.
2. A rule that allows us to obtain the value of $f(n+1)$ from the values of $f(n), f(n-1), \cdots$.

e.g.

- The factorial function
- The Fibonacci sequence

Recursive Defined Functions (P129)

$f : \mathbb{N}$ is defined by $f(0) = n_0$ and $(n+1, f(n+1)) = G(n, (f(n))$

$$(n, f(n)) \xrightarrow{G(\cdot,\cdot)} (n+1, f(n+1))$$

G can be regarded as a function $G : \mathbb{N} \times \mathbb{N} \to \mathbb{N} \times \mathbb{N}$.

1. Let $X = \{R \in \mathcal{P}(\mathbb{N} \times \mathbb{N}) | (0, n_0) \in R\}$.
2. $(X, \subseteq)$ is a complete lattice(why?).
3. Define $F : X \to X$ by $F(R) = R \cup G''R$
4. $F : (X, \subseteq) \to (X, \subseteq)$ is order-preserving. By TK Theorem, F has a least fixed point (a $\subseteq$-least f in X such that $F(f) = f$).
5. This f is the function given by the recursive definition.

General Recursive Definitions (P130-P131)

You have:

- Initial Set B with initial objects (values,pairs,$\cdots$).
- Construction Rules $C_1, C_2, \cdots, C_n$.

You get:

- The resulting set A by recursively applying construction rules to the initial set B.
- A is the least fixed point of an order-preserving function on a complete lattice.

Structural Induction (P132)

Let B be a set and let $C_1, C_2, \cdots, C_n$ be construction rules. Let A be recursively defined to be the $\subseteq$-least set such that $B \subseteq A$ and A is closed under the rules $C_1, \cdots, C_n$. Let $P(x)$ be a property. If

1. For all $b \in B, P(b)$ holds.
2. For all $a_1, \cdots, a_m$ and $1 \leqslant i \leqslant n$, if $P(a_1), \cdots, P(a_m)$ all hold and c is obtained from $a_1, \cdots, a_m$ by a single application of the rule C_i, then $P(c)$ holds.

Then $P(x)$ holds for every elements of A.

Examples of Recursive Definitions

- Construction rule: $a_{n+1} = 2a_n$
  1. $B_1 = \{2\}$
  2. $B_2 = \{2, 3\}$

  For B_1, what about $A' = \{2, 3, 4, 8, 16, \cdots\}$?
- Let $S \subseteq \mathbb{N}$ be the $\subseteq$-least set such that $3 \in S$ and if $x, y \in S$, then $x + y \in S$. Then $S = \{n \in \mathbb{N} | 3 | n\}$ (P133).

Proof.

Let $X = \{n \in \mathbb{N} | 3 | n\}$. Since S is the $\subseteq$-least set. $S \subseteq X$. By induction, $X \subseteq S$. Now $3 \in S$ and if $3k \in S$, then $3(k + 1) = 3k + 3 \in S$. $\square$

Subsets of size k (P136)

Definitions

Given A a finite set, $0 \leqslant k \leqslant |A, , k \in \mathbb{N}, n \in \mathbb{N} \setminus \{0\}$

- $\mathcal{P}_k(A) = \{x \in \mathcal{P}(A) \mid |x| = k\}$ The collection of subsets (whose cardinality is k) of A.
- $[n] = \{0, 1, \cdots, n-1\}$, $[0] = \emptyset$
- $\binom{n}{k}$ is the cardinality of the set $\mathcal{P}_k([n])$

Pascal's Triangle (P138)

Lemma

For all $n \in \mathbb{N}$ *and for all* $0 \leqslant k \leqslant n$, $\binom{n}{k} = \binom{n}{n-k}$

Proof.

The function $F : \mathcal{P}_k([n]) \to \mathcal{P}_{n-k}([n])$ defined by: for all $x \in \mathcal{P}_k([n]), F(x) = [n] \setminus x$ is a bijection. (recall the definition of equal cardinality). $\square$

Pascal's Triangle (P138-P139)

Theorem

For all $n \in \mathbb{N}$ *with* $n \geqslant 1$ *and for all* $0 < k \leqslant n$,

$$\binom{n+1}{k} = \binom{n}{k-1} + \binom{n}{k}$$

You are selecting k distinct objects from $n+1$ distinct objects.
You have two choices:

1. Directly select k distinct objects from n distinct objects.
   $A = \{x \cup \{n\} | x \in \mathcal{P}_{k-1}([n])\}$
2. Select $k-1$ distinct objects from n distinct objects, and then select the remaining $n+1's$ object.
   $B = \mathcal{P}_k([n])$

Note that $A \cap B = \emptyset$ since n is not a member of any element of B.
Thus $|A \cup B| = |A| + |B|$ (recall addition($+$) defined in $\mathbb{N}_{def}$).

Pascal's Triangle (P139)

This theorem gives a recursive definition of $\binom{n}{k}$ with initial values $\binom{n}{0} = \binom{n}{n} = 1$ and the construction rule

$$\binom{n+1}{k} = \binom{n-1}{k} + \binom{n}{k}$$

Pascal Triangle:

$$\begin{array}{lccccccccc}
n=0 & & & & & 1 & & & & \\
n=1 & & & & 1 & & 1 & & & \\
n=2 & & & 1 & & 2 & & 1 & & \\
n=3 & & 1 & & 3 & & 3 & & 1 & \\
n=4 & 1 & & 4 & & 6 & & 4 & & 1
\end{array}$$

Binomial Theorem (P140)

Theorem

For all $n \in \mathbb{N}$ with $n \geqslant 1$ and for all numbers x and y,

$$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^{n-k} y^k$$

Proof.

By induction

$$P(n) : (x+y)^n = \sum_{k=0}^{n} x^{n-k} y^k$$

1. $P(1)$ holds as $(x+y)^1 = x + y = \binom{1}{0} x + \binom{1}{1} y$.

Binomial Theorem (P141)

Proof.

Assume that $P(n)$ holds. For $n+1$

$$(x+y)^{n+1} = (x+y)(x+y)^n = (x+y)\left(\sum_{k=0}^{n}\binom{n}{k}x^{n-k}y^k\right)$$

Coefficient for x^{n+1}, y^{n+1} is $\binom{n+1}{0}=1$ and $\binom{n+1}{n+1}=1$ The coefficient of the term $x^{n+1-k}y^k$ is

$$\binom{n+1}{k} = \binom{n-1}{k} + \binom{n}{k}$$

We focus on the power of y, it is either originally equal to k, or originally equal to $k-1$, but multiplied by the extra y.

Binomial Theorem (P142)

Proof.

Thus we obtain for $n+1$,

$$(x+y)^{n+1} = \sum_{k=0}^{n+1} \binom{n+1}{k} x^{n+1-k} y^k$$

which means $P(n+1)$ holds, $P(n)$ holds for all $n \in \mathbb{N} \setminus \{0\}$. $\square$

Corollary

- *When* $x = 1$,

$$(1+y)^n = \sum_{k=0}^{n} \binom{n}{k} y^k$$

- *When* $x = y = 1$,

$$2^n = \sum_{k=0}^{n} \binom{n}{k}$$

Other Finite Sets (P143)

Theorem

$$|\mathcal{P}_n([2n])| = \sum_{k=0}^{n} \binom{n}{k}^2$$

Proof.

Since $(1+x)^n(1+x)^n = (1+x)^{2n}$, we have

$$\left(\sum_{k=0}^{n} \binom{n}{k} x^k\right)\left(\sum_{k=0}^{n} \binom{n}{k} x^k\right) = \sum_{k=0}^{2n} \binom{2n}{k} x^k$$

$$\text{Coefficient of } x^n = \sum_{k=0}^{n} \binom{n}{k}\binom{n}{n-k} = \sum_{k=0}^{n} \binom{n}{k}^2 = \binom{2n}{n}$$

□

Other Finite Sets (P144)

Theorem

$|\mathcal{P}([n])| = 2^n$

Proof.

$$\mathcal{P}([n]) = \bigcup_{k=0}^{n} \mathcal{P}_k([n])$$

Since for all $0 \leqslant i < j \leqslant n$, $\mathcal{P}_i([n]) \cap \mathcal{P}_j([n]) = \emptyset$. It follows that

$$|\mathcal{P}([n])| = \sum_{k=0}^{n} |\mathcal{P}_k([n])| = \sum_{k=0}^{n} \binom{n}{k} = 2^n$$

$\square$

Counting (P146)

Theorem

Let $n, r \in \mathbb{N}$. The number of solutions to the equation $x_1 + x_2 + \cdots + x_n = r$ with $x_1, x_2, \cdots, x_n \in \mathbb{N}$ is

$$\binom{n+r-1}{r}$$

Proof.

Let $A = \{(x_1, \cdots, x_n) \in \mathbb{N}^n | x_1 + \cdots + x_n = r\}$. We need to show that $|A| = |\mathcal{P}_r([n+r-1])| = |\mathcal{P}_{n-1}([n+r-1])|$. Since $|\mathcal{P}_r([n+r-1])| = |\mathcal{P}_{n-1}([n+r-1])|$. Define $F : A \longrightarrow \mathcal{P}_{n-1}([n+r-1])$ by

$$F(x_1, \ldots, x_n) = \left\{x_1, x_1 + x_2 + 1, \ldots, n - 2 + \sum_{i=1}^{n-1} x_i\right\}$$

Counting (P147-P148)

Proof(continue).

If $x_1, \cdots, x_n \in \mathbb{N}$ is such that $x_1 + \cdots + x_n = r$, then

$$0 \leq x_1 < x_1 + x_2 + 1 < \cdots < x_1 + \cdots + x_{n-1} + n - 2 < n + r - 2$$

and so each element of A is mapped to an element of $\mathcal{P}_{n-1}([n+r-1])$. The function F is clearly injective. If $\{y_1 < \cdots < y_{n-1}\} \in \mathscr{P}_{n-1}([n+r-1])$, then by letting $x_1 = y_1$, $x_2 = y_2 - (x_1 + 1), \ldots, x_{n-1} = y_{n-1} - (x_1 + \cdots + x_{n-2} + n - 2)$ and $x_n = r - (x_1 + \cdots + x_{n-1})$ we get an element

$$(x_1, \ldots, x_n) \in A \text{ with } F(x_1, \ldots, x_n) = \{y_1 < \cdots < y_{n-1}\}$$

This shows that F is surjective and completes the proof. □

Counting (P148)

Theorem

The number of ways of selecting r objects from n objects when the order does not matter and repetitions are allowed is

$$\binom{n+r-1}{r}$$

Proof.

The number of ways of selecting r objects from n objects when the order does not matter and repitions are allowed is the number of solutions to the e.q. $x_1 + \cdots + x_n = r$ where $x_1, \ldots, x_n \in \mathbb{N}$. $\square$

Theorem

The number of bijections from $[n]$ to $[n]$ is $n!$. I.e.

$$|\{f | f : [n] \longrightarrow [n] \text{ is a bijection } \}| = n!$$

Counting (P149)

Proof.

We prove this result by induction. Note that the number of bijections from [1] to [1] (and [0] to [0]!) is 1. Assume that the number of bijections from $[n]$ to $[n]$ is $n!$. Let $A = \{f | f : [n+1] \to [n+1] \text{ is a bijection}\}$. For all $k \in [n+1]$, let $A_k = \{f \in A | f(0) = k\}$. It is clear that, by the induction hypothesis, $|A_k| = n!$. Moreover, for all $0 \leqslant i < j < n+1$, $A_i \cap A_j = \emptyset$. Therefore, $|A| = (n+1)n! = (n+1)!$. □

Counting (P149)

Theorem

Let $n \in \mathbb{N}$ and let $0 \leqslant k \leqslant n$. The number of ordered $k-$tuples of distinct elements of $[n]$ is

$$\binom{n}{k} k!$$

i.e. $\left|\{(x_1, \ldots, x_k) \in [n]^k \mid \text{for all } 0 \leq i < j \leq k, x_i \neq x_j\}\right| = \binom{n}{k} k!$

Proof.

An ordered $k-$tuple of distinct things from $[n]$ is just an $A \in \mathcal{P}_k([n])$ coupled with a bijection $f : A \to [k]$. $\square$

Permutation & Combination

Definitions

Given $n \in \mathbb{N} \setminus \{0\}$, $r \in \mathbb{N}, r \leqslant n$:

- $0! = 1$.
- Permutation with repetition not allowed. (DMA408)

$$P_n^r = P(n,r) = n(n-1)(n-2)\cdots(n-r+1) = \frac{n!}{(n-r)!}$$

- Combination with repetition not allowed.(DMA410)

$$C_n^r = C(n,r) = \frac{P(n,r)}{P(r,r)} = \frac{n!}{(n-r)!r!} = C(n,n-r)$$

Permutation & Combination

Definitions

Given $n \in \mathbb{N} \setminus \{0\}$, $r \in \mathbb{N}$:

- Permutation with repetition allowed. (DMA423)

$$\# = n^r$$

- Combination with repetition allowed. (DMA425)

$$\# = \binom{n+r-1}{r}$$

Permutation & Combination

Summary (DMA427)

TABLE 1 Combinations and Permutations With and Without Repetition.

Type	*Repetition Allowed?*	*Formula*
r-permutations	No	$\frac{n!}{(n-r)!}$
r-combinations	No	$\frac{n!}{r!\,(n-r)!}$
r-permutations	Yes	n^r
r-combinations	Yes	$\frac{(n+r-1)!}{r!\,(n-1)!}$

Permutations with Indistinguishable Objects (DMA428)

Theorem

The number of different permutations of n objects, where there are n_1 indistinguishable objects of type 1, n_2 indistinguishable objects of type 2, $\cdots$, and n_k indistinguishable objects of type k, is

$$\begin{aligned} & C_n^{n_1} \cdot C_{n-n_1}^{n_2} \cdot \ldots \cdot C_{n_k}^{n_k} \\ = & \frac{n!}{n_1!n_2!\cdots n_k!} \\ = & \frac{P_n^n}{P_{n_1}^{n_1} \cdot P_{n_2}^{n_2} \cdot \ldots \cdot P_{n_k}^{n_k}} \end{aligned}$$

Distributing Objects into Boxes (DMA429)

- Distinguishable Objects & Distinguishable Boxes:

Theorem

The number of ways to distribute n distinguishable objects into k distinguishable boxes so that n_i objects are placed into box i, $i = 1, 2, \cdots, k$, equals

$$\frac{n!}{n_1!n_2!\cdots n_k!} = \frac{P_n^n}{P_{n_1}^{n_1} \cdot P_{n_2}^{n_2} \cdot \ldots \cdot P_{n_k}^{n_k}}$$

Distributing Objects into Boxes (DMA430-DMA431)

- Indistinguishable Objects & Distinguishable Boxes:
  Distribute n indistinguishable objects into k distinguishable boxes: $\# = \binom{n+k-1}{k-1}$
  e.g. How many ways are there to place 10 indistinguishable balls into eight distinguishable bins?
- Distinguishable Objects & Indistinguishable Boxes:
  Distribute n distinguishable objects into k indistinguishable boxes: $\# = \sum_{j=1}^{k} S(n,j)$ Stirling Numbers of the second kind (will not be talked about here, you can refer to DMA)
- Indistinguishable Objects & Indistinguishable Boxes:
  Enumeration

Binomial Theorem (DMA416-DMA417)

Theorem

For all $n \in \mathbb{N}$ and for all numbers x and y,

$$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^{n-k} y^k$$

e.g.

$$\sum_{k=0}^{n} \binom{n}{k} = 2^n \qquad \sum_{\substack{k=0 \\ \text{k is even}}}^{n} \binom{n}{k} = \sum_{\substack{k=1 \\ \text{k is odd}}}^{n} \binom{n}{k} = 2^{n-1}.$$

Important Identities

- Pascal's Identity (DMA418)

$$\binom{n+1}{k} = \binom{n}{k-1} + \binom{n}{k}$$

- Vandermonde's Identity (DMA420)
  Let m, n, and r be nonnegative integers with r not exceeding either m or n. Then

$$\binom{m+n}{r} = \sum_{k=0}^{r} \binom{m}{r-k}\binom{n}{k}$$

- (DMA421) Let n and r be nonnegative integers with $r \leqslant n$. Then

$$\binom{n+1}{r+1} = \sum_{j=r}^{n} \binom{j}{r}$$