Basics of Discrete Mathematics

Handout

2017. 12. 29.

1 Notation

Numbers natural numbers: $\mathbb{N} = \{0, 1, 2, 3, \dots\}$
integers: $\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$
rationals: $\mathbb{Q} = \{p/q : p, q \in \mathbb{Z}\}$
real numbers: $\mathbb{R}$, usually associate with a straight line,
Ex.: $\pi, e, \sqrt{2}$
irrational numbers: $\mathbb{R} \setminus \mathbb{Q} = \mathbb{Q}^*$
complex numbers: $\mathbb{C} = \{a+ib : a, b \in \mathbb{R}\}$, where i (the imaginary number) is the root of $x^2 + 1 = 0$ so $i^2 = -1$.

Basics Lower integer: $\lfloor x \rfloor$, the biggest integer which smaller or equal x
Upper integer: $\lceil x \rceil$, the smallest integer which bigger or equal x
Factorial: $n! = 1 \cdot 2 \cdot \dots \cdot n$
Binomial coefficients:

$$\binom{n}{k} = \frac{n!}{k! \cdot (n-k)!} =$$

= the number of choice of k elements from an n-element set.
$\sum_{i=1}^{n} a_i = a_1 + a_2 + \ldots + a_n$, the sum of a_i's.
$\prod_{i=1}^{n} a_i = a_1 \cdot a_2 \cdot \ldots \cdot a_n$, the product of a_i's.

2 Method of proof

Exercise 1. (Double counting method)

$$\sum_{i=1}^{n}\sum_{j=1}^{n}(i+j) = \frac{n^2 \cdot (n+1)}{2} = A$$

Exercise 2.

$$I = \sum_{i=1}^{n}\sum_{j=1}^{i}(i+j) = \sum_{i=1}^{n}\sum_{j=i}^{n}(i+j) = II$$

And

$$I + II = A + \sum_{i=1}^{n}(i+i) = A + n \cdot (n+1)$$

Thus $I = (n+1)^2 \cdot n/2$.

Remark: There are other ways to calculate this (I) expression.

Direct method See Exercise 1 and 2.

Indirect method

Proposition 1. $\sqrt{2}$ *is irrational.*

Proposition 2. $e = \sum_{i=1}^{\infty} \frac{1}{n!}$ *is irrational.*

Induction

Proposition 3. *For any* $n \in \mathbb{N}$

$$1 + 2 + \cdots + 2^n = 2^{n+1} - 1.$$

Behind the proof we found the following mathematical object:

Proposition 4 (Mathematical Induction)**.** *Let X be a set of natural numbers with the following properties:*

(i) The number 1 belongs to X

(ii) If some natural number n is the element of X, the number $n+1$ belongs to X, as well.

Usually we use this statement to verify statements $A(1), A(2), A(3), \ldots,$ where $A(i)$ denotes the i^{th} statement.

Proposition 5 (Well ordering 'axiom')**.** *Any non-empty subset of* $\mathbb{N}$ *possesses a smallest element.*

The smallest element u of a set $X \subset \mathbb{N}$ means there is no element $y \in X$ such that $u < x$, with the natural ordering of $\mathbb{N}$.

Proposition 6. *The Proposition Mathematical Induction and Proposition Well ordering are equivalent.*

The following proposition is the example of a tricky induction.

Proposition 7 (Arithmetic and geometric inequality)**.** *Let $a_1, a_2, \ldots, a_n$ be non-negative real numbers for any $n \geq 1$. Then*

$$\frac{a_1 + a_2 + \cdots + a_n}{n} \geq \sqrt[n]{a_1 \cdot a_2 \cdot \cdots \cdot a_n}$$

3 Sets

We denote the sets by A, B, C, X, Y, Z, etc. The elements are denoted by a, b, c, x, y, z, etc. The operation $\in$ means belonging to, is the element of something. Example: $x \in X$, x is belongs to X, x is the element of X. For a finite set X we denote the cardinality (the number of distinct elements) by $|X|$.

Basic operations $\cap$: $X \cap Y = \{x : x \in X \text{ and y} \in \text{Y}\}$
$\cup$: $X \cup Y = \{x : x \in X \text{ or y} \in \text{Y}\}$.
The complement of A in X is $A^c = \{x \in X : x \notin A\}$. We also denote it by $\overline{A}$ or $X \setminus A$.
$\setminus$: There are two sets A, B in X. $A \setminus B = A \cup B^c$.

Basic properties: associativity:
$(A \cap B) \cap C = A \cap (B \cap C)$
$(A \cup B) \cup C = A \cup (B \cup C)$
commutativity:
$A \cap B = B \cap A$
$A \cup B = B \cup A$
distributivity:
$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$
$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$
generalization of distributivity:
$A \cap (\bigcup_{i=1}^{\infty} B_i) = \bigcup_{i=1}^{\infty}(A \cap B)$
$A \cup (\bigcap_{i=1}^{\infty} B_i) = \bigcap_{i=1}^{\infty}(A \cup B)$
De-Morgan formulas:
$A \setminus (B \cup C) = (A \setminus B) \cap (A \setminus C)$
$A \setminus (B \cap C) = (A \setminus B) \cup (A \setminus C)$
generalization of De-Morgan formulas:
$A \setminus (\bigcup_{i=1}^{\infty} B_i) = \bigcap_{i=1}^{\infty}(A \setminus B_i)$
$A \setminus (\bigcap_{i=1}^{\infty} B_i) = \bigcup_{i=1}^{\infty}(A \setminus B_i)$

Proving formulas: Venn-diagram (not precise, but gives good intuition)
Precise proof: separately show that Left side $\subseteq$ Right side **and** Right side $\subseteq$ Left side.

Ordered pairs: $(x, y) = \{\{x\}, \{x, y\}\}$
Cartesian product: $X \times Y = \{(x, y) : x \in X, y \in Y\}$
Example: $\mathbb{R}^2$ is the plain.
n-times Cartesian product of X: $X^n = \underbrace{X \times X \times \cdots \times X}_{n} = \{(x_1, x_2, \ldots, x_n) : x_i \in X, 1 \leq i \leq n\}$

4 Functions

Let $f : X \to Y$ is a set of ordered pairs such that for every y there exists at most one x such that $f(x) = y$. (A function is a subset of $X \times Y$).

Decomposition: $f : X \to Y$, $g : Y \to Z$ then $h = g \circ f : X \to Z$ is the composition, such that $h(x) = z$ if there exists y such that $f(x) = y$ and $g(y) = z$.

Properties **Onto**: $f : X \to Y$ is onto (surjective) if for every $y \in Y$, there exists at least $x \in X$ such that $f(x) = y$.

One-to-one: $f : X \to Y$ is one-to-one (injective) if $f(x_1) = f(x_2) \Rightarrow x_1 = x_2$.

Bijective: $f : X \to Y$ is bijective if for every y there exists one x such that $f(y) = x$.

Proposition 8. *The function f is bijective if and only if onto and one-to-one.*

Proposition 9. *(a) If $f : Y \to Z, g : X \to Y$ are onto then $h = f \circ g$ is also onto.*

(b) If $f : Y \to Z, g : X \to Y$ are one-to-one then $h = f \circ g$ is also one-to-one.

(c) If $f : Y \to Z, g : X \to Y$ are bijective then $h = f \circ g$ is also bijective.

(d) For every function $h : X \to Y$ there exists a set Z and two functions f, g such that $f : Z \to Y$ one-to-one and $g : X \to Z$ onto.

Inverse function: Inverse: If $f : X \to Y$ is bijection, then the inverse of f can be defined by $f^{-1} : Y \to X$ such that $f^{-1}(y) = x$ if $f(x) = y$.
Then f^{-1} is also a bijection.

For a set X, let $\mathrm{id}_X : X \to X$ denote the function defined by $\mathrm{id}_X(x) = x$ for all $x \in X$ (the identity function). As an exercise one can show the following statement.

Proposition 10. *Let $f : X \to Y$ be some function. Then the following are true.*

(a) A function $g : Y \to X$ such that $g \circ f = id_X$ exists if and only if f is one-to-one.

(b) A function $g : Y \to X$ such that $f \circ g = id_Y$ exists if and only if f is onto.

(c) A function $g : Y \to X$ such that both $g \circ f = id_X$ and $f \circ g = id_Y$ exist if and only if f is bijection.

(d) If $f : X \to Y$ is a bijection, then the following three condition are equivalent for a function $g : Y \to X$:

(i) $g = f^{-1}$

(ii) $g \circ f = id_X$

(iii) $f \circ g = id_Y$.

4.1 Asymptotic Behaviour

Let $f, g : \mathbb{N} \mapsto \mathbb{R}$, $(f, g \geq 0)$

(a) $f(n) = O(g(n))$ if $\exists n_0$ and $C > 0$ such that $\forall n \geq n_0$

$$f(n) \leq C \cdot g(n).$$

(b) $f(n) = o(g(n))$ if

$$\lim_{n \to \infty} \frac{f(n)}{g(n)} = 0.$$

(c) $f(n) = \Theta(g(n))$ if $\exists n_0$ and $C_1, C_2 > 0$ such that $\forall n \geq n_0$

$$C_1 \cdot g(n) \leq f(n) \leq C_2 \cdot g(n).$$

So f and g has the same "speed of increasing".

(d) $f(n) \sim g(n)$ if

$$\lim_{n \to \infty} \frac{f(n)}{g(n)} = 1.$$

So f and g are asymptotically the same.

Example 11. We will see later that

(a) $\sum_{i=1}^{n} \frac{1}{n} = H_n \sim \ln x$

(b) $n! \sim f(n) = \sqrt{2\pi n}(\frac{n}{e})^n$

Proposition 12. *(a)* $n^\alpha = o(n^\beta)$ *if* $\alpha < \beta$.

(b) $n^c = o(a^n)$ *if* $a > 1$.

(c) $(\ln n)^c = o(n^\alpha)$ *if* $\alpha > 0$

Then there can be defined a partial ordering $f < g$ if $f = o(g)$. So $(\ln n)^c < n^\alpha < a^n$, where $\alpha > 0, a > 1$.

Proposition 13.

$$\binom{n}{k} \sim \frac{n^k}{k!}$$

5 Relations

Every subset R of the Cartesian product $X \times Y$ is called relation. we denote it by xRy or $(x, y) \in R$.
Very important case when $X = Y$.
Examples: $=, \leq, <$ are typical example for a relation.
Composition of relations: $R \subseteq X \times Y$ and $S \subseteq Y \times Z$, then we can define the composition $T = R \circ S$ such that for any $x \in X$ and $z \in Z$, $(x, z) \in T$ if there exists $y \in Y$ such that $(x, y) \in R$ and $(y, z) \in S$.

Representations We denote the relation by $R \subset X \times Y$. Drawing a rectangle: Briefly, let $|X| = n$, $|Y| = m$. In $n \times m$ grid space we color black if the coordinates of that square is in the relation.
Matrix representation: $n \times m$ matrix represents the relation R if for every $i \in X, j \in Y$, $a_{ij} = 1$ if $(i, j) \in R$, and $a_{ij} = 0$, if $(i, j) \notin R$.
Graph representation: We draw a bipartite graph with the corresponding relation. If $R \subset X \times X$, then we may draw a graph on n points.

Now deal only with the relations which is the subset of $X \times X$

Properties Reflexivity: R is reflexive, if $(x, x) \in R$, for every $x \in X$.
Symmetry: R is symmetric if $(x, y) \in R$ if and only if $(y, x) \in R$.
Antisymmetry: R is antisymmetric if $(x, y) \in R$ then $(y, x) \notin R$ and if

$(y,x) \in R$ then $(x,y) \notin R$.
Transitivity: R is transitive, if $(x,y) \in R$ and $(y,x) \in R$ then $(x,z) \in R$.

Inverse relation: The inverse relation of $R \subseteq X \times Y$ is $R^{-1} \subseteq Y \times X$ which satisfies $(y,x) \in R^{-1}$ if $(x,y) \in R$.

Diagonal relation: $\Delta_X = \{(x,x) : x \in X\}$

Equivalence $R \subset X \times X$ is equivalence on X if R is reflexive, symmetric and transitive.
Examples:

(a) $X = \mathbb{N}$: $R = \sim$
$x \sim y$ iff $x - y$ is even

(b) Triangles

Equiv. class $R[x] = \{y \in X : xRy\}$ *equivalence class* of R determined by x.

Proposition 14. *For any equivalence R on X, we have*

(a) $R[x]$ is nonempty for every $x \in X$.

(b) $\forall x, y \in X$ $R[x] = R[y]$ or $R[x] \cap R[y] = \emptyset$.

(c) The equivalence class uniquely determine R. (If R and S are equiv. on X and $R[x] = S[x]$ for every $x \in X$ then $R = S$.)

6 Cardinality of sets

We define an equivalence relation $\sim$ in the following way: $X \sim Y$ if and only if there exists a bijection $X \to Y$.
Notation: $|X| = |Y|$ if and only if $X \sim Y$.
The symbol $|X|$ called the cardinality of X.
For finite sets this is the number of the elements.
If the set of X is not finite, then we say that it has infinite cardinality.
Furthermore, we say that $|X| \leq |Y|$ if there exists an injection $X \to Y$.
Then $<$ is a partial ordering.
Antisymmetry comes form the following theorem:

Theorem 15 (Cantor-Bernstein-Schroeder)**.** *If there exists an injection $X \to Y$ and there exists an injection $Y \to X$ then there exists a bijection $X \to Y$ (so of $|X| \leq |Y|$ and $|Y| \leq |X|$ then $|X| = |Y|$).*

So there are four possibilities: $(|X| < |Y|)$ or $(|Y| < |X|)$ or $(|X| = |Y|)$ or (X and Y are not comparable.

Axiom of Choice A choice function is a function f, defined on a collection $\mathcal{X}$ of nonempty sets, such that for every set A in $\mathcal{X}$, $f(A)$ is an element of A.
Axiom of choice: For any set $\mathcal{X}$ of nonempty sets, there exists a choice function f defined on $\mathcal{X}$.

Theorem 16. *With the axiom of choice it can be proved that X and Y are comparable.*

Thus $\leq$ is a linear ordering on the equivalence classes of $\sim$.
Countable sets: A set X is countable if $|X| = |\mathbb{N}|$.

Proposition 17 (Countable sets)**.**

$$|\mathbb{N}| = |\mathbb{Q}| = |\mathbb{Q} \times \mathbb{Q}| = \underbrace{|\mathbb{Q} \times \cdots \times \mathbb{Q}|}_{n} = |\bigcup_{i=1}^{n} A_i|,$$

where $|A_i| = |\mathbb{N}|$ for any $i \in \mathbb{N}$.

Theorem 18 (Continuum is not Countable)**.**

$$|\mathbb{R}| > |\mathbb{N}| = |\mathbb{Q}|,$$

$$|2^X| > |X|.$$

The proof based on the diagonal method.
Consequence: There are infinitely many different infinite cardinality exists.
Continuum hypothesis: There is no other cardinality exists between $|\mathbb{N}|$ and $|\mathbb{R}| = c$.

7 Ordering

The relation R is an ordering if it is reflexive, antisymmetric, transitive.
(X, R) is called ordered set.
Notation: $R = \leq$, $a \leq b$
Ordered sets= partially ordered sets= POSETs
Ordering= partial ordering

R is a linear ordering if it is ordering and $\forall x, y \in R$ xRy or yRx.
Examples:

(a) Lexicographic ordering is a linear ordering.
(b) Parameters of computers
(c) $a|b$
(d) X be a set and 2^X the power set. The relation is $\subseteq$.

Drawing Posets Do not denote transitivity, arrows and loops. Vertical position.

Hesse diagram Examples:

(a) Linear ordering
(b) Cartesian product

(c) Subset system of an n-element set with inclusion (We drawn it for $n = 2, 3$).

Immed. pred.: Let $(X, \leq)$ be a poset. We say that $x \in X$ is an immediate predecessor of the element y if

- $x < y$ and
- There is no $t \in X$ s.t. $x < t < y$-

We denote this relation by $\triangleleft$.

Proposition 19. *Let $(X, \leq)$ be a finite ordered set and let $\triangleleft$ the immediate relation. Then for any two elements $x, y \in X, x < y$ holds iff there are elements $x_1, \ldots, x_k \in X$ s.t $x \triangleleft x_1 \triangleleft \ldots \triangleleft x_k \triangleleft y$ (if $k = 0$ then $x \triangleleft y$).*

Lemma 20. *Let $x, y \in X, x < y$ be two elements s.t. there exist at most n elements $t \in X$ satisfying $x < t < y$. Then there are elements $x_1, \ldots, x_k \in X$ s.t $x \triangleleft x_1 \triangleleft \ldots \triangleleft x_k \triangleleft y$.*

Hesse diagram Examples:

(a) Linear ordering

(b) Cartesian product

(c) Power set, etc.

Linear extension Every linear ordering is an ordering but the reverse is not true. But...

Theorem 21. *Let $P = (X, \preceq)$ be a finite poset. Then there exists a linear ordering $\leq$ on X s.t $x \preceq y$ implies $x \leq y$.*

Remark: This might call the linear extension and this exists if X is not finite (Equivalent AC).

Let $(X, \preceq)$ be a poset. An element $a \in X$ is called minimal of X if $\nexists x \in X$ s.t. $x \prec a$. (Similar: maximal)

Theorem 22. *Every finite poset has a minimal element.*

$(\mathbb{Z}, \leq)$ has no minimal and maximal elements.

Embedding Let $(X, \preceq)$ and $(X', \preceq')$be two ordered sets. A mapping $f : X \to X'$ is called embedding of $(X, \preceq)$ into $(X', \preceq')$ if the following hold:

(a) f is one-to-one.

(b) $f(x) \preceq' f(y)$ iff $x \preceq y$.

If f is onto, then it is an isomorphism between the posets.

Theorem 23. *For every finite poset $P = (X, \preceq)$ there exists an embedding into $(2^X, \subseteq)$.*

Large implies tall or wide Let $(X, \preceq) = P$ be a poset.

Independent sets The set $A \subseteq X$ is called independent if $\forall x, y \in X, x \npreceq y$ and $x \npreceq y$. (Antichain)
In this case x and y are incomparable.
$\alpha(P) = max\{|A| : A \text{ indep. set of } P = (X, \preceq)\}$.

Proposition 24. *The set of all minimal (or maximal) elements is an independent set.*

Chain The set $B \subseteq X$ is a chain if $\forall x, y \in B x \preceq y$ or $y \preceq x$.
$\omega(P) = max\{|B| : B \text{ is a chain in } P = (X, \preceq)\}$.

Theorem 25. *For every finite set $P = (X, \preceq)$, we have*

$$\alpha(P) \cdot \omega(P) \geq |X|.$$

Corollary 26 (Erdos-Szekeres Thm.)**.** *Arbitrary sequence $(x_1, \dots, x_{n^2+1})$ of real numbers contains a monotone subsequence of length $n + 1$.*

Sperner's theorem This theorem states that any independent system of subsets of n-element set contains at most $\binom{n}{\lceil n/2 \rceil}$ sets.

Theorem 27. $\alpha(B_n) \leq \binom{n}{\lceil n/2 \rceil}$

LYM inequality This inequality was named by Lubell, Meschalkin and Yamamoto.

Proposition 28. *Let $\mathcal{M}$ be an independent system of subsets in B_n. Then*

$$\sum_{M \in \mathcal{M}} \frac{1}{\binom{n}{|M|}} \leq 1.$$

8 Combinatorial counting

Proposition 29 (Variation with repetitions)**.** *Let N be an n-element set (it may be empty, i.e. we admit $n = 0, 1, 2, \dots$) and let M be an m-element set $m \geq 1$. Then the number of possible mapping $f : N \to M$ is m^n.*

Proposition 30 (Variation without repetitions)**.** *For given numbers $n \geq m \geq 0$, there exist exactly*

$$n(n-1)\dots(m-n+1) = \prod_{i=0}^{m-1}(n-i)$$

injective mappings of a given m-element set to a given n-element set.

Proposition 31 (Permutation without repetitions)**.** *For given $n \geq 0$, the number of bijective functions $f : \{0, \dots, n\} \to \{0, \dots, n\}$ is $n!$.*

Proposition 32 (Permutation with repetitions)**.** *There is k_1 number of 1's, k_2 number of 2's, ..., and k_L number of L's such that $k_1 + \dots + k_s = n$ Then there can be written*

$$\frac{n!}{k_1! \dots k_L!}$$

different numbers with these characters.

Proposition 33 (Combination without repetitions)**.** *Let n different objects in a queue. The number of the choice of k object at the same time from this n is $\binom{n}{k}$.*

Theorem 34 (Binomial theorem)**.**

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

Theorem 35 (Multinomial theorem)**.**

$$(x_1 + x_2 + \cdots + x_m)^n = \sum_{k_1+k_2+\cdots+k_m=n} \binom{n}{k_1, k_2, \ldots, k_m} x_1^{k_1} x_2^{k_2} \cdots x_m^{k_m},$$

$(n \geq 1, k_1 + k_2 + \cdots + k_m = n, k_i \geq 1)$.

Example 36. How many ways are there to write a non-negative integer as a sum of r non-negative integers, where the order of the integers counts (i.e. $i_1 + \cdots + i_r = m$ and $i_1, \ldots, i_r \geq 0$)?

Pascal triangle

Proposition 37 (Combination with repetitions)**.** *Let k different type of objects but we may choose arbitrarily many from any of them. Then the number of the choice of n object from them is $\binom{n+k-1}{k-1}$.*

Formulas

Proposition 38. *(a) The number of the subsets of an n-element set is 2^n, moreover:*

$$2^n = \sum_{k=1}^{n} \binom{n}{k}.$$

(b) The number of the subsets containing odd number of element is equal the number of the subsets containing even number of element. i.e.

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

(c) Easy:

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

(d) Easier:

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

Method of proofs Now we collected the techniques that we usually use to prove a combinatorial identity of binomial coefficients.

(a) Induction and/or direct calculation.

(b) Find out a combinatorial problem and count the corresponding quantity with double counting.

(c) Use binomial or multinomial theorem or some polynomial expression.

(d) Use Pascal's triangle.

(e) Use Probability Theory by finding a proper distribution.

1. Vandermonde's identity

$$\binom{m+n}{r} = \sum_{k=0}^{r} \binom{m}{k}\binom{n}{r-k}, \qquad m, n, r \in \mathbb{N}_0.$$

2. generalization of Vandermonde's identity

$$\binom{n_1 + \cdots + n_p}{m} = \sum_{k_1+\cdots+k_p=m} \binom{n_1}{k_1}\binom{n_2}{k_2}\cdots\binom{n_p}{k_p}$$

Example 39.

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

$$\sum_{k=0}^{m} (-1)^k \binom{n}{k}\binom{n}{m-k} = (-1)^{m/2}\binom{n}{m/2},$$

otherwise it is 0 for odd m.

3. Connections with this identity
We can prove Vandermonde's identity using Pascal triangle or with probability theory using hypergeometric distribution
(For further information, see: https://en.wikipedia.org/wiki/Hypergeometric_distribution)

9 Estimations

Reminder We recall some basic definitions and results about the asymptotic behaviour of functions:
Let $f, g : \mathbb{N} \mapsto \mathbb{R}$, $(f, g \geq 0)$

(a) $f(n) = O(g(n))$ if $\exists n_0$ and $C > 0$ such that $\forall n \geq n_0$

$$f(n) \leq C \cdot g(n).$$

(b) $f(n) = o(g(n))$ if

$$\lim_{n\to\infty} \frac{f(n)}{g(n)} = 0.$$

(c) $f(n) = \Theta(g(n))$ if $\exists n_0$ and $C_1, C_2 > 0$ such that $\forall n \geq n_0$

$$C_1 \cdot g(n) \leq f(n) \leq C_2 \cdot g(n).$$

So f and g has the same "speed of increasing".

(d) $f(n) \sim g(n)$ if

$$\lim_{n\to\infty} \frac{f(n)}{g(n)} = 1.$$

So f and g are asymptotically the same.

Proposition 40. *(a)* $n^\alpha = o(n^\beta)$ *if* $\alpha < \beta$.

(b) $n^c = o(a^n)$ *if* $a > 1$.

(c) $(\ln n)^c = o(n^\alpha)$ *if* $\alpha > 0$

Then there can be defined a partial ordering $f < g$ if $f = o(g)$. So $(\ln n)^c < n^\alpha < a^n$, where $\alpha > 0, a > 1$.

Question 41. *(a) What is the asymptotic behaviour of* $\binom{n}{k}$ *when* $n \to \infty$*?*

(b) Let

$$A_n = \frac{1}{n} + \cdots + \frac{1}{2n}.$$

What is the asymptotic behaviour of $A(n)$*?*

(c) What is the asymptotic behaviour of $n!$ *when* $n \to \infty$*?*

(d) What is $\sum_{k=1}^n k^3$ *asymptotically?*

(e) $a(R)$ *denote the number of the lattice points* (x, y) *of a grid which satisfy* $x^2 + y^2 \le R^2$*. What is* $a(R)$ *asymptotically?*

Binomial coeff.

Proposition 42 (Easy)**.**

$$\left(\frac{n}{k}\right)^k \le \binom{n}{k} \le n^k,$$

$$\frac{2^n}{n+1} \le \binom{n}{\lfloor n/2 \rfloor} \le 2^n.$$

Proposition 43.

$$\binom{n}{k} \le \sum_{i=1}^k \binom{n}{i} \le \left(\frac{en}{k}\right)^k$$

In the depth of the previous proof we can find the Generating Function method.

Proposition 44.

$$\frac{2^{2m}}{2\sqrt{m}} \le \binom{2m}{m} \le \frac{2^2 m}{\sqrt{2m}}.$$

More precisely, $\binom{2m}{m} \sim \frac{2^2 m}{\sqrt{\pi m}}$, by Stirling formula.

Harmonic series

$$H_n = 1 + \frac{1}{2} + \cdots + \frac{1}{n}$$

Proposition 45.

$$\frac{1}{2}\lfloor log_2(n)\rfloor + 1 \leq H_n \leq \lfloor log_2(n)\rfloor + 1.$$

Proposition 46. *A_n bounded and converge.*

Integral method

Theorem 47. *If $f \geq 0$ is monotone increasing function, then*

$$\sum_{i=1}^{N-1} f(i) \leq \int_1^N f(x)dx \leq \sum_{i=2}^{N} f(i).$$

If $f \geq 0$ is monotone decreasing function, then

$$\sum_{i=1}^{N-1} f(i) \geq \int_1^N f(x)dx \geq \sum_{i=2}^{N} f(i).$$

(Think on that what happen if $f \leq 0$.)

Proposition 48. *For $f(x) = 1/x$, we get $\frac{H_n}{\ln n} \to 1$ whenever $n \to \infty$ (i.e: $H_n \sim \ln x$).*

Proposition 49.

$$A_n \to \ln 2,$$

whenever $n \to \infty$.

Factorial function Using the Integral Method we showed the following estimation:

Proposition 50. *For $f(x) = \ln x$ we get*

$$e\Big(\frac{n}{e}\Big)^N \leq N! \leq Ne\Big(\frac{n}{e}\Big)^N.$$

Stirling's formula The precious asymptotic can be given by the Stirling formula:

Theorem 51. *Let $f(n) = \sqrt{2\pi n}(\frac{n}{e})^n$, then $\frac{f(n)}{n!} \to 1$ whenever $n \to \infty$ (i.e. $n! \sim \sqrt{2\pi n}(\frac{n}{e})^n$).*

(Not prove)

Sum of powers We proved using integral method:

Proposition 52.

$$\sum_{i=1}^{n} i^k \sim \frac{n^{k+1}}{k+1}.$$

(Further details see: https://en.wikipedia.org/wiki/Faulhaber%27s_formula)

4. Another type of asymptotic question: By a geometric construction we showed:

Proposition 53.

$$a(R) \sim R^2\pi.$$

10 Inclusion-exclusion principle

Example 54. How many numbers are not divisible by $2, 3, 5$ up to 100? The answer given by the formula:

$$|A \cup B \cup C| = |A| + |B| + |C| - (|A \cap B| + |A \cap C| + |B \cap C|) + |A \cap B \cap C|,$$

where $|A|, |B|, |C|$ are sets.

Generally, it is given a collection of N objects. Each object has one or more properties. We label them by $a_1, \dots, a_r$.

$N(a_i)$ is the number of objects having property a_i.
$N(a_i a_j)$ is the number of objects having properties a_i and a_i.
N_0 the number of objects which has no property.

Theorem 55.

$$N_0 = N - \sum_i N(a_i) + \sum_{i<j} N(a_i, a_j) - \cdots + (-1)^r N(a_1 \dots a_r) \qquad (1)$$

Euler function: $\phi(n)$ is the number of positive integers less, than n that are relatively prime to n.

Proposition 56. *If $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$, then*

$$\phi_n = n - \sum_i \frac{n}{p_i} + \cdots + (-1)^r \frac{n}{p_1 \cdots p_k} = n \prod_{i=1}^{k} \big(1 - \frac{1}{p_i}\big).$$

fixed point free Let π be a permutation of the the set $\{1, 2, \dots, n\}$ We say that π is fixed point free if there is **no** number $1 \geq k \geq n$ such that $\pi(k) = k$.

Proposition 57. *The number of the fixed point free permutations is*

$$n!(1 - \binom{n}{1}(n-1)! + \binom{n}{2}(n-2)! - \cdots + (-1)^{n-1}) =$$
$$n!(1 - 1 + \frac{1}{2!} - \frac{1}{3!} + \dots) \xrightarrow{n \to \infty} \frac{n!}{e}$$

This situation arises in many questions, for instance in the following exercise.

Example 58. There are 5 people in a party. Everybody has a hat, which they took off next to the entrance. After some beer they go home, but that time they do not really care which hat they put on. What is the probability that no one has his own hat?

11 Generating function

11.1 Power series

Let (a_n) be a sequence of real numbers. We say that the form $\sum_{n=1}^{\infty} a_n x^n$ is a power series.
It may converge, may not.

Example 59. (a) Finite power series are polynomials

(b)

$$1 + x + x^2 + \dots + x^n + \dots$$

(c)

$$1 + x + \frac{x^2}{2} + \frac{x^3}{3!} + \dots + \frac{x^n}{n!} + \dots$$

Generally,

$$f(x) = \sum_{i=0}^{\infty} a_n x^n \qquad \text{(Maclaurin series)}$$

$$f(x) = \sum_{i=0}^{\infty} a_n (x-c)^n \qquad \text{(Taylor series)}$$

$f(x)$ is converge for $x = c$ ($x = 0$ i the first case).
If $f(x)$ is converge in any small neighbourhood of c, then there exists an $r \in (0, \infty]$ such that the series converge whenever $|x - c| < r$ and diverge if $|x - c| > r$. This r is called the convergence radius of f in c.

C-H thm. The radius r can be given by (a_n).

Theorem 60 (Cauchy-Hadamard theorem)**.**

$$r = \liminf_{n\to\infty} \frac{1}{\sqrt[n]{|a_n|}}$$

Most of our cases the limit exists, then $r = \lim_{n\to\infty} \frac{1}{\sqrt[n]{|a_n|}}$.(Examples again.)
We do not know only from this theorem what happens on the boundary $|x - c| = r$ (Further analysis needed).
(Absolute convergence, uniform convergence)

Operation Let us assume that $f(x) = \sum_{n=1}^{\infty} a_n (x-c)^n$ and $g(x) = \sum_{n=1}^{\infty} b_n (x-c)^n$

(a) Then

$$f(x) \pm g(x) = \sum_{n=1}^{\infty} (a_n \pm b_n)(x-c)^n.$$

(b)

$$f(x)\cdot g(x) = (\sum_{n=1}^{\infty} a_n(x-c)^n)(\sum_{n=1}^{\infty} b_n(x-c)^n) = \sum_{n=1}^{\infty}(\sum_{i=0}^{n} a_i\cdot b_{n-i})(x-c)^n.$$

(c) f is differentiable, f' has the same radius r and

$$f'(x) = \sum_{n=1}^{\infty} n a_n (x-c)^{n-1} = \sum_{n=0}^{\infty} a_{n+1}(n+1)(x-c)^n.$$

(d) f is integrable, $\int f(x)dx$ has the same radius r and

$$\int f(x)dx = \sum_{n=0}^{\infty} \frac{a_n(x-c)^{n+1}}{n+1} + C = \sum_{n=1}^{\infty} \frac{a_{n-1}(x-c)^n}{n} + C.$$

Taylor-series Now we start with function f and we would like to find out the coefficient a_n such that

$$f(x) = \sum_{n=0}^{\infty} a_n(x-c)^n$$

Theorem 61. *If f is the differentiable (around c) infinitely many times, then*

$$f(x) = \sum_{n=1}^{n} \frac{f^{(n)}(c)}{n!}(x-c)^n.$$

So $a_n = \frac{f^{(n)}(c)}{n!}$.

And if $r > 0$ then $f(x) =$ its Taylor series in $|x-c| < r$.

Remark 62. (a) Polynomials

(b) Good approximation

Examples again.

Theorem 63 (Generalized binomial theorem)**.**

$$(1+x)^\alpha = \sum_{n=0}^{\infty} \binom{\alpha}{n} x^n \quad (\forall |x| < 1, \alpha \in \mathbb{R},$$

where $\binom{\alpha}{n} = \frac{\alpha(\alpha-1)\dots(\alpha-n+1)}{n!}$

Examples: $(1+x)^{1/2}$, $(1+x)^3$.

Let $(a_0, a_1, a_2, \dots)$ be a sequence of real numbers. If a_n is not growing 'too fast', then $a(x) = a_0 + a_1 x + a_2 x^2 + \dots$ is a well defined function in the neighborhood of 0.

Proposition 64. *Let $(a_0, a_1, a_2, \dots)$ be a sequence of reals, and let us assume that for some real numbers K, we have $|a_n| \le K^n \;\; \forall a_n \ge 1$. Then for every $x \in (-\frac{1}{K}, \frac{1}{K})$, $a(x) = \sum_{i=0}^{\infty} a_i x^i$ converges (even absolutely). Moreover: The values of the function $a(x)$ on any small neighborhood of 0 determine the whole sequence $(a_0, a_1, a_2, \dots)$. (Uniqueness)*

We call this $a(x)$ the generating function (gen. function) of (a_n).

Operations Let $a(x)$ and $b(x)$ be the generating functions of $(a_0, a_1, a_2, \dots)$ and $(b_0, b_1, b_2, \dots)$, respectively

(a) Summation:
$a(x) + b(x)$ be the gen. function of $(a_0 + b_0, a_1 + b_1, a_2 + b_2, \dots)$.

(b) Multiplication with fixed reals:
For any $\alpha \neq 0$ $\alpha \cdot a(x)$ is the gen. function of $(\alpha a_0, \alpha a_1, \alpha a_2, \dots)$.

(c) Shift to the right:
For any natural number n, $x^n a(x)$ is the gen. function of $(\underbrace{0, \dots, 0}_{n}, a_0, a_1, \dots)$

(d) Shift to the left:
For the sequence $(a_n, a_{n+1}, \dots)$ the gen. function is

$$\frac{a(x) - (a_0 + \cdots + a_{n-1}x^{n-1})}{x^n}.$$

(e) Substitution 1.:
We can put αx instead of x:
$c(x) = a(\alpha x)$ is the gen. function of $(a_0, \alpha a_1, \alpha^2 a_2, \dots)$. (examples)

(f) Substitution 2.:
We can put x^n instead of x:
The $n \cdot k$th term equal the original sequence kth term.
So $d(x) = a(x^n)$ is the gen. function of

$$(a_0, \underbrace{0, \dots, 0}_{n-1}, a_1, \underbrace{0, \dots, 0}_{n-1}, a_2, \dots).$$

(examples)

(g) Differentiation and integration:
$a'(x)$ is the gen. function of $(a_1, 2a_2, 3a_3, \dots)$ and
$\int_0^x a(t)dt$ is the gen. function of $(0, a_0, \frac{1}{2}a_1, \frac{1}{3}a_2, \dots)$ (examples)

(h) Product:
$a(x)b(x) = c(x)$ is the gen. function of $(c_0, c_1, c_2, \dots)$, where

$$c_k = \sum_{i,j \geq 0, i+j=k} a_i b_j.$$

11.2 Application

List of application:

(a) There are 30 red, 40 blue, 50 white balls, the same colors are distinguishable. How many ways are there of selection of 70 balls?

(b) Fibonacci numbers, golden ratio, Linear recursion;

(c) Catalan numbers;

(d) Probability theory:
Example: Average value of a non-negative, integer valued distribution.

(e) Integer partitions

11.3 Linear recursion, Fibonacci numbers

We calculate the generating function and separate it with partial rational functions. Calculate the coefficients.
OR
Calculate the characteristic polynomial coming from the recursion and count the roots of it.
Example: $a_n = Aa_{n-1} + Ba_{n-2}$ and a_0 and a_1 are given real numbers (A, B are also reals). Both method gives us to calculate the roots of the following polynomial:

$$x^2 - Ax - B = 0.$$

(a) If the roots λ_1, λ_2 are different and reals, then easily the solution is the linear combination of the roots: $a_n = c_1\lambda_1^n + c_2\lambda_2^n$ for some c_1, c_2. Using substitution $n = 0$ and 1 and the fact that a_0, a_1 is given we can calculate c_1, c_2.

(b) If some roots are the same, say $\lambda = \lambda_1 = \lambda_2$, then the member of the recursion (a_n) can be given as a linear combination of the form: $a_n = c_1 \cdot \lambda^n + c_2 \cdot n \cdot \lambda^n$. Using the same argument as in (a) we can calculate c_1, c_2.

(c)* If the roots are complex then the roots are conjugates, $\lambda_1 = \overline{\lambda_2}$. Then the roots can be written in the trigonometric form:

$$\lambda_1 = r(\cos(\phi) + i \cdot \sin(\phi)), \lambda_2 = r(\cos(\phi) - i \cdot \sin(\phi)),$$

and

$$\lambda_1^n = r^n(\cos(n \cdot \phi) + i \cdot \sin(n \cdot \phi)), \lambda_2^n = r^n(\cos(n \cdot \phi) - i \cdot \sin(n \cdot \phi)).$$

The equation $a_n = c_1\lambda_1^n + c_2\lambda_2^n$ gives a solution for the recursion and we can calculate c_1, c_2 by substituting for $n = 1, 2$, again. (Generally, c_1 and c_2 are also complex numbers.)

11.4 Catalan numbers

(Algebraic generator function method):

$$c_n = \sum_{i=0}^{n-1} c_0 \cdot c_{n-1} + c_1 \cdot c_{n-2} + \ldots c_{n-1} \cdot c_0,$$

and $c_0 = 1, c_1 = 1$.
The generating function is

$$C(x) = c_0 + c_1x + \cdots + c_nx^n + \ldots.$$

It satisfies the following equation (check that):

$$xC^2(x) + C(x) + c_0 = 0.$$

Thus

$$C(x) = \frac{1 \pm \sqrt{1-4x}}{2x},$$

this converge if $|x| < 1/4$ and $\pm$ must be $-$ since every $c_i > 0$, so for small x the function $C(x)$ is converging and monotone increasing. By the general binomial theorem:

$$(1-4x)^{\frac{1}{2}} = \sum_{n=0}^{\infty} \binom{1/2}{n} (-4x)^n.$$

$$\begin{aligned} \binom{1/2}{n} = \frac{(1/2)(-1/2)(-3/2)\dots(-(2n-3)/2)}{n!} &= \frac{1}{2^n}(-1)^{n-1}\frac{1\cdot 3\cdot\dots(2n-3)}{n!} = \\ \frac{(-1)^{n-1}\big(1\cdot 3\cdot\dots(2n-3)\big)\big(2\cdot 4\cdot\dots(2n-2)\big)}{\big(2^n\cdot n!\big)\big(2^{n-1}\cdot(n-1)!\big)} &= \frac{(-1)^{n-1}}{2^{2n-1}}\binom{2(n-1)}{n-1}\frac{1}{n}. \end{aligned}$$

Thus

$$(1-4x)^{\frac{1}{2}} = \sum_{n=0}^{\infty}\binom{1/2}{n}(-4x)^n = 1 + \sum_{n=1}^{\infty}\frac{(-1)^{n-1}}{2^{2n-1}}\binom{2(n-1)}{n-1}\frac{1}{n}4^n(-1)^n x^n = 1 - \sum_{n=1}^{\infty}\frac{2}{n}\binom{2(n-1)}{n-1}x^n.$$

We get

$$C(x) = \frac{1-(1-\sum_{n=1}^{\infty}\frac{2}{n}\binom{2(n-1)}{n-1}x^n)}{2x} = \sum_{n=1}^{\infty}\frac{1}{n}\binom{2(n-1)}{n-1}x^{n-1} = \sum_{n=0}^{\infty}\frac{1}{n+1}\binom{2n}{n}x^n.$$

By the uniqueness of the generating function $c_n = \frac{1}{n+1}\binom{2n}{n}$.

11.5 Probability theory

Let $(p_0, p_1, \dots)$ be a distribution on $\mathbb{N}$ $(\sum_{i=0}^{\infty} p_i = 0)$. We denote

$$G(x) = p_0 + p_1 x + p_2 x^2 + \cdot$$

the generating function of the distribution.

Proposition 65. *For every distribution $(p_1, p_2, \dots)$ and X be realization of a choice according to the distribution. Then*

$$G'(1) = E(X) = \sum_{i=1}^{\infty} i \cdot p_i.$$

Example 66. If we role with two dice. The average of the sum of the dices is 7.
The average time to get 1 as a result of a role with one dice is 6.

11.5.1 Making dice*

Can we write non-negative integers on the sides of two dices such that the probability of the sum of them is the same as the sum of two 'normal dices'? (The dices could be fake.):
We role any number with probability 1/6 in a normal dice. So we can say that it has a generating function:

$$g(x) = 1/6x + \cdots + 1/6x^6.$$

If we role with two dices:

$$g(x)^2 = (1/6(x + \cdots + x^6))^2$$

It is not hard to see that it is equal:

$$(1/6)^2 x^2 (x+1)^2 (x^2 - x + 1)^2 (x^2 + x + 1)^2).$$

Now we would like to make the two dice with at most 6 sides and in every side can be written a nonnegative integer number. In our language we need to separate these factors into two parts such that the product of each part has at most 6 nonnegative integer coefficients.

After some calculation we can find that it can happen only if

$$(x+1)^2(x^2 - x + 1)^2 = x^6 + 2x^3 + 1,$$

$$x^2(x^2 + x + 1)^2 = x^6 + 2x^5 + 3x^4 + 2x^3 + x^2.$$

How can we get dices from this result?

11.6 Integer partitions*

The main idea about integer partitions is the following. Find a 'nice' bijection on the class of the partitions and you get an identity for integer partitions. Now we present some methods for finding this type of results:

Merging process: If there are two sets with the same size in an integer partition then we substitute them with one set of double size.

Splitting process: If there is an even set in an integer partition the split them into two equal part. For instance the following statement can be proved by the use of splitting-merging process.

Proposition 67. *(Euler's identity) Every number has as many integer partitions into odd parts as into distinct parts parts.*

If we fits the process for Fibonacci numbers for instance: Merge two consecutive one, split a Fibonacci number by two smaller one.

Proposition 68. *Every number can be written* **uniquely** *as a sum of some non-consecutive Fibonacci numbers.*

Ferrer's diagram In the next link you can find what was mentioned mainly on the class.
$https://en.wikipedia.org/wiki/Partition\_(number\_theory)$
Here also you can see more the an example for the use of generating function method.

12 Impartial game theory

This lecture have been sent in an independent file.