universität innsbruck

Discrete structures

Manuel Eberl
Jan Jakubuv
Jamie Hochrainer
Cezary Kaliszyk

http://cl-informatik.uibk.ac.at/

Summary last week

- using induction on well-founded relations to prove properties
- lexicographic product $(x_1, x_2) \leq_1 \times_{\text{lex}} \leq_2 (y_1, y_2)$ if $x_1 <_1 y_1$ or ($x_1 = y_1$, $x_2 \leq_2 y_2$)
- preserves well-foundedness of partial orders $\leq_1, \leq_2$

Summary last week

- using induction on well-founded relations to prove properties
- lexicographic product $(x_1, x_2) \leq_1 \times_{\text{lex}} \leq_2 (y_1, y_2)$ if $x_1 <_1 y_1$ or $(x_1 = y_1, x_2 \leq_2 y_2)$
- preserves well-foundedness of partial orders $\leq_1, \leq_2$
- dags as directed acyclic graphs
- topological $\leq$-sorting $(a_0, \ldots, a_n)$ of partial order $\leq$ on $\{a_0, \ldots, a_n\}$: $i < j$ if $a_i < a_j$.
- topological sorting algorithm by repeated selection of $\leq$-minimal element
- O(n) shortest/longest path algorithm on dags based on topological sorting

Summary last week

- using induction on well-founded relations to prove properties
- lexicographic product $(x_1, x_2) \leq_1 \times_{\text{lex}} \leq_2 (y_1, y_2)$ if $x_1 <_1 y_1$ or ($x_1 = y_1$, $x_2 \leq_2 y_2$)
- preserves well-foundedness of partial orders $\leq_1, \leq_2$
- dags as directed acyclic graphs
- topological $\leq$-sorting $(a_0, \ldots, a_n)$ of partial order $\leq$ on $\{a_0, \ldots, a_n\}$: $i < j$ if $a_i < a_j$.
- topological sorting algorithm by repeated selection of $\leq$-minimal element
- O(n) shortest/longest path algorithm on dags based on topological sorting
- forests as dags with nodes of in-degree ≤ 1
- trees as forests where pairs of nodes have common ancestors
- rooted trees as trees having a root (ancestor of all nodes)
- for trees, number of vertices $=$ number of edges $+1$

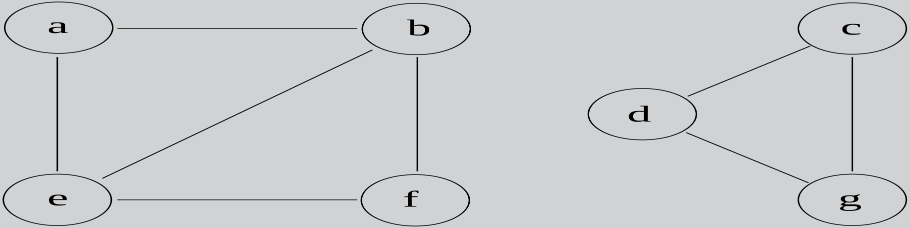
- undirected multigraph
- vertex *c* is a neighbour of the vertex *d*, if there exists an edge joining both
- loop, parallel edges
- the degree of a vertex *v* is the number of edges having *v* as endpoint
- undirected graph, sub-multigraph, sub-graph
- paths, cycles

Definition

- Let G be an undirected multigraph
- A sub-graph G' of G is a spanning forest of G, if
  1. G is a forest, and
  2. the partitionings of G resp. G' into connected components are the same.
- Then $V' = V$

Example

The following graph has $8 \cdot 3 = 24$ spanning forests



Course themes

- directed and undirected graphs
- relations and functions
- orders and induction
- trees and dags
- finite and infinite counting
- elementary number theory
- Turing machines, algorithms, and complexity
- decidable and undecidable problem

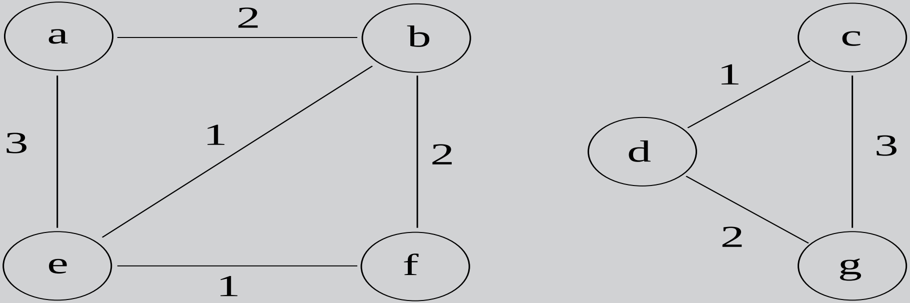
Theorem (Kruskal's algorithm)

1. *Let $G = (V, E)$ be an undirected multigraph with weights b*
2. *We want to construct a partitioning of V into connected components, and a set of edges F that constitutes a spanning forest of G having minimal weight $\sum_{e \in F} b(e)$*
3. *We preprocess G by removing all loops and all parallel edges except for a single one of least weight, and sorting those such that $b(e_0) \leqslant b(e_1) \leqslant \ldots \leqslant b(e_{m-1})$*
4. *The algorithm then proceeds as follows, with complexity $\mathrm{O}(\#(V) \cdot \#(E))$*

> *Set $F = \varnothing$ and $P = \{\{v\} \mid v \in V\}$*
> *For i from 0 to $m - 1$ repeat:*
>   *if the nodes v and u of e_i are in distinct blocks of P,*
>   *combine both blocks of P and adjoin e_i to F*

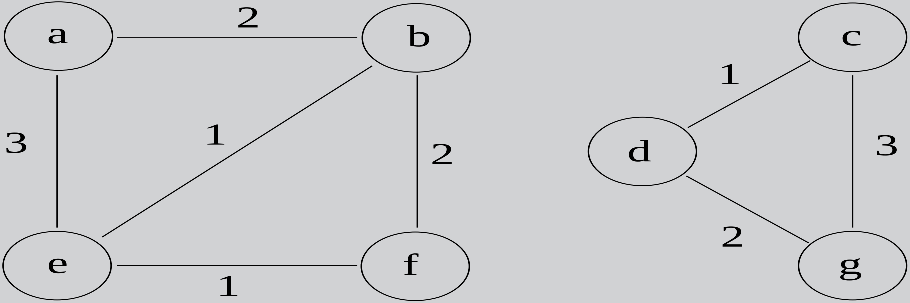
Example

For the weighted graph



Example

For the weighted graph



Kruskal's algorithm starts with $F = \varnothing$; $P = \{\{a\}, \{b\}, \{c\}, \{d\}, \{e\}, \{f\}, \{g\}\}$ and terminates with

$$F = \{\{a, b\}, \{b, e\}, \{c, d\}, \{d, g\}, \{e, f\}\}$$
$$P = \{\{a, b, e, f\}, \{c, d, g\}\}$$

Proof.

- Let G_i be the sub-graph of G with V as nodes and edges $\{e_0, e_1, , \ldots, e_i\}$

Proof.

- Let G_i be the sub-graph of G with V as nodes and edges $\{e_0, e_1, , \ldots, e_i\}$
- The algorithm starts with partitioning into singletons of nodes and then proceeds by combining blocks by edges connecting them

Proof.

- Let G_i be the sub-graph of G with V as nodes and edges $\{e_0, e_1, , \ldots, e_i\}$
- The algorithm starts with partitioning into singletons of nodes and then proceeds by combining blocks by edges connecting them
- After step i, P is a partitioning of G_i into connected components

Proof.

- Let G_i be the sub-graph of G with V as nodes and edges $\{e_0, e_1, , \ldots, e_i\}$
- The algorithm starts with partitioning into singletons of nodes and then proceeds by combining blocks by edges connecting them
- After step i, P is a partitioning of G_i into connected components
- Initially, the set F is empty, and in step i it is extended by a connecting edge whose endpoints are in the combined block.

Proof.

- Let G_i be the sub-graph of G with V as nodes and edges $\{e_0, e_1, , \ldots, e_i\}$
- The algorithm starts with partitioning into singletons of nodes and then proceeds by combining blocks by edges connecting them
- After step i, P is a partitioning of G_i into connected components
- Initially, the set F is empty, and in step i it is extended by a connecting edge whose endpoints are in the combined block.
- For every block B, the sub-graph restricted to nodes B and the corresponding edges in F, is a tree

Proof.

- Let G_i be the sub-graph of G with V as nodes and edges $\{e_0, e_1, , \ldots, e_i\}$
- The algorithm starts with partitioning into singletons of nodes and then proceeds by combining blocks by edges connecting them
- After step i, P is a partitioning of G_i into connected components
- Initially, the set F is empty, and in step i it is extended by a connecting edge whose endpoints are in the combined block.
- For every block B, the sub-graph restricted to nodes B and the corresponding edges in F, is a tree
- Therefore, after step i, the sub-graph having nodes V and edges F is a spanning forest of G_i

Proof.

- Let G_i be the sub-graph of G with V as nodes and edges $\{e_0, e_1, , \ldots, e_i\}$
- The algorithm starts with partitioning into singletons of nodes and then proceeds by combining blocks by edges connecting them
- After step i, P is a partitioning of G_i into connected components
- Initially, the set F is empty, and in step i it is extended by a connecting edge whose endpoints are in the combined block.
- For every block B, the sub-graph restricted to nodes B and the corresponding edges in F, is a tree
- Therefore, after step i, the sub-graph having nodes V and edges F is a spanning forest of G_i
- We show that the greedy strategy employed, yields a spanning forest of minimal weight

Proof (continued).

- Let F' be the set of edges of a spanning forest of minimal weight, and suppose $F' \neq F$; then there exists an edge e_i in F not in F'.

Proof (continued).

- Let F' be the set of edges of a spanning forest of minimal weight, and suppose $F' \neq F$; then there exists an edge e_i in F not in F'.
- Let v_1, v_2 be the endpoints of e_i and V_1, V_2 the corresponding blocks in the algorithm

Proof (continued).

- Let F' be the set of edges of a spanning forest of minimal weight, and suppose $F' \neq F$; then there exists an edge e_i in F not in F'.
- Let v_1, v_2 be the endpoints of e_i and V_1, V_2 the corresponding blocks in the algorithm
- Since there is a path p from v_1 to v_2 with edges in F', there exists an edge e_j in the path p having one endpoint in V_1 and the other endpoint not in it. Hence, $j > i$ and $b(e_j) \geq b(e_i)$.

Proof (continued).

- Let F' be the set of edges of a spanning forest of minimal weight, and suppose $F' \neq F$; then there exists an edge e_i in F not in F'.
- Let v_1, v_2 be the endpoints of e_i and V_1, V_2 the corresponding blocks in the algorithm
- Since there is a path p from v_1 to v_2 with edges in F', there exists an edge e_j in the path p having one endpoint in V_1 and the other endpoint not in it. Hence, $j > i$ and $b(e_j) \geq b(e_i)$.
- The sub-graph with nodes V and edges defined by $E' := (F' \setminus \{e_j\}) \cup \{e_i\}$ then is a spanning tree, because every path via e_j can be transformed into one via e_i and the other edges of p and vice versa; moreover that sub-graph has minimal weight.

Proof (continued).

- Let F' be the set of edges of a spanning forest of minimal weight, and suppose $F' \neq F$; then there exists an edge e_i in F not in F'.
- Let v_1, v_2 be the endpoints of e_i and V_1, V_2 the corresponding blocks in the algorithm
- Since there is a path p from v_1 to v_2 with edges in F', there exists an edge e_j in the path p having one endpoint in V_1 and the other endpoint not in it. Hence, $j > i$ and $b(e_j) \geq b(e_i)$.
- The sub-graph with nodes V and edges defined by $E' := (F' \setminus \{e_j\}) \cup \{e_i\}$ then is a spanning tree, because every path via e_j can be transformed into one via e_i and the other edges of p and vice versa; moreover that sub-graph has minimal weight.
- by finitely many such exchanges we obtain F from F'

Proof (continued).

- Let F' be the set of edges of a spanning forest of minimal weight, and suppose $F' \neq F$; then there exists an edge e_i in F not in F'.
- Let v_1, v_2 be the endpoints of e_i and V_1, V_2 the corresponding blocks in the algorithm
- Since there is a path p from v_1 to v_2 with edges in F', there exists an edge e_j in the path p having one endpoint in V_1 and the other endpoint not in it. Hence, $j > i$ and $b(e_j) \geq b(e_i)$.
- The sub-graph with nodes V and edges defined by $E' := (F' \setminus \{e_j\}) \cup \{e_i\}$ then is a spanning tree, because every path via e_j can be transformed into one via e_i and the other edges of p and vice versa; moreover that sub-graph has minimal weight.
- by finitely many such exchanges we obtain F from F'
- Since F' has a minimal weight, so has F

Proof (continued).

- Let F' be the set of edges of a spanning forest of minimal weight, and suppose $F' \neq F$; then there exists an edge e_i in F not in F'.
- Let v_1, v_2 be the endpoints of e_i and V_1, V_2 the corresponding blocks in the algorithm
- Since there is a path p from v_1 to v_2 with edges in F', there exists an edge e_j in the path p having one endpoint in V_1 and the other endpoint not in it. Hence, $j > i$ and $b(e_j) \geq b(e_i)$.
- The sub-graph with nodes V and edges defined by $E' := (F' \setminus \{e_j\}) \cup \{e_i\}$ then is a spanning tree, because every path via e_j can be transformed into one via e_i and the other edges of p and vice versa; moreover that sub-graph has minimal weight.
- by finitely many such exchanges we obtain F from F'
- Since F' has a minimal weight, so has F ∎

Cardinals

Motivation/intuition

Capture cardinals as in counting: e.g. 1, 2, 100.
(only number no order)

Cardinals

Motivation/intuition

Capture cardinals as in counting: e.g. 1, 2, 100.
(only number no order)

Definition

If there exists a bijection $f : M \to N$, then the sets M and N are equinumerous (or equipollent, equipotent). Cardinals represent equinumerous sets.

Example

Each finite set equinumerous to set $\{m \mid m < n\}$ for some $n \in \mathbb{N}$.

Example

$\mathbb{N} \cup \{*\}$ is equinumerous to $\mathbb{N}$; witnessed by bijection f mapping $*$ to 0, and n to $n + 1$.

Definition

- set A is finite if there exist $n \in \mathbb{N}$ and bijective function $e\colon \{0, 1, \ldots, n-1\} \to A$
- then n is unique, denoted by $\#(A) := n$, and called the number or cardinality of A
- the function e is in general not unique, and is called an enumeration of A
- a bijection $\nu\colon A \to \{0, 1, \ldots, m-1\}$ is called a numbering of A
- an inverse of an enumeration is a numbering and vice versa
- A is infinite if it is not finite, and then we write $\#(A) = \infty$

Cardinalities for operations on finite sets

Lemma

Let $e : \{0, \dots, m-1\} \to A$ *and* $f : \{0, \dots, n-1\} \to B$ *be enumerations of A,B.*

1. $\#(\emptyset) = 0$

Cardinalities for operations on finite sets

Lemma

Let $e : \{0, \ldots, m-1\} \to A$ *and* $f : \{0, \ldots, n-1\} \to B$ *be enumerations of A,B.*

1. $\#(\emptyset) = 0$
2. $\#(\{a\}) = 1$

Cardinalities for operations on finite sets

Lemma

Let $e : \{0, \ldots, m-1\} \to A$ *and* $f : \{0, \ldots, n-1\} \to B$ *be enumerations of A,B.*

1. $\#(\emptyset) = 0$
2. $\#(\{a\}) = 1$
3. $\#(A \times B) = \#(A) \cdot \#(B) = m \cdot n$

Cardinalities for operations on finite sets

Lemma

Let $e : \{0, \ldots, m-1\} \to A$ *and* $f : \{0, \ldots, n-1\} \to B$ *be enumerations of* A,B.

1. $\#(\emptyset) = 0$
2. $\#(\{a\}) = 1$
3. $\#(A \times B) = \#(A) \cdot \#(B) = m \cdot n$
4. $\#(A \cup B) = \#(A) + \#(B) = m + n$, *if* $A \cap B = \emptyset$

Cardinalities for operations on finite sets

Lemma

Let $e : \{0, \ldots, m-1\} \to A$ *and* $f : \{0, \ldots, n-1\} \to B$ *be enumerations of A,B.*

1. $\#(\emptyset) = 0$
2. $\#(\{a\}) = 1$
3. $\#(A \times B) = \#(A) \cdot \#(B) = m \cdot n$
4. $\#(A \cup B) = \#(A) + \#(B) = m + n$, *if* $A \cap B = \emptyset$
5. $\#(A^B) = \#(A)^{\#(B)} = m^n$, *for* A^B *the set of functions from B to A*

Cardinalities for operations on finite sets

Proof.

1. the empty set $\emptyset$ (of pairs) is a bijection from $\emptyset$ to $\emptyset$.

Cardinalities for operations on finite sets

Proof.

1. the empty set $\emptyset$ (of pairs) is a bijection from $\emptyset$ to $\emptyset$.
2. mapping 0 to a is a bijection from $\{0\}$ to $\{a\}$.

Cardinalities for operations on finite sets

Proof.

1. the empty set $\emptyset$ (of pairs) is a bijection from $\emptyset$ to $\emptyset$.
2. mapping 0 to a is a bijection from $\{0\}$ to $\{a\}$.
3. mapping k to $(e(k \div n), f(k \bmod n))$ is a bijection from $\{0, \ldots, m \cdot n - 1\}$ to $A \times B$, with inverse numbering given by $(a, b) \mapsto e^{-1}(a) \cdot n + f^{-1}(b)$.

Cardinalities for operations on finite sets

Proof.

1. the empty set $\emptyset$ (of pairs) is a bijection from $\emptyset$ to $\emptyset$.
2. mapping 0 to a is a bijection from $\{0\}$ to $\{a\}$.
3. mapping k to $(e(k \div n), f(k \bmod n))$ is a bijection from $\{0, \ldots, m \cdot n - 1\}$ to $A \times B$, with inverse numbering given by $(a, b) \mapsto e^{-1}(a) \cdot n + f^{-1}(b)$.
4. mapping k to $e(k)$ if $k < m$ and to $f(k - m)$ otherwise, is a bijection from $\{0, \ldots, m + n - 1\}$ to $A \cup B$, with inverse numbering given by $c \mapsto e^{-1}(c)$ if $c \in A$ and $c \mapsto f^{-1}(c) + m$ if $c \in B$.

Cardinalities for operations on finite sets

Proof.

1. the empty set $\emptyset$ (of pairs) is a bijection from $\emptyset$ to $\emptyset$.
2. mapping 0 to a is a bijection from $\{0\}$ to $\{a\}$.
3. mapping k to $(e(k \div n), f(k \bmod n))$ is a bijection from $\{0, \dots, m \cdot n - 1\}$ to $A \times B$, with inverse numbering given by $(a, b) \mapsto e^{-1}(a) \cdot n + f^{-1}(b)$.
4. mapping k to $e(k)$ if $k < m$ and to $f(k - m)$ otherwise, is a bijection from $\{0, \dots, m + n - 1\}$ to $A \cup B$, with inverse numbering given by $c \mapsto e^{-1}(c)$ if $c \in A$ and $c \mapsto f^{-1}(c) + m$ if $c \in B$.
5. writing $k \in \{0, \dots, m^n - 1\}$ as $k_{n-1} \dots k_0$ in base-m, mapping it to the function $g : B \to A$ that maps for $0 \leq i < n$, $f(i)$ to $e(k_i)$ is a bijection to A^B, with inverse numbering of elements of A^B given by mapping a function $g : B \to A$ to the number $\sum_{b \in B} f^{-1}(g(b)) m^{e^{-1}(b)}$ in $\{0, \dots, m^n - 1\}$.

Cardinalities for operations on finite sets

Proof.

1. the empty set $\emptyset$ (of pairs) is a bijection from $\emptyset$ to $\emptyset$.
2. mapping 0 to a is a bijection from $\{0\}$ to $\{a\}$.
3. mapping k to $(e(k \div n), f(k \bmod n))$ is a bijection from $\{0, \ldots, m \cdot n - 1\}$ to $A \times B$, with inverse numbering given by $(a, b) \mapsto e^{-1}(a) \cdot n + f^{-1}(b)$.
4. mapping k to $e(k)$ if $k < m$ and to $f(k - m)$ otherwise, is a bijection from $\{0, \ldots, m + n - 1\}$ to $A \cup B$, with inverse numbering given by $c \mapsto e^{-1}(c)$ if $c \in A$ and $c \mapsto f^{-1}(c) + m$ if $c \in B$.
5. writing $k \in \{0, \ldots, m^n - 1\}$ as $k_{n-1} \ldots k_0$ in base-m, mapping it to the function $g : B \to A$ that maps for $0 \leq i < n$, $f(i)$ to $e(k_i)$ is a bijection to A^B, with inverse numbering of elements of A^B given by mapping a function $g : B \to A$ to the number $\sum_{b \in B} f^{-1}(g(b)) m^{e^{-1}(b)}$ in $\{0, \ldots, m^n - 1\}$.
   Writing $B = \{b_0, \ldots, b_{n-1}\}$, then $g : B \to A$ is uniquely determined by the tuple $(g(b_i))_{i=0}^{n-1}$ in B^m.

∎

Derived cardinalities for operations, inclusion/exclusion

Theorem

1. *If, for finite sets A and B there is a bijection $f : A \to B$, then* $\#(A) = \#(B)$

Derived cardinalities for operations, inclusion/exclusion

Theorem

1. *If, for finite sets A and B there is a bijection* $f: A \to B$*, then* $\#(A) = \#(B)$
2. *For pairwise disjoint sets* $A_1, A_2, \ldots, A_k$

$$\#(\bigcup_{i=1}^{k} A_k) = \#(A_1 \cup A_2 \cup \ldots \cup A_k) = \#(A_1) + \#(A_2) + \ldots + \#(A_k) = \sum_{i=1}^{k} \#(A_i)\,.$$

Derived cardinalities for operations, inclusion/exclusion

Theorem

1. *If, for finite sets A and B there is a bijection $f: A \to B$, then $\#(A) = \#(B)$*
2. *For pairwise disjoint sets $A_1, A_2, \ldots, A_k$*

$$\#(\bigcup_{i=1}^{k} A_k) = \#(A_1 \cup A_2 \cup \ldots \cup A_k) = \#(A_1) + \#(A_2) + \ldots + \#(A_k) = \sum_{i=1}^{k} \#(A_i) .$$

3. *For finite sets A and B,*

$$\#(A - B) = \#(A \setminus B) = \#(A) - \#(A \cap B) .$$

Proof.

(1) A is finite, hence by definition there are a natural number m and a bijection $e\colon \{0, 1, \ldots, m-1\} \to A$.

Proof.

(1) A is finite, hence by definition there are a natural number m and a bijection $e\colon \{0, 1, \ldots, m-1\} \to A$.

Then consider the function composition

$$f \circ e\colon \{0, 1, \ldots, m-1\} \to B\ ,\ i \mapsto f(e(i))\,,$$

Proof.

(1) A is finite, hence by definition there are a natural number m and a bijection $e\colon \{0, 1, \ldots, m-1\} \to A$.

Then consider the function composition

$$f \circ e\colon \{0, 1, \ldots, m-1\} \to B \ , \ i \mapsto f(e(i)) \, ,$$

$f \circ e$ is bijective, therefore $\#(B) = m$

Proof.

(1) A is finite, hence by definition there are a natural number m and a bijection $e\colon \{0, 1, \ldots, m-1\} \to A$.

Then consider the function composition

$$f \circ e\colon \{0, 1, \ldots, m-1\} \to B\ ,\ i \mapsto f(e(i))\,,$$

$f \circ e$ is bijective, therefore $\#(B) = m$

(3) Because we have for arbitrary sets that

$$A = (A \setminus B) \cup (A \cap B)$$

with the union disjoint, it follows by (2) that

$$\#(A \setminus B) = \#(A) - \#(A \cap B)$$

Proof.

(2) Given bijections

$$e_1\colon \{0,1,\ldots,m_1-1\} \to M_1, \ldots, e_k\colon \{0,1,\ldots,m_k-1\} \to M_k$$

their composition $e\colon \{0,1,\ldots,m_1+\ldots+m_k-1\} \to M_1 \cup \ldots \cup M_k$ is again a bijection

$$i \mapsto \begin{cases} e_1(i) & i \in \{0,1,\cdots,m_1-1\} \\ e_2(i-m_1) & i \in \{m_1,\cdots,m_1+m_2-1\} \\ \vdots & \vdots \\ e_k(i-m_1-\ldots-m_{k-1}) & i \in \{m_1+\ldots+m_{k-1},\cdots,m_1+\ldots+m_k-1\} \end{cases}$$

Proof.

(2) Given bijections

$$e_1\colon \{0,1,\dots,m_1-1\} \to M_1, \dots, e_k\colon \{0,1,\dots,m_k-1\} \to M_k$$

their composition $e\colon \{0,1,\dots,m_1+\ldots+m_k-1\} \to M_1 \cup \ldots \cup M_k$ is again a bijection

$$i \mapsto \begin{cases} e_1(i) & i \in \{0,1,\cdots,m_1-1\} \\ e_2(i-m_1) & i \in \{m_1,\cdots,m_1+m_2-1\} \\ \vdots & \vdots \\ e_k(i-m_1-\ldots-m_{k-1}) & i \in \{m_1+\ldots+m_{k-1},\cdots,m_1+\ldots+m_k-1\} \end{cases}$$

∎

Theorem

4 *Inclusion/exclusion principle*

For finite sets $A_1, A_2, \ldots, A_k$

$$\#(\bigcup_{i=1}^{k} A_i) =$$

In particular,

$\#(A \cup B) = \#(A) + \#(B) - \#(A \cap B)$

Theorem

4 *Inclusion/exclusion principle*

For finite sets $A_1, A_2, \ldots, A_k$

$$\#\left(\bigcup_{i=1}^{k} A_i\right) = \left(\sum_{I \subseteq \{1,\ldots,k\},\ \#(I)\ odd} \#\left(\bigcap_{i\in I} A_i\right)\right) - \left(\sum_{I \subseteq \{1,\ldots,k\},\ \#(I)\ even} \#\left(\bigcap_{i\in I} A_i\right)\right)$$

In particular,

$\#(A \cup B) = \#(A) + \#(B) - \#(A \cap B)$

Theorem

4 *Inclusion/exclusion principle*

For finite sets $A_1, A_2, \ldots, A_k$

$$\#\left(\bigcup_{i=1}^{k} A_i\right) = \sum_{\substack{I \subseteq \{1,2,\ldots,k\} \\ I \neq \emptyset}} (-1)^{\#(I)-1} \, \#\left(\bigcap_{i \in I} A_i\right)$$

In particular,

$\#(A \cup B) = \#(A) + \#(B) - \#(A \cap B)$

Theorem

4. *Inclusion/exclusion principle*
   For finite sets $A_1, A_2, \ldots, A_k$

$$\#(\bigcup_{i=1}^{k} A_i) = \sum_{\substack{I \subseteq \{1,2,\ldots,k\} \\ I \neq \varnothing}} (-1)^{\#(I)-1} \#(\bigcap_{i \in I} A_i)$$

   In particular,
   $\#(A \cup B) = \#(A) + \#(B) - \#(A \cap B)$

5. *Let* $M_1, M_2, \ldots, M_k$ *be finite sets. Then cardinality of their Cartesian product, is the product of their cardinalities:*

$$\#(M_1 \times M_2 \times \ldots \times M_k) = \prod_{i=1}^{k} \#(M_i) \,.$$

   In particular, $\#(M^k) = \#(M)^k$

Proof.

(4) By induction on k. In case $k = 2$, $A_1 \cup A_2 = A_1 \cup (A_2 \setminus A_1)$

$$\#(A_1 \cup A_2) = \#(A_1) + \#(A_2 \setminus A_1) = \#(A_1) + \#(A_2) - \#(A_1 \cap A_2)$$

Proof.

(4) By induction on k. In case $k = 2$, $A_1 \cup A_2 = A_1 \cup (A_2 \setminus A_1)$

$$\#(A_1 \cup A_2) = \#(A_1) + \#(A_2 \setminus A_1) = \#(A_1) + \#(A_2) - \#(A_1 \cap A_2)$$

For $k > 2$ we have by the IH

$$\#(\bigcup_{i=1}^{k} A_i) = \#((\bigcup_{i=1}^{k-1} A_i) \cup A_k) = \#(\bigcup_{i=1}^{k-1} A_i) + \#(A_k) - \#(\bigcup_{i=1}^{k-1} (A_i \cap A_k)) =$$

$$= \sum_{\substack{I \subseteq \{1,\ldots,k-1\} \\ I \neq \varnothing}} (-1)^{\#(I)-1} \#(\bigcap_{i \in I} A_i) + \#(A_k) -$$

$$- \sum_{\substack{I \subseteq \{1,\ldots,k-1\} \\ I \neq \varnothing}} (-1)^{\#(I)-1} \#(\bigcap_{i \in I} A_i \cap A_k) = \sum_{\substack{J \subseteq \{1,\ldots,k\} \\ J \neq \varnothing}} (-1)^{\#(J)-1} \#(\bigcap_{i \in J} A_i)$$

Proof.

(4) By induction on k. In case $k = 2$, $A_1 \cup A_2 = A_1 \cup (A_2 \setminus A_1)$

$$\#(A_1 \cup A_2) = \#(A_1) + \#(A_2 \setminus A_1) = \#(A_1) + \#(A_2) - \#(A_1 \cap A_2)$$

For $k > 2$ we have by the IH

$$\#(\bigcup_{i=1}^{k} A_i) = \#((\bigcup_{i=1}^{k-1} A_i) \cup A_k) = \#(\bigcup_{i=1}^{k-1} A_i) + \#(A_k) - \#(\bigcup_{i=1}^{k-1} (A_i \cap A_k)) =$$

$$= \sum_{\substack{I \subseteq \{1,\ldots,k-1\} \\ I \neq \emptyset}} (-1)^{\#(I)-1} \#(\bigcap_{i \in I} A_i) + \#(A_k) -$$

$$- \sum_{\substack{I \subseteq \{1,\ldots,k-1\} \\ I \neq \emptyset}} (-1)^{\#(I)-1} \#(\bigcap_{i \in I} A_i \cap A_k) = \sum_{\substack{J \subseteq \{1,\ldots,k\} \\ J \neq \emptyset}} (-1)^{\#(J)-1} \#(\bigcap_{i \in J} A_i)$$

The final equation holds for the three cases (i) $J = I$, (ii) $J = \{k\}$, (iii) $J = I \cup \{k\}$

Proof.

(5) By assumption we have bijections e_i

$$e_1\colon \{0,1,\dots,m_1-1\} \to M_1, \dots, e_k\colon \{0,1,\dots,m_k-1\} \to M_k$$

Proof.

(5) By assumption we have bijections e_i

$$e_1 \colon \{0, 1, \ldots, m_1 - 1\} \to M_1, \ldots, e_k \colon \{0, 1, \ldots, m_k - 1\} \to M_k$$

Therefore, $e \colon \{0, 1, \ldots, m_1 \cdots m_k - 1\} \to M_1 \times \ldots \times M_k$ with

$$n \mapsto (e_1(n/m_2 \cdots m_k), \ldots, e_{k-1}((n/m_k) \bmod m_{k-1}), e_k(n \bmod m_k))$$

is a bijection again.

Proof.

(5) By assumption we have bijections e_i

$$e_1\colon \{0,1,\ldots,m_1-1\} \to M_1, \ldots, e_k\colon \{0,1,\ldots,m_k-1\} \to M_k$$

Therefore, $e\colon \{0,1,\ldots,m_1\cdots m_k-1\} \to M_1 \times \ldots \times M_k$ with

$$n \mapsto (e_1(n/m_2\cdots m_k), \ldots, e_{k-1}((n/m_k) \bmod m_{k-1}), e_k(n \bmod m_k))$$

is a bijection again. From the respective numbers

$$\begin{aligned} i_k &= n \bmod m_k \\ i_{k-1} &= (n/m_k) \bmod m_{k-1} \\ &\vdots \\ i_2 &= (n/(m_3\cdots m_k)) \bmod m_2 \\ i_1 &= n/(m_2\cdots m_k) \end{aligned}$$

the number n is obtained by

$$n := i_1 \cdot m_2\cdots m_k + i_2 \cdot m_3\cdots m_k + \ldots + i_{k-1}\cdot m_k + i_k$$

Proof.

(5) By assumption we have bijections e_i

$$e_1\colon \{0,1,\ldots,m_1-1\} \to M_1, \ldots, e_k\colon \{0,1,\ldots,m_k-1\} \to M_k$$

Therefore, $e\colon \{0,1,\ldots,m_1\cdots m_k-1\} \to M_1 \times \ldots \times M_k$ with

$$n \mapsto (e_1(n/m_2\cdots m_k), \ldots, e_{k-1}((n/m_k) \bmod m_{k-1}), e_k(n \bmod m_k))$$

is a bijection again. From the respective numbers

$$\begin{aligned} i_k &= n \bmod m_k \\ i_{k-1} &= (n/m_k) \bmod m_{k-1} \\ &\vdots \\ i_2 &= (n/(m_3\cdots m_k)) \bmod m_2 \\ i_1 &= n/(m_2\cdots m_k) \end{aligned}$$

the number n is obtained by

$$n := i_1 \cdot m_2 \cdots m_k + i_2 \cdot m_3 \cdots m_k + \ldots + i_{k-1} \cdot m_k + i_k$$

Example

In C-programs, the elements of a multi-dimensional array are stored consecutively in memory, where their order is such that „later indices go faster than earlier ones“. For example, the elements of

```
int M[2][3] = {{3,5,-2},{1,0,2}};
```

are arranged in memory as:

M[0][0]	M[0][1]	M[0][2]	M[1][0]	M[1][1]	M[1][2]
3	5	-2	1	0	2

M

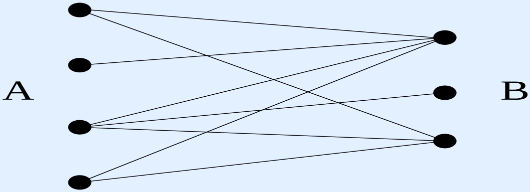
Example (continued)

```
double f(double *z, int m1, int m2, int m3)
{
  ...
}
...
int main( void)
{
   double x, y, A[2][3][4], B[3][4][2];
   ...
   x = f(&A[0][0][0],2,3,4);
   y = f(&B[0][0][0],3,4,2);
   ...
}
```

In the function `f`, the element "‘`z[i][j][k]`"’ can be addressed as `*(z+i*m2*m3+j*m3+k)` the indices `i`, `j`, `k` of the element located at address `z+l` can be computed as `k = l%m3`, `j = (l/m3)%m2` and `i = l/(m2*m3)`

Theorem

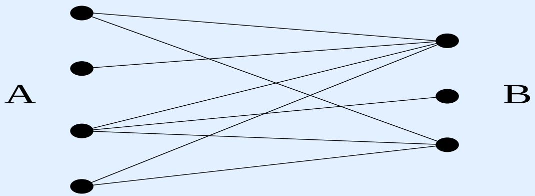
6 *Double counting An undirected graph is bipartite, if there exists a partition of its set of nodes in two blocks A and B, such that every edge has one endpoint in A and one in B.*



For a finite bipartite graph $\sum_{e_1 \in A} \mathrm{Deg}(e_1) = \sum_{e_2 \in B} \mathrm{Deg}(e_2)$

Theorem

6 *Double counting An undirected graph is bipartite, if there exists a partition of its set of nodes in two blocks A and B, such that every edge has one endpoint in A and one in B.*



For a finite bipartite graph $\sum_{e_1 \in A} \mathrm{Deg}(e_1) = \sum_{e_2 \in B} \mathrm{Deg}(e_2)$

Proof.

(6) Both sums denote the number of edges ∎

Theorem (Pigeon hole principle)

Let $f : M \to N$ be a function, with M, N finite. If $\#(M) > \#(N)$, then there is at least one element $y \in N$ having an inverse image with more than one element.

Theorem (Pigeon hole principle)

Let $f: M \to N$ be a function, with M, N finite. If $\#(M) > \#(N)$, then there is at least one element $y \in N$ having an inverse image with more than one element.

Proof.

Assuming the inverse image of each element of N has at most one element, f is injective, and therefore $M \to f(M)$ bijective. Hence $\#(M) = \#(f(M))$ and by $f(M) \subseteq N$ we have $\#(M) \leqslant \#(N)$ ∎

Lemma

Maximum $\geq$ average. For $R = (r_i)_{i \in I}$ a collection of numbers, $\max(R) \geq \frac{\sum R}{\#(I)}$.

Theorem (Pigeon hole principle)

Let $f: M \to N$ be a function, with M, N finite. If $\#(M) > \#(N)$, then there is at least one element $y \in N$ having an inverse image with more than one element.

Proof.

Assuming the inverse image of each element of N has at most one element, f is injective, and therefore $M \to f(M)$ bijective. Hence $\#(M) = \#(f(M))$ and by $f(M) \subseteq N$ we have $\#(M) \leqslant \#(N)$ ∎

Lemma

Maximum $\geq$ average. For $R = (r_i)_{i \in I}$ a collection of numbers, $\max(R) \geq \frac{\sum R}{\#(I)}$.

Alternative proof of PHP

Let $R = (\#(f^{-1}(n))_{n \in N}$. By the lemma $\max(R) \geq \frac{\sum R}{\#(N)} = \frac{\#(M)}{\#(N)} > 1$.

Counting the number of injective functions

Theorem

Let K and M be finite sets having k resp. m elements. Then there are exactly

$$(m)_k := \begin{cases} m(m-1)(m-2)\cdots(m-k+1) & \text{if } k \geqslant 1 \\ 1 & \text{if } k = 0 \end{cases}$$

injective functions from K to M. The number $(m)_k$ is the falling factorial of m and k.

Counting the number of injective functions

Theorem

Let K and M be finite sets having k resp. m elements. Then there are exactly

$$(m)_k := \begin{cases} m(m-1)(m-2)\cdots(m-k+1) & \text{if } k \geqslant 1 \\ 1 & \text{if } k = 0 \end{cases}$$

injective functions from K to M. The number $(m)_k$ is the falling factorial of m and k.

Example

Obviously, there are no (total) injective functions from $\{0, 1, 2, 3\}$ to $\{0, 1\}$, which agrees with the theorem as $(2)_4 = 2 \cdot 1 \cdot 0 \cdot -1 = 0$.

Proof.

We show the claim by mathematical induction on k. In the base case, $k = 0$, we have that K is the empty set and the empty function is the only injective function. In the step case, we write

$$K = \{x_0, x_1, \ldots, x_k\}$$

and consider how to construct injective functions $f : K \to M$.

Proof.

We show the claim by mathematical induction on k. In the base case, $k = 0$, we have that K is the empty set and the empty function is the only injective function. In the step case, we write

$$K = \{x_0, x_1, \ldots, x_k\}$$

and consider how to construct injective functions $f : K \to M$. For x_0 we have m ways to choose an image $f(x_0) \in M$. That element

$$y_0 := f(x_0)$$

then cannot by chosen as image of the other elements of K. That is, as images of $x_1, \ldots, x_k$ we must choose elements among $M \setminus \{y_0\}$.

Proof.

We show the claim by mathematical induction on k. In the base case, $k = 0$, we have that K is the empty set and the empty function is the only injective function. In the step case, we write

$$K = \{x_0, x_1, \dots, x_k\}$$

and consider how to construct injective functions $f\colon K \to M$. For x_0 we have m ways to choose an image $f(x_0) \in M$. That element

$$y_0 := f(x_0)$$

then cannot by chosen as image of the other elements of K. That is, as images of $x_1, \dots, x_k$ we must choose elements among $M \setminus \{y_0\}$. By the IH there are $(m-1)_k$ such choices. Therefore, the total number of injective functions is

$$m \cdot (m-1)_k = (m)_{k+1}$$

Proof.

We show the claim by mathematical induction on k. In the base case, $k = 0$, we have that K is the empty set and the empty function is the only injective function. In the step case, we write

$$K = \{x_0, x_1, \ldots, x_k\}$$

and consider how to construct injective functions $f\colon K \to M$. For x_0 we have m ways to choose an image $f(x_0) \in M$. That element

$$y_0 := f(x_0)$$

then cannot by chosen as image of the other elements of K. That is, as images of $x_1, \ldots, x_k$ we must choose elements among $M \setminus \{y_0\}$. By the IH there are $(m-1)_k$ such choices. Therefore, the total number of injective functions is

$$m \cdot (m-1)_k = (m)_{k+1}$$

∎

Counting the number of bijective functions

Theorem

Let K and M be finite sets having m elements each. Then there are exactly

$$m! := \begin{cases} m(m-1)(m-2)\cdots 3\cdot 2\cdot 1 & m \geqslant 1 \\ 1 & m = 0 \end{cases}$$

bijections from K to M. The number $m!$ is called m factorial

Counting the number of bijective functions

Theorem

Let K and M be finite sets having m elements each. Then there are exactly

$$m! := \begin{cases} m(m-1)(m-2)\cdots 3\cdot 2\cdot 1 & m \geqslant 1 \\ 1 & m = 0 \end{cases}$$

bijections from K to M. The number $m!$ is called m factorial

Proof.

Since $\#(K) = \#(M) = m$ every injective function from K to M is a bijection, hence the claim follows from the theorem, with $(m)_m = m!$.

Counting the number of bijective functions

Theorem

Let K and M be finite sets having m elements each. Then there are exactly

$$m! \; := \begin{cases} m(m-1)(m-2)\cdots 3\cdot 2\cdot 1 & m \geqslant 1 \\ 1 & m = 0 \end{cases}$$

bijections from K to M. The number $m!$ is called m factorial

Proof.

Since $\#(K) = \#(M) = m$ every injective function from K to M is a bijection, hence the claim follows from the theorem, with $(m)_m = m!$. ∎

Theorem

Let M be a finite set with m elements. Then

$$\#(\mathcal{P}(M)) = 2^m\,.$$

Theorem

Let M be a finite set with m elements. Then

$$\#(\mathcal{P}(M)) = 2^m \,.$$

Proof.

We take some arbitrary but fixed enumeration $e\colon \{0,1,\ldots,m-1\} \to M$. The following function then is a bijection:

$$F\colon \mathcal{P}(M) \to \{0,1\}^m \;,\; T \mapsto (t_0,\ldots,t_{m-1}) \;,\; t_i := \begin{cases} 1 & \text{if } e(i) \in T \\ 0 & \text{otherwise.} \end{cases}$$

Theorem

Let M be a finite set with m elements. Then

$$\#(\mathcal{P}(M)) = 2^m \,.$$

Proof.

We take some arbitrary but fixed enumeration $e\colon \{0,1,\ldots,m-1\} \to M$. The following function then is a bijection:

$$F\colon \mathcal{P}(M) \to \{0,1\}^m \;,\; T \mapsto (t_0,\ldots,t_{m-1}) \;,\; t_i := \begin{cases} 1 & \text{if } e(i) \in T \\ 0 & \text{otherwise.} \end{cases}$$

■

Naming

For $T \subseteq M$, the function $\chi_T : M \to \{0,1\}$ defined by $\chi_T(t) = 1$ if $t \in T$ and 0 otherwise, is the characteristic function of T.

Counting the number of subsets of given size

Theorem

Let M be a finite set with m elements, and let k be a natural number. Then

$$\#(\mathcal{P}_k(M)) = \binom{m}{k}.$$

where $\mathcal{P}_k(M)$ denotes the subsets of size k, and where the binomial *coefficient „m choose k" or „m over k" is defined by*

$$\binom{m}{k} := \frac{m \cdot (m-1) \cdots (m-k+1)}{k \cdot (k-1) \cdots 1} = \begin{cases} \dfrac{m!}{k!(m-k)!} & \text{if } k \leqslant m \\ 0 & \text{otherwise} \end{cases}$$

Proof.

An enumeration $e\colon \{0,1,\ldots,k-1\} \to T$ of a subset T of M having k elements, is obtained by choosing

- an arbitrary element $e(0) \in M$,
- an arbitrary element $e(1) \in M \setminus \{e(0)\}$,
- an arbitrary element $e(2) \in M \setminus \{e(0), e(1)\}$, etc.

Since the order of choosing the elements of T is irrelevant, the number of such choices is

$$m \cdot (m-1) \cdots (m-k+1)/k!\,.$$

Proof.

An enumeration $e\colon \{0,1,\ldots,k-1\} \to T$ of a subset T of M having k elements, is obtained by choosing

- an arbitrary element $e(0) \in M$,
- an arbitrary element $e(1) \in M \setminus \{e(0)\}$,
- an arbitrary element $e(2) \in M \setminus \{e(0), e(1)\}$, etc.

Since the order of choosing the elements of T is irrelevant, the number of such choices is

$$m \cdot (m-1) \cdots (m-k+1)/k!\,.$$

∎