Lecture Notes: Discrete Mathematics

Note 0.1:
Contributions to this summary and the corresponding formula sheet are welcome on Github .

Inhaltsverzeichnis

Graph Theory

Definition 0.1: simple graph
A simple graph $G = (V, E)$ has vertices V and edges $E \subseteq \{\{u, v\} \mid u, v \in V, u \neq v\}$

TODO example

Definition 0.2: adjacent
Vertices a and b are adjacent if there is an edge f in E with $f = \{a, b\}$

Definition 0.3: incident
Vertex a is incident to edge f if $a \in f$

Definition 0.4: graph
A graph also allows loops, i.e. edges of the form $\{a\}$ for a vertex a.

Definition 0.5: multigraph
A multigraph is a graph where two vertices may be connected by several edges. E is now a multiset. A vertex in a multigraph may have several loops.

TODO example

Definition 0.6: weighted graph
A weighted graph is a (multi)graph together with a weight function $w : E \to \mathbb{R}$.

Definition 0.7: neighbors
The set of neighbors is $N(u) = \{v \in V \mid \exists e \in E : e = \{u, v\}\}$ for vertex u.

Definition 0.8: degree

The degree of vertex u is $d(u) = |N(u)|$ for a simple graph, and in general $d(u) = |\{e \in E | uisincidenttoe\}|$.

Definition 0.9: directed graph

A directed (multi)graph is a graph where every edge has a head and a tail. Alternatively: Edges are pairs of vertices (u, v). \ $d^+(u) = |\{e \in E \mid e = (u, v) for some v \in V\}|$ \ $d^-(u) = |\{e \in E \mid e = (v, u) for some v \in V\}|$

Remark 0.1:

A (di)graph can be regarded as a relation $uRv \iff (u, v) \in R$ and if it's a symmetric then the graph is undirected.

Definition 0.10:

A graph is regular of degree r if $d(u) = r \forall u \in V$

Lemma 0.1: handshaking lemma

$\sum_{v \in V} deg(v) = 2 \cdot |E|$

Example 0.1:

- $K_n = (\{1, ..., n\}, \{\{i, j\} \mid i \neq j \wedge i, j \geq 0 \wedge i, j \leq n\})$ is the complete graph on n vertices.
- P_n path
- C_n cycle
- hypercube: $V = \{0, 1\}^n$ (i.e., 2^n vertices), $E = \{\{u, v\} \mid \sum_{i=1}^{n} |u_i - v_i| = 1\}$

Definition 0.11:

The adjacency matrix $A = (a_{ij})$ of graph G is the $|V| \times |V|$ matrix with $a_{ij} = \begin{cases} 1 & \text{if } \{i, j\} \in E \\ 0 & \text{otherwise} \end{cases}$ if G is simple,

- $= \#edges\{i, j\}$ if G is a multigraph,
- $= \#edges(i, j)$ if G is a digraph,
- $= \sum_{e=(i,j) \in E} w(e)$ if G is weighted and directed.

Different graphs can have the same adjacency matrix, because the labels are forgotten. Different adjacency matrices can correspond to the same graph.

Definition 0.12: isomorphic

Simple graphs G, H are isomorphic, $G \cong H$ if there is a bijection $g : V(G) \to V(H)$ sucht that $\{u, v\} \in E(G) \iff \{g(u), g(v)\} \in E(H)$

TODO example

Problem: It is unknown whether there is an algorithm that decides in polynomial time graph isomorphism (unknown if NP-complete).

Definition 0.13: Walk, Trail, Path

A walk/trail/path is a sequence $u_1e_1u_2e_2...u_l$ of vertices $u_1, ..., u_l$ and edges $e_1, ..., e_l$ such that $e_i = \{u_i, u_{i+1}\}$. A trail has no repeated edges. A path has no repeated vertices. Every path is a trail, and every trail is a walk.

Definition 0.14: closed walk, circuit, cycle

A closed walk/circuit/cycle is a walk/trail/path with an $e_l = \{u_l, u_1\}$

Lemma 0.2:

Let A be the adjacency matrix of a weighted(multi)graph, then $(A^k)_{ij}$ is the number of walks from i to j of length k

Proof 0.1:

By induction: $k = 0 \to A^0 = I$ and the number of walks of length zero (0 edges) from i to j is 1 if $i = j$ and 0 otherwise. \ Statement for k implies statement for $k+1$: $(A^{k+1})_{ij} = (A * A^k)_{ij} = \sum_{v \in V} A_{iv} * (A^k)_{vj}$. A walk from i to j of length $k+1$ is an edge from i to v followed by a walk of length k from v to j.

Definition 0.15: connected graph

A graph is connected if for any two vertices u, v there is a walk from u to v. For a digraph, this is called strongly connected. A digraph is weakly connected if the underlying graph is connected. A bridge is an edge whose removal increases the number of connected components.

Definition 0.16: subgraph

H is a subgraph of G if H is a graph (of the same kind) and $V(H) \subseteq V(G)$, $E(H) \subseteq E(H)$ (note that H must be a graph by itself).

Definition 0.17: bipartite

A (simple) graph is bipartite if its vertices can be coloured red and blue such that edges only connect vertices of different colours.

Theorem 0.1: König 1936

G is bipartite iff G contains no cycles of odd length

Proof 0.2:

$\rightarrow$, every cycle visits blue and red vertices alternatingly $\rightarrow$ even length $\setminus \leftarrow$, without loss of generality G connected, fix $u \in V$, colour u blue; for any path from u to v of odd length, colour v red, for even length blue. If there are two different paths from u to v both have even length or both have odd length (because there is no cycle of odd length)

Definition 0.18: Eularian Trail

A Eulerian Trail is a trail that uses every edge exactly once.

Theorem 0.2:

A connected graph has a Eulerian circuit if and only if all its vertices have even degree.

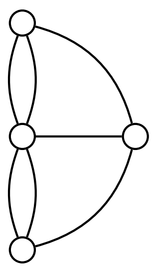


Abbildung 1: no eulerian circuit as every vertex has odd degree

Proof 0.3:

$\Rightarrow$: In any circuit every vertex is entered as often as it serves as a point of departure.

$\Leftarrow$: Induction on the number of edges

- if the graph G has no edges $G = (V = 1, E = \emptyset)$
- otherwise let W be any circuit in G (this exists: start anywhere, choose any edge unused so far, continue until you hit starting vertex)
- let $G' = (V(G), E(G) \setminus E(W))$, all vertices in G' have even degree and G' need not be connected.
- let $G'_1, ...G'_c$ be the connected components of G'. In each component of G'_i find a Eulerian circuit W_i. W_i and W have atleast one vertex in common, because G is connected and removing W produces the components.
- therefore $W_1, ...W_c$ and W can be combined to a Eulerian circuit.

Trees and Forests

Definition 0.19:

- A *forest* is a graph without cylces (=acyclic).
- A *tree* is a connected forest.
- A *leaf* is a vertex of degree 1.

Lemma 0.3:
If T is a tree and has two vertices it has at least 2 leafs.

Proof 0.4:
$V(T)$ and $E(T)$ are finite $\Rightarrow$ T contains a maximal path and this path has two leafs (because it is maximal).

Definition 0.20: Spanning subgraphs
A subgraph H of a graph G is spanning if $V(H) = V(G)$.

Theorem 0.3:
Let T be a graph, then the following are equivalent:

1. T is a tree.
2. Any 2 vertices are connected with a unique path.
3. T is connected and every edge is a bridge (min. connected).
4. T has no cycles and adding any edge yields a cycle (maximal acyclic)

Proof 0.5:

- $1 \Rightarrow 2$: otherwise T would not be connected or T would have a cylce.
- $2 \Rightarrow 3$: A unique path from u to v exists, which means every edge has to be a bridge.
- $3 \Rightarrow 4$: An edge in a cycle would not be a bridge $\Rightarrow$ T has no cycles, adding an edge would yield a cyle because T is connected.
- $4 \rightarrow 1$: adding any edge (u, v) yields a cycle $= T$ is connected.

Theorem 0.4:
A connected graph G has a spanning tree.

Proof 0.6:
As long as there is a non-bridge, remove it, and use 3. of the previous theorem.

Theorem 0.5:
A graph is a tree if and only if it is connected and $|V| = |E| + 1$.

Proof 0.7:
$\Rightarrow$: induction on $|V| : |V| = 1$

If $|V| \geq 2$: remove a leaf to obtain T', by induction $|V(T') \models |V(T)| - 1$ and $|E(T')| = |E(T)| - 1$

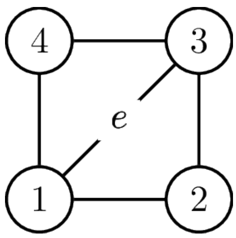
$|V(T)| = |V(T')| + 1 = |E(T')| + 1 + 1 = |E(T) + 1|$

$\Leftarrow$: Let T' be a spanning tree of T

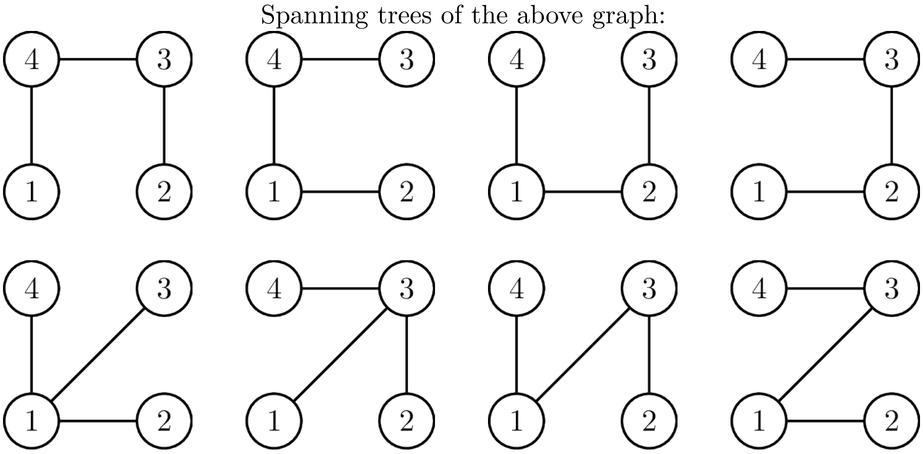
$|V(T') \models |E(T')| + 1$

$|V(T) \models |E(T)| + 1$, $|V(T) \models |V(T')| \Rightarrow |E(T) \models |E(T')| \Rightarrow T = T'$

How many spanning trees are there?



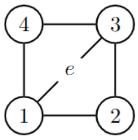
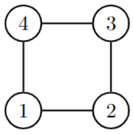
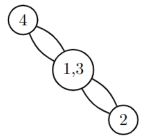
Spanning trees of the above graph:



Definition 0.21:
- $\tau(G)$ is the number of spanning trees of G.
- $G \backslash e$ is the graph obtained by removing edge e.
- G/e is the graph obtained by contracting edge e.

Theorem 0.6: Deletion Contraction Theorem
$\tau(G) = \tau(G\backslash e) + \tau(G/e)$

Example 0.2:

$\tau($  $) = \tau($  $) + \tau($  $) = 4 + 4 = 8$ (1)

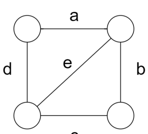
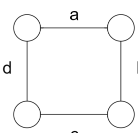
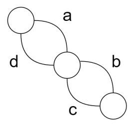
Proof 0.8:
The set of spanning trees is the disjoint union of spanning trees containing e and spanning trees not containing e.

More generally: If G is a weighted graph with $w : E(G) \to \mathbb{R}$ and H is a subgraph of G, then $w(H) = \prod_{e \in E(H)} w(e)$

For weighted graphs, $\tau(G)$ is the sum of the weights of the spanning trees of G

$$\tau(G) = \sum_{T} \prod_{e \in E(T)} w(e)$$

Example 0.3:

$\tau($  $) = \tau($  $) + e \cdot \tau($  $) = abc + abd + acd + bcd + e(a+d)(b+c)$

Definition 0.22: Degree Matrix
The degree matrix of a graph is

$$D = \begin{pmatrix} d(v_1) & & 0 \\ & \ddots & \\ 0 & & d(v_n) \end{pmatrix}$$

(The degree of a vertex in a weighted graph is $d(u) = \sum_{(u,v) \in E(G)} w(v,u)$)

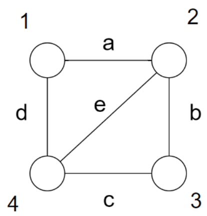
Theorem 0.7: Matrix Tree Theorem

Let $n = |V(G)|$, let $\lambda_1, \ldots, \lambda_n$ be the eigenvalues of $D - A$. One of these is 0, w.l.o.g. $\lambda_1 = 0$

Then, $\tau(G) = \frac{1}{n} \cdot \lambda_2 \cdots \lambda_n$.

Equivalently: $\tau(G) = det((D-A)_{i,i})$, where $M_{i,i}$ is obtained by removing row and column i. $M = D - A$

Example 0.4:



$$det(D-A)_{4,4} = \begin{pmatrix} a+d & -a & 0 & \cancel{-d} \\ -a & a+b+e & -b & \cancel{-e} \\ 0 & -b & b+c & \cancel{-e} \\ \cancel{-d} & \cancel{-e} & \cancel{-e} & \cancel{c+d+e} \end{pmatrix}$$

$$= (a+d) \begin{vmatrix} a+b+e & -b \\ -b & b+c \end{vmatrix} + a \begin{vmatrix} -a & 0 \\ -b & b+c \end{vmatrix}$$

$$= (a+d)((a+b+e)(b+c) - b^2) - a^2(b+c)$$

Spanning Trees of Minimal Weight

Assume graph G is connected.

Kruskal's Algorithm:

Require: Sorted edges by weight: $w(e_1) \leq \cdots \leq w(e_m)$.
  $T_1 \leftarrow \emptyset$
  for i in $1...m$ **do**
    if $E(T_i) \cup e_i$ is acyclic **then**
      $E(T_{i+1}) \leftarrow E(T_i) \sqcup e_i$
    else
      $E(T_{i+1}) \leftarrow E(T_i)$
    end if
    if $|E(T_{i+1}| + 1 = n - 1$ **then**
      return $E(T) \leftarrow E(T_{i+1})$
    end if
  end for

Remark 0.2:
Kurskal is a so-called greedy algorithm: In every step, it adds the locally optimal edge. The result is also globally optimal.

Theorem 0.8:
Kruskal yields a spanning tree of minimal weight

Proof 0.9:
- T is acyclic by construction.
- Suppose the algorithm reaches the return statement and T_{m+1} is not connectced with components A and B. There has to be an edge e_l which connects the two components A and B. Kruskal would habe added e_l becuase $T_l \subseteq T_{m+1}$ is acyclic.
- T is of minimal weight: see proof in matroid setting

Metroids

Motivation: Metroids are an abstraction of graphs and provide a framework for greedy algorithms.

Definition 0.23: Matroids
Let E be a set, I a set of subsets of E (the set of independant sets). Then, (E, I) is a matroid iff
- M1: $\emptyset \in I$
- M2: $B \in I, A \subseteq B \rightarrow A \in I$
- M3: $A, B \in I, |B| = |A| + 1 \Rightarrow \exists e \in B \backslash A : A \cup \{e\} \in I$ ("exchange axiom")

Theorem 0.9:
G a graph, $I := \{F \subset E(G) | F \text{ acyclic}\} \Rightarrow (E, I)$ is a matroid

Proof 0.10:
- M1: $\emptyset$ is a forest
- M2: B is a forest, $A \subseteq B \Rightarrow A$ is a forest
- M3: A, B edge sets of spanning forests, $|B \models |A| + 1$, find edge $e \in B \backslash A$ such that $A \cup e$ is a forest.
  Suppose A has connecdted components $T_1 ... T_c$ Show $\exists e$ in $B \backslash A$ that is not in any of these components. Count edges:
  TODO$\{\ldots\}$
  B has more than $|A|$ edges, so there is an edge not in any B restricted by $V(T_i)$

Greedy: (E, I) matroid, $w : E \to \mathbb{R}$

Require: Sorted E by weight: $w(e_1) \leq ... \leq w(e_m)$.

```
T_1 ← ∅
for i in 1...m do
    if E(T_i) ∪ e_i ∈ I then
        E(T_{i+1}) ← E(T_i) ⊔ e_i
    else
        E(T_{i+1}) ← E(T_i)
    end if
end for
return E(T) ← E(T_{m+1})
```

Definition 0.24: Basis

A *basis* of a matroid (E, I) is a (inclusionwise) maximal independent set $b \in I$.

Theorem 0.10:

Greedy returns a basis of minimal weight, that is $\sum_{e \in T} w(e)$ is minimal among all bases.

Proof 0.11:

T is a maximal independent set as in Kruskal.

$\sum_{e \in T} w(e)$ is minimal: let $T = \{t_1, ..., t_s\} w(t_1) \leq ... \leq w(t_s)$

suppose that $B = \{b_1, ..., b_r\}$ with $w(b_1) \leq .. \leq w(b_r)$ is a basis with $\sum_{b \in B} w(b) < \sum_{e \in T} w(e)$

let $i := min\{j | w(b_j) < w(t_j)\}$ ie, $w(b_j) \geq w(t_j)$ for $j < i$ and $w(b_j) < w(t_i)$

let $T_{i-1} = \{t_1, .., t_{i-1}\} B_i = \{b_1, ..., b_i\}$

apply $M3$

$\Rightarrow \exists b_j \in B_i \backslash T_{i-1} : T_{i-1} \cup b_j \in I$

$w(b_j) \leq w(b_i) < w(t_i)$ so greedy should have chosen b_j instead of t_i

j with $w(b_j) < w(t_j)$ exists becuase all bases have the same cordinality.

Theorem 0.11:

Suppose that (E, I) satisfies $M1$ and $M2$, and that for any weight function $w : E \to \mathbb{R}$ the greedy algorithm produces a maximal independent set $A \in I$ such that $\sum_{e \in A} w(e)$ is minimal among all maximal sets in I. Then, (E, I) satisfies $M3$ and therefore is a matroid.

(That is, an independence system is a matroid iff greedy works as expected.)

Proof 0.12:

- all maximal sets in I have the same cardinality. Suppose $A, B \in I$ maximal, $|A| < |B|$ (we will determine $\varepsilon > 0$ in a suitable way).\ for any $\varepsilon > 0$ greedy returns B. $w(B) = |B| \geq |A| + 1$
  $w(A) = |A \cap B| + (1 + \varepsilon)|A \backslash B \models |A| + \varepsilon |A \backslash B| \Rightarrow$ choose $\varepsilon < \frac{1}{|A \backslash B|}$
  $(A \backslash B \neq \emptyset)$

- (E, I) satisfies $M3$, let $A, b \in I, |B \models |A| + 1$ greedy chooses all of A first: since $|A| < |B|$ we have that A is not maximal\ suppose $\nexists e \in B \backslash A | A \cup e \in I$
  $\Rightarrow$ greedy chooses $r - |A|$ elements of weight x, where r is the size of any basis. call this set A', also $\exists$ basis $B' = B \cup \{e_1, ...e_{r-|B|}\}$
  $w(A') = w(A) + x(r - |A|) = x(r - |A|)$
  $w(B') \leq |B \backslash A| + x(r - |B|) = |B \backslash A| + x(r - |A \vdash 1) \leq w(A') + |B \backslash A \vdash x$
  $\Rightarrow$ choose $x > |B \backslash A|$, then $w(B') < w(A')$ but greedy returned A'

Prims algorithm: let G connected, r any vertex

Require: Sorted E by weight: $w(e_1) \leq ... \leq w(e_m)$.
  $Q \leftarrow V(G) \backslash r$
  $T \leftarrow \emptyset$
  $V_T \leftarrow \{r\}$
  while $Q \neq \emptyset$ **do**
    $u \leftarrow$ a vertex in Q connected to T with an edge of minimal weight
    $Q \leftarrow Q \backslash u$
    $T \leftarrow T \cup e$
    $V_T \leftarrow V_T \cup u$
  end while

Prim is a greedy algorithm, but there is no matroid underlying

Minimal Distances

Definition 0.25: Distance
G a weighted directed graph $w : E \rightarrow \mathbb{R}$.

The *distance* (or length) of a path P is $\sum_{e \in P} w(e)$

TODO{illustration}

Algorithms:

- *Dijkstra:* (1950s) sinlge source, only for $w : E \rightarrow \mathbb{R}_+$, $O(|V| log |V| + |E|)$
- *Bellman-Ford-Moore:* single source, G loopless, $O(|V||E|)$
- *Floyd-Warshall:* all distances, $O(|V|^3)$

Dijkstra algorithm: $d(v)$ (array of distances) $= 0$ if $v = v_0$ else ∞
  $Q \leftarrow V$
  while $Q \neq \emptyset$ **do**
    find $u \in Q$ with minimal $d(u)$
    $Q \leftarrow Q \backslash u$
    for $v \in Q, (u, v) \in E$ **do**
      $d(v) \leftarrow min(d(v), d(u) + w(u, v))$
      (predecessor of v is u if $d(u)w(u, v) < d(v)$)
    end for
  end while

Example 0.5:
TODO

Definition 0.26:
A *cut* of a (di)graph is a set of edges(arcs) S such that V is the disjoint union of V_1 and V_2 and there is no edge within V_1 or V_2 in S. (We will redefine cuts later a bit differently.)

Remark 0.3:
Dijkstra chooses the minmial weight edge between Q and $V \backslash Q$, this is called *breadth-first search*

Bellman-For-Moore algorithm: $d(v)$ (array of distances) $= 0$ if $v = v_0$ else ∞ $l(v)$ (length of path) $= 0$ if $v = v_0$ else ∞

```
step ← 0
while True do
    modified ← False
    for u ∈ V with l(u) = step do
        for e = (u, v) ∈ E do
            if d(v) > d(u) + w(e) then
                modified ← True
                d(v) ← d(u) + w(e)
                l(v) ← l(u) + 1
            end if
        end for
    end for
    if not modified then
        return d
    else
        if step = |V ⊢ 1 then
            throw error: negative cycle
        else
            step ← step + 1
        end if
    end if
end while
```

Example 0.6:
TODO

Example 0.7:
TODO{example with negative cycle}

Floyd-Warshall algorithm: $d(u,v)$ (array of distances) $= 0$ if $u = v$ else if $(u,v) \in E$ $w(u,v)$ else ∞ (adjacency matrix with 0 replaced by ∞)

```
step ← 0
for u ∈ V do
    for v ∈ V do
        for w ∈ V do
            d(v,w) = min(d(v,w), d(v,u) + d(u,w))
        end for
        if d(v,v) < 0 then
            error: negative cycle
        end if
    end for
end for
```

Flows

Definition 0.27: Flow

Let G be a weighted (di)graph with:

- $w : E \to \mathbb{R}_+$
- s a source in V, i.e. indegree of s is 0
- t a sink, i.e. outdegree of $t $ is 0.

Then, $\phi : E \to \mathbb{R}$ is called a *flow* iff

- F1: $\forall e \in E : 0 \leq \phi(e) \leq w(e)$ (Weights indicate maximal capacity.)
- F2: $\forall v \in V \backslash \{s,t\} \sum_{(v,u) \in E} \phi(v,u) = \sum_{(u,v) \in E} \phi(u,v)$ (What flows in flows out.)

Definition 0.28: Value of a Flow

For a flow from source s to sink t:

$val(\phi) := \sum_{(s,u) \in E} \phi(s,u) = \sum_{(u,t) \in E} \phi(u,t)$

Proof 0.13:

sum over outbound edges:
$\sum_{(s,u) \in E} \phi(s,u) + \sum_{v \neq s,t; v \in V} \sum_{(v,u) \in E} \phi(v,u) = \sum_{e \in E} \phi(e)$

sum over inbound edges:
$\sum_{(u,t) \in E} \phi(u,t) + \sum_{v \neq s,t; v \in V} \sum_{(u,v) \in E} \phi(u,v) = \sum_{e \in E} \phi(e)$

Definition 0.29: Cut

$S \subseteq V, s \in S, t \notin S$ then $(S, V \backslash S)$ is a **cut**, any edge from S to $V \backslash S$ is said to be *crossing* the cut.

The *capacity* of a cut is

$$c(S, V \backslash S) = \sum_{(u,v) \ inE; u \in S, v \notin S} w(u,v)$$

A *cut* is *minimal* if its capactiy is minimal along all cuts.
A *flow* is *maximal* if its value is maximal among all flows.

Lemma 0.4:
$val(\phi) \leq c(S, V \backslash S)$ for any flow ϕ and all cuts $c(S, V \backslash S)$

Proof 0.14:
TODO

Definition 0.30: Augmenting Path
An *augmenting path* P for ϕ is an (unoriented) path from s to t with
- $\phi(e) < w(e) \forall e \in P$ traversed in the forward direction.
- $\phi(e) > 0 \forall e \in P$ traversed in the backward direction.

Theorem 0.12:
Let ϕ be any flow, then
- $val(\phi)$ is maximal $\iff \nexists$augmenting path for ϕ
- $val(\phi)$ is maximal $\iff val(\phi) = c(S, V \backslash S)$ for some S

Proof 0.15:
$val(\phi)$ is max $\Rightarrow \nexists$augmenting path for ϕ

suppose P is an augmenting path, let $\delta_1 := min_{e \in P; forward}(w(e) - \phi(e)), \delta_2 := min_{e \in P; backward}(\phi(e)) \delta := min(\delta_1, \delta_2)$ $\widetilde{\phi}$ is a flow: check $F2$ for a vertex v on the path.

$$\sum_{(v,u) \in E} \widetilde{\phi}(e) = \sum_{(v,u) \in E} \phi(e) +$$

function 2\ $\nexists$ augmenting path $\Rightarrow$ property 2 of theorem.\ let $S = \{v \in V | \exists$"augmenting path" from s to v$\}$\ $(S, V \backslash S)$ is a cut (because $s \in S$).\ for forward crossing edges we have $\phi(e) = w(e)$ in this cut\ for backward crossing edges we have $\phi(e) = 0$\ use lemma $val(\phi) = \sum_{eforward} \phi(e) - \sum_{ebackward} \phi(e) = c(S, V \backslash S) - 0$\ TODO{illustrations} property 2 $\Rightarrow val(\phi)$ is maximal.\ Lemma: $val(\phi) \leq c(S, V \backslash T)$, so $val(\phi)$ is maximal.

Theorem 0.13:
A maximal flow exists.

Proof 0.16:
- If $w : E \to \mathbb{N}$ an augmenting path increases $val(\phi)$ by at least one.
- If $w : E \to \mathbb{Q}$ multiply all weights by the lcm of the denominators.
- If $w : E \to \mathbb{R}$ any continous real function on a compact set has a maximum.

Remark 0.4: Max-Flow-Min-Cut theorem
val of max flow = capacity of a min cut.

Ford-Fulkerson algorithm:

```
ϕ_1(e) ← 0 for all e
while ∃ augmenting path P for ϕ_i do
    function 3
end while
```

Hall's marriage theorem

X, Y finite disjoint sets $|X \models |Y|$, $D \subseteq X \times Y$

Definition 0.31: Perfect Matchnig
$M \subseteq D$ is called a *perfect matching* iff $\forall x \in X \exists! y \in Y : (x, y) \in M$

Theorem 0.14: Hall's Marriage Theorem
D admits a perfect matching $\iff \forall X' \subset X : |N^+(X')| \geq |X'|$

Proof 0.17:
$\Rightarrow$: use the perfect matching, every x is matched to a different y

$\Leftarrow$: TODO{illustration} the value of the max flow is the size of the largest matching.
let $(\{s\} \cup \widetilde{X} \cup \widetilde{Y}, X \backslash \widetilde{X} \cup Y \backslash \widetilde{Y} \cup \{t\})$ be a minimal cut.
$\widetilde{Y} \supseteq N^+(\widetilde{X})$ because $w(x, y) = \infty$
$c(S, V \backslash S) = |X \backslash \widetilde{X}| + |\widetilde{Y}|$
$c(S, V \backslash S) \geq |X|$ because $|\widetilde{Y}| \geq |N^+(\widetilde{X})| \geq |\widetilde{X}|$ and $|X \backslash \widetilde{X}| + |\widetilde{Y}| \geq |X \backslash \widetilde{X}| + |\widetilde{X}| = |X|$

Hamiltonian Graphs

Definition 0.32: Hamiltonian Graphs
A graph is *hamiltonian* if it contains a hamiltonian cycle, which is a cycle which visits every vertex exactly once.

Remark 0.5:
It is NP-hard to find a hamiltonian cycle.

Definition 0.33: Closure of a Graph
$G = (V, E)$ a graph.

$[G] = (V, \widetilde{E})$ with $E_1 := E, E_{i+1} := E_i \cup \{e = (u, v) \notin E | d(u) + d(v) \geq |V|\}$.

That is, $\widetilde{E}$ is the set E_k s.t. $d(u) + d(v) < |V|$ for all $(u, v) \notin E_k$

$[G]$ is called the closure of G.

Theorem 0.15:
G is hamiltonian iff $[G]$ is hamiltonian.

Proof 0.18:
$\Rightarrow$: $[G]$ is G with some morde edges.
$\Leftarrow$: suppose H is a hamiltonian cycle in $[G]$, but G is not hamiltonian,
$\Rightarrow \exists e = (u, v) \in E([G]) \backslash E(G)$ which is in every hamiltonian cycle of $[G]$
$\Rightarrow d_G(u) + d_G(v) \geq |V|$ because TODO{add picture}

Corollary 0.1:

- $|V| \geq 3, d(u) + d(v) \geq |V| \forall u, v \in V \Rightarrow G$ is hamiltonian (Ore 1960)
- $d(v) \geq \frac{|V|}{2} \forall v \in V \Rightarrow$ G is hamiltonian (Dirac 1952)

Planarity

Definition 0.34: Planar Graphs
A graph is called *planar* if there is a drawing of G in $\mathbb{R}^2$ s.t. no two edges intersect (except at vertices).

Example 0.8:
TODO{illustration}

Theorem 0.16:
$K_{3,3}$ (complete bipartite graph) and K_5 are not planar.

TODO{illustrations}

Definition 0.35: Faces
A *face* of a drawing of a graph is a region bounded by edges.

Theorem 0.17: Euler's Polyhedran Formula
$|V| - |E| + |F| = 2$ for any drawing of a planar connected graph.

Proof 0.19:
Induction on $|F|$.

Induction Start: $|F| = 1$
$\Rightarrow G$ is a tree

$\Rightarrow |V| - |E| + |F| = 2$

Induction Step: $|F| > 1$.
$\Rightarrow \exists e$ bounding two faces, let $G' = G \backslash e$
$\Rightarrow |V'| = |V|, |E'| = |E| - 1, |F'| = |F| - 1$
$\Rightarrow 2 = |V'| - |E'| + |F'| = |V| - |E| + 1 + |F| - 1$

Lemma 0.5:
G simple planar connected graph and every edge bounds two faces, then

- $|E| \leq 3|V| - 6$ and
- if G additionally has no triangles then $|E| \leq 2|V| - 4$

Proof 0.20:
$f_j := |\{\text{faces with } j \text{ bounding edges}\}|$
$\Rightarrow |F| = \sum_{j \geq 3} f_j$
$\Rightarrow 3|F| \leq \sum_{j \geq 3} j f_j = 2|E|$
$\Rightarrow 0 = 3|V| - 3|E| + 3|F| - 6 \leq 3|V| - 3|E| + 2|E| - 6 = 3|V| - |E| - 6$

If no triangles:
$4|F| \leq 2|E|$
$\Rightarrow 0 = 2|V| - 2|E| + 2|F| - 4 \leq 2|V| - 2|E| + |E| - 4 = 2|V| - |E| - 4$

Corollary 0.2:

- $K_{3,3}$ is not planar: no triangles and $|V| = 6, |E| = 9$
- K_5 is not planar $|V| = 5, |E| = 10$

Theorem 0.18: Kuratowski-Wagner
G is planar if and only if G has no subgraph which is a subdivision of $K_{3,3}$ or K_5.

TODO{include lecture 7}

Combinatorics

unfinished

Balls in Boxes

We have k balls and n boxes. Balls and boxes could be labelled. Count any assignment

$$f : [k] \to [n] \ .$$

Notation: $[n] = \{1, \dots, n\}$. f means ''put balls into boxes''. f can be injective (no two balls in same box) or surjective (no empty box). How many *arbitrary* functions from $[k]$ to $[n]$ are there? Answer: n^k. For injective case: $n \cdot (n-1) \cdots (n-k+1)$. For surjective case: not a nice formula.

TODOmake table of combinatoric equalities

Let the balls be unlabelled and the boxes labelled. Injective case:

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

because $k! \cdots \binom{n}{k} = n \cdot (n-1) \cdots (n-k+1)$. For the arbitrary case: $\binom{n+k-1}{k}$.

TODO{make table for these verbal descriptions}

Some identities:

- $(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}$ means n balls and 2 boxes. TODOswitch k and n For instance, the term $2xy^3$ means two possibilities to put 1 ball in the x-box and 3 balls in the y-box.
- $\sum_{m=0}^{n} \binom{m}{k} = \binom{n+1}{k+1}$
- $\sum_{k=0}^{n} \binom{m+k}{k} = \binom{m+n+1}{n}$

Lemma 0.6:
$\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k} \forall n \in \mathbb{C}$

Proof 0.21:
left hand side is a polynomial in n. call it $p(n)$ with degree k. The right hand side is $q(n)$ with degree $max\{k-1, k\} = k$.

We have two polynomials with the same degree $\Rightarrow p(x) = q(x) \forall x \in \mathbb{C}$ because $p(n) = q(n) \forall n \in \mathbb{N}$ (which is left as an exercise).

Theorem 0.19: Vandermonde
$\binom{x+y}{n} = \sum_{k=0}^{n} \binom{x}{k}\binom{y}{n-k}$

Proof 0.22:
$x, y \in \mathbb{N}$: let $|X| = x$, $|Y| = y$, $X \cap Y = \emptyset$

$\binom{x+y}{n}$: #subsets of $X \cup Y$ of size n

$\binom{x}{k}\binom{y}{n-k}$: # subsets of $x \cup Y$ with $|X| = k$

Stirling Numbers

Every permutation of $[n]$ is a product of cycles: start at 1, apply π, obtain $\pi(1)$, apply again, obtain $\pi(\pi(1))$, eventually we will reach $\pi^k(1) = 1$ again, which forms a cycle. Take any $i \in [n]$ that is not contained in the cycle and repeat.

Notations:

- Two-line notation: $\begin{pmatrix} 1 & 2 & \cdots & n \\ \pi(1) & \pi(2) & \cdots & \pi(n) \end{pmatrix}$
- Cycle Notation: $(1, \pi(1), \dots, \pi^k(1))(\dots)(\dots)$

Example 0.9:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 \\ 3 & 1 & 8 & 9 & 2 & 4 & 7 & 5 & 6 & 11 & 10 \end{pmatrix}$$

is the same as

$$(10, 11)(1, 3, 8, 5, 2)(6, 4, 9)(7)$$

In this case, (7) is called a fixed point and (10, 11) is a transposition. If a number is not written in the cycle notation, then it is a fixed point (by convention).

Product:

$$(1, 3, 2) \cdot (2, 3, 4) = (1, 3, 4)(2)$$

Definition 0.36: Stirling Numbers (First Kind)

$s_{n,k}$ is the number of permutations in $\mathfrak{S}_n$ with k cycles. It's called the Stirling number of the first kind.

Example 0.10:

- $s_{n,1} = (n - 1!)$
- $s_{n,n-1} = \binom{n}{2}$
- $s_{n,n} = 1$

Theorem 0.20:

$s_{n,k} = s_{n-1,k-1} + (n - 1)s_{n-1,k}$

Proof 0.23:

- Case: 1 is a fixed point, then $s_{n-1,k-1}$
- otherwise: $s_{n-1,k}$ has k cycles but element 1 is missing, put 1 before any of $\{2, \dots, n\}$

Definition 0.37: Set Partition

A set partition of a finite set A is a set of disjoint, non-empty sets with union A. The sets are called parts or blocks. (Block is more common.)

Definition 0.38: Stirling Number (Second Kind)
$S_{n,k}$ is the number of set partitions of $[n]$ with k parts. This is called the Stirling number of the second kind.

Example 0.11:

- $S_{0,0} = 1$
- $S_{n,0} = S_{0,n} = 0$ for $n > 0$

Theorem 0.21:
$S_{n,k} = S_{n-1,k-1} + k \cdot S_{n-1,k}$

Proof 0.24:

- Case: $\{n\}$ is a singleton block. Then $S_{n-1,k-1}$
- otherwise: put n into one of the k blocks: $k \cdot S_{n-1,k}$

Notation: the standard way to write set partitions is to sort each set and then sort the sets by their minimal elements:

$$\{5,9,3\}\{4,2,6\}\{7\} \to \{2,4,6\}\{3,5,9\}\{7\}$$

Theorem 0.22:

- $(x)_n := x^{\underline{n}} = x \cdot (x-1) \cdots (x-n+1) = \sum_{k=0}^{n} (-1)^{n-k} \cdot s_{n,k} \cdot x^k$
- $x^n = \sum_{k=0}^{n} S_{n,k} \cdots x^{\underline{n}}$

Remark 0.6:
$V_n = \{\}$ is a vector space. $\{1, x, \cdots, x^n\}$ is a basis of V_n and $\{1, x, x^{\underline{2}}, \ldots, x^{\underline{n}}\}$ is also a basis. The change of basis matrices are $(S_{n,k})_{n,k}$ and $((-1)^{n-k} s_{n,k})_{n,k}$
TODO: finish

Proof 0.25:
Induction on n: $x^{\underline{0}} = 1 = s_{0,0} \cdot x^0$
$x^{\underline{n}} = x^{\underline{n-1}} \cdot (x-n+1) = (x-n+1) \sum (-1)^{n-1+k} \cdot s_{n-1,k} \cdot x^k = \sum (-1)^{n-1+k} \cdot s_{n-1,k} \cdot x^{k+1} + (n-1) \sum (-1)^{n-1+k} \cdot s_{n-1,k} \cdot x^k = TODO$

Generating Functions

Power series: a sequence $(a_n)_{n \in \mathbb{N}}, a_n \in \mathbb{C}$

Consider $\sum_{n\geq 0} a_n z^n$ is the series with cofficients a_n.

Idea: Power series is useful for approximating functions.

$\sum a_n z^n$ may or may not converge for a given $z \in \mathbb{C}$.

Definition 0.39: Formal Power Series (FPS)

A formal power series (FPS), written $\sum a_n z^n$ is the same information as the sequence $(a_n)_{n\in\mathbb{N}}$

Operations on FPS, like addition, multiplication, differentiation, etc.

$\sum_{n=0}^{\infty} a_n z^n \overset{powerset}{:=} \lim_{N\to\infty} \sum_{n=0}^{N} a_n z^n$ is a limit of a sequence of complex numbers: $a_0, (a_0 + a_1 z), \ldots$

Theorem 0.23:

$\lim_{N\to\infty} \sum_{n=0}^{N} a_n z^n$ exists, if $|z| < \frac{1}{\limsup_{n\to\infty} \sqrt{|a_n|}} =: R$ TODO{it should be the nth root}

If $|z| > R$, the series diverges.

(If $|z| = R$, an ad hoc analysis is necessary.)

Remark 0.7:

$\{z|\text{series converges}\}$ is the domain of convergence, essentially a circle centered at the origin

Example 0.12:

- $\sum_{n\geq 0} z^n = \frac{1}{1-z}$ ... geometric series, $R = 1$
- $\sum_{n\geq 0} \frac{z^n}{n!} = e^z$ ... exponential series, $R = \infty$
- $\sum_{n\geq 0} \binom{\alpha}{n} z^n = (1+z)^\alpha$, $\alpha \in \mathbb{C}$

Theorem 0.24: Identity Theorem for Power Series

$f(z) = \sum a_n z^n$ converges for $|z| < R$ and $R > 0$

$\Rightarrow a_n = \frac{f^{(n)(0)}}{n!}$

Corollary 0.3:

If $|z| < R$:

$$
\begin{aligned}
f(z) & \qquad (2)\\
&= \sum a_n z^n \qquad (3)\\
&= \sum b_n z^n \qquad (4)\\
\Rightarrow a_n &= b_n \forall n \qquad (5)
\end{aligned}
$$

Operations on Formal Power Series

Let $A(z) = \sum a_n z^n, B(z) = \sum b_n z^n$, however, z is not a complex number now.

Write $(a_n) \leftrightarrow A(z), (b_n) \leftrightarrow B(z)$

$((0, 1, 0, \dots) \leftrightarrow z,\ (1, 0, 0, \dots) \leftrightarrow 1,\ (0, 0, 0, \dots) \leftrightarrow 0)$

Definition 0.40: Operations on FPS

- $(\alpha a_n + \beta b_n)_{n \in \mathbb{N}} \leftrightarrow: \alpha A(z) + \beta B(z)$
- $(\sum_{k=0}^{n} a_k b_{n-k})_{n \in \mathbb{N}} \leftrightarrow: A(z) \cdot B(z)$
- $(a_n \gamma^n)_{n \in \mathbb{N}} \leftrightarrow: A(\gamma z)$
- $(a_{n-1})_{n \in \mathbb{N}_{\geq 1}} \leftrightarrow: zA(z)$
- $(na_n) \leftrightarrow: zA'(z)$

Note 0.2:
We will use the term generating function for formal power series. Therefore, a generating function is *not* a function

Example 0.13:

- $\frac{1}{1+z} = \sum_{n \geq 0} (-1)^n z^n$ is an equality of FPS
- $\frac{z}{(1-z)^2} = z(\frac{1}{1-z})' = \sum nz^n$
- $\frac{1}{(1-z)^k} = \sum_{n \geq 0} \binom{n+k-1}{k-1} z^n$

Remark 0.8:
if $A(z) = B(z)$ as FPS and $A(z)$ and $B(z)$ converge as power series for $|z| < R$, then $A(z) = B(z)$ as power series

For instance, $\sum_{n \geq 0} n! z^n$ is a FPS. It converges only at 0 as a power series

Why are FPS useful?

Example 0.14: Towers of Hanoi

Discs of different sizes on three pegs. Goal: move discs to another peg, but no disc is allowed to be under a larger disc, and we may only move one disc at a time.

Recurrence for number of required moves a_n to move n discs to a different peg.

First move smaller $n-1$ discs to other peg, then move largest disc to third peg, and then move the $n-1$ discs on top of that.

$a_n = 2a_{n-1} + 1$ and $a_0 = 0$, but we want an explicit formula for a_n:

- $a_n = 2a_{n-1} + 1 | z^n$
- $a_n z^n = 2a_{n-1} z^n + z^n | \sum$
- $\underbrace{\sum a_n z^n}_{A(z)} = 2 \underbrace{\sum a_{n-1} z^n}_{zA(z)} + \underbrace{\sum z^n}_{\frac{1}{1-z}}$
- $A(z) - a_0 = 2zA(z) + \frac{1}{1-z} - 1$
- $A(z)(1-2z) = a_0 + \frac{1}{1-z} - 1 = \frac{z}{1-z}$
- $A(z) = \frac{z}{(1-z)(1-2z)} = \frac{-1}{1-z} + \frac{1}{1-2z}$
- $A(z) = -\sum z^n + \sum 2^n z^n = \sum (2^n - 1) z^n$
- $\Rightarrow a_n = 2^n - 1$

Example 0.15: Solving Recurrences with Generating Functions

$F_0 = 0, F_1 = 1, F_{n+2} = F_{n+1} + F_n$

- $F(z) := \sum F_n z^n$
- $\sum F_{n+2} z^{n+2} = \sum F_{n+1} z^{n+2} + F_n z^{n+2}$
- $F(z) - F_0 - F_1 z = z(F(z) - F_0) + z^2 F(z)$
- $F(z)(1 - z - z^2) = F_0 + z(F_1 - F_0)$

In general $a_{n+k} + q_1 a_{n+k-1} + \cdots q_k a_n = 0$ for $n \geq 0$, $a_0, \ldots, a_{k-1}$ are given as initial conditions

$$A(z) = \sum_{n\geq 0} a_n z^z$$

$$\sum_{n\geq 0} a_{n+k} z^{n+k} + q_1 \sum a_{n+k-1} z^{n+k} + \cdots + q_k \sum a_n z^{n+k} = 0$$

$$A(z) - a_0 - a_1 z - \cdots - a_{k-1} z^{k-1} + q_1 z(A(z) - \sum_{i=0}^{k-2} a_i z^i) + \cdots q_k z^k A(z) = 0$$

$$A(z) \underbrace{(1 + q_1 z + \cdots q_k z^k)}_{q(z)} = p(z)$$

with $p(z)$ a polynomial of degree at most $k-1$. Essentially, $p(z)$ contains the initial conditions while $q(z)$ describes the recurrence.

Then, $A(z) = \frac{p(z)}{q(z)}$, which is a reational function! (very nice)

Partial fraction decomposition:

1. find roots of $q(z) = \prod_{i=1}^{r} (z - z_i)^{\lambda_i}$, $\sum \lambda_i = l$
2. Ansatz: $\frac{p(z)}{q(z)} = \sum_{i=1}^{r} \sum_{j=1}^{\lambda_i} \frac{\tilde{A}_{ij}}{(z-z_i)^j}$
3. expand to generating function: $\sum_{i=1}^{r} \sum_{j=1}^{\lambda_i} \frac{A_{ij}}{(1-z/z_i)^j}$
4. $\sum_{n\geq 0} \underbrace{(A_{11} + \binom{n+1}{1} A_{12} + \cdots + \binom{n+\lambda_1-1}{\lambda_1} A_{1\lambda_1})}_{p_1(n)} (\frac{z}{z_1})^n + \cdots + \sum \ldots$
5. $= \sum \underbrace{(p_1(n)(\frac{1}{z_1})^n + \cdots + p_r(n)(\frac{1}{z_r})^n)}_{=a_n} z^n$

Definition 0.41: Characteristic Polynomial

$\chi(z) := z^k + q_1 z^{k-1} + \cdots + q_k$ is the characterisitc polynomial of the recurrence relation.

$(\chi(z) = q(z)|_{z^k n \to z^n - k})$

$\chi(z) = \prod_{i=1}^{r} (z - \frac{1}{z_i})^{\lambda_i}$

Example 0.16: Characteristic Polynomial of Fibonacci Sequence

$a_n = \frac{1}{\sqrt{5}}$ TODO{finish formula}

Unlabelled Enumeration

Definition 0.42: Binary Trees
A binary tree is a rooted tree where each node has no successors or 2 successors.

Definition 0.43: Set of all Binary Trees
$\mathcal{B}$ is the set of all binary trees

$\mathcal{B} = \{\cdot\} \cup \{\}$ TODO{finish depiction}

$\mathcal{B}(z) = \sum_{n \geq 0} b_n z^n$ where b_n is the number of binary trees with n internal nodes, $b_0 = 1$, $b_1 = 1$, $b_2 = 2$

- $\mathcal{B}(z) = 1 + z\mathcal{B}^2(z)$
- $\mathcal{B} = \frac{1-\sqrt{1-4z}}{2z} = 1 + z + 2z^2 + 5z^3 + 14z^4 + 42z^5 + \dots$

Dictionary for unlabelled structures

Definition 0.44:
$A(z) = \sum_{n \geq 0} \#\text{elements of size } n \cdot z^n$

- $(\mathcal{A} \cup \mathcal{B})(z) = A(z) + B(z)$
- $(A \times B)(z) = A(z) \cdots B(z)$, (size of (a, b) is the size of a plus size of b)
- $(sequencesofobjectsinA)(z) = 1 + A(z) + A^2(z) + \cdots = \frac{1}{1-A(z)}$

Example 0.17: Sequences of Ones and Twos
Ones have size 1, twos have size 2.

- $\emptyset$
- 1
- $1 + 1, 2$
- $1 + 1 + 1, 1 + 2, 2 + 1$
- $1 + 1 + 1 + 1, 1 + 1 + 2, 1 + 2 + 1, 2 + 1 + 1, 2 + 2$
- $\dots$

$1 + (z + z^2)^2 + (z + z^2)^3 + (z + z^2)^4 + \cdots = \frac{1}{1-(z+z^2)}$

Example 0.18:
We have red, blue and yellow balls. $\underbrace{\text{2 or 3 red ones}}_{r^2+r^3}$, $\underbrace{\text{at least one blue}}_{b+b^2+b^3+\cdots=\frac{b}{1-b}}$ and $\underbrace{\text{at most one yellow}}_{1+y}$. We have n ball. How many possibilities are there?

$\Rightarrow A(z) = ((rz)^2 + (rz)^3)\frac{bz}{1-bz}(1+yz)$

We want to find $[z^n]A(z) =$ generating function in r, b, y

Example 0.19: Combinations without Repetitions

Balls $a_1, a_2, \ldots, a_N$ Select balls, but no ball twice, generating function:

$(1+a_1)(1+a_2)\cdots(1+a_N)$, $a_i := z$: $(1+z)^N = \sum_n \geq 0\binom{N}{n}z^n$

If we allow repetition: $(\sum a_1^n)(\sum a_2^n)\cdots(\sum a_N^n) \to (\frac{1}{1-z})^N = \sum \binom{n+N-1}{n}z^n$

Labelled Enumeration

For the unlabelled case, we had $A(z) = \sum a_n z^n$, where a_n was the number of objects of size n.

For the labelled case, it is a bit more complicated: $\hat{A}(z) = \sum a_n \frac{z^n}{n!}$. This is called the exponential generating function.

Example 0.20: Permutations

$A(z) = \sum n! z^n$

$\hat{A}(z) = \sum n! \cdot z^n/n! = \frac{1}{1-z}$

Example 0.21: Cyclic Permutations

$\hat{A}(z) = \sum_{n\geq 1}(n-1)! \cdot z^n/n! = ln(\frac{1}{1-z})$

Dictionary for labelled enumeration

- $(\widehat{A \cup B})(z) = \hat{A}(z) + \hat{B}(z)$
- $(\widehat{A \times B})(z) = \hat{A}(z) \cdot \hat{B}(z)$
- $setofobjectsin\hat{A}(z) = e^{\hat{A}(z)}$
- $cyclesofobjectsin\hat{A}(z) = log(\frac{1}{1-\hat{A}(z)})$
- $\widehat{AB}$

Definition 0.45: Product of Labelled Set (Pairs of Labelled Objects)

Let $\mathcal{A}, \mathcal{B}$ be sets of labelled objects that are closed under relabelling. Let $\mathcal{A}[1, \ldots, n]$ be the set of objects with labels $1, \ldots, n$.

Then, $\mathcal{A} \times \mathcal{B}[1, \ldots, n]$ is the set of pairs (a, b) with $a \in \mathcal{A}, b \in \mathcal{B}$ such that the total set of labels is $1, \ldots, n$.

Formally, $\mathcal{A} \times \mathcal{B}[1, \ldots, n] = \bigcup_{TODO} \mathcal{A}[U] \times [V]$.

Example 0.22:

$A[1,2,3] = \{1,2,3\}$ is *not* closed under relabelling. $A[1,2,3]$ produces *all* objects with labels $\{1,2,3\}$

Example 0.23:

$A[1,2] = \{12, 21\}$

$B[1,2] = \{12, 21\}$

$A \times B[1,2,3,4] = \{(13,42),(12,34),(13,24),(31,42),(21,34),(12,43),\dots\}$

(There will be 24 pairs.)

$$
\begin{aligned}
[z^n](\widehat{A \times B})(z) &= \sum_{k=0}^{n} \binom{n}{k} a_k b_{n-k} \\
(\widehat{A \times B})(z) &= \sum_{n} \sum_{k=0}^{n} \binom{n}{k} a_k b_{n-k} \cdot z^n / n! \\
&= \sum_{n} \sum_{k=0}^{n} \frac{n!}{k!(n-k!)} \frac{1}{n!} a_k b_{n-k} z^k z^{n-k} \\
&= \sum_{n} \sum_{k=0}^{n} \frac{a_k z^k}{k!} \frac{b_{n-k} z^{n-k}}{(\underbrace{n-k}_{l})!} \\
&= \sum_{k \geq 0} \sum_{l \geq 0} \frac{a_k z^k}{k!} \frac{b_{n-k} z^{n-k}}{l!} \\
&= \hat{A}(z) \cdot \hat{B}(z)
\end{aligned}
$$

Definition 0.46:

Let A be a set closed under relablling. Then, $set(A)[1,\dots,n]$ is the set of objects $\{a_1,\dots,a_l\}$ such that the total set of labels is $\{1,\dots,n\}$

Example 0.24:

Sets of cycles with lables $\{1,2,3,4\}$

Cycles of $\{1\}$

TODO

Sets of cycles are permutations!

$\widehat{sets}(z) = e^z$, $\widehat{cycles}(z) = ln(\frac{1}{1-z})$

$set(\widehat{cycles})(z) = e^{ln(\frac{1}{1-z})} = \frac{1}{1-z} = \widehat{permutations}(z)$

$B := setsofnon - emptysets$

$$\hat{B}(z) = e^{e^z - 1}$$

$\hat{B}(z) istheexponentialgeneratingfunctionforsetpartitions.$

Partially Ordered Sets

Definition 0.47: Partial Order

A partial order $(P, <)$ is a set P together with a relation $<$, such that

- $a < b \Rightarrow \neg b < a$ (anti-symmetry)
- $a < b, b < c \Rightarrow a < c$ (transitivity)

Notation:

- $a \leq b$ means $a < b \vee a = b$.
- $a \lessdot b$ means $a < b$ and $\nexists c : a < c \wedge c < b$, "$a$ is covered by b"

Remark 0.9:

Notation: In Hasse diagrams, the arcs are drawn from bottom to top.

Example 0.25:

$(\mathbb{N}, |)$

TODO

Remark 0.10:

$1|6$ but *not* $a \lessdot 6$

Definition 0.48: Total Order

A linear (or total) order is a poset with $a \leq b$ or $b \leq a$ for all a, b

Example 0.26:

$(2^A, \subseteq)$

TODO

Definition 0.49: Minimal/Maximal Elements

A minimal element of a poset $(P, \leq)$ is an element $a \in P$ such that $\forall b \in P : a \leq b$. Analogously for maximal elements.

(Minimal/maximal elements are not necessarily unique.)

Definition 0.50: Interval
An interval is a subset $[x, y] := \{z|x \leq z \leq y\}$ of P

$(P, \leq)$ is locally finite if $|[x, y]| \leq \infty \forall x, y \in P$

Definition 0.51: Boundedness
P is bounded if

- $\exists M \subseteq P : \forall x \in P \exists y \in M : x \leq y$ and
- $\exists M \subseteq P : \forall x \in P \exists y \in M : y \leq x$

$(P, \leq)$ a poset, $f : P \to \mathbb{R}$, $S_f(x) := \sum_{z \leq x} f(z)$.

Given S_f, can we recover f?: Yes!

Definition 0.52: Möbius Function
$(P, \leq)$ a poset, locally finite, with a minimal element 0

$\mu : P \times P \to \mathbb{R}$ is the Möbius function of P if it satisfies

$$\forall x, y : \sum_{z \in [x,y]} \mu(z, y) = \delta_{x,y} = \begin{cases} 0 & x \neq y \\ 1 & x = y \end{cases}$$

Remark 0.11:
This Relation determines μ uniquely.

Remark 0.12:
For $x \not\leq y : \mu(x, y) := 0$

Example 0.27:

- $[x, x] = \{x\} \Rightarrow \mu(x, x) = 1$
- $[x, y] = \{x, y\} \Rightarrow \mu(x, y) + \mu(y, y) = 0 \Rightarrow \mu(x, y) = -1$

Example 0.28:
$(\mathbb{N}, \leq)$:

- $\mu(n, n) = 1$
- $\mu(n, n + 1) = -1$
- $\mu(n, m) = 0 \forall m \geq n + 2 \vee m < n$

Example 0.29:
TODO{finish example}

Definition 0.53: Product of Posets
$(P_1, \leq), (P_2, \leq)$ Posets. Then $(P_1, \leq) \times (P_2, \leq) := (P_1 \times P_2, \leq)$:

Has $(x_1, x_y) \leq (y_1, y_2) \Leftrightarrow (x_1 \leq y_1) \wedge (x_2 \leq y_2)$

Theorem 0.25:
If both P_1 and P_2 have a unique minimal element, then $P_1 \times P_2$ has a unique minimal element and $\mu_{P_1 \times P_2}(\vec{x}, \vec{y}) = \mu_{P_1}(x_1, y_1) \cdot \mu_{P_2}(x_2, y_2)$ with $\vec{x} = (x_1, x_2)$ and $\vec{y} = (y_1, y_2)$

Proof 0.26:
Left as an exercise to the reader

Example 0.30:
$A = \{a_1, \ldots, a_n\}$, $(2^A, \subseteq) \cong (\{0,1\}, \leq)^n$

e.g. $n = 5$, $X = \{a_2, a_5\} \cong 01001$, $Y = \{a_1, a_3, a_3, a_5\} \cong 11101 \Rightarrow X \leq Y$

$\mu(X,Y) = \mu(0,1)\mu(1,1)\mu(0,1)\mu(0,0)\mu(1,1) = (-1) \cdot 1 \cdot (-1) \cdot 1 \cdot 1 = 1$

Note: The relation is a component wise comparison. It is *not* the lexicographical order.

In general, $X \subseteq Y : \mu(X,Y) = (-1)^{\text{different places}} = (-1)^{|Y \setminus X|} = (-1)^{|Y|-|X|}$

Theorem 0.26: Möbius Inversion
$(P, \leq)$ locally finite with a unique minimal element 0

$f : P \to \mathbb{R}$, $S_f(x) = \sum_{z \in [0,x]} f(z) \Rightarrow f(x) = \sum_{z \in [0,x]} S_f(z)\mu(z,x)$

Proof 0.27:

$$\begin{aligned}
\sum_{z \in [0,x]} S_f(z)\mu(z,x) &= \sum_{0 \leq z \leq x} \sum_{0 \leq y \leq z} f(y)\mu(z,x) \\
&= \sum_{0 \leq y \leq z} \sum_{y \leq z \leq x} f(y)\mu(z,x) \\
&= TODO \\
&= \sum_{y \in [0,x]} f(y)\delta_{y,x} \\
&= f(x)
\end{aligned}$$

Example 0.31:
$(\mathbb{N}, \leq)$

$$\mu(m,n) = \begin{cases} 1 & m = n \\ -1 & m+1 = n \\ 0 & \text{otherwise} \end{cases}$$

$f : \mathbb{N}_0 \to \mathbb{R}$

TODO

Example 0.32: Inclusion Exclusion

$A_1, \dots, A_m \subseteq M$

consider $(2^{\{1,\dots,m\}}, \supseteq)$ (the poset of indices)

$I \subseteq \{1, \dots, m\}$

$f(I) := |\bigcap_{i \in I} A_i \cap \bigcap_{j \in \{1,\dots,m\} \setminus I} \overline{A_j}|$

$f(I)$ is the number of elements *precisely* in all $A_i, i \in I$

$S_f(I) = \sum\limits_{J \supseteq I} f(J) = |\bigcap_{i \in I} A_i|$

$S_f(I)$ is the number of elements in $A_i, i \in I$ (but not *precisely* in A_i)

Möbius inversion: $f(I) = \sum\limits_{J \supseteq I} S_f(J)\mu(J,I) = \sum\limits_{J \supseteq I} (-1)^{|I|+|J|} |\bigcap_{j \in J} A_j|$

In particular, $f(\emptyset) = |\bigcap_{j \in \{i,\dots,m\}} \overline{A_j}| = \sum\limits_{J \subseteq \{1,\dots,m\}} (-1)^{|J|| \bigcap_{j \in J} A_j|}$

This is the principle of inclusion/exclusion

Example 0.33:

"classical" number theoretic Möbius functions

$(\mathbb{N}, |)$

$m = p_1^{e_1} \cdots p_r^{e_r} \setminus n = p_1^{f_1} \cdots p_r^{f_r}$ with $e_i, f_i \in \mathbb{N}_0$

$m|n \Leftrightarrow e_i \leq f_i \forall i$

$(\mathbb{N}, |) \cong (\mathbb{N}_0, \leq) \times (\mathbb{N}_0, \leq) \times \dots$

$\mu(n) := \mu_{(\mathbb{N},|)}(1,n) = \mu(0,e_1) \cdot \mu(0,e_2) \cdots \mu(0,e_r) \cdot \underbrace{\mu(0,0)}_{1} \cdots$

$$\mu(0,k) = \left\{ \begin{array}{ll} 1 & k = 0 \\ -1 & k = 1 \\ 0 & k > 1 \end{array} \right\} = \begin{cases} 1 & \dots \\ (-1)^r & \dots \\ 0 & \text{otherwise} \end{cases} \quad \text{TODO\{finish formula\}}$$

Conclusion: $f : \mathbb{N}_+ \to \mathbb{R}$ TODO{finish example}

Lattices

Definition 0.54:
$(P, \leq)$ poset, $x, a, b \in P$, then if $a \leq x \leq b$, then a is called a lower bound and b an upper bound for x.

Let $x \vee y$ (say "x join y") be **the** smallest common upper bound of x and y (if it exists).

Let $x \wedge y$ (say "x meet y") be **the** largest common lower bound of x and y (if it exists).

(If x, y have no common upper/lower bound or more than one, they cannot be joined/met.)

Notation: TODO{insert big vee}

Basic properties:

- $x \vee y = y \vee x$
- $x \vee x = x$
- $(x \vee y) \vee z = x \vee (y \vee z)$
- $a \vee (a \wedge b) = a = a \wedge (a \vee b)$

Definition 0.55: Lattices
L is a lattice if $\forall x, y \in L : \exists x \vee y$ and $x \wedge y$.

J is a join-semi-lattice if $\forall x, y \in J : \exists x \vee y$.\ J is a meet-semi-lattice if $\forall x, y \in J : \exists x \wedge y$.

L is a complete lattice if $\forall X \in L : \exists V_{x \in X} x$ and & $_{x \in X} x$ TODO{fix notation}

Example 0.34:
$(2^M, \subseteq)$ is a lattice: $A, B \subseteq M \Rightarrow A \vee B := A \cup B$ and $A \wedge B := A \cap B$.

Lemma 0.7:
L lattice, $x, y, s, t \in L$

- $x \leq s$ and $y \leq s \Rightarrow x \vee y \leq s$
- $x \geq t$ and $y \geq t \Rightarrow x \wedge y \geq t$
- $x \leq y \Leftrightarrow x \vee y = y \Leftrightarrow x \wedge y = x$

Lemma 0.8:
L a finite meet-semi-lattice with a ''1" element (a top element which is larger than all others)

$\Rightarrow L$ is a lattice

Proof 0.28:

$x, y \in L$, $B = \{u \in L | x \leq u \text{ and } y \leq u\}$

$B \neq \emptyset$ because $1 \in B$

$|B| < \infty$ (because L is finite) $\Rightarrow B = \{u_1, \ldots, u_m\}$

$u := u_1 \wedge \ldots \wedge u_m \in B$

$\Rightarrow u =: x \vee y$

Example 0.35:

$\Pi_n = \{\pi \text{ a set partition of [n]}\}$

Π_n, refinement is a lattice. (Refinement means take a block and split it into two.)

"1" is the set partition with one block.

"0" is the set with all singletons.

$\alpha, \beta \in \Pi_n : \alpha \wedge \beta =$ set partition where i, j are in the same block $\Leftrightarrow i, j$ are in the same block in α and in β

Theorem 0.27:

L lattice with "0" and "1" elements, $b \in L, b \neq 1$

$$\Rightarrow \mu(0,1) = -\sum_{x:x\wedge b=0, x\neq 0} \mu(x,1)$$

Proof 0.29:

$$\Leftrightarrow \sum_{x:x\wedge b=0} \mu(x,1) = 0 \text{ (because } 0 \wedge b = 0)$$

$$N(y) := \sum_{x:x\wedge b=y} \mu(x,1) \forall y \leq b$$

$$S_N(b) := \sum_{y:y\leq b} N(y) = \sum_{y\leq b} \sum_{x\wedge b=y} \mu(x,1) = \sum_{x\in L} \mu(x,1) = \sum_{x\in[0,1]} \mu(x,1) = 0$$

Möbius inversion $\Rightarrow N(b) = \sum_{y\leq b} \underbrace{S(y)}_{0} \mu(y,b) = 0$

And therefore, in particular, $N(0) = 0$.

Corollary 0.4:

$\mu_{\Pi_n}(0,1) = (-1)^{n-1}(n-1)!$

Proof 0.30:

choose $b = \{\{1 \ldots n-1\}\{n\}\}$

then use induction

Number Theory

Definition 0.56: Divisibility

$a, b \in \mathbb{Z}$ then $a|b \Leftrightarrow \exists c \in \mathbb{Z} : a \cdot c = b$

More generally, this applys to any ring, e.g. $\mathbb{Z}[X]$ or $\mathbb{Z}_m$)

Definition 0.57: GCD

$a, b \in \mathbb{Z}$, $d = gcd(a, b) \Leftrightarrow d|a$ and $d|b$ and it is the greates TODO{notation}

$b > 0 \Rightarrow \exists q, r \in \mathbb{Z} : a = bq + r$ and $0 \leq r < b$

Euclidean Algorithm:

TODO{insert algorithm}

Theorem 0.28:

$d = gcd(a, b) \Rightarrow \exists e, f \in \mathbb{N} : d = ae + bf$

Proof 0.31:

Euclidean Algorithm backwards

Remark 0.13:

$d = ae + bf \Rightarrow gcd(a, b)|d$

Definition 0.58: Integral Domain

R is an integral domain if it has no zero-divisors:

$a \cdot b = 0 \Rightarrow a = 0$ or $b = 0$

Example 0.36:

$\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$

$2 \cdot 3 = 0$, therefore, 2 and 3 are zero-divisors

Example 0.37:

- $\mathbb{Z}_p$ for p prime
- $\mathbb{Z}[X]$

Definition 0.59: Euclidean Ring

R is a Euclidean ring if R is an integral domain and there exists a "Euclidean function" $n : R \to \mathbb{N}_0$ such that $\forall a, b, \in R, b \neq 0 \exists q, r \in R : a = bq + r$ TODO{finish definition}

Example 0.38:

- $\mathbb{Z}$: $n(a) := |a|$
- k a field, $k[X]$: $n(a) := deg(a)$ (Warning: $\mathbb{Z}[X]$ is not euclidean)

Remark 0.14:
If x is invertible (x is a unit, i.e. $\exists \bar{x} : x \cdot \bar{x} = 1$) then $gcd(a, b) = gcd(a, x \cdot b)$

Remark 0.15:
$R^* := \{x | x \text{ a unit}\}$

Example 0.39:

gcd(x^4 + 3x^3 - 3x^2 - 7x + 6, x^3 + x^2 - x + 15) = x+3

because

$$x^4 + 3x^3 - 3x^2 - 7x + 6 = (x^3 + x^2 - x + 15) \cdot x + \underbrace{2x^3 - 2x^2 - 22x + 6}_{deg(\cdot)=3<4}$$

$$x^3 + x^2 - x + 15 = (2x^3 - 2x^2 - 2xx + 6) \cdot \frac{1}{2} + 2x^2 \dots$$

$\vdots$

Definition 0.60: Prime Numbers
$p \in \mathbb{N}_{>1}$ is a prime number if $m | p \Rightarrow m \in \{\pm 1, \pm p\}$

$\mathbb{P}$ is the set of primes.

Remark 0.16:
In arbitrary integral domains, such a p is called irreducible. In Euclidean domains, prime and irreducible is the same.

Remark 0.17:
properly:

$p \in R$ is irreducible if $\forall m : m | p \Rightarrow m \in \{\pm 1, \pm p\}$.

$p \in R$ is prime if $\forall a, b : p | ab \Rightarrow p | a \vee p | b$.

If R is a euclidean domain (e.g. $\mathbb{Z}$), then prime and irreducible are equivalend

Theorem 0.29:
$p \in \mathbb{P}, p | a \cdot b \Rightarrow p | a \vee p | b$

(In Euclidean domains, this is the denition of primes.)

Proof 0.32:
two cases:

- $p|a$
- $p \not| a \Rightarrow gcd(p, a) = 1$ and therefore $\exists e, f : pe + af = 1$. $b = b \cdot 1 = b \cdot (pe + af) = bpe + abf$. We see that $p|bpe$ and $p|abf$. Therefore, $p|b$

Remark 0.18:
Consider $\mathbb{Z}[\sqrt{-5}]$, then 3 is irreducible, i.e. $m|3 \Rightarrow m \in \{\pm 1, \pm 3\}$, but $3|9 = (2+\sqrt{-5})(2-\sqrt{-5})$ but neither is divisble by 3.

Theorem 0.30: Prime Factorization
$n \in \mathbb{N}_{\geq 1} \Rightarrow n = p_1 \cdots p_r$ for $p_i \in \mathbb{P}$

Proof 0.33:
Induction: Base case: $n \in \mathbb{P} \Rightarrow n = p$

Otherwise: $\exists n_1, n_2 < n : n = n_1 n_2 \Rightarrow n_1 = p_1 \cdots p_k, n_2 = p_{k+1} \dots p_r$

Theorem 0.31:
The factorization into primes is unique (except for the ordering), i.e.:

$$n = \prod_{p \in \mathbb{R}} p^{\nu_p(n)}$$

where $\nu_p(n)$ is the multiplicity of p in n

Remark 0.19:
We can use the prime factorization to find the gcd and the lcm:
- $gcd(a, b) = \prod_{p \in \mathbb{P}} p^{min(\nu_p(a), \nu_p(b))}$
- $lcm(a, b) = \prod_{p \in \mathbb{P}} p^{max(\nu_p(a), \nu_p(b))}$

Theorem 0.32:
There are infinitely many primes.

Proof 0.34:
Let $a, b, c, \dots, k$ be (finitely many) prime numbers. Take the product $P = abc \cdots k$ and add 1. Either $P+1$ is prime or not. If it is prime, then it is larger than $a, b, c, \dots, k$. Otherwise, there exists a prime p which divides $P+1$. p is different from $a, b, c, \dots, k$ because it would divide P and $P+1$ so it would divide $P - P + 1 = 1$, which is impossible.

Congruence Relations and Residue Classes

Definition 0.61:
$m \in \mathbb{Z}_{\geq 1}$, we call it "modulus"; $\bar{a} := a + m \cdot \mathbb{Z} := \{a + m \cdot z | z \in \mathbb{Z}\}$

Remark 0.20:
$a \in \bar{a}, \bar{a} = \bar{b} \Leftrightarrow m | a - b$

Notation:

$a \equiv b \mod m$
$a = b \ (m)$

Definition 0.62:
$\mathbb{Z}_m = \{\bar{a} = a + m\mathbb{Z} | a \in \mathbb{Z}\} = \{\bar{0}, \bar{1}, \ldots, \overline{m-1}\}$

Example 0.40:
$\mathbb{Z}_2 = \{\bar{0}, \bar{1}\}$

$\bar{0}$ are the even numbers, $\bar{1}$ are the odd ones.

Definition 0.63:
$(\mathbb{Z}_m, +, \cdot)$ with $\bar{a} + \bar{b} := \overline{a+b}$ and $\bar{a} \cdot \bar{b} := \overline{a \cdot b}$, then $(\mathbb{Z}_m, +, \cdot)$ is a commutative ring.

Remark 0.21:
Notation: $\bar{x} \cdot \bar{a} = 1$, then $\bar{x}^{-1} := \bar{a}$

Example 0.41:
$m = 5$, $\bar{2}^{-1} = \bar{6}$

Theorem 0.33:
$\exists \bar{a}^{-1} \in \mathbb{Z}_m \Leftrightarrow gcd(a, m) = 1$ (i.e. a and m are coprime)

Proof 0.35:
TODO

Definition 0.64:
$\mathbb{Z}_m^* = \{\bar{a} \in \mathbb{Z}_m | gcd(a, m) = 1\}$

Example 0.42:

- $\mathbb{Z}_5^* = \{1, 2, 3, 4\}$
- $\mathbb{Z}_6^* = \{1, 5\}$

Example 0.43:

$n \in \mathbb{N}$

$9|n \Leftrightarrow 9|\text{sum of digits of } n$

Proof: TODO

Chinese Remainder Theorem

Theorem 0.34:

$m = m_1 \cdot m_2$, $gcd(m_1, m_2) = 1$ (coprime)

Then, $x \equiv y \mod m \Leftrightarrow x \equiv y \mod m_1 \wedge x \equiv y \mod m_2$

Proof 0.36:

TODO

Corollary 0.5:

$m = \prod_{i=1}^{r} m_i$ with m_i pairwise coprime

then, $x \equiv y \mod m \Leftrightarrow \forall i : x \equiv y \mod m_i$

Theorem 0.35: Chinese Remainder Theorem

$$\begin{aligned} x &\equiv a_1 \mod m_1 \\ &\vdots \\ x &\equiv a_r \mod m_r \end{aligned}$$

where all m_i are pairwise coprime.

This system of congruences has a unique solution mod $m = \prod_{i=1}^{r} m_i$

The solution is given by

$$x := \sum_{j=1}^{r} \frac{m}{m_j} b_j a_j$$

with $b_j := (\frac{m}{m_j})^{-1} \mod m_j$

Example 0.44:

$$3x \equiv 2 \mod 5$$
$$2x \equiv 7 \mod 11$$

$$\Downarrow$$

$$x \equiv 4 \mod 5$$
$$x \equiv 9 \mod 11$$

$$\Downarrow$$

$$b_1 = 11^{-1} = 1 \mod 5$$
$$b_2 = 5^{-1} = 9 \mod 11$$

$$\Downarrow$$

$$x = 11 \cdot 1 \cdot 4 + 5 \cdot 9 \cdot 9 = 9 \mod 55$$

(which is the unique solution mod 55)

Proof 0.37:

1. x is a solution:
   since $gcd(m_i, m_j) = 1$ for $i \neq j$ it follows that $gcd(\frac{m}{m_j}, m_j) = 1 \Rightarrow \exists b_j$

   $\frac{m}{m_j} \equiv 0 \mod m_i \forall i \neq j \Rightarrow \sum_{j=1}^{r} \frac{m}{m_j} b_j a_j \equiv \frac{m}{m_i} b_i a_i \equiv a_i \mod m_i$
2. x is unique mod m:
   suppose $x \equiv a_i \mod m_i$ and $y \equiv a_i \mod m_i$ for all i

   $\Rightarrow x \equiv y \mod m_i \Rightarrow x \equiv y \mod m$

Example 0.45: finding inverses

$m = 17$, find 13^{-1}, ie, solve $13x \equiv 1 \mod 17$

$gcd(13, 17) = 1$, which is the condition for the existence of an inverse

$\Rightarrow \exists e, f : 13e + 17f = 1$

$\Rightarrow 13e = 1 \mod 17$

e and f can be found with the extended Euclidean algorithm. In this case, it gives us $e = 4, f = -3$

Remark 0.22: Reduction of congruence relations

$3b \equiv 3c \mod 5 \Rightarrow b \equiv c \mod 5$ because 3 has an inverse mod 5.

But: In $3b \equiv 3c \mod 6$, 3 has no inverse

- $\Rightarrow 3b = 3c + 6k$
- $\Rightarrow b = c + 2k$
- $\Rightarrow b \equiv c \mod 2$

In general: $ab \equiv ac \mod am \Rightarrow b \equiv c \mod m$

Euler-Fermat and Rivest-Shamir-Adleman

Definition 0.65:

$< \mathbb{Z}_m^*, \cdot >$ is a group

$|\mathbb{Z}_m| = m$
$|\mathbb{Z}_m^*| =: \phi(m)$ is the (Euler) totient, i.e. the number elements coprime m

Example 0.46:

- $\phi(5) = 4$
- $\phi(6) = 2$
- $\phi(7) = 6$

Theorem 0.36:

For $p \in \mathbb{P}$: $\phi(p) = p - 1$

- $$\begin{aligned}\phi(p^e) &= |\{0, \dots, p^e - 1\}| - |\{0, p, 2, p, \dots, (p^{e-1} - 1)p\}| \\ &= p^e - p^{e-1} \\ &= p^{e(1-1/p)}\end{aligned}$$
- $\phi(\underbrace{p_1^{e_1} \cdot p_2^{e_2}}_{m}) = m \cdot (1 - 1/p_1) \cdot (1 - 1/p_2)$ TODOproof
- $m = p_1^{e_1} \cdots p_r^{e_r} \Rightarrow \phi(m) = m \cdot (1 - 1/p_1) \cdots (1 - 1/p_r)$

Example 0.47:

$\phi(6) = \phi(2 \cdot 3) = 6(1 - 1/2)(1 - 1/3) = 2$

Theorem 0.37: Euler-Fermat

$gcd(a, m) = 1 \Rightarrow a^{\phi(m)} = 1 \mod m$

Special Case: $p \in \mathbb{P}, p \not| a \Rightarrow a^{p-1} = 1 \mod p$

Proof 0.38:

$\mathbb{Z}_m^*)\{\bar{a}_1, \dots, \bar{a}_k\}$, $k = \phi(m)$

$gcd(a, m) \Rightarrow a$ is invertible in $\mathbb{Z}_m \Rightarrow \bar{a} \in \mathbb{Z}_m^*$

$\Rightarrow \mathbb{Z}_m^* = \{\bar{a}\bar{a}_1, \dots, \bar{a}\bar{a}_k\}$ is a permutation of the original residue classes

$\Rightarrow$ TODO{finish}

Theorem 0.38:

$p, q \in \mathbb{P}$ different odd primes, $m = pq$, $v = lcm(p-1, q-1)$

$\Rightarrow \forall a, k \in \mathbb{Z} : a^{kv+1} \equiv a \mod m$

Proof 0.39:

$pq | a^{kv+1} - a$ iff. $p | a^{kv+1} - a$ and $q | a^{kv+1} - a$

$p | a^{kv+1} - a$ because : case 1: $p | a$ or case2: $a^{p-1} \equiv 1 \mod p \Rightarrow a^{kv} \equiv 1 \mod p \Rightarrow a^{kv+1} \equiv a \mod p$

(same for q)

Definition 0.66: RSA Algorithm

$m = p \cdot q$, $gcd(e, v) = 1$ with $v = lcm(p-1, q-1) \Rightarrow \exists d : d \cdot e \equiv 1 \mod v$

message: $a_1, a_2, \dots$ with $0 \leq a_i < m$

$E(a_j) = (a_j^e \mod m) =: b_j \setminus D(b_j) = (b_j^d \mod m)$

Note that $(a_j^e)^d = a_j^{kv+1} \equiv a_j \mod m$

(m, e) is called the "public key"

"E-Signature": several pairs (e_j, d_j) and e_j's are public

User i sends $y := E_j(D_i(x)) = x^{d_i e_j} \mod m$ to user j

User j checks: $D_j(y) = D_j E_j D_i(x) = D_i(x)$ and $E_i(D_i(x)) = x$

Problem: $E(x)$ may have (many) fixed points in $\mathbb{Z}_m$

Primitive Roots

Definition 0.67:

G is a group: $|G|$ is the oder of G.

minimal k such that $x^k = 1$ is the order $ord_G(x)$ of x in G.

Proposition: $ord_G(x) | \; |G|$

Definition 0.68: Cyclic Group

A group generated by a single element, $G =< x >= \{x^0, x^1, x^2, x^3, \dots\}$ is called cyclic.

Remark 0.23:

Groups may be written multiplicatively or additively, depending on convention. Abelian groups are often (but not always) written additively.

Definition 0.69: Primitive Roots

$\bar{a} \in \mathbb{Z}_m^*$ such that $\mathbb{Z}_m^* =< \bar{a} >$, then $\bar{a}$ is called a primitive root mod m.

Example 0.48:

- $\mathbb{Z}_2^* =< \bar{1} >$
- $\mathbb{Z}_3^* =< \bar{2} >$
- $\mathbb{Z}_5^* =< \bar{2} >$
- $\mathbb{Z}_8^* = \{\bar{1}, \bar{3}, \bar{5}, \bar{7}\}$ has no generator

Proposition: $\bar{a}$ is a primitive root mod m, then $\mathbb{Z}_m^* = \{a, a^2, \dots, a^{\phi(m)}\}$ and $a^{\phi(m)} \equiv 1$.

Theorem 0.39:

$\mathbb{Z}_m^*$ is cyclic iff $m \in \{2, 4, p^e, 2p^e\}$ with $p \in \mathbb{P} \backslash \{2\}$ and $e \in \mathbb{N}_{\geq 1}$

Lemma 0.9:

- g is a primitive root mod $p \Rightarrow g$ or $g + p$ is a primitive root mod p^e
- g is a primitive root mod $p^e \Rightarrow g$ or $g + p$ is a primitive root mod $2p^e$

Proof 0.40:

(using the following lemma)

$\phi(p^2) = p(p-1)$, assum that $p - 1 = kl$ with $k, l < p - 1$ and $ord_{\mathbb{Z}_{p^2}^*}(g) = pl$

Lemma 0.10:

$g^{p-1} \equiv 1 \mod p^2$ or $(g+p)^{p-1} \not\equiv 1 \mod p^2$ for g a primitive root mod p

TODO

Proof 0.41:

$(g+p)^{p-1} \equiv g^{p-1} + pg^{p-2} \mod p^2$ (by the binomial theorem)

TODO

Example 0.49:

14 is a primitive root mod 29 but not 29^2.

Definition 0.70: Carmichael Function

$\lambda(m) = \max_{a \in \mathbb{Z}_m^*} ord_{(\mathbb{Z}_m^*, \cdot)}(a)$ is the Carmichael function

Remark 0.24:

- $\lambda(m) | \phi(m)$
- $\lambda(m_1 \cdots m_k) = lcm(\lambda(m_1), \ldots, \lambda(m_k))$
- For $p \in \mathbb{P}$:
  $\lambda(p^r) = \begin{cases} \frac{1}{2}\phi(p^r) & \text{if } p = 2 \wedge r \leq 3 \\ \phi(p^r) & \text{otherwise} \end{cases}$

TODO{include lecture 17}

Polynomials over Finite Fields

Definition 0.71: Rings

$(R, +, \cdot)$ is a ring if $(R, +)$ is an abelian group with neutral element 0 and multiplication satisfies

- $(a + b)c = ac + bc$
- $c(a + b) = ca + cb$
- $a(b \cdot c) = (a \cdot b)c$
- $\exists 1 \in R : \forall a \in R : a \cdot 1 = 1 \cdot a = a$

Remark 0.25:

1. A ring is not a field because in a ring, multiplication does not necessarily have inverse elements.
2. Recall that $(R^*, \cdot)$ is the group of units where R^* is the set of elements with multiplicative inverse.
3. R is an integral domain if $ab = 0 \Rightarrow a = 0 \vee b = 0$ and multiplication is commutative.

Definition 0.72: Euclidean Ring

R is a euclidean ring if there is a map $n : R\backslash\{0\} \to \mathbb{N}_0$ such that $\forall a, b \in R \exists q, r \in R, q \neq 0 : a = bq + r$ with $n(r) < n(b)$ or $r = 0$, and $\forall a, b \in R\backslash\{0\} : n(a) \leq n(ab)$

The reason we are interested in integral domains is that there, we have a theory of divisibility.

- $t|a :\Leftrightarrow \exists c : a = t \cdot c$
- $d = gcd(a, b,) :\Leftrightarrow d|a \wedge d|b \wedge (t|a \wedge t|b \Rightarrow t|d)$

Definition 0.73: Associated Elements

$a, b \in R$ are called associated (write $a \sim b$) iff $\exists r \in R^* : a = rb$

Lemma 0.11:

1. R euclidean ring, $a, b \in R, b \neq 0$, $a|b \Rightarrow n(a) \leq n(b)$.
2. If $a, b \notin R^* \cup \{0\} \Rightarrow n(a) < n(ab)$

Proof 0.42:

1. $a|b \Rightarrow \exists c : b = ac$, $n(a) \leq n(ac) = n(b)$
2. $x = ab$, $\ldots$ Professor didn't manage to prove this

Corollary 0.6:

If d and d' are gcd's of a and b, then $n(d) = n(d')$

Definition 0.74: Irreducibility and Primality

R integral domain, $a \in R \backslash (R^* \cup \{0\})$, then

- a is called *irreducible* iff $a = bc \Rightarrow b \in R^* \vee c \in R^*$
- a is called *prime* iff $a|bc \Rightarrow a|b \vee a|c$

Example 0.50:

$R = \mathbb{Z}$, then $x \in R$ irreducible $\Leftrightarrow x \in \mathbb{P}$ or

TODO

Theorem 0.40:

- prime $\Rightarrow$ irreducibe
- R euclidean, then irreducible $\Leftrightarrow$ prime

Proof 0.43:

- a prime, $a = bc$, if $a|b$ then c TODO
- TODO

Example 0.51:

$R = \mathbb{Z}[i\sqrt(5)] = \{a + bi\sqrt{5} | a, b \in \mathbb{Z}\}$

$6 = 2 \cdot 3 = (1 + i\sqrt{5})(1 - i\sqrt{5})$

$2|6$ but $2|1 + i\sqrt{5}$ because

$$\begin{aligned}1 + i\sqrt{5} &= 2c \\ &= 2(a + bi\sqrt{5}) \\ &= 2a + 2bi\sqrt{5} \\ 1 = 2a &\Rightarrow a \notin \mathbb{Z}\end{aligned}$$

Similarilly, $2 \not| 1 - i\sqrt{5}$. Therefore, 2 is not prime.

But 2 is irreducible:

$2 = (a + bi\sqrt{5})(c + di\sqrt{5})$

TODO

Example 0.52:

K a field $\Rightarrow K[x]$ is a euclidean ring (with euclidean function $n(\cdot) = deg(\cdot)$)

$\Rightarrow$ primes are irreducible polynomials

That is, $a(x) = b(x) \cdot c(x) \Rightarrow deg(b(x)) = 0$ or $deg(c(x)) = 0$

In $\mathbb{C}[x]$, these are the linear polynomials $ax + b$ with $a \neq 0$.

Definition 0.75: Unique-Factorization Domain

R integral domain. R is a unique fractorization domain (UFD) or factorial ring if $\forall a \in R \backslash \{R^* \cup \{0\}\}$ there exists a unique factorization $a = \varepsilon \cdot p_1 \cdots p_k$ with $\varepsilon \in R^*$, p_i prime

(unique: TODO)

Theorem 0.41:

R euclidean $\Rightarrow R$ UFD

Proof 0.44:

Existence of a factorization:

- Case 1: a irreducible $\Rightarrow a$ prime $\Rightarrow a = 1 \cdot a$
- Case 2:$a = bc$, $bc \in R^* \Rightarrow n(b), n(c) < n(a)$. Suppose a has no factorisation, $n(a)$ minimal. Then $b = \varepsilon \cdot p_1 \cdots p_k$ and $c = \eta \cdot q_1 \cdots q_l$ $\Rightarrow a = bc = \varepsilon \cdot \eta \cdot p_1 \cdots p_k \cdot q_1 \cdots q_1$

Uniqueness:

`TODO`

Definition 0.76: Ideals
$(R, +\cdot)$ integral domain.

$J \subseteq R$ is called an *ideal* of R iff

- $(J, +) \leq (R, +)$ (additive subgroup)
- $\forall a \in R : a \cdot J \subseteq J$

Example 0.53:
$m\mathbb{Z}$ is an ideal of $\mathbb{Z}$.

Definition 0.77:
J ideal of R

$a \equiv b \mod J$ iff $a - b \in J$ ($\Leftrightarrow a + J = b + J$).

Lemma 0.12:
J ideal of R

$$\left.\begin{array}{c} a \equiv b \mod J \\ c \equiv d \mod J \end{array}\right\} \Rightarrow \left\{\begin{array}{c} a + c \equiv b + d \mod J \\ a \cdot c \equiv b \cdot d \mod J \end{array}\right.$$

$R/J = \{a + J | a \in R\}$
$(a + J) + (b + J) := (a + b) + J$
$(a + J) \cdot (b + J) := a \cdot b + J$
$\Rightarrow (R/J, +, \cdot)$ is a ring!

For instance, $\mathbb{Z}_m = \mathbb{Z}/m\mathbb{Z}$

The ideals $J = \{0\}$ and $J = R$ are trivial ideals.

Definition 0.78: Principal Ideals
$m \in R$.

$(m) := mR = \{m \cdot a | a \in R\}$ is an ideal of R. Ideals of this form are called *principal* Ideals.

Remark 0.26:
K field (i.e. $K^* = K \backslash \{0\}$)

$\Rightarrow \{0\}$ and K are the only ideals of K.

Proof 0.45:
TODO

Definition 0.79: Ring Homomorphism

R, S integral domains.

$\varphi : R \to S$ is called a ring homomorphism iff $\forall a, b \in R$:

- $\varphi(a + b) = \varphi(a) + \varphi(b)$
- $\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$

$ker(\varphi) := \{a | a \in R, \varphi(a) = 0\}$

Lemma 0.13:

$\varphi : R \to S$ ring homomorphism.

$\Rightarrow ker(\varphi)$ is an ideal of R

Proof 0.46:

TODO

Lemma 0.14:

$J_i, i \in I$ ideals of R.

$\Rightarrow \bigcap_{i \in I} J_i$ ideal of R

Definition 0.80: Ideal Generated by a Set

$M \subseteq R$ (any subset)

The set that is generated by M is

$$(M) := \bigcap (\text{ideals that contain } M)$$

(If $M = \{m\}$, then $(M) = (m) = mR$.)

R euclidean.
$M = \{m_1, \dots, m_k\}$
$\Rightarrow (M) = (gcd(m_1, \dots, m_k)) = gcd(m_1, \dots, m_k) \cdot R$ principal ideal

Theorem 0.42:

R euclidean ring.

J ideal of $R \Rightarrow \exists m \in R : J = (m) = mR$

That is, all ideals are principal!

Proof 0.47:

TODO

R euclidean, $J = (m) = mR$
$a \equiv b \mod J \Leftrightarrow a \equiv b \mod m \Leftrightarrow m | a - b$

Example 0.54:

$R = \mathbb{Z}$, J ideal of $\mathbb{Z} \Rightarrow J = m\mathbb{Z}$

$R/J = \mathbb{Z}/m\mathbb{Z}$

TODO{I think there is something missing or out of sequence}

TODO{Rewatch recording 4.2 and complete the following section}

Definition 0.81: Field

$(K, +, \cdot)$ is a *field* iff

- $(K, +, \cdot)$ is an integral domain
- and $K^* = K \backslash \{0\}$ (all elements are invertible except 0)

Remark 0.27:

If $p \in \mathbb{P}$, then $\mathbb{Z}_p$ is a field.

Lemma 0.15:

$(K_i)_{i \in I}$ subfields of K,

Then, $\bigcap_{i \in I} K_i$ is also a subfield of K.

Proof 0.48:

TODO

Definition 0.82: Prime Field of a Field

K field.

The *prime field* $P(K)$ of K is the intersection of all subfields of K. (Therefore, it is the smalles subfield of K.)

Definition 0.83: Characteristic of a Field

K field.

The characteristic $char(K)$ of K is given by

$$char(K) := \begin{cases} ord_{(K,+)}(1) & \text{if } ord_{(K,+)}(1) < \infty \\ 0 & \text{otherwise} \end{cases}$$

(That is, the characteristic tells us how often we can add 1 until we arrive at 0.)

Lemma 0.16:
If $ord_{(K,+)}(1) < \infty$, then $ord_{(K,+)}(1) \in \mathbb{P}$

Proof 0.49:
$char(K) = p < \infty$.

This means that $\underbrace{1 + 1 + 1 + \cdots + 1}_{p} = 0$.

Now assume that p is not prime. Then we have that $p = a \cdot b = 0$. But because the integers are an inegral domain, either a or b already have to be 0, so p cannot be the characteristic.

$\Rightarrow p \in \mathbb{P}$

Theorem 0.43:
- If $char(K) = p < \infty$, then
  - $p \in \mathbb{P}$
  - $P(K) \cong \mathbb{Z}_p$
- If $char(K) = 0$ (i.e. $ord_{(K,+)}(1) = \infty$), then
  - $P(K) \cong \mathbb{Q}$

Theorem 0.44:
K finite field.

$\exists p \in \mathbb{P}, n \in \mathbb{N}_{<0} : |K| = p^n$.

(The size of a finite field has to be a prime power.)

Proof 0.50:
TODO

Theorem 0.45:
- $\forall p \in \mathbb{P}, n \in \mathbb{N}_{>0} \exists \text{field } K : |K| = p^n$
- K_1, K_2 finite fields. $|K_1| = |K_2| \Rightarrow K_1 \cong K_2$

That is, up to isomorphism, there is only one unique field of finite size p^n. It is called *the* Galois-field $GF(p^n)$.

Remark 0.28:
- $\mathbb{R}[x]/(x^2-1)$ is not an integral domain because $(x-1)(x+1) = x^2-1 = 0$ (zero dividers).
- $p(x) \equiv 0 \Rightarrow x^n \equiv -a_{n-1}x^{n-1} \cdots - a_0 \Rightarrow$ any polynomial in $K[x]/(p(x))$ has a representative of degree strictly less than n.

Theorem 0.46:
K a field, $p(x) \in K[x]$, then $K[x]/p(x)$ is a field iff $p(x)$ irreducible.

Remark 0.29:

- $p(x)$ irreducible $\Rightarrow$ p(x) has no zeros, because otherwise $x - a | p(x)$
- K is a subfield of $K[x]/p(x)$

Algebraic Extensions

Let $p(x)$ be monic (leading coefficient 1) and irreducible of field K.

Define a new element $a \in L$ by $p(a) = 0$.

Theorem 0.47:
Let $L \supseteq K$ such that a is a zero of $p(x) \in K[x]$, then exists a unique monic, irreducible polynomial $m \in K[x]$ with $m(a) = 0$, which is the *minimal* polynomial.

Example 0.55:
$\mathbb{C}$ is defined as the field containing $\mathbb{R}$ and the roots of $x^2 + 1$.

Proof 0.51:
$p_1(x), p_2(x)$ monic irreducible p_1(a)=p_2(a)=0

$d(x) := gcd(p_1, p_2) = A(x)p_1(x) + B(x)p_2(x)$

$\Rightarrow d(a) = A(a)p_1(a) + B(a)p_2(a) = 0 \Rightarrow p_1(x) = p_2(x)$

Remark 0.30:
$m(x)$ has minimal degree among all polynomials with $p(a) = 0$.

```
$p\in K[x], p(a) = 0 \Rightarrow m(x)|p(x)$
```

Remark 0.31:
$m(x)$ has minimal degree among all polynomials with $p(a) = 0$.

Proof 0.52:
$p(x) = q(x)m(x) + r(x)$ with $deg(r) < deg(m)$ or $r = 0$

$\Rightarrow 0 = p(a) = q(a)m(a) + r(a) = r(a)$

Since m is minimal, we have $r(x) = 0$ and therefore $m(x)|p(x)$.

Let $L := \{\sum_{i=0}^{n-1} b_i a^i | b_i \in K\}$ is the smallest field containing K and a, because $a^n = -\sum_{k=0}^{n-1} c_k a^k$, with $deg(m) = n$ and $m(x) = \sum_{k=0}^{n} c_k x^k$.

$L \cong K[x]/m(x)$

Example 0.56:

$K = \mathbb{R}$, $m(x) = x^2 + 1$, $a = i$ with $i^2 = -1$.

$K[x]/m(x) = \mathbb{R} \cup \{ax + b | a \neq 0\}$, eg. $x^3 = x \cdot x^2 = -x$.

$L = \{a \cdot i + b | a, b \in \mathbb{R}\}$

Definition 0.84: Algebraic Elements

$a \in L$ is called *algebraic* over K iff

$$\exists p(x) \in K[x] \backslash \{0\} : p(a) = 0$$

Example 0.57:

- $\mathbb{Q}[x]/(x^2 - 2) \cong \mathbb{Q}[\sqrt{2}] = \{a + b \cdot \sqrt{2} | a, b \in \mathbb{Q}\}$
- $a, b \in K$, $K[x]/(ax + b) \cong K$

Definition 0.85: Algebraic Closure

A field with no algebraic extensions (i.e. any polynomial is a product of linear factors) is *algebraically closed.*

Remark 0.32:

- For any field K, there is an algebraically closed field $L \supseteq K$.
- If $|K| = p \in \mathbb{P}$ (i.e., $K \cong \mathbb{Z}_p$), then, $\forall n \in \mathbb{N} \exists m(x)$ such that $|K[x]/m(x)| = p^n$.

Finite Fields

Theorem 0.48:

Field K finite. $(K^*, \cdot)$ is a cyclic group of order $p^n - 1 = |K^*|$.

$\forall a \in K : a^{p^n} = a$

Proof 0.53:

$|K^*| = p^n - 1$, let $a \in K^*$ with $ord_{(K^*,\cdot)}(a) =: r$ is maximal.

$\Rightarrow r | p^n - 1$ and $\forall y \in K^* : ord_{(K^*,\cdot)}(y) | r$

$\Rightarrow \forall y \in K^* : y^r - 1 = 0$ but the number of zeros of $x^r - 1 \leq r$

$\Rightarrow p^n - 1 \leq r \rightarrow p^n - 1 = r$

Since the maximal order of an element equals the order of the group, the group is cyclic.

Definition 0.86: Primitive Element and Primitive Polynomial

K finite field.

- $a \in K$ is called *primitive element* if it generates $(K \backslash \{0\}, \cdot)$.
- The minimal polynomial of a primitive element is called *primitive polynomial.*

Definition 0.87: Generator

A generator of $(K^*, \cdot)$ is a primitive element. Its minimal polynomial (in $\mathbb{Z}_p[x]$ is the primitive polynomial).

Theorem 0.49:

$q(x)$ is a primitive polynomial of $k = GF(p^n)$ (Galois-field of size p^n)

$\Leftrightarrow q(x)|x^{p^n-1} - 1$ and $q(x) \not| x^k - 1$ for $1 \leq k < p^n - 1$ and q is irreducible (in $\mathbb{Z}_p[x]$).

Proof 0.54:

TODO

Theorem 0.50:

$q(x)$ has the following form:

$q(x) = (x - a)(x - a^p)(x - a^{p^2}) \cdots (x - a^{p^{n-1}})$, that is it has n zeros

Lemma 0.17:

$\phi : GF(p^n) \to GF(p^n)$ (field-automorphism)
$x \mapsto x^p$ (i.e. a homomorphism and bijective)

Proof 0.55:

homomorphism:

- $(a + b)^p = a^p + b^p$ (no joke, see exercise)
- $(ab)^p = a^p \cdot b^p$

bijektive:

- $ker(\phi)$ is an ideal of $GF(p^n)$ but fields only have two (trivial) ideals: the field itself and zero.
- but $ker(\phi) \neq GF(p^n)$ because $\phi(1) = 1$

Fact: All automophisms are powers of ϕ: $\{\phi, \phi^2, \dots, \phi^n = id_K\}$
$\Rightarrow$ TODO

Let $q(x)$ be a primitive polynomial:
$GF(p^n) = \mathbb{Z}_p[x]/q(x)$
$b = \phi(a)$ for an automorphism ϕ
$\Rightarrow q(b) = q(\phi(a)) = \phi(q(a)) = \phi(0) = 0$

Since $\phi(x) = x, \phi(x) = x^p, \ldots, \phi(x) = x^{p^2}$ are all automorphisms, we have that $\phi_0(a), \phi_1(a), \ldots$ are zeros of $q(x)$ and these are actually *all* zeros of $q(x)$

Corollary 0.7:

The number of primitive polynomials is $\frac{1}{n}\phi(p^n - 1)$, because any two primitive polynomials have no common root.

Linear Codes

Definition 0.88: Linear Codes, Generator Matrix, Codewords

$K = GF(q)$, $f : K^k \to K^n$ linear (i.e. homomorphic) and injective

$C = f(K^k)$ is an (n, k)-linear code

Let $\{c_1, \ldots, c_k\}$ be a basis of C, then

$$G = \begin{pmatrix} c_1 \\ c_2 \\ \vdots \\ c_k \end{pmatrix} \in M_{k \times n}$$

(with the c_i's as row vectors) is the generator matrix.

Codewords are elements of C, i.e. linear combinations of $\{c_1, \ldots, c_k\}$.

Definition 0.89: Check Matrix

A generator matrix of $C^\perp := \{v \in K^n | v \cdot u = 0 \forall u \in C\}$ (orthogonal space to C) is called *check matrix.*

Proposition: Let H be a check matrix, then $G \cdot H^\top = \mathbf{0}_{k \times (n-k)}$

Remark 0.33:

A code C is called systematic if $G = (I_k || F)$, i.e. if $v = (v_1, \ldots, v_k)$ is the message then the encoding is $vG = (v_1, \ldots, v_k, w_k + 1, \ldots, w_n)$. That is, the code just appends stuff.

If C is systematic, then $H = (-F^\top || I_{n-k})$

Definition 0.90: Syndromes

$s_H(c) = c \cdot H^\top$ is called the syndrome of c (with $c \in K^n$).

The syndrom is 0 iff c is a correct codeword (no error detected).

Proposition: C an (n,k)-linear code, then u,v are in the same coset of $a+C \Leftrightarrow s_H(u) = s_H(v)$

Polynomial Codes

Polynomial Codes are linear codes, but we take a different vector space

$K_{n-1}[x] = \{p(x) \in K[x] | deg(p(x) \leq n-1)\}$
$(dim(K_{n-1}[x]) = n)$

$g(x) \in K[x]$, $deg(g) = n-k$ (generator polynomial)

Encoding: $f(p(x)) = p(x) \cdot g(x)$ for $p(x) \in K_{k-1}[x]$
(f injective and linear)

$C = f(K_{k-1}[x])$ is a k-dimensional subspace of $K_{n-1}[x]$

To check a an encoded message, choose $f(x) \in K[x]$ with $deg(f) = n$ and $h(x)$ such that $c(x) \in C \Leftrightarrow c(x) \cdot h(x) = 0 \mod f(x)$.

Proposition: $f(x) = \lambda g(x) h(x)$, $\lambda \in K^*$

Definition 0.91:
$s(v(x)) := v(x) \mod g(x)$ is the syndrome of $v(x)$

Proposition: $v(x)$ is a code iff $s(v(x)) = 0$

Definition 0.92:
A code is cyclic if for any $c_0 + c_1 \cdot x + \cdots + c_{n-1} \cdot x^{n-1} \in C$ also the cyclic shift is in C. TODO

Theorem 0.51:
C is cyclic iff $g(x) | x^n - 1$.

Linear (Feedback) Shift Registers (LFSRs)

start with sequence $R_0, \ldots, R_{k_1}$

TODO{Create Graphic of LFSR (tikz)}

e.g. $R_n \in GF(2)$

$R_k = a_0 R_0 + a_1 R_1 + \cdots + a_{k-1} R_{k-1}$

Remark: We assume $a_0 \neq 0$. Otherwise, the LFSR behaves like a different LFSR with the leading zero-multipliers cut off.

new sequence is $R_1, \ldots, R_k$

Example 0.58:
TODO

$101 \to 010 \to 100 \to 001 \to 011 \to 111 \to 110 \to 101$

Observations:

- If $K = GF(2)$, there are 2^n states. Therefore, the sequence of states is periodic $\rightarrow$ this forms a cycle.
- The zero-state will always be a fixed point

The maximally possible period is $2^k - 1$ (for $GF(2)$). But when is the period actually maximal?

The register sequence is the sequence $(R_n)_{n \geq 0}$ and it satisfies the linear recurrence

$$R_n + k = \sum_{i=0}^{k-1} a_i R_{n+1}$$

The generating function $R(x) := \sum_{n \geq 0} R_n x^n = \frac{g(x)}{f(x)}$ for two polynomials $g, f \in GF(2)[x]$. We know that $f(x) = 1 - a_{k-1}x - a_{k-2}x^2 - \ldots - a_0 x^k$ and $deg(g) < k$

Example 0.59:

$(a_0, a_1, a_2, a_3) = (1, 1, 0, 1)$

$\Rightarrow f(x) = 1 + x + x^3 + x4$ (addition and subtraction is the same in $GF(2)$)

TODO{finish example (tabular)}

Theorem 0.52:
Let $(R_n)_{n \geq 0}$ be a register sequence with denominator polynomial $f(x)$ *irreducible*. Then, the period equals $t \Leftrightarrow f(x) | 1 - x^t$

Proof 0.56:

- $R_{n+t} = R_n \forall n \geq 0$
  $R(x) = \underbrace{(R_0 + \ldots + R_{t-1}x^{t-1})}_{\sigma(x)} \cdot \underbrace{(1 + x^t + x^{2t} + \cdots)}_{\frac{1}{1-x^t}}$
  $R(x) = \frac{\sigma(x)}{1-x^t}$
  TODO
- TODO

Remark 0.34:
In the example above, the polynomial is not irreducible. Therefore, the theorem does not apply. This is also why the period depends on the initial state (which does not reflect) in the theorem.

Recall the following theorem we had before:

Theorem 0.53:
$q(x)$ is primitive polynomial iff $q(x) | x^{p^n - 1}$ and $q(x) \not| x^k - 1$ for $k < p^n - 1$

Therefore:

Theorem 0.54:
R_n has period $2^n - 1$ iff $R(x) = \frac{g(x)}{f(x)}$ with $f(x)$ a primitive polynomial.

Repetition on Counting Structures with Generating Functions (Combinatorial Species)

Definition 0.93:
A combinatorial species F is an assignment

- of finite sets (of labels) U to finite sets (of strutures) $F[U]$
- of bijections $\sigma : U \to V$ between sets of labels to bijections $F[\sigma] : F[U] \to F[V]$

such that

- $F[\sigma \circ \tau] = F[\sigma] \circ F[\tau]$
- and $F[id_U] = id_{F[U]}$

Example 0.60:
Linear Orders $\mathcal{L}[\{1, a, \heartsuit\}] = \{1a\heartsuit, 1\heartsuit a, a1\heartsuit, a\heartsuit 1, \heartsuit 1a, \heartsuit a1\}$

Relabelling: $\mathcal{L}\begin{bmatrix} 1, a, \heartsuit \\ 1, 2, 3 \end{bmatrix}(\heartsuit a1) = 321 \in \mathcal{L}[\{1, 2, 3\}]$

Permutations $S[\{1, a, \heartsuit\}] = TODO$

- $S\begin{bmatrix} 1, 2, 3 \\ 2, 3, 1 \end{bmatrix}(TODO) = TODO$
- $S\begin{bmatrix} 1, 2, 3 \\ 2, 3, 1 \end{bmatrix}(TODO) = TODO$

TODO

Definition 0.94: Atom or Singleton or X

$$X[U] : \begin{cases} \{U\} & \ldots |U| = 1 \\ \emptyset & \ldots \text{otherwise} \end{cases}$$

$X[id_U] = id_{x[U]}$

Definition 0.95: Empty Set or One or 1
1[U] = TODO

Definition 0.96: Set Species ()

TODO

Definition 0.97:

two structures $f_1 \in F[U]$ and $f_2 \in F[V]$ are isomorphic iff there is a relabelling $\sigma : U \to V$ such that $F[\sigma](f_1) = f_2$

Notation: $F[n] := F[\{1, \ldots, n\}]$, $\tilde{F}[n]$ is the set of isomorphism classes in $F[n]$

($f_1 \in F[U_1], f_2 \in F[U_2]$ are isomorphic if $\exists \sigma : U_1 \to U_2 : F[\sigma](f_1) = f(2)$.)

Example 0.61:

$S[\{1, a, \heartsuit\}] = TODO$

$\tilde{S}[3] = TODO$

Remark: $|\tilde{S}[n]|$ = number of integer partitions

$\tilde{\mathcal{L}} = \{TODO\}$

Definition 0.98:

The exponential generating function of a species F is $F(x) = \sum_{n \geq 0} |F[n]| \cdot \frac{x^n}{n!}$

The ordinary generating function of a species F is $\tilde{F}(x) = \sum_{n \geq 0} |\tilde{F}[n]| \cdot x^n$

Operations on Species

F, G combinatorial species

Addition:

$(F + G)[U] := F[U] \cup G[U]$

$(F + G)[\sigma : U \to V](s) := \begin{matrix} F[\sigma](s) & s \in F[U] \\ G[\sigma](s) & s \in G[U] \end{matrix}$

Example 0.62:

$F = G = X$

$(F + G)[\{\heartsuit\}] = \{(left, \heartsuit), (right, \heartsuit)\}$

Multiplication:

$(F \cdot G)[U] := \bigcup_{V, W, V \cup W = U} F[V] \times G[W]$

$(F \cdot G)[\sigma : U \to U'](f_v, g_w) := (F[\sigma|_V](f_V), G[\sigma|_W](g_W))$ where σ is restricted to V or W respectively.

Example 0.63:

$\mathcal{L}$ ... linear orders
$\mathcal{L} = 1 + X \cdot \mathcal{L}$ (say out loud: "A linear oder is either the empty order or a first element concatenated with a linear order.")

$\mathcal{L}[\{a,b\}] = 1[\{a,b\}] \cup (X \cdot \mathcal{L})[\{a,b\}]$
$1[\{a,b\}] = \emptyset$
$(X \cdot \mathcal{L})[\{a,b\}] = X[\emptyset] \times \mathcal{L}[\{a,b\}] \cup X[\{a\}] \times \mathcal{L}[\{b\}] \cup X[\{b\}] \times \mathcal{L}[\{a\}] \cup X[\{a,b\}] \times \mathcal{L}[\emptyset]$
$= \emptyset \cup \{(a,b)\} \cup (\{b,a\}) \cup \emptyset$
$= \{(a,b),(b,a)\}$

Example 0.64:

binary (rooted ordered) trees

TODO

$\mathcal{B} = 1 + X \cdot \mathcal{B} \cdot \mathcal{B}$

e.g. $\mathcal{B}[\{a\}] = 1[\{a\}] \cup (X \cdot \mathcal{B} \cdot \mathcal{B})[\{a\}] \cup \ldots$
$= \emptyset \cup (a, \emptyset, \emptyset)$

Theorem 0.55:

F, G comb. species

$(F+G)(x) = F(x) + G(x)$
$(F \cdot G)(x) = F(x) \cdot G(x)$

$(\widetilde{F+G})(x) = \tilde{F}(x) + \tilde{G}(x)$
$(\widetilde{F \cdot G})(x) = \tilde{F}(x) \cdot \tilde{G}(x)$

(This theorem is the reason why combinatorial species work. In the original article the author said that species are a liftig of generating functions.)

Example 0.65:

$\mathcal{B} = 1 + X \cdot \mathcal{B} \cdot \mathcal{B} \Rightarrow \mathcal{B}(x) = 1 + X \cdot \mathcal{B}^2(x)$ and $\tilde{\mathcal{B}}(x) = 1 + \tilde{\mathcal{B}}^2(x)$

$\mathcal{L} = 1 + X \cdot \mathcal{L} \Rightarrow \mathcal{L}(x) = \tilde{\mathcal{L}}(x) = \frac{1}{1-x}$

Substitution:
$G[\emptyset] = \emptyset$

$$(F \circ G)[U] := \bigcup_{P=\{B_1,\ldots,B_k\}, partition} F[P] \times \prod_{i=1}^{k} G[B_i]$$

Theorem 0.56:

$(F \circ G)(x) = F(G(x))$

WARNING: $(\widetilde{F \circ G})(x) \neq \tilde{F}(\tilde{G}(x))$!

Example 0.66:

rooted (but unordered) trees:

TODO{illustration}

$\mathcal{A} = X \cdot (\mathcal{E} \circ \mathcal{A})$
$\mathcal{A}(x) = x \cdot exp(\mathcal{A}(x))$

$A[\{1,2,3\}] = X[\{1\}] \times (\mathcal{E} \circ \mathcal{A})[\{2,3\}] \cup TODO$

Example 0.67:

ordered rooted trees (order of successors matters):

TODO{illustration}

$\mathcal{A}_{\mathcal{L}} = X \cdot (\mathcal{L} \circ \mathcal{A}_{\mathcal{L}})$
$\mathcal{A}_{\mathcal{L}}(x) = x \cdot \frac{1}{1-\mathcal{A}_{\mathcal{L}}(x)}$

Example 0.68:

plane rooted trees:

TODO{illustration}

$F = X + X \cdot (\mathcal{C} \circ \mathcal{A}_{\mathcal{L}})$ with $\mathcal{C}$ being the cycle structure

Example 0.69:

Permutation:

$S = \mathcal{E} \circ \mathcal{C}$
$\Rightarrow TODO$

A permutation is just a set of cycles (of labels).

Example 0.70:

Involutions:

$I = \mathcal{E} \circ (X + \mathcal{E}_2)$
$I(x) = exp(x + \frac{x^2}{2})$