

AuW Recap

Axel Montini
amontini@student.ethz.ch

July 28, 2021

Cannot be used during the exam, but it's a nice short recap of everything done in the second semester.

1 Last semester

Go read again about MST algorithms and so on.

2 Graphentheorie

2.1 Zusammenhang

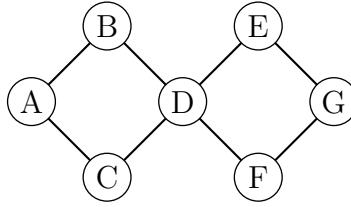
Definition 1. A graph $G = (V, E)$ is *k-zusammenhängend* if $|V| \geq k + 1$ and for all $X \subseteq V$, $|X| < k$ the following is true:

The graph $G[V \setminus X]$ is zusammengehängend

Definition 2. A graph $G = (V, E)$ is *k-kanten-zusammenhängend* if for all $X \subseteq E$, $|X| < k$ the following is true:

The graph $G(V, E \setminus X)$ is zusammengehängend

Note 1. A graph can be both 2-kanten-zusammengehängend and be only 1-zusammengehängend at the same time. Example:



Definition 3. In a zusammengehängend Graph, *Artikulationsknoten* disconnect the graph when removed. Only 1-zusammengehängend graphs can have Artikulationsknoten

Theorem 1. In zusammenhängende Graphs it's possible to find Artikulationsknoten in $\mathcal{O}(|E|)$ if an adjacency list is used.

Definition 4. A zusammenhängend Graph may contain *Brücke*. In this case, it's **not 2-kanten-zusammenhängend**.

An edge is a bridge if it disconnects the graph when removed.

Theorem 2. *Brücke* can also be computed in $\mathcal{O}(|E|)$ using an adjacency list.

Definition 5. $G = (V, E)$ is zusammenhängend. For $e, f \in E$ we define the relation

$$e \sim f \Leftrightarrow e = f \text{ or there is a Kreis containing both edges}$$

This is an equivalence relation. Each equivalence class is called a Block (plural Blöcke).

2.2 Kreise

Definition 6. An *Eulertour* in a graph G is a closed path (*Zyklus*) that contains every edge $\in E$ exactly once.

A graph containing an Eulertour is called *eulersch*.

Definition 7.

Theorem 3.

$$A \text{ graph is eulersch} \Leftrightarrow \deg(v) \text{ is even for all vertices}$$

Theorem 4. In a connected and eulersch Graph it's possible to find an Eulertour in $\mathcal{O}(|E|)$.

Definition 8. A *Hamintonkreis* in G is a cycle that goes through every vertex exactly once. A graph containing an Hamintonkreis is called *hamintonsch*.

Theorem 5. The algorithm seen in class can find an Hamintonkreis in time $\mathcal{O}(n^2 \cdot 2^n)$ and memory $\mathcal{O}(n \cdot 2^n)$, where $n = |V|$.

Theorem 6. A bipartite graph $G = (A \uplus B, E)$ cannot contain an Hamintonkreis.

Theorem 7 (Dirac). A graph G with $V \geq 3$ in which every vertex has at least $|V|/2$ neighbors is hamintonsch.

Definition 9. In a complete graph K_n (all vertices are connected together), the metric Traveling Salesman Problem consists in finding an Hamintonkreis C with minimal cost (distance).

Definition 10. An α -Approximationsalgorithmus of this problem finds an H.kreis C so that

$$\sum_{e \in C} l(e) \leq \alpha \cdot \text{opt}(K_n, l)$$

Meaning that it finds a solution worse by the optimal solution by a factor α .

Theorem 8. If there's an α -Approximationsalgorithmus with $\alpha > 1$ for the TSP with running time $\mathcal{O}(f(n))$ then there's also an algorithm that decides whether a graph with n vertices is hamintonsch in $\mathcal{O}(f(n))$.

Theorem 9. For the metric TSP there's a 2-Approximationsalgorithmus with running time $\mathcal{O}(n^2)$. It find the MST in $\mathcal{O}(n^2)$ and then uses it to find the H.k.

2.3 Matching

Definition 11. A set of edges $M \subseteq E$ is called *Matching* in a graph G if

$$\forall e, f \in M \ (e \cap f = \emptyset)$$

- A vertex v is said to be *überdeckt* by a matching M if the matching contains an edge containing v .
- A matching M is called *perfektes Matching* if every vertex is überdeckt (equivalent: $|M| = |V|/2$).

Definition 12. A matching M is said to be:

- *inklusionsmaximal* if $M \cup \{e\}$ is not a matching for all $e \in E \setminus M$.
- *kardinalitätsmaximal* if $|M| \geq |M'|$ for all matchings M' in G .

Note that *kardinalitätsmaximal* \Rightarrow *inklusionsmaximal* (the opposite might not be true).

Algorithm 1: Greedy-Matching

Result: The inklusionsmaximales matching M

while $E \neq \emptyset$ **do**

choose an edge $e \in E$;
 $M \leftarrow M \cup \{e\}$;
 remove e and all incident edges from G ;

Theorem 10. The greedy-matching algorithm finds an inklusionsmaximal Matching in time $\mathcal{O}(|E|)$ for which the following holds: $|M_{\text{Greedy}}| \geq \frac{1}{2}|M_{\text{max}}|$, where M_{max} is a kardinalitätsmaximales Matching.

Theorem 11 (Berge). Let M be a matching in G that is not k -maximal, then there is an augmenting path to M .

Theorem 12. Is n even K_n a complete graph, then it's possible to find a minimal perfekte Matching in time $\mathcal{O}(n^3)$

Theorem 13. There's a 3/2-Approximationsalgorithmus for the TSP that runs in $\mathcal{O}(n^3)$.

Definition 13. Nachbarschaft einer Knotenmenge $X \subseteq V$:

$$N(X) := \bigcup_{v \in X} N(v)$$

Theorem 14 (Hall, Heiratssatz). For a bipartite graph $G = (A \uplus B, E)$ there's a matching M with $|M| = |A|$ if and only if $|N(X)| \geq |X|$ for all $X \subseteq A$.

Definition 14. A bipartite graph is called k -regulär if every vertex has degree k .

Theorem 15. Let G be a k -regular bipartite graph. Then there's M_1, \dots, M_k so that $E = M_1 \uplus M_2 \uplus \dots \uplus M_k$ and all $M_i, 1 \leq i \leq k$ are perfect matchings.

Theorem 16. Is $G = (V, E)$ a 2^k -regular bipartite Graph, then it's possible to find a perfect matching in $\mathcal{O}(|E|)$.

Algos
at
page
65 and
67

2.4 Färbungen

Definition 15. A *(Knoten)-Färbung* (vertex coloring) of a graph G with k colors is $c : V \rightarrow [k]$, so that

$$c(u) \neq c(v) \quad \forall \{u, v\} \in E$$

The *chromatische Zahl* (chromatic number) $X(G)$ of a graph is the minimal amount of colors that can be used to color G .

Theorem 17. A graph is bipartite if and only if doesn't contain any *Kreis* of odd length.

Theorem 18 (Vierfarbensatz). Every map can be colored with 4 colors.

Algorithm 2: Greedy-Färbung

Data: G

Result: array c mapping each vertex to a color

$c(v_1) \leftarrow 1;$

for $i = 2, \dots, n$ **do**

$c(v_i) \leftarrow \min \{k \in \mathbb{N} \mid k \neq c(u) \text{ for all } u \in N(v_i) \cap \{v_1, \dots, v_{i-1}\}\}$

Theorem 19. Let G be a connected graph and $C(G)$ the amount of colors used by the Greedy-Färbung algorithm. Then

$$\mathcal{X}(G) \leq C(G) \leq \Delta(G) + 1$$

Where $\Delta(G) := \max_{v \in V} \deg(v)$ is the max degree in the graph.

The running time is $\mathcal{O}(|E|)$ if an adjacency list is used.

Theorem 20 (Brooks). Let G be a connected graph that is neither complete nor an odd *Kreis* ($G \neq K_n$ and $G \neq C_{2n+1}$). Then

$$\mathcal{X}(G) \leq \Delta(G)$$

And there's an algorithm that can color the vertices of G in time $\mathcal{O}(|E|)$ and with $\Delta(G)$ colors.

Theorem 21 (Mycielski-Konstruktion). For all $k \geq 2$ there's a triangle-free graph G_k with $\mathcal{X}(G) \geq k$.

Theorem 22. Every 3-färbbaren graph can be colored in time $\mathcal{O}(|E|)$ with $\mathcal{O}(\sqrt{|V|})$ colors.

3 Randomized algorithms

3.1 Grundbegriffe und Notationen

Definition 16. A *diskreter Wahrscheinlichkeitsraum* is defined through a *Ergebnismenge* $\Omega = \{\omega_1, \omega_2, \dots\}$ of *Elementarereignissen*.

A probability $\Pr[\omega_i]$ corresponds to each ω_i .

$$0 \leq \Pr[\omega_i] \leq 1, \quad \sum_{\omega \in \Omega} \Pr[\omega] = 1$$

A set $E \subseteq \Omega$ is called *Ereignis*. The probability is defined as

$$\Pr[E] := \sum_{\omega \in E} \Pr[\omega]$$

The *Komplementärereignis* zu E is defined as $\bar{E} := \Omega \setminus E$

Lemma 1. For *Ereignisse* A, B :

1. $\Pr[\emptyset] = 0, \Pr[\Omega] = 1$
2. $0 \leq \Pr[A] \leq 1$
3. $\Pr[\bar{A}] = 1 - \Pr[A]$
4. If $A \subseteq B$ then $\Pr[A] \leq \Pr[B]$

Theorem 23 (Additionssatz). When the *Ereignisse* are pairwise disjoint then

$$\Pr \left[\bigcup_{i=1}^n A_i \right] = \sum_{i=1}^n \Pr[A_i]$$

For infinite sets of disjoint *Ereignissen* A_1, A_2, \dots then

$$\Pr \left[\bigcup_{i=1}^{\infty} A_i \right] = \sum_{i=1}^{\infty} \Pr[A_i]$$

Theorem 24 (Siebformel, Prinzip der Inklusion/Exklusion). For *Ereignisse* A_1, \dots, A_n ($n \geq 2$):

$$\Pr \left[\bigcup_{i=1}^n A_i \right] = \sum_{l=1}^n (-1)^{l+1} \sum_{1 \leq i_1 < \dots < i_l \leq n} \Pr[A_{i_1} \cap \dots \cap A_{i_l}]$$

Lemma 2 (A special case of the Siebformel). *Let $\Omega = A_1 \cup \dots \cup A_n$ with $\Pr[\omega] = 1/|\Omega|$, where A_i are finite sets. Then*

$$\left| \bigcup_{i=1}^n A_i \right| = \sum_{l=1}^n (-1)^{l+1} \sum_{1 \leq i_1 < \dots < i_l \leq n} |A_{i_1} \cap \dots \cap A_{i_l}|$$

Corollary 1 (Boolsche Ungleichung, Union Bound). *For some Ereignisse A_1, \dots, A_n :*

$$\Pr \left[\bigcup_{i=1}^n A_i \right] \leq \sum_{i=1}^n \Pr[A_i]$$

For an infinite set of Ereignisse, replace n with ∞ .

3.2 Bedingte Wahrscheinlichkeiten

Definition 17. Let A and B be Ereignisse with $\Pr[B] > 0$. The *bedingte Wahrscheinlichkeit* $\Pr[A|B]$ of A given B is defined through

$$\Pr[A|B] := \frac{\Pr[A \cap B]}{\Pr[B]}$$

Theorem 25 (Multiplikationssatz). *The Ereignisse A_1, \dots, A_n are given. If $\Pr[A_1 \cap \dots \cap A_n] > 0$, then:*

$$\Pr[A_1 \cap \dots \cap A_n] = \Pr[A_1] \cdot \Pr[A_2|A_1] \cdot \Pr[A_3|A_1 \cap A_2] \cdot \dots \cdot \Pr[A_n|A_1 \cap \dots \cap A_{n-1}]$$

Theorem 26 (Satz von der totalen Wahrscheinlichkeit). *A_1, \dots, A_n are pairwise disjoint and $B \subseteq A_1 \cup \dots \cup A_n$. Then*

$$\Pr[B] = \sum_{i=1}^n \Pr[B|A_i] \cdot \Pr[A_i]$$

Analogous for an infinite set of A_i s.

Theorem 27 (Satz von Bayes). *A_1, \dots, A_n pairwise disjoint. Let $B \subseteq A_1 \cup \dots \cup A_n$ with $\Pr[B] > 0$. Then for any $i = 1, \dots, n$:*

$$\Pr[A_i|B] = \frac{\Pr[A_i \cap B]}{\Pr[B]} = \frac{\Pr[B|A_i] \cdot \Pr[A_i]}{\sum_{j=1}^n \Pr[B|A_j] \cdot \Pr[A_j]}$$

Analogous for ∞ instead of n .

3.3 Unabhängigkeit

Definition 18. Die Ereignisse A, B are *unabhängig* when

$$\Pr[A \cap B] = \Pr[A] \cdot \Pr[B]$$

Definition 19. Die Ereignisse A_1, \dots, A_n are unabhängig when for all $I \subseteq \{1, \dots, n\}$ with $I = i_1, \dots, i_k$:

$$\Pr[A_{i_1} \cap \dots \cap A_{i_k}] = \Pr[A_{i_1}] \cdot \dots \cdot \Pr[A_{i_k}]$$

Lemma 3. Die Ereignisse A_1, \dots, A_n are unabhängig *if and only if*

$$\forall (s_1, \dots, s_n) \in \{0, 1\}^n \quad (\Pr[A_1^{s_1} \cap \dots \cap A_n^{s_n}] = \Pr[A_1^{s_1}] \cdot \Pr[A_n^{s_n}])$$

where $A_i^0 = \overline{A_i}$ and $A_i^1 = A_i$

Lemma 4. A, B, C unabhängige Ereignisse. Then $A \cap B$ and C and $A \cup B$ and C are also independent.

3.4 Zufallsvariablen

Definition 20. A *Zufallsvariable* is $X : \Omega \rightarrow \mathbb{R}$, where Ω is the Ergebnismenge of a Wahrscheinlichkeitsraum.

The *Wertebereich* of a Zufallsvariable is

$$W_X := X(\Omega) = \{x \in \mathbb{R} \mid \exists \omega \in \Omega \text{ with } X(\omega) = x\}$$

Definition 21. The *Erwartungswert* of X is $\mathbb{E}[X]$, defined as

$$\mathbb{E}[X] := \sum_{x \in W_x} x \cdot \Pr[X = x]$$

when the sum absolut konvergiert. Otherwise the Erwartungswert is *undefiniert / undefined*.

Lemma 5. Is X a Zufallsvariable, then:

$$\mathbb{E}[X] = \sum_{\omega \in \Omega} X(\omega) \cdot \Pr[\omega]$$

Theorem 28. X Zufallsvariable mit $W_X \subseteq \mathbb{N}_0$. Then

$$\mathbb{E}[X] = \sum_{i=1}^{\infty} \Pr[X \geq i]$$

Theorem 29. X a Zufallsvariable. For pairwise disjoint Ereignisse A_1, \dots, A_n with $A_1 \cup \dots \cup A_n = \Omega$ and $\Pr[A_1], \dots, \Pr[A_n] > 0$ then

$$\mathbb{E}[X] = \sum_{i=1}^n \mathbb{E}[X|A_i] \cdot \Pr[A_i]$$

Analogous for ∞ instead of n .

Theorem 30 (Linearität des Erwartungswert). For X_1, \dots, X_n and $X := a_1X_1 + \dots + a_nX_n + b$ with $a_1, \dots, a_n, b \in \mathbb{R}$:

$$\mathbb{E}[X] = a_1\mathbb{E}[X_1] + \dots + a_n\mathbb{E}[X_n] + b$$

Note 2. For an Ereignis $A \subseteq \Omega$ the Indikatorvariable X_A is defined as

$$X_A(\omega) := \begin{cases} 1, & \text{if } \omega \in A \\ 0, & \text{otherwise} \end{cases}$$

Also $\mathbb{E}[X_A] = \Pr[A]$

Definition 22. For a Zufallsvariable X mit $\mu = \mathbb{E}[X]$ the Varianz $\text{Var}[X]$ is defined through

$$\text{Var}[X] := \mathbb{E}[(X - \mu)^2] = \sum_{x \in W_X} (x - \mu)^2 \Pr[X = x]$$

The Standardabweichung of X is $\sigma := \sqrt{\text{Var}[X]}$.

Theorem 31. For any Zufallsvariable X and $a, b \in \mathbb{R}$:

$$\text{Var}[X] = \mathbb{E}[X^2] - \mathbb{E}[X]^2$$

$$\text{Var}[a \cdot X + b] = a^2 \cdot \text{Var}[X]$$

Definition 23. For a Zufallsvariable X , $\mathbb{E}[X^k]$ is called k -te Moment and $\mathbb{E}[(X - \mathbb{E}[X])^k]$ is called k -te zentrale Moment.

3.5 Wichtige diskrete Verteilungen

Bernoulli, Binomial, Geometrische, Poisson

Maybe
write,
or use
the
Formel-
samm-
lung

3.6 Mehrere Zufallsvariablen

Definition 24. Zufallsvariablen X_1, \dots, X_n are *unabhängig* if and only if for all $(x_1, \dots, x_n) \in W_{X_1} \times \dots \times W_{X_n}$ the following holds:

$$\Pr[X_1 = x_1, \dots, X_n = x_n] = \Pr[X_1 = x_1] \cdot \dots \cdot \Pr[X_n = x_n]$$

Theorem 32 (Linearität des Erwartungswerts). For X_1, \dots, X_n and $X := a_1 X_1 + \dots + a_n X_n$ with $a_i \in \mathbb{R}$:

$$\mathbb{E}[X] = a_1 \mathbb{E}[X_1] + \dots + a_n \mathbb{E}[X_n]$$

Theorem 33 (Multiplikativität des Erwartungswerts). For X_1, \dots, X_n :

$$\mathbb{E}[X_1 \cdot \dots \cdot X_n] = \mathbb{E}[X_1] \cdot \dots \cdot \mathbb{E}[X_n]$$

Theorem 34. For independent X_1, \dots, X_n and $X := X_1 + \dots + X_n$ then

$$\text{Var}[X] = \text{Var}[X_1] + \dots + \text{Var}[X_n]$$

3.7 Abschätzen von Wahrscheinlichkeiten

Theorem 35 (Ungleichung von Markov). $X \geq 0$ Zufallsvariable. Then, for all $t > 0 \in \mathbb{R}$:

$$\Pr[X \geq t] \leq \frac{\mathbb{E}[X]}{t} \text{ und } \Pr[X \geq t \cdot \mathbb{E}[X]] \leq \frac{1}{t}$$

Theorem 36 (Ungleichung von Chebyshev). X Zufallsvariable and $t > 0 \in \mathbb{R}$. Then

$$\Pr[|X - \mathbb{E}[X]| \geq t] \leq \frac{\text{Var}[X]}{t^2}$$

Theorem 37 (Ungleichung von Chernoff). X_1, \dots, X_n independent Bernoulli-verteilte Zufallsvariablen with $\Pr[X_i = 1] = p_i$ and $\Pr[X_i = 0] = 1 - p_i$.

Then for $X := \sum_{i=1}^n X_i$:

$$\Pr[X \geq (1 + \delta)\mathbb{E}[X]] \leq e^{-\frac{1}{3}\delta^2\mathbb{E}[X]} \text{ for all } 0 < \delta \leq 1 \quad (1)$$

$$\Pr[X \geq (1 - \delta)\mathbb{E}[X]] \leq e^{-\frac{1}{2}\delta^2\mathbb{E}[X]} \text{ for all } 0 < \delta \leq 1 \quad (2)$$

$$\Pr[X \geq t] \leq 2^{-t} \quad \text{for } t \geq 2e\mathbb{E}[X] \quad (3)$$

3.8 Randomized algorithms

Theorem 38. *Let \mathcal{A} be a randomized algorithm that always never gives a wrong answer, but outputs "???" when*

$$\Pr[\mathcal{A}(I) \text{ correct}] \geq \epsilon$$

Then for all $\delta > 0$: let \mathcal{A}_δ be the algorithm that calls \mathcal{A} until either an answer different from "???" is returned (\mathcal{A}_δ gives this answer) or until "???" is returned $N = \epsilon^{-1} \ln \delta^{-1}$ times (\mathcal{A}_δ returns "???").

Then the following is true:

$$\Pr[\mathcal{A}_\delta \text{ correct}] \geq 1 - \delta$$

Theorem 39. *Let \mathcal{A} be a randomized algorithm that always gives "Yes" or "No" as answers, where*

$$\Pr[\mathcal{A}(I) = \text{Yes}] = 1 \quad \text{if the correct answer is Yes} \quad (4)$$

$$\Pr[\mathcal{A}(I) = \text{No}] \geq \epsilon \quad \text{if the correct answer is No} \quad (5)$$

Then for all $\delta > 0$: let \mathcal{A}_δ be the algorithm that calls \mathcal{A} either until "No" is returned (then it returns "No") or until "Yes" is returned $N = \epsilon^{-1} \ln \delta^{-1}$ times (then it returns "Yes").

Then for all instances I :

$$\Pr[\mathcal{A}_\delta(I) \text{ correct}] \geq 1 - \delta$$

Theorem 40. *Let $\epsilon > 0$ and \mathcal{A} be a randomized algorithm that always returns either "Yes" or "No", Where*

$$\Pr[\mathcal{A}_\delta(I) \text{ correct}] \geq \frac{1}{2} + \epsilon$$

Then for all $\delta > 0$: let \mathcal{A}_δ be the algorithm that calls \mathcal{A} a total of $N = 4\epsilon^{-2} \ln \delta^{-1}$ times and returns the answer that was encountered the most.

Then

$$\Pr[\mathcal{A}_\delta(I) \text{ correct}] \geq 1 - \delta$$

Theorem 41. *Let $\epsilon > 0$ and \mathcal{A} be a randomized algorithm for a Maximierungsproblem, where*

$$\Pr[\mathcal{A}(I) \geq f(I)] \geq \epsilon$$

Then for all $\delta > 0$: let \mathcal{A}_δ be the algo that calls \mathcal{A} a total of $N = \epsilon^{-1} \ln \delta^{-1}$ times and returns the best answer. Then

$$\Pr[\mathcal{A}_\delta(I) \geq f(I)] \geq 1 - \delta$$

Analogous for Minimierungsprobleme, replace $\geq f(I)$ with $\leq f(I)$.

Note 3. Stuff about random pivot selection for QuickSort and so on

Theorem 42 (Kleiner fermatscher satz). If $n \in \mathbb{N}$ is prime, then for all $0 < a < n$

$$a^{n-1} \equiv 1 \pmod{n}$$

Target shooting:

Theorem 43. Let $\delta, \epsilon > 0$. If $N \geq 3 \frac{|U|}{|S|} \cdot \epsilon^{-2} \cdot \ln(2/\delta)$, then the output of the algorithm Target-Shooting is in the interval $\left[(1 - \epsilon) \frac{|S|}{|U|}, (1 + \epsilon) \frac{|S|}{|U|}\right]$ with probability $1 - \delta$.

4 Algorithmen

4.1 Graphenalgorithmen