Berechenbarkeit und Komplexität
14. Vorlesung

Prof. Dr. Dietrich Kuske

FG Automaten und Logik, TU Ilmenau

Sommersemester 2023

Ziel dieser Vorlesung

Nicht nur SAT, sondern auch viele andere Probleme sind NP-vollständig, d.h. für jedes dieser Probleme A gilt:

Wer A „schnell“ lösen kann, der kann alle Probleme in NP „schnell“ lösen.

Weitere NP-vollständige Probleme

Wir betrachten nun folgende Reduktionen und weisen dadurch nach, daß alle diese Probleme NP-hart sind (sie sind auch in NP und damit NP-vollständig).

$$\begin{aligned} \text{SAT} \quad \leq_P \quad & \text{3-SAT} \leq_P \text{3C und} \\ & \text{3-SAT} \leq_P \text{DHC} \leq_P \text{HC} \leq_P \text{TSP} \end{aligned}$$

- 3-SAT: Ist eine aussagenlogische Formel in konjunktiver Normalform mit ≤ 3 Literalen pro Klausel erfüllbar?
- 3C: Ist ein ungerichteter Graph drei-färbbar?
- DHC: Enthält ein gerichteter Graph einen Hamiltonkreis?
- HC: Enthält ein ungerichteter Graph einen Hamiltonkreis?
- TSP: Travelling Salesman Problem

3-SAT ist NP-vollständig

Ein Literal ist eine möglicherweise negierte atomare Formel, d.h. eine Formel der Form x_i oder $\neg x_i$. Eine Klausel ist eine Disjunktion von Literalen, z.B. $(x_1 \vee \neg x_2 \vee x_3)$.

Erfüllbarkeitsproblem 3-SAT

EINGABE: eine aussagenlogische Formel φ in konjunktiver Normalform mit höchstens drei Literalen pro Klausel.

FRAGE: Hat φ eine erfüllende Belegung?

Definition 3-SAT

3-SAT ist die Menge der erfüllbaren aussagenlogischen Formeln in konjunktiver Normalform mit höchstens drei Literalen pro Klausel.

Beispiel: Die Formel $\varphi = (x_1 \vee \neg x_2) \wedge (x_1 \vee x_2 \vee x_3) \wedge \neg x_1 \wedge \neg x_3$ ist in der geforderten Form und hat <u>keine</u> erfüllende Belegung. Das heißt $\varphi \notin$ 3-SAT.

Satz

Das Problem 3-SAT ist NP-vollständig.

Beweis:
Wie SAT ist auch 3-SAT in NP.
Für die NP-Härte reicht es, SAT $\leq_P$ 3-SAT zu zeigen (da SAT nach dem Satz von Cook-Levin NP-hart ist). Wir müssen also in polynomieller Zeit aus einer beliebigen Formel φ eine Formel φ' in KNF mit höchstens drei Literalen pro Klausel bestimmen, so daß

$$\varphi \text{ erfüllbar} \iff \varphi' \text{ erfüllbar}$$

Dies haben wir bereits in der 8. Vorlesung „Logik und Logikprogrammierung“ getan: Stichwort „Tseitin-Konstruktion“. $\square$

Wir haben gezeigt:

Satz

Die Probleme SAT und 3-SAT sind NP-vollständig.

Das heißt, schon Formeln in KNF mit höchstens drei Literalen pro Klausel enthalten „die volle Schwierigkeit des Erfüllbarkeitsproblems" SAT.

Was ist mit noch einfacher aussehenden Formeln?

- DNF: Das Erfüllbarkeitsproblem ist in P.
- 2-SAT: Formeln in KNF, die höchstens zwei Literale pro Klausel enthalten?

Satz

Es ist in Polynomialzeit entscheidbar, ob eine Formel φ in KNF mit höchstens zwei Literalen pro Klausel erfüllbar ist.

Beweisidee: konstruieren gerichteten Graphen G:

- Für jede atomare Formel x aus φ gibt es die Knoten x und $\neg x$.
- Für jede Klausel $\alpha \vee \beta$ in φ gibt es Kanten $\sim\alpha \to \beta$ und $\sim\beta \to \alpha$, wobei $\sim x = \neg x$ und $\sim\neg x = x$ gelte.

Dann sind äquivalent:

1. φ ist nicht erfüllbar.
2. es gibt atomare Formel x und Pfad $x \to^* \neg x \to^* x$ (d.h., x und $\neg x$ liegen in derselben starken Zusammenhangskomponente).

Dies kann in Polyomialzeit entschieden werden. $\square$

Wir haben gezeigt:

Satz

- Die Erfüllbarkeitsprobleme SAT und 3-SAT sind NP-vollständig.
- Das Erfüllbarkeitsproblem 2-SAT ist in P.

Die Grenze zwischen „einfachen“ und „schwierigen“ Formeln liegt also zwischen Formeln in KNF mit höchstens zwei bzw. höchstens drei Literalen pro Klausel.

3C ist NP-vollständig

k-Färbbarkeit von Graphen

EINGABE: Ein ungerichteter Graph $G = (V, E)$.

FRAGE: Gibt es Zuordnung von k verschiedenen Farben zu Knoten in V, so daß keine zwei benachbarten Knoten v_1, v_2 dieselbe Farbe haben?

Definition kC

kC ist die Menge der ungerichteten Graphen, die sich mit k Farben färben lassen.

Ein Graph ist genau dann 2-färbbar, wenn er bipartit ist. Das Problem 2C ist also in P.

Satz

Das Problem 3C ist NP-vollständig.

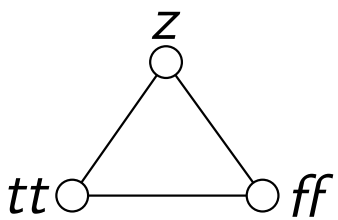
Beweis: 3C $\in$ NP ist einfach zu sehen, da eine Färbung geraten und in polynomieller Zeit überprüft werden kann, ob sie die Bedingungen erfüllt.

Für die NP-Härte zeigen wir 3-SAT $\leq_P$ 3C:
Wir bestimmen dazu eine Reduktionsfunktion, die einer gegebenen Formel φ einen ungerichteten Graphen G zuordnet, so daß φ genau dann erfüllbar ist, wenn G drei-färbbar ist.

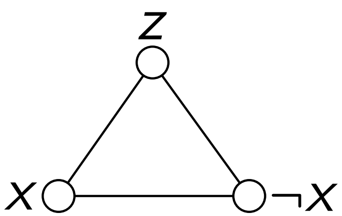
Dabei können wir davon ausgehen, daß φ in konjunktiver Normalform ist und höchstens drei Literale pro Klausel hat.

Sei also φ Formel in KNF, deren Klauseln genau drei Literale enthalten (ggf. ersetze z.B. $x_1 \vee x_2$ durch $x_1 \vee x_2 \vee x_2$). Der Graph G setzt sich wie folgt zusammen:

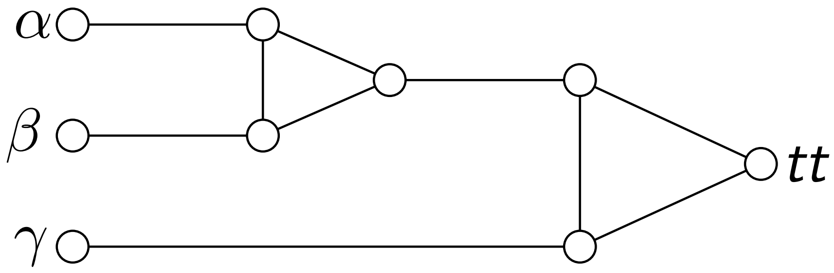
- ein zentrales Dreieck



- für jede atomare Formel x das folgende Atomformel-Dreieck (das den Knoten z des zentralen Dreiecks enthält):

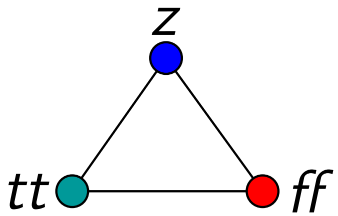


- für jede Klausel $\alpha \vee \beta \vee \gamma$ den folgenden Klausel-Teilgraphen (der die Knoten *tt* des zentralen und α, β und γ der Atomformel-Dreiecke enthält):

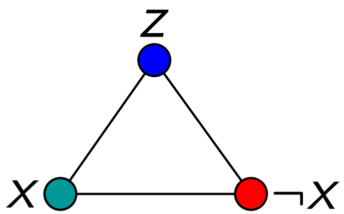


Sei nun $\mathcal{B}$ eine Belegung der Variablen von φ mit $\mathcal{B}(\varphi) = 1$. Wir färben G wie folgt mit den Farben •, • und •:

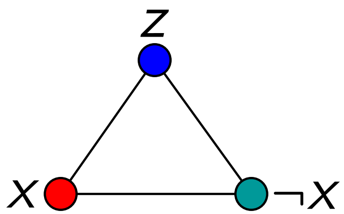
- zentrales Dreieck:



- Atomformel-Dreieck für atomare Formel x:

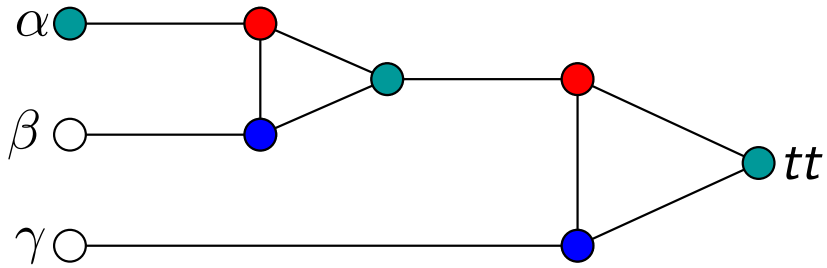


falls $\mathcal{B}(x) = 1$

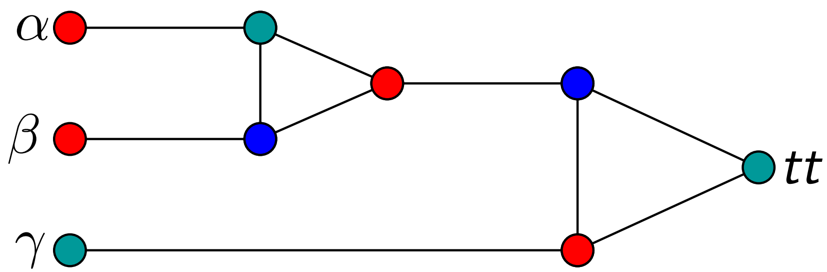


falls $\mathcal{B}(x) = 0$

- Sei $\alpha \vee \beta \vee \gamma$ Klausel. Wegen $\mathcal{B}(\varphi) = 1$ gilt $\mathcal{B}(\alpha) = 1$ oder $\mathcal{B}(\beta) = 1$ oder $\mathcal{B}(\gamma) = 1$. Keiner der Knoten α, β und γ hat die Farbe •.
  1. $\mathcal{B}(\alpha) = 1$. Dann sind die Knoten α und tt •.

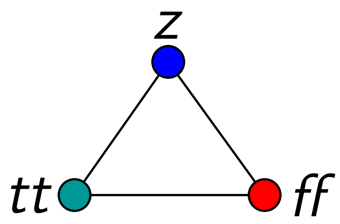


  2. $\mathcal{B}(\beta) = 1$. Man erhält eine analoge Färbung.
  3. $\mathcal{B}(\gamma) = 1$. Wir können annehmen, daß $\mathcal{B}(\alpha) = \mathcal{B}(\beta) = 0$.

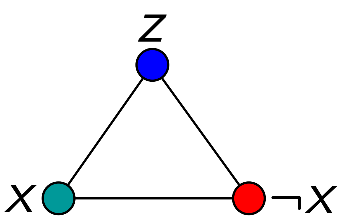


Damit gilt: φ erfüllbar $\Longrightarrow$ G 3-färbbar.

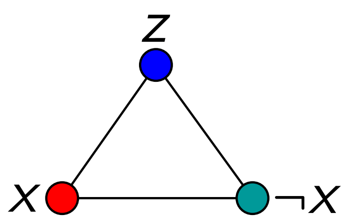
Sei umgekehrt eine Färbung des Graphen G mit drei Farben gegeben. Wir konstruieren eine Belegung $\mathcal{B}$ mit $\mathcal{B}(\varphi) = 1$.
Sei Färbung des zentralen Dreiecks wie folgt:



Dann ergibt sich für die Atomformel-Dreiecke:

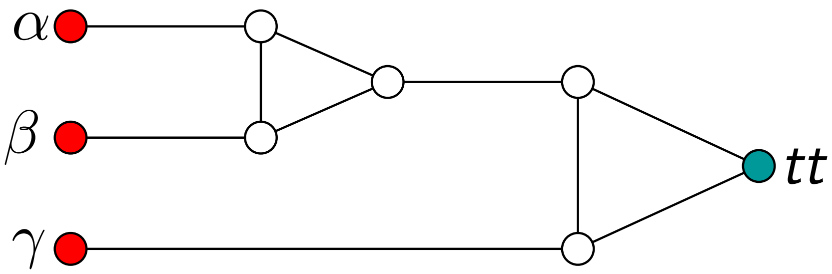


oder



Im ersten Fall setze $\mathcal{B}(x) = 1$, im zweiten $\mathcal{B}(x) = 0$.

Angenommen, $\mathcal{B}(\varphi) = 0$ mit der eben definierten Belegung $\mathcal{B}$. Dann existiert eine Klausel $\alpha \vee \beta \vee \gamma$ mit $\mathcal{B}(\alpha \vee \beta \vee \gamma) = 0$, also $\mathcal{B}(\alpha) = \mathcal{B}(\beta) = \mathcal{B}(\gamma) = 0$. Damit hat der zugehörige Klausel-Teilgraph die Farben



Dies läßt sich nicht zu einer 3-Färbung fortsetzen. Also gilt $\mathcal{B}(\varphi) = 1$, d.h. es gilt: φ erfüllbar $\Longleftarrow$ G 3-färbbar.

Da der Graph G in Polynomialzeit aus der Formel φ berechnet werden kann, haben wir also 3-SAT $\leq_P$ 3C. $\square$

DHC ist NP-vollständig

DHC – Gerichteter Hamiltonkreis

EINGABE: ein gerichteter Graph $G = (V, E)$ mit Knotenmenge V und Kantenmenge $E \subseteq V \times V$.

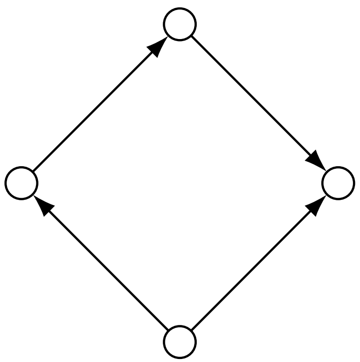
FRAGE: Besitzt der Graph G einen Hamiltonkreis, d.h. kann man den Graphen so durchlaufen, daß jeder Knoten genau einmal besucht wird?

Definition DHC

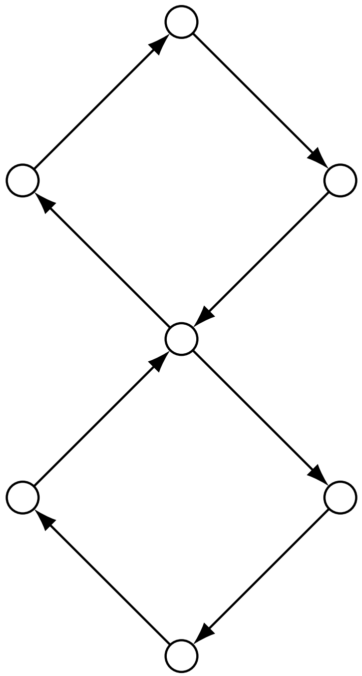
DHC ist die Menge der gerichteten Graphen, die einen Hamiltonkreis enthalten.

Beispiele

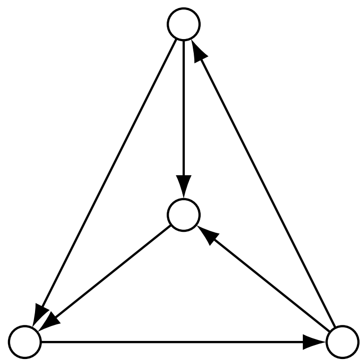
für Graphen mit und ohne Hamiltonkreis:



$\notin$ DHC



$\notin$ DHC



$\in$ DHC

Man kennt keine Charakterisierung dieser Graphen wie im Satz über die Existenz von Eulerkreisen (obwohl man seit 1857 danach sucht)

Satz

Das Problem DHC ist NP-vollständig.

Beweis: zunächst gilt DHC $\in$ NP, denn man kann einen Hamilton-Kreis raten und in polynomieller Zeit prüfen, ob es sich tatsächlich um einen handelt.
noch zu zeigen ist NP-Härte, wofür 3-SAT $\leq_P$ DHC ausreicht.

Wir bestimmen dazu eine Reduktionsfunktion, die einer gegebenen Formel φ einen gerichteten Graphen G zuordnet, so daß φ genau dann erfüllbar ist, wenn G einen Hamiltonkreis besitzt.

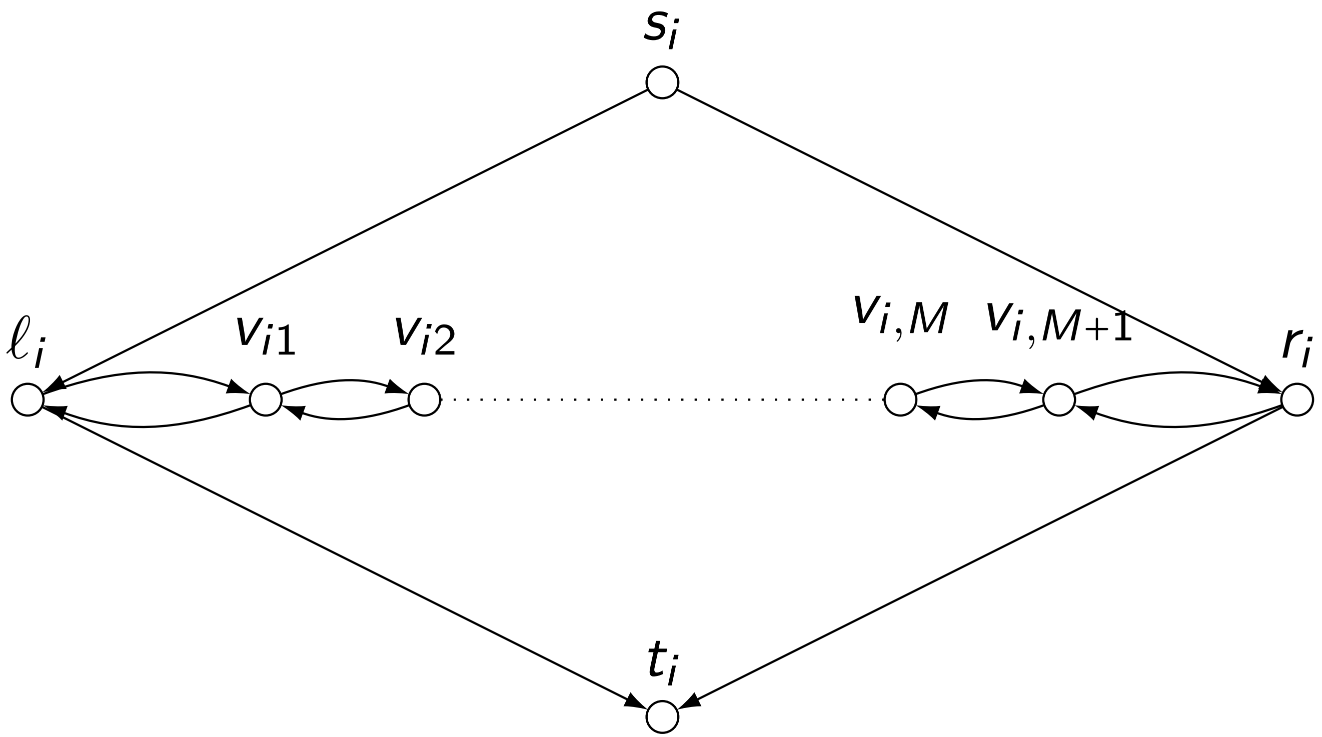
Dabei können wir davon ausgehen, daß φ in konjunktiver Normalform ist und höchstens drei Literale pro Klausel hat.

Sei also φ Formel in KNF mit Klauseln $c_1, c_2, \ldots, c_M$ und atomaren Formeln $x_1, x_2, \ldots, x_N$

Ziel: Berechnung eines gerichteten Graphen G in polynomieller Zeit, der genau dann einen Hamilton-Kreis enthält, wenn φ erfüllbar ist.

Der Graph G enthält

- für jede Klausel c_j einen Knoten C_j $(1 \leq j \leq M)$und
- für jede atomare Formel x_i das folgende „Diamantengadget“ D_i $(1 \leq i \leq N)$:

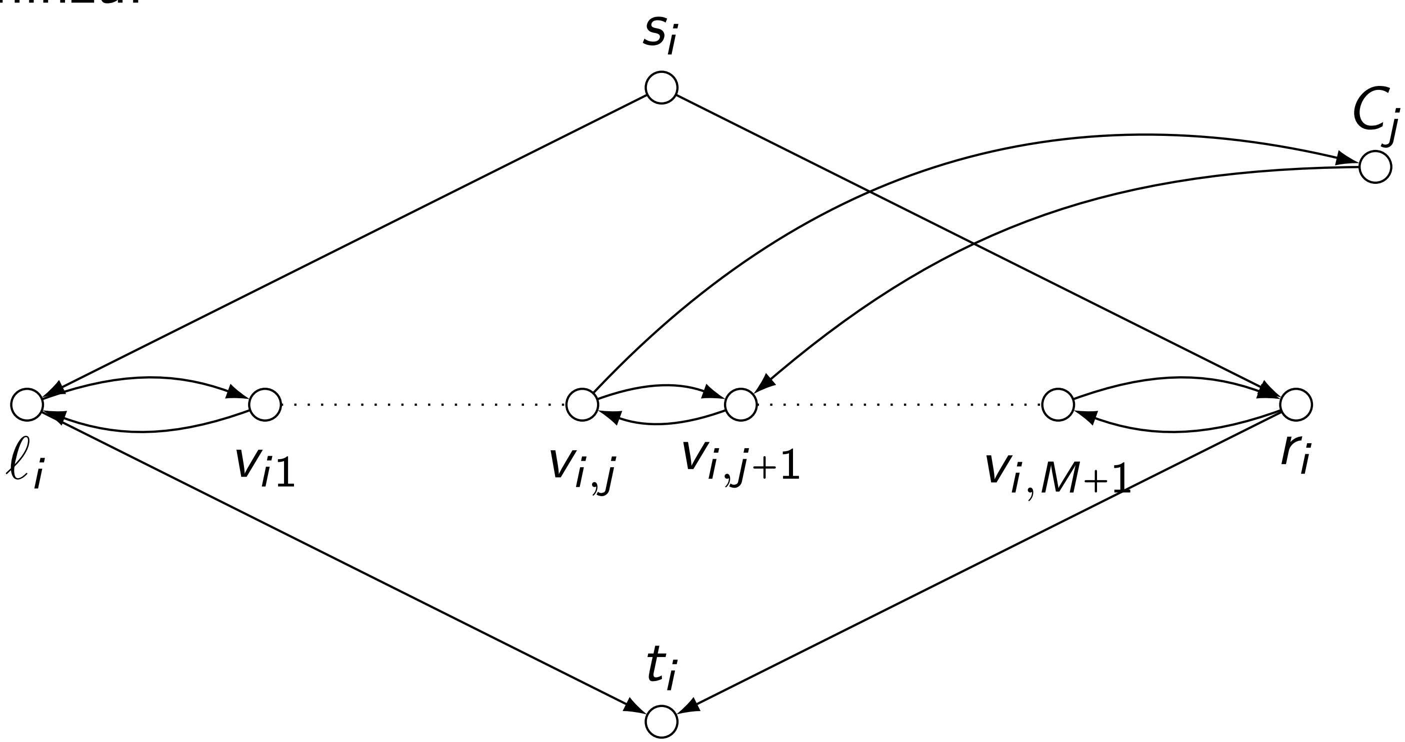


Die Diamantengadgets D_i werden „in einem Ring angeordnet" durch Kanten (t_i, s_{i+1}) (für alle $1 \leq i < N$) und (t_N, s_1).
$\rightsquigarrow$ jeder Hamiltonkreis muß die Gadgets in der Reihenfolge $D_1, D_2, \ldots, D_N$ durchlaufen und jedes Gadget von rechts nach links oder umgekehrt

Idee: Durchlauf von D_i von links nach rechts kodiert „die atomare Formel x_i wird mit 1 belegt", Durchlauf von D_i von rechts nach links kodiert „die atomare Formel x_i wird mit 0 belegt"

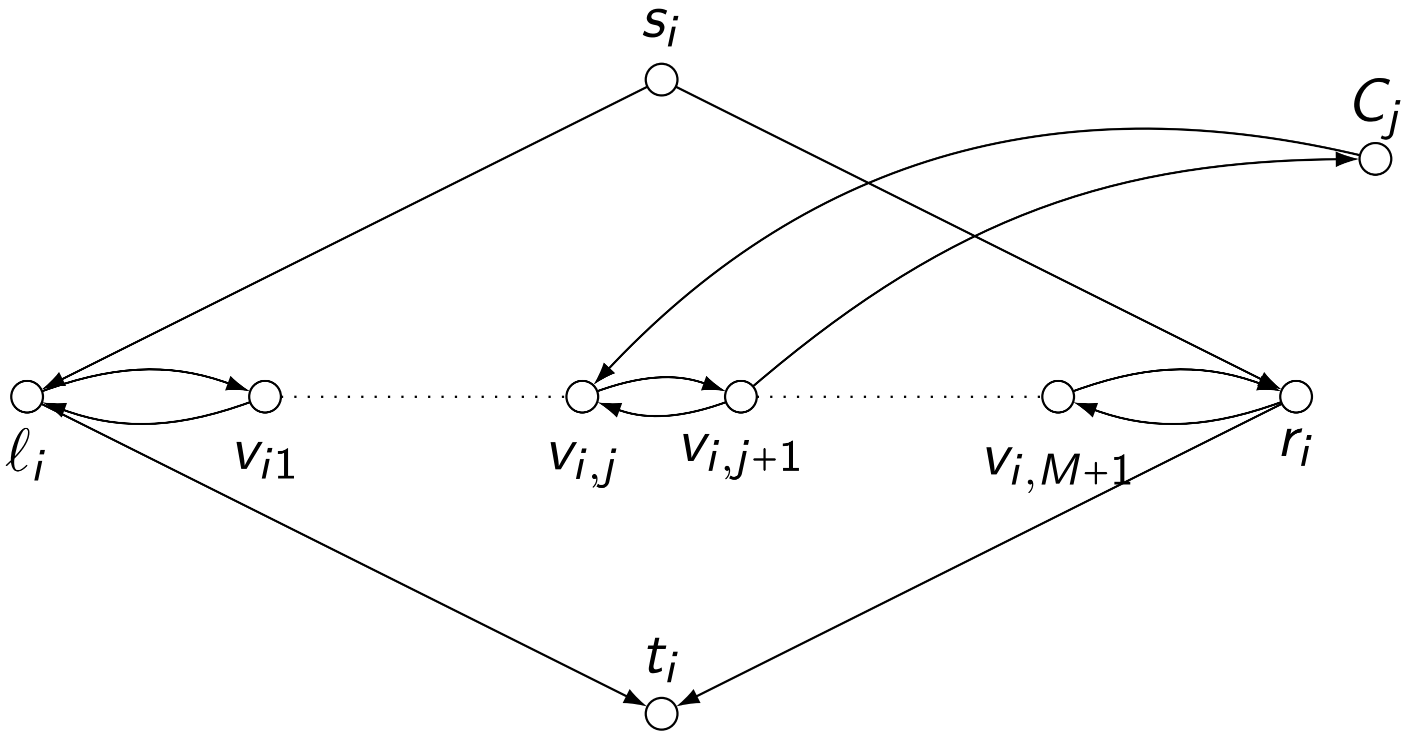
damit: Hamiltonkreise in diesem „Ring" entsprechen den Belegungen der atomaren Formeln $x_1, \ldots, x_N$

Enthält die Klausel c_j das Literal x_i, so füge Kantenzug $v_{i,j} \to C_j \to v_{i,j+1}$ hinzu:



Idee: Durchlauf von D_i von links nach rechts hieß „atomare Formel x_i mit 1 belegt“, also Klausel c_j wahr - und der ihr zugeordnete Knoten C_j kann im Hamiltonkreis beim Durchlauf von D_i besucht werden

Enthält die Klausel c_j das Literal $\neg x_i$, so füge Kantenzug $v_{i,j+1} \to C_j \to v_{i,j}$ hinzu:



Idee: Durchlauf von D_i von rechts nach links hieß „atomare Formel x_i mit 0 belegt“, also Klausel c_j wahr - und der ihr zugeordnete Knoten C_j kann im Hamiltonkreis beim Durchlauf von D_i besucht werden

Damit gilt für den so definierten Graphen G:

- G hat Hamilton-Kreis $\Longleftrightarrow$ φ ist erfüllbar
- G kann aus φ in polynomieller Zeit berechnet werden.

also: 3-SAT $\leq_P$ DHC, womit folgt, daß DHC NP-hart und damit NP-vollständig ist. $\square$

HC ist NP-vollständig

Im nächsten Schritt zeigen wir, daß auch das analoge Problem für ungerichtete Graphen NP-vollständig ist.

HC – Ungerichteter Hamiltonkreis

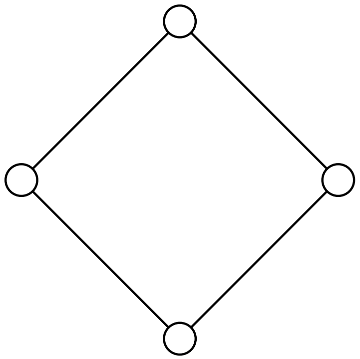
EINGABE: ein ungerichteter Graph $G = (V, E)$ mit Knotenmenge V und Kantenmenge $E \subseteq \binom{V}{2} = \{X \subseteq V \mid |X| = 2\}$.

FRAGE: Besitzt der Graph G einen Hamiltonkreis, d.h. kann man den Graphen so durchlaufen, daß jeder Knoten genau einmal besucht wird?

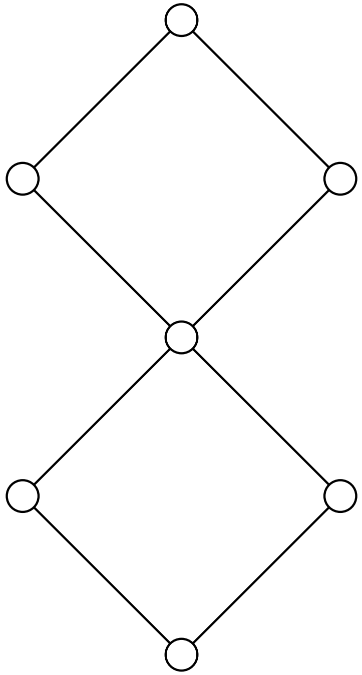
Definition HC

HC ist die Menge der ungerichteten Graphen, die einen Hamiltonkreis enthalten.

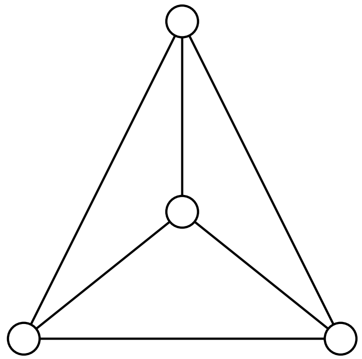
Beispiele für Graphen mit und ohne Hamiltonkreis:



$\in \mathrm{HC}$



$\notin \mathrm{HC}$



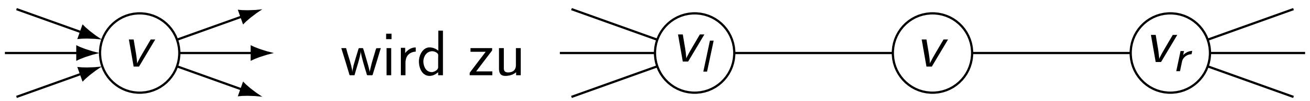
$\in \mathrm{HC}$

Satz

Das Problem HC ist NP-vollständig.

Beweis: HC $\in$ NP ist einfach zu sehen, da ein Hamilton-Kreis geraten und in polynomieller Zeit überprüft werden kann, daß es sich in der Tat um einen Hamilton-Kreis handelt.
Für die NP-Härte reicht es, DHC $\leq_P$ HC zu zeigen. Daher müssen wir zu jedem gerichteten Graphen G einen ungerichteten Graphen G' konstruieren, so daß G genau dann einen Hamiltonkreis hat, wenn G' einen Hamiltonkreis hat.

Idee: Ersetze einen Knoten mit ein- und ausgehenden Kanten wie folgt:



$\square$

TSP ist NP-vollständig

Wir zeigen nun, daß auch das Travelling-Salesman-Problem NP-vollständig ist.

TSP – Travelling Salesman

EINGABE: eine $n \times n$-Matrix $M = (M_{i,j})$ von Entfernungen zwischen n Städten und eine Zahl d.

FRAGE: Gibt es eine Tour durch alle Städte, die maximal die Länge d hat? Das heißt, gibt es eine Indexfolge $i_1, \ldots, i_m$, so daß gilt:

- $\{i_1, \ldots, i_m\} = \{1, \ldots, n\}$ (jede Stadt kommt vor)
- $M_{i_1,i_2} + M_{i_2,i_3} + \cdots + M_{i_{m-1},i_m} + M_{i_m,i_1} \leq d$ (die Länge der Tour ist höchstens d)

Satz

Das Problem TSP ist NP-vollständig.

Beweis: TSP $\in$ NP ist einfach zu sehen, da eine Indexfolge geraten und in polynomieller Zeit überprüft werden kann, ob sie die Bedingungen erfüllt.

Für die NP-Härte zeigen wir HC $\leq_P$ TSP:
Sei $G = (V, E)$ ein ungerichteter Graph, o.E. $V = \{1, \ldots, n\}$. Wir konstruieren dazu folgende Matrix:

$$M_{i,j} = \begin{cases} 1 & \text{falls } \{i,j\} \in E \\ 2 & \text{falls } \{i,j\} \notin E \end{cases}$$

Außerdem setzen wir $d = n$. $\square$

— 188 —

in den Händen der Niederländer ist, kann im Allgemeinen, als eines der angenehmsten betrachtet werden. Das Geschäft ist reell und Chikane finden weniger dabei Statt, als bei den meisten andern Artikeln. Uebrigens muß es den Niederländern auch nachgerühmt werden, daß sie pünktlich und gewissenhaft im Handel sind. Sie geben selten Anlaß zu Beschwerden, und der Reisende hat also nicht ewige Streitigkeiten zu schlichten.

9.

Die Geschäfte führen den Handlungsreisenden bald hier, bald dort hin, und es lassen sich nicht füglich Reisetouren angeben, die für alle vorkommende Fälle passend sind; aber es kann durch eine zweckmäßige Wahl und Eintheilung der Tour, manchmal so viel Zeit gewonnen werden, daß wir es nicht glauben umgehen zu dürfen, auch hierüber einige Vorschriften zu geben. Ein Jeder möge so viel davon benutzen, als er es seinem Zwecke für dienlich hält; so viel glauben wir aber davon versichern zu dürfen, daß es nicht wohl thunlich sein wird, die Touren durch Deutschland in Absicht

— 189 —

der Entfernungen und, worauf der Reisende hauptsächlich zu sehen hat, des Hin= und Herreisens, mit mehr Oekonomie einzurichten. Die Hauptsache besteht immer darin: so viele Orte wie möglich mitzunehmen, ohne den nämlichen Ort zweimal berühren zu müssen. Wir nehmen Frankfurt a. M. als den Ausgangspunkt an und beginnen mit der Tour nach Westphalen und durch Churhessen zurück. An allen angeführten Orten sind solide Leute anzutreffen. Die Addressen geben wir nicht auf, weil sich die Verhältnisse zu häufig ändern; jedoch finden sich die Gasthöfe meistens angemerkt, und nur an Orten, wo man nicht leicht in den Fall kommt, zu übernachten, sich etwa nur kurze Zeit verweilt, ist es unterblieben. Die mit * bezeichnete Orte sind zwar nur Flecken oder Dörfer, aber es sind solide und zum Theil nicht unbedeutende Leute da *).

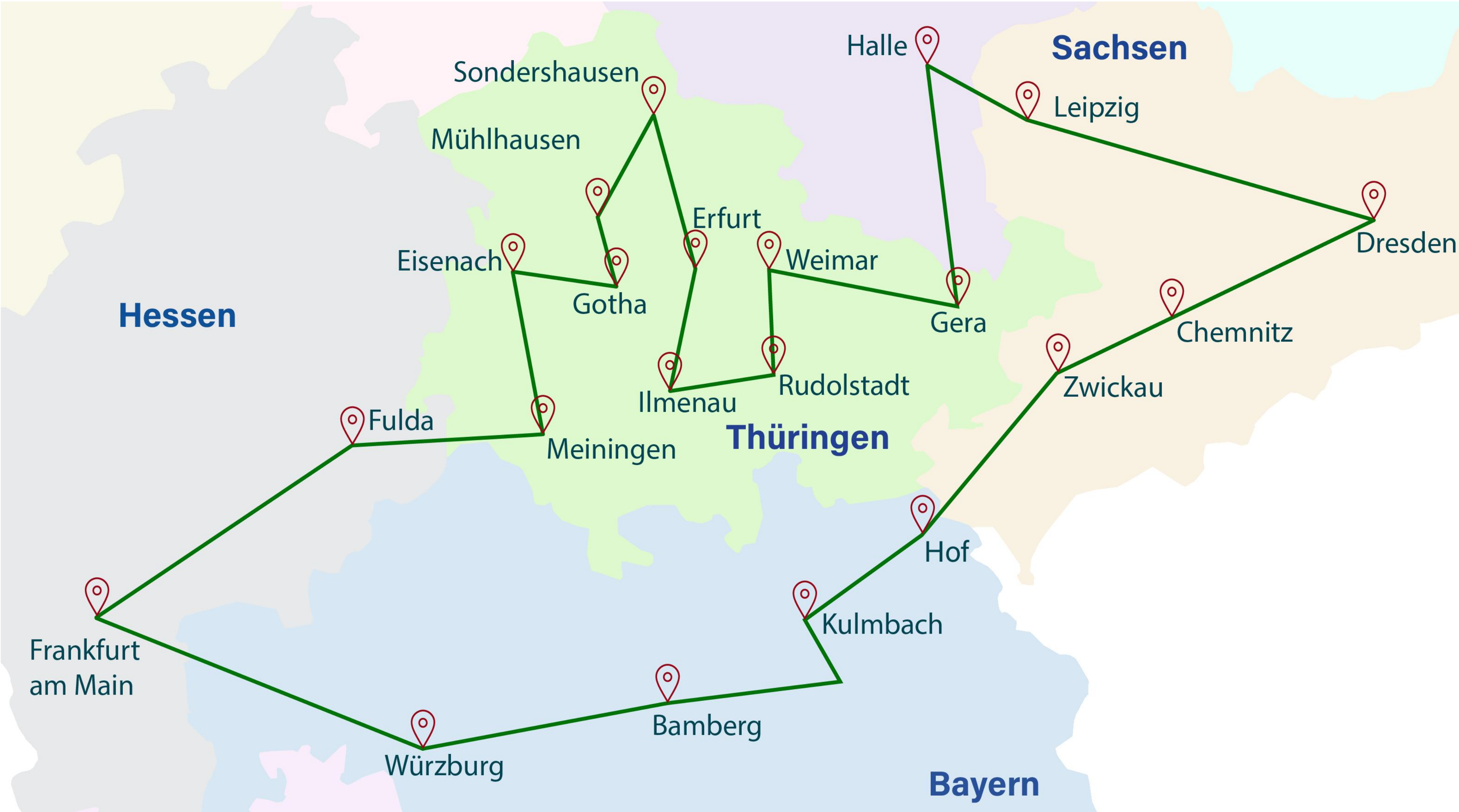
*) Da ich Andern nicht gern etwas empfehle und zu etwas rathe, was sich nicht auf meine eigene Ueberzeugung und Erfahrung gründet, so habe ich hier nur die Touren aufgenommen, die ich genauer kenne und meist selbst wiederholt bereist habe. Sie durch ganz Deutschland aufzu-

— 190 —

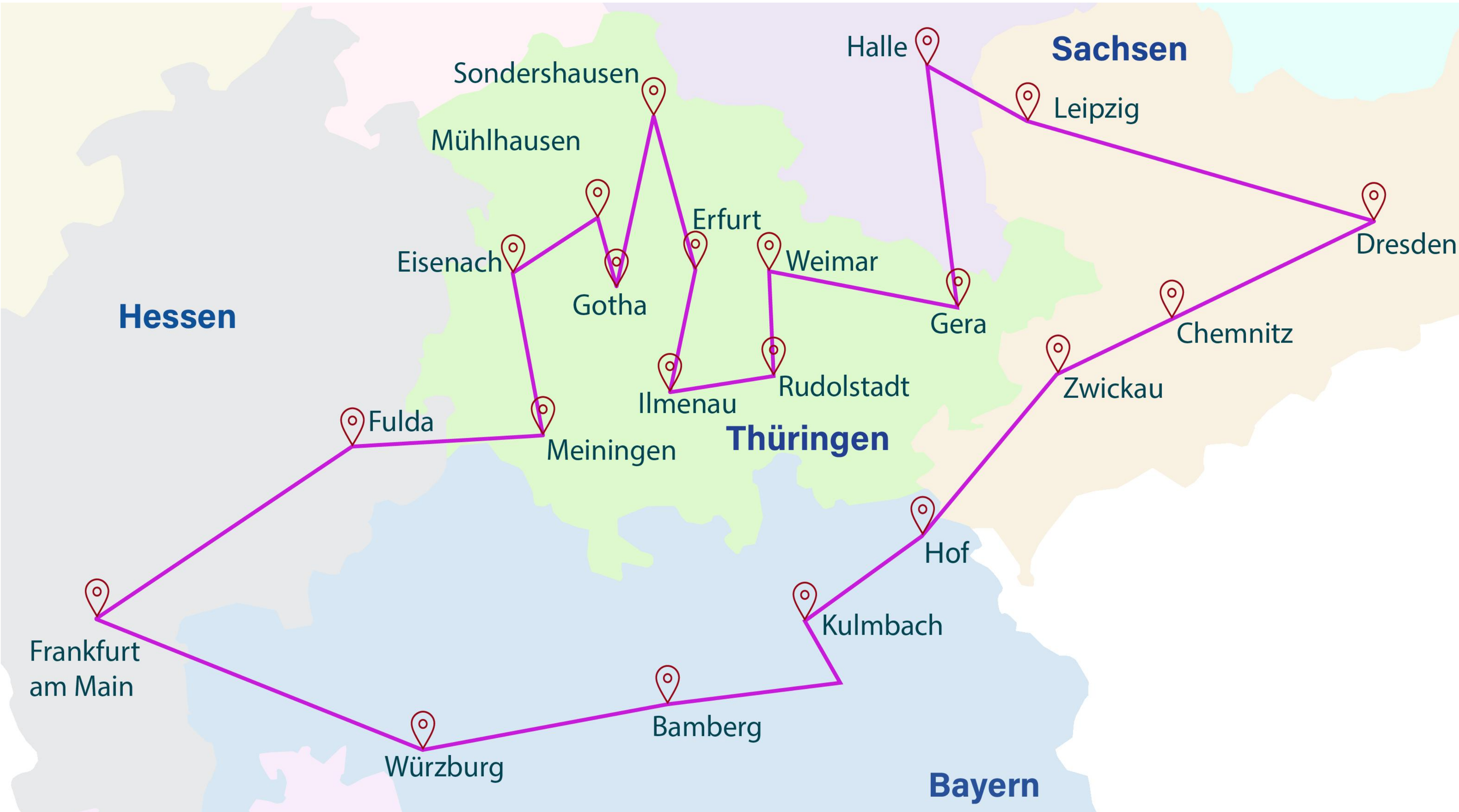
10.

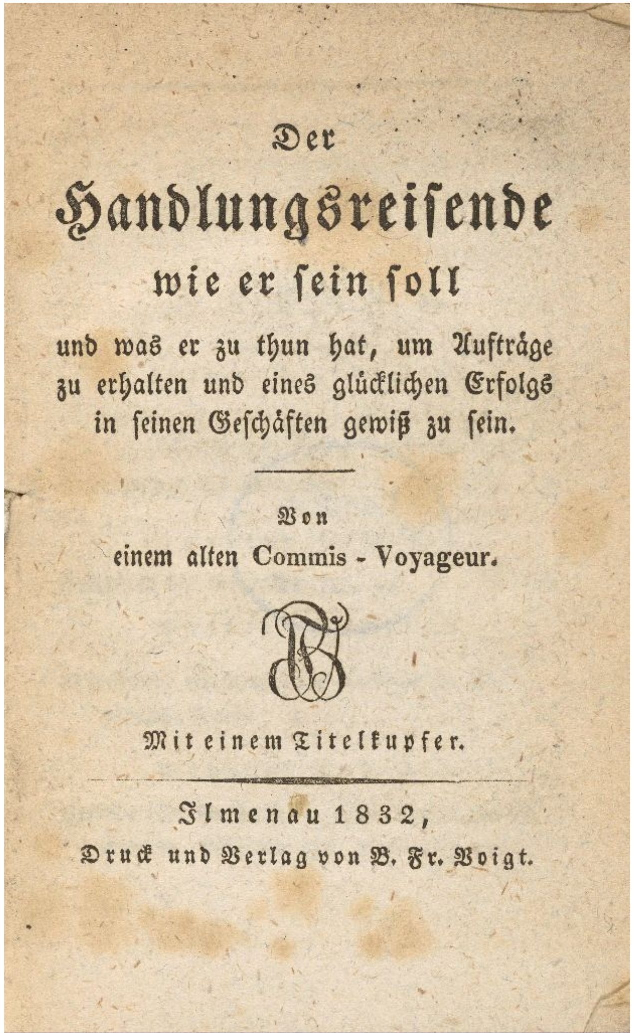
Frankfurt a. M. im Weidenbusch, Weidenhof u. Pariserhof.
Homburg v. d. Höhe im Engel.
Friedrichsdorf im Ritter.
Alsingen in der Post.
Butzbach im Löwen oder bei Sarasin.
Hungen im Gemeindewirthshaus.
Laubach im gold. Löwen.
Grünberg im wilden Mann.
Gießen im Einhorn oder Rappen.
Wetzlar im Erbprinz.
Herborn im Ritter.
Dillenburg im Hirsch.
Hayger bei der Amtsjägerin.
Siegen im Löwen. Von da zurück nach Dillenburg, und über Gladenbach nach
Marburg im Ritter.
Biedenkopf im Hirsch.
Laasphe bei Renaud.
Battenberg.
Battenfeld am Battenberg bei Arnold.
Berleburg bei Prinz.

führen, hätte ich nicht mit meiner eigenen Erfahrung vereinigen können, und das würde auch für den Raum dieses kleinen Werkchens zu viel geworden sein. Die neueste Auflage von Reichardts Passagier durch Deutschland und mehrere ähnliche Werke von Fick, Engelmann ꝛc. können hier Jedem zur Ergänzung dienen. Auch sind ja diese Routen nur Nebenzweck bei gegenwärtigem Büchlein.


Halle
Sachsen
Sondershausen
Leipzig
Mühlhausen
Erfurt
Dresden
Eisenach
Weimar
Gotha
Gera
Hessen
Chemnitz
Zwickau
Rudolstadt
Ilmenau
Fulda
Thüringen
Meiningen
Hof
Kulmbach
Frankfurt
am Main
Bamberg
Würzburg
Bayern


Halle
Sachsen
Sondershausen
Leipzig
Mühlhausen
Erfurt
Eisenach
Weimar
Dresden
Gotha
Gera
Hessen
Chemnitz
Zwickau
Rudolstadt
Ilmenau
Fulda
Thüringen
Meiningen
Hof
Kulmbach
Frankfurt
am Main
Bamberg
Würzburg
Bayern


Halle
Sachsen
Sondershausen
Leipzig
Mühlhausen
Erfurt
Dresden
Eisenach
Weimar
Gotha
Gera
Hessen
Chemnitz
Zwickau
Rudolstadt
Ilmenau
Fulda
Meiningen
Thüringen
Hof
Kulmbach
Frankfurt
am Main
Bamberg
Würzburg
Bayern

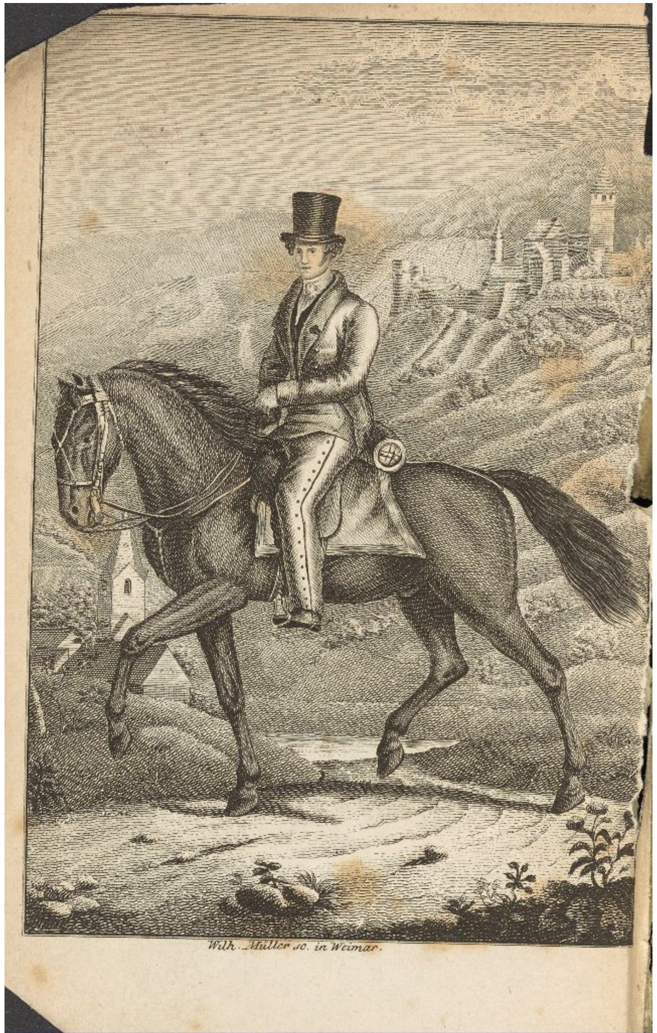


Der
Handlungsreisende
wie er sein soll
und was er zu thun hat, um Aufträge
zu erhalten und eines glücklichen Erfolgs
in seinen Geschäften gewiß zu sein.

Von
einem alten Commis - Voyageur.

Mit einem Titelkupfer.

Ilmenau 1832,
Druck und Verlag von B. Fr. Voigt.



Zusammenfassung 14. Vorlesung

in dieser Vorlesung neu

- Die Probleme 3-SAT, 3C, DHC, HC und TSP sind ebenfalls NP-vollständig.
  Es gibt sehr viele NP-vollständige Probleme, die NP-Vollständigkeit ist also ein weitverbreitetes und natürliches Phänomen.

Zusammenfassung (Komplexitätstheorie)

- Man kann entscheidbare Probleme klassifizieren bezüglich der Ressourcen, die zu ihrer Lösung benötigt werden (Zeit, Platz).
- Man unterscheidet insbesondere zwischen Problemen, die in Polynomialzeit gelöst werden können (Probleme in P) und Problemen, bei denen in Polynomialzeit überprüft werden kann, ob eine geratene und polynomial große Lösung korrekt ist (Probleme in NP).
- Die schwersten Probleme in der Komplexitätsklasse NP heißen NP-vollständig. Viele natürliche Problem fallen in diese Klasse. Für sie gibt es keine bekannten polynomialen Algorithmen.
- Klassifiziert man die entscheidbaren Probleme bzgl. ihres Platzbedarfs, so erhält man Klassen wie PSPACE und EXPSPACE, die ebenfalls natürliche vollständige Probleme enthalten.

Church-Turing These

Die Church-Turing These besagt, daß die Funktionen, die durch Turingmaschinen bzw. While-/Goto-Programme berechnet werden können, genau die intuitiv berechenbaren Funktionen sind.

Unentscheidbarkeit

Probleme, die nicht durch Turing-Maschinen gelöst werden können, sind damit prinzipiell unlösbar (wenn auch u.U. semi-entscheidbar).

Erweiterte Church-Turing These

Die erweiterte Church-Turing These besagt, daß die Funktionen, die durch Turingmaschine bzw. While-/Goto-Programme in Polynomialzeit berechnet werden können, genau die intuitiv und effizient berechenbaren Funktionen sind.

NP und darüber

Probleme, die durch Turing-Maschinen nicht in Polynomialzeit gelöst werden können, sind damit prinzipiell nicht effizient lösbar.