VERTEX COVER (VC)
Eingabe: Ein Graph G und ein $k \in \mathbb{N}$.
Frage: Gibt es ein Eckenüberdeckung[1] V' von G mit $|V'| \leq k$?

DIRECTED HAMILTON PATH (DHP)
Eingabe: Ein gerichteter Graph G und $s, t \in V(G)$, $s \neq t$.
Frage: Gibt es einen gerichteten s-t-Pfad, der alle Ecken von G durchläuft?

Ebenfalls NP-vollst.: HAMILTON PATH (HP) und HK

3COLORING (3COL)
Eingabe: Ein Graph G.
Frage: Gilt $\chi(G) \leq 3$?

3COLORING FOR PLANAR GRAPHS (PLANAR 3COL)
Eingabe: Ein planarer Graph G.
Frage: wie 3COL

Man erhält „Reduktionsketten" wie z. B. (vergl. S. Even, Graph Algorithms):

---

1) vergl. Seite E.112

$$SAT \propto 3SAT \propto 3DM \propto CLIQUE \propto VC \propto DHP \propto DHC$$
$$\& \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \&$$
$$3COL \propto PLANAR\ 3COL \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad HP \propto HC$$

Listen von NP-vollst. Problemen aus den unterschiedlichsten Gebieten findet man beispielsweise in M.R. Garey, D.S. Johnson: Computers and Intractability sowie D. Jungnickel: Graphen, Netzwerke und Algorithmen. Von Tausenden Problemen wurde bislang nachgewiesen werden, dass sie NP-vollständig sind Für keines dieser Probleme konnte bisher ein polynomialer Algorithmus gefunden werden. Es gilt (aufgrund von (ii) in der Definition des Begriffs der NP-Vollständigkeit):

(*) Gelänge es nur für ein einziges NP-vollständiges Problem einen polynomialen Algorithmus zu finden, so gäbe es für jedes dieser Probleme und alle anderen Probleme aus NP einen polynomialen Algorithmus (d.h., es würde P = NP gelten).

6) Zwei Beispiele für NP-Vollständigkeitsbeweise

Wir nehmen an, dass die NP-Vollständigkeit von SAT, 3SAT und 3DM bereits bewiesen ist, und zeigen, dass CLIQUE und 3COL ebenfalls NP-vollständig sind.

Satz. CLIQUE ist NP-vollständig.

Beweis. CLIQUE ist klarerweise in NP, da man eine Clique C von G mit $|C| \geq k$ raten und in polynomialer Zeit nachweisen kann, dass es sich tatsächlich um eine Clique von G mit mindestens k Ecken handelt.

Zum Nachweis der NP-Vollständigkeit von CLIQUE haben wir für ein NP-vollständiges Problem D zu zeigen, dass $D \propto$ CLIQUE gilt.

Wir zeigen $3DM \propto$ CLIQUE. Hierzu sei eine Eingabe I für 3DM gegeben: $M \subseteq W \times X \times Y$. Wir setzen $k = |W|$ und definieren eine Eingabe $f(I)$ für CLIQUE: Diese besteht aus k und $G = (V, E)$ mit $V = M$ und

$$E = \{ m_1 m_2 : m_1, m_2 \in M \text{ und } m_1, m_2 \text{ haben keine Komponente gemeinsam} \}.$$

Es gilt: $G=(V,E)$ hat eine Clique C mit $|C| \geq k \Leftrightarrow$ Es gibt ein $M' \subseteq M$ mit $|M'| = |W| (=k)$ so dass keine zwei Tripel aus M' in einer ihrer Komponenten übereinstimmen. □

Satz. 3COL ist NP-vollständig.

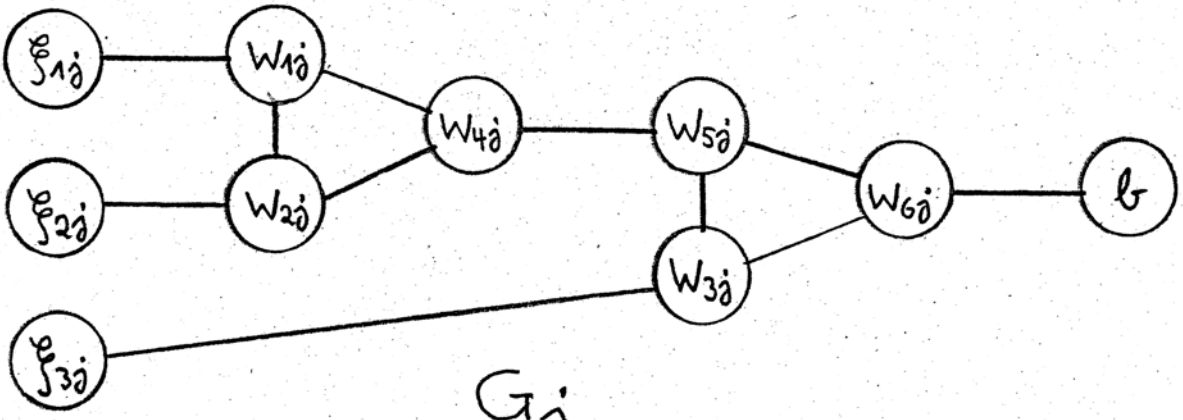
Beweis. $3COL \in NP$: ✓. Wir zeigen $3SAT \propto 3COL$. Hierzu sei I eine Eingabe für 3SAT mit Literalen $\{x_1, \ldots, x_n, \bar{x}_1, \ldots, \bar{x}_n\}$ und Klauseln $C_1, \ldots, C_m$. Es sei $C_j = \{\xi_{1j}, \xi_{2j}, \xi_{3j}\}$ $(j=1, \ldots, m)$.

Die dazugehörige Eingabe $f(I)$ für 3COL sei der Graph $G=(V,E)$, dessen Eckenmenge V aus den Literalen $x_1, \ldots, x_n, \bar{x}_1, \ldots, \bar{x}_n$ sowie $6m+2$ weiteren Ecken besteht, die mit a, b und w_{ij} $(1 \leq i \leq 6, 1 \leq j \leq m)$ bezeichnet seien. Die Kantenmenge E sei definiert durch

$$E = \{ab\} \cup \{a x_i, a \bar{x}_i, x_i \bar{x}_i : 1 \leq i \leq n\} \cup$$

$$\{w_{1j}w_{2j}, w_{1j}w_{4j}, w_{2j}w_{4j}, w_{4j}w_{5j}, w_{3j}w_{5j}, w_{3j}w_{6j}, w_{5j}w_{6j}, w_{6j}b : 1 \leq j \leq m\} \cup$$

$$\{\xi_{1j}w_{1j}, \xi_{2j}w_{2j}, \xi_{3j}w_{3j} : 1 \leq j \leq m\}.$$



G_j

Mit G_j sei der oben abgebildete Teilgraph von G bezeichnet ($j = 1, \dots, m$). Dieser Graph hat folgende Eigenschaften (nachprüfen!):

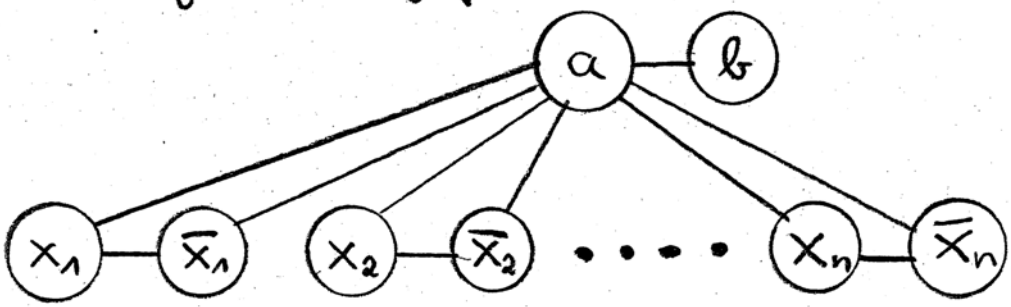
(i) Sind die Ecken $\xi_{1j}, \xi_{2j}, \xi_{3j}$ mit 0 oder 1 gefärbt, wobei mindestens eine dieser drei Ecken die Farbe 1 erhalten hat, so kann man dies zu einer Eckenfärbung von G_j mit 0, 1 und 2 fortsetzen, für die w_{6j} die Farbe 1 bekommt.

(ii) Liegt eine Eckenfärbung von G_j mit 0, 1, 2 vor, wobei für die ξ_{ij} ($i = 1, 2, 3$) nur die Farben 0 und 1 verwendet wurden und w_{6j} nicht mit 0 gefärbt ist, so ist mindestens eine der Ecken $\xi_{1j}, \xi_{2j}, \xi_{3j}$ mit 1 gefärbt.

Mit Hilfe von (i), (ii) zeigen wir: I ist erfüllbar $\Leftrightarrow$ $f(I)$ ist 3-färbbar.

Nachweis dieser Behauptung: a) I sei erfüllbar. Dann gibt es also eine Funktion, die jedem Literal 0 oder 1 zuordnet, so dass in jeder Klausel $C_j = \{\xi_{1j}, \xi_{2j}, \xi_{3j}\}$ mindestens einmal 1 auftritt. Aufgrund von (i) lässt sich dies für alle G_j zu einer Färbung von G_j fortsetzen, wobei alle Ecken w_{6j} die Farbe 1 bekommen. Man kann also b mit 0 und a mit 2 färben.

b) Es liege eine 3-Färbung des Graphen $G = (V, E) = f(I)$ vor. Da a und b durch eine Kante verbunden sind, haben diese Ecken unterschiedliche Farben und wir können daher o.B.d.A. annehmen, dass a mit 2 und b mit 0 gefärbt ist. Es folgt, dass für alle G_j die Voraussetzungen von (ii) vorliegen. Nach (ii) ist also für jede Klausel $C_j = \{\xi_{1j}, \xi_{2j}, \xi_{3j}\}$ mindestens eine Ecke aus C_j mit 1 gefärbt. □



7) NP-schwere Probleme

Ein Entscheidungsproblem D heißt NP-schwer, falls $D' \propto D$ für alle $D' \in NP$ gilt. (Unterschied zu NP-vollst.: Es braucht nicht $D \in NP$ zu gelten.) Außerdem bezeichnet man auch Probleme D, die keine Entscheidungsprobleme, sondern z.B. Optimierungsprobleme sind als NP-schwer, falls gilt: Wenn es einen polynomialen Algorithmus gibt, der D löst, so gibt es für jedes $D' \in NP$ einen pol. Alg. (, d.h., es gilt $P = NP$).

Zwei Optimierungsprobleme, die NP-schwer sind: Das Traveling Salesman Problem (vergl. Steger Seite 77) und das Knapsack Problem (Steger S. 152–154).

8) Turingmaschinen und Random Access Maschinen

Als ein realistisches Modell eines (sequentiell arbeitenden) Computers wird eine RAM (Random Access Machine) angesehen[1]. Im Allgemeinen wird die Zahl der Rechenschritte zur Lösung eines Entscheidungsproblems D sehr viel größer sein, wenn man das Turingmaschinen Modell zugrunde legt, als bei Zugrundelegung des RAM-Modells. Es gilt jedoch: Beide Modelle sind polynomial äquivalent, d.h., die Mengen der in polynomialer Zeit lösbaren Entscheidungsprobleme ist für beide Modelle gleich.

---

1) vergl. etwa K. Mehlhorn, Effiziente Algorithmen, Teubner (1977).

9) Gute Charakterisierungen

Es sei $\mathcal{J}$ eine unendliche Menge, die im Folgenden als zugrunde liegende Menge von Instanzen fest gegeben sei, und $\mathcal{E}$ sei eine Eigenschaft, die sich auf die Elemente von $\mathcal{J}$ bezieht. Wir bezeichnen das zugehörige Entscheidungsproblem mit $D(\mathcal{E}, \mathcal{J})$:

EIGENSCHAFT $\mathcal{E}$ FÜR $\mathcal{J}$ ($D(\mathcal{E}, \mathcal{J})$)

Eingabe: $I \in \mathcal{J}$.

Frage: Hat I die Eigenschaft $\mathcal{E}$?

Eine Eigenschaft $\mathcal{E}$ heißt NP-Eigenschaft, falls $D(\mathcal{E}, \mathcal{J}) \in NP$. Analog: $\mathcal{E}$ wird co-NP-Eigenschaft genannt, falls $D(\mathcal{E}, \mathcal{J}) \in$ co-NP.

Mit $\overline{\mathcal{E}}$ (oder non-$\mathcal{E}$) bezeichnet man die Negation von $\mathcal{E}$, d.h., $\overline{\mathcal{E}}$ ist die Eigenschaft, $\mathcal{E}$ nicht zu besitzen. Die Feststellung „$\mathcal{E}$ ist eine co-NP-Eigenschaft" kann man mit Hilfe von $\overline{\mathcal{E}}$ auch ausdrücken als „$\overline{\mathcal{E}}$ ist eine NP-Eigenschaft".

Eine Charakterisierung einer Eigenschaft $\mathcal{E}$ ist ein Theorem, das feststellt, dass für eine andere Eigenschaft $\tilde{\mathcal{E}}$ und für alle $I \in \mathcal{J}$ gilt: I besitzt $\mathcal{E}$ genau dann, wenn I die Eigenschaft $\tilde{\mathcal{E}}$ hat.

Definition. Es sei $\mathcal{E}$ eine NP-Eigenschaft. Eine Charakterisierung von $\mathcal{E}$, die aussagt, dass $\mathcal{E}$ auch eine co-NP-Eigenschaft ist, nennt man eine gute Charakterisierung ("good characterization") von $\mathcal{E}$.

Dasselbe, nur etwas anders ausgedrückt: Eine gute Charakterisierung stellt von einer gegebenen NP-Eigenschaft $\mathcal{E}$ fest, dass auch $\overline{\mathcal{E}}$ eine NP-Eigenschaft ist.

Beispiele: 1) Der Heiratssatz liefert eine gute Charakterisierung derjenigen bipartiten Graphen $G=(V,E)$ mit zugehöriger Eckenpartition $V=A \dot\cup B$, die ein Matching besitzen, das alle Ecken aus A trifft

2) Der Satz von Kuratowski liefert eine gute Charakterisierung der planaren Graphen. Begründung hierfür: Das zugehörige Entscheidungsproblem lautet

PLANARER GRAPH (PG)
Eingabe: Ein Graph G.
Frage: Ist G planar?

Wir überzeugen uns zunächst davon, dass PG ∈ NP gilt. Zu diesem Zweck nehmen wir an, dass G ein planarer Graph sei, und stellen uns vor, dass wir eine andere Person „schnell" davon überzeugen sollen, dass G tatsächlich planar ist. Das ist einfach: Wir brauchen nur eine Darstellung von G als ebener Graph anzugeben und dann vorzuführen, dass sich in der Tat keine Kanten kreuzen. (Häufig wird dies auch so ausgedrückt: Man „rät" eine Darstellung als ebener Graph und weist dann in polynomialer Zeit nach, dass es sich tatsächlich um eine solche Darstellung handelt.)

Außerdem haben wir zu prüfen, ob auch PG ∈ co-NP gilt. Zu diesem Zweck nehmen wir an, dass G kein planarer Graph ist. Wie können wir nun eine andere Person „schnell" davon überzeugen, dass G tatsächlich nicht planar ist? Der Satz von Kuratowski sagt uns, wie es geht: Aufgrund dieses Satzes wissen wir, dass G eine Unterteilung U des K_5 oder $K_{3,3}$ enthält. Ein solches U präsentieren wir und führen vor, dass U tatsächlich eine Unterteilung von K_5 oder $K_{3,3}$ ist. Dies zeigt, dass der Satz von Kuratowski eine gute Charakterisierung der planaren Graphen ist.

3) Der Satz von Euler (Steger, Seite 79) liefert eine gute Charakterisierung derjenigen zusammenhängenden Graphen, die eine Eulertour enthalten. (Wieso nämlich?)

Die Liste ließe sich verlängern, beispielsweise um ein Entscheidungsproblem über die Existenz von kreuzungsfreien a-b-Pfaden, für das der Satz von Menger eine entsprechende gute Charakterisierung liefert.

Viele bekannte graphentheoretische Sätze haben also die Form von guten Charakterisierungen, d.h., sie zeigen, dass eine bestimmte NP-Eigenschaft $\mathcal{E}$ auch eine co-NP-Eigenschaft ist.

Gänzlich anders ist die Situation jedoch bei Eigenschaften $\mathcal{E}$, für die das zugehörige Entscheidungsproblem $D(\mathcal{E}, \hat{\mathcal{I}})$ ein NP-vollständiges Problem ist: Für kein NP-vollständiges Problem D konnte bislang gezeigt werden, dass $D \in$ co-NP gilt, und es wird allgemein vermutet, dass $D \notin$ co-NP für alle NP-vollständigen Probleme D gilt. Es gilt (ähnlich wie (*) auf Seite E.241):

(**) Gelänge es nur für ein einziges NP-vollständiges Problem D nachzuweisen, dass D in co-NP liegt, so würde daraus NP = co-NP folgen.

Beispiel. Keine gute Charakterisierung (aber natürlich ein interessanter Satz):

Satz (Gallai 1968). Für einen Graphen G gilt $\chi(G) \leq k$ genau dann, wenn sich die Kanten von G so orientieren lassen, dass der entstehende gerichtete Graph keinen gerichteten Pfad mit k Kanten enthält.

Im Zusammenhang mit diesem Beispiel sei darauf hingewiesen, dass das folgende Problem für alle $k \geq 3$ NP-vollständig ist:

k COLORING (kCOL)
Eingabe: Ein Graph G.
Frage: Gilt $\chi(G) \leq k$?

Welche Konsequenzen hat es nun, wenn man von einem Entscheidungsproblem $D(E,J)$ feststellt, dass es NP-vollständig ist?

Antwort: (i) Man kann nicht erwarten, dass man einen polynomialen Algorithmus für dieses Problem findet. (Genauer: Ein polynomialer Algorithmus existiert nur, falls $P = NP$ gilt.) Man muss bei der algorithmischen Behandlung also etwas anderes ins Auge fassen, z.B. Approximationsalgorithmen oder probabilistische Methoden.

(ii) Man kann nicht erwarten, dass man für die Eigenschaft E eine gute Charakterisierung findet. (Genauer: Eine solche existiert nur, falls $NP = co\text{-}NP$ gilt.) Man könnte in diesem Fall beispielsweise versuchen, die Eigenschaft E für eine interessante Teilmenge J' von J nachzuweisen.

15 Ein Hauch von Komplexität und Kryptographie

Aus: L. Lovász, J. Pelikán, K. Vesztergombi, Diskrete Mathematik, Springer-Verlag

15.1 Eine Klasse aus Connecticut an König Arthurs Hof

15.1

Am Hofe von König Arthur[1] wohnten 150 Ritter und 150 Burgfräuleins. Eines Tages entschloss sich der König sie miteinander zu verheiraten. Es zeigte sich jedoch, dass einige Paare einander derartig hassten, dass an eine Heirat zwischen ihnen gar nicht zu denken war! König Arthur versuchte mehrere Male, die Paare anders zusammenzustellen, aber jedes Mal ergaben sich neue Konflikte. Er ließ daher den Zauberer Merlin rufen und befahl ihm, die Paare so zusammenzustellen, dass jeder zu einer Heirat bereit war. Nun, Merlin besaß übernatürliche Kräfte und erkannte daher sofort, dass keine der 150! möglichen Zusammenstellungen brauchbar war. Dies teilte er dem König mit. König Arthur traute ihm aber nicht so recht, da Merlin nicht nur ein großer Zauberer, sondern auch eine etwas zwielichtige Persönlichkeit war. „Finde eine Lösung oder ich verurteile dich dazu, für den Rest Deines Lebens eingesperrt in einer Höhle zu leben!" sagte Arthur.

Merlin hatte das Glück, aufgrund seiner übernatürlichen Kräfte zukünftige wissenschaftliche Literatur durchsehen zu können. Er fand mehrere Artikel des frühen zwanzigsten Jahrhunderts, in denen der *Grund* dafür enthalten war, warum es keine brauchbare Lösung für ihr Problem gab. Mit diesem Wissen kehrte er zum König zurück. Es waren gerade alle Ritter und Damen zugegen und er forderte 56 (bestimmte) Damen auf, sich auf die eine Seite des Königs zu stellen, während 95 Ritter auf die andere Seite gehen sollten. Dann fragte er: „Ist eine von Euch jungen Damen bereit, einen dieser Ritter zu heiraten?" Als alle mit „Nein!" antworteten, sagte Merlin zum König: „Oh König, wie kannst Du von mir verlangen, für jede dieser 56 Damen einen Ehemann unter den verbliebenen 55 Rittern zu finden?" Da erkannte der König, dessen Erziehung und Ausbildung bei Hofe auch das Taubenschlagprinzip umfasst hatte, dass Merlin in diesem Fall die Wahrheit gesagt hat und entließ ihn daher gnädig.

Es verging einige Zeit und der König bemerkte, dass sich seine 150 Ritter beim Abendessen an der berühmten Tafelrunde, häufig mit ihren jeweiligen Nachbarn stritten und manchmal sogar mit ihnen kämpften. Arthur meinte, dies sei schlecht für die Verdauung und ließ Merlin erneut rufen. Er befahl ihm, eine Sitzordnung für die 150 Ritter zu finden, bei der jeder von ihnen zwischen zwei von seinen Freunden sitzen kann. Wie-

[1] Aus L. Lovász and M.D. Plummer: *Matching Theory*, Akadémiai Kiadó, Nord Holland, Budapest, 1986 (mit kleinen Änderungen), mit freundlicher Erlaubnis von Mike Plummer. Der Stoff wurde als 'Handout' an der Yale University, New Haven in Connecticut entwickelt.

derum erkannte Merlin mit Hilfe seiner übernatürlichen Kräfte sofort, dass keine der 150! Sitzordnungen dies erfüllen würde und teilte es dem König mit. Dieser verlangte entweder eine Lösung oder die Erklärung, warum es nicht möglich ist, eine solche zu finden. „Oh, ich wünschte, es gäbe einen einfachen Grund, den ich Euch nennen könnte! Mit ein bisschen Glück gäbe es einen Ritter, der nur einen Freund hat, so dass Ihr ebenfalls sofort erkennt, dass Ihr Unmögliches von mir verlangt. Aber leider (!) gibt es hier keinen solch einfachen Grund und ich kann Euch Sterblichen nicht erklären, warum so eine Sitzordnung nicht existiert, wenn Ihr nicht bereit seid, den Rest Eures Lebens damit zu verbringen, meinen Ausführungen zuzuhören!" Dazu war der König natürlich nicht bereit und daher lebt Merlin seither eingesperrt in einer Höhle. (Eine harte Niederlage der angewandten Mathematik!)

Die Moral dieser Geschichte lautet, dass es Grapheneigenschaften gibt, die einfach nachgewiesen werden können, wenn sie gelten. Enthält der Graph ein perfektes Matching oder einen Hamiltonschen Kreis, kann dies einfach durch Angabe eines solchen „bewiesen" werden. Wenn ein bipartiter Graph *kein* perfektes Matching enthält, dann kann dies „bewiesen" werden, indem eine Teilmenge X der einen Klasse angegeben wird, die weniger als $|X|$ Nachbarn in der anderen Klasse besitzt. Der Leser (und König Arthur) sollten sich Bild 15.1 ansehen. Der Graph auf der linken Seite enthält ein perfektes Matching (durch die dickeren Linien angedeutet), während der Graph auf der rechten Seite keines enthält. Um sich selbst (und den König) davon zu überzeugen, betrachte man die vier schwarzen Punkte und ihre Nachbarn.

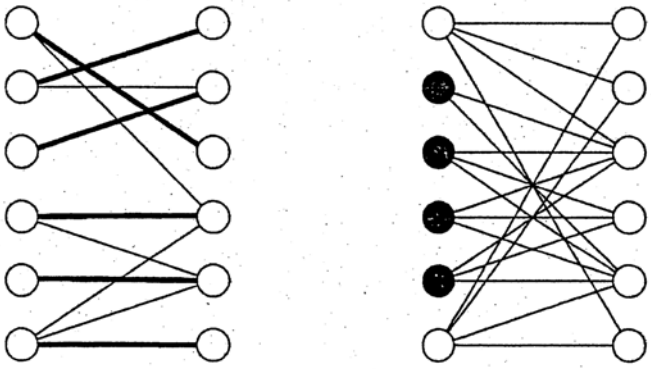


Abbildung 15.1. Ein bipartiter Graph mit einem perfekten Matching und einer ohne.

Die meisten uns interessierenden Eigenschaften in der Graphentheorie weisen diese logische Struktur auf. Ist der Nachweis (Bestätigung, Angabe), dass eine Eigenschaft gilt, einfach, dann wird diese Eigenschaft (in der Sprache der Informatik) eine *NP Eigenschaft* genannt (falls Sie es wirklich wissen möchten, NP ist die Abkürzung für *Non-deterministic Polynomial Time*, aber woher dieser sehr technische Begriff kommt, wäre etwas schwierig zu erklären). Die beiden Problemstellungen, mit denen Merlin konfrontiert worden ist – die Existenz eines perfekten Matchings und die Existenz eines Hamiltonschen Kreises –, sind eindeutig NP Eigenschaften. NP Eigenschaften kommen allerdings auch recht häufig in anderen Bereichen der Mathematik vor. Eine

sehr wichtige NP Eigenschaft bei den natürlichen Zahlen besteht in ihrer *Zusammensetzbarkeit*: Ist eine natürliche Zahl zusammensetzbar, dann kann dies einfach durch Angabe einer Zerlegung $n = ab$ $(a, b > 1)$ dieser Zahl gezeigt werden.

Die bisher gemachten Bemerkungen erklären, wie Merlin auf freiem Fuß bleibt, wenn er Glück hat und die ihm durch König Arthur gestellte Aufgabe eine Lösung besitzt. Nehmen wir beispielsweise an, er wäre in der Lage, eine gute Sitzordnung für die Ritter zu finden. Er könnte König Arthur davon überzeugen, dass sein Sitzplan „gut" ist, indem er fragt, ob irgendjemand neben einem seiner Feinde sitzt (oder einfach wartet, ob das Abendessen friedlich verläuft). Dies zeigt, dass die Eigenschaft des zugehörigen „Freundschaftsgraphen" einen Hamiltonschen Kreis zu enthalten, eine NP Eigenschaft ist. Wieso konnte er, als diese Fragen *keine* Lösungen besaßen, im Fall des Heiratsproblems Arthurs Zorn überstehen, während ihm dies beim Sitzplatzproblem nicht gelang? Worin unterscheidet sich die Nicht-Existenz eines Hamiltonschen Kreises von der Nicht-Existenz eines perfekten Matchings in einem bipartiten Graphen? Die Antwort sollte durch unsere Geschichte bereits klar sein: *Die Nicht-Existenz eines perfekten Matchings in einem bipartiten Graphen ist ebenfalls eine NP Eigenschaft* (dies ist eine der Hauptimplikationen des Heiratssatzes, Satz 10.3.1), während die Nicht-Existenz eines Hamiltonschen Kreises in einem Graphen dies nicht ist! (Um genau zu sein: Für die letzte Aussage ist kein Beweis bekannt, es gibt jedoch sehr deutliche Hinweise dafür.)

Für bestimmte NP Eigenschaften ist die Negation dieser Eigenschaft also wieder eine NP Eigenschaft. Ein Satz, der die Äquivalenz einer NP Eigenschaft mit der Negation einer weiteren NP Eigenschaft feststellt, wird eine *gute Charakterisierung* genannt. Es gibt überall in der Graphentheorie und auch anderswo berühmte gute Charakterisierungen.

Viele NP Eigenschaften sind sogar noch besser. Wenn man Arthur mit dem Heiratsproblem seiner Ritter und Burgfräuleins konfrontiert, kann er (nachdem er zum Beispiel dieses Buch gelesen hat) selbst entscheiden, ob es lösbar ist oder nicht: Er könnte den in Kapitel 10.4 beschriebenen Algorithmus anwenden. Das ist eine Menge Arbeit, aber man kann sie wahrscheinlich mit ganz normalen Personen bewältigen, ohne auf die übernatürlichen Talente von Merlin zurückgreifen zu müssen. Eigenschaften, über die man effizient entscheiden kann, werden Eigenschaften *in der Komplexitätsklasse* P genannt (das P steht hier für *polynomiale Zeit*, eine genaue, aber sehr technische Definition des Ausdrucks „effizient"). Eine Menge anderer in diesem Buch behandelte einfache Eigenschaften eines Graphen, wie der Zusammenhang und die Existenz eines Kreises, gehören ebenfalls dieser Klasse an. Eines unserer Lieblingsprobleme, nämlich die Entscheidung ob eine Zahl eine Primzahl ist oder nicht, gehört auch dazu. Dies wurde kurz bevor dieses Buch in Druck ging gezeigt. (Der in Kapitel 6.10 beschriebene Algorithmus genügt nicht ganz für die Klasse P, da er die zufällige Auswahl der Basis a enthält.)

Die Einführung der Begriffe polynomiale Zeit und NP Eigenschaften signalisierte die Geburtsstunde der modernen Komplexitätstheorie. Begriffe und Paradigmen dieser Theorie sind in weite Teile der Mathematik und ihrer Anwendungen vorgedrungen. Im Folgenden beschreiben wir, wie Ideen aus der Komplexitätstheorie in einer der wichtigsten Bereiche der theoretischen Informatik, nämlich der Kryptographie angewandt werden können.