III. Probleme, die zum Erfüllungsproblem der Aussagenlogik polynomial äquivalent sind

von Peter Schuster

Hier führen wir 12 Sprachen vor, die alle vollständig in NP sind (Def. 4 in II). Damit geben wir einen Teil der Ergebnisse von Karp (1972) wieder. (Bei Resultaten, die nicht von Karp stammen, merken wir den Urheber an (Cook, Lawler, Tarjan)). Die Sprachen stellen vor allem graphentheoretische und kombinatorische Probleme dar.

Aus II, Satz 3 wissen wir, dass E^0 (Def. 5 in II) vollständig in NP ist. Zum Nachweis der Vollständigkeit einer Sprache $S \subset \{0,1\}^*$ genügt es daher, $S \in NP$ und $E^0 \leq_\pi S$ zu zeigen. Allgemeiner können wir aus der Vollständigkeit einer Sprache S', $S' \leq_\pi S$ und $S \in NP$ auf die Vollständigkeit von S schliessen. Den Beweis von $S \in NP$ überlassen wir jeweils dem Leser (man vergleiche dazu die Beweisskizze von Satz 2 in II).

Wir benutzen die in II.2. erklärte Kodierung für aussagenlogische Formeln. Weiter unten führen wir noch Kodierungen für andere mathematische Objekte ein. Wenn einmal eine Kodierung eingeführt ist, wird unsere Sprechweise nicht mehr zwischen dem Objekt und dessen Kodierung unterscheiden.

Anhand der folgenden Sprache SPEZIELLE ERFUELLBARKEIT, die wir aus technischen Gründen hier einführen, wollen wir weitere Konventionen für diesen und die nächsten Vorträge erläutern:

1. Wenn $C_1 \wedge \ldots \wedge C_m$ eine aussagenlogische Formel in den Variablen $x_1,\ldots,x_n$ ist und in KD liegt, jedes der C_i also die Form $y_{i1} \vee \ldots \vee y_{in_i}$ mit $y_{ik} \in \{x_1,\ldots,x_n,\bar{x}_1,\ldots,\bar{x}_n\}$ hat, so setzen wir $OccC_i := \{y_{ik} \mid k \leq n_i\}$ ("Okkurenzmenge"). SPEZIELLE ERFUELLBARKEIT besteht nun aus denjenigen $C_1 \wedge \ldots \wedge C_m \in KD$, für die keine der Disjunktionen C_i eine Aussagenvariable mehrmals enthält ($h \neq k \Longrightarrow (y_{ih} \neq y_{ik} \;\&\; y_{ih} \neq \overline{y_{ik}})$) und in denen zu verschiedenen Indizes Disjunktionen mit verschiedenen Okkurenzmengen gehören ($i \neq j \Longrightarrow OccC_i \neq OccC_j$), und mit der Eigenschaft: $C_1 \wedge \ldots \wedge C_m$ ist erfüllbar.

Diese Sprache SPEZIELLE ERFUELLBARKEIT ist vollständig in NP. (Cook)

Beweis Um $E^0 \leq_\pi$ SPEZIELLE ERFUELLBARKEIT zu zeigen, konstruieren wir ein $f: \{0,1\}^* \longrightarrow \{0,1\}^*$ aus II mit

$(\forall w \in \{0,1\}^*)\quad w \in E^0 \iff f(w) \in$ SPEZIELLE ERFUELLBARKEIT.

Man macht sich leicht klar, dass die Sprache bestehend aus allen Formeln aus KD in P ist (Def. 5 in I). Auf jedem $w \in \{0,1\}^*$, das nicht in dieser Sprache liegt, definieren wir $f(w) = w$ oder irgendwie so, dass $f(w) \notin$ SPEZIELLE ERFUELLBARKEIT ist. Auf den Formeln von KD legen wir f durch die Zuordnung $B_1 \wedge \ldots \wedge B_\ell \longmapsto C_1 \wedge \ldots \wedge C_m$ fest, die entsteht durch:

- Weglassen von $B_i = y_{i1} \vee \ldots \vee y_{in_i}$, falls $y_{ih} = \overline{y_{ik}}$ für ein h,k ist
- Streichen von überflüssigen y_{ik} in den verbleibenden B_i, so dass auch $h \neq k \Longrightarrow y_{ih} \neq y_{ik}$ erreicht wird
- Weglassen von überflüssigen B_i, wenn nämlich mehrere solche (von Anfang an oder infolge Streichungen) die gleiche Okkurenzmenge besitzen.

Nun prüft man leicht $f \in \Pi$ und $w \in E^0 \iff f(w) \in$ SPEZIELLE ERFUELLBARKEIT nach: Es gilt also $E^0 \leq_\pi$ SPEZIELLE ERFUELLBARKEIT.

In dieser Weise werden wir zum Beweis von $S' \leq_\pi S$ für zwei Sprachen S, S' stets verfahren: Die Definition der Sprache S' (hier: E^0) spalten wir in einen ersten, leicht als "polynomial" erkennbaren Teil (hier: "ist Formel aus KD") und einen zweiten Teil (hier: "ist erfüllbar") auf, für den es möglicherweise keinen polynomial beschränkten Algorithmus auf einer TM gibt (Cook'sche Hypothese, II.2). Getrennt werden die beiden Teile der Definition stets durch die feste Wendung "... mit der Eigenschaft ..." oder "... die die Eigenschaft ... haben" (E^0 ist dann also die Sprache aller Formeln $C_1 \wedge \ldots \wedge C_m \in$ KD mit der Eigenschaft: $C_1 \wedge \ldots \wedge C_m$ ist erfüllbar. Man vergleiche auch die obige Aufteilung der Definition von SPEZIELLE ERFUELLBARKEIT.) Das zum Nachweis von $S' \leq_\pi S$ zu konstruierende $f: \{0,1\}^* \longrightarrow \{0,1\}^*$ aus Π werden wir dann nur auf einer Teilmenge von $\{0,1\}^*$ angeben, nämlich auf der Menge, die durch den ersten ("polynomialen") Teil der Definition von S' charakterisiert wird; dies in der stillschweigenden Annahme, dass f auf den restlichen $w \in \{0,1\}^*$ irgendwie so festgelegt wird, dass $f(w) \notin S$. Auch werden wir es stets dem Leser überlassen, $f \in \Pi$ nachzukontrollieren.

Wesentlich in der Definition einer Sprache ist natürlich die Kodierung der mathematischen Objekte (s. oben). Z.B. findet man leicht eine Kodierung von Formeln aus KD (etwa durch Transformation auf disjunkte Normalform), bezüglich der sich Erfüllbarkeit in polynomialer Zeit testen lässt. Andererseits wird der Leser leicht jeweils neue Kodie-

rungen konstruieren können, die ebenfalls vollständige Sprachen liefern.

Die folgenden Sprachen beziehen sich auf graphentheoretische Probleme.

Definition Ein Graph ist ein Paar (P,K), wobei P eine Menge (Punktmenge ist und $K \subset \binom{P}{2}$ (Kantenmenge) ist. $\binom{P}{2}$ = Menge der zweipunktigen Teilmengen von P.) [Die Kante $k = \{p,q\} \in K$ "verbindet" ihre Endpunkte p und q miteinander. p "liegt auf" $k \in K$, wenn $p \in k$.] $S_p := \{k \in K \mid p \in k\}$ ("Stern im Punkt p") ist die Menge aller Kanten von (P,K) mit Endpunkt p. Ein Graph (P',K') heisst Teilgraph von (P,K), wenn $P' \subset P$ und $K' \subset K$.

Die Punktmengen aller im weiteren auftretenden Graphen seien endlich.

Kodierung Der Graph (P,K) mit $P = \{p_1,\ldots,p_{|P|}\}$ wird charakterisiert durch die $|P| \times |P|$-Matrix

$$a_{ij} = \begin{cases} 1 & \text{falls } \{p_i,p_j\} \in K \\ 0 & \text{sonst.} \end{cases}$$

Da im folgenden auch Matrizen mit rationalen Koeffizienten auftreten, definieren wir sogleich die Kodierung solcher Matrizen:

Eine ganze Zahl a kodieren wir als

$$\lambda(a) = d_1 d_1 d_2 d_2 \ldots d_k d_k,$$

wo $d_2 d_3 \ldots d_k$ die Dualdarstellung von a und $d_1 = \begin{cases} 0 & a \leq 0 \\ 1 & a > 0 \end{cases}$ ist. Für eine rationale Zahl a sei $a = b/c$ die eindeutige gekürzte Darstellung mit $b,c \in \mathbb{Z}$, $c>0$. Dann ist die Kodierung von q

$$\lambda(a) = \lambda(b)01\lambda(c).$$

Einen Vektor $(a_1,\ldots,a_n)$ von ganzen oder rationalen Zahlen kodieren wir als

$$\lambda(a_1,\ldots,a_n) = \lambda(a_1)0101\lambda(a_2)0101\ldots\lambda(a_n).$$

Das Paar (A,b), wo $A = (a_{ij})$ eine $m \times n$-Matrix und $b = (b_i)$ ein m-Vektor ist, hat die Kodierung

$$\lambda(A,b) = \lambda(a_{11},\ldots,a_{1n})0101\lambda(a_{21},\ldots,a_{2n}) \ldots$$
$$\ldots 0101\lambda(a_{m1},\ldots,a_{mn})01010101\lambda(b_1,\ldots,b_m).$$

Entsprechend werden wir auch Paare von Matrizen kodieren.

2. Die Sprache CLIQUE ist vollständig (Cook). Sie besteht aus allen Paaren $((P,K),\ell)$, wo (P,K) ein Graph ist, $\ell \in \mathbb{N}$, $|P| \geq \ell$, mit der Eigenschaft: Es existiert eine ℓ-punktige Clique Q in (P,K), d.h.

$$(\exists\, Q \subset P)\ \binom{Q}{2} \subset K \ \&\ |Q| = \ell$$

[ℓ Punkte, die paarweise miteinander verbunden sind.]

Beweis Wir zeigen SPEZIELLE ERFUELLBARKEIT $\leq_\pi$ CLIQUE mit der Zuordnung $C_1 \wedge \ldots \wedge C_m \longmapsto ((P,K),m)$, wo

$$P = \{(y,C_i) \mid 1 \leq i \leq m, y \in \mathrm{Occ}C_i\} \text{ und}$$

$$K = \{\{(y_1,C_i),(y_2,C_j)\} \in \binom{P}{2} \mid i \neq j, y_1 \neq \overline{y_2}, \overline{y_1} \neq y_2\}.$$

[Die Punktmenge des Graphen ist die disjunkte Vereinigung der $\mathrm{Occ}C_i$. Innerhalb eines $\mathrm{Occ}C_i$ werden keine Punkte miteinander verbunden, nach aussen aber alle, die sich nicht widersprechen.]

Wir zeigen, dass $C_1 \wedge \ldots \wedge C_m$ genau dann erfüllbar ist, wenn das zugeordnete $((P,K),\ell)$ in CLIQUE liegt: Sei $C_1 \wedge \ldots \wedge C_m$ erfüllbar. Dann (siehe II.2.) existiert eine Belegung $v: \{x_1,\ldots,x_n\} \longrightarrow \{0,1\}$ und es existiert für jedes $i \leq m$ ein $y_i \in \mathrm{Occ}C_i$ mit $v(y_i) = 1$. Wegen $v(y_i) = 1 = v(y_j) \neq v(\overline{y}_j)$ gilt dann für $\{(y_i,C_i) \mid i \leq m\} \subset P$ $i \neq j \Longrightarrow y_i \neq \overline{y_j}$; in (P,K) ist also $\{(y_i,C_i) \mid i \leq m\}$ eine ℓ-punktige Clique.
Sei umgekehrt Q eine m-punktige Clique in (P,K). Wegen $\{(y,C_i),(y',C_j)\} \in K \Longrightarrow (i \neq j \ \&\ y \neq \overline{y}' \ \&\ \overline{y} \neq y')$ hat dann Q die Gestalt $Q = \{(y_i,C_i) \mid i \leq m\}$ mit $y_i \neq \overline{y_j}$ für alle i und j.

$$v(x_j) := \begin{cases} 1 & \text{für } x_j \in \{y_1,\ldots,y_m\} \\ 0 & \text{sonst} \end{cases}$$

für alle $j \leq n$ definiert eine Belegung, die für jedes $i \leq m$ den Wert 1 auf y_i annimmt, denn für alle $i \leq m$ ist entweder $y_i = x_h$ für ein gewisses $h \leq n$, also $v(y_i) = v(x_h) = 1$, oder $y_i = \overline{x}_h$ für ein gewisses $h \leq n$, also $x_h \notin \{y_1,\ldots,y_m\}$ (da $y_i \neq \overline{y}_j$ für alle j), d.h. $v(x_h) = 0$ und damit ebenfalls $v(y_i) = v(\overline{x}_h) = 1$. Für alle $i \leq m$ existiert also y_i mit $v(y_i) = 1$ und $y_i \in \mathrm{Occ}C_i$, d.h. $v(C_1 \wedge \ldots \wedge C_m) = 1$.

3. Als Korollar hat man die Vollständigkeit der Sprache EINBETTUNG VON GRAPHEN bestehend aus den Paaren von Graphen, $((P',K'),(P,K))$, mit der

Eigenschaft: Es existiert eine Einbettung von (P',K') in (P,K), d.h. es existiert eine injektive Abbildung $e: P' \longrightarrow P$ mit $k \in K' \Longrightarrow e(k) \in K$.

Der Beweis von CLIQUE $\leq_\pi$ EINBETTUNG VON GRAPHEN ist offensichtlich.

Es ist auch klar, dass die Vollständigkeit nicht verletzt wird, wenn man hier $k \in K' \Longrightarrow e(k) \in K$ durch $k \in K' \Longleftrightarrow e(k) \in K$ ersetzt (ISOMORPHIE ZU EINEM UNTERGRAPHEN).

4. Vollständig ist ferner die Sprache DISKRETER UNTERGRAPH. Sie besteht aus allen Paaren $((P',K'),\ell')$ mit einem Graphen (P',K'), $\ell' \in \mathbb{N}$, $|P'| \geq \ell'$ und Eigenschaft: Es gibt eine Menge von ℓ' paarweise unverbundenen Punkten in (P',K').

Beweis Die Reduzierbarkeit CLIQUE $\leq_\pi$ DISKRETER UNTERGRAPH sieht man unmittelbar anhand der Zuordnung

$$((P,K),\ell) \longmapsto ((P,\tbinom{P}{2} \setminus K),\ell).$$

[Genau die Punkte verbinden, die in (P,K) unverbunden.]

Die folgende Sprache behandelt ein kombinatorisches Problem. Daher zunächst eine Bemerkung zur Kodierung von Mengenfamilien. Sei I endlich und $\bigcup_{i \in I} M_i = \{x_1,\ldots,x_n\}$. Die $|I| \times n$-Matrix

$$a_{ij} := \begin{cases} 1 & \text{für } x_j \in M_i \\ 0 & \text{sonst} \end{cases}$$

beschreibt die Mengenfamilie $(M_i)_{i \in I}$. Diese, sowie das Paar $((M_i)_{i \in I},\ell)$ kodieren wir, wie oben ausgeführt.

5. Die Sprache TEILPARTITION ist vollständig. Sie besteht aus allen Paaren $((M_i)_{i \in I},\ell)$, wo $(M_i)_{i \in I}$ eine endliche Familie von lauter endlichen Mengen M_i, $\ell \in \mathbb{N}$ und $|I| \geq \ell$, ist, mit der Eigenschaft: Es existieren ℓ paarweise disjunkte Mengen unter den M_i.

Beweis Mit der Zuordnung $((P',K')\ell') \longmapsto ((S_p)_{p\in P'},\ell')$ zeigt man unmittelbar DISKRETER UNTERGRAPH $\leq_\pi$ TEILPARTITION, da p und q genau dann unverbunden sind, wenn ihre Sterne disjunkt sind, $S_p \cap S_q = \emptyset$. (Natürlich kann sehr wohl $S_p = S_q$ für $p \neq q$ sein.)

6. Ebenfalls vollständig ist die Sprache STERNUEBERDECKUNG, zu der genau die Paare $((P,K),\ell)$ gehören mit (P,K) Graph, $\ell \in \mathbb{N}$, $|P| \geq \ell$, und mit der Eigenschaft:

$$(\exists Q \subset P)\ |Q| \leq \ell \ \&\ \bigcup_{p\in Q} S_p = K.$$

[Jeder Punkt von P ist mit mindestens einem Punkt von Q verbunden.]

Beweis $((P',K'),\ell') \longmapsto ((P',K'),|P'|-\ell')$ liefert DISKRETER UNTERGRAPH $\leq_\pi$ STERNUEBERDECKUNG, denn die Punkte von $Q \subset P'$ sind genau dann paarweise unverbunden, wenn $\bigcup_{p\in P'\setminus Q} S_p = K$.

Einige der nächsten Sprachen beschäftigen sich mit Digraphen (gerichteten Graphen):

Definition Ein Digraph ist ein Paar (V,A), wo V eine Menge ist und $A \subset V^2 \setminus \{(v,v) \mid v \in V\}$. Die Elemente von V heissen Punkte, die von A Pfeile.
[Der Pfeil (u,v) zeigt von u nach v.]

Wieder werden alle vorkommenden Digraphen endlich sein.

Kodierung Sei $V = \{u_1,\ldots,u_{|V|}\}$. Dann beschreibt die $|V| \times |V|$-Matrix

$$a_{ij} := \begin{cases} 1 & \text{für } (u_i,u_j) \in A \\ 0 & \text{sonst} \end{cases}$$

den Digraphen (V,A).

7. Die Sprache HAMILTON-ZYKLUS ist vollständig. (Lawler) Sie besteht aus allen Digraphen (V,A) mit der Eigenschaft: Es existiert ein Hamilton-Zyklus in (V,A), d.h.: Wenn $|V| > 1$, existiert eine auf V surjektive Folge $(v_1,\ldots,v_{|V|})$ mit:

$$i < |V| \Longrightarrow (v_i, v_{i+1}) \in A \quad \text{und}$$

$$(v_{|V|}, v_1) \in A.$$

[Ein geschlossener Pfad, der - in Pfeilrichtung - jeden Punkt von (V,A) genau einmal durchläuft.]

Beweis (Vereinfacht von M. Fürer) Wir zeigen STERNUEBERDECKUNG $\leq_\pi$ HAMILTON-ZYKLUS mit der Zuordnung $((P,K), (P,K),\ell) \mapsto (V,A)$, wo

$$V = \{1,\ldots,\ell\} \cup \{(p,q) \mid \{p,q\} \in K\}$$

(die $i \leq \ell$ nennen wir Zahl-Punkte, die (p,q) Kanten-Punkte) und

$$A = \{((p,q),(q,p')) \mid \{p,q\} \in K, \{q,p'\} \in K, p \leq p'\}$$

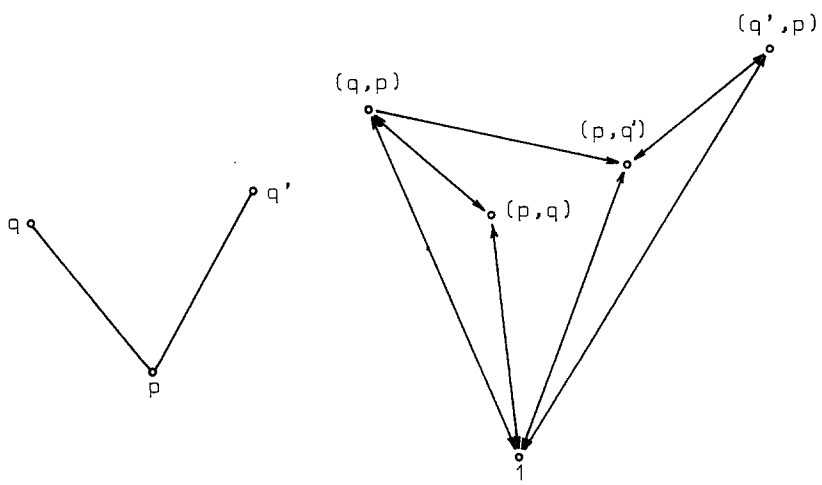
$$\cup \{(i,(p,q)) \mid \{p,q\} \in K, i \leq \ell\}$$

$$\cup \{((p,q),i) \mid \{p,q\} \in K, i \leq \ell\}$$

$$\cup \{(i,i+1) \mid i < \ell\} \cup \{(\ell,1)\}$$

für eine beliebige, fest gewählte Totalordnung $\leq$ auf P.

Beispiel $(q<q', \ell=1)$



Sei nun $Q \subset P$ gegeben mit $|Q| \leq \ell$, $\bigcup_{p \in Q} S_p = K$. Wir zählen K nach den Mengen S_p geordnet (injektiv) auf:

$$(\{p_1,q_1^1\}, \{p_1,q_1^2\},\ldots,\{p_1,q_1^{n_1}\}, \{p_2,q_2^1\},\ldots,\{p_i,q_i^j\}\ldots\{p_m,q_m^{n_m}\}),$$

so dass also $p_i \in Q$, $\sum_{i=1}^{m} n_i = |K|$ und so dass $q_i^j < q_i^{j+1}$.

(Die Menge $S_i := \{\{p_i,q_i^1\},\ldots,\{p_i,q_i^{n_i}\}\}$ ist also Teilmenge von S_{p_i}.)

Dann ist folgendes offenbar ein Hamilton-Zyklus in (V,A):

$$(1,(p_1,q_1^1), (q_1^1,p_1), (p_1,q_1^2), (q_1^2,p_1),\ldots,(p_1,q_1^{n_1}), (q_1^{n_1},p_1),$$

$$2,(p_2,q_2^1), (q_2^1,p_2),\ldots$$

$$\ldots\ldots$$

$$m, (p_m,q_m^1),\ldots \quad ,(q_m^{n_m},p_m), m+1,m+2,\ldots,\ell)$$

[Zwischen den Zahl-Punkten i und i+1 besucht der Hamilton-Zyklus genau die zu S_i gehörenden Kantenpunkte]

Sei umgekehrt $(v_1,\ldots,v_{|V|})$ ein Hamilton-Zyklus in (V,A). Für $1 \leq i \leq j \leq |V|$ nennen wir $(v_i,v_{i+1},\ldots,v_j)$ und auch $(v_j,v_{j+1},\ldots,v_{|V|},v_1,v_2,\ldots,v_i)$ Abschnitt des Hamilton-Zyklus $(v_1,\ldots,v_{|V|})$.

Definiere $Q = \{p \in P \mid \exists$ Zahlpunkt $i \in V$ und $\exists\, q \in P$ so dass $(i,(p,q))$ Abschnitt des Hamilton-Zyklus ist$\}$.

Behauptung 1: Für alle $\{p,q\} \in K$ gilt:
Falls $((q,p),(p,q))$ kein Abschnitt des Hamilton-Zyklus ist, so gilt $p \in Q$.

Wähle zu festem p das kleinste q', so dass $\{p,q'\} \in K$ und $((q',p),(p,q'))$ kein Abschnitt des Hamilton-Zyklus ist.

Für jedes q" mit $\{p,q"\} \in K$ und $q"<q'$ ist also $((q",p),(p,q"))$ ein Abschnitt und folglich $((q",p),(p,q'))$ kein Abschnitt des Hamilton-Zyklus. Im Abschnitt $(v,(p,q'))$ muss deshalb v ein Zahlpunkt sein, also $p \in Q$.

Behauptung 2: Q bildet eine höchstens ℓ-punktige Sternüberdeckung von (P,K), d.h.

1. $|Q| \leq \ell$
2. $\bigcup_{p \in Q} S_p = K$

1. Ist klar, da es nur ℓ Zahlpunkte gibt.
2. Weil $((q,p),(p,q))$ und $((p,q),(q,p))$ nicht beides Abschnitte des Hamilton-Zyklus sein können, so liegt nach Behauptung 1 p oder q in Q, also liegt die Kante $\{p,q\}$ in S_p oder in S_q.

8. Die Sprache HAMILTON-KREIS ist vollständig (Tarjan). Sie besteht aus allen Graphen (P,K) mit der Eigenschaft: Es existiert ein Hamilton-Kreis in (P,K), d.h. entweder $|P| \leq 1$ oder es existiert eine surjektive Folge $(p_1,\ldots,p_{|P|})$ in P mit:

$$i < |P| \Longrightarrow \{p_i,p_{i+1}\} \in K \quad \text{und}$$

$$\{p_{|P|},p_1\} \in K.$$

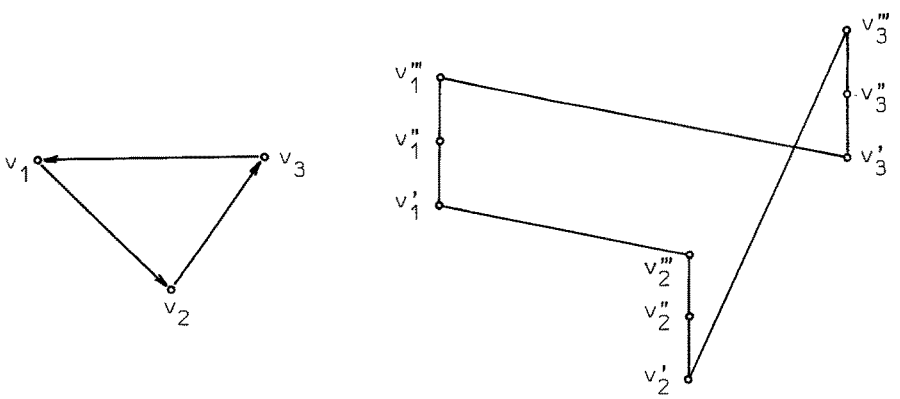
[Ein geschlossener Pfad, der jeden Punkt des (ungerichteten) Graphen (P,K) genau einmal besucht.]

Beweis Wir zeigen: HAMILTON-ZYKLUS $\leq_\pi$ HAMILTON-KREIS mit der Zuordnung $(V,A) \mapsto (P,K)$, wo

$$P = V \times \{',",'''\} \text{ und}$$

$$K = \{\{v',v"\} \mid v \in V\}$$
$$\cup \{\{v",v'''\} \mid v \in V\}$$
$$\cup \{\{v_o',v_1'''\} \mid (v_o,v_1) \in A\}.$$

Beispiel



Wenn $(v_1,v_2,\ldots,v_n)$ ein Hamilton-Zyklus in (V,A) ist, dann ist $(v_1''',v_1",v_1',v_2''',\ldots,v_n''',v_n",v_n')$ ein Hamilton-Kreis in (P,K).

Ist umgekehrt $(p_1,\ldots,p_{|P|})$ ein Hamilton-Kreis in (P,K), so steht darin jedes v_i'' immer zwischen v_i' und v_i''', da v_i'' mit keinen weiteren Punkten verbunden ist.
O.B.d.A. können wir annehmen: $p_1 = v_1'''$, $p_2 = v_1''$. Der Hamilton-Kreis $(p_1,\ldots,p_{|P|})$ hat dann die Form $(v_1''',v_1'',v_1',v_2''',v_2',\ldots,v_n''',v_n'',v_n')$. Dann ist aber auch $(v_1,\ldots,v_n)$ ein Hamilton-Zyklus in (V,A).

9. Hiermit sieht man leicht, dass TRAVELLING SALESMAN vollständig in NP ist: Dies ist die Sprache aller Paare $((x_{p,q})_{\substack{p\in P\\ q\in P}},k)$, wo $k\in\mathbb{N}$ und für alle $p,q\in P$ $x_{p,q} = x_{q,p}\in\mathbb{N}$ sowie $x_{p,p} = 0$ gilt, mit der Eigenschaft: Es existiert eine zyklische Permutation π von P, so dass

$$\sum_{p\in P} x_{p,\pi(p)} \leq k.$$

[Ist $x_{p,q}$ die Entfernung zwischen den Punkten p und q, so legt man beim Durchlaufen aller Punkte von P in der Reihenfolge des Zyklus π die Entfernung $\sum_{p\in P} x_{p,\pi(p)}$ zurück.]
HAMILTON-KREIS transformiert sich auf TRAVELLING SALESMAN durch die Zuordnung $(P,K) \longmapsto ((x_{p,q})_{\substack{p\in P\\ q\in P}}, 0)$ mit

$$x_{p,q} = \begin{cases} 0 & \{p,q\}\in K \\ 1 & \text{sonst.} \end{cases}$$

10. Auch die Sprache UNGERICHTETER HAMILTON-PFAD ist vollständig. Sie enthält genau die Graphen (P',K'), die die Eigenschaft haben: Es existiert ein Hamilton-Pfad in (P',K'), d.h. es existiert eine auf P' surjektive Folge $(p_1,\ldots,p_{|P|})$ mit:

$$i < |P'| \Longrightarrow \{p_i,p_{i+1}\}\in K'.$$

[Ein Pfad, der jeden Punkt von (P',K') genau einmal besucht.]

Zum Beweis von HAMILTON-KREIS $\leq_\pi$ UNGERICHTETER HAMILTON-PFAD wählen wir ein beliebiges $q\in P$ und ein festes Symbol q'.
O.B.d.A. $\{q',0,1\}\cap P = \emptyset$. Wir definieren die Zuordnung $(P,K) \longmapsto (P',K')$ so:

$$P' = P \cup \{q',0,1\}$$
$$K' = K \cup \{\{q',p\} \mid \{q,p\}\in K\} \cup \{\{0,q\},\{1,q'\}\}$$

Ein Hamilton-Kreis in (P,K) hat dann einen Abschnitt $(q,p_1,\ldots,p_n,q)$, und damit gibt es in (P',K') den Hamilton-Pfad $(0,q,p_1,\ldots,p_n,q',1)$. Umgekehrt hat jeder Hamilton-Pfad in (P',K') die Gestalt $(0,q,p_1,\ldots,p_n,q',1)$ oder $(1,q',p_n,\ldots,p_1,q,0)$ (denn durch 0 und 1 geht nur je eine Kante) und damit ist $(q,p_1,\ldots,p_n)$ ein Hamilton-Kreis in (P,K).

11. GERICHTETER HAMILTON-PFAD ist vollständig: Das ist die Menge aller Digraphen (V,A) mit der Eigenschaft: Es existiert ein Hamilton-Pfad in (V,A), d.h. es existiert eine auf V surjektive Folge $(v_1,\ldots,v_{|V|})$ mit:

$$i < |V| \Longrightarrow (v_i,v_{i+1}) \in A.$$

[Ein in Pfeilrichtung zu durchlaufender Pfad, der jeden Punkt von (V,A) genau einmal besucht.]

Beweis Wir zeigen:

UNGERICHTETER HAMILTON-PFAD $\leq$ GERICHTETER HAMILTON-PFAD

durch die Zuordnung $(P,K) \longmapsto (V,A)$ mit

$V = P$ und

$A = \{(p,q) \mid \{p,q\} \in K\}$

Jeder ungerichtete Hamilton-Pfad ist auch ein gerichteter Hamilton-Pfad und umgekehrt.

12. Die folgende Sprache ERFUELLBARKEIT MIT HOECHSTENS 3 VARIABLEN PRO KLAUSEL wird beweistechnische Vorteile in Vortrag IV erbringen. Besonders interessant ist die Vollständigkeit dieser Sprache aber im Vergleich mit der Tatsache, dass die Sprache ERFUELLBARKEIT MIT HOECHSTENS 2 VARIABLEN PRO KLAUSEL in P liegt. (Cook 1971 (?); Definition von P: I, Def. 5).

Die Sprache ERFUELLBARKEIT MIT HOECHSTENS 3 VARIABLEN PRO KLAUSEL ist definiert als die Menge aller aussagenlogischen Formeln
$C_1 \wedge \ldots \wedge C_m \in KD$ in den Variablen $x_1,\ldots,x_n$, so dass
$C_i = y_{i1} \vee \ldots \vee y_{in_i}$, $y_{ij} \in \{x_1,\ldots,x_n,\bar{x}_1,\ldots,\bar{x}_n\}$ und $n_i \leq 3$ für alle $i \leq m$, und die die Eigenschaft haben, erfüllbar zu sein.
Sie ist vollständig.

Zum Beweis von $E^0 \leq_\pi$ ERFUELLBARKEIT MIT HOECHSTENS 3 VARIABLEN PRO KLAUSEL definieren wir die Abbildung f in Schritten auf $B_1 \wedge \ldots \wedge B_\ell \in KD$.

1. Schritt: Sei $B_i = z_{i1} \vee \ldots \vee z_{ik_i}$, $z_{ij} \in \{x_1,\ldots,x_k,\bar{x}_1,\ldots,\bar{x}_k\}$ für jedes $i \leq \ell$ und sei i_o das kleinste der $i \leq \ell$, für die $k_i > 3$ ist. Dann ordnen wir $B_1 \wedge \ldots \wedge B_\ell$ die Formel $B_1^1 \wedge \ldots \wedge B_{\ell+1}^1$ über der neuen Variablenmenge $\{x_1,\ldots,x_k,u_1\}$ zu mit:

$$B_i^1 = B_i \quad \text{für} \quad i \notin \{i_o, \ell+1\}$$

$$B_{i_o}^1 = z_{i_o 1} \vee z_{i_o 2} \vee u_1$$

$$B_{\ell+1}^1 = z_{i_o 3} \vee \ldots \vee z_{i_o k_{i_o}} \vee \bar{u}_1.$$

Im 2. Schritt wenden wir dieses Zuordnungsverfahren auf $B_1^1 \wedge \ldots \wedge B_{\ell+1}^1$ an und erhalten $B_1^2 \wedge \ldots \wedge B_{\ell+2}^2$. Iteration führt offensichtlich in $\sum_{\substack{i \leq \ell \\ k_i \geq 3}} (k_i - 3)$ Schritten zu einer Formel $C_1 \wedge \ldots \wedge C_m$ mit höchstens 3 Variablen pro Klausel C_i.

$B_1 \wedge \ldots \wedge B_\ell$ ist genau dann erfüllbar, wenn $C_1 \wedge \ldots \wedge C_m$ es ist. Es genügt zu zeigen:

$$B_1 \wedge \ldots \wedge B_\ell \text{ erfüllbar} \Longleftrightarrow B_1^1 \wedge \ldots \wedge B_{\ell+1}^1 \text{ erfüllbar:}$$

Wenn nun $v(B_1 \wedge \ldots \wedge B_\ell) = 1$ ist, so gilt für die Belegung $v^1: \{x_1,\ldots,x_k,u_1\} \to \{0,1\}$ mit $v^1(x_i) = v(x_i)$ für alle $i \leq k$ und

$$v^1(u_1) = \begin{cases} 0 & \text{falls } v(z_{i_o 1}) = 1 \text{ oder } v(z_{i_o 2}) = 1 \\ 1 & \text{sonst} \end{cases}$$

offenbar $v^1(B_1^1 \wedge \ldots \wedge B_{\ell+1}^1) = 1$, und wenn umgekehrt $v^1(B_1^1 \wedge \ldots \wedge B_{\ell+1}^1) = 1$ ist, so haben wir für die Restriktion v von v^1 auf $\{x_1,\ldots,x_k\}$ gerade $v(B_1 \wedge \ldots \wedge B_\ell) = 1$.

Selbstverständlich ist auch ERFUELLBARKEIT MIT HOECHSTENS k VARIABLEN PRO KLAUSEL für $k \geq 3$ vollständig.

Von der folgenden wichtigen Sprache ISOMORPHIE VON GRAPHEN, die eine Teilmenge der vollständigen Sprache EINBETTUNG VON GRAPHEN (III.3.) ist, ist nicht bekannt, ob sie auch vollständig ist: ISOMORPHIE VON GRAPHEN besteht aus allen Paaren $((P',K'),(P,K))$ von Graphen mit der Eigenschaft: (P',K') ist isomorph zu (P,K), d.h. es existiert eine Bijektion $f: P' \to P$ mit $k \in K' \Longleftrightarrow f(k) \in K$.

Literatur

Karp, R.M., Reducibility among combinatorial problems, IBM Symposiu
1972: Complexity of Computer Computations, Plenum Press, New
York, 1972.