Hiermit haben wir gezeigt, dass

PERFECT-BIPARTITE-MATCHING

$= \{ \langle G \rangle : G = (V,E)$ bipartit und G besitzt perfekten Matching $\} \in RP$.

[Wir wissen natürlich aus OR, dass dieses Problem $\in P$ liegt, aber dieser prob. Algo ist 1. sehr einfach, 2. auf allg. Graphen leicht übertragbar (Stichwort: Pfaffsche Determinante), 3. sehr gut parallelisierbar].

fehlt noch:

<u>Bew.:</u> (Schwartz-Zippel)

<u>zu zeigen:</u> Anzahl von $(\alpha_1, \dots, \alpha_m) \in S^m$ mit $p(\alpha_1, \dots, \alpha_m) = 0$ ist $\leq d\,|S|^{m-1}$

Bew. per Induktion nach m.

<u>$m = 1$:</u> p ist univariat und hat höchstens d Nullstellen.

<u>$m > 1$:</u> Ang. Unbestimmte x_1 kommt in einem

Monom von p vor [falls nicht, benenne Variablen um].

Dann schreibe

$$p(x_1, \dots, x_m) = \sum_{i=0}^{k} x_1^k \, p_i(x_2, \dots, x_m),$$

wobei k der größte in p vorkommende Exponent von x_1 ist.

Sei $\alpha_1, \dots, \alpha_m$ mit $p(\alpha_1, \dots, \alpha_m) = 0$.

<u>1. Fall</u> $p_k(\alpha_2, \dots, \alpha_m) = 0$

$p_k \neq 0$ und hat Grad $\leq d-k$. Nach I.V. gibt es höchstens $(d-k)|S|^{m-2}$ viele mögliche Wahlen für $\alpha_2, \dots, \alpha_m$. Also höchstens $(d-k)|S|^{m-1}$ viele mögliche Wahlen für $\alpha_1, \dots, \alpha_m$

<u>2. Fall</u> $p_k(\alpha_2, \dots, \alpha_m) \neq 0$.

Es gibt $|S|^{m-1}$ viele mögliche Wahlen für $\alpha_2, \dots, \alpha_m$.

Falls $\alpha_2, \dots, \alpha_m$ fest gewählt sind mit $p_k(\alpha_2, \dots, \alpha_m) \neq 0$, dann ist α_1 eine Nullstelle des univariaten Polynoms $p(x_1, \alpha_2, \dots, \alpha_m)$. Dieses Polynom hat Grad k, also gibt es im 2 Fall höchstens $k \cdot |S|^{m-1}$ viele mögliche Wahlen für $\alpha_1, \dots, \alpha_m$. <u>Zusammen</u>: $\leq (d-k)|S|^{m-1} + k|S|^{m-1}$
$= d|S|^{m-1}$. $\boxtimes$

§2 Die Polynomielle Hierarchie

Haben gesehen: $P \subseteq RP$, $P, RP, coRP \subseteq BPP$,
$P, RP \subseteq NP$, $coRP \subseteq coNP$, ...

<u>Ziel</u>: Inklusionen strukturiert untersuchen.

<u>Def</u>: (Klasse Σ_2^P)
Sei $L \subseteq \Sigma^*$. Dann ist $L \in \Sigma_2^P$, falls es ein Polynom p und eine pzb TM M gibt, so dass für jedes $x \in \Sigma^*$ gilt:

$$x \in L \iff \exists u \in \Sigma^{p(|x|)} \forall v \in \Sigma^{p(|x|)} : M(x,u,v) = 1.$$

<u>Bsp</u>: Variante von

$$INDSET = \{\langle G,k\rangle : G = (V,E) \text{ hat unabh. Menge } M \subseteq V \text{ mit } |M| \geq k\}$$

Jetzt: Bestimme die exakte Größe der größten unabh. Menge in G:

$$EXACT\text{-}INDSET = \{\langle G,k\rangle : \text{Die größte unabh. Menge in } G \text{ hat Größe } k\}$$

<u>Also</u>: $\langle G,k\rangle \in EXACT\text{-}INDSET \iff \exists$ Menge M, $|M| = k$, $\forall$ Mengen $N \subseteq V$ mit $|N| \geq k+1$: M unabh., N nicht.

<u>Beobachtung</u>: Es ist nicht klar, ob es ein pzb Zertifikat für die Mitgliedschaft in EXACT-INDSET geben kann.

<u>Bsp</u>: Finde die kürzeste Formel, die äquivalent zu einer gegebenen Formel ist. Als Entscheidungsproblem formuliert:

$$\text{MIN-EQ-KNF} = \{ \langle \varphi, k \rangle : \exists \text{ KNF-Formel } \psi \text{ der Länge} \leq k, \text{ die äquivalent zu } \varphi \text{ ist.} \}$$

Also: $\langle \varphi, k \rangle \in \text{MIN-EQ-KNF} \Leftrightarrow \exists\, \psi$ KNF, $|\psi| \leq k$ $\forall$ Belegungen u gilt $\psi(u) = \varphi(u)$.

Wieder ist nicht klar, wie ein pzb Zertifikat aussehen könnte.

Umgekehrt kann man auch nach "minimalen" Formeln fragen:

$$\overline{\text{MIN-EQ-KNF}} = \{ \langle \varphi, k \rangle : \forall \text{ KNF-Formeln } \psi \text{ der Länge} \leq k \ \exists \text{ Belegung } u \text{ mit } \psi(u) \neq \varphi(u) \}$$

Auch hier gibt es kein offensichtliches pzb Zertifikat.

<u>Def</u>: (Klassen Σ_i^P, Π_i^P, PH)

Sei $L \subseteq \Sigma^*$. Dann ist $L \in \Sigma_i^P$, falls es ein Polynom p und eine pzb TM M gibt, so dass

für jedes $x \in \Sigma^*$ gilt:

$$x \in L \iff \exists u_1 \in \Sigma^{p(|x|)} \forall u_2 \in \Sigma^{p(|x|)} \dots Q_i\, u_i \in \Sigma^{p(|x|)} : M(x, u_1, \dots, u_i) = 1,$$

wobei $Q_i \in \{\forall, \exists\}$ davon abhängt, ob i gerade oder ungerade ist.

Definiere weiter $\Pi_i^P = co\Sigma_i^P = \{\overline{L} : L \in \Sigma_i^P\}$ und

$$PH = \bigcup_{i \geq 1} \Sigma_i^P .$$

<u>Beobachtung</u>:

- $\Sigma_1^P = NP$, $\Pi_1^P = coNP$
- $\Sigma_i^P \subseteq \Pi_{i+1}^P \subseteq \Sigma_{i+2}^P \implies PH = \bigcup_{i \geq 1} \Pi_i^P$

Die verschiedenen Komplexitätsklassen haben also folgende Struktur zueinander: