$P \neq NP \Rightarrow$ MAX 3-SAT $\notin$ PTAS :

Sei A NP-vollständig.

PCP-Thm: $(r(n), q)$-beschränkter Verifikator für A

mit $r(n) = O(\log n)$, $q > 2$ konst.
$\leq c \log n$

Geg. $x \in \Sigma^*$, konstruiere 3-CNF-Formel $F(x)$ mit m Klauseln
so dass:

$x \in \Sigma_A \rightsquigarrow F(x)$ erfüllbar

$x \notin \Sigma_A \rightarrow$ höchstens $(1-\varepsilon)\cdot m$ der m Klauseln in $F(x)$ erfüllbar.

für konst. $\varepsilon > 0$.

Lückentechnik $\rightarrow$ MAX-3-SAT $\notin$ PTAS.

Für jedes Bit im Beweis π eine Variable.

$\rightsquigarrow 2^{r(n)} \cdot q \leq q \cdot n^c$.

Für Zufallsbits ρ: $v_{\rho,1} \dots v_{\rho,q}$ Variablen zu Bits, die V bei ρ fragt.

$A_\rho \subseteq \{0,1\}^q = \{(v_{\rho,1}, \dots, v_{\rho,q}) : V$ akzeptiert $\}$.

$$F_\rho = \bigwedge_{(\varepsilon_1 \dots \varepsilon_q) \in A_\rho} v_{\rho,1}^{\varepsilon_1} \vee \dots \vee v_{\rho,q}^{\varepsilon_q}$$

erfüllt wenn Wahl nicht in A_ρ.

$$F(x) = \bigwedge_{\rho \in \{0,1\}^{r(n)}} F_\rho$$

$$|F(x)| \leq 2^{r(n)} \cdot 2^q \cdot q \leq 2^q \cdot n^c .$$

$x \in L \rightsquigarrow$ V akzeptiert für alle $p \in \{0,1\}^{r(n)}$ für ein π

$\rightsquigarrow$ $F(x)$ erfüllbar. ✓

$x \notin L \rightsquigarrow$ Für jeden π gibt es $2^{r(n)-1}$ Zufallsstr. p s.d. V zurückweist.

$\rightsquigarrow$ in F_p mindestens eine Klausel unerfüllt.

$\rightsquigarrow$ $2^{r(n)-1} / 2^{q+r(n)} = 1/2^{q+1}$ Anteil

der Klauseln unerfüllt für jedes π. □

$\frac{m}{m(\delta)} \leq \frac{1}{a_k}$

$\frac{m(\delta)}{m} \geq a_n^n$

MAX-CLIQUE:

Sei A r-Approx.-Alg. für MAX-Clique.

Aus $G = (V, E)$ baue neuen Graphen G'
s.d. $A(G')$ liefert brauchbare Lösung für G.

$G^k := (V^k, E^{(k)})$ wobei $|G^k| = |G|^k$.

$\{(v_1 \dots v_k)(w_1 \dots w_k)\} \in E^{(k)}$ falls
$\forall i \quad v_i = w_i$ oder $\{v_i, w_i\} \in E$.

C Clique in G $\rightsquigarrow$ C^k Clique in G^k
$|C^k| = |C|^k$.

Also $\omega^*(G^k) \geq (\omega^*(G))^k$.

Sei C' Clique in G^k mit $|C'| \geq m^k$.

$C_i' := \{v \in V,$ es gibt $u_1 \dots u_{i-1}, v_{i+1} \dots v_k$
mit $(u_1 \dots u_{i-1} v v_{i+1} \dots v_k) \in C'\}$

Für $i = 1 \dots k$ ist C_i' Clique in G.
für mindestens ein $i = 1 \dots k$ ist $|C_i'| \geq m$.

Also: aus Clique C' in G^k berechnet man
Clique C'' in G der Größe $|C''| \geq |C'|^{1/k}$.

$C'' := g(C')$

Performanz:

$$\frac{m^*(G)}{m(G, g(A(G^k)))} \leq \left(\frac{m^*(G^k)}{m(G^k, A(G^k))} \right)^{1/k} \leq r^{1/k}$$

PTAS: gewünschte Performance r'

$\rightsquigarrow$ Problem für $k \geq \frac{\log r'}{\log r}$

$$r^{\frac{\log r'}{\log r}} = 2^{\log r \cdot \frac{\log r'}{\log r}} = 2^{\log r'} = r'$$

Also: MAX CLIQUE $\in$ APX

$\rightarrow$ MAX-CLIQUE $\in$ PTAS $\rightarrow$ P = NP

analog für MAX IND. SET

□

Beweis des PCP-Theorems

V_1 mit $r_1(n) = d \cdot \log n$ $\quad q_1(n) = \log^k n$

Komposition (V_1, V_1):

$r_2 = d \log n + d \cdot \log(c \cdot \log^k n) = O(\log n) = c$

$q_2 = \log^k(c \cdot \log^k n) = (\log \log n)^{O(1)}$

V_1

V_3 $\quad r_3(n) = n^k$ $\quad q_3(n) = d$

Komposition (V_2, V_3):

$r_4 = c \log n + \left(c \cdot (\log \log n)^{k'}\right)^k$

V_4 $\quad = O(\log n)$

$q_4 = d$

□

Hier nur Beweis von (1.): $\boxed{NP \subseteq PCP(O(n^3), O(1))}$.

1. Arithmetisierung der Formeln.

F in 3-CNF $\rightsquigarrow$ P_F Polynom 5. Grades !

Arithmetisierung erzeugt die FAP

bleibt: x so modifizieren, dass

$$P_F(x) \neq 0$$

mit wenigen Anfragen getestet werden kann

Codierung durch lineare Funktionen

$$p(x_1 \dots x_n) = \alpha_p + \sum_{i \in I_{p,1}} x_i + \sum_{(i,j) \in I_{p,2}} x_i x_j + \dots \sum_{(i,j,k) \in I_{p,3}} x_i x_j x_k$$

α_p konstanter Term

$I_{p,1} = \{ i ; x_i \text{ monom in } p \}$ ...

$I_{p,2} = \{ (i,j) ; x_i x_j \text{ binom in } p \}$ ...

$$p(\vec{a}) = \alpha_p + \sum_{i \in I_{p,1}} a_i + \sum_{(i,j) \in I_{p,2}} a_i a_j + \sum_{(i,j,k) \in I_{p,3}} a_i a_j a_k$$

Allg.

$$A_a := \sum_{i=1}^{n} a_i \gamma_i \qquad q_{p,1}(i) = \begin{cases} 0 & i \notin I_{p,1} \\ 1 & i \in I_{p,1} \end{cases}$$

$$B_a := \sum_{i=1}^{n} \sum_{j=1}^{n} a_i a_j \gamma_{ij} \qquad q_{p,2}[i,j] = \begin{cases} 1 & (i,j) \in I_{p,2} \\ 0 & \text{sonst} \end{cases}$$

$$C_a := \sum_{i=1}^{n} \sum_{j=1}^{n} \sum_{k=1}^{n} a_i a_j a_k \gamma_{ijk} \qquad q_{p,3}[i,j,k] = \begin{cases} 1 & (i,j,k) \in I_{p,3} \\ 0 & \text{sonst} \end{cases}$$

$\rightsquigarrow$ $p(\vec{a}) = \alpha_p + A_a(q_{p,1}) + B_a(q_{p,2}) + C_a(q_{p,3})$

berechnet wird von $p(a)$ mit 3 Queries in A_a, B_a, C_a

a erfüllt F $\rightarrow$ $p_F^i(a) = 0$ für alle i

$\rightarrow$ a erfüllt als A_a, B_a, C_a kann mit 3 Queries gepüft werden

f verstellbar a Bereich

A_a, B_a, C_a mit hoher W'keit zurückgewiesen.

Aber: muss für jede Parameter zurückgewiesen werden, auch solche die nicht von der Form sind !!

~ Linearitätstest $(\delta < \frac{1}{2})$

Sei $f(x) =: b \in \mathbb{Z}_2$ s.d.

$$\Pr_y [g(x+y) - g(y) = b] \geq \frac{1}{2}$$

① f, g sind δ-nah:

Sei $\Pr_x [f(x) \neq g(x)] > \delta$

i. $\forall x$ $\Pr_y [f(x) = g(x+y) - g(y)] \geq \frac{1}{2}$ per Def.

also $\Pr_{x,y} [g(x+y) - g(y) \neq g(x)] > \frac{\delta}{2}$ ↯ zur Annahme.

② f ist linear

Sei $a \in \mathbb{Z}_2^n$. $p_a := \Pr_x [f(a) = g(x+a) - g(x)] \geq 1-\delta$

nach Def. $p_a \geq \frac{1}{2}$.

Nach Vorr.: $\Pr_{x,y} [g(x+a+y) \neq g(x+a) + g(y)] \leq \delta/2$

$\Pr_{x,y} [g(x+y+a) \neq g(x) + g(y+a)] \leq \delta/2$

$\rightsquigarrow$ $\Pr_{x,y} [g(x+a) + g(y) = g(x) + g(y+a)] \geq 1-\delta$

□

Problem: g δ-nah zu f linear.
wollen $f(x)$ berechnen aber Orakel für g.
$f(x) \neq g(x)$ für wenige x ⇝ nutzt nichts

Lösung: wähle y zufällig, berechne
$$g(x+y) - g(y).$$
(komplexwertig nehmen!)

Beweis: zz.: $\forall x \; Pr_y[g(x+y)-g(y) \neq f(x)] \leq 2\delta$

y, $x+y$ beide gleichverteilt auf $\mathbb{Z}_2^m$
⇝ $Pr_y[g(y) \neq f(y)] \leq \delta$
& $Pr_y[g(x+y) \neq f(x+y)] \leq \delta$) wg. δ-Nähe!

⇝ $Pr_y[g(x+y) - g(y) \neq \underbrace{f(x+y)+f(y)}_{=f(x) \text{ wg. Linearität}}] \leq 2\delta$

Können testen, ob A, B, C durch zu linearen Fkt. A', B', C'.

Frage: sind A', B', C' von der Form

$A' = A_a \cdot a$ $B' = B_a = a \cdot a$, $C' = C_a \cdot a \cdot a \cdot a$

für ein $a \in \mathbb{Z}_2^n$

→ Konsistenztest. (k-mal wiederholen für ein $k(\delta)$). ⇒ Übung

f. $\delta < 1/2F$

es gibt k konst. so d.p

→ A', B', C' nicht konsistent → zurückgeben

bei k-facher Wdh. mit W'keit $1-\delta$.

→ Verifikator

1. Linearitätstest
2. Konsistenztest
3. wähle $\vec{r}$ zufällig $p := P_F^{\vec{r}}$.

berechne q_{p1} q_{p2} q_{p3}

$v := \alpha_p + A(q_{p1}) + B(q_{p2}) + C(q_{p3})$

if $v = 0$ accept else reject

F erfüllbar → $a \vdash F$ → A_a, B_a, C_a richtig abgelehnt

F unerfüllbar → jedes A, B, C:

erfüllt nicht linear → mit hoher W'keit im Lin.-test

nicht konsistent → mit hoh W'k. im Konsistenztest

sonst $A = A_a$, $B = B_a$, $C = C_a$

dann $a \not\vdash F$, also mit W'keit $1/2$ zurückgewiesen !

Zufallsbit. $O(n)$ für $\bar{r}$ $= O(n^2)$

für jede Berechnung in Linearität & Konsistenzcheck $\rightsquigarrow$ konstant $* O(n^2)$ □.

Anzahl der Orakelfragen = konstant (sehr groß).

$\rightsquigarrow$ $SAT \in PCP[O(n^2), O(1)]$ □

Running Example

$$F = (x_1 \vee \bar{x}_3 \vee \bar{x}_4) \wedge (\bar{x}_1 \vee x_2 \vee \bar{x}_4) \wedge (x_2 \vee x_3 \vee \bar{x}_4)$$

$$r_1[(1-x_1)x_3x_4] + r_2[x_1(1-x_2)x_4] + r_3[(1-x_2)(1-x_3)x_4]$$

$F = (1,1,1) \Rightarrow$ ~~x_3x_4~~ $+ x_1x_3x_4 + \underline{x_1x_4} + x_1x_2x_4 + \underline{x_4} + \underline{x_2x_4} + x_2x_3 + x_2x_3x_4$

$$x_4 + x_1x_4 + x_2x_4 + x_1x_2x_4 + x_1x_3x_4 + x_2x_3x_4$$

r	p_F^r	$p_F^r(1,0,0,1)$
0 0 0	0	0
0 0 1	$x_4 + x_2x_4 + x_3x_4 + x_2x_3x_4$	1
0 1 0	$x_1x_4 + x_1x_2x_4$	1
0 1 1	$x_4 + x_1x_4 + x_2x_4 + x_3x_4 + x_1x_3x_4 + x_2x_3x_4$	0
1 0 0	$x_3x_4 + x_1x_3x_4$	0
1 0 1	$x_4 + x_2x_4 + x_1x_3x_4 + x_2x_3x_4$	1
1 1 0	$x_1x_4 + x_3x_4 + x_1x_2x_4 + x_1x_3x_4$	1
1 1 1	5.0	0

$(0001) \notin F \rightsquigarrow p_F^r(0001) = 1$

$(1001) \notin F \rightsquigarrow p_F^r(1001) = 0$ } for $r = 111$

$p = p_F^r$ $\qquad \alpha_p = 0$

$I_{p,1} = \{4\}$ $\qquad q_{p,1} = 0001$

$I_{p,2} = \{(1,4), (2,4)\}$ $\qquad q_{p,2} = 0001000100000000$

$I_{p,3} = \{(1,2,4), (1,3,4), (2,3,4)\}$

$a = (1,0,0,1)$

$A_a = y_1 + y_4$ $\qquad A_a(q_{p,1}) = 1$

$B_a = y_{14} + y_{41} + y_{44} + y_{44}$

$B_c(q_{1,2}) = 1$

$C_c = y_{111} + y_{114} + y_{141} + y_{144} + y_{411} + y_{414} + y_{441} + y_{444}$

$C_a(q_{p,3}) = a_1 a_1 a_4 + a_1 a_3 a_4 + a_2 a_3 a_4 = 0$

$\Rightarrow \quad p_F^{\Gamma}(a) = 0 + 1 + 1 + 0 = 0$ $\qquad \square$

03