Complexidade computacional

Classifica os problemas em relação à dificuldade de resolvê-los algoritmicamente.

CLRS 34

Classes P e NP

Por algoritmo eficiente entende-se um algoritmo polinomial.

Classes P e NP

Por algoritmo eficiente entende-se um algoritmo polinomial.

Classe P:

classe de todos os problemas de decisão que podem ser resolvidos por algoritmos polinomiais.

Classes P e NP

Por algoritmo eficiente entende-se um algoritmo polinomial.

Classe P:

classe de todos os problemas de decisão que podem ser resolvidos por algoritmos polinomiais.

Classe NP:

classe de todos os problemas de decisão que possuem um verificador polinomial para a resposta SIM

Verificador polinomial para sim

Um verificador polinomial para a resposta SIM a um problema Π é um algoritmo polinomial ALG que recebe uma instância I de Π e um objeto C, tal que $\langle C \rangle$ é $\operatorname{O}(\langle I \rangle^{\alpha})$ para alguma constante α

Verificador polinomial para sim

```
Um verificador polinomial para a resposta SIM a um problema \Pi é um algoritmo polinomial ALG que recebe uma instância I de \Pi e um objeto C, tal que \langle C \rangle é O(\langle I \rangle^{\alpha}) para alguma constante \alpha e devolve SIM para algum C se a resposta a \Pi(I) é SIM; NÃO para todo C se a resposta a \Pi(I) é NÃO.
```

Verificador polinomial para sim

```
Um verificador polinomial para a resposta SIM a um problema \Pi é um algoritmo polinomial ALG que recebe uma instância I de \Pi e um objeto C, tal que \langle C \rangle é O(\langle I \rangle^{\alpha}) para alguma constante \alpha
```

e devolve

```
SIM para algum C se a resposta a \Pi(I) é SIM;
NÃO para todo C se a resposta a \Pi(I) é NÃO.
```

No caso de resposta SIM, o objeto C é dito um certificado polinomial ou certificado curto da resposta SIM a $\Pi(I)$.

$P \neq NP$?

É crença de muitos que a classe NP é maior que a classe P, ainda que isso não tenha sido provado até agora.

Este é o intrigante problema matemático conhecido pelo rótulo " $P \neq NP$?"

Não confunda NP com "não-polinomial".

Classe co-NP

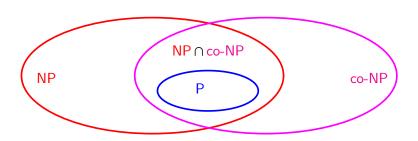
A classe co-NP é definida trocando-se SIM por NÃO na definição de NP.

Um problema de decisão Π está em co-NP se admite um certificado polinomial para a resposta NÃO.

Os problemas em $NP \cap co-NP$ admitem certificados polinomiais para as respostas $SIM \in N\~AO$.

Em particular, $P \subseteq NP \cap co-NP$.

P, NP e co-NP



 $P \neq NP$?

 $NP \cap co-NP \neq P$?

 $NP \neq co-NP$?

Classes P, NP e co-NP

Classe P:

classe de todos os problemas de decisão que podem ser resolvidos por algoritmos polinomiais.

Classe NP:

classe de todos os problemas de decisão que possuem um verificador polinomial para a resposta SIM

Classe co-NP:

classe de todos os problemas de decisão que possuem um verificador polinomial para a resposta NÃO

Permite comparar

o "grau de complexidade" de problemas diferentes.

Permite comparar o "grau de complexidade" de problemas diferentes.

 Π , Π' : problemas

Uma redução de Π a Π' é um algoritmo ALG que resolve Π usando uma subrotina hipotética ALG' que resolve Π' ,

Permite comparar o "grau de complexidade" de problemas diferentes.

 Π , Π' : problemas

Uma redução de Π a Π' é um algoritmo ALG que resolve Π usando uma subrotina hipotética ALG' que resolve Π' , de forma que, se ALG' é um algoritmo polinomial, então ALG é um algoritmo polinomial.

Permite comparar o "grau de complexidade" de problemas diferentes.

 Π , Π' : problemas

Uma redução de Π a Π' é um algoritmo ALG que resolve Π usando uma subrotina hipotética ALG' que resolve Π' , de forma que, se ALG' é um algoritmo polinomial, então ALG é um algoritmo polinomial.

 $\Pi \prec_P \Pi' = \text{ existe uma redução de } \Pi \text{ a } \Pi'.$

Se $\Pi \prec_P \Pi'$ e Π' está em P, então Π está em P.

 Π = encontrar um ciclo hamiltoniano

 Π' = existe um ciclo hamiltoniano?

 Π = encontrar um ciclo hamiltoniano

 Π' = existe um ciclo hamiltoniano?

Redução de Π a Π' :

Suponha que ALG' é um algoritmo que resolve Π' .

 Π = encontrar um ciclo hamiltoniano

 Π' = existe um ciclo hamiltoniano?

Redução de Π a Π' :

Suponha que ALG' é um algoritmo que resolve Π' .

Como você poderia resolver Π usando ALG'?

 Π = encontrar um ciclo hamiltoniano

 Π' = existe um ciclo hamiltoniano?

Redução de Π a Π':

Suponha que ALG' é um algoritmo que resolve Π' .

Como você poderia resolver Π usando ALG'?

Ideias?

 Π = encontrar um ciclo hamiltoniano

 Π' = existe um ciclo hamiltoniano?

Redução de Π a Π' :

Suponha que ALG' é um algoritmo que resolve Π' .

Como você poderia resolver Π usando ALG'?

Ideias?

Se posso decidir se um grafo tem ou não um ciclo hamiltoniano, o que posso fazer para, dado um grafo G, encontrar um ciclo hamiltoniano em G?

 Π = encontrar um ciclo hamiltoniano

 Π' = existe um ciclo hamiltoniano?

Redução de Π a Π' :

Suponha que ALG' é um algoritmo que resolve Π' .

Como você poderia resolver Π usando ALG'?

Ideias?

Se posso decidir se um grafo tem ou não um ciclo hamiltoniano, o que posso fazer para, dado um grafo G, encontrar um ciclo hamiltoniano em G?

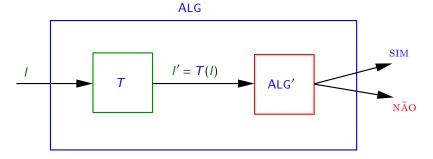
Como posso descobrir as arestas de algum ciclo hamiltoniano de G?

```
\Pi = encontrar um ciclo hamiltoniano
\Pi' = existe um ciclo hamiltoniano?
Redução de \Pi a \Pi': ALG' é um algoritmo que resolve \Pi'.
     ALG(G)
        se ALG'(G) = N\tilde{A}O
            então devolva "G não é hamiltoniano"
        para cada aresta uv de G faça
            H \leftarrow G - uv
            se ALG'(H) = SIM
                então G \leftarrow G - \mu\nu
     6
        devolva G
```

```
\Pi = encontrar um ciclo hamiltoniano
\Pi' = existe um ciclo hamiltoniano?
Redução de \Pi a \Pi': ALG' é um algoritmo que resolve \Pi'.
     ALG(G)
        se ALG'(G) = N\tilde{A}O
             então devolva "G não é hamiltoniano"
        para cada aresta uv de G faça
            H \leftarrow G - \mu \nu
            se ALG'(H) = SIM
                então G \leftarrow G - \mu\nu
     6
         devolva G
Se ALG' consome tempo O(p(n)),
```

então ALG consome tempo $O(m p(\langle G \rangle))$, onde m = número de arestas de G.

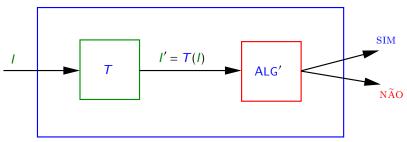
Esquema comum de redução



Faz apenas uma chamada ao algoritmo ALG'.

Esquema comum de redução





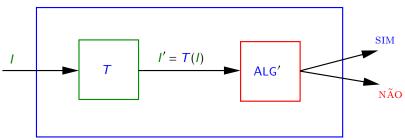
Faz apenas uma chamada ao algoritmo ALG'.

T transforma uma instância I de Π em uma instância I' = T(I) de Π' tal que

$$\Pi(I) = \text{SIM se e somente se } \Pi'(I') = \text{SIM}$$

Esquema comum de redução





Faz apenas uma chamada ao algoritmo ALG'.

T transforma uma instância I de Π em uma instância I' = T(I) de Π' tal que

$$\Pi(I) = \text{SIM}$$
 se e somente se $\Pi'(I') = \text{SIM}$

T é uma espécie de "filtro" ou "compilador".

Problema: Dada uma fórmula booleana ϕ nas variáveis x_1, \dots, x_n , existe uma atribuição

$$t: \{x_1, \dots, x_n\} \to \{\text{VERDADE}, \text{FALSO}\}$$

que torna ϕ verdadeira?

Problema: Dada uma fórmula booleana ϕ nas variáveis x_1, \dots, x_n , existe uma atribuição

$$t: \{x_1, \dots, x_n\} \rightarrow \{\text{VERDADE}, \text{FALSO}\}\$$

que torna ϕ verdadeira?

Exemplo:

$$\phi = (x_1) \land (\neg x_1 \lor \neg x_2 \lor x_3) \land (\neg x_3)$$

Problema: Dada uma fórmula booleana ϕ nas variáveis x_1, \dots, x_n , existe uma atribuição

$$t: \{x_1, \dots, x_n\} \rightarrow \{\text{VERDADE}, \text{FALSO}\}$$

que torna ϕ verdadeira?

Exemplo:

$$\phi = (x_1) \land (\neg x_1 \lor \neg x_2 \lor x_3) \land (\neg x_3)$$

Se $t(x_1) = \text{VERDADE}$, $t(x_2) = \text{FALSO}$, $t(x_3) = \text{FALSO}$, então $t(\phi) = \text{VERDADE}$.

Problema: Dada uma fórmula booleana ϕ nas variáveis x_1, \dots, x_n , existe uma atribuição

$$t: \{x_1, \dots, x_n\} \rightarrow \{\text{VERDADE}, \text{FALSO}\}$$

que torna ϕ verdadeira?

Exemplo:

$$\phi = (x_1) \land (\neg x_1 \lor \neg x_2 \lor x_3) \land (\neg x_3)$$

Se $t(x_1) = \text{VERDADE}$, $t(x_2) = \text{FALSO}$, $t(x_3) = \text{FALSO}$, então $t(\phi) = \text{VERDADE}$.

Se $t(x_1)$ = VERDADE, $t(x_2)$ = VERDADE, $t(x_3)$ = FALSO, então $t(\phi)$ = FALSO.

Sistemas lineares 0-1

Problema: Dados uma matriz A e um vetor b,

$$Ax \geq b$$

possui uma solução tal que $x_i = 0$ ou $x_i = 1$ para todo i?

Sistemas lineares 0-1

Problema: Dados uma matriz A e um vetor b,

$$Ax \geq b$$

possui uma solução tal que $x_i = 0$ ou $x_i = 1$ para todo i?

Exemplo:

$$x_1$$
 ≥ 1
- x_1 - x_2 + x_3 ≥ -1
- x_3 ≥ 0

tem uma solução 0-1?

Sistemas lineares 0-1

Problema: Dados uma matriz A e um vetor b,

$$Ax \geq b$$

possui uma solução tal que $x_i = 0$ ou $x_i = 1$ para todo i?

Exemplo:

$$x_1$$
 ≥ 1
- x_1 - x_2 + x_3 ≥ -1
- x_3 ≥ 0

tem uma solução 0-1?

Sim! $x_1 = 1$, $x_2 = 0$ e $x_3 = 0$ é solução.

Satisfatibilidade <*P* Sistemas lineares 0-1

Satisfatibilidade $\langle P \rangle$ Sistemas lineares 0-1

A transformação deve receber uma fórmula booleana ϕ e devolver um sistema linear $Ax \ge b$ tal que ϕ é satisfatível se e somente se o sistema $Ax \ge b$ admite uma solução 0-1.

Satisfatibilidade <*P* Sistemas lineares 0-1

A transformação deve receber uma fórmula booleana ϕ

e devolver um sistema linear $Ax \ge b$

tal que ϕ é satisfatível se e somente se o sistema $Ax \ge b$ admite uma solução 0-1.

Exemplo:

$$\phi = (x_1) \land (\neg x_1 \lor \neg x_2 \lor x_3) \land (\neg x_3)$$

Como fazer um sistema que tem solução sse ϕ é satisfatível?

Satisfatibilidade <*P* Sistemas lineares 0-1

A transformação deve receber uma fórmula booleana ϕ

e devolver um sistema linear $Ax \ge b$

tal que ϕ é satisfatível se e somente se o sistema $Ax \ge b$ admite uma solução 0-1.

Exemplo:

$$\phi = (x_1) \land (\neg x_1 \lor \neg x_2 \lor x_3) \land (\neg x_3)$$

Como fazer um sistema que tem solução sse ϕ é satisfatível?

Quem podem ser as variáveis do sistema?

Satisfatibilidade <*P* Sistemas lineares 0-1

A transformação deve receber uma fórmula booleana ϕ

e devolver um sistema linear $Ax \ge b$

tal que ϕ é satisfatível se e somente se o sistema $Ax \ge b$ admite uma solução 0-1.

Exemplo:

$$\phi = (x_1) \land (\neg x_1 \lor \neg x_2 \lor x_3) \land (\neg x_3)$$

Como fazer um sistema que tem solução sse ϕ é satisfatível?

Quem podem ser as variáveis do sistema?

E quais seriam as restrições?

Satisfatibilidade <*P* Sistemas lineares 0-1

A transformação deve receber uma fórmula booleana ϕ

e devolver um sistema linear $Ax \ge b$

tal que ϕ é satisfatível se e somente se o sistema $Ax \ge b$ admite uma solução 0-1.

Exemplo:

$$\phi = (x_1) \land (\neg x_1 \lor \neg x_2 \lor x_3) \land (\neg x_3)$$

Como fazer um sistema que tem solução sse ϕ é satisfatível?

Quem podem ser as variáveis do sistema?

E quais seriam as restrições?

Ideias?

Satisfatibilidade <*P* Sistemas lineares 0-1

A transformação T recebe uma fórmula booleana ϕ

e devolve um sistema linear $Ax \ge b$

tal que ϕ é satisfatível se e somente se o sistema $Ax \ge b$ admite uma solução 0-1.

Exemplo:

$$\phi = (x_1) \land (\neg x_1 \lor \neg x_2 \lor x_3) \land (\neg x_3)$$

Satisfatibilidade <*P* Sistemas lineares 0-1

A transformação ${\cal T}$ recebe uma fórmula booleana ϕ

- e devolve um sistema linear $Ax \ge b$
- tal que ϕ é satisfatível se e somente se o sistema $Ax \ge b$ admite uma solução 0-1.

Exemplo:

$$\phi = (x_1) \land (\neg x_1 \lor \neg x_2 \lor x_3) \land (\neg x_3)$$

Satisfatibilidade \prec_P Sistemas lineares 0-1

A transformação ${\cal T}$ recebe uma fórmula booleana ϕ

e devolve um sistema linear $Ax \ge b$

tal que ϕ é satisfatível se e somente se o sistema $Ax \ge b$ admite uma solução 0-1.

Exemplo:

$$\phi = (x_1) \land (\neg x_1 \lor \neg x_2 \lor x_3) \land (\neg x_3)$$

Verifique que

Caminho hamiltoniano entre u e $v \prec_P$ Caminho hamiltoniano

Verifique que

Caminho hamiltoniano entre u e $v \prec_P$ Caminho hamiltoniano

Verifique que

Ciclo hamiltoniano \prec_P Caminho hamiltoniano entre u e v

Caminho hamiltoniano \prec_P Satisfatibilidade

Descreveremos um algoritmo polinomial T que recebe um grafo G e devolve uma fórmula booleana $\phi(G)$ tal que

G tem caminho hamiltoniano $\Leftrightarrow \phi(G)$ é satisfatível.

Caminho hamiltoniano <p Satisfatibilidade

Descreveremos um algoritmo polinomial T que recebe um grafo G e devolve uma fórmula booleana $\phi(G)$ tal que

G tem caminho hamiltoniano $\Leftrightarrow \phi(G)$ é satisfatível.

Suponha que G tem vértices $1, \ldots, n$.

Caminho hamiltoniano <p Satisfatibilidade

Descreveremos um algoritmo polinomial T que recebe um grafo G e devolve uma fórmula booleana $\phi(G)$ tal que

G tem caminho hamiltoniano $\Leftrightarrow \phi(G)$ é satisfatível.

Suponha que G tem vértices $1, \ldots, n$.

 $\phi(G)$ tem n^2 variáveis $x_{i,j}$, $1 \le i,j \le n$.

Caminho hamiltoniano <p Satisfatibilidade

Descreveremos um algoritmo polinomial T que recebe um grafo G e devolve uma fórmula booleana $\phi(G)$ tal que

G tem caminho hamiltoniano $\Leftrightarrow \phi(G)$ é satisfatível.

Suponha que G tem vértices $1, \ldots, n$.

 $\phi(G)$ tem n^2 variáveis $x_{i,j}$, $1 \le i,j \le n$.

Interpretação: $x_{i,j} = \text{VERDADE} \Leftrightarrow \text{vértice } j \text{ é o } i\text{-ésimo}$ vértice do caminho.

Claúsulas de $\phi(G)$:

vértice j faz parte do caminho:

$$(x_{1,j} \lor x_{2,j} \lor \cdots \lor x_{n,j})$$

para cada j (n claúsulas).

Claúsulas de $\phi(G)$:

vértice j faz parte do caminho:

$$(x_{1,j} \lor x_{2,j} \lor \cdots \lor x_{n,j})$$
 para cada j (n claúsulas).

vértice j não está em duas posições do caminho:

$$(\neg x_{\pmb{i},\pmb{j}} \vee \neg x_{\pmb{k},\pmb{j}})$$

para cada $j \in i \neq k$ (O(n^3) claúsulas).

Claúsulas de $\phi(G)$:

vértice j faz parte do caminho:

$$(x_{1,j} \lor x_{2,j} \lor \cdots \lor x_{n,j})$$
 para cada j (n claúsulas).

vértice j não está em duas posições do caminho:

$$(\neg x_{i,j} \lor \neg x_{k,j})$$

para cada j e $i \neq k$ (O(n^3) claúsulas).

algum vértice é o i-ésimo do caminho:

$$(x_{i,1} \vee x_{i,2} \vee \cdots \vee x_{i,n})$$

para cada i (n claúsulas).

Mais claúsulas de $\phi(G)$:

dois vértices não podem ser o i-ésimo:

$$(\neg x_{i,j} \lor \neg x_{i,k})$$

para cada $i \in j \neq k$ (O(n^3) claúsulas).

Mais claúsulas de $\phi(G)$:

▶ dois vértices não podem ser o *i*-ésimo:

$$(\neg x_{i,j} \lor \neg x_{i,k})$$

para cada $i \in j \neq k$ (O(n^3) claúsulas).

▶ se ij não é aresta, j não pode seguir i no caminho:

$$(\neg x_{k,i} \lor \neg x_{k+1,j})$$

para cada ij que não é aresta $(O(n^3)$ claúsulas).

Mais claúsulas de $\phi(G)$:

dois vértices não podem ser o i-ésimo:

$$(\neg x_{i,j} \lor \neg x_{i,k})$$

para cada $i \in j \neq k$ (O(n^3) claúsulas).

▶ se *ij* não é aresta, *j* não pode seguir *i* no caminho:

$$(\neg x_{k,i} \lor \neg x_{k+1,j})$$

para cada ij que não é aresta $(O(n^3)$ claúsulas).

A fórmula $\phi(G)$ tem $O(n^3)$ claúsulas e cada claúsula tem $\leq n$ literais. Logo, $\langle \phi(G) \rangle$ é $O(n^4)$.

Mais claúsulas de $\phi(G)$:

▶ dois vértices não podem ser o *i*-ésimo:

$$(\neg x_{i,j} \lor \neg x_{i,k})$$

para cada $i \in j \neq k$ (O(n^3) claúsulas).

▶ se *ij* não é aresta, *j* não pode seguir *i* no caminho:

$$(\neg x_{k,i} \lor \neg x_{k+1,j})$$

para cada ij que não é aresta $(O(n^3)$ claúsulas).

A fórmula $\phi(G)$ tem $O(n^3)$ claúsulas e cada claúsula tem $\leq n$ literais. Logo, $\langle \phi(G) \rangle$ é $O(n^4)$.

Não é difícil projetar o algoritmo polinomial T.

 $\phi(G)$ satisfatível $\Rightarrow G$ tem caminho hamiltoniano.

Prova: Seja $t: \{\text{variáveis}\} \rightarrow \{\text{VERDADE}, \text{FALSO}\}\$ tal que $t(\phi(G)) = \text{VERDADE}.$

 $\phi(G)$ satisfatível $\Rightarrow G$ tem caminho hamiltoniano.

```
Prova: Seja t: \{\text{variáveis}\} \rightarrow \{\text{VERDADE}, \text{FALSO}\}\ tal que t(\phi(G)) = \text{VERDADE}.
```

Para cada *i*, existe um único *j* tal que $t(x_{i,j}) = VERDADE$.

 $\phi(G)$ satisfatível $\Rightarrow G$ tem caminho hamiltoniano.

Prova: Seja $t: \{\text{variáveis}\} \rightarrow \{\text{VERDADE}, \text{FALSO}\}\$ tal que $t(\phi(G)) = \text{VERDADE}.$

Para cada i, existe um único j tal que $t(x_{j,j}) = \text{VERDADE}$. Logo, t é a codificação de uma permutação

$$\pi(1), \pi(2), \ldots, \pi(n)$$

dos vértices de G, onde

$$\pi(i) = j \Leftrightarrow t(x_{i,j}) = \text{VERDADE}.$$

 $\phi(G)$ satisfatível $\Rightarrow G$ tem caminho hamiltoniano.

Prova: Seja $t: \{\text{variáveis}\} \rightarrow \{\text{VERDADE}, \text{FALSO}\}\$ tal que $t(\phi(G)) = \text{VERDADE}.$

Para cada i, existe um único j tal que $t(x_{i,j}) = \text{VERDADE}$. Logo, t é a codificação de uma permutação

$$\pi(1), \pi(2), \ldots, \pi(n)$$

dos vértices de G, onde

$$\pi(i) = j \Leftrightarrow t(x_{i,j}) = \text{VERDADE}.$$

Para cada k, $(\pi(k), \pi(k+1))$ é uma aresta de G.

 $\phi(G)$ satisfatível $\Rightarrow G$ tem caminho hamiltoniano.

Prova: Seja $t: \{\text{variáveis}\} \rightarrow \{\text{VERDADE}, \text{FALSO}\}\$ tal que $t(\phi(G)) = \text{VERDADE}.$

Para cada i, existe um único j tal que $t(x_{j,j}) = \text{VERDADE}$. Logo, t é a codificação de uma permutação

$$\pi(1), \pi(2), \ldots, \pi(n)$$

dos vértices de G, onde

$$\pi(i) = j \Leftrightarrow t(x_{i,j}) = \text{VERDADE}.$$

Para cada k, $(\pi(k), \pi(k+1))$ é uma aresta de G.

Logo, $(\pi(1), \pi(2), \dots, \pi(n))$ é um caminho hamiltoniano.

G tem caminho hamiltoniano $\Rightarrow \phi(G)$ satisfatível.

Suponha que $(\pi(1), \pi(2), \dots, \pi(n))$ é um caminho hamiltoniano, onde π é uma permutação dos vértices de G.

G tem caminho hamiltoniano $\Rightarrow \phi(G)$ satisfatível.

Suponha que $(\pi(1), \pi(2), \dots, \pi(n))$ é um caminho hamiltoniano, onde π é uma permutação dos vértices de G.

Então

$$t(x_{i,j}) = \text{VERDADE se } \pi(i) = j \text{ e}$$

 $t(x_{i,j}) = \text{FALSO se } \pi(i) \neq j,$

é uma atribuição de valores que satisfaz todas as claúsulas de $\phi(G)$.

Um problema Π em NP é NP-completo se cada problema em NP pode ser reduzido a Π .

Um problema Π em NP é NP-completo se cada problema em NP pode ser reduzido a Π .

Teorema de S. Cook e L.A. Levin: Satisfatibilidade é NP-completo.

Um problema Π em NP é NP-completo se cada problema em NP pode ser reduzido a Π .

Teorema de S. Cook e L.A. Levin: Satisfatibilidade é NP-completo.

Se $\Pi \prec_P \Pi'$ e Π é NP-completo, então

Um problema Π em NP é NP-completo se cada problema em NP pode ser reduzido a Π .

Teorema de S. Cook e L.A. Levin: Satisfatibilidade é NP-completo.

Se $\Pi \prec_P \Pi'$ e Π é NP-completo, então Π' é NP-completo.

Um problema Π em NP é NP-completo se cada problema em NP pode ser reduzido a Π .

Teorema de S. Cook e L.A. Levin: Satisfatibilidade é NP-completo.

Se $\Pi \prec_P \Pi'$ e Π é NP-completo, então Π' é NP-completo.

Existe um algoritmo polinomial para um problema NP-completo se e somente se P = NP.