Fundamental Computer Science
Lecture 3: first steps in complexity
Reductions

Denis Trystram
MoSIG1 and M1Info – University Grenoble-Alpes

February, 2021
Agenda

- Reduction
- Goal: to classify the problems in complexity classes
- A focus on randomized algorithms
- (if enough time): The class NP-complete (Cook’s Theorem)
Reductions

Definition

A function \( f : \Sigma^* \rightarrow \Sigma^* \) is called \textit{polynomial time computable} if there is a polynomially bounded Turing Machine that computes it.

A language \( A \) is polynomial time reducible to language \( B \), denoted \( A \leq_P B \), if there is a polynomial time computable function \( f : \Sigma^* \rightarrow \Sigma^* \), where for every input \( w \), it holds that \( w \in A \iff f(w) \in B \). This function \( f \) is called a \textit{polynomial time reduction} from \( A \) to \( B \).
A function $f : \Sigma^* \rightarrow \Sigma^*$ is called \textit{polynomial time computable} if there is a polynomially bounded Turing Machine that computes it.

A language $A$ is \textit{polynomial time reducible} to language $B$, denoted $A \leq_P B$, if there is a polynomial time computable function $f : \Sigma^* \rightarrow \Sigma^*$, where for every input $w$, it holds that

$$w \in A \iff f(w) \in B$$

This function $f$ is called a \textit{polynomial time reduction} from $A$ to $B$. 

![Diagram](image.png)
Theorem

If $A \leq_{P} B$ and $B \in \mathcal{P}$, then $A \in \mathcal{P}$.

Proof:
Reductions

**Theorem**

If \( A \leq_p B \) and \( B \in \mathcal{P} \), then \( A \in \mathcal{P} \).

**Proof:**

- \( M \): a polynomially bounded Turing Machine deciding \( B \)
- \( f \): a polynomial time reduction from \( A \) to \( B \)
- Create a polynomially bounded Turing Machine \( M' \) deciding \( A \)
Theorem

If $A \leq_P B$ and $B \in \mathcal{P}$, then $A \in \mathcal{P}$.

Proof:

- $M$: a polynomially bounded Turing Machine deciding $B$
- $f$: a polynomial time reduction from $A$ to $B$
- Create a polynomially bounded Turing Machine $M'$ deciding $A$

$M' = "On \text{ input } w:\n\begin{enumerate}
1. Compute $f(w)$.
2. Run $M$ on $f(w)$ and output whatever $M$ outputs."$"
A first straightforward example

\[ \text{HPATH} = \{ \langle G, s, t \rangle \mid G \text{ is a graph with a Hamiltonian path from } s \text{ to } t \} \]
\[ \text{HCYCLE} = \{ \langle G \rangle \mid G \text{ is a graph with a Hamiltonian cycle} \} \]

Show that HPATH is polynomial time reducible to HCYCLE.
Solution:

- input of HPATH: a graph $G = (V, E)$ and two vertices $s, t \in V$
- create an instance of HCYCLE
  - $G' = (V', E')$ where $V' = V \cup \{v_0\}$ and $E' = E \cup \{(v_0, s), (v_0, t)\}$

![Diagram of graph $G$ and graph $G'$ with vertices $s$, $t$, and $v_0$.]
Solution:

- **input of HPATH:** a graph $G = (V, E)$ and two vertices $s, t \in V$
- **create an instance of HCYCLE**
  - $G' = (V', E')$ where $V' = V \cup \{v_0\}$ and $E' = E \cup \{(v_0, s), (v_0, t)\}$

The transformation (reduction) is clearly polynomial
Solution:

- input of HPATH: a graph $G = (V, E)$ and two vertices $s, t \in V$
- create an instance of HCYCLE
  - $G' = (V', E')$ where $V' = V \cup \{v_0\}$ and $E' = E \cup \{(v_0, s), (v_0, t)\}$

The transformation (reduction) is clearly polynomial

We are not done!!!
Solution (cont’d)

There is a Hamiltonian Path from $s$ to $t$ in $G$ if and only if there is a Hamiltonian Cycle in $G'$
There is a Hamiltonian Path from $s$ to $t$ in $G$ if and only if there is a Hamiltonian Cycle in $G'$

$(\Rightarrow)$

- consider a Hamiltonian Path from $s$ to $t$ in $G'$:
  
  $s \to v_2 \to \ldots \to v_{n-1} \to t$
Solution (cont’d)

There is a Hamiltonian Path from \( s \) to \( t \) in \( G \) if and only if there is a Hamiltonian Cycle in \( G' \)

\( \Rightarrow \)

- consider a Hamiltonian Path from \( s \) to \( t \) in \( G \):
  \[
  s \rightarrow v_2 \rightarrow \ldots \rightarrow v_{n-1} \rightarrow t
  \]
- then \( v_0 \rightarrow s \rightarrow v_2 \rightarrow \ldots \rightarrow v_{n-1} \rightarrow t \rightarrow v_0 \) is a Hamiltonian Cycle in \( G' \)
There is a Hamiltonian Path from $s$ to $t$ in $G$ if and only if there is a Hamiltonian Cycle in $G'$

$(\Rightarrow)$

- consider a Hamiltonian Path from $s$ to $t$ in $G$:
  
  $s \to v_2 \to \ldots \to v_{n-1} \to t$

- then $v_0 \to s \to v_2 \to \ldots \to v_{n-1} \to t \to v_0$ is a Hamiltonian Cycle in $G'$

$(\Leftarrow)$

- consider a Hamiltonian Cycle in $G'$
There is a Hamiltonian Path from \(s\) to \(t\) in \(G\) if and only if there is a Hamiltonian Cycle in \(G'\)

\((\Rightarrow)\)

\(\quad\)

\(\quad\quad\) consider a Hamiltonian Path from \(s\) to \(t\) in \(G\):

\[s \rightarrow v_2 \rightarrow \ldots \rightarrow v_{n-1} \rightarrow t\]

\(\quad\quad\) then \(v_0 \rightarrow s \rightarrow v_2 \rightarrow \ldots \rightarrow v_{n-1} \rightarrow t \rightarrow v_0\) is a Hamiltonian Cycle in \(G'\)

\((\Leftarrow)\)

\(\quad\)

\(\quad\quad\) consider a Hamiltonian Cycle in \(G'\)

\(\quad\quad\) this cycle should pass from \(v_0\)
There is a Hamiltonian Path from $s$ to $t$ in $G$ if and only if there is a Hamiltonian Cycle in $G'$

($\Rightarrow$)

- consider a Hamiltonian Path from $s$ to $t$ in $G$:
  \[ s \rightarrow v_2 \rightarrow \ldots \rightarrow v_{n-1} \rightarrow t \]
- then $v_0 \rightarrow s \rightarrow v_2 \rightarrow \ldots \rightarrow v_{n-1} \rightarrow t \rightarrow v_0$ is a Hamiltonian Cycle in $G'$

($\Leftarrow$)

- consider a Hamiltonian Cycle in $G'$
- this cycle should pass from $v_0$
- there are only two edges incident to $v_0$: $(s, v_0)$ and $(t, v_0)$
- both $(s, v_0)$ and $(t, v_0)$ should be part of the Hamiltonian Cycle
Solution (cont’d)

There is a Hamiltonian Path from $s$ to $t$ in $G$ if and only if there is a Hamiltonian Cycle in $G'$

($\Rightarrow$)

- consider a Hamiltonian Path from $s$ to $t$ in $G'$:
  
  $s \rightarrow v_2 \rightarrow \ldots \rightarrow v_{n-1} \rightarrow t$

- then $v_0 \rightarrow s \rightarrow v_2 \rightarrow \ldots \rightarrow v_{n-1} \rightarrow t \rightarrow v_0$ is a Hamiltonian Cycle in $G'$

($\Leftarrow$)

- consider a Hamiltonian Cycle in $G'$

- this cycle should pass from $v_0$

- there are only two edges incident to $v_0$: $(s,v_0)$ and $(t,v_0)$

- both $(s,v_0)$ and $(t,v_0)$ should be part of the Hamiltonian Cycle

- Hamiltonian Cycle in $G'$: $t \rightarrow v_0 \rightarrow s \rightarrow \ldots \rightarrow t$
There is a Hamiltonian Path from $s$ to $t$ in $G$ if and only if there is a Hamiltonian Cycle in $G'$

$(\Rightarrow)$

- consider a Hamiltonian Path from $s$ to $t$ in $G$:
  $s \rightarrow v_2 \rightarrow \ldots \rightarrow v_{n-1} \rightarrow t$
- then $v_0 \rightarrow s \rightarrow v_2 \rightarrow \ldots \rightarrow v_{n-1} \rightarrow t \rightarrow v_0$ is a Hamiltonian Cycle in $G'$

$(\Leftarrow)$

- consider a Hamiltonian Cycle in $G'$
- this cycle should pass from $v_0$
- there are only two edges incident to $v_0$: $(s, v_0)$ and $(t, v_0)$
- both $(s, v_0)$ and $(t, v_0)$ should be part of the Hamiltonian Cycle
- Hamiltonian Cycle in $G'$: $t \rightarrow v_0 \rightarrow s \rightarrow \ldots \rightarrow t$
- there is a Hamiltonian Path from $s$ to $t$ in $G$
Steps of a reduction

Reduction from A to B

1. transform an instance $I_A$ of A to an instance $I_B$ of B
2. show that the reduction is of polynomial size
3. prove that:
   “there is a solution for the problem A on the instance $I_A$
   if and only if
   there is a solution for the problem B on the instance $I_B$”
Steps of a reduction

Reduction from A to B

1. transform an instance $I_A$ of A to an instance $I_B$ of B
2. show that the reduction is of polynomial size
3. prove that:
   “there is a solution for the problem A on the instance $I_A$
   if and only if
   there is a solution for the problem B on the instance $I_B”

Comments

▷ usually the one direction is trivial (due to the transformation)
▷ $|I_B|$ is polynomially bounded by $|I_A|$
Let us extend our previous example:

$\text{HPATH} = \{ \langle G \rangle \mid G \text{ is a graph with a Hamiltonian path} \}$

- **HPATH**
- **Instance:** A graph $G = (V, E)$
- **Question** Is there an hamiltonian path in $G$?

We want to show that this problem reduces to $HCYCLE$. 
Let us consider an instance $I_{\text{HPATH}}$, that is a graph $G$. 

We build a particular instance $\tau(G) = G'$ of $\text{HCYCLE}$ by adding a new vertex $x$ that is linked with all the other vertices of $G$: $G' = (V', E')$ where $V' = V \cup \{x\}$ and $E' = E \cup \{x, y\} \forall y \in V$. 

Let us consider an instance $I_{\text{HPATH}}$, that is a graph $G$.

- We build a particular instance $\tau(G) = G'$ of $HCYCLE$ by adding a new vertex $x$ that is linked with all the other vertices of $G$:
- $G' = (V', E')$ where $V' = V \cup \{x\}$ and $E' = E \cup \{x, y\} \ \forall y \in V$
Principle of the reduction from $\textit{HPATH}$ to $\textit{HCYCLE}$
A Hamiltonian path in $G$ (left) leads to a cycle in $\tau(G)$ (right)
Proof

- The transformation $\tau$ is obviously polynomial.
- Let us **show that it is a reduction**: $G$ has an hamiltonian path if and only if $\tau(G)$ has an hamiltonian cycle.
\(\Rightarrow\)

If \(G\) has an hamiltonian path (called \(\varphi\)), then, the cycle \(x \rightarrow \varphi \rightarrow x\) is hamiltonian in \(\tau(G)\).

Since \(x\) is linked with all the vertices in \(G\).
\[ (\Rightarrow) \]
If \( G \) has an hamiltonian path (called \( \varphi \)), then, the cycle \( x \rightarrow \varphi \rightarrow x \) is hamiltonian in \( \tau(G) \).
Since \( x \) is linked with all the vertices in \( G \).

\[ (\Leftarrow) \]
If \( G' \) has an hamiltonian cycle, its sub-graph without \( x \), \( G \), has an hamiltonian path.
- consider a Hamiltonian Cycle in \( G' \)
$(\Rightarrow)$

If $G$ has an hamiltonian path (called $\varphi$), then, the cycle $x \rightarrow \varphi \rightarrow x$ is hamiltonian in $\tau(G)$.
Since $x$ is linked with all the vertices in $G$.

$(\Leftarrow)$

If $G'$ has an hamiltonian cycle, its sub-graph without $x$, $G$, has an hamiltonian path.

- consider a Hamiltonian Cycle in $G'$
- this hamiltonian cycle should pass through $x$ that connects two vertices of $G$: $(s, x)$ and $(t, x)$
(⇒)
If $G$ has an hamiltonian path (called $\varphi$), then, the cycle $x \rightarrow \varphi \rightarrow x$ is hamiltonian in $\tau(G)$.
Since $x$ is linked with all the vertices in $G$.

(⇐)
If $G'$ has an hamiltonian cycle, its sub-graph without $x$, $G$, has an hamiltonian path.

- consider a Hamiltonian Cycle in $G'$
- this hamiltonian cycle should pass through $x$ that connects two vertices of $G$: $(s, x)$ and $(t, x)$
- the hamiltonian Cycle in $G'$ is $t \rightarrow x \rightarrow s \rightarrow \ldots \rightarrow t$
\begin{itemize}
  \item \((\Rightarrow)\)
  If \(G\) has an hamiltonian path \(\varphi\), then, the cycle \(x \rightarrow \varphi \rightarrow x\) is hamiltonian in \(\tau(G)\).
  Since \(x\) is linked with all the vertices in \(G\).

  \item \((\Leftarrow)\)
  If \(G'\) has an hamiltonian cycle, its sub-graph without \(x\), \(G\), has an hamiltonian path.

    \begin{itemize}
      \item consider a Hamiltonian Cycle in \(G'\)
      \item this hamiltonian cycle should pass through \(x\) that connects two vertices of \(G\): \((s, x)\) and \((t, x)\)
      \item the hamiltonian Cycle in \(G'\) is \(t \rightarrow x \rightarrow s \rightarrow \ldots \rightarrow t\)
      \item there is a Hamiltonian Path from \(s\) to \(t\) in \(G\)
    \end{itemize}
\end{itemize}
Exercise

It is also possible to establish the following reduction:
\( \text{HCYCLE} \leq_P \text{HPATH} \).

This result is not immediate, even if it *is/seems* easy to extract a path from a cycle...

**What is the problem here?**
It is also possible to establish the following reduction: \( HCYCLE \leq_p HPATH. \)

This result is not immediate, even if it is/ seems easy to extract a path from a cycle...

**What is the problem here?**

We can not have a characterization of the hamiltonian path (and particularly of its extremities...).
Principle of the reduction from HCYCLE to HPATH

\( \tau \) transforms an instance \( G \) of HCYCLE to an instance \( \tau(G) \) of HPATH:
We duplicate one vertex (any one) $x$ of $G$ in $(x_1, x_2)$
- We duplicate one vertex (any one) $x$ of $G$ in $(x_1, x_2)$
- We link $x_1$ and $x_2$ respectively to two new vertices $y_1$ and $y_2$ as depicted in the figure.
Analysis

This transformation is polynomial.

Show that it is a reduction:
$G$ has an hamiltonian cycle $\text{hamiltonian}$ iif $\tau(G)$ has a hamiltonian path.
Analysis

This transformation is polynomial.

Show that it is a reduction:

$G$ has an hamiltonian cycle hamiltonian iif $\tau(G)$ has a hamiltonian path.

$\Rightarrow$

If $G$ has an hamiltonian cycle, the path starting at $y_1 \rightarrow x_1$, joining the cycle until reaching the neighbor of $x_1$, then, $x_2 \rightarrow y_2$ is an hamiltonian path in $\tau(G)$.

$\Leftarrow$

If there is a hamiltonian path $\varphi$ in $\tau(G)$, it is necessarily like $y_1 \rightarrow x_1 \rightarrow \psi \rightarrow x_2 \rightarrow y_2$ since there is no other choice for $y_1$ and $y_2$.

Then, $x\psi x$ is an hamiltonian cycle in $G$. 
We consider now the decision version of the Travel Saleswoman Person (D-TSP).

- **D-TSP**
- **Instance.** a set $V$ of $n$ cities with the distance matrix $(d_{i,j})$ and an integer $k$.
- **Question.** is there an itinerary of length at most $k$ passing through each city exactly once?

**Show** $HCYCLE \leq_P D-TSP$
Illustration on an instance
The set of the cities corresponds to the vertices of the graph $G$, the distances are given by the particular matrix $d_{i,j} = 1$ if $i$ and $j$ are linked, 2 otherwise.

The constant $k$ is equal to $n$ (number of cities).

This transformation is polynomial, show that it is a reduction.