22.2.3 Examples to problems with efficient certifiers
Example: Vertex Cover

Problem: Does $G$ have a vertex cover of size $\leq k$?

Certificate: $S \subseteq V$.

Certifier: Check $|S| \leq k$ and that for every edge at least one endpoint is in $S$. 
Example: SAT

Problem: Does formula $\varphi$ have a satisfying truth assignment?

Certificate: Assignment $a$ of $0/1$ values to each variable.

Certifier: Check each clause under $a$ and say “yes” if all clauses are true.
Example: Composites

Problem: Composite

**Instance:** A number \( s \).
**Question:** Is the number \( s \) a composite?

1. Problem: Composite.
   1. Certificate: A factor \( t \leq s \) such that \( t \neq 1 \) and \( t \neq s \).
   2. Certifier: Check that \( t \) divides \( s \).
Example: NFA Universality

**Problem:** NFA Universality

**Instance:** Description of a NFA $M$.

**Question:** Is $L(M) = \Sigma^*$, that is, does $M$ accept all strings?

**1. Problem:** NFA Universality.

1. **Certificate:** A DFA $M'$ equivalent to $M$

2. **Certifier:** Check that $L(M') = \Sigma^*$

Certifier is efficient but certificate is not necessarily short! We do not know if the problem is in $NP$. 

Example: NFA Universality

Problem: NFA Universality

**Instance:** Description of a NFA $M$.

**Question:** Is $L(M) = \Sigma^*$, that is, does $M$ accept all strings?

Problem: NFA Universality.

1. **Certificate:** A DFA $M'$ equivalent to $M$
2. **Certifier:** Check that $L(M') = \Sigma^*$

Certifier is efficient but certificate is not necessarily short! We do not know if the problem is in $NP$. 
Example: A String Problem

**Problem:** PCP

**Instance:** Two sets of binary strings $\alpha_1, \ldots, \alpha_n$ and $\beta_1, \ldots, \beta_n$

**Question:** Are there indices $i_1, i_2, \ldots, i_k$ such that $\alpha_{i_1} \alpha_{i_2} \ldots \alpha_{i_k} = \beta_{i_1} \beta_{i_2} \ldots \beta_{i_k}$

**Certificate:** A sequence of indices $i_1, i_2, \ldots, i_k$

**Certifier:** Check that $\alpha_{i_1} \alpha_{i_2} \ldots \alpha_{i_k} = \beta_{i_1} \beta_{i_2} \ldots \beta_{i_k}$

PCP = Posts Correspondence Problem and it is undecidable!

Implies no finite bound on length of certificate!
Example: A String Problem

Problem: **PCP**

| **Instance:** Two sets of binary strings $\alpha_1, \ldots, \alpha_n$ and $\beta_1, \ldots, \beta_n$
| **Question:** Are there indices $i_1, i_2, \ldots, i_k$ such that $\alpha_{i_1}\alpha_{i_2}\ldots\alpha_{i_k} = \beta_{i_1}\beta_{i_2}\ldots\beta_{i_k}$

1. **Problem: PCP**
   1. **Certificate:** A sequence of indices $i_1, i_2, \ldots, i_k$
   2. **Certifier:** Check that $\alpha_{i_1}\alpha_{i_2}\ldots\alpha_{i_k} = \beta_{i_1}\beta_{i_2}\ldots\beta_{i_k}$

PCP = Posts Correspondence Problem and it is undecidable!
Implies no finite bound on length of certificate!
THE END

... (for now)