P versus NP

An algorithm has polynomial running time if there is a constant $c \geq 1$, such that for every input of length n, the algorithm takes $O(n^c)$ time.

exponential running time:

$O(2^{n^c})$ for some constant $c \geq 1$.

polynomial = good, fast, efficient, easy, ...

exponential = bad, slow, "try all possible solutions", difficult, ...

Complexity class

answer is YES or NO

$\mathbb{P}$ = set of all decision problems that can be solved in polynomial time.

Examples of problems that are in $\mathbb{P}$:

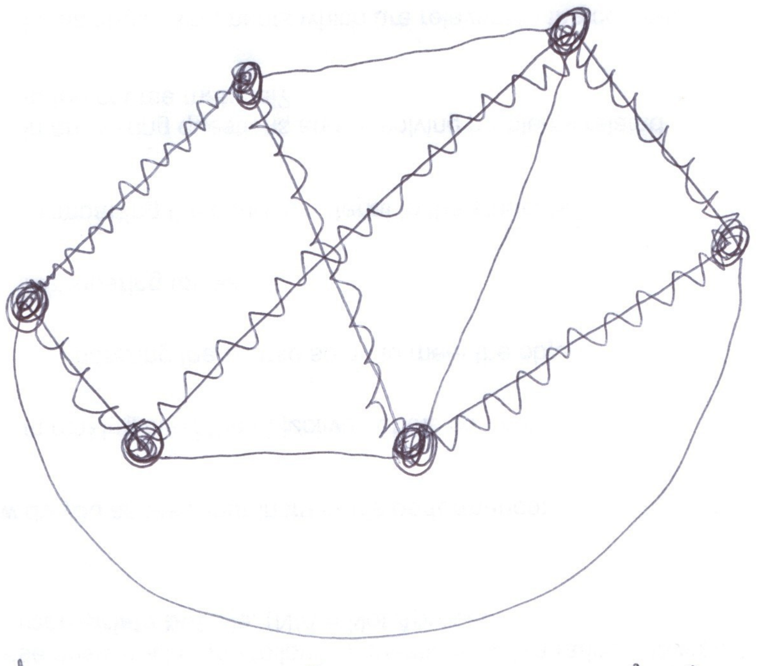
* is a given input graph connected?
* is a given input graph bipartite?
* does a given input graph contain an Euler cycle (= cycle that traverses each edge exactly once)?

Some other problems:

HAM-CYCLE

Input: graph $G = (V, E)$

Question: does G contain a Hamilton cycle (= cycle that visits each vertex exactly once)?



Not known if this problem is in $\mathcal{P}$.

TSP (Traveling Salesman Problem)

Input: $n \times n$ matrix (c_{ij}) of non-negative integers and an integer K.

(c_{ij} = cost to travel from i to j)

Question: does there exist a permutation $\pi_1, \ldots, \pi_n$ of $1, \ldots, n$ such that

$$\sum_{i=1}^{n-1} c_{\pi_i \pi_{i+1}} + c_{\pi_n \pi_1} \leq K \, ?$$

Not known if this problem is in $\mathbb{P}$.

SUBSET-SUM

Input: set S of integers, and integer t.

Question: is there a subset S' of S such that

$$\sum_{x \in S'} x = t \; ?$$

$S = \{5, 7, 56, 23, 2902\}$, $t = 2963$

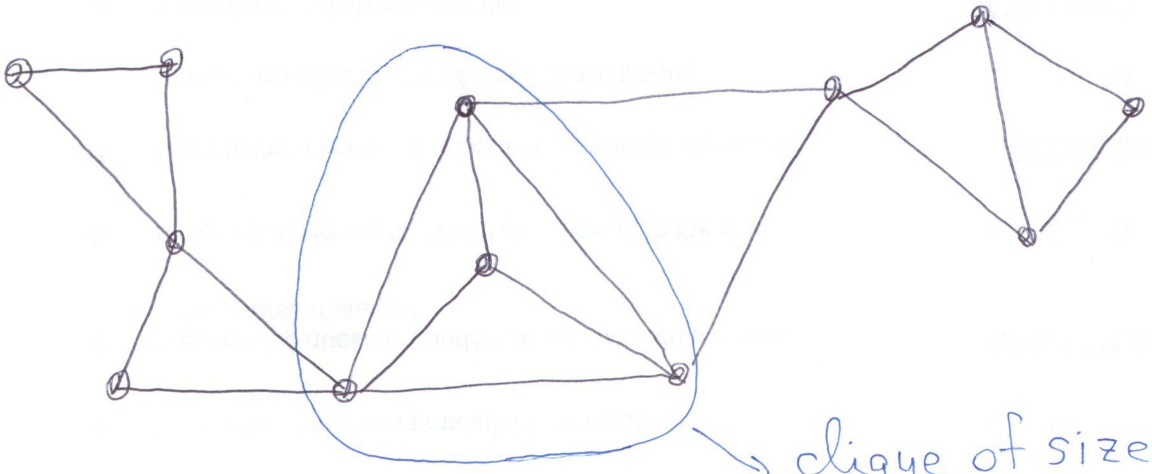
$S' = \{5, 56, 2902\}$

Not known if this problem is in $\mathbb{P}$.

CLIQUE

Input: graph $G = (V, E)$ and integer K.

Question: does G contain a clique (= complete subgraph) with K vertices?



clique of size 4.

Not known if this problem is in $\mathbb{P}$.

For each of the 4 problems on pages 166-169:

* not known if it can be solved in polynomial time.

* if the answer to the question is YES, then

  - there is a $\underbrace{\text{"short"}}_{\text{length is polynomial in the length of the input}}$ proof for this.

  - if someone gives us such a short proof, then we can $\underbrace{\text{"easily"}}_{\text{in polynomial time}}$ verify if this proof is correct.

HAM-CYCLE:

proof/solution = sequence $v_0, v_1, \dots, v_{n-1}$ of vertices

verify: - no duplicates in $v_0, \dots, v_{n-1}$?

- for each $0 \le i \le n-1$,

  $\{v_i, v_{(i+1) \bmod n}\}$ is an edge?

TSP:

proof/solution = ~~perm~~ sequence $\pi_1, \dots, \pi_n$

verify: - $\pi_1, \dots, \pi_n$ is a permutation of $1, \dots, n$?

- $\sum_{i=1}^{n-1} c_{\pi_i \pi_{i+1}} + c_{\pi_n \pi_1} \le K$?

Subset-Sum:

proof/solution: set S'

verify: - is S' a subset of S?

- $\sum_{x \in S'} x = t$?

Clique:

proof/solution: set V'

verify: - is V' a subset of V?

- is $|V'| = K$?

- for each $u \in V', v \in V', u \neq v$:

is $\{u,v\}$ an edge in G?

Complexity class NP:

Decision problem A is in NP if:

* if for a given input I, the answer to the question A(I) is YES, then there exists a proof/solution/certificate C such that
  - C is "short" (= polynomial in the length of I)
  - in polynomial time, we can verify that C is a correct proof for the fact that A(I) = YES.

From previous pages:

HAM-CYCLE, TSP, SUBSET-SUM, CLIQUE are in NP.