

# Theory of Computation

George Karakostas, Rm. ITB/218, [karakos@mcmaster.ca](mailto:karakos@mcmaster.ca)

## Computability vs Complexity

- **Computability:** Problems that can be solved by algorithms (or *impossibility of an **algorithm***).
- **Complexity:** Most efficient algorithm for a *computable* problem (or *impossibility of a **better** algorithm*).

In this course we will focus on **Computational Complexity**.

## Basic complexity questions

- ① Can we do better than **exhaustive search**? (cf.  $P \neq NP$ )
- ② Does **randomness** help? (cf. pseudorandom generators)
- ③ Are there efficient **approximation algorithms**? (cf. Independent Set)
- ④ Can we exploit problem **hardness**? (cf. cryptography)
- ⑤ Are **quantum computers** more powerful than classical computers?  
(cf. Shor's algorithm)
- ⑥ Can **proofs** be efficiently produced automatically? (cf.  $P \neq NP$ )
- ⑦ Can **check** a proof reading only a few bits of it? (cf. PCP theorem)
- ⑧ Are proofs produced by **prover/verifier dialogue** more powerful ? (cf. interactive proofs)