§3 Basic Complexity Theory

- Computing *with* (bit) cost: **WHILE+** programs
- Complexity of Integer Arithmetic / Un-/Pairing
- Major Complexity classes

  $\mathcal{P}$, $\mathcal{NP}$, $\mathcal{PSPACE}$, $\mathcal{EXP}$

  and their relations
- Encoding graphs/non-integer data
- Example problems:

  3COL, EC, HC, VC, EC, ILP, IS, Clique
- *Non*-deterministic **WHILE+** programs
- (Time) Hierarchy Theorem: $\mathcal{P} \neq \mathcal{EXP}$

Model of Computational Cost

KAIST

$$P := (x_j := 0 \mid x_j := 1 \mid x_j := x_i \pm x_k \mid P\,;P \mid \; x_j := x_i \div 2 \mid \text{LOOP } x_j \text{ DO } P \text{ END} \mid \text{WHILE } x_i \text{ DO } P \text{ END})$$

WHILE program to add two n-bit integers: expon. #steps!

Now **WHILE+** programs! (Input in $x_1 \in \mathbb{N}$, output in $x_0 \in \mathbb{N}$)

Observe: Each step increases memory $\ell(\underline{x})$ by ≤ 1!

polynom.time $\Rightarrow$ polynom. space

Definitions: • binary *length* of $x \in \mathbb{N}$: $\ell(x) = \lceil \log_2(1+x) \rceil$

- time of a WHILE+ program P on input $\underline{x}=(x_1,\ldots x_k)$: #steps
- space (=memory) used currently: $\ell(\underline{x}) := \max\{\ell(x_1),..\ell(x_k)\}$
  - used throughout some computation: $\max \ell(\underline{x})$
- asymptotic time/space $t(n)/s(n)$:
  worst-case over all inputs $\underline{x}$ with $\ell(\underline{x})<n$

$\ell(\langle \underline{x} \rangle) \leq O(k \cdot \ell(\underline{x}))$

$\ell(\underline{x}) \leq O(\ell(\langle \underline{x} \rangle))$

Complexity of Arithmetic

KAIST
CS422 M. Ziegler

$$P := (x_j := 0 \mid x_j := 1 \mid x_j := x_i \pm x_k \mid P\,;P \mid \; x_j := x_i \div 2 \mid \text{LOOP } x_j \text{ DO } P \text{ END} \mid \text{WHILE } x_i \text{ DO } P \text{ END})$$

WHILE program to add two n-bit integers: expon. #steps!

Now **WHILE+** programs: (Input in $x_1 \in \mathbb{N}$, output in $x_0 \in \mathbb{N}$)

Recall pairing function $\langle x,y \rangle := x + (x+y)\cdot(x+y+1)/2$

- Multiplication by repeated addition: expon. #steps
- Long multiplication: linear #steps
- Long division: linear #steps
- Un-/pairing: polyn. #steps

in dependence on $n = \ell(\text{input})$

Exercise

asymptotic time/space $t(n)/s(n)$:
worst-case over all inputs $\underline{x}$ with $\ell(\underline{x}) < n$

$$\ell(\langle \underline{x} \rangle) \cong \ell(\underline{x})$$
$$\ell(x) \cong \log x$$

Major Complexity Classes

Definition: a) A **WHILE+** program computes the total function $f:\mathbb{N}\to\mathbb{N}$ if on input x it prints $f(x)$ and terminates in time $t(n)$ / space $s(n)$, $n:=\ell(x)$

Polynomial growth $\mathrm{poly}(n) :\Leftrightarrow \exists k\ t(n)\leq O(n^k)$

closed under compositions: $\mathrm{poly}\circ\mathrm{poly}=\mathrm{poly}$ and $g\circ f$

$V := \{\langle x,y\rangle\in\mathbb{N} : x\in L\} \in \mathcal{P}$

Memory$\leq s \Rightarrow$ #distinct configurations $\leq 2^{O(s)}$

exponential: $2^{\mathrm{poly}(n)}$

- $\mathcal{P} = \{ L\subseteq\mathbb{N}$ decidable in polynomial time $\}$
- $\mathcal{NP} = \{ L\subseteq\mathbb{N}$ verifiable in polynomial time $\}$, i.e. of form

$$L = \{ x\in\mathbb{N} : \exists y\in\mathbb{N},\ \ell(y)\leq \mathrm{poly}(\ell(x)),\ \langle x,y\rangle\in V \},\ V\in\mathcal{P}$$

- $\mathcal{PSPACE} = \{ L\subseteq\mathbb{N}$ decidable in polynomial space $\}$
- $\mathcal{EXP} = \{ L\subseteq\mathbb{N}$ decidable in exponential time $\}$

Theorem: $\mathcal{P}\subseteq\mathcal{NP}\subseteq\mathcal{PSPACE}\subseteq\mathcal{EXP}$

$\ell(x)\cong\log x$

Preliminaries: Graphs and Coding

- Recall: *directed* graph $G=(V,E)$:
  finite set V of n *vertices* and set $E \subseteq V \times V$ of m *edges*
- G *un*directed iff $(u,v) \in E \Leftrightarrow (v,u) \in E$
- Sometimes assign *weights* to edges: $c : E \to \mathbb{N}$

For input/output to **`WHILE+`** programs:

- Encode (G,c) as adjacency matrix $A \in \mathbb{N}^{V \times V}$
  - $A[u,v] := c(i,j)$ for $(u,v) \in E$,
  - $A[u,v] := \infty$ for $(u,v) \notin E$
- Undirected case: only upper triangular matrix.
- Encoding $\langle G,c \rangle \in \mathbb{N}$ has

$$|V| \leq |\langle G,c \rangle| \leq O(|V|^2 \cdot \log \max_{i,j} |c(i,j)|)$$

$$\ell(\langle \underline{x} \rangle) \cong \ell(\underline{x})$$

$$\ell(x) \cong \log x$$

Example Problem (0)

Def: A *3-coloring* of $G=(V,E)$ is a mapping

$$\gamma: V \to \{R,G,B\} \text{ s.t. } \gamma(u) \neq \gamma(v) \text{ for every } (u,v) \in E.$$

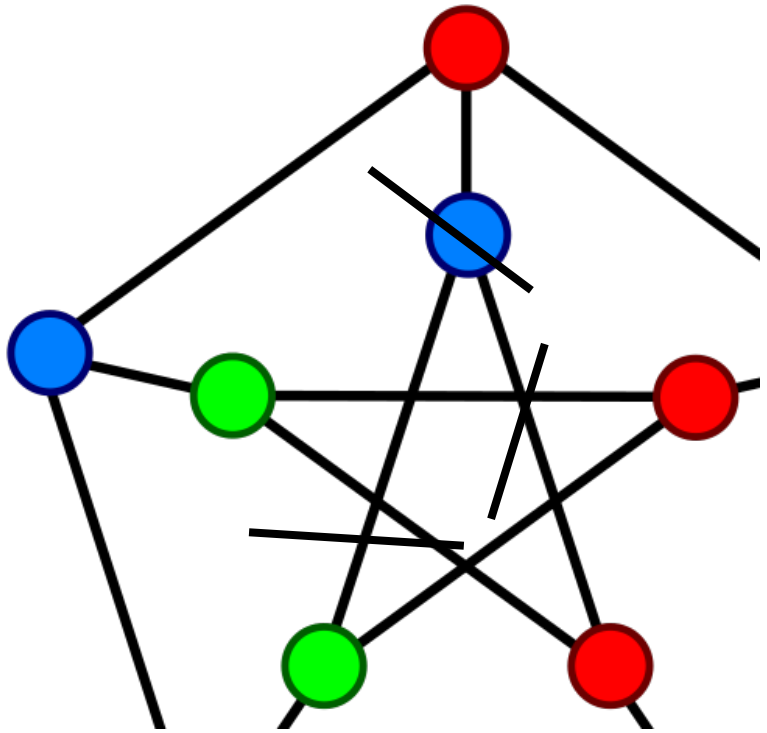
Examples:

a) The *Petersen Graph admits* a 3-coloring.

b) This graph, too.

c) This one still.

d) But not this one.



$$x := \langle G \rangle, \quad y := \langle \gamma(1), \ldots \gamma(|V|) \rangle$$

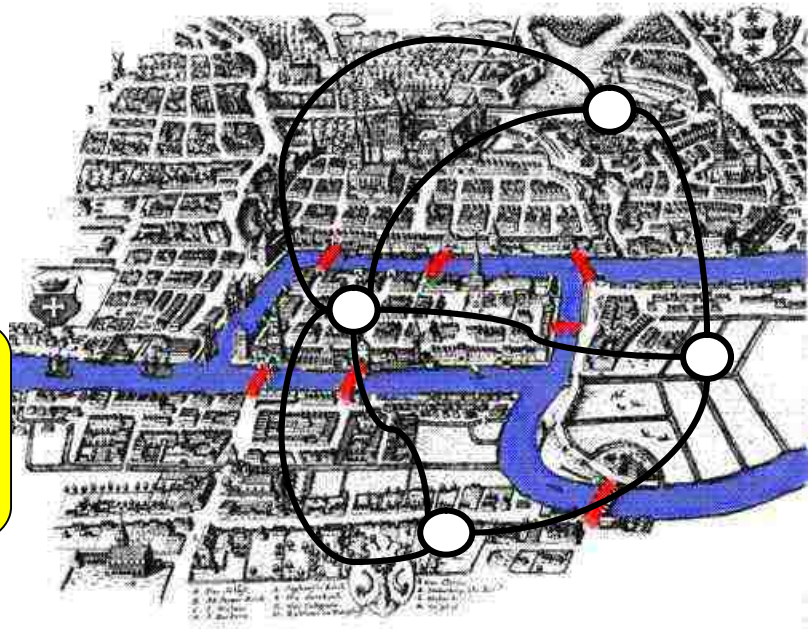
3COL$= \{ \langle G \rangle \mid G$ admits a 3-coloring $\} \quad \in \mathcal{NP}$

$$\mathcal{NP} \ni \{x \in \mathbb{N}: \exists y, \ell(y) \leq \text{poly}(\ell(x)), \langle x,y \rangle \in V\}, \quad V \in \mathcal{P}$$

Example Problems (I)

In an undirected graph G, Eulerian cycle traverses each edge precisely once;

Hamiltonian cycle visits each vertex precisely once.



G admitting a Eulerian cycle is connected and has an even number of edges incident to each vertex.

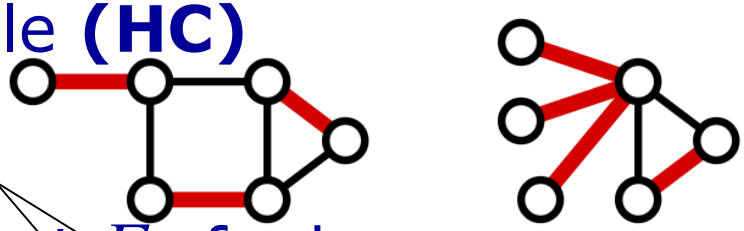
save isolated vertices

Fact: Conversely every *connected* graph with an *even* number of edges incident to each vertex does admit a Eulerian cycle.

$\mathbf{EC} := \{\langle G\rangle \mid G \text{ has a Eulerian cycle}\}$	$\mathcal{P}$
$\mathbf{HC} := \{\langle G\rangle \mid G \text{ has Hamiltonian cycle}\}$	$\mathcal{NP}$

Example Problems (II)

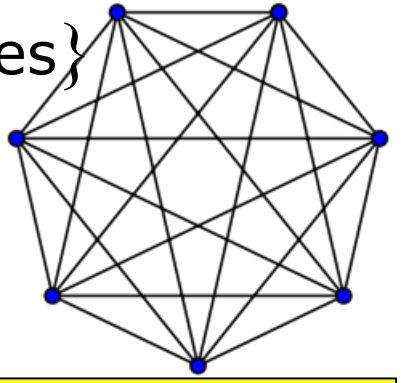
- Eulerian **(EC)** vs. Hamiltonian Cycle **(HC)**
- (Minimum) **Edge Cover** $\mathcal{P}$



"To graph G, find a smallest subset F of edges s.t. any vertex v is adjacent to at least one $e \in F$."

Greedily extend a maximum matching

- vs. **Vertex Cover (VC)** $\mathcal{NP}$
- $\mathbf{CLIQUE} = \{ \langle G,k \rangle \mid G \text{ contains a } k\text{-clique} \}$ $\mathcal{NP}$
- $\mathbf{IS} = \{ \langle G,k \rangle : G \text{ has } k \text{ pairwise non-adjacent vertices} \}$



- Integer Linear Programming $\mathcal{NP}$?

$$\mathbf{ILP} = \{ \langle \underline{A},\underline{b} \rangle : \underline{A} \in \mathbb{Z}^{n \times m}, \underline{b} \in \mathbb{Z}^{m}, \exists \underline{x} \in \mathbb{Z}^{n} : \underline{A} \cdot \underline{x} = \underline{b} \}$$

$$\mathbf{VC} = \{ \langle V,E,k \rangle : \exists U \subseteq V, |U| = k, \forall (x,y) \in E : x \in U \vee y \in U \}$$

$$\mathcal{NP} \ni \{ x \in \mathbb{N} : \exists y, \ell(y) \leq \mathrm{poly}(\ell(x)), \langle x,y \rangle \in V \}, \ V \in \mathcal{P}$$

Example Problems (III)

Def: A Boolean term $\Phi(Y_1,\dots Y_n)$ is composed from variables $Y_1,\dots Y_n$, constants 0 and 1, and operations $\vee$, $\wedge$, $\neg$.

Examples:

- 0
- $(\neg x \vee y) \wedge (x \vee \neg y)$
- $(\neg x \vee y) \wedge (x \vee y) \wedge \neg y$
- $(\neg x \vee y) \wedge (x \vee \neg z) \wedge (z \vee \neg y) \wedge x \wedge (\neg y)$

literals

Φ in 3-CNF if $\Phi = \bigwedge$ *clause* $((\neg)y_i \vee (\neg)y_j \vee (\neg)y_\ell)$

EVAL: Given $\langle\Phi(Y_1,\dots Y_n)\rangle$ and $y_1,\dots y_n \in \{0,1\}$, does $\Phi(y_1,\dots y_n)$ evaluate to 1 ? $\in \mathcal{P}$

[*k*-] SAT: Given $\Phi(Y_1,\dots Y_n)$ [in k-CNF], does it hold $\exists y_1,\dots y_n \in \{0,1\}: \Phi(y_1,\dots y_n)=1$?

Non-Deterministic WHILE+

$$P := (x_j := 0 \mid x_j := 1 \mid x_j := x_i \pm x_k \mid P\,;P \mid \; x_j := x_i \div 2 \mid$$
$$x_j := \text{guess} \mid \text{WHILE } x_i \text{ DO } P \text{ END })$$

Definition: A *non*-deterministic WHILE+ program P may (repeatedly) guess a bit (`0`/`1`).

- Its runtime is $\leq t(n)$ if it makes no more than $t(\ell(x))$ steps, regardless of the guesses.
- P accepts input x if there exists some choice of guessed values such as to return $x_0{=}1$.
- P rejects input x if no choice of guesses returns $x_0{=}1$.

Theorem: $L \subseteq \mathbb{N}$ is accepted by a *non*-deterministic polynomial-time WHILE+ program iff $L \in \mathcal{NP}$.

Non-Deterministic WHILE+

KAIST
CS422 M. Ziegler

$P := (x_j := 0 \mid x_j := 1 \mid x_j := x_i \pm x_k \mid P ; P \mid x_j := x_i \div 2 \mid$
guess x_j $\mid$LOOP x_j DO P END $\mid$ WHILE x_i DO P END)

$\mathcal{NP} \ni \{x \in \mathbb{N}: \exists y, \ell(y) \leq \text{poly}(\ell(x)), \langle x,y \rangle \in V\}, \ V \in \mathcal{P}$

Proof $\Leftarrow$: Let P on input x guess $y \in \mathbb{N}$ bitwise,
then execute program deciding $\langle x,y \rangle \in V$.

$\Rightarrow$: Let P accept L in time $\text{poly}(n)$,
guessing $\leq \text{poly}(n)$ bits y_j. Define $V := \{ \langle x, \text{bin}(y_j) \rangle : \ldots \}$

- P accepts input x if there exists some choice of guessed values such as to return $x_0=1$.
- P rejects input x if no choice of guesses returns $x_0=1$.

Theorem: $L \subseteq \mathbb{N}$ is accepted by a *non*-deterministic polynomial-time WHILE+ program iff $L \in \mathcal{NP}$.

Recap of §3 *Basic Complexity*

KAIST
CS422 M. Ziegler

- Computing *with* (bit) cost: **WHILE+** programs
- Complexity of Integer Arithmetic / Un-/Pairing
- Major Complexity classes
  $\mathcal{P}$, $\mathcal{NP}$, $\mathcal{PSPACE}$, $\mathcal{EXP}$
  and their relations
- Encoding graphs/non-integer data
- Example problems:
  3COL, EC, HC, VC, EC, ILP, IS, Clique
- *Non*-deterministic **WHILE+** programs
- (Time) Hierarchy Theorem: $\mathcal{P} \neq \mathcal{EXP}$