CS-524: Computational Complexity
Prof. Mika Göös
22 December 2022

Sample Solution

SCIPER : Signature :

Final Exam, Computational Complexity 2022

- Books, notes, communication, calculators, cell phones, computers, etc... are not allowed.
- Your explanations and proofs should be clear enough and in sufficient detail so that they are easy to understand and have no ambiguities.
- You are allowed to refer to material covered in **lectures and exercises** (but *not* homeworks) including theorems without reproving them.
- Please answer inside the space indicated (the exams will be scanned for grading purposes).

Good luck and have fun!

Problem 1 / 15 points	Problem 2 / 20 points	Problem 3 / 15 points	Problem 4 / 20 points	Problem 5 / 15 points	Problem 6 / 15 points

Total / 100

1. Quick-fire round. *(15 pts)* Consider the following statements.

1. Graph isomorphism is NP-complete.
2. $\textsc{Clique} \leq_p \overline{\textsc{Clique}}$.
3. $\mathsf{TIME}^A(n) \neq \mathsf{TIME}^A(n^{2022})$ for every oracle A.
4. $\mathsf{PSPACE} = \mathsf{NPSPACE}$.
5. P^{NP} is closed under complement.
6. $\Sigma_2\mathsf{P}$ has a complete problem.
7. If $\mathsf{NP} \subseteq \mathsf{P/poly}$, then $\mathsf{P} = \mathsf{NP}$.
8. If $\mathsf{NP} \subseteq \mathsf{BPP}$, then $\mathsf{RP} = \mathsf{NP}$.
9. If $\Sigma_2\mathsf{P} = \Pi_2\mathsf{P}$, then $\mathsf{NP} = \mathsf{coNP}$.
10. $\mathsf{L} \neq \mathsf{PH}$.
11. $\mathrm{s}(f) \leq \mathrm{bs}(f)$ for any boolean function f.
12. The n^2-bit function $\textsc{And}_n \circ \textsc{Or}_n$ has sensitivity $\Omega(n^2)$.
13. Every unsatisfiable CNF formula admits a polynomial-size Resolution refutation.
14. There exists a language $L \subseteq \{0,1\}^*$ that cannot be computed by any family of boolean circuits.
15. Nondeterministic communication complexity of *non-equality* $\neg\textsc{Eq}_n$ is $\mathrm{N}_1(\neg\textsc{Eq}_n) = O(\log n)$.

For each box below, write one of the following symbols:

- **T** if the statement is known to be true.
- **F** if the statement is false *or not known to be true* (e.g., both $\mathsf{P} = \mathsf{NP}$ and $\mathsf{P} \neq \mathsf{NP}$ should be marked **F**).
- or leave the box empty.

A correct **T**/**F** answer is worth +1 point, an incorrect answer is worth −1 point, and an empty answer is worth 0 points.

Your answers:

1.	F
2.	F
3.	T
4.	T
5.	T

6.	T
7.	F
8.	T
9.	F
10.	F

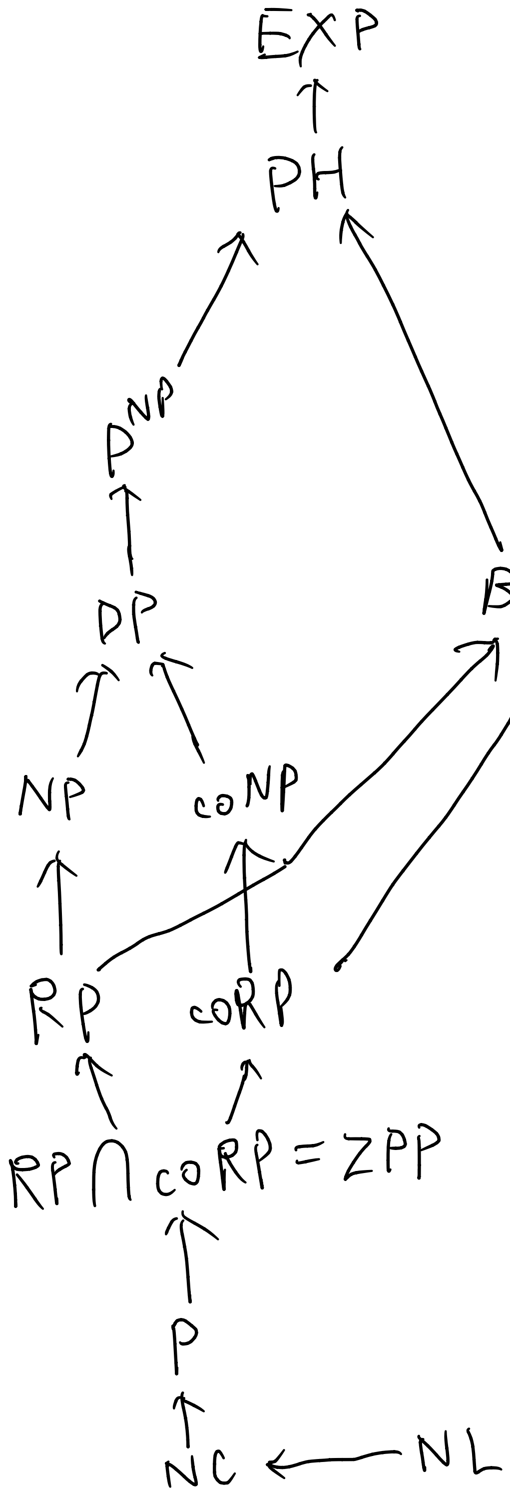
11.	T
12.	F
13.	F
14.	F
15.	T

2. Complexity Zoo. *(20 pts)* Consider the following list of complexity classes:

P, NP, coNP, PH, P^{NP}, DP, EXP, BPP, RP, coRP, RP ∩ coRP, ZPP, NC, NL.

Draw a ***class inclusion diagram*** for the above classes that has a directed arrow $A \to B$ between classes A and B whenever $A \subseteq B$. You do not have to draw *transitive arrows*, i.e., if $A \to B$ and $B \to C$, you can leave out $A \to C$. For ease of readability, please draw the smallest class at the bottom, and the largest class at the top of the page.

Please answer inside the box



3. Problem Garden. *(15 pts)*

For each problem below, classify it into the smallest possible complexity class (as seen in lectures/exercises). If you use a class not mentioned in Problem 2, then relate your class to those in Problem 2 by inclusions. (You do not need to justify your answers.)

1. **Input:** DNF formulas φ and ψ. **Output:** YES iff $\varphi(x) = \psi(x)$ for all x.
2. **Input:** Directed graph G. **Output:** YES iff there is a directed cycle in G.
3. **Input:** Boolean circuit C and unary number 1^k. **Output:** YES iff C can be written as a CNF of size at most k.
4. **Input:** Turing Machine M and binary number k. **Output:** YES iff M, on empty input, halts within k steps.
5. **Input:** Graph G and number k. **Output:** YES iff the chromatic number of G is k. (The *chromatic number* of G is the least k such that G can be coloured with k colours.)

Please answer inside the box

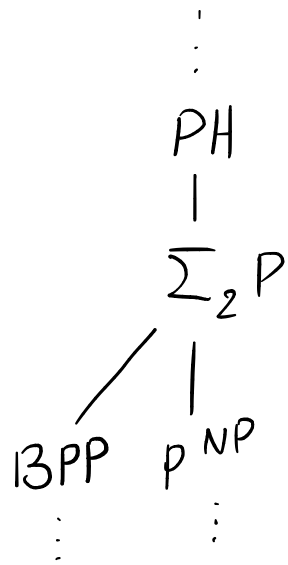
1) coNP

2) NL

3) $\Sigma_2 P$

4) EXP

5) DP



4. NP-completeness. *(20 pts)* Consider the following model of cellphone conversations. We have an undirected graph $G = (V, E)$ where the vertices are people, and each edge indicates that two people are within range of each other. Whenever two people are talking, their neighbours must stay silent to avoid interference. Thus a set of conversations is a set of edges $C \subseteq E$, where vertices in different edges in C are not neighbours of each other. The *cellphone capacity* of G is the largest number of conversations that can take place simultaneously without interference, i.e., the size of the largest such set C. Prove that the following problem is NP-complete:

$$\text{CELLCAP} = \{\langle G, k\rangle : G \text{ has cellphone capacity at least } k\}.$$

In your proof, you may assume the NP-completeness of any of the problems discussed in the course (SAT, INDEPENDENTSET, CLIQUE, SUBSETSUM, VERTEXCOVER, SETCOVER, 3-COLOUR, etc.).

Remember to prove the correctness of your reduction!

Please answer inside the box

$CC \in NP$

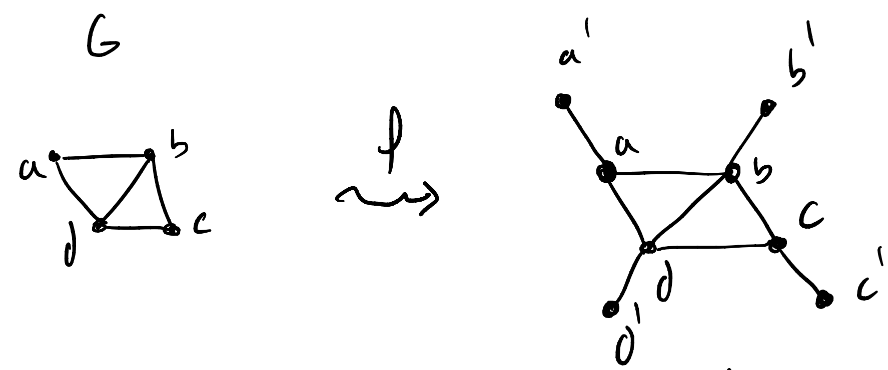
a certificate is some $C \subseteq E$. the verifier checks:

1) $|C| \geq k$
2) C is a valid CC (iterate over pairs of edges in C and check no conflict)

$IS \leq CC$

On input $\langle G, k\rangle$, the reduction returns $\langle G', k\rangle$ where G' is a copy of G but where each vertex v has a new "satelite" vertex v' attached.

e.g



Note that $f: \{0,1\}^* \to \{0,1\}^*$ is polytime computable

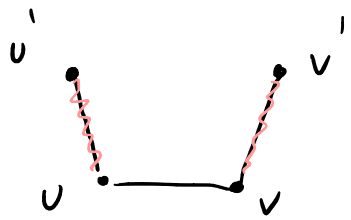
We show correctness i.e: $\forall \langle G,k\rangle$:

$$\langle G,k\rangle \in IS \iff \langle G',k\rangle \in CC$$

$\Rightarrow$

fix an IS $S \subseteq V$ of size k in G and let $C = \{\{v,v'\} : v \in S\} \subseteq E'$. Note $|C| = k$ and C is a valid CC. Suppose not because $\{u,u'\}$ and $\{v,v'\}$ clashes:

thus in G':

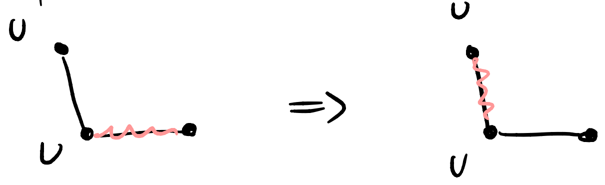


but note that $\{u,v\} \in G$ so S is not IS ↯

$$\Rightarrow \langle G',k\rangle \in CC \quad \#$$

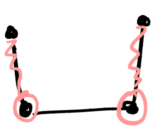
$\Leftarrow$

fix a CC $C \subseteq E'$ of size k in G. wlog, one can assume C only takes "satelite" edges. Indeed if not, can swap edges without creating conflicts:



define $S = \{v : \{v,v'\} \in C\} \subseteq V$. Note $|S| = k$ and S is an IS in G if not:

in G':



so C not a CC ↯

$$\Rightarrow \langle G,k\rangle \in IS \quad \#$$

Since IS is NP-hard, CC is NP-complete #

5. Communication complexity. *(15 pts)* Let $f\colon \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$ be a two-party communication problem.

(a) Define what a nondeterministic communication protocol is. Define also the cost of the protocol and the associated 1-sided complexity measure $\mathrm{N}_1(f)$.

(b) Suppose $\mathrm{N}_1(f) = k$. Show that there is a deterministic protocol for f of cost at most $2^k + 1$.

Please answer inside the box

(a)

The nondeterministic communication protocol is a pair of functions $A, B : \{0,1\}^n \times \{0,1\}^s \to \{0,1\}$. The protocol accepts an input $(x,y) \in \{0,1\}^n \times \{0,1\}^n$ iff. there is some certificate w such that $A(x,w) = B(y,w) = 1$. The cost of the protocol is the size of the certificate s. The associated 1-sided complexity measure $N_1(f)$ is the least cost of all protocols that compute f.

(b)

Let $A, B : \{0,1\}^n \times \{0,1\}^k \to \{0,1\}$ denote the nondeterministic protocol for f of cost k. We give a deterministic protocol for f of cost $2^k + 1$ as follows. Assume that Alice holds $x \in \{0,1\}^n$ and Bob holds $y \in \{0,1\}^n$. Then Alice sends a 2^k-bit string $S = A(x,0)\|A(x,1)\|\cdots\|A(x,2^k-1)$ to Bob, where we identify each k-bit string with an integer in $[0, 2^k - 1]$. Then Bob can check if there is some certificate $w \in [0, 2^k - 1]$ such that both the $(w+1)$-th bit of S and $B(y,w)$ are 1. If there exists such a certificate, Bob outputs 1 as the answer, otherwise he outputs 0.

6. Circuits vs. decision trees. *(15 pts)*

(a) Suppose that a boolean function $f\colon \{0,1\}^n \to \{0,1\}$ is computed by a decision tree of size s. Show that f can be computed by a boolean circuit of size $O(s)$.

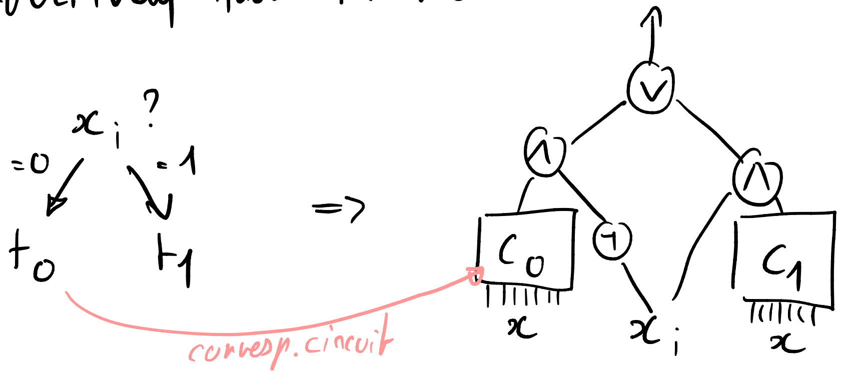
(b) Show that the converse fails: For every $n \in \mathbb{N}$, exhibit a function $f\colon \{0,1\}^n \to \{0,1\}$ such that f can be computed by a circuit of size $O(n)$, but every decision tree computing f requires size $2^{\Omega(n)}$.

For problem (b), prove a lower bound from first principles. If you want, you may define, and then apply, *Tree–Adversary games* to prove your lower bound. Do not directly use any other results from exercises/homeworks.

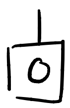
Please answer inside the box

(a) Fix a dt t computing f with size s. We build the graph inductively from the root

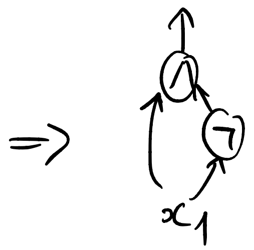
if t of form:



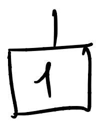
if t of form:



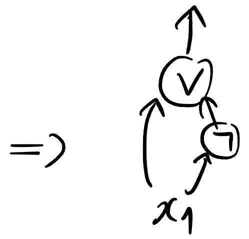
i.e a 0-leaf



if t of form:



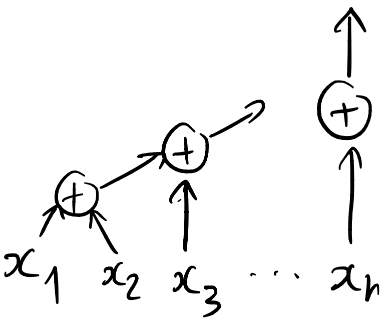
i.e a 1-leaf



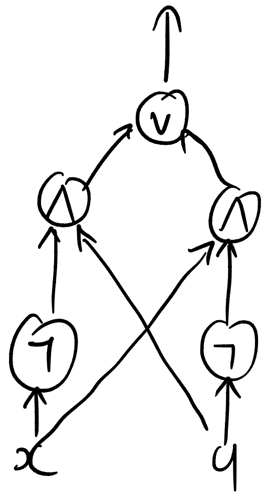
Note each node gets replaced by $O(1)$ gates so that the entire circuit has size $O(s)$.

(b) choose XOR_n

• it has a circuit of size $O(n)$:



where $x \oplus y$ can be computed with: i.e $O(1)$ gates



• any dt t computing it has size $2^{\Omega(n)}$:

actually if t is not complete of depth n, t fails on at least one input. indeed fix a leaf ℓ of size $<n$ and suppose w.l.o.g it does not query x_1.

let x be st $\ell(x)=1$ fix x' with:

$$x'_i = \begin{cases} x_i & \text{if } i \neq 1 \\ 1-x_i & \text{if } i=1 \end{cases}$$

then note $\ell(x')=1$ but $XOR(x) \neq XOR(x')$ so t errs on x or x' #

Note: could also have used Tree-Adversary games.