COMPUTATIONAL COMPLEXITY THEORY (COMS 30126)
GUIDE TO EXAMINABLE MATERIAL

⋆ Anything not explicitly listed as omitted should be regarded as examinable. (This includes unlisted topics). If in doubt, please enquire!

⋆ For many theorems, *proofs* are omitted, but *statement* of the theorem is still required i.e. you need to be able to accurately state the theorem and understand what it says!

⋆ All exercise sheets are examinable material with the following questions OMITTED: sheet 1: 1,4,7; sheet 2: 5; sheet 3: 3; sheet 4: 3; sheet 5: no omissions; sheet 6: 3,4.

COURSE OUTLINE WITH OMITTED ITEMS IDENTIFIED:

TMs: basic structure and operation (transition table). How to specify a configuration.

NDTMs: definition, computational paths, branching tree of all paths, notion of accepting/rejecting an input (asymmetrical definition).

Languages $\mathcal{L} = \{0,1\}^*$. TM or NDTM recognising/deciding a language.

Theorem: set of all TMs can be enumerated. OMIT proof.
Theorem: halting problem is undecidable. OMIT proof.

Big/small O notation. Statements of principal properties comparing log/poly/exponential growths.

Theorem (page 12): NDTMs can be simulated on TM with exponential time overhead. OMIT proof.

The class P.
PATH problem. Adjacency matrix of a directed graph. Argument that PATH∈P.

Verifiers. Poly-time verifiers.
The class NP (defined by verifiers). co-NP.
Theorem: A∈NP iff A is decided by a poly-time NDTM. OMIT proof.

Notion of poly-time reduction. NP completeness.

Satisfiability problem. Cook-Levin theorem. OMIT proof.

Theorem: 3-SAT is NPC. OMIT proof.

Oracle TMs (page 18-20): definition of oracle TM. Theorems A and B. OMIT proofs.

Theorem: 2-SAT $\in$ P. OMIT proof.

Space complexity. PSPACE.
Savitch theorem. OMIT proof.
NPSPACE=PSPACE and proof.
PSPACE completeness, definition.

Definitions of: space bounded TMs, log space transducer and its configurations. L, NL, NL completeness.

Theorem: PATH is NL complete. OMIT proof.

Randomised complexity: OMIT examples of randomised algorithms (on page 27-29).

Definitions of: PTMs, accept/reject probability for an input, BPP.

Amplification lemma statement. OMIT proof.

Definitions of: RP, co-RP, ZPP, PP, MAJSAT.
Theorem: NP$\subseteq$PP and proof.

Circuits: definition of Boolean circuit.
Proposition (page 35): universality of AND, OR, NOT gates, and proof.

Theorem: "most Boolean functions need exp big circuits". OMIT proof.

Definitions of: circuit family, decision of $\mathcal{L}$ by a circuit family, size and depth complexity.

Example of parity function.

Definition of uniform circuit family.
Proposition: "undecidable languages can have poly sized circuits". and proof.

Theorem C: $\mathcal{L} \in$ P iff $\mathcal{L}$ has uniform circuit family. OMIT proof.

Notion of P completeness. CIRCUIT-VALUE problem.

Theorem: CIRCUIT-VALUE is P complete, and proof.

Theorem: any $\mathcal{L} \in$ BPP has poly sized circuits. OMIT proof.

Definition of parallel complexity classes NC^i and NC.

Theorem: $\mathrm{NC}^1 \subseteq \mathrm{L} \subseteq \mathrm{NL} \subseteq \mathrm{NC}^2$. OMIT proofs.

Definition of interactive proof system and class IP.
BPP$\subseteq$IP, NP$\subseteq$IP.

Remarks on probabilities in the definition: OMIT these remarks.

Theorem: dIP=NP, and proof.

Graph non-isomorphism problem and its interactive proof system.

Program checking application: OMIT this section.

Theorem: IP=PSPACE. OMIT proof.

Theorem: $\sharp$-SAT is in IP. OMIT proof.