Problem Set 6
Exercises on Oracles
CSCI 6114 Fall 2023

Joshua A. Grochow

Released: October 10, 2023
Due: Monday October 16, 2023

Exercises

1. Build an oracle A such that $\mathsf{PSPACE}^A \neq \mathsf{NP}^A$. *Hints:* (1) Use the language $L_A := \{0^n | \text{the number of strings in } A \cap \Sigma^n \text{ is even}\}$. Show that this language is in PSPACE^A for all oracles A. (2) Construct the oracle in stages, similar to the oracle separating P from NP that we did in class. The construction of an oracle separating NP from coNP at the start of Section 3 of Ko's survey uses a similar trick to the trick needed in this problem—look at the two cases near the bottom of p. 10.

2. Build an oracle B such that $\mathsf{PSPACE}^B \neq \mathsf{NP}^B \neq \mathsf{P}^B$. *Hint:* Combine the construction from the previous problem with the construction we did in class of an oracle separating P from NP. Interleave the stages of the two constructions.

3. Build an oracle C such that $\mathsf{P}^C \neq \mathsf{NP}^C \cap \mathsf{coNP}^C$. *Hint:* One way to do this is to build C such that $\mathsf{P}^C \neq \mathsf{NP}^C = \mathsf{coNP}^C$ (which is in Du & Ko Theorem 4.20(b)), but that is far from the only way! If you want to try this route, try to first build an oracle "directly" that makes $\mathsf{NP} = \mathsf{coNP}$ (that is, don't just use a PSPACE oracle and make them both equal to PSPACE, but build the oracle inductively by stages.) In Du & Ko, you can use SAT^C instead of the "resource-bounded halting language" K_C that they use. Relativized Boolean Satisfiability can be defined this way:

Boolean Satisfiability with oracle C
Input: A Boolean formula built from variables $x_1, \ldots, x_n$, and OR, AND, NOT, and ORACLE gates. An ORACLE gate can take any number of inputs, and $\text{ORACLE}(q_1, \ldots, q_m) = C(q_1 q_2 \ldots q_m)$. That is, the oracle gate treats its input as a string q, and outputs 1 or 0 according to whether q is in the oracle C or not.
Decide: Is there an assignment to the variables that makes the Boolean formula true?

Resources

- Sipser Section 9.2 defines oracle TMs and constructs oracles showing that P vs. NP does not relativize.
- Du & Ko Section 4.3 covers similar material, as does Homer & Selman Section 7.5.1.1.
- Du & Ko Section 4.8 covers more advanced oracles around NP, which are harder than but still potentially relevant to this problem set. In particular they give oracles that collapse some classes while separating others, e.g., $\mathsf{P}^X \neq \mathsf{NP}^X = \mathsf{coNP}^X$.
- Ker-I Ko has an expository survey giving many examples of the connection between circuit lower bounds and oracles.
- Du & Ko Sections 4.6 and 4.7 cover more advanced topics in relativization: positive relativization and random oracles, respectively. Random oracles are also covered in Gems of TCS Chapter 22. In both of these sources they show that "$\mathsf{P}^A \neq \mathsf{NP}^A$ with probability 1."
- Arora & Barak Section 3.5 covers oracles showing that P vs. NP does not relativize. Warning: their comments about non-relativizing proof techniques in the freely available online book draft are misleading. While it is true that 3SAT itself is not NP^A-complete for all oracles A, there is a straightforward relativization of 3SAT, and 3SAT^A is NP^A-complete under $\leq_m^p$ (unrelativized reductions) for all oracle A, and because of the latter it is generally said that the Cook–Levin Theorem *does* relativize.
- The original construction of an oracle relative to which P was different from NP (and also an oracle answering question 3 above) is due to

Baker, Gill, and Solovay and independently by Dekhtiar. This mathoverflow question has references and lots of interesting history!