Homework 2
Due Fri Nov 4, 5:00pm

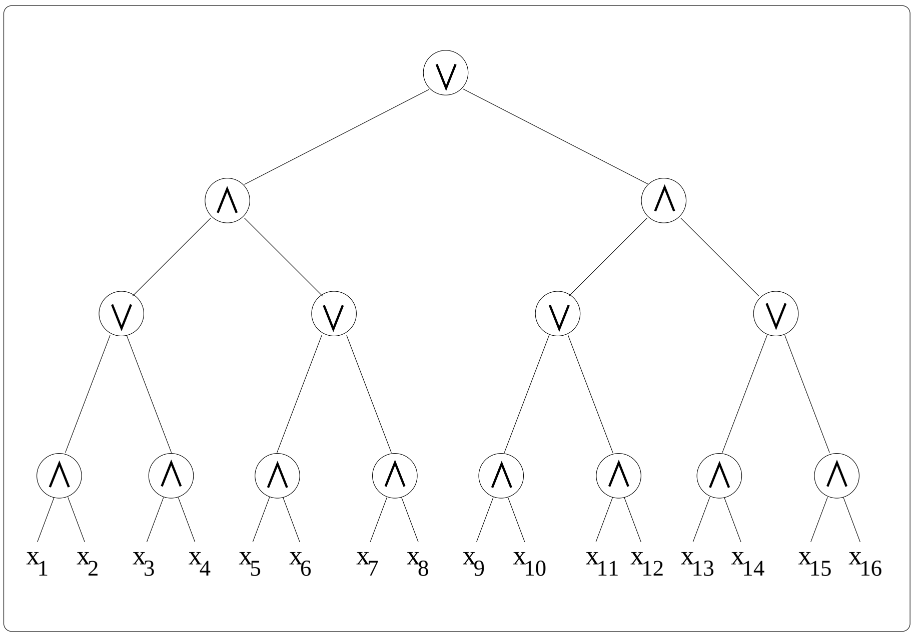
Prof. Amit Chakrabarti
Department of Computer Science
Dartmouth College

General Instructions. Each problem has a fairly short solution; if you find yourself writing more than a page of proof, you have probably not found the best solution; you might want to rethink your approach. **Each problem is worth 10 points.**

Honor Prinicple. You are allowed to discuss the problems and exchange solution ideas with your classmates. But when you write up any solutions for submission, you must work alone. You may refer to any textbook you like, including online ones. However, you may not refer to published or online solutions to the specific problems on the homework. *If in doubt, ask the professor for clarification!*

This homework is very enjoyable and also fairly challenging. Start early!

6. By suitably generalizing the function in the figure below, construct a family of functions $f_n : \{0,1\}^n \to \{0,1\}$ such that, for infinitely many n, we have $\mathrm{D}(f_n) = \Theta(n)$ whereas $\mathrm{C}(f_n) = \Theta(\sqrt{n})$.



Make sure you define f_n for *all* integers n, even if you happen to start with a definition for certain special values of n.

7. Let G be a group of permutations of $[n]$ (not necessarily the group of *all* permutations). Let $\alpha \in \{0,1,\star\}^n$ be a partial assignment. For $\pi \in G$, define $\pi \circ \alpha$ to be the partial assignment obtained by applying the permutation π to α. We define a function $F_{\alpha,G} : \{0,1\}^n \to \{0,1\}$ as follows:

$$\forall\, x \in \{0,1\}^n : \quad F_{\alpha,G}(x) = \begin{cases} 1, & \text{if } \exists\, \pi \in G :\ x \text{ matches } \pi \circ \alpha \\ 0, & \text{otherwise.} \end{cases}$$

7.1. Prove that $\mathrm{C}_1(F_{\alpha,G}) = \mathrm{Ex}(\alpha)$. Recall that $\mathrm{Ex}(\alpha)$ denotes the number of exposed bits in α.

7.2. Prove that $s(F_{\alpha,G}) \geq \mathrm{Ex}(\alpha)/2$.

8. For a Boolean function $f : \{0,1\}^n \to \{0,1\}$, let $\mathrm{R}_\varepsilon(f)$ denote its ε-error (two-sided) randomized query complexity. That is, we are considering distributions over decision trees with a *worst case* bound on the number of queries made, but we allow the trees to make errors. Formally, for a probability distribution τ on n-input binary decision trees, let $\mathrm{depth}(\tau)$ denote the *maximum* depth of a tree in the support of τ. Let $T(x)$ denote the output of the decision tree T on the input x. Then

$$\mathrm{R}_\varepsilon(f) \;=\; \min\left\{\mathrm{depth}(\tau) : \forall x \in \{0,1\}^n \ \Pr_{T\sim\tau}[T(x) \neq f(x)] \leq \varepsilon\right\}.$$

Let $\mathrm{R}(f)$ denote the zero-error version of randomized query complexity, familiar from class (i.e., the "Las Vegas" version):

$$\mathrm{R}(f) \;=\; \min_{\tau} \max_{x\in\{0,1\}^n} \mathbb{E}_{T\sim\tau}[\mathrm{cost}(T,x)]\,,$$

where the min is over all distributions over trees that *always* correctly compute $f(x)$.

This problem walks you through some general theorems about randomized query complexity, and its relation to other measures.

8.1. Show that $\mathrm{R}_\varepsilon(f) \le \varepsilon^{-1}\,\mathrm{R}(f)$. In particular, $\mathrm{R}_{1/3}(f) = O(\mathrm{R}(f))$. There is an easy proof via Markov's inequality.

8.2. Prove that $\mathrm{R}_\varepsilon(f) \ge (1-2\varepsilon)\mathrm{bs}(f)$. For this, consider a distribution τ that achieves the minimum in the definition of R_ε and then consider the probability that a random tree from τ queries each sensitive block of an input.

8.3. Let $\widetilde{\deg}_\varepsilon(f)$ denote the ε-approximate degree of f, i.e.,

$$\widetilde{\deg}_\varepsilon(f) \;=\; \min\{\deg(p) : p \text{ multilinear polynomial and } \forall\, x\in\{0,1\}^n \text{ we have } |p(x)-f(x)|\le\varepsilon\}\,.$$

Let $T\sim\tau$, where τ is a distribution over depth-d decision trees. Let $x\in\{0,1\}^n$. Show that $\Pr_T[T(x)=1]$ can be expressed as a degree-d polynomial in $x_1,\ldots,x_n$. Using this, prove that $\widetilde{\deg}_\varepsilon(f)\le \mathrm{R}_\varepsilon(f)$ for $\varepsilon\in(0,\frac{1}{3})$.

8.4. Prove that $\mathrm{bs}(f)\le 6\,\widetilde{\deg}_{1/3}(f)^2$. Generalize the argument from class (using Markov's inequality) relating $\mathrm{bs}(f)$ to $\deg(f)$. Conclude that $\mathrm{bs}(f)$ and $\mathrm{R}_{1/3}(f)$ are polynomially related.

9. Treating an n-bit vector $\vec{x}$ as a string (so that the ordering of the variables is important) we can define a Boolean function $A_n^s : \{0,1\}^n \to \{0,1\}$ as follows: $A_n^s(\vec{x}) = 1$ iff $\vec{x}$ contains s as a substring. Here s is a fixed string.

9.1. Show that A_5^{111} and A_6^{111} are not evasive, i.e., it is possible to compute these functions without ever having to look at every input bit.

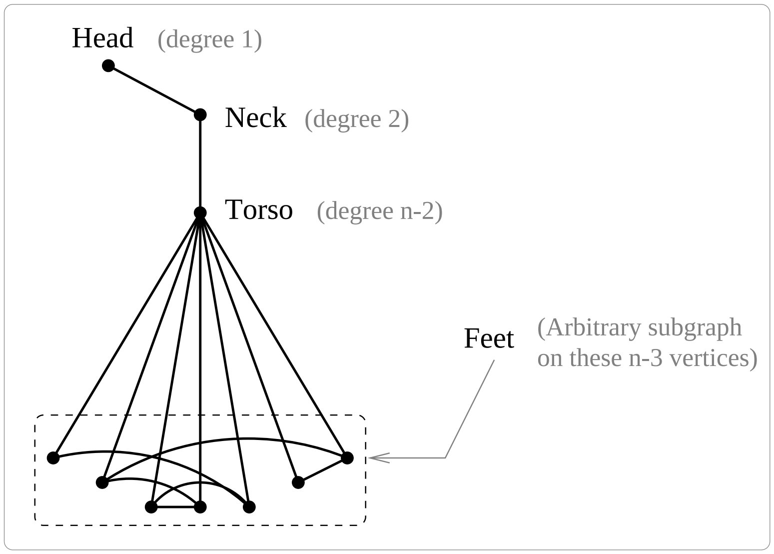
9.2. Show that A_3^{111} and A_4^{111} are evasive.

9.3. Prove that A_n^{111} is evasive iff $n\equiv 0$ or $3 \pmod 4$. Hint: For the "if" direction, use a recurrence for the number of strings of length n that satisfy A_n^{111}, and prove that sometimes just looking at this number tells you that the function is evasive. For the "only if" direction, use the ideas from your solution to #9.1, plus induction.

9.4. Find all integers n for which A_n^{100} is evasive. Hint: Consider $n \bmod 3$.

10. Even while working on lower bounds one often has to prove upper bounds, if only to provide counterexamples for plausible but false lower bound conjectures. In the early 1970s it was conjectured that any nontrivial graph property f_n on n-vertex graphs has $\mathrm{D}(f_n) = \Omega(n^2)$. The Rivest-Vuillemin theorem proves this for monotone f_n, but what about non-monotone properties?

Call an n-vertex graph a *scorpion* if it has the structure shown in the following figure.



Let f_n be the property of being a scorpion.

10.1. Argue that f_n is not monotone.

10.2. Design an algorithm that computes f_n while querying at most $6n$ of the $\binom{n}{2}$ Boolean variables representing the possible edges of the n-vertex graph. This shows that far from having an $\Omega(n^2)$ lower bound, we have an upper bound: $\mathrm{D}(f_n) \le 6n = O(n)$.

Hint: If an input graph is indeed a scorpion, it is easy to verify this if an oracle tells you which vertex is the torso.

11. In class, we *almost* finished the proof of the Rivest-Vuillemin theorem. We proved that if $f : \{0,1\}^N \to \{0,1\}$ is a nonconstant monotone Boolean function invariant under a transitive group of permutations of the variables, then:

   (a) If N is a power of 2, then f is evasive.

   (b) If f is an n-vertex graph property (and so, $N = \binom{n}{2}$) and n is a power of 2, then $\mathrm{D}(f) \ge n^2/4$.

This problem walks you through the last bit of the proof, where we handle n-vertex graph properties f for arbitrary $n \ge 2$. Let $k = \lfloor \log_2 n \rfloor$, so that $2^k \le n < 2^{k+1}$. The basic idea is to identify a suitable subfunction g of f, note that $\mathrm{D}(f) \ge \mathrm{D}(g)$ and lower bound $\mathrm{D}(g)$ either directly, using one of facts (a) or (b) above, or indirectly, through an induction hypothesis.

11.1. Let the variables of f be named x_{ij}, with $1 \le i < j \le n$. Consider the two possible subfunctions of f obtained by setting $x_{1j} = b$ for all possible j, where $b \in \{0,1\}$. Show that if either of these subfunctions is nonconstant, then you can "make progress," according to the above plan.

11.2. Give an example of a natural (and very common) nonconstant graph property that causes both the above subfunctions to be constant.

11.3. Now suppose both the above subfunctions are constant. Partition the vertex set $[n]$ into disjoint parts A, B, C with $A < B < C$,[1] $|A| = |B| = 2^{k-1}$ and $|C| = n - 2^k$. Consider the subfunction of f obtained by setting

$$x_{ij} = \begin{cases} 0, & \text{if } i \in A \text{ and } j \in A \cup C\,, \\ 1, & \text{if } i, j \in B \cup C\,. \end{cases}$$

Prove that this subfunction is nonconstant. Identify a transitive permutation group under which it is invariant.

11.4. Based on the above observations, conclude that $\mathrm{D}(f) \ge n^2/16$, thereby finishing the proof.

[1]This notation means that we have $a < b < c$ for all $a \in A, b \in B, c \in C$.