Homework 5
Due 2017-Feb-13, 11:59pm

Prof. Amit Chakrabarti
Department of Computer Science
Dartmouth College

General Instructions. Same as for Homework 1.

Honor Prinicple. Same as for Homework 1.

---

10. 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 transitively symmetric Boolean function, then:

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

    (b) If f is a v-vertex graph property—which makes $n = \binom{v}{2}$—and v is a power of 2, then $\mathrm{D}(f) \geq v^2/4$.

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

    10.1. Let the variables of f be named x_{ij}, with $1 \leq i < j \leq v$. 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.

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

    10.3. 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 $|C| = v - 2^k$. 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. By identifying a suitable group of permutations, prove that this subfunction is transitively symmetric.

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

11. Recall that Shannon's lower bound says that there exists a Boolean function $f : \{0,1\}^n \to \{0,1\}$ such that its circuit complexity $\mathrm{C}(f) = \Omega(2^n/n)$. In fact, almost all n-input Boolean functions have this property.

    Prove that this lower bound is tight up to constant factors. That is, improve the upper bound we showed in class by proving that every function $f : \{0,1\}^n \to \{0,1\}$ has an n-input circuit of size $O(2^n/n)$.

    Hint: Consider the function f as being $f(y,z)$, where $y = \{x_1, \ldots, x_k\}$ and $z = \{x_{k+1}, \ldots, x_n\}$. Now, the truth table of f can be viewed as a $2^k \times 2^{n-k}$ matrix, with the rows indexed by all possible assignments to y. Each column of this matrix gives us a certain pattern in $\{0,1\}^{2^k}$. What if there aren't too many different patterns? Can we use that fact to cut down on the circuit size?

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