Please turn in your solution in class on Tuesday October 15. You are encouraged to collaborate on the homework and ask for assistance, but you are required to write your own solutions, list your collaborators, acknowledge any sources of help, and provide external references if you have used any.

Question 1

In this question you will improve the lower bound on the decision tree size for recursive majority by a different method. Given a function $f\colon \{-1,1\}^n \to \{-1,1\}$, let $L(f) = \sum|\hat{f}_S|$ be the sum of the absolute values of the coefficients of its polynomial (Fourier) representation. For example, $MAJ_3(x_1,x_2,x_3) = \frac{1}{2}x_1 + \frac{1}{2}x_2 + \frac{1}{2}x_3 - \frac{1}{2}x_1x_2x_3$ and so $L(MAJ_3) = 4 \cdot \frac{1}{2} = 2$. In this question we represent both inputs and outputs by $-1/1$ values.

(a) Let f be the AND of n literals (variables or their negations) in $-1/1$ representation. What is $L(f)$?

(b) Use part (a) to show that if f has a decision tree of size at most s then $L(f) \le 3s$.

(c) Let $h(y_1,y_2,y_3) = f(g(y_1),g(y_2),g(y_3))$, where y_1,y_2,y_3 are sets of disjoint variables and g has no constant term (i.e. $\hat{g}_\varnothing = 0$). Show that $L(h) = F(L(g),L(g),L(g))$, where F is the polynomial obtained from f by turning all its coefficients positive (i.e., $F(x) = \sum_S|\hat{f}_S|\prod_{i\in S}x_i$).

(d) Use part (c) to show that $L(RMAJ_d) \ge L(RMAJ_{d-1})^3/2$.

(e) Use parts (b) and (d) to show that $RMAJ_d$ requires decision tree size $2^{\Omega(3^d)}$.

Question 2

In Lecture 4 we showed that $R_0(RMAJ_d) \le (8/3)^d$ for the recursive majority of threes function $RMAJ_d\colon \{0,1\}^n \to \{0,1\}$, $n = 3^d$. In this question you will prove a lower bound for $R_{1/3}(RMAJ_d)$. We say a bit is ε-biased (where $-1 \le \varepsilon \le 1$) if it takes value 0 with probability $(1-\varepsilon)/2$ and value 1 with probability $(1+\varepsilon)/2$.

(a) Let X,Y,Z be independent ε-biased bits. Let ε' be the bias of $MAJ_3(X,Y,Z)$. What is ε' as a function of ε?

(b) Show that there exists some small constant $\varepsilon_0 > 0$ such that if $|\varepsilon| \le \varepsilon_0$ then $\varepsilon' + \varepsilon'^2 \ge \frac{3}{2}(\varepsilon+\varepsilon^2)$.

(c) Now let $X_1,\dots,X_n$, where $n = 3^d$ be $(2/3)^d$-biased bits. Use part (b) to show that the bias of the bit $RMAJ(X_1,\dots,X_n)$ is lower bounded by some constant independent of d.

For the last part you will need the following theorem from statistics: If $X_1,\dots,X_\ell$ and $Y_1,\dots,Y_\ell$ are independent ε-biased and $(-\varepsilon)$-biased bits respectively, then $(X_1,\dots,X_\ell)$ and $(Y_1,\dots,Y_\ell)$ are $O(\sqrt{\varepsilon^2\ell})$-indistinguishable by all algorithms.

(d) Show that $R_{1/3}(RMAJ_d) \ge \Omega((9/4)^d)$.

(e) (**Extra credit:**) In conclusion, $(9/4)^d \preceq R_{1/3}(RMAJ_d) \preceq R_0(RMAJ_d) \le (8/3)^d$. Can you improve any of these bounds?

Question 3

In Lecture 5 we claimed there exist $\varepsilon\sqrt{n}$-wise indistinguishable distributions μ and ν on $\{-1,1\}^n$ such that μ assigns probability at least 0.99 to the all-ones string and ν assigns probability at least 0.62 to all strings with exactly one -1 for some $\varepsilon > 0$. Let $\phi\colon \{-1,1\}^n \to \mathbb{R}$ be the function

$$\phi(x) = \left(\prod_{i=1}^{n} x_i\right) \cdot \mathrm{E}_S\left[\prod_{i\in S} x_i\right]^2,$$

where S is a random subset of $\{1,\dots,n\}$ of size at most $(n-d)/2$ (chosen uniformly among all such subsets), and E_S is expected value.

(a) Show that if $p\colon \{-1,1\}^n \to \mathbb{R}$ is a polynomial of degree less than d then $\sum_{x\in\{-1,1\}^n} p(x)\phi(x) = 0$. (**Hint:** Look at the monomials of p and ϕ.)

(b) Let $\mu(x) = \max\{2\phi(x)/Z, 0\}$ and $\nu(x) = \max\{-2\phi(x)/Z, 0\}$. Use part (a) to show that for some choice of Z, μ and ν are probability distributions that are $(d-1)$-wise indistinguishable.

(c) Show that $Z = \sum_{x\in\{-1,1\}^n} \mathrm{E}_S\left[\prod_{i\in S} x_i\right]^2$. Calculate $2/Z$ in terms of n and d.

(d) Let $d = \varepsilon\sqrt{n}$. Calculate $\lim_{\varepsilon\to 0}\lim_{n\to\infty} \mu(1^n)$, where 1^n is the all-ones string.

(e) Let $W = (n - 2|S|)/\sqrt{n}$. Show that $\sum_{x\in N} \nu(x) = 2\,\mathrm{E}[W]^2/Z$, where N is the set of strings with exactly one -1.

(f) Use part (e) and the Central Limit Theorem to calculate $\lim_{\varepsilon\to 0}\lim_{n\to\infty}\sum_{x\in N}\nu(x)$.

(g) Use parts (b), (d), and (f) to prove the claim.

(h) **(Research project:)** Can you come up with $\varepsilon\sqrt{n}$-wise indistinguishable μ and ν for which both the limits in part (d) and part (f) are 1? I know that they exist but I don't know a "nice" formula for them.