Propositional Proof Complexity
Assignment # 2
Due: Monday April 28, 2025, 11:59pm

1. Recall the negation of the induction principle, $\neg\textsc{Ind}_n$: the underlying variables are x_i, $i \in [n]$, and the clauses are:

   (i) (x_1);

   (ii) $(\neg x_n)$;

   (iii) For all $i \in [n-1]$: $(\neg x_i \vee x_{i+1})$.

   Give a constant-degree Polynomial Calculus refutation of $\neg\textsc{Ind}_n$.

2. Recall the mod 2 counting principle, $\textsc{Mod}2_n$, discussed in Homework 1, that asserts that there is no perfect matching on an odd number of vertices. The negation of the mod 2 counting principle, $\neg\textsc{Mod}2_n$ is a CNF formula with underlying variables $x_{i,j}$ for $i \neq j$, $i, j \leq 2n+1$ to represent whether or not there is a matching between vertices i and j. The clauses of $\neg\textsc{Mod}2_n$ are of two types:

   (i) For every $i \leq 2n+1$ we have the clause $(\vee_{j \neq i}\, x_{i,j})$ stating that each vertex is included in at least one matching.

   (ii) Secondly, for every $i, j, k \leq 2n+1$, $i \neq j \neq k$, we have the clause $(\neg x_{ij} \vee \neg x_{i,k})$, stating that every vertex i is matched with at most one other vertex.

   Recall the negation of the bijective pigeonhole principle, $\neg\text{Bi-PHP}_n^{n+1}$. The underlying variables are $p_{i,j}$, $i \in [n+1]$, $j \in [n]$, and the clauses are:

   (i) For every $i \in [n+1]$, we have the clause $(\vee_{j\in[n]} p_{i,j})$;

   (ii) For every $i \in [n+1]$, $j \neq j' \in [n]$: $(\neg p_{i,j} \vee \neg p_{i,j'})$;

   (iii) For every $j \in [n]$: $(\vee_{i\in[n+1]} p_{i,j})$;

   (iv) For every $i \neq i' \in [n+1]$, $j \in [n]$: $(\neg p_{i,j} \vee \neg p_{i',j})$.

   Clauses of type (i) and (ii) express that every pigeon is mapped to exactly one hole, and clauses (iii),(iv) express that the mapping is bijective.

   Prove that if $\neg\textsc{Mod}2_n$ has a polynomial-sized Resolution refutation, then so does the negation of the bijective pigeonhole principle, $\neg\text{Bi-PHP}_n^{n+1}$.

3. Search versus Decision Problems. A *randomized* depth-d decision tree for a search problem $S \subseteq 0, 1^n \times [m]$ is a collection of decision trees $\mathcal{T} = \{T_1, \ldots, T_q\}$ satisfying:

   (i) Each T_i is a deterministic decision tree over $\vec{x} = x_1, \ldots, x_n$ with each leaf of T_i labelled by some $j \in [m]$;

   (ii) For every assignment $\alpha \in \{0, 1\}^n$, $Pr_{i\in[q]}[(\alpha, T_i(\alpha)) \in S] \geq 2/3$.

It is known that the randomized decision tree complexity of any function is at most the deterministic decision tree complexity squared: $R^{\mathrm{CC}}(f) \leq D^{\mathrm{CC}}(f)^2$.

In this problem you will prove that in contrast, there is no polynomial relationship between deterministic and randomized decision tree complexity for the more general class of *search problems*. Assume that $M = 2^m$, and $N = 2^n$ (so both M and N are powers of two), and let $n = 2m$. Consider two functions $F : [N] \to [M]$, and $G : [M] \to [N]$. Since $M < N$, the composed function $G \circ F$ cannot be the identity mapping, so we can define the associated total search problem, $\textsc{Find-Viol}_{M,N}$: The variables of $\textsc{Find-Viol}_{M,N}$ are: $F_{i,j}$, $i \in [N]$, $j \in [m]$, and $G_{k,l}$, $k \in [M]$, $l \in [n]$. We view $F_{i,1}, \ldots, F_{i,m}$ as the bit representation of the element $F(i) \in [M]$ that pigeon i is mapped to, and similarly $G_{k,1}, \ldots, G_{k,n}$ is the bit representation of the element $G(k) \in [N]$ that k is mapped to. On input F, G, $\textsc{Find-Viol}_{M,N}(F, G)$ is the set of $i \in [N]$ such that $G(F(i)) \neq i$; that is, valid solutions are elements $i \in [N]$ that are not mapped to themselves by the composed function $G \circ F$.

(a) Prove that there are constant-error randomized decision trees solving the search problem $\textsc{Find-Viol}_{M,N}(F, G)$.

(b) Prove that any deterministic decision tree for $\textsc{Find-Viol}_{M,N}$ requires depth $\Omega(M)$.

4. (EXTRA CREDIT) Sherali-Adams versus Nullsatz. Recall the standard *equational* translation of a clause into an equivalent polynomial equation, e.g., $(x_1 \vee \neg x_2 \vee x_3)$ becomes $(1 - x_1)(x_2)(1 - x_3) = 0$. In this question we will compare Nullsatz versus SA refutations for unsat 3CNFs; in order to make this comparison fairly, in both cases we assume the underlying field is the reals, and the translation is equational. Let $\mathcal{P} = \{p_1, \ldots, p_m\}$ be a set of polynomial inequalities over $x_1, \ldots, x_n$. Recall that a Sherali-Adams refutation of $\mathcal{P}$ is a set $\{J_0, J_1, \ldots, J_m\}$ of conical juntas such that $J_0 + \sum_{i=1}^{m} J_i p_i = -1$. In this problem we consider the relative strength of SA refutations of unsatisfiable 3CNFs with and without the leading junta J_0.

(a) Prove that degree-d SA_0 refutations of unsat 3CNFs (translated into equations) over the reals is equivalent to degree-d NS refutations.

(b) Show that degree-d SA over the reals can simulate width-d Resolution.

(c) Show that degree-d SA_0 cannot simulate degree-d SA (over the reals) by exhibiting a family of unsatisfiable CNFs that require $\Omega(\log n)$-degree SA_0 refutations but that have SA refutations of degree $O(1)$.

Hint: You may use parts (a),(b) from this question, in addition to results that were discussed in class.