Question 1

The bounded halting problem BH is the following search problem: On input \((M, x, r)\), where \(M\) is the description of a Turing Machine, does there exist a \(y\) of length at most \(|r|\) such that \(M\) accepts \((x, y)\) in at most \(|r|\) steps?

(a) Show that BH is in NP and every NP search problem reduces to BH in polynomial time.

(b) Show that for every NP search problem \(S\) there is a polynomial \(p\) such that if \((BH, U)\) has a randomized polynomial-time heuristic with error \(\varepsilon(n)\), then \((S, U)\) has one with error \(\varepsilon(n)p(n)\). Here \(U\) is the uniform ensemble.

(c) Use part (a) and Theorem 8 from Lecture 6 to show that there exists a polynomial-time samplable ensemble \(D\) on 3SAT instances so that if \((3SAT, D)\) has a polynomial-time heuristic with negligible error so does every search problem in distributional NP.

Question 2

Consider the following search problem. The input is a nondeterministic circuit \(C\) with the promise that it accepts exactly half of its inputs:

\[
\Pr_{x \sim \{0,1\}^n}[\text{there exists } w \text{ such that } C(x, w) = 1] = \frac{1}{2}.
\]  

(1)

The objective is to find a no instance of \(C\) (an \(x\) such that \(C(x, w) = 0\) for all \(w\)). Here is a prover-assisted interactive algorithm for this task:

\(V\): Sample \(x_1, \ldots, x_{1000} \sim \{0,1\}^n\) independently uniformly at random and send them to the prover.

\(P\): For every \(x_i\), send back \(w_i\) such that \(C(x_i, w_i) = 1\) if one exists or the special symbol \(w_i = \text{no}\) if not.

\(V\): If \(C(x_i, w_i) = 0\) for any \(w_i \neq \text{no}\), or if there are more than 540 \text{nos}, reject.

Otherwise output a random \(x_i\) among those for which \(w_i = \text{no}\).

(a) Assuming the promise (1) holds, show that \((V, P)(C)\) outputs a no instance of \(C\) with probability at least 99%.

(b) Assuming the promise (1) holds, show that for every prover \(P^*\), \((V, P^*)(C)\) either rejects or outputs a no instance of \(C\) with probability at least 90%.
Question 3

Given an undirected graph $G$, let $G^2$ be the graph whose vertices are ordered pairs of vertices in $G$ and whose edges are those pairs $\{(u, v), (u', v')\}$ such that $\{u, u'\}$ is an edge in $G$ or $u = u'$, and $\{v, v'\}$ is an edge in $G$ or $v = v'$.

(a) Show that if $G$ has a clique of size $k$ then $G^2$ has a clique of size $k^2$.

(b) Show that if $G^2$ has a clique of size $K$ then $G$ has a clique of size $\lceil \sqrt{K} \rceil$.

(c) Show that if there exists a polynomial-time algorithm that finds a clique of size at 1% of the size of the largest clique in a graph, then there is a polynomial-time algorithm that finds a clique of size at least 99% the size of the largest clique.

Question 4

A function $f : \{0, 1\}^n \to \{0, 1\}$ is affine if it is of the form $f(x) = \langle a, x \rangle + b$ for some $a \in \{0, 1\}^n$ and $b \in \{0, 1\}$.

(a) Show that there exists a test $T'$ that makes a constant number of queries into its oracle, accepts affine functions with probability 1, and rejects functions that are at least $\delta$-far from affine with probability $\Omega(\delta)$. (Hint: Reduce to the linearity test.)

(b) Show that if $T'$ makes at most 3 queries and $T^f$ accepts all affine functions $f$ with probability 1 then $T^g$ accepts all possible $g$ with probability 1.

(c) Conclude from part (b) that there is no 3-query test that accepts all affine functions but rejects all functions that are 1/4-far from affine with positive constant probability when $n$ is sufficiently large.

(d) (Extra credit) Show (without looking up the answer) that the test in part (a) can be carried out with four queries.