1 Question 1, section c

What most of you did Most of you stated that if \( f_{\text{code}} \) is OWF but not a PRG this is a direct contradiction to GL theorem due to section b.

Why it is not accurate For the input \( C, x, \chi(e) \) to \( f_{\text{code}} \), GL theorem talks about finding \( \langle C \circ x \circ \chi(e), r \rangle \) for \( r \in \{0, 1\}^{2k^2+k+\frac{k}{4}} \), while section b shows just how to find \( \langle x, r \rangle \) for \( r \in \{0, 1\}^k \).

What you should have done State that from knowing \( \langle x, r \rangle \) with proba-bility greater then \( \frac{1}{2} + \frac{1}{p(n)} \) we are able to extract x (A conclusion that is used to prove GL theorem and was mentioned in class), and from there state that we can calculate \( \langle C \circ x \circ \chi(e), r \rangle \) for \( r \in \{0, 1\}^{2k^2+k+\frac{k}{4}} \) because \( C \) is known and given \( C, x, f_{\text{code}}(C, x, \chi(e)) \) it is trivial to find \( \chi(e) \).

2 Question 4, section a

What most of you did Most of you detailed correctly the game between \( \text{Com}, \text{Ver} \), but then for binding required that: "There are no \( m_0, m_1, \text{com}, \text{dec}_0, \text{dec}_1 \) such that for every bit b: \( \Pr[\text{VER}(1^n, m_b, \text{com}, \text{dec}_b) = \text{acc}] > \text{negl} \)" (or wrote something equivalent).

Why its wrong This requirement is too weak. Ask yourself: What is the probability space here? It is all the random coins that \( \text{Ver} \) flips. Therefore, imagine a commitment interactive protocol, in which on the last message \( \text{Ver} \) sends to \( \text{Com} \) two random messages \( m_0, m_1 \) along with two random polynomial length decommitments \( \text{dec}_0, \text{dec}_1 \), such that it is promised that for every bit b: \( \Pr[\text{VER}(1^n, m_b, \text{com}, \text{dec}_b) = \text{acc}] = 1 \). Intuitively of course we wouldn’t want that such protocol will be considered as a valid commitment scheme. But notice that for every \( m_0, m_1, \text{dec}_0, \text{dec}_1 \) it’s chance to be picked by \( \text{Ver} \) is negligible and therefore such protocol might fulfill the requirement you gave at your definition.
What you should have done  Is to reverse the order of quantifiers. That is - require that the probability that there are $m_0, m_1, com, dec_0, dec_1$ such that for every bit $b$: $\Pr[\text{VER}(1^n, m_b, com, dec_b) = \text{acc}] > \text{negl}$ is negligible.

3  Question 6

What most of you did  Most of you stated that if $\text{Gen}, \text{Eval}$ is a CRHF then $f_k(x) = f(k, x)$ is a one way functions family (or wrote something equivalent), and the proof sketch went like this:

- Assume by contradiction that there is an $A$ inverting $f_k$.
- Given random $k, x$, $A(1^n, f_k(x))$ will give us $x'$ such that $H_k(x) = H_k(x')$ with non negligible probability.
- With non negligible (in fact, constant) probability there is a chance that there is $x' \neq x$ such that $H_k(x) = H_k(x')$.
- Therefore, the probability of finding collisions in the CRHF using $A$ is at least $\frac{1}{\text{poly}(n)} \times \frac{1}{4}$ which is non negligible (where the $\frac{1}{4}$ is a lower bound on the probability that there is $x' \neq x$ such that $H_k(x) = H_k(x')$ (at least half), times the probability that $A$ is right and does not return $x$ (at least half).

Why its wrong  This argument implicitly assume that the events: "A succeeds to invert f" and "there is $x' \neq x$ such that $H_k(x) = H_k(x')$" are independent - but what if $A$ succeeds in non negligible probability $\frac{1}{\text{poly}(n)}$, and it succeeds Only on $f_k(x)$ such there is no $x' \neq x$ such that $H_k(x) = H_k(x')$?

What you should have done  You had two ways to get it right:

- Show that the build mentioned above is a weak one way function and use the statement given in class that if there exists a weak one way function then OWF exists.
- Prove the existence of CRHF with $l(n) = o(n)$ and prove the correctness of this construction with this CRHF.

4  Question 7 - section a

What most of you did  Most of you claimed that the probability that an adversary $A$ will ask its oracle question with $k = x$ is negligible because the probability that it will ask about $k$ in each query is $\frac{1}{2^n}$ and it is only allowed to make polynomial number of queries.
**Why it's wrong**  This statement ignores the fact that $A$ is *adaptive*. That is, he potentially deduce information about $k$ from its queries to $F_k()$ and use it to narrow down his search and ask about $k$ with higher probability than $\frac{p(n)}{2^n}$.

**What you should have done**  You should have bound the probability that $A$ will ask about $k$ with negligible function by showing that if it is not the case then $F$ is not a PRF (=build a distinguisher that "guesses" all of $A$ queries as the key and checks if it was right).