As mentioned in class, this proof is **optional** material.

For simplicity, we prove the claim for receivers R that draw r in an "honest" way, i.e. uniformly at random. (A-priori, a "cheating" R could have also drawn r in another clever way, to try and discover the commitment bit.)

Given the simplifying assumption, the distribution that the receiver sees has r (chosen at random) and a string that may be either $G(s)$ (when $b = 0$) or $G(s) \oplus r$ (when $b = 1$). We'd like to argue that there is no efficient R that can ϵ-distinguish between the two distributions, for any $\epsilon(n) = 1/\text{poly}(n)$.

Lemma 1. *If the PRG conjecture is true, then for every polynomial-time R, we have*

$$\left| \Pr_{r,s}[R(r, G(s)) = 1] - \Pr_{s,r}[R(r, G(s) \oplus r) = 1] \right| \leq n^{-\omega(1)} ,$$

where r and s are chosen independently in the distributions above.

Proof. Assume towards a contradiction that there is a polynomial-time R that ϵ-distinguishes between $(r, G(s))$ and $(r, G(s) \oplus r)$, for some $\epsilon = \epsilon(n) = 1/\text{poly}(n)$. We construct a polynomial-time D that $(\epsilon/2)$-distinguishes the output distribution $G(s)$ of the PRG from a random n-bit string, as follows.

- **Input:** $x \in \{0,1\}^n$. (We want to decide if x is a random string or $x = G(s)$ for some s.)
- Draw $b \in \{0,1\}$ and $r \in \{0,1\}^n$ uniformly at random.
- If $R(r, x \oplus b \cdot r) = b$ then $D(x)$ outputs 1, otherwise $D(x)$ outputs 0.

Analysis. Clearly D runs in time $\text{poly}(n)$ (the dominant step is running R). We argue that D behaves differently on the uniform distribution and on the distribution of $G(s)$ for a random s. Specifically, on the former D accepts with probability $1/2$, and on the latter D accepts with probability bounded away from $1/2$ (by $\geq \epsilon/2$).

Claim 1.1. $\left| \Pr_s[D(G(s)) = 1] - 1/2 \right| \geq (\epsilon/2)$.

Proof. Note that

$$\begin{aligned}
&\Pr_s[D(G(s)) = 1] = \Pr_{s,b,r}[R(r, G(s) \oplus b \cdot r) = b] && \text{(definition of } D\text{)} \\
&= \frac{1}{2} \cdot \Pr_{s,r}[R(r, G(s) \oplus r) = 1] + \frac{1}{2} \cdot \Pr_{s,r}[R(r, G(s)) = 0] && \text{(law of total probability)} \\
&= \frac{1}{2} \cdot \Pr_{s,r}[R(r, G(s) \oplus r) = 1] + \frac{1}{2} \cdot (1 - \Pr_{s,r}[R(r, G(s)) = 1]) && (\Pr[\mathcal{E}] = 1 - \Pr[\mathcal{E}^C]) \\
&= 1/2 + \frac{1}{2} \cdot \left(\Pr_{s,r}[R(r, G(s) \oplus r) = 1] - \Pr_{s,r}[R(r, G(s)) = 1] \right) ,
\end{aligned}$$

and by our assumption that R is an ϵ-distinguisher between $(r, G(s))$ and $(r, G(s) \oplus r)$, the right-most term is either at least $\epsilon/2$ or at most $-\epsilon/2$. □

Claim 1.2. $\Pr_{u \in \{0,1\}^n}[D(u) = 1] = 1/2$.

Proof. Note that

$$\begin{aligned}
&\Pr_u[D(u) = 1] = \Pr_{u,b,r}[R(r, u \oplus b \cdot r) = b] && \text{(definition of } D\text{)} \\
&= \frac{1}{2} \cdot \Pr_{r,u}[R(r,u) = 0] + \frac{1}{2} \cdot \Pr_{r,u}[R(r, u \oplus r) = 1] && \text{(law of total probability)} \\
&= \frac{1}{2} \cdot \mathbb{E}_r \left[\Pr_u[R(r,u) = 0]\right] + \frac{1}{2} \cdot \mathbb{E}_r \left[\Pr_u[R(r, u \oplus r) = 1]\right] && \text{(elementary fact)} \\
&= \frac{1}{2} \cdot \mathbb{E}_r \left[\Pr_u[R(r,u) = 0]\right] + \frac{1}{2} \cdot \mathbb{E}_r \left[\Pr_u[R(r,u) = 1]\right] && \text{(see below)} \\
&= \frac{1}{2} \cdot \mathbb{E}_r \left[\Pr_u[R(r,u) = 0] + \Pr_u[R(r,u) = 1]\right] && \text{(linearity of expectation)} \\
&= 1/2\,. && (\Pr[\mathcal{E}] + \Pr[\mathcal{E}^C] = 1)
\end{aligned}$$

The missing claim above that needs justification is that $\Pr_u[R(r, u \oplus r) = 1] = \Pr_u[R(r,u) = 1]$. This follows from the fact that for every fixed $z \in \{0,1\}^n$ we have $\Pr_{r,u}[(r, u \oplus r) = (r,z)] = 1/2^n$ and also $\Pr_{r,u}[(r,u) = (r,z)] = 1/2^n$. □

By combining Claims 1.1 and 1.2, we deduce that

$$\left| \Pr_s[D(G(s)) = 1] - \Pr_{u \in \{0,1\}^n}[D(u) = 1] \right| = \left| \Pr_s[D(G(s)) = 1] - 1/2 \right| \geq \epsilon/2\,,$$

contradicting the PRG conjecture (since $\epsilon(n)/2 \geq 1/\text{poly}(n)$). ■