Problem 1

Let $G : \{0,1\}^n \to \{0,1\}^{2n}$ be pseudorandom generator. Let $s \xleftarrow{\$} \{0,1\}^n, r \xleftarrow{\$} \{0,1\}^{2n}$ and $y = G(s)$. Consider the following $P_{r,y}$:

1. On input $x \in \{0,1\}^n$, check that $G(x) \oplus r = y$.
2. If true: output 1, else output 0.

Show for any PPT $\mathcal{A}$ with input (r, y) and output $x \in \{0,1\}^n$,

$$\Pr\left[P_{r,y}(x) = 1 : x \leftarrow \mathcal{A}(r,y)\right] \leq \nu(n).$$

Solution: Consider the following

$$\begin{aligned}
&\Pr\left[P_{r,y}(x) = 1 : x \leftarrow \mathcal{A}(r,y), r \leftarrow \{0,1\}^{2n}, y \leftarrow G(s), s \leftarrow \{0,1\}^n\right] \\
&= \Pr[G(x) \oplus r = y : x \leftarrow \mathcal{A}(r,y), r \leftarrow \{0,1\}^{2n}, y \leftarrow G(s), s \leftarrow \{0,1\}^n] \\
&= \Pr[G(x) \oplus r = G(s) : x \leftarrow \mathcal{A}(r, G(s)), r \leftarrow \{0,1\}^{2n}, s \leftarrow \{0,1\}^n] \\
&= \Pr[G(x) = r \oplus G(s) : x \leftarrow \mathcal{A}(r, G(s)), r \leftarrow \{0,1\}^{2n}, s \leftarrow \{0,1\}^n] \\
&= \Pr[G(x) = r \oplus a : x \leftarrow \mathcal{A}(r, a), r \leftarrow \{0,1\}^{2n}, a \leftarrow \{0,1\}^{2n}] \\
&= \Pr[G(x) = r \oplus a : x \leftarrow \mathcal{A}(r \oplus a, a), r \leftarrow \{0,1\}^{2n}, a \leftarrow \{0,1\}^{2n}] \\
&= \Pr[G(x) = b : x \leftarrow \mathcal{A}(b, a), b \leftarrow \{0,1\}^{2n}, a \leftarrow \{0,1\}^{2n}] \\
&= \Pr\left[G(x) = G(d) : x \leftarrow \mathcal{A}(G(d), a), d \xleftarrow{\$} \{0,1\}^{2n}, a \xleftarrow{\$} \{0,1\}^{2n}\right] \Pr\left[b \in G(\{0,1\}^{2n}) : b \xleftarrow{\$} \{0,1\}^{2n}\right] \\
&\quad + 0 \cdot \Pr\left[b \notin G(\{0,1\}^{2n}) : b \xleftarrow{\$} \{0,1\}^{2n}\right] \\
&\leq \Pr\left[G(x) = G(d) : x \leftarrow \mathcal{A}(G(d), a), d \xleftarrow{\$} \{0,1\}^{2n}, a \xleftarrow{\$} \{0,1\}^{2n}\right] \\
&= \Pr\left[G(\mathcal{A}(G(d), a)) = G(d) : d \xleftarrow{\$} \{0,1\}^{2n}, a \xleftarrow{\$} \{0,1\}^{2n}\right] \\
&\leq \nu(n)
\end{aligned}$$

since G is a one-way function because its a pseudorandom generator, where $\nu(n)$ is a negligible function. Note in the above we equate $\mathcal{A}(r, a)$ and $\mathcal{A}(r \oplus a, a)$. This is possible as the adversary $\mathcal{A}$ is not actually losing information as it can recover r by $(r \oplus a) \oplus a$. Therefore we have that for any PPT $\mathcal{A}$ with input (r, y) and output $x \in \{0,1\}^n$ we have

$$\Pr\left[P_{r,y}(x) = 1 : x \leftarrow \mathcal{A}(r,y)\right] \leq \nu(n).$$