Problem 2.

Part A. f' is a OWF and we prove by contradiction.

Suppose an adversary $\mathcal{A}'$ could invert f' , we can construct an adversary $\mathcal{A}'$ that invert f . Define $\mathcal{A}(y) = \mathcal{A}'(y \| f(y)) = x$.

$$f'(x) = y \| f(y) \Rightarrow f(x) = y$$

Part B. f' is not necessarily a OWF.

We write $x = x_L \| x_R$ and let f_0 be a length-preserving OWF. Set $f(x) = 0 \dots 0 \| f_0(x_L)$. Then $f'(x) = x_L \| (x_R \oplus f(x_L))$. Adversary gets x_L from the first half of $f'(x)$ and can calculate x_R by XORing $f(x_L)$ and the second half of $f'(x)$.

Part C. f' is not necessarily a OWF.

We write $x = x_L \| x_R$ and let f_0 be an OWF. Set

$$f(x) = \begin{cases} x_L \| f_0(x_R), & \text{if the first bit of } x \text{ is } 0 \\ x_R \| f_0(x_L), & \text{if the first bit of } x \text{ is } 1 \end{cases}$$

Then

$$f'(x) = \begin{cases} x_L \| f_0(x_R) \| x_R \| f_0(x_L), & \text{if the first bit of } x \text{ is } 0 \\ x_R \| f_0(x_L) \| x_L \| f_0(x_R), & \text{if the first bit of } x \text{ is } 1 \end{cases}$$

Adversary can easily read x_L, x_R from $f'(x)$.

Part D. f' is a OWF.

Let $\mathcal{A}'$ be a p.p.t. algorithm try to invert f'.

Define $\mathcal{A}$ such that $\mathcal{A}(y) = G(\mathcal{A}'(y))$. Since f is a OWF,

$$\Pr\left[\mathcal{A}(y) \in f^{-1}(y) : \begin{matrix} r \leftarrow \{0,1\}^{n+1} \\ y = f(r) \end{matrix}\right] = \Pr\left[G(\mathcal{A}'(y)) \in f^{-1}(y) : \begin{matrix} r \leftarrow \{0,1\}^{n+1} \\ y = f(r) \end{matrix}\right] \leq \text{negl}(n)$$

Define D such that, $D(r)$ outputs 1 if and only if $G(\mathcal{A}'(f(r))) \in f^{-1}(f(r))$. Since G is a PRG.

$$\Pr\left[G(\mathcal{A}'(y)) \in f^{-1}(y) : \begin{matrix} s \leftarrow \{0,1\}^{n} \\ y = f(G(s)) \end{matrix}\right] - \Pr\left[G(\mathcal{A}'(y)) \in f^{-1}(y) : \begin{matrix} r \leftarrow \{0,1\}^{n+1} \\ y = f(r) \end{matrix}\right]$$
$$= \Pr_{s \leftarrow \{0,1\}^n}[D(G(s)) \rightarrow 1] - \Pr_{r \leftarrow \{0,1\}^{n+1}}[D(r) \rightarrow 1] \leq \text{negl}(n)$$

Then $\mathcal{A}'$ can not invert f' with non-negligible probability, because

$$\Pr\left[\mathcal{A}'(y) \in (f')^{-1}(y) : \begin{matrix} s \leftarrow \{0,1\}^{n} \\ y = f'(s) \end{matrix}\right] = \Pr\left[G(\mathcal{A}'(y)) \in f^{-1}(y) : \begin{matrix} s \leftarrow \{0,1\}^{n} \\ y = f(G(s)) \end{matrix}\right] \leq \text{negl}(n).$$

Part E. f' is not necessarily a OWF.

Consider a PRG g with stretch $\ell(n) = 2n + 1$. Let $f(x_L \| x_R) = f_0(x_L) \| 0 \dots 0$ and $G(x_L \| x_R) = g(x_R)$. Then $f'(x) = G(f(x)) = g(0 \dots 0)$, so any x is an inverse.

Part F. f' is a OWF.

The inputs who has $\log n$ tailing 0's make up of $\frac{1}{n}$ fraction of the inputs. If the adversary inverts with non-negligible probability conditioning on the input is sampled from this fraction, it can invert with non-negligible probability without the conditioning.

Part G. f is not necessarily a OWF.

Suppose $x = x_L \| x_R$ (here $|x_L| = \lceil n/2 \rceil$, $|x_R| \leq \lfloor n/2 \rfloor$). Set f as

$$f(x) = \begin{cases} x_L \| 0^{\lfloor n/2 \rfloor}, & \text{if } x_R = 0\dots0 \\ f_0(x_L) \| 0^{\lfloor n/2 \rfloor - 1}1, & \text{if } x_R \neq 0\dots0 \end{cases}$$

f is a OWF. The difficulty of inverting f is essentially the same as inverting f_0.

However, f' is not a OWF. The output y always has $n/2 - \log n$ tailing 0's, appending $\log n$ more 0's to y yields an inverse of y.

Problem 3.

Part A. When $f(\hat{x}_1) = f(x_1), \ldots, f(\hat{x}_m) = f(x_m)$, we say $\mathcal{A}'$ succeeds.

$$\begin{aligned}
&\Pr[f(\hat{x}_1) = f(x_1) \ldots f(\hat{x}_m) = f(x_m)] \\
&= \Pr[\text{every } x_i \text{ is ``good'' and } \mathcal{A}' \text{ succeeds}] + \Pr[\text{exists } x_i \text{ is ``bad'' and } \mathcal{A}' \text{ succeeds}] \\
&\le (\Pr[x \text{ is ``good''}])^m + \sum_i \Pr[x_i \text{ is ``bad'' and } \mathcal{A}' \text{ succeeds}] \\
&\le (\Pr[x \text{ is ``good''}])^m + \sum_i \Pr\big[\mathcal{A}' \text{ succeeds} \bigm| x_i \text{ is ``bad''}\big]
\end{aligned}$$

By our definition of $\mathcal{A}$

$$\begin{aligned}
\Pr_{x \leftarrow \{0,1\}^n}\big[\mathcal{A} \text{ inverts } f(x) \bigm| x \text{ is ``bad''}\big] &\ge \Pr_{\substack{i \leftarrow \{1,\ldots,m\} \\ x \leftarrow (\{0,1\}^n)^m}}\big[\mathcal{A}' \text{ succeeds} \bigm| x_i \text{ is ``bad''}\big] \\
&= \frac{1}{m} \sum_{i=1}^{m} \Pr_{x \leftarrow (\{0,1\}^n)^m}\big[\mathcal{A}' \text{ succeeds} \bigm| x_i \text{ is ``bad''}\big]
\end{aligned}$$

By the definition of "bad",

$$\sum_i \Pr\big[\mathcal{A}' \text{ succeeds} \bigm| x_i \text{ is ``bad''}\big] \le m \Pr_{x \leftarrow \{0,1\}^n}\big[\mathcal{A} \text{ inverts } f(x) \bigm| x \text{ is ``bad''}\big] \le \frac{m}{r(n)},$$

which implies a stronger statement than what is required.

Part B. For infinitely many n,

$$(\Pr[x \text{ is ``good''}])^m \ge \frac{1}{p(n)} - \frac{m^2}{r(n)}.$$

Thus for each of such n,

$$\Pr[x \text{ is ``bad''}] = 1 - \Pr[x \text{ is ``good''}] \le 1 - \left(\frac{1}{p(n)} - \frac{m^2}{r(n)}\right)^{\frac{1}{m}}.$$

Set $r(n)$ so that $\frac{m^2}{r(n)} \le \frac{1}{2p(n)}$. Set $m(n)$ so that $1 - (\frac{1}{2p(n)})^{1/m} \le \frac{1}{2q(n)}$. Concretely, we can let

$$m(n) = nq(n) \qquad r(n) = 2p(n)m^2(n) = 2np(n)q^2(n).$$

Then

$$1 - \left(\frac{1}{p(n)} - \frac{m^2}{r(n)}\right)^{\frac{1}{m}} \le \frac{1}{2q(n)}$$

for any sufficiently large n.

Part C. For infinitely many n,

$$\begin{aligned}
&\Pr[\mathcal{A}_{\text{repeat}}(f(x)) \in f^{-1}(f(x))] \\
&\ge \Pr[x \text{ is ``good'' and } \mathcal{A}_{\text{repeat}}(f(x)) \in f^{-1}(f(x)) \\
&= \Pr[\mathcal{A}_{\text{repeat}}(f(x)) \in f^{-1}(f(x)) | x \text{ is ``good''}] \Pr[x \text{ is ``good''}] \\
&\ge \left(1 - \left(1 - \frac{1}{r(n)}\right)^{n \cdot r(n)}\right)\left(1 - \frac{1}{2q(n)}\right) \\
&= (1 - \text{negl}(n))\left(1 - \frac{1}{2q(n)}\right)
\end{aligned}$$

Problem 4.

We use the standard Goldreich-Goldwasser-Micali construction of PRF, which is based on a PRG $G : \{0,1\}^\lambda \to \{0,1\}^{2\lambda}$. Let G_0, G_1 denote the first and second half of G respectively, i.e., $G(s) = G_0(s) \| G_1(s)$. For each $x \in \{0,1\}^*$, define G_x recursively as

$$\begin{aligned} G_\varepsilon(s) &= s \qquad \text{here } \varepsilon \text{ denotes the empty string} \\ G_x(s) &= G_{x_n}(G_{x_{1:n-1}}(s)) \qquad \text{if } |x| = n \end{aligned}$$

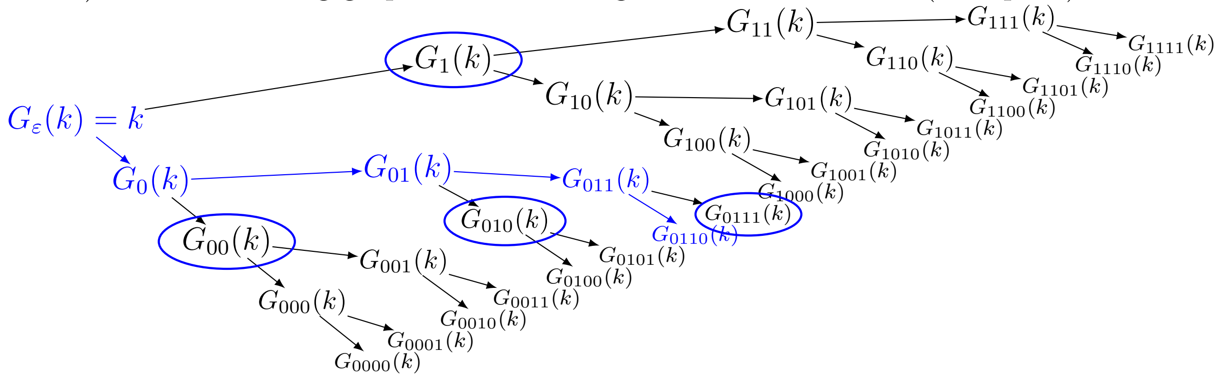
We know the following $F : \{0,1\}^\lambda \times \{0,1\}^\lambda \to \{0,1\}^\lambda$ is a PRF

$$F(k, x) := G_x(k) = G_{x_\lambda}(G_{x_{\lambda-1}}(\dots G_{x_2}(G_{x_1}(k)) \dots)).$$

The punctured key and the $\mathsf{puncture}$ function are defined as

$$\begin{aligned} k_{-x} = \mathsf{puncture}(k, x) &:= (G_{x_{1:i-1}\|(1-x_i)}(k))_{i=1}^{\lambda} \\ &= (G_{1-x_1}(k), G_{x_1\|(1-x_2)}(k), G_{x_{1:2}\|(1-x_3)}(k), \dots, G_{x_{1:\lambda-1}\|(1-x_\lambda)}(k)). \end{aligned}$$

As illustrated in the following graph, the punctured key consists of all the roots (circled nodes) of the remaining graph after removing all the ancestor of x (blue path).



Function $\mathsf{eval}(k_{-x}, x')$ is supposed to evaluate $F(k, x)$ given k_{-x} and $x' \neq x$. Let t be the first index such that $x_t \neq x'_t$, note that $G_{x'_{1:t}}(k)$ is in k_{-x},

$$\mathsf{eval}(k_{-x}, x') = G_{x'_{t+1:\lambda}}(G_{x'_{1:t}}(k)).$$

Since G is PRG, the joint distribution of $(k_{-x}, F_k(x))$ is indistinguishable from uniform. Intuitively,

$$\begin{aligned} &k \text{ is uniform} \implies (G_{1-x_1}(k), G_{x_1}(k)) \text{ is indistinguishable from uniform} \\ &\implies (G_{1-x_1}(k), G_{x_1\|(1-x_2)}(k), G_{x_{1:2}}(k)) \text{ is indistinguishable from uniform} \\ &\quad \vdots \\ &\implies (G_{1-x_1}(k), \dots, G_{x_{1:\lambda-1}\|(1-x_\lambda)}(k), G_{x_{1:\lambda}}(k)) \text{ is indistinguishable from uniform} \\ &\iff k_{-x}, F(k, x)) \text{ is indistinguishable from uniform} \end{aligned}$$

This can be formalized by a hybrid argument. There are $\lambda + 1$ hybrids $H_0, \dots, H_\lambda$.

- H_0 is the real world, where distinguisher receives $(k_1, \dots, k_\lambda, y) = (k_{-x}, F(k, x))$
- H_λ is the ideal world, where $(k_1, \dots, k_\lambda, y)$ are i.i.d. uniform.
- In hybrid H_i, $k_1, \dots, k_i, k$ are uniform and let $k_j = G_{x_{i+1:j-1}\|(1-x_j)}(k), y = G_{x_{i+1:\lambda}}(k)$.

If a p.p.t. distinguisher can tell H_0, H_λ apart, it distinguishes a pair of adjacent hybrid with non-negligible advantage, which leads to any distinguisher that breaks PRG G.

Problem 5.

The distinguisher performs the following tests. The given candidate PRF will always pass the tests, but a random function will fail the tests with overwhelming probability.

Part A Given oracle access to $\mathcal{O}(\cdot) = F(k, \cdot)$, the distinguisher checks if $\mathcal{O}(x) = \mathcal{O}(0) \oplus x$ for an arbitrarily chosen $x \neq 0$.

Part B Given oracle access to $\mathcal{O}(\cdot) = F(k, \cdot)$, the distinguisher checks if $\mathcal{O}(x) \oplus \mathcal{O}(0) = F(k', x) \oplus F(k', 0)$ for arbitrarily chosen $x \neq 0$ and k'.

Part C Let $e_1, \ldots, e_n$ be the natural basis of $\{0,1\}^n$. Given oracle access to $\mathcal{O}(\cdot) = F(k, \cdot)$, the distinguisher checks if

$$\begin{bmatrix} \mathcal{O}(x_1) \\ \vdots \\ \mathcal{O}(x_m) \end{bmatrix} \text{ is in the column span of } \begin{bmatrix} F(e_1, x_1) & \cdots & F(e_n, x_1) \\ \vdots & \ddots & \vdots \\ F(e_1, x_m) & \cdots & F(e_n, x_m) \end{bmatrix}$$

for arbitrarily chosen distinct $x_1, \ldots, x_m$ $(m > n)$.