Problem 1.

W.l.o.g., assume $\ell(n) = n + 1$. Define $G' : \{0,1\}^* \to \{0,1\}^*$ as

$$\forall s \in \{0,1\}^n, G'(s) = G(s_{1:m}) \| s_{m+1:n}$$

where $m = m(n) = \max\{m : m \in \mathcal{I}, m \leq n\}$. In particular, if $n \in \mathcal{I}$, then $G'(s) = G(s)$ for all $s \in \{0,1\}^n$. We prove that G' is a PRG.

First show that G' is polynomial-time computable. By the polynomial-time enumerability of $\mathcal{I}$, the set $\{m : m \in \mathcal{I}, m \leq n\}$ can be computed in $\text{poly}(n)$ time. Thus $m = m(n)$ can be computed in $\text{poly}(n)$ time.

It remains to prove the indistinguishability. For any p.p.t. distinguisher $\mathcal{D}'$ and any integer n,

$$\begin{aligned}
&\left| \Pr_{s \leftarrow \{0,1\}^n} \left[D'(G'(s)) \to 1 \right] - \Pr_{r \leftarrow \{0,1\}^{n+1}} [D'(r) \to 1] \right| \\
= &\left| \Pr_{\substack{s \leftarrow \{0,1\}^{m(n)} \\ z \leftarrow \{0,1\}^{n-m(n)}}} \left[D'(G(s)\|z) \to 1 \right] - \Pr_{\substack{r \leftarrow \{0,1\}^{m+1} \\ z \leftarrow \{0,1\}^{n-m(n)}}} [D'(r\|z) \to 1] \right| \\
= &\left| \Pr_{s \leftarrow \{0,1\}^m} \left[D'(G(s)) \to 1 \right] - \Pr_{r \leftarrow \{0,1\}^{m+1}} [D'(r) \to 1] \right| \\
\leq &\ \text{negl}(m) = \text{negl}(n)
\end{aligned}$$

Remark: There is a flaw in the above informal proof. Formally, the proof is a reduction. If there is a distinguisher $\mathcal{D}'$ that distinguishes the output of G' from uniform with non-negligible advantage, then the reduction provides another distinguisher $\mathcal{D}$ that distinguishes the output of G from uniform with non-negligible advantage. But in the "fake proof", the reduction from $\mathcal{D}$ to $\mathcal{D}'$ is not explicit. $\mathcal{D}$ does not know how many random bits should be appended.

Problem 2.

Part A. G' is not necessarily a PRG.

Consider a PRG G such that the first bit of $G(s)$ always equals s_1. The existence of such PRG is guaranteed by part B. Then G' always outputs a string leading by 0, thus is not a PRG.

Part B. G' is not necessarily a PRG.

Let $\ell(n) = n + 1$, then G' is length-preserving.

Part C. G' is not necessarily a PRG.

Let $H : \{0,1\}^n \to \{0,1\}^{\ell(n+1)-1}$ be a PRG. Consider G defined as $G(s) = H(s_{1:n-1})\|s_n$ for any $s \in \{0,1\}^n$. By an argument similar to part B, G is a PRG. For any $s \in \{0,1\}^n$, the last bit of s and the last bit of $s+1$ differ. So the $(n+1)$-th bit of $G'(s)$ and the $(2n+2)$-th bit of $G'(s)$ always differ. Thus $G'(s)$ is not a PRG.

Part D. G' is a PRG.

For any p.p.t. distinguisher D,

$$\begin{aligned}
&\left|\Pr_{s\leftarrow\{0,1\}^n}[D(G'(s)) \to 1] - \Pr_{r\leftarrow\{0,1\}^{\ell(\ell(n))}}[D(r) \to 1]\right| \\
&= \left|\Pr_{s\leftarrow\{0,1\}^n}[D(G_1(G_2(s))) \to 1] - \Pr_{r\leftarrow\{0,1\}^{\ell(\ell(n))}}[D(r) \to 1]\right| \\
&\le \left|\Pr_{s\leftarrow\{0,1\}^n}[D(G_1(G_2(s))) \to 1] - \Pr_{u\leftarrow\{0,1\}^{\ell(n)}}[D(G_1(u)) \to 1]\right| \\
&\quad + \left|\Pr_{u\leftarrow\{0,1\}^{\ell(n)}}[D(G_1(u)) \to 1] - \Pr_{r\leftarrow\{0,1\}^{\ell(\ell(n))}}[D(r) \to 1]\right|
\end{aligned}$$

is negligible because

$$\left|\Pr_{s\leftarrow\{0,1\}^n}[D(G_1(G_2(s))) \to 1] - \Pr_{u\leftarrow\{0,1\}^{\ell(n)}}[D(G_1(u)) \to 1]\right| \le \mathrm{negl}(n)$$

(otherwise, G_2 is not PRG) and

$$\left|\Pr_{u\leftarrow\{0,1\}^{\ell(n)}}[D(G_1(u)) \to 1] - \Pr_{r\leftarrow\{0,1\}^{\ell(\ell(n))}}[D(r) \to 1]\right| \le \mathrm{negl}(n)$$

(otherwise, G_1 is not a PRG).

Part E. G' is not necessarily a PRG.

To construct a counterexample, let $H : \{0,1\}^n \to \{0,1\}^{\ell(n+1)-1}$ be a PRG. Define G_0 and G_1 as

$$G_0(s) = s_1\|H(s_{2:n}) \qquad\qquad G_1(s) = \bar{s}_1\|H(s_{2:n})$$

for any $s \in \{0,1\}^n$. Similar to the argument in part B, G_0, G_1 are PRGs. However,

$$G'(s) = G_{s_1}(s) = 0\|H(s_{2:n}).$$

The first output bit is always zero.

Part F. G' is a PRG.

The intuition is that the first bit only tells the adversary which PRG is used, the chosen PRG is fed with fresh randomness that are completely hidden from the distinguisher.

For any PPT distinguisher D, define two distinguishers D_0, D_1 as $D_0(r) = D(0\|r)$ and $D_1(r) = D(1\|r)$.

$$\begin{aligned}
&\Pr_{s\leftarrow\{0,1\}^n}\big[D(s_1\|G_{s_1}(s_{2:n}))\to 1\big] - \Pr_{r\leftarrow\{0,1\}^{\ell(n-1)+1}}[D(r)\to 1]\\
&= \frac{1}{2}\Big(\Pr_{s\leftarrow\{0,1\}^{n-1}}\big[D(0\|G_0(s))\to 1\big] - \Pr_{r\leftarrow\{0,1\}^{\ell(n-1)}}[D(0\|r)\to 1]\Big)\\
&\quad + \frac{1}{2}\Big(\Pr_{s\leftarrow\{0,1\}^{n-1}}\big[D(1\|G_1(s))\to 1\big] - \Pr_{r\leftarrow\{0,1\}^{\ell(n-1)}}[D(1\|r)\to 1]\Big)\\
&= \frac{1}{2}\Big(\Pr_{s\leftarrow\{0,1\}^{n-1}}\big[D_0(G_0(s))\to 1\big] - \Pr_{r\leftarrow\{0,1\}^{\ell(n-1)}}[D_0(r)\to 1]\Big)\\
&\quad + \frac{1}{2}\Big(\Pr_{s\leftarrow\{0,1\}^{n-1}}\big[D_1(G_1(s))\to 1\big] - \Pr_{r\leftarrow\{0,1\}^{\ell(n-1)}}[D_1(r)\to 1]\Big)\\
&= \mathrm{negl}(n-1) + \mathrm{negl}(n-1) = \mathrm{negl}(n).
\end{aligned}$$

Part G. G' is not necessarily a PRG.

The distinguisher D is constructed as follows: The distinguisher only reads the $\ell(\lfloor\log n\rfloor)$-bit prefix, can checks if the prefix belongs to

$$\{G_1(s)|s\in\{0,1\}^{\lfloor\log n\rfloor}\}.$$

The prefix of the output of G' always lies in the above mentioned set. While the prefix of a random string lies in the above mentioned set with probability at most $1/2$.

Problem 3.

Part B. A function G is a *non-uniform* PRG if

- G is polynomial-time computable;
- there is a stretch function $\ell : \mathbb{N} \to \mathbb{N}$ such that $\ell(n) > n$ and $|G(x)| = \ell(|x|)$,
- for any family $\{C_n\}_{n\in\mathbb{N}}$ of polynomial-size circuits, there exists a negligible function negl such that

$$\left| \Pr_{s\leftarrow\{0,1\}^n}[C_n(G(s)) = 1] - \Pr_{r\leftarrow\{0,1\}^{\ell(n)}}[C_n(r) = 1] \right| \le \mathrm{negl}(n).$$

The last bullet has an equivalent expression

- for any p.p.t. distinguisher D and any infinite sequence of poly-length advice strings $\{a_n\}_{n\in\mathbb{N}}$, there exists a negligible function negl such that

$$\left| \Pr_{s\leftarrow\{0,1\}^n}[D(a_n, G(s)) = 1] - \Pr_{r\leftarrow\{0,1\}^{\ell(n)}}[D(a_n, r) = 1] \right| \le \mathrm{negl}(n).$$

Part A. Since $\mathcal{L} \in \mathbf{BPP}$, there exists a p.p.t. Turing machine M such that

$$x \in \mathcal{L} \implies \Pr[M(x) \to 1] \ge \frac{5}{6} \qquad x \notin \mathcal{L} \implies \Pr[M(x) \to 1] \le \frac{1}{6}.$$

Let G be a non-uniform PRG with sufficient stretch. Define p.p.t. Turing machine M' as

> On input $x \in \{0,1\}^n$, $M'(x)$ samples a random string $s \in \{0,1\}^n$, emulates the execution of $M(x)$ where the random tape is replace by $G(s)$, outputs what $M(x)$ outputs.

We claim that M and M' do not differ significantly for any sufficiently long input. There exists $N \in \mathbb{N}$ such that for all $n > N$, for all $x \in \{0,1\}^n$,

$$x \in \mathcal{L} \implies \Pr[M'(x) \to 1] \ge \frac{2}{3} \qquad x \notin \mathcal{L} \implies \Pr[M'(x) \to 1] \le \frac{1}{3},$$

because G is a non-uniform PRG. To prove the claim, consider advice strings $\{x_n\}_{n\in\mathbb{N}}$

$$x_n = \arg\max_{x\in\{0,1\}^n} \left| \Pr[M'(x) \to 1] - \Pr[M(x) \to 1] \right|,$$

and define a non-uniform distinguisher D using $\{x_n\}_{n\in\mathbb{N}}$ as advice

> Given advice string $x_n \in \{0,1\}^n$ and $r \in \{0,1\}^{\ell(n)}$, the distinguisher computes $b' = M(x_n, r)$, using r as the random tape, and outputs b.

Then

$$\begin{aligned}
&\left| \Pr_{s\leftarrow\{0,1\}^n}[D(x_n, G(s)) \to 1] - \Pr_{r\leftarrow\{0,1\}^{\ell(n)}}[D(x_n, r) \to 1] \right| \\
&= \left| \Pr[M'(x_n) \to 1] - \Pr[M(x_n) \to 1] \right| \\
&= \max_{x\in\{0,1\}^n} \left| \Pr[M'(x) \to 1] - \Pr[M(x) \to 1] \right| = \mathrm{negl}(n).
\end{aligned}$$

In particular, if n is sufficiently large, the difference is bounded by $1/6$.

Incorporating the finitely many "bad" inputs into M'. Define M'' such that M'' remembers the truth-table for all inputs of length at most N. For longer inputs, M'' lets M' compute the outcome.

Problem 4.

Construct the following distinguisher D:

> On input $r \in \{0,1\}^{\lambda+1}$, samples random $i \in \{1, 2, \ldots, \ell(\lambda) - \lambda\}$, samples random prefix $u \in \{0,1\}^{i-1}$, outputs the outcome of
>
> $$D'(G_{\ell(\lambda)-\lambda-1}(\ldots G_{i+1}(G_i(u\|r))\ldots)).$$

$$
\begin{aligned}
&\Pr_{s\in\{0,1\}^\lambda}[D(G(s)) \to 1] - \Pr_{r\in\{0,1\}^{\lambda+1}}[D(r) \to 1] \\
&= \frac{1}{\ell(\lambda)-\lambda} \sum_{i=1}^{\ell(\lambda)-\lambda} \Pr_{\substack{s\in\{0,1\}^\lambda \\ u\in\{0,1\}^{i-1}}} [D'(G_{\ell(\lambda)-\lambda-1}(\ldots G_{i+1}(G_i(u\|G(s)))\ldots)) \to 1] \\
&\quad - \frac{1}{\ell(\lambda)-\lambda} \sum_{i=1}^{\ell(\lambda)-\lambda} \Pr_{\substack{r\in\{0,1\}^{\lambda+1} \\ u\in\{0,1\}^{i-1}}} [D'(G_{\ell(\lambda)-\lambda-1}(\ldots G_{i+1}(G_i(u\|r))\ldots)) \to 1] \\
&= \frac{1}{\ell(\lambda)-\lambda} \sum_{i=1}^{\ell(\lambda)-\lambda} \Pr_{u\in\{0,1\}^{\lambda+i-1}} [D'(G_{\ell(\lambda)-\lambda-1}(\ldots G_{i+1}(G_i(G_{i-1}(u)))\ldots)) \to 1] \\
&\quad - \frac{1}{\ell(\lambda)-\lambda} \sum_{i=1}^{\ell(\lambda)-\lambda} \Pr_{u\in\{0,1\}^{\lambda+i}} [D'(G_{\ell(\lambda)-\lambda-1}(\ldots G_{i+1}(G_i(u))\ldots)) \to 1] \\
&= \frac{1}{\ell(\lambda)-\lambda} \Big(\Pr_{u\leftarrow\{0,1\}^\lambda} [D'(G'(u)) \to 1] - \Pr_{u\leftarrow\{0,1\}^{\ell(\lambda)}} [D'(u) \to 1] \Big)
\end{aligned}
$$

Problem 5.

Let $F' : \{0,1\}^\lambda \times \{0,1\}^n \to \{0,1\}^\lambda$ be a secure PRF. Construct F as

$$F(k,x) = \begin{cases} F'(k,0), & \text{if } x = 0 \\ F'(k,x) \oplus F'(k,x-1), & \text{otherwise} \end{cases}$$

Then $\text{psum}(k,x) = F(k',x)$.

To show that F is PRF, consider the following hybrids.

- In the real world, the distinguish has oracle access to $F(k,\cdot)$.
- In the ideal world, the distinguish has oracle access to a random function $f(\cdot)$.
- Define a hybrid world, the distinguish has oracle access to

$$g(x) = \begin{cases} f(0), & \text{if } x = 0 \\ f(x) \oplus f(x-1), & \text{otherwise} \end{cases}$$

  where f is a randomly sampled function.

The hybrid world is indistinguishable from the ideal world, because their distributions are identical. The hybrid world is indistinguishable from the real world, due to security of F'.