1. Let G and F be PRGs with expansion factor $l(n)=2n$

World 0: We generate a n-bit random seed s and are given $F(G(s))$

World 1: We are given a uniform bit string r of length 4n.

Let D be a PPTA distinguisher, which outputs 1 if it thinks it is in World 0.

Intermediate world: World I. In this world, we generate a 2n-bit random string z and provide $F(z)$ to the distinguisher.

Difference between world 1 and I

Since F is a PRG, by definition,

$$|Pr[D(r)=1]-Pr[D(F(z))=1]| \leq negl_1(n)$$

Difference between world I and 0

Let $D'=D\circ F$. Since F runs in polynomial time, so does D'

Since D is a distinguisher, so does D'. By definition,

$$|Pr[D'(z)=1]-Pr[D'(G(s))=1]| \leq negl_2(n)$$

which is equivalent to

$$|Pr[D(F(z))=1]-Pr[D(F(G(s)))=1] \leq negl_2(n)$$

Using $|a-c|+|c-b| \geq |a-b|$

$$|Pr[D(r)=1]-Pr[D(F(G(s)))=1]| \leq |Pr[D(r)=1]-Pr[D(F(z))=1]| + |Pr[D(F(z))=1]-Pr[D(F(G(s)))=1] = negl_1(n)+negl_2(n) = negl(n)$$

Since $|Pr[D(r)=1]-Pr[D(F(G(s)))=1] \leq negl(n)$,

$F\circ G$ is a PRG.

2. (F, G) is not a PRG. Here is a counter example:
Let $F = G$ and their expansion factor be $l(n) = 2n$.
For input string $w = (w_1, w_2) \in \{0,1\}^{4n}$, define a distinguisher D such that

$$D(w) = \begin{cases} 1 & \text{if } w_1 = w_2 \\ 0 & \text{if } w_1 \neq w_2 \end{cases}$$

Thus $D((F(s), G(s))) = 1$ and
for a uniform random string $r \in \{0,1\}^{4n}$

$$D(r) = \frac{2^{2n}}{2^{4n}} = \frac{1}{2^{2n}}$$

$|Pr[D((F(s), G(s))) = 1] - Pr[D(r) = 1]| = 1 - \frac{1}{2^{2n}}$, which is not negligible.

3(a) Since G is a PRG,

$$|Pr[D(G(s)) = 1] - Pr[D(r) = 1]| \leq negl(n)$$

Let $r \in \{0,1\}^{\frac{n}{2}}$ be a uniform random string. Rewrite the above equation:

$$|Pr[D(G'(s)) = 1] - Pr[D(r') = 1] \leq negl(\tfrac{n}{2})$$

Since $negl(n)$ is negligible, so is $negl(\frac{n}{2})$
Thus G' is a PRG.

3(b) Define H to be a PRG with $l(n) = 6n$. and $G(s_1 || s_2) = H(s_1)$ with $l(n) = 3n$
G is also a PRG.
$G'(s) = G(0^{|s|} || s) = H(0^{|s|})$
Define a distinguisher D such that

$$D(w) = \begin{cases} 1 & \text{if } w = H(0^n) \\ 0 & \text{if } w \neq H(0^n) \end{cases}$$

$$|Pr[D(G'(s))=1] - Pr[D(w)=1]| = 1 - \frac{1}{2^{6n}}$$

which is not negligible.

Thus G' is not a PRG

3(c) Define H to be a PRG with $l(n) = 2n+2$ ($\{0,1\}^{n-1} \to \{0,1\}^{2n}$)

and $G(s) = H(s_1 \cdots s_{n-1})$

G is also a PRG.

If the last bit of s is 0, then

$$G'(s) = G(s) \| G(s+1) = H(s_1 \cdots s_{n-1}) \| H(s_1 \cdots s_{n-1})$$

Since the seed is uniform, the last bit has $\frac{1}{2}$ probability to be 0.

Define a distinguisher D such that on input $w = (w_1, w_2)$

$$D(w) = \begin{cases} 1 & \text{if } w_1 = w_2 \\ 0 & \text{if } w_1 \neq w_2. \end{cases}$$

$$|Pr[D(G'(s))=1] - Pr[D(r)=1]| = \frac{1}{2} - \frac{1}{2^n}$$

which is not negligible.

Thus G' is not a PRG.

4. Let $e_i = [0, 0 \cdots 1 \cdots 0]'$ be a column vector such that all the entries are 0s and the ith entry is 1.

Define a distinguisher D and let D do the following

D queries the oracle with $[0, 0 \cdots 0]', e_1, e_2 \cdots e_n$.

D recovers A and b because $b = O([0, 0 \cdots 0]')$ and

$a_i = O(e_i) - b$ where a_i is the ith column of A.

D queries the oracle with a new string x. Let $y = O(x)$

$$D(x) = \begin{cases} 1 & \text{if } y = Ax+b \\ 0 & \text{if } y \neq Ax+b \end{cases}$$

D only performs $n+2$ queries, so it is PPTA.

If $O = F_{A,b}$, D outputs 1. If $O = f$, $f \in Func_n$, the probability that $f(x) = Ax+b$ is $\frac{(2^n)^{2^n-1}}{(2^n)^{2^n}} = \frac{1}{2^n}$

$$\left| Pr[D^{F_k(\cdot)}(1^n)=1] - Pr[D^{f(\cdot)}(1^n)=1] \right| = 1 - \frac{1}{2^n}$$

which is not negligible.

Thus. F is not a PRF.