证明：

定义如下三个实验：

EXP(0)：　　$r=G_2(s)=G(s_1)||G(s_2)$

EXP(0.1)：　$r=r_1||G(s_2), r_1 \overset{R}{\leftarrow} \{0,1\}^n$

EXP(1)：　　$r=r_1||r_2, r_1, r_2 \overset{R}{\leftarrow} \{0,1\}^n$

(1) 假设存在算法 A 能区分 EXP(0)和 EXP(0.1)，若 A(r)=0，则表示 A 的参数 r 来自 EXP(0)中的串；若 A(r)=1，则表示 A 的参数 r 来自 EXP(0.1)中的串

我们可以通过算法 A 来构造一个算法 B，算法 B 可以用来区分 G(s)和真随机，给定 r_1' 作为 B 的输入，其中 $r_1' \in \{0,1\}^n$，对应 EXP(0)或 EXP(0.1)中前 n 位的字符串，然后进行接下来的操作：

① 令 $r_2'=G(s_2)$，$s_2 \leftarrow K$，K 为密钥空间，$r_2' \in \{0,1\}^n$

② Call　Alg. $A(r_1'||r_2')$

③ 若 $A(r_1'||r_2')=0$，则返回 0，表示 r_1' 为 G(s)；否则返回 1，表示 r_1' 为真随机

$$\boxed{Adv_{PRG}[G,B]=Adv_{PRG}[G_2,A]=|\Pr[EXP(0)=1]-\Pr[EXP(0.1)=1]|>\varepsilon\ (\varepsilon \text{ 不可忽略})}$$

因此 G(s)为一个不安全的 PRG，与已知相矛盾，假设不成立，所以 EXP(0)和 EXP(0.1)不可区分

(2) 假设存在算法 A 能区分 EXP(0.1)和 EXP(1)，若 $A'(r)=0$，则表示 A′ 的参数 r 来自 EXP(0.1)中的串；若 $A'(r)=1$，则表示 A′ 的参数 r 来自 EXP(1)中的串

我们可以通过算法 A′ 来构造一个算法 B′，算法 B′ 可以用来区分 G(s)和真随机，给定 r_2' 作为 B 的输入，其中 $r_2' \in \{0,1\}^n$，对应 EXP(0.1)或 EXP(1)中后 n 位的字符串，然后进行接下来的操作：

① 令 $r_1'=G(s_1)$，$s_1 \leftarrow K$，K 为密钥空间，$r_1' \in \{0,1\}^n$

② Call　Alg. $A(r_1'||r_2')$

③ 若 $A(r_1'||r_2')=0$，则返回 0，表示 r_2' 为 G(s)；否则返回 1，表示 r_2' 为真随机

$$\boxed{Adv_{PRG}[G,B']=Adv_{PRG}[G_2,A']=|\Pr[EXP(0.1)=1]-\Pr[EXP(1)=1]|>\varepsilon\ (\varepsilon \text{ 不可忽略})}$$

因此 G(s)为一个不安全的 PRG，与已知相矛盾，假设不成立，所以 EXP(0.1)和 EXP(1)不可区分

根据(1)和(2)中的结论以及不可区分的传递性得，EXP(0)和 EXP(1)不可区分，因此 $G_2(s)$是一个安全的 PRG。