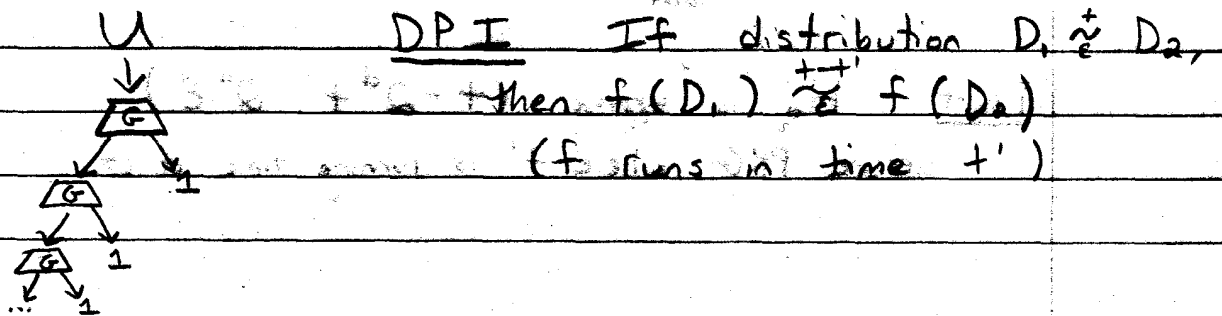
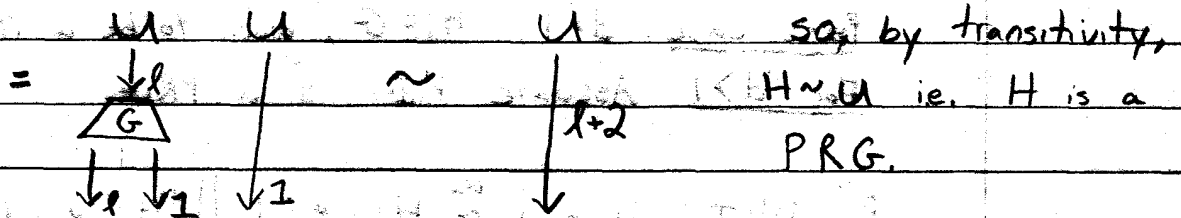
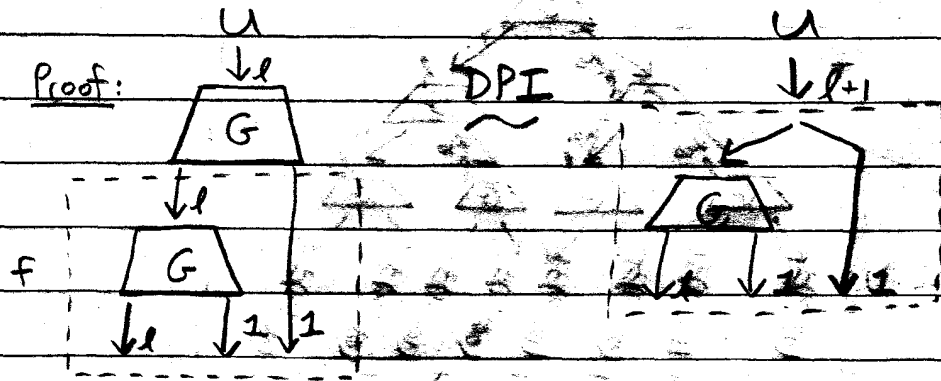


Suppose $G: \{0, 1\}^l \rightarrow \{0, 1\}^{l+1}$ is PRG
 Then we can build a PRG as follows:



$$G \circ U_d \sim U_{d+1}$$

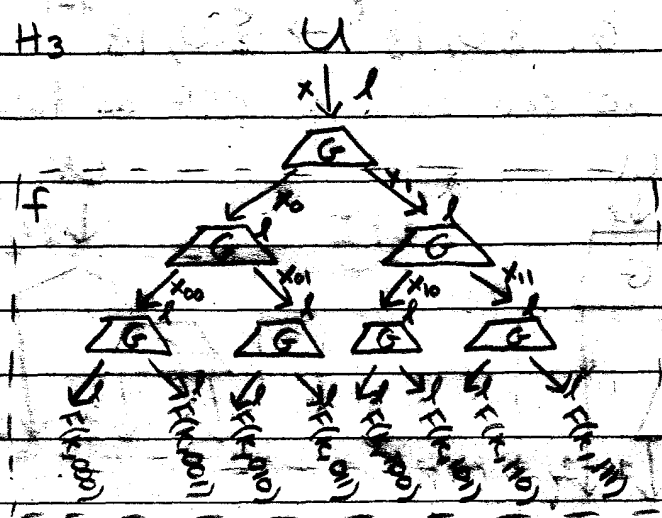
$$f \circ G \circ U_d \sim f \circ U_{d+1}$$

Goldreich - Goldwasser - Micali (GGM) construction -

If G is a secure PRG

$$G: \{0,1\}^l \rightarrow \{0,1\}^{2l}$$

Then H_d is a secure PRG.



Proof (by induction on d)

Base case: $d=1$, $H_1 = G$, given to be a PRG

For $d > 1$ Assume H_{d-1} is a PRG

$$\text{By DPI, } H_d \circ U \stackrel{\text{DPI}}{\sim} H_{d-1} \circ U \parallel H_{d-1} \circ U$$

$$\stackrel{\text{IHOP}}{\sim} U$$

concat

Fact: H_d is approx. $(t - 2^d t', 2^d \epsilon)$

secure PRG, where t' is running time of G

Pseudo - Random Functions

$F(k, p) = x_p$ from leaves of $H_d(k)$

$F: \text{keys} \times \{0, 1\}^d \rightarrow \{0, 1\}^l$;

$R \stackrel{\$}{\leftarrow} \text{Functions} (\{0, 1\}^d \rightarrow \{0, 1\}^l)$

If $x \neq y$, then $R(x)$ and $R(y)$ are independent

Question: Can you distinguish $F_k = F(k, \cdot)$, $k \stackrel{\$}{\leftarrow} U$, from R ?

Theorem: F is a pseudo-random function (family) if H_d is.

"Proof": Suppose adversary A can distinguish F_k ; $k \stackrel{\$}{\leftarrow} U$ from R by making queries on P_1, \dots, P_q .

Then $A'(x) =$ ① break x into y_1, \dots, y_{q-1}

② run A , but whenever A makes a

call to its black box on input P_i , return y_i

Can distinguish H_d from U .

Defn: Let $F: \text{keys} \times X \rightarrow Y$. For algorithm A ,

$\text{Adv } A = \left| \Pr [A^{F_k} = 1; k \stackrel{\$}{\leftarrow} U] - \right.$

$\left. \Pr [A^R = 1; R \stackrel{\$}{\leftarrow} \text{Functions} (X \rightarrow Y)] \right|$

Def: F is a (t, q, ϵ) secure PRF if $\forall A$ running in time t and making at most q oracle queries, $\text{Adv } A \leq \epsilon$