From PRG to PRF

Define: A collection of functions
\[ \exists x \in \mathbb{R}^n : \exists K \in \mathbb{R}^{n \times m} \times \exists D \in \mathbb{D}^m \rightarrow S(n) \]

is PRF if:  
- \( k \in K \)
- Query \((x)\): return \( \delta(k,x) \)

Adv. can choose

\[ \exists \mathcal{E}_1, x \in \mathcal{R}_{D,k} \]
- All functions
- \( \exists g : D \rightarrow \mathcal{C} \)
- \( \mathcal{E}_2 \) Dict = \( \emptyset \)
- Query \((k)\): if \( x \) has not been queried,
  - \( x \in \mathcal{C} \),
  - Store \((x,y)\) and return \( y \) at \((x,y)\) in Dict.

Q: \( \exists \mathcal{E}_3 \), \( \mathcal{C} \) Dict = \( \emptyset \)
- Query \((x)\): return \( g(x) \)

Illustrate PRG vs PRF

\[ \begin{array}{c}
\text{PRG} \\
\text{Real} \\
\mathcal{G}(s) \\
\text{UA} \\
\end{array} \]

\[ \begin{array}{c}
\text{PRF} \\
\text{Real} \\
\mathcal{G}(s,x) \\
\text{UA} \\
\end{array} \]

\[ \begin{array}{c}
\text{Read} \\
\mathcal{C} \in \mathcal{C} \\
\text{UA} \\
\end{array} \]
The diagram illustrates a construction of a PRF from a PRG. The process involves the following steps:

1. **Construction**: PRG => PRF
2. **Length Doubling**: PRG

The construction is as follows:

- Given a key $k = s_0$, the process starts with $G_L$ and $G_R$.
- The output is $y_0$ and $y_1$.

The function $f(k, x)$ is defined as:

$$f(k, x) = G_L(G_R(G_R(k), ...))$$

The tree construct is shown below, where each level represents a step in the construction process.