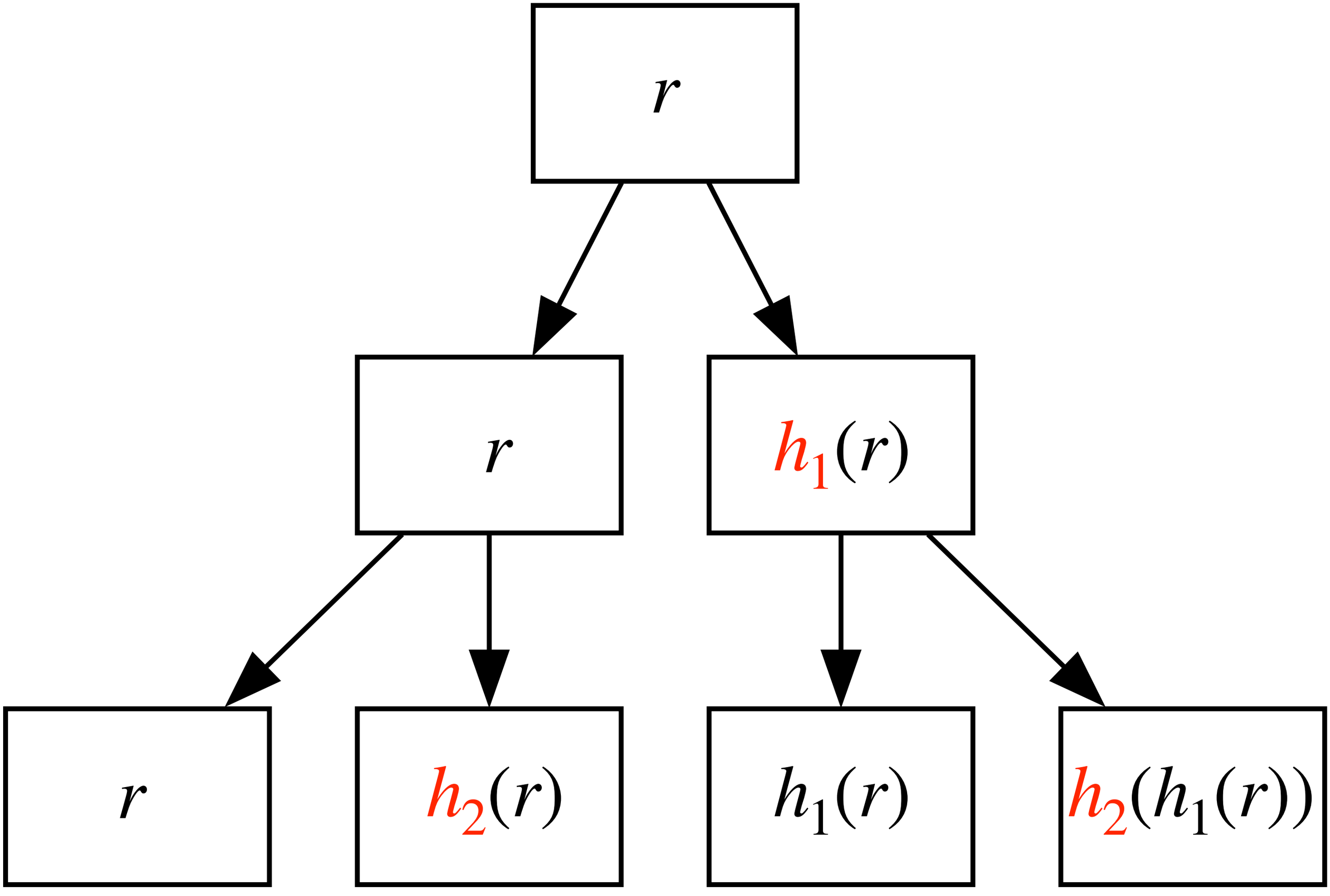

r
r
h1(r)
r
h2(r)
h1(r)
h2(h1(r))

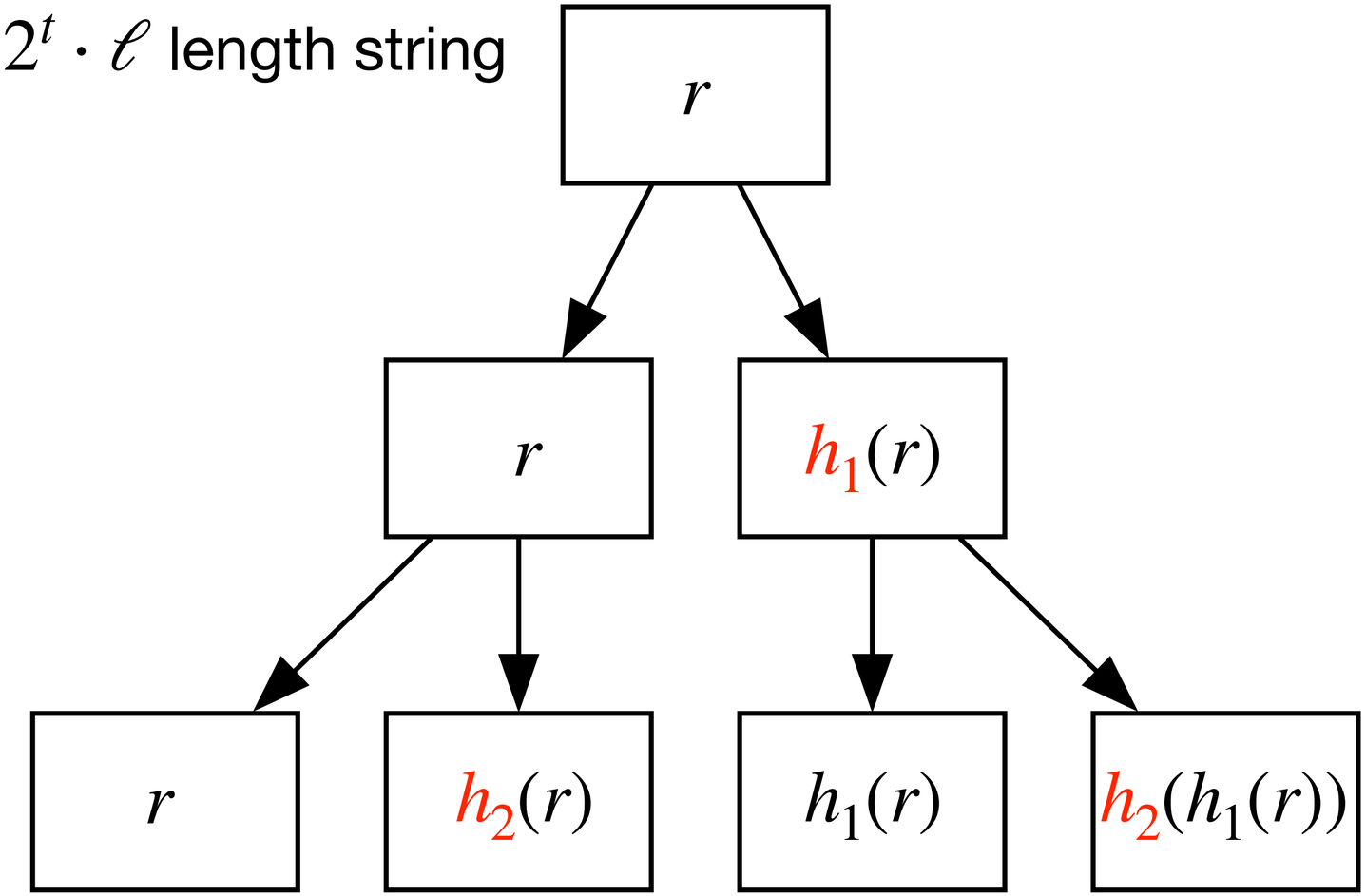
- Let $r \sim \{0,1\}^{\ell}$ and $h_1, \ldots, h_t$ 2-wise independent $\Rightarrow$ seed length of $O(t \cdot \ell)$

- Extending the tree gives a length $2^t \cdot \ell$ length string

Nisan's PRG

Nisan's PRG

- Let $r \sim \{0,1\}^{\ell}$ and $h_1, \ldots, h_t$ 2-wise independent $\Rightarrow$ seed length of $O(t \cdot \ell)$
- Extending the tree gives a length $2^t \cdot \ell$ length string



Nisan's Guarantees

- Nisan shows that if $t, w \leq c \cdot \ell$ for a constant c, then the PRG fools a w space algorithm
- If $w = \Omega(\log d)$ and we need poly(d) bits $\Rightarrow$ seed length of $O(w \log d)$ bits
- Can compute any block in time required to apply t hash functions from $\{0,1\}^{\ell} \rightarrow \{0,1\}^{\ell}$
  - Fool larger space $\Rightarrow$ ℓ needs to be large and the evaluation is slow