- $r \sim \{0,1\}^{\ell}$ and $h_1, \ldots, h_t : \{0,1\}^{\ell} \to \{0,1\}^{\ell}$ 2-wise independent

- Seed length of $O(t \cdot \ell)$

- $2^t \cdot \ell$ length string at the bottom

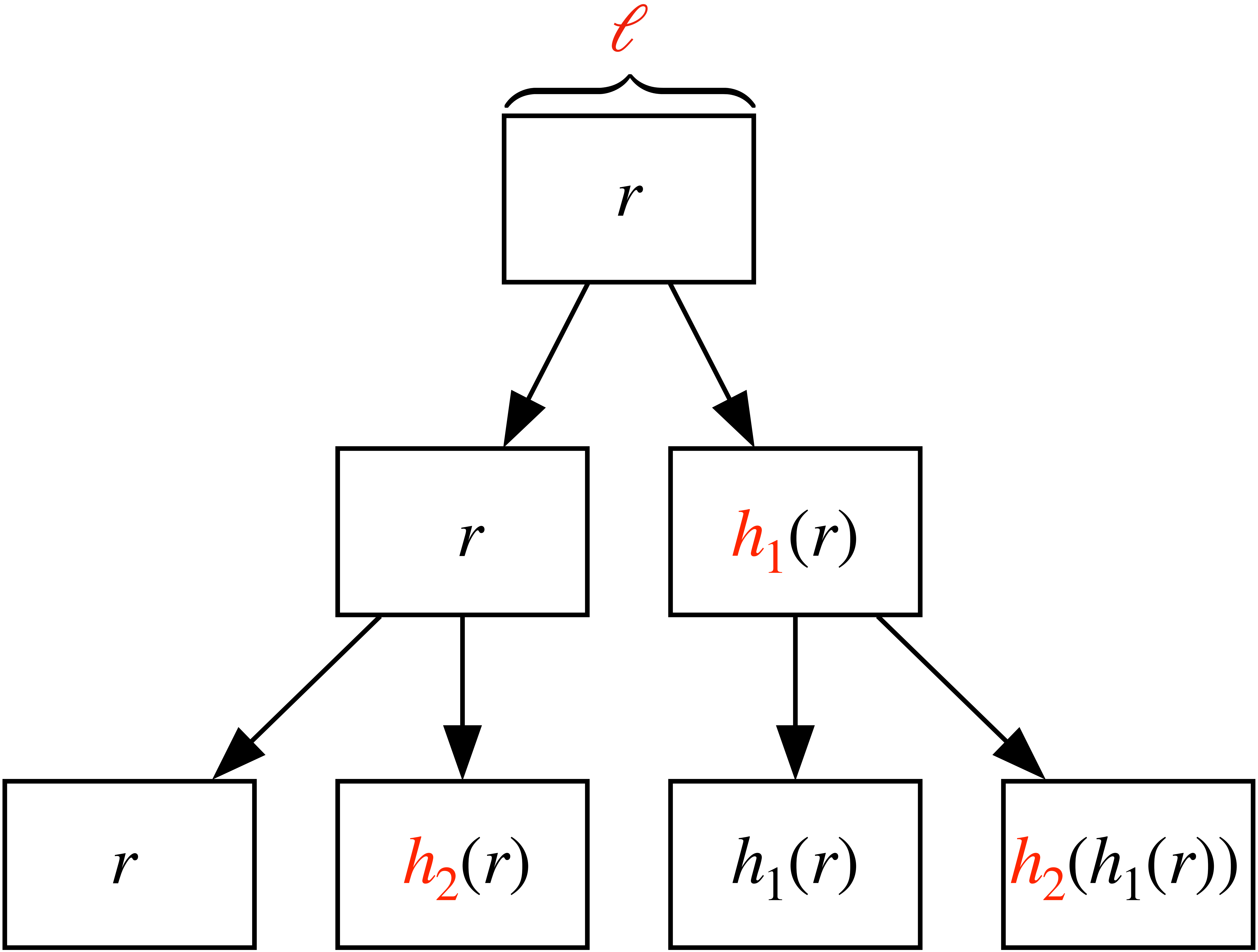
Nisan's PRG

19

- If $t, w \leq c \cdot \ell$, the PRG fools an algorithm which uses w bits of space

- Compute block with t hash evaluations

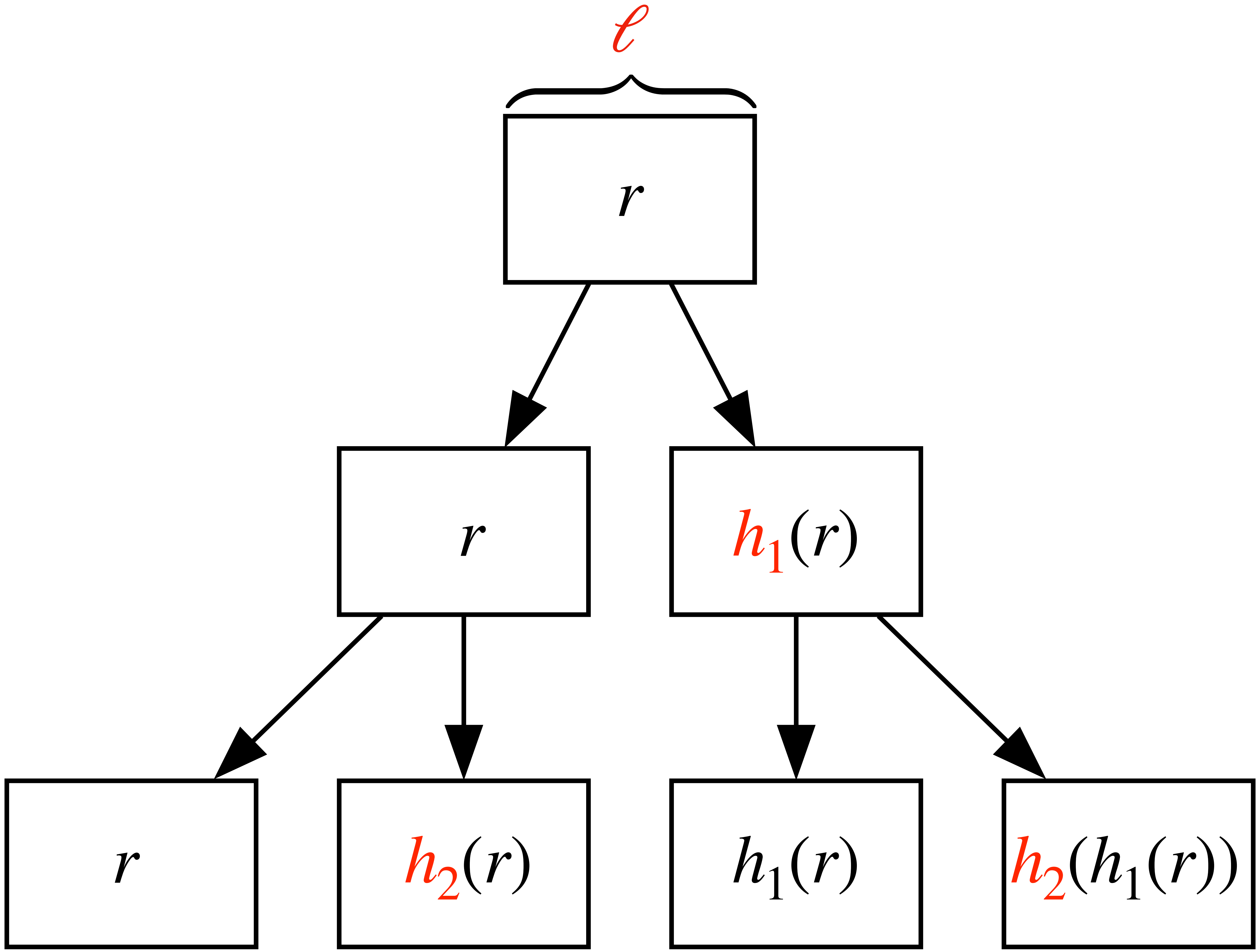
- Keep t and ℓ small


ℓ
r
r
$h_1(r)$
r
$h_2(r)$
$h_1(r)$
$h_2(h_1(r))$

Nisan's PRG

- $r \sim \{0,1\}^{\ell}$ and $h_1, \ldots, h_t : \{0,1\}^{\ell} \to \{0,1\}^{\ell}$ 2-wise independent
- Seed length of $O(t \cdot \ell)$
- $2^t \cdot \ell$ length string at the bottom

- If $t, w \leq c \cdot \ell$, the PRG fools an algorithm which uses w bits of space
- Compute block with t hash evaluations
    - Keep t and ℓ small



HashPRG