Nisan's Guarantees

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

- If $w = \Omega(\log n)$ and we need poly(n) bits ⇒ seed length of $O(w \log n)$ bits

- Can compute any block in time required to apply t hash functions from $\{0,1\}^{\ell} \rightarrow \{0,1\}^{\ell}$

- Fool larger space $\Rightarrow \ell$ needs to be large and the evaluation is slow

Nisan's Guarantees

- If $t, w \leq c \cdot \ell$, the PRG fools an algorithm which uses w bits of space
- If $w = \Omega(\log n)$ and we need poly(n) bits ⇒ seed length of $O(w \log n)$ bits
- Can compute any block in time required to apply t hash functions from $\{0,1\}^\ell \to \{0,1\}^\ell$
    - Fool larger space ⇒ ℓ needs to be large and the evaluation is slow

HashPRG