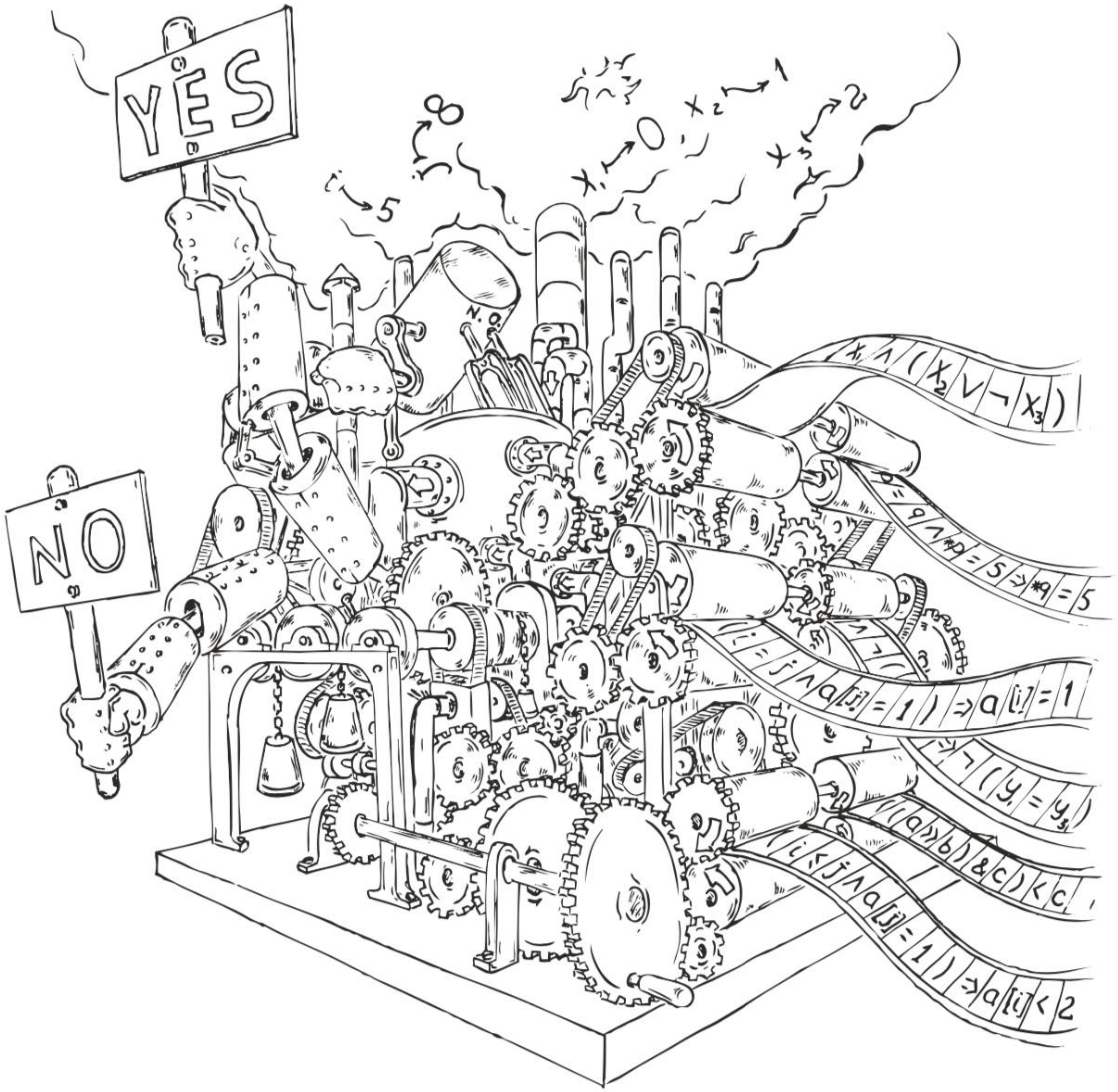
11

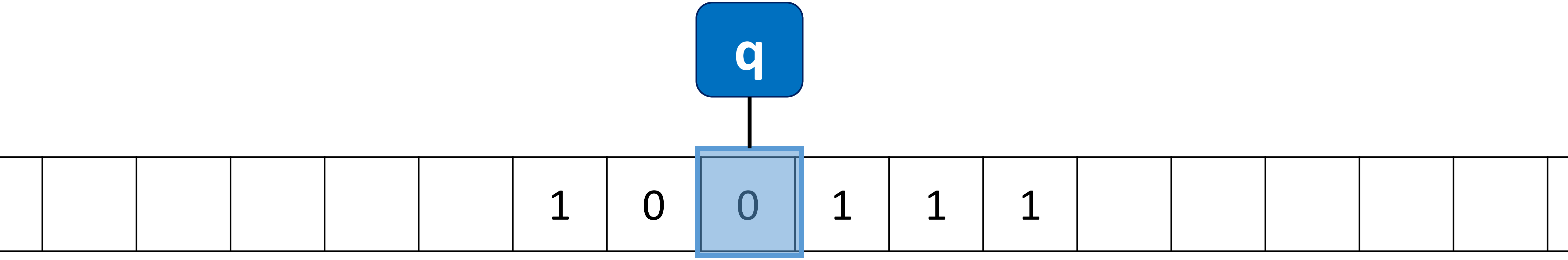


$\boldsymbol{P}$ vs. $\boldsymbol{NP}$

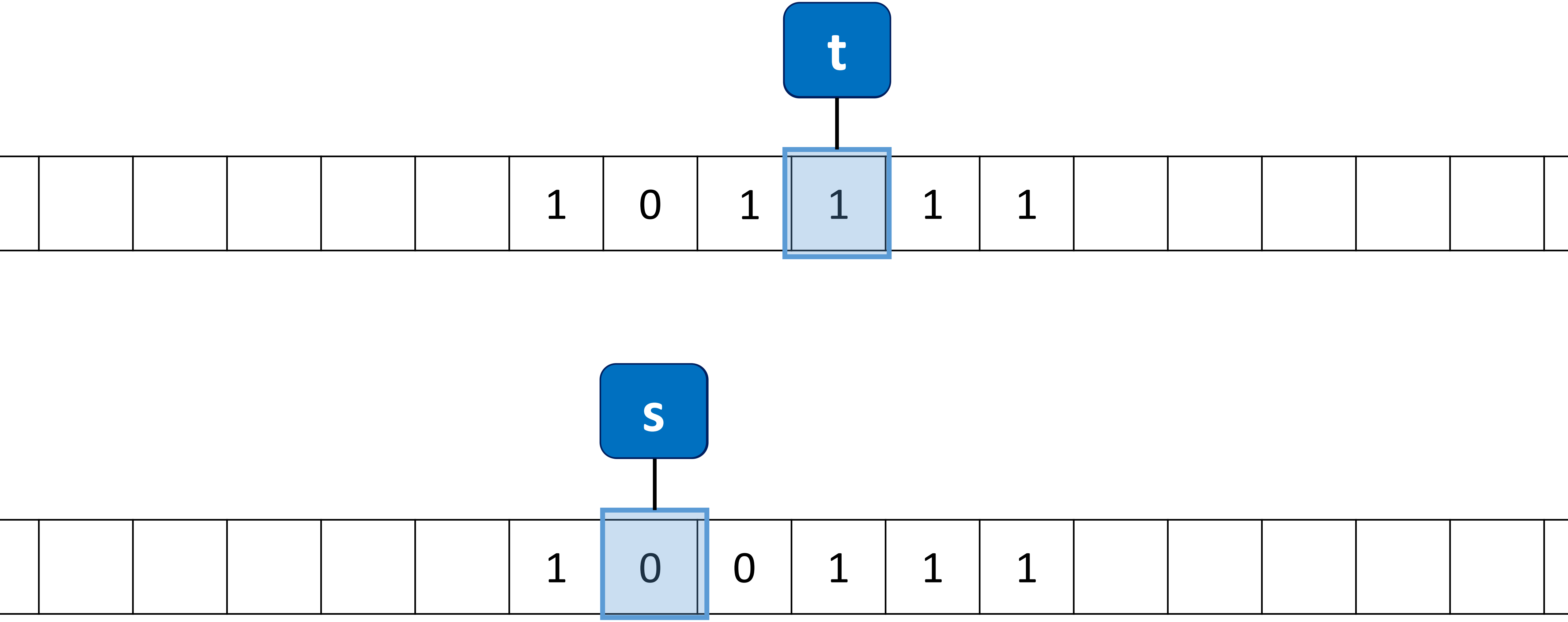
Analiza Algoritmilor

Drawing by Ilya Yodovsky Jr., from *Decision Procedures: An Algorithmic Point of View* by Daniel Kroening and Ofer Strichman
Source: https://decomposition.al/CSE290Q-2019-09/

Nondeterminism

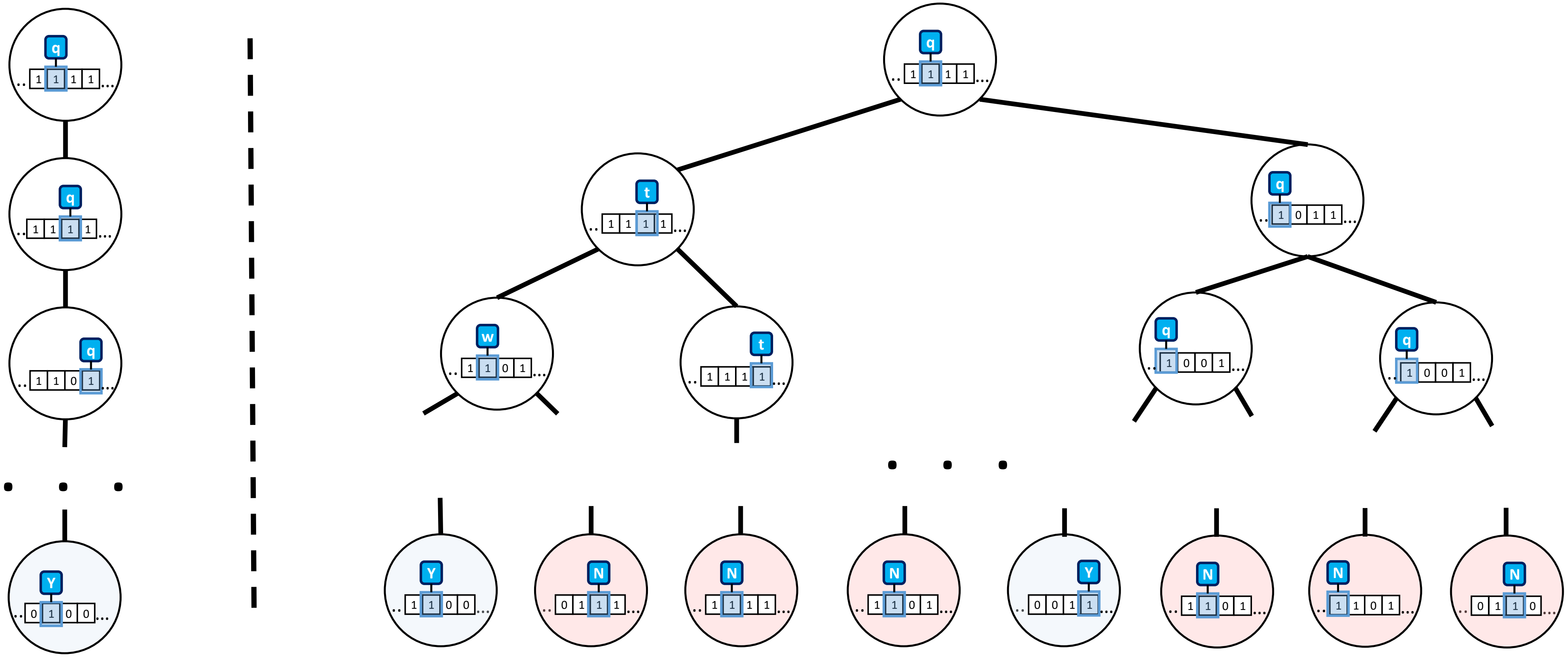


Nondeterminism



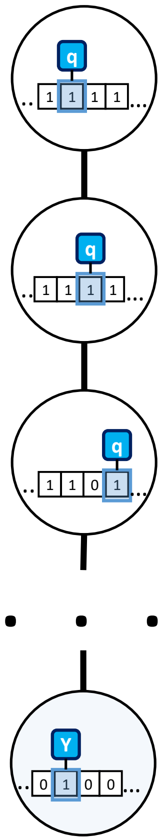
Computational histories

Deterministic Nondeterministic

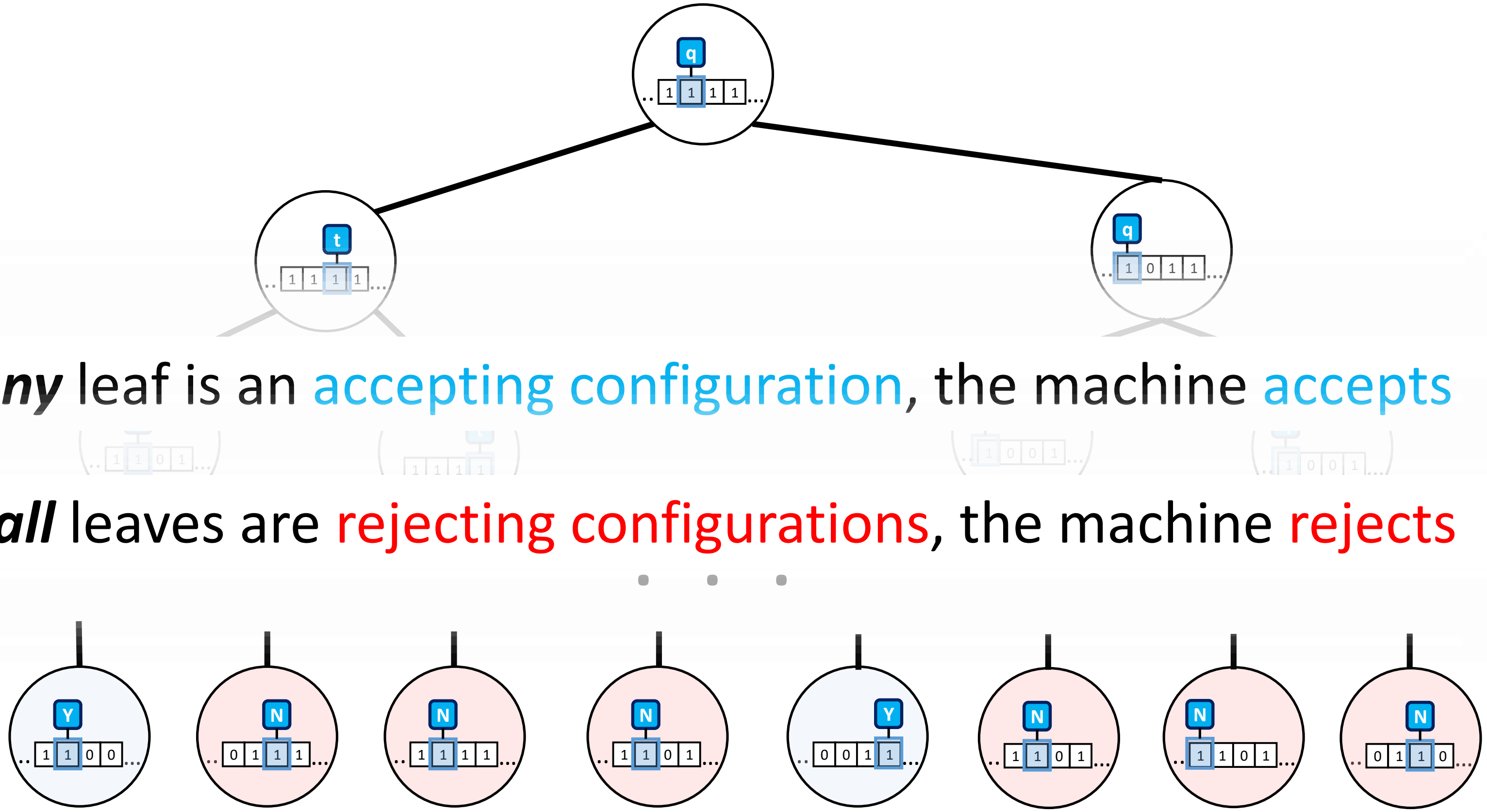


Computational histories

Deterministic



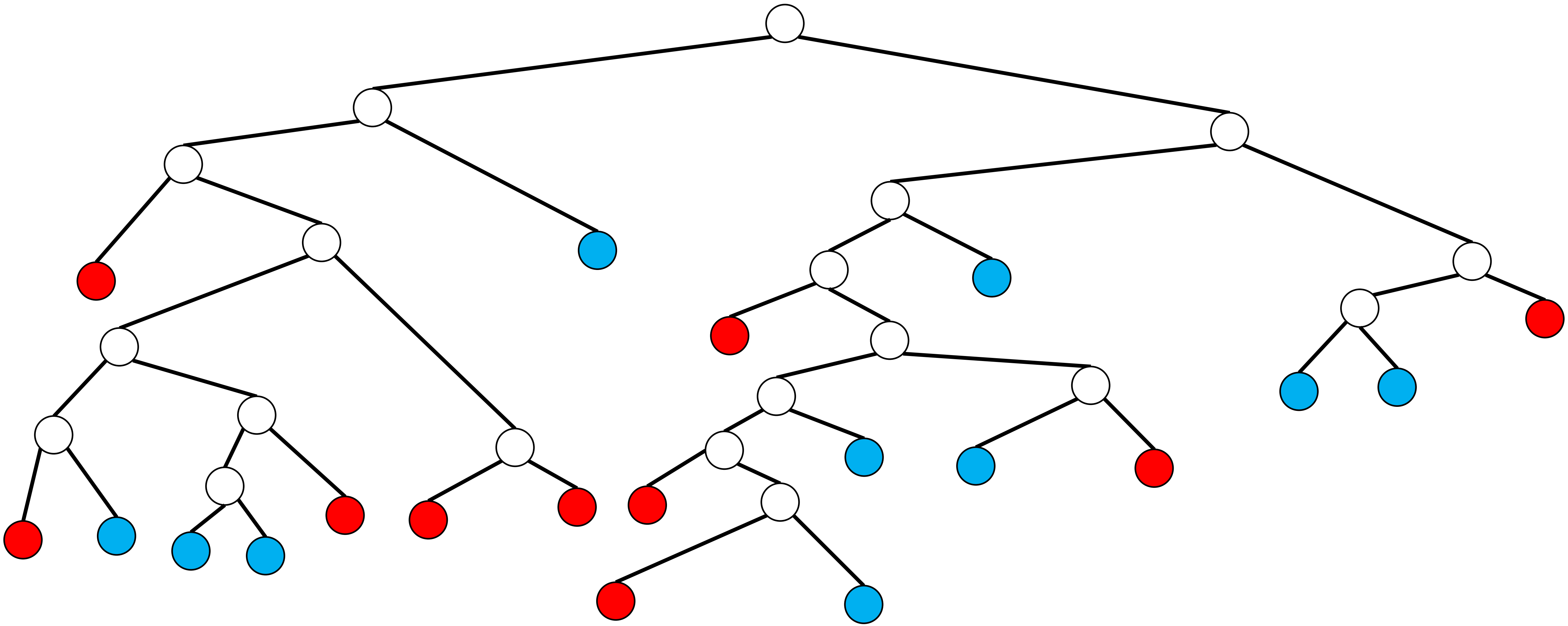
Nondeterministic



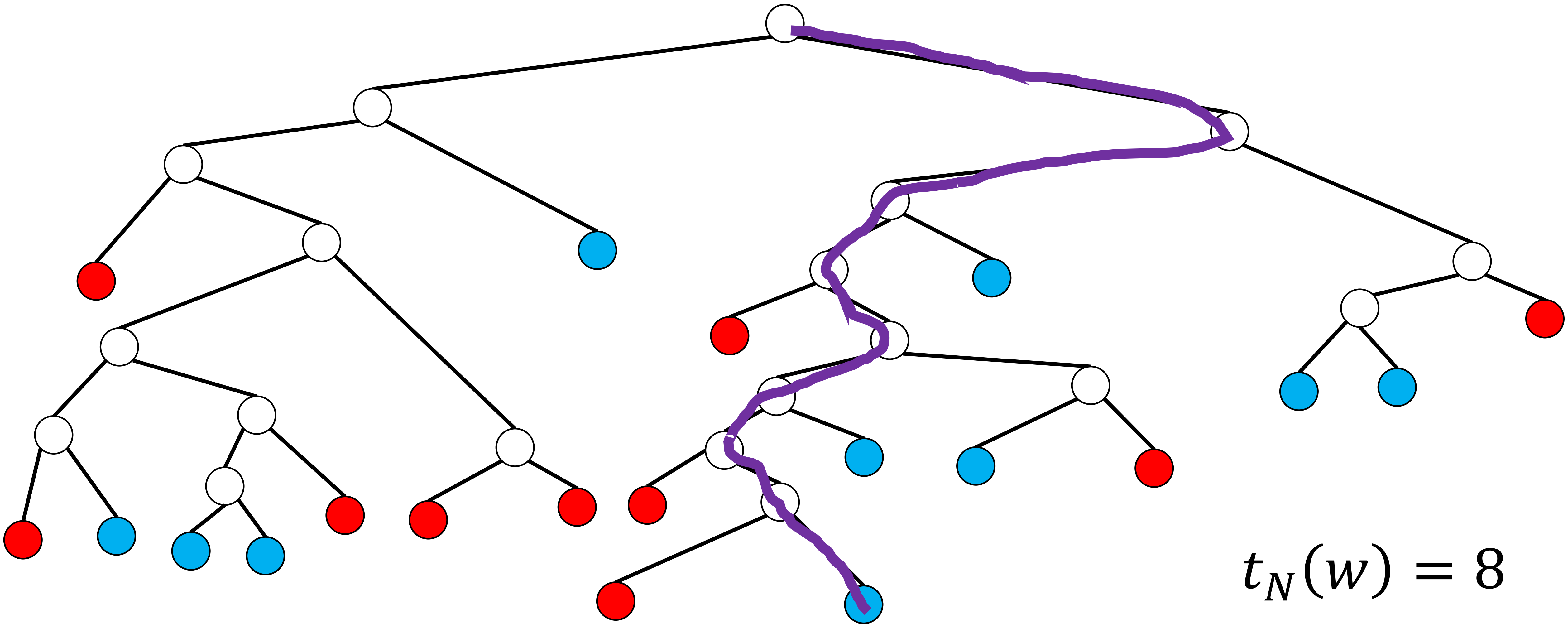
If ***any*** leaf is an accepting configuration, the machine accepts

If ***all*** leaves are rejecting configurations, the machine rejects

Running time for an NTM

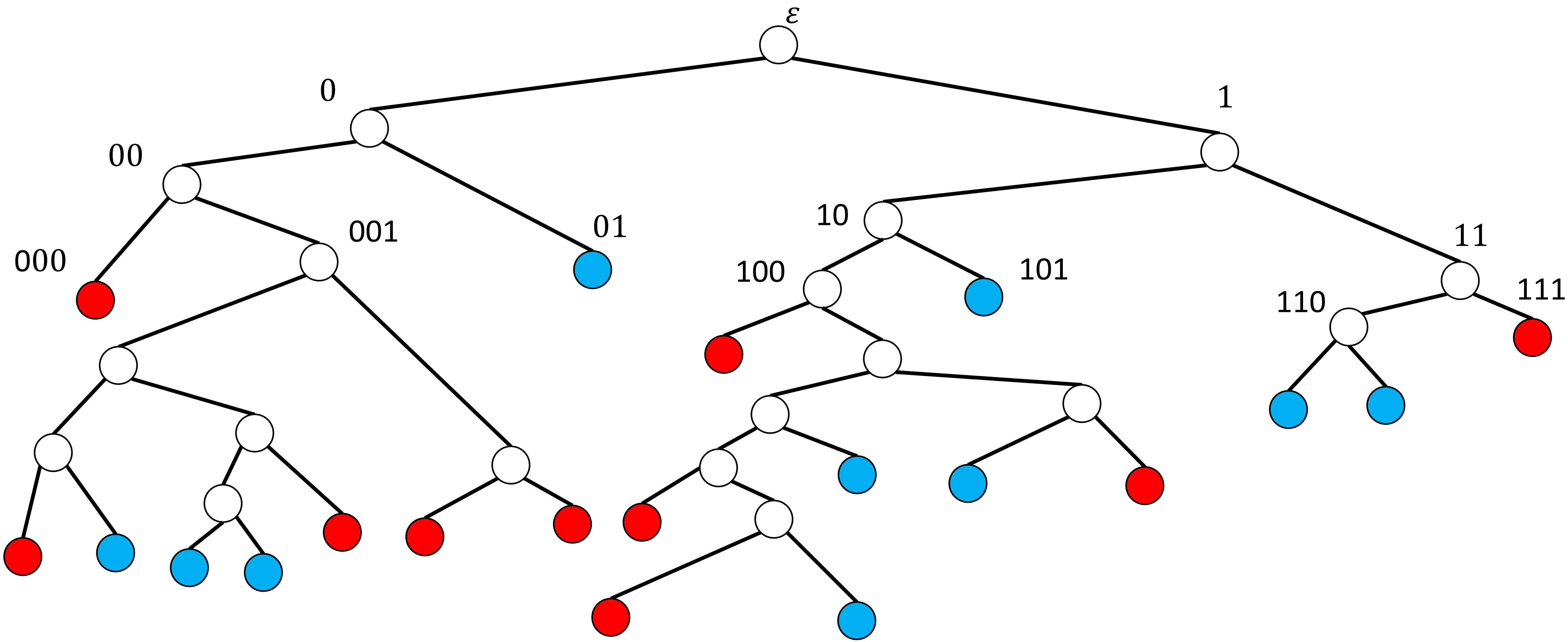


Running time for an NTM

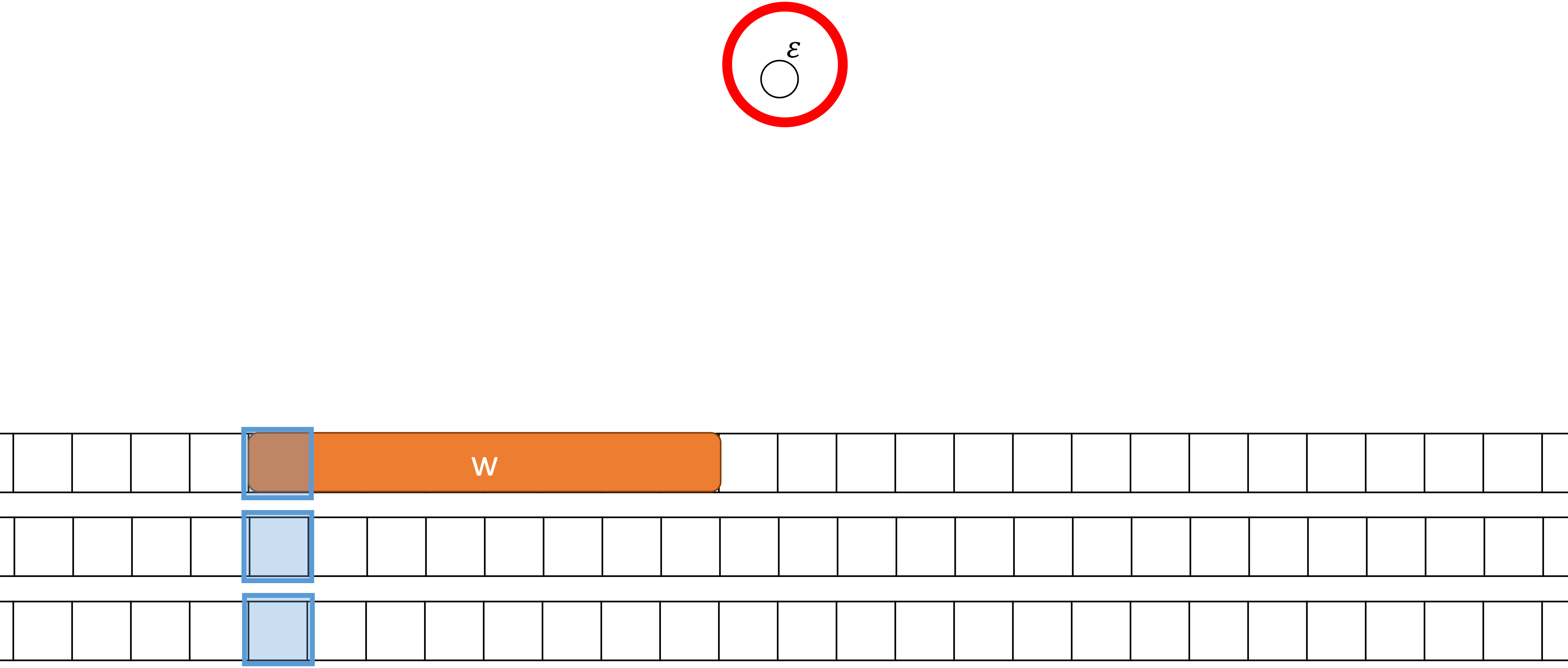


$$t_N(w) = 8$$

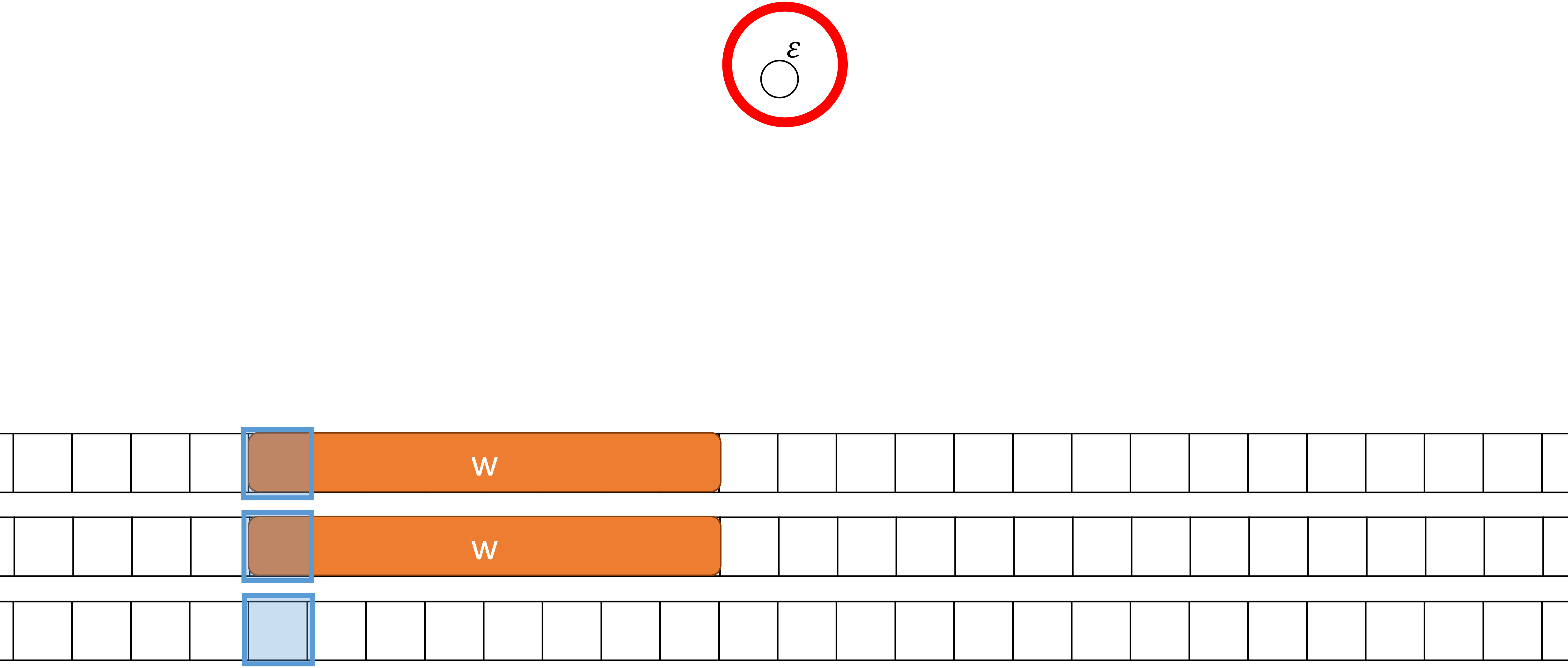
Address of a node



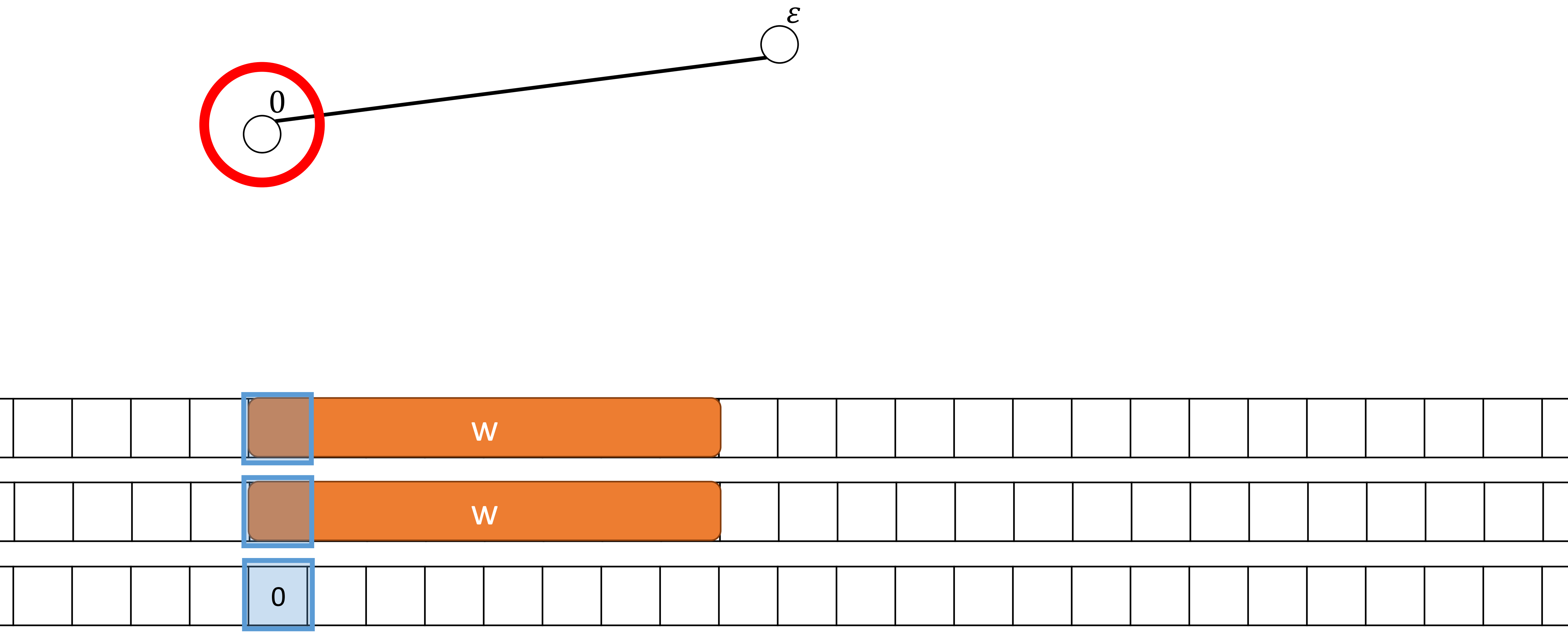
Deterministic simulation



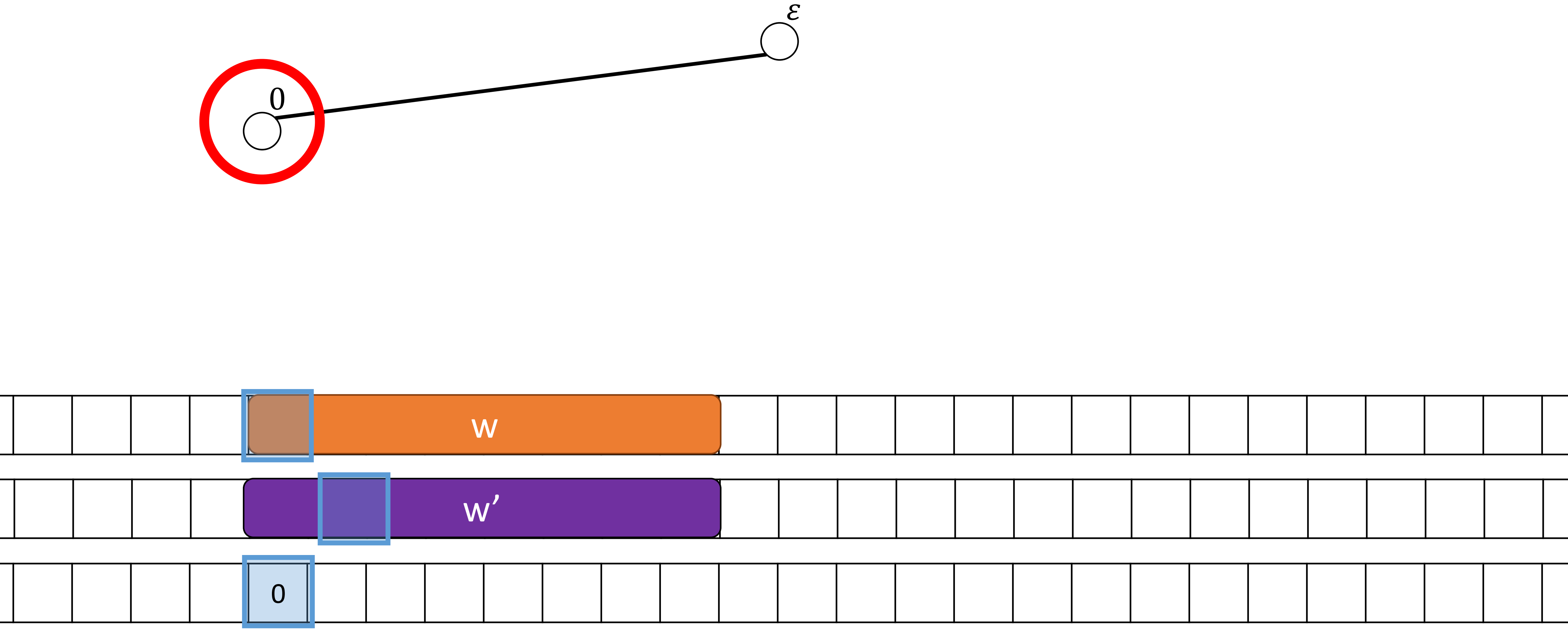
Deterministic simulation



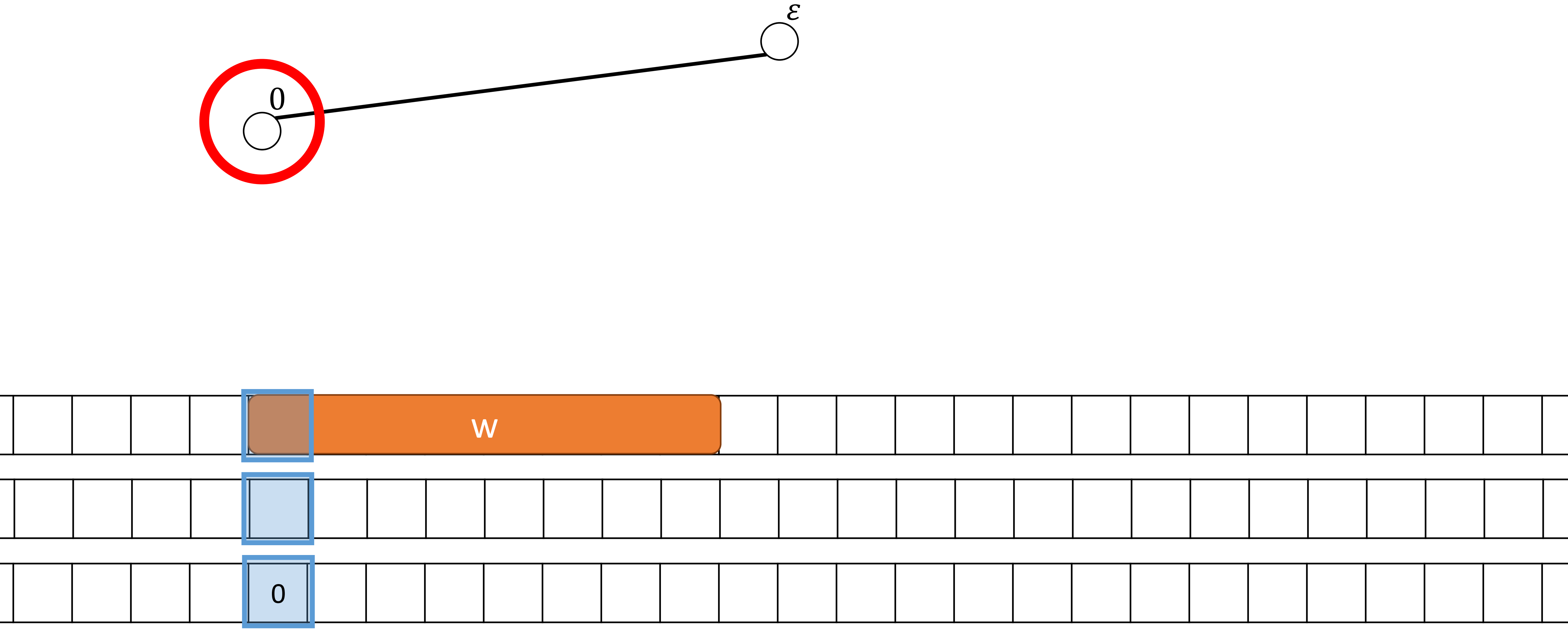
Deterministic simulation



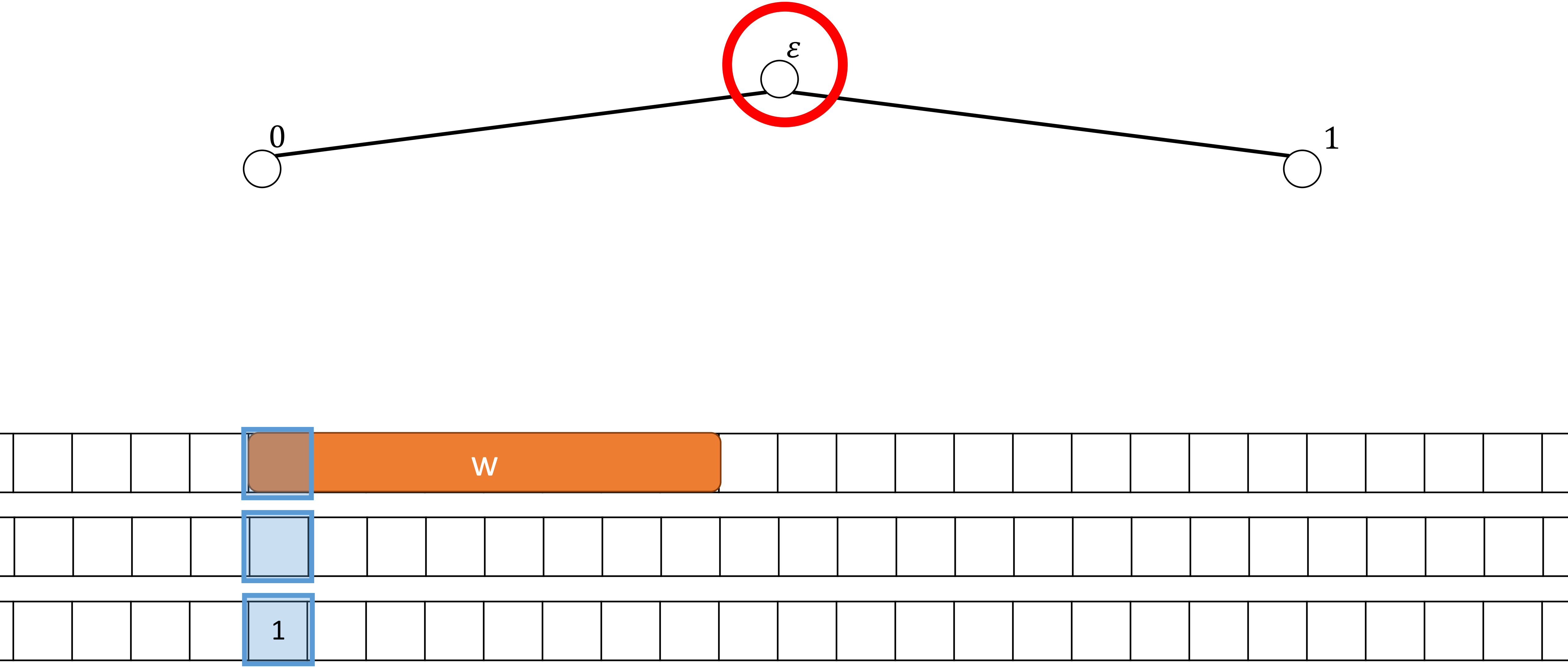
Deterministic simulation



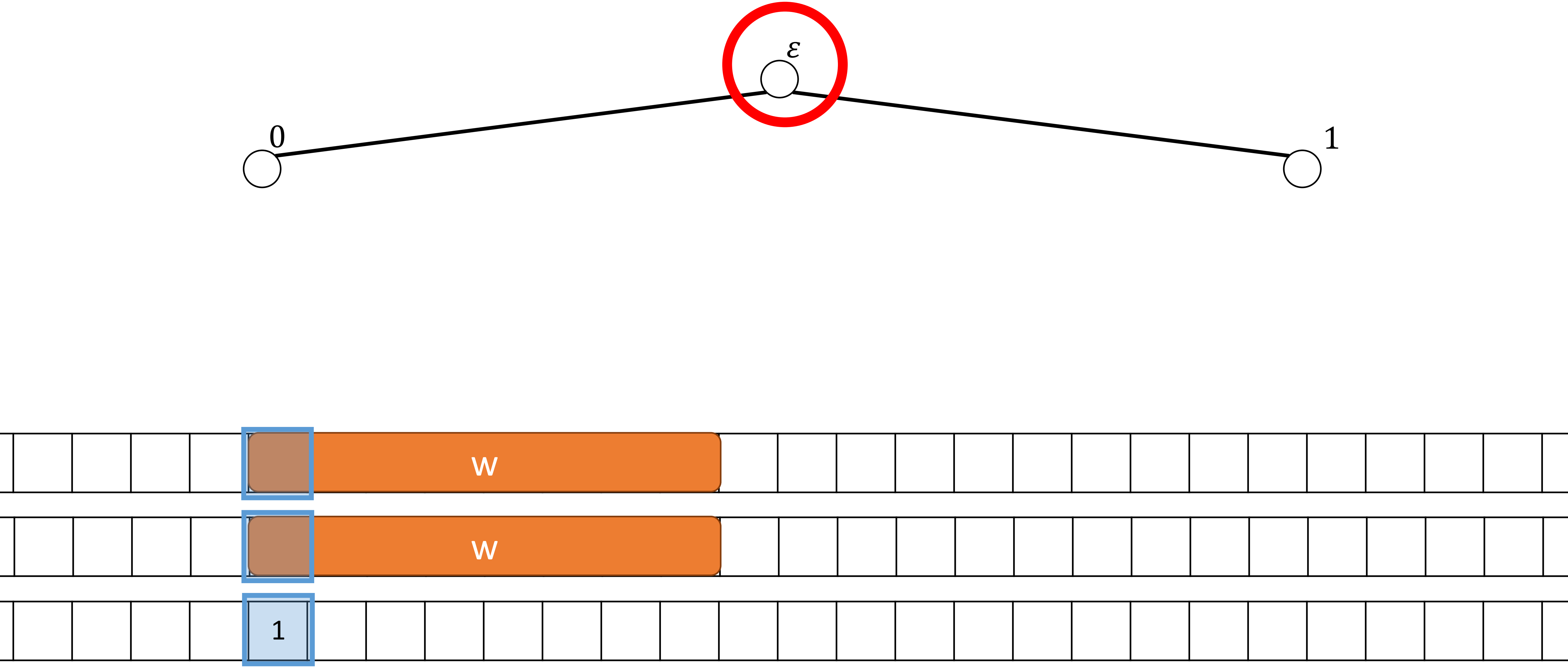
Deterministic simulation



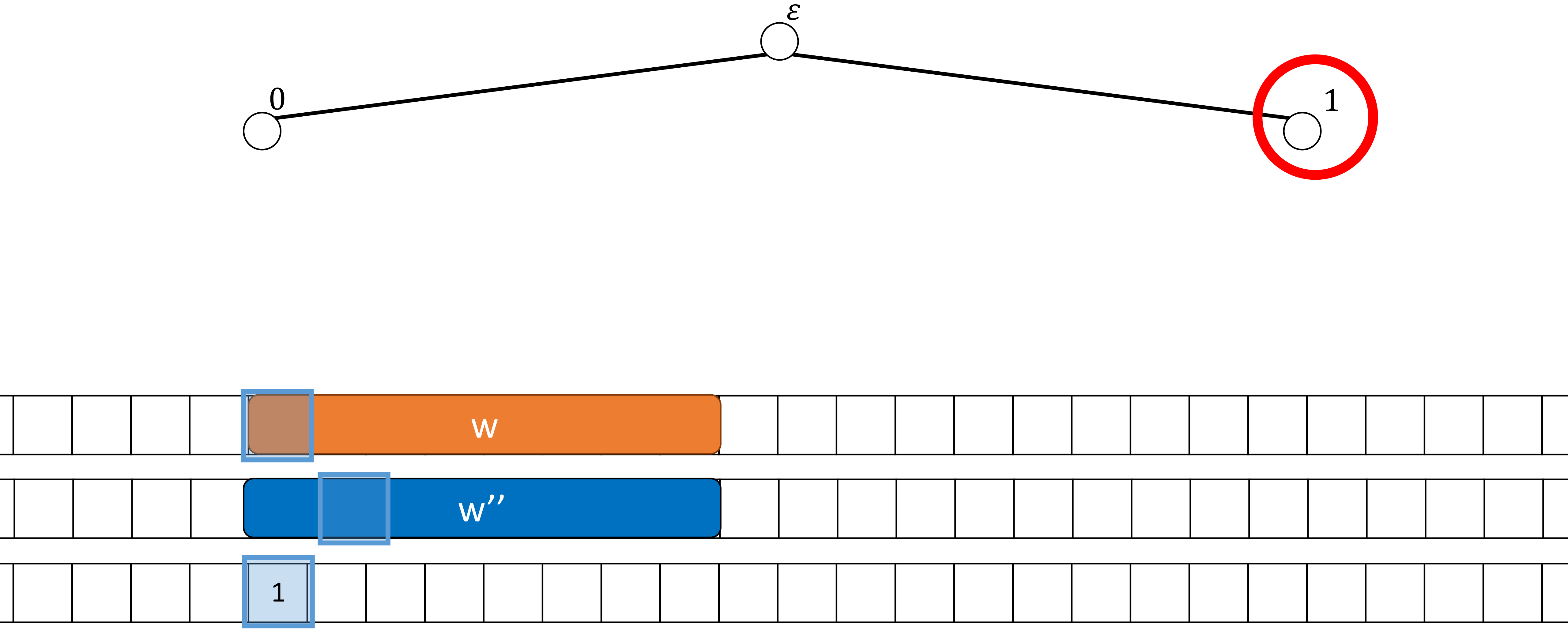
Deterministic simulation



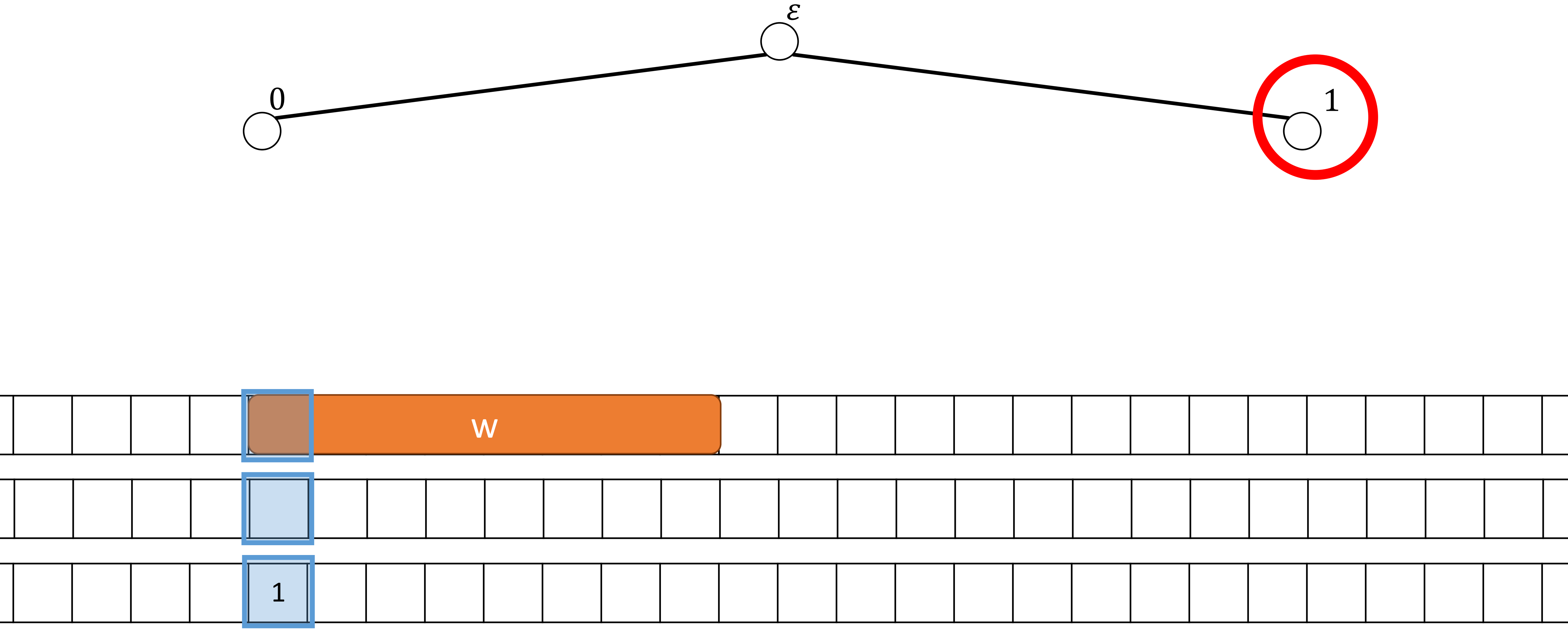
Deterministic simulation



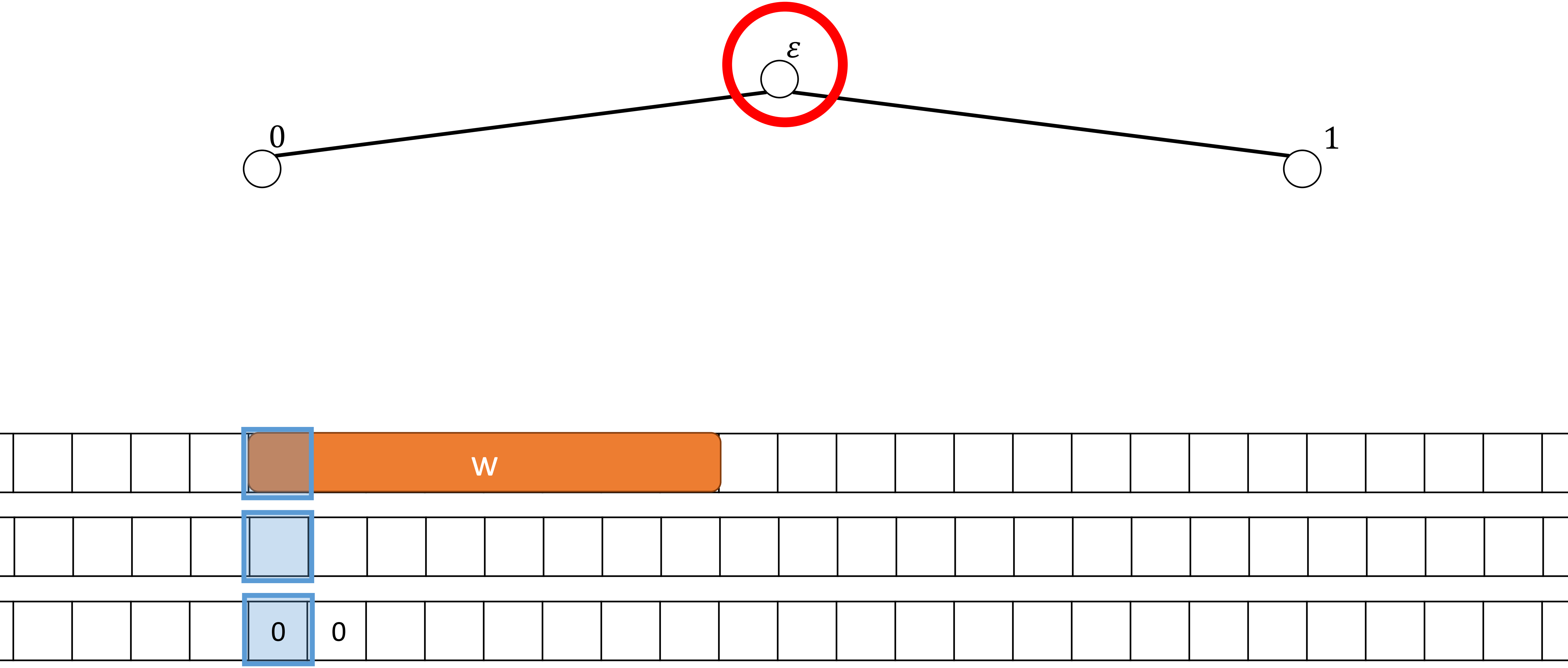
Deterministic simulation



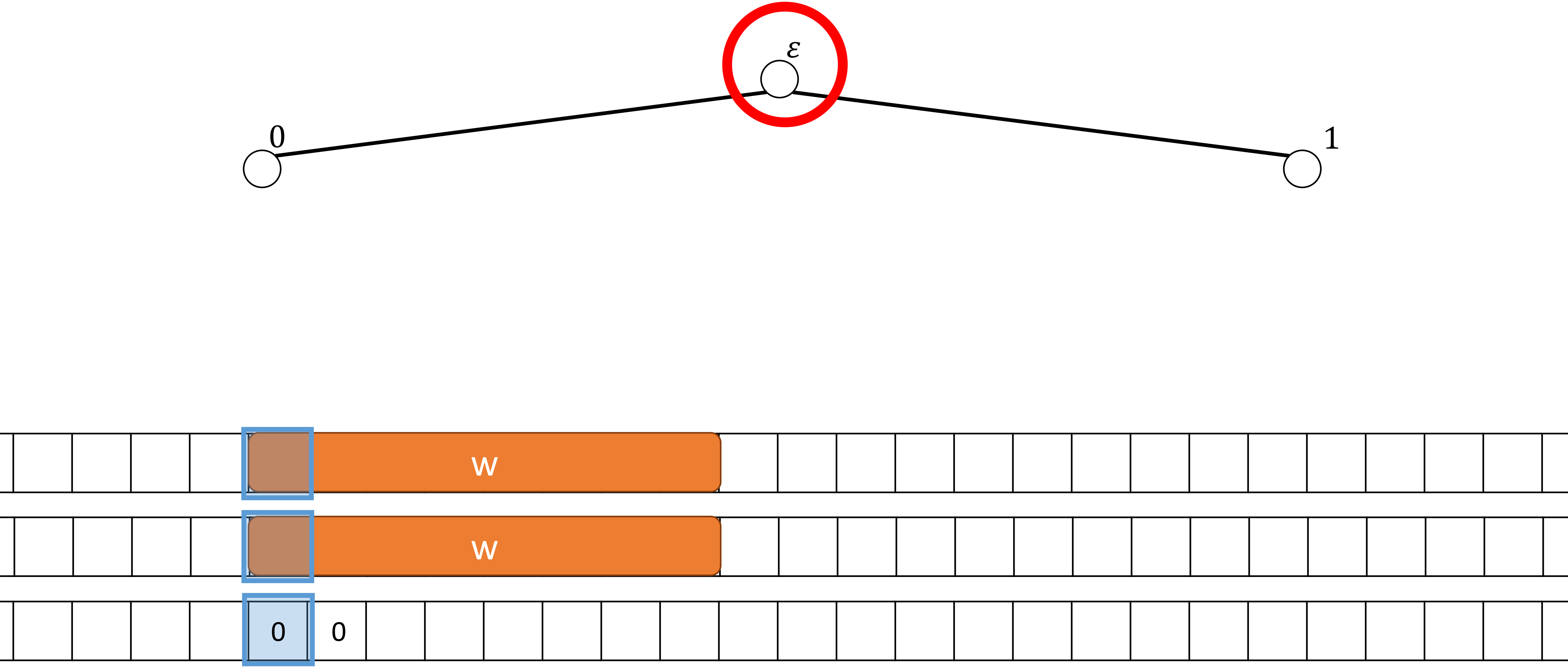
Deterministic simulation



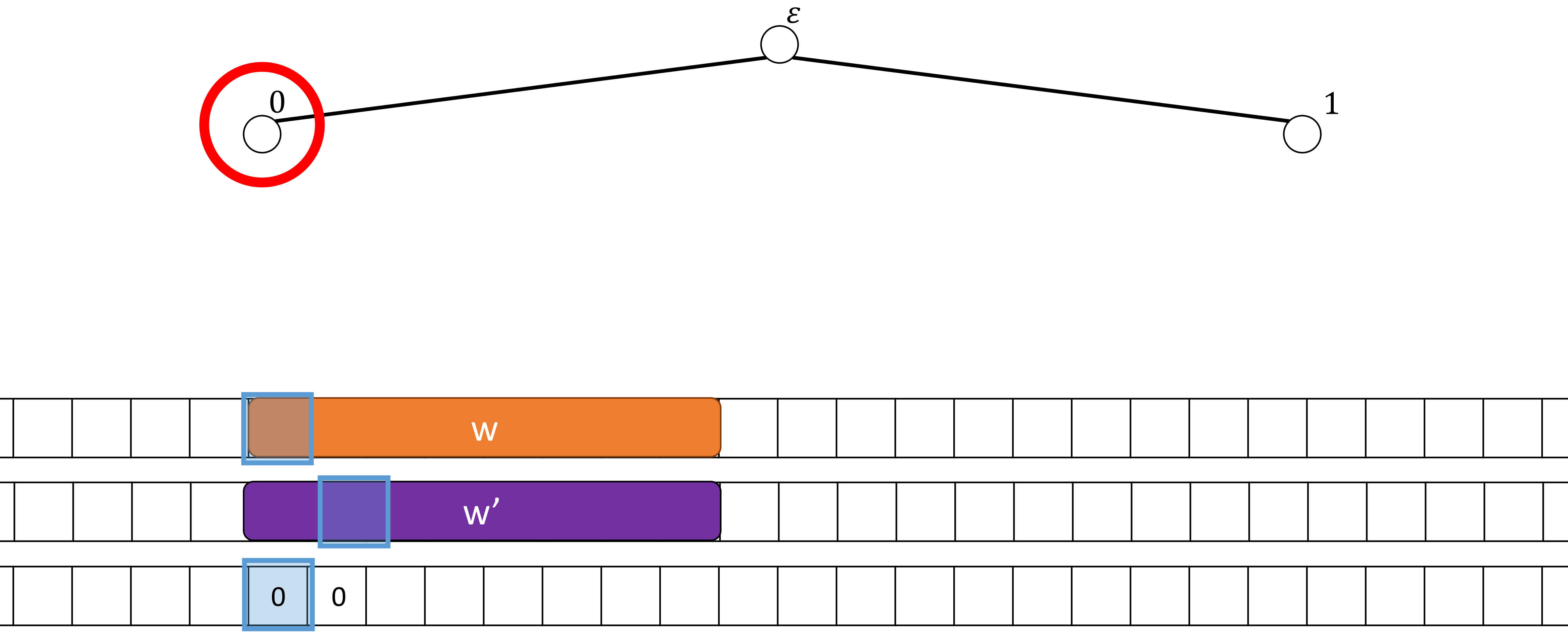
Deterministic simulation



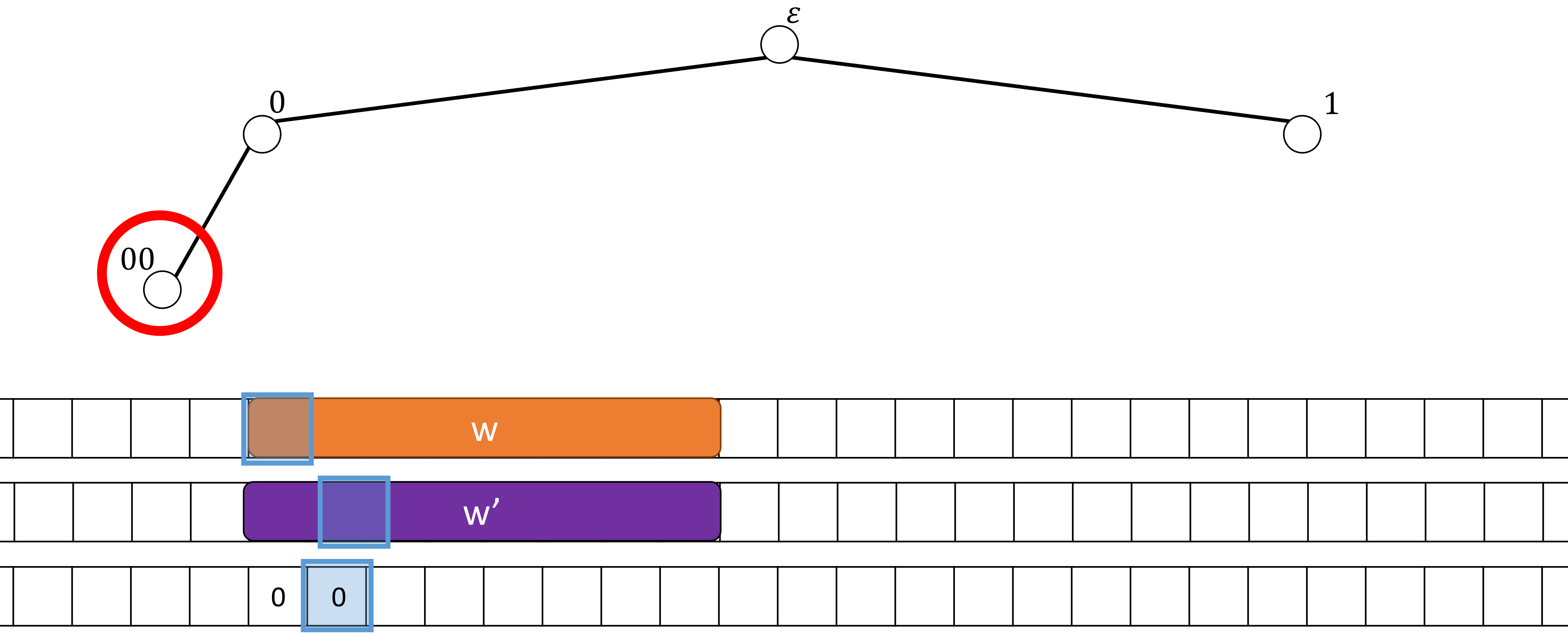
Deterministic simulation



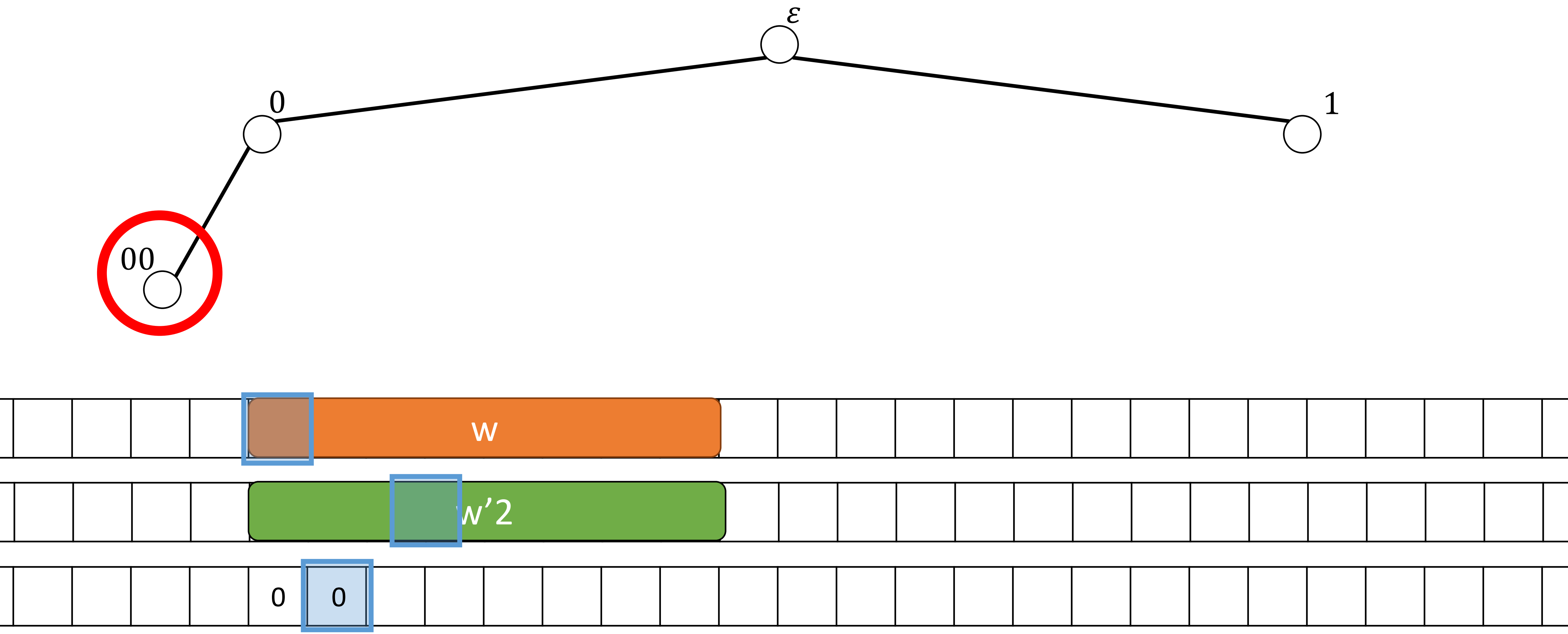
Deterministic simulation



Deterministic simulation



Deterministic simulation



The class $\boldsymbol{P}$

$$\boldsymbol{P} \stackrel{\text{def}}{=} \bigcup_{k \in \mathbb{N}} DTIME(n^k)$$

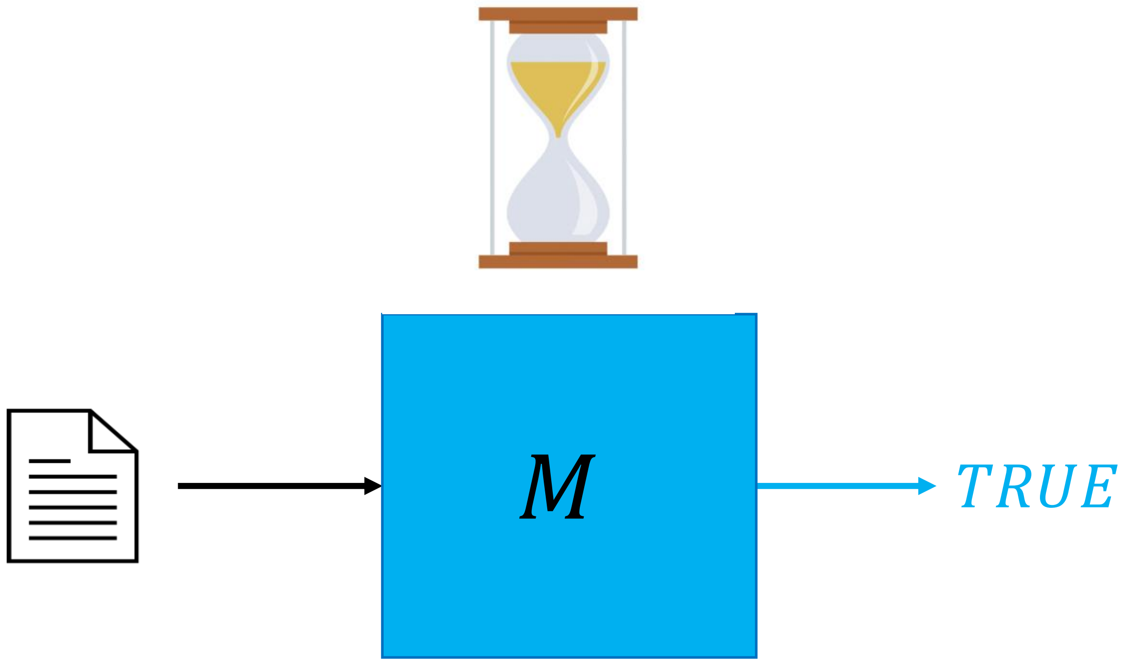
The class of tractable problems

The class $\boldsymbol{NP}$

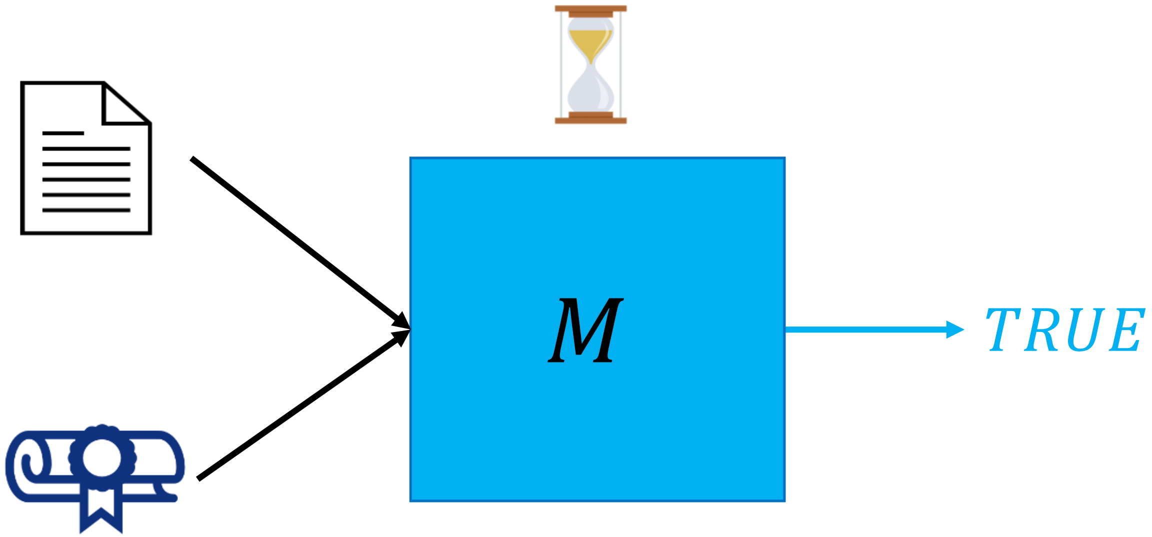
$$\boldsymbol{NP} \overset{\text{def}}{=} \bigcup_{k \in \mathbb{N}} NTIME(n^k)$$

The class of … ?

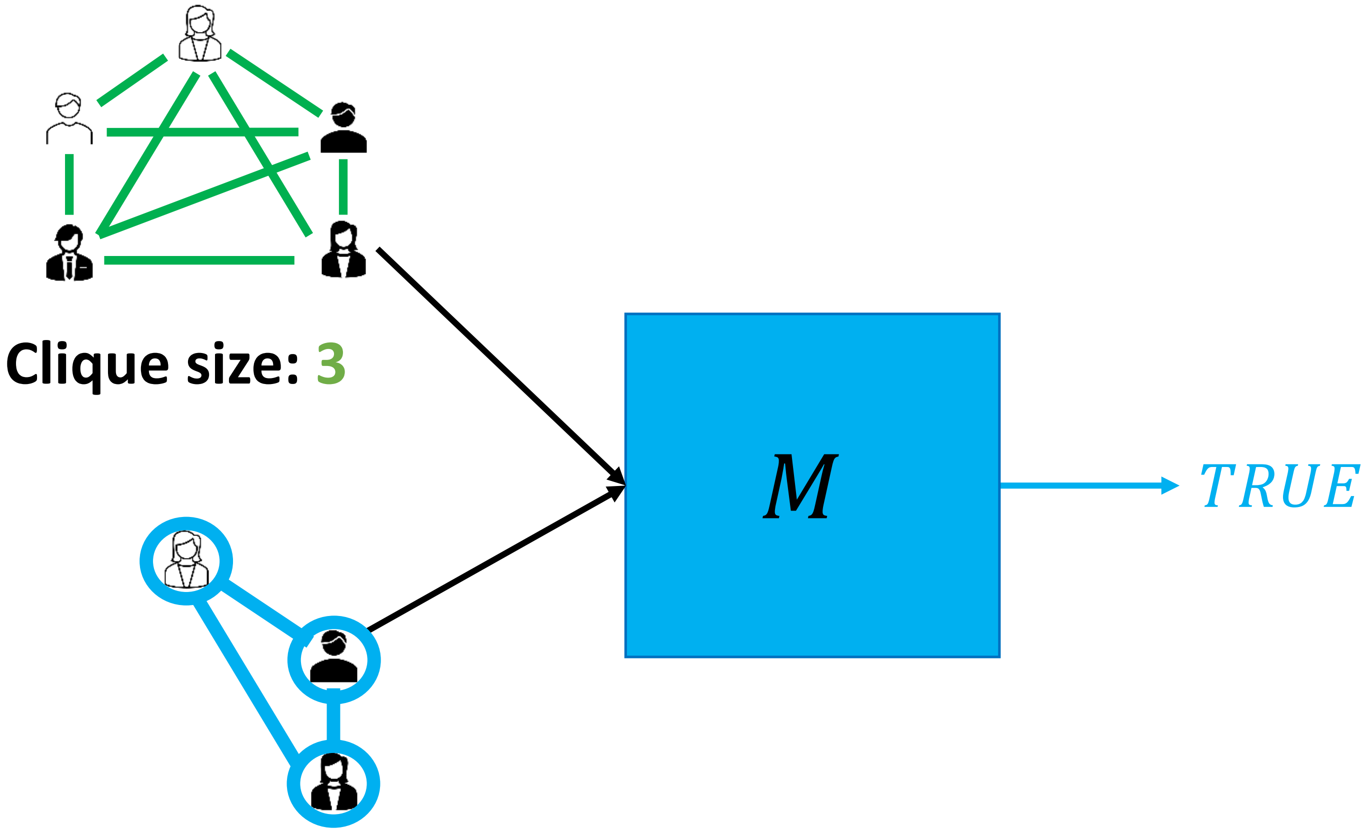
Polynomial certificates



Polynomial certificates

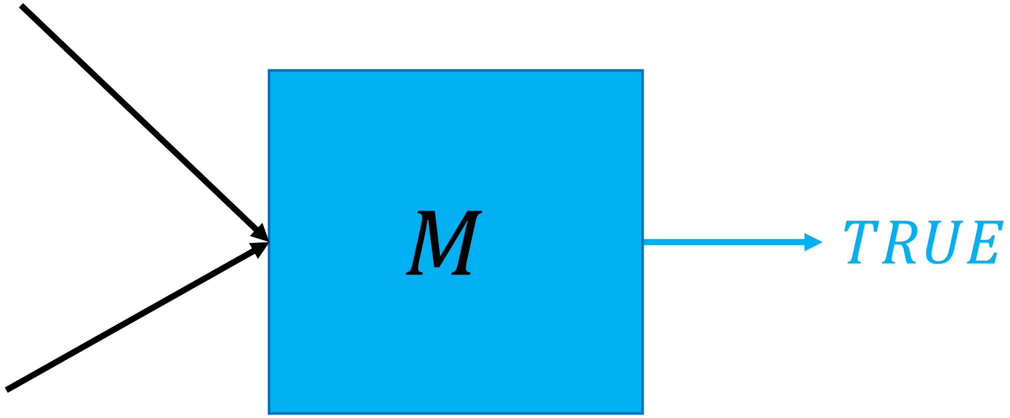


Polynomial certificate for `CLIQUE`



Polynomial certificate for SAT

$$\phi = \left(\left(x \vee \bar{y} \vee (\bar{z} \wedge y)\right) \wedge \bar{t}\right) \vee (t \wedge \bar{x})$$



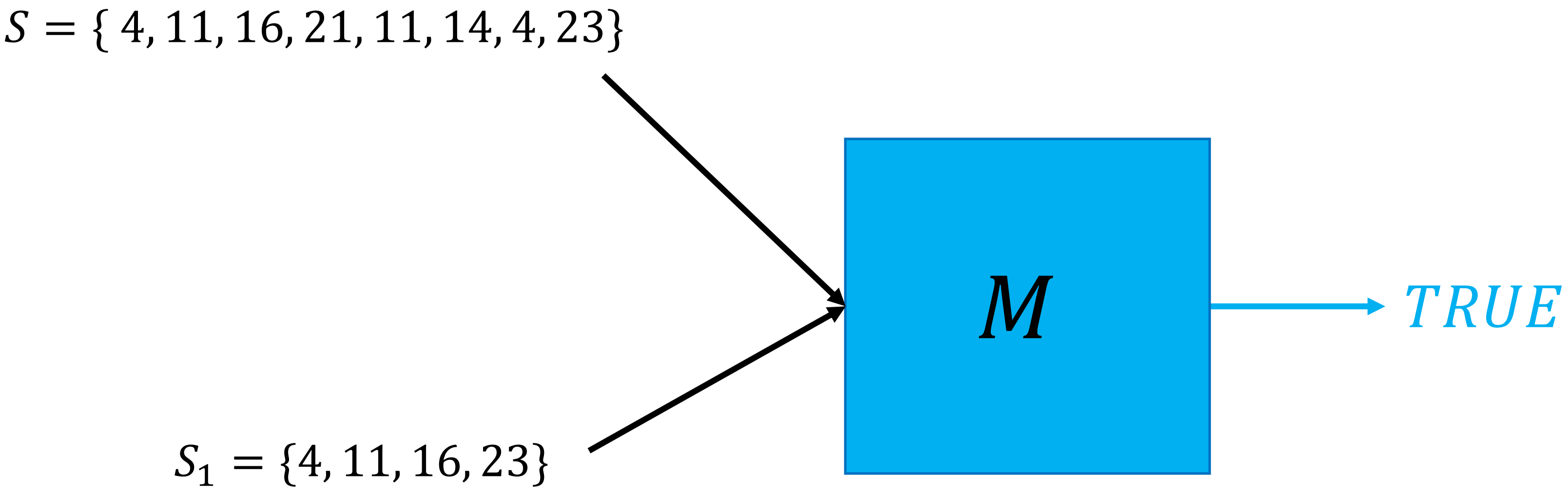
$T(x) = TRUE$

$T(y) = TRUE$

$T(z) = TRUE$

$T(t) = FALSE$

Polynomial certificate for `PARTITIONING`



PARTITIONING – Solution

```
SOLVE_SUBSET_SUM(S, K):
    r1 ← GENERATE_AND_CHECK(∅, 1, FALSE)
    r2 ← GENERATE_AND_CHECK(∅, 1, TRUE)
    return r1 ∨ r2
```

```
GENERATE_AND_CHECK(S1, i, choose):
    if choose
        S1 ← S1 ∪ {S[i]}

    if VALIDATE_SUBSET(S1)
        return TRUE

    r1 ← GENERATE_AND_CHECK(S1, i + 1, FALSE)
    r2 ← GENERATE_AND_CHECK(S1, i + 1, TRUE)
    return r1 ∨ r2
```

```
VALIDATE_SUBSET(S1):
    sum1 ← 0
    sum2 ← 0
    for each x ∈ S
        if x ∈ S1
            sum1 ← sum1 + x
        else
            sum2 ← sum2 + x

    return sum1 = sum2
```

The class $\boldsymbol{NP}$ – alternative definition

$$\boldsymbol{NP} \stackrel{\text{def}}{=} \{\text{problems with polynomial-sized certificates}\}$$

The class of problems with a ***usable solution***

$$\boldsymbol{P \subseteq NP}$$

$$\boldsymbol{P = NP}\ ?$$

$$\boldsymbol{P \neq NP}\ ?$$

It is currently unknown whether $\boldsymbol{P = NP}$...