Reductions

Recall: Showed the following language undecidable (Halting problem)

$$L_{TM} = \{ \langle M \rangle \# w \mid M \text{ is a TM and } M \text{ accepts } w \}$$

Used a diagonalization technique to prove this

For L_{TM}, we assumed the existence of a machine H which decided it

We then constructed D, which invoked H to do its computation*

Since we ran into a paradox about the operation of D on $\langle D \rangle$,
we claimed that D could not exist, and
this led us to contradict our assumption about the existence of H.

One can, in general, do this for any undecidable language.
Only the specific machines involved change!
But they might be quite complicated to set up
One can use a different technique instead: Reductions
Suppose I want to compute the product of $m, n \in \mathbb{N}$.
If I prove that $m * n = \underbrace{m + m + \cdots + m}_{n \text{ times}}$, then
if someone provides me a machine to compute $+$, I can compute $*$.
If no machine can compute $*$, no machine can compute $+$.

Suppose I can "easily" convert every string in $\mathcal{L}$ to one in R.

Conversion σ maps every string in $\mathcal{L}$ to some string in R

every string not in $\mathcal{L}$ to some string not in R

$$\omega \in \mathcal{L} \text{ iff } \sigma(\omega) \in R$$

Then, from a decider for R, I can build a decider for $\mathcal{L}$.

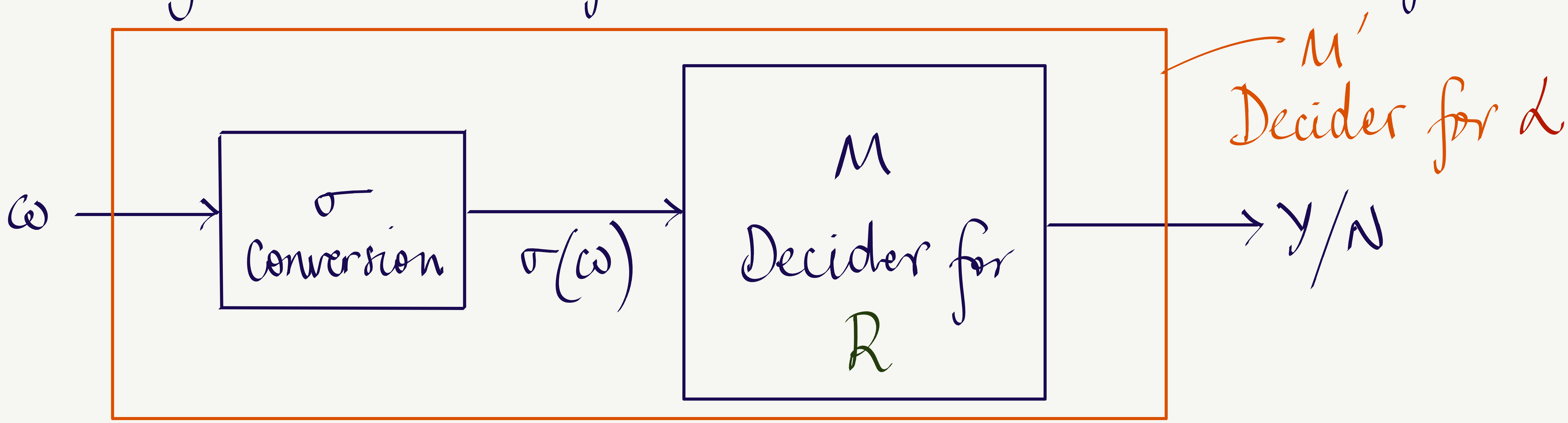
Suppose I can "easily" convert every string in $\mathcal{L}$ to one in R.

Conversion σ maps every string in $\mathcal{L}$ to some string in R

every string not in $\mathcal{L}$ to some string not in R

$$\omega \in \mathcal{L} \text{ iff } \sigma(\omega) \in R$$

Then, from a decider for R, I can build a decider for $\mathcal{L}$.



If output of M on $\sigma(\omega)$ is Y : $\sigma(\omega) \in R$, so $\omega \in \mathcal{L}$

N : $\sigma(\omega) \notin R$, so $\omega \notin \mathcal{L}$.

What if $\mathcal{L}$ is known to be undecidable? Then so is R.

For any two languages $\mathcal{L}$ and R over alphabets Σ_1 and Σ_2,
if there is a total and computable function $\sigma : \Sigma_1^* \to \Sigma_2^*$ s.t.
for any $\omega \in \Sigma_1^*$, $\omega \in \mathcal{L}$ iff $\sigma(\omega) \in R$, then,
we say that $\mathcal{L}$ reduces to R (denoted $\mathcal{L} \leq R$), and
if $\mathcal{L}$ is (independently shown to be) undecidable, so is R

$\mathcal{L} \leq R$: R is at least as difficult (to decide) as $\mathcal{L}$
If there is a decider for R, there is one for $\mathcal{L}$
If $\mathcal{L}$ is undecidable, so is R

Proof strategy: Assume R is decidable, show $\mathcal{L}$ would become decidable
Contradict the decidability of R.

usually Halting problem