Writing Proofs by Reduction

Reduction proofs are quite short, and the proofs you'll write for homework (and exam) problems will be very similar to the examples in your textbook and in the lecture slides. However, the form of abstraction reductions involve will be unfamiliar to most students, so you may find these problems challenging. This handout provides some additional help and more examples to consider.

Is my language decidable or not?

Some problems ask you to determine whether some language \( L \) is decidable or not (and perhaps prove that your answer is correct).

Rice's theorem\(^1\) states that any non-trivial property of Turing machines that depends only on the language that the Turing machine accepts is undecidable. For example, it's undecidable whether a Turing machine has a language that's non-empty, contains 17 elements, contains the string \( \text{Vassar} \), is infinite, and so forth.

On the other hand, facts about the Turing machine's structure are decidable. For example, you can tell if the Turing machine has more than 15 states, has no transitions into its accept state, or the like. Such properties just require parsing the encoding of the Turing machine and doing some straightforward check (e.g., counting the number of states listed).

Facts about a Turing machine's behavior may or may not be decidable, and it's not always easy to tell which. For example, it is decidable whether a Turing machine ever moves left, but it is not decidable whether a Turing ever moves left three times in a row.\(^2\)

Basic template

To prove that a language \( L \) is undecidable, you will normally want to use a reduction from a language already proven to be undecidable (e.g., \( A_{TM} \) or \( HALT_{TM} \)). A reduction proof will look something like:

Suppose that \( L \) is decidable. Let \( R \) be a Turing machine deciding \( L \). We will now construct a Turing machine \( S \) that decides \( A_{TM} \).

\( S \) is constructed as follows:

- Input is \( \langle M, w \rangle \), where \( M \) is the code for a Turing machine, and \( w \) is a string.
- [Pseudocode explaining how \( S \) decides whether \( M \) accepts \( w \), using \( R \) as a subroutine.]

\(^1\) Sipser solved exercise 5.28

\(^2\) Why? Ask yourself whether each property is essential for a Turing machine to have its full computational ability or not.
We know that \( A_{\text{TM}} \) is undecidable, so \( S \) can't exist. Therefore we have a contradiction, and \( L \) must have been undecidable.

This is called “reducing \( A_{\text{TM}} \) to \( L \).”

Sometimes you can write a shorter or simpler proof by replacing \( A_{\text{TM}} \) with some other problem that’s known to be undecidable. If so, remember that you may need to change the inputs to \( S \). For instance, elements of the language \( E_{\text{TM}} \) are pairs of Turing machines, so a reduction from \( E_{\text{TM}} \) requires constructing a Turing machine \( S \) whose inputs are pairs \( \langle M_1, M_2 \rangle \) of two Turing machines.

If you aren’t sure what problem to reduce to \( L \), use \( A_{\text{TM}} \).

\section*{Turing machine language problems}

In the simple examples above, \( S \) fed its inputs \( M \) and \( w \) more or less directly into the subroutine \( R \). Many other problems require \( S \) to rewrite the code for \( M \) before feeding it to \( R \).

It is often easier to imagine your Turing machines as computer programs written, e.g., in Python or C. That is, \( S \) reads the source code for program \( M \), and it writes to disk a new file of source code for a program \( M' \).

Often, you can imagine \( S \) doing the rewrite by simple copy-and-paste, e.g., copying the input code for \( M \) and then adding a new \texttt{main()} function and perhaps a few additional declarations.

The new Turing machine typically has the input \( w \) “hardcoded” into it. If you were writing the new machine’s code in Python or C, you would write a local variable declaration and copy the input value of \( w \) into that declaration.

E.g., if the input value was the string \texttt{Quokkas are cute}, the code for the new machine would contain a line like this:

\begin{verbatim}
 w = "Quokkas are cute"
\end{verbatim}

When we hardcode the input \( w \), we will often use \( M_w \) as the name for the new Turing machine to make it easy to remember.

The Turing machine \( M_w \) is typically designed so it accepts one set of strings (call the set \( X \)) if \( M \) accepts \( w \), and it accepts a totally different set of strings (call the set \( Y \)) if \( M \) doesn't accept \( w \). One of these sets should have the property that \( R \) tests for, and the other should not.

The code for \( M_w \) typically involves simulating \( M \) on \( w \), plus some other tests on \( x \) that can clearly be computed in a finite amount of time.

For some reductions, we have \( M_w \) test \( x \) first, e.g.,

1. Input is a string \( x \).
2. If \( x \) has some easily tested property \( P \), accept.

\footnote{For simple examples of the basic idea, see Sipser’s proofs of the undecidability of that \text{HALT}_{\text{TM}} (p. 217) and \text{EQ}_{\text{TM}} (p. 220).}

\footnote{E.g., see the reductions for \text{L}_{\text{VASSAR}} and \text{HALTEMP}_{\text{TM}} in the additional examples section below, where \( M_w \) accepts all input strings \( x \) if \( M \) accepts \( w \), and it accepts no input string \( x \) if \( M \) doesn't accept \( w \).}
Otherwise, simulate \( M \) on \( w \) and accept if \( M \) accepts \( w \).

For either of these two steps, you could also take the opposite action, e.g., reject all strings \( x \) that have property \( P \).\(^5\)

For other reductions, we have \( M_w \) simulate \( M \) on \( w \) first, before we test \( x \), e.g.,\(^6\)

1. Simulate \( M \) on \( w \).
2. If \( M \) rejects, reject.
3. Otherwise, accept exactly when \( x \) has some easily tested property \( P \).

**Common problems writing reductions**

A common problem is to get confused about which values are input to which Turing machines. In the above proofs, the string \( w \) is an input to the machine \( S \), i.e., the machine that decides \( A_{\text{TM}} \). The string \( x \) is an input to the Turing machine \( M_w \). Look back through the proofs and check carefully where \( x \) occurs and where \( w \) occurs.

The input to the Turing machine \( R \) is usually the code for the machine \( M_w \). You can imagine \( R \) as a Python or C program, which reads an plain text file of source code for some other program. Note that \( w \) and \( x \) are not inputs to \( R \). The value of \( w \) is hardcoded into the code for \( M_w \). The value of \( x \) is not specified. You can imagine that \( M_w \) will ask the user to input a value for \( x \).

Since the value of \( x \) is not specified, \( R \) has to consider all possible values for the input \( x \) and figure out what \( M_w \) would do on each of these values. If \( R \) is testing a non-trivial property of \( M_w \), you can imagine that it might be hard to figure out what it will do on all possible input strings \( x \). Remember that \( R \) is only a hypothetical Turing machine whose existence will be contradicted at the end of the proof. That is, \( R \) can't really exist, because it's trying to do a task that's too hard.

**Proving that a behavior is undecidable**

Undecidable behavior properties normally restrict the Turing machine's behavior in cosmetic ways but still allow it to complete the standard range of Turing machine tasks. Such a problem involves a language \( L \) which is a set of all Turing machines with a specific behavior \( B \). E.g.,

\[
L = \{ \langle M \rangle \mid M \text{ prints three 1s in a row on blank input} \}
\]

or

\[
L = \{ \langle M \rangle \mid M \text{ has a state which is never entered on any input string} \}.
\]

For this class of problems, reductions typically require modifying the input Turing machine code \( \langle M \rangle \) to create code for a new Turing
machine \( \langle M' \rangle \) which does pretty much the same thing as \( M \) except that

1. When \( M \) would have halted, \( M' \) does behavior \( B \) then halts, and
2. \( M' \) never accidentally does behavior \( B \) while it's computing.

Typical examples of this type of reduction are the proofs for \( L_{\mathbb{N}} \) and \( L_{\mathbb{X}} \) in the additional examples section. In the case of \( L_{\mathbb{N}} \), we ensure that \( M' \) can never accidentally print three ones in a row by replacing every instance of 1 in its code by a new character 1'.

*Proving that a behavior is decidable*

Decidable behavior properties normally restrict the Turing machine's behavior in a way that significantly cripples it. For an example of a decidable Turing machine behavior, consider the language

\[
L = \{ \langle M \rangle \mid M \text{ never moves left on input VASSAR} \}.
\]

\( L \) is decidable because Turing machines that never move left are so crippled that they either halt very quickly, or not at all.

More precisely, if a Turing machine \( M \) never moves left, it reads through the whole input, then starts looking at blank tape cells. Once it is on the blank part of the tape, it can cycle through its set of states, but after \(|Q|\) moves, it has run out of distinct configurations and must be in a loop. So, if you watch \( M \) for six moves (the length of the string \text{VASSAR}) and then for an additional \(|Q| + 1 \) moves, it has either halted or it is in an infinite loop.

Therefore, to decide \( L \), you run the input Turing machine for \(|Q| + 7 \) moves. After that many moves, it has either

- moved left (in which case you *reject*),
- halted (in which case you *accept*), or
- gone into an infinite loop without ever moving left (in which case you *accept*).

This algorithm is a decider (not just a recognizer) for \( L \), because it definitely halts on any input Turing machine \( M \).
Example: $L_{VASSAR}$

**Theorem** The language

$$L_{VASSAR} = \{\langle M \rangle \mid L(M) \text{ contains the string \textit{VASSAR}}\}$$

is undecidable.

**Proof** We can prove this language is undecidable by reduction from $A_{TM}$. Suppose that $L_{VASSAR}$ were decidable and let $R$ be a Turing machine deciding it. We use $R$ to construct a Turing machine $S$ that decides $A_{TM}$. $S$ is constructed as follows:

- Input is $\langle M, w \rangle$, where $M$ is the code for a Turing machine and $w$ is a string.

- Construct code for a new Turing machine $M_w$ as follows:
  - Input is a string $x$.
  - Simulate $M$ on $w$. If $M$ accepts, accept; if $M$ rejects, reject.

- Feed $\langle M_w \rangle$ to $R$. If $R$ accepts, accept. If $R$ rejects, reject.

If $M$ accepts $w$, the language of $M_w$ contains all strings and, thus, the string \textit{VASSAR}. If $M$ doesn't accept $w$, the language of $M_w$ is the empty set and, thus, doesn't contain the string \textit{VASSAR}. So $R(\langle M_w \rangle)$ accepts exactly when $M$ accepts $w$. Thus, $S$ decides $A_{TM}$.

But we know that $A_{TM}$ is undecidable, so $S$ can't exist. Therefore we have a contradiction, and $L_{VASSAR}$ must have been undecidable. ■
Example: $HALTEMPTY_{TM}$

**Theorem** The language

$$HALTEMPTY_{TM} = \{ \{M\} \mid M \text{ halts on blank input} \}$$

is undecidable.

**Proof** We can prove this language is undecidable by reduction from $A_{TM}$. Suppose that $HALTEMPTY_{TM}$ were decidable and let $R$ be a Turing machine deciding it. We use $R$ to construct a Turing machine deciding $A_{TM}$. $S$ is constructed as follows:

- 
  - Input is $\langle M, w \rangle$, where $M$ is the code for a Turing machine and $w$ is a string.
  - Construct code for a new Turing machine $M_w$ as follows:
    - Input tape is blank.
    - Write $w$ on the tape.
    - Simulate $M$ on $w$. If $M$ accepts, accept; if $M$ rejects, reject.
  - Feed $\langle M_w \rangle$ to $R$. If $R$ accepts, accept. If $R$ rejects, reject.

If $M$ accepts $w$, then $M_w$ accepts when started with a blank tape. If $M$ doesn't accept $w$, $M_w$ does not accept when started on a blank tape. So $R(\langle M_w \rangle)$ accepts exactly when $M$ accepts $w$. Thus, $S$ decides $A_{TM}$.

But we know that $A_{TM}$ is undecidable, so $S$ can't exist. Therefore we have a contradiction, and $HALTEMPTY_{TM}$ must have been undecidable. ■
Example: $L_{\text{III}}$

**Theorem**  The language

$$L_{\text{III}} = \{ \langle M \rangle \mid M \text{ prints three } 1\text{s in a row on blank input} \}$$

is undecidable

**Proof**  We can prove this language is undecidable by reduction from $A_{\text{TM}}$. Suppose that $L_{\text{III}}$ were decidable. Let $R$ be a Turing machine deciding $L_{\text{III}}$. We will now construct a Turing machine $S$ that decides $A_{\text{TM}}$.

$S$ is constructed as follows:

- Input is $\langle M, w \rangle$, where $M$ is the code for a Turing machine and $w$ is a string.
- Construct the code for a new Turing machine $M'$, which is just like $M$ except that
  - every use of the character 1 is replaced by a new character $1'$ which $M$ does not use.
  - when $M$ would accept, $M'$ first prints 111 and then accepts
- Similarly, create a string $w'$ in which every character 1 has been replaced by $1'$.
- Create a second new Turing machine $M'_w$ which simulates $M'$ on the hardcoded string $w'$.
- Run $R$ on $\langle M'_w \rangle$. If $R$ accepts, accept. If $R$ rejects, reject.

If $M$ accepts $w$, then $M'_w$ will print 111 on any input (and thus on a blank input). If $M$ does not accept $w$, then $M'_w$ is guaranteed never to print 111 accidentally. So $R$ will accept $\langle M'_w \rangle$ exactly when $M$ accepts $w$. Therefore, $S$ decides $A_{\text{TM}}$.

But we know that $A_{\text{TM}}$ is undecidable, so $S$ can't exist. Therefore we have a contradiction, and $L_{\text{III}}$ must have been undecidable. □
Example: $L_x$

**Theorem** The language

$$L_x = \{ \langle M \rangle \mid M \text{ writes an } x \text{ at some point, when started on blank input} \}$$

is undecidable.

**Proof** Suppose that $L_x$ were decidable. Let $R$ be a Turing machine deciding $L_x$. We will now construct a Turing machine $S$ that decides $A_{TM}$.

$S$ is constructed as follows:

- Input is $\langle M, w \rangle$, where $M$ is the code for a Turing machine and $w$ is a string.

- Construct the code for a new Turing machine $M_w$ as follows
  
  - On input $y$ (which will be ignored).
  - Simulate $M$ on $w$, but substituting some previously unused symbol $\psi$ for $x$, everywhere that $x$ occurs in $w$ or the code for $M$.
  - If $M$ rejects $w$, reject.
  - If $M$ accepts $w$, print $x$ on the tape and then accept.

- Run $R$ on $\langle M_w \rangle$. If $R$ accepts, accept. If $R$ rejects, reject.

If $M$ accepts $w$, then $M_w$ will print $x$ on any input (and thus on a blank input). If $M$ rejects $w$ or loops on $w$, then $M_w$ is guaranteed never to print $x$ accidentally. So $R$ will accept $\langle M_w \rangle$ exactly when $M$ accepts $w$. Therefore, $S$ decides $A_{TM}$.

But we know that $A_{TM}$ is undecidable, so $S$ can't exist. Therefore we have a contradiction, and $L_x$ must have been undecidable. ■
Example: \( L_3 \)

**Theorem** The language

\[
L_3 = \{ \langle M \rangle \mid |L(M)| = 3 \},
\]

that is, the language that contains all Turing machines whose languages contain exactly three strings, is undecidable.

**Proof** Proof by reduction from \( A_{TM} \). Suppose that \( L_3 \) were decidable and let \( R \) be a Turing machine deciding it. We use \( R \) to construct a Turing machine deciding \( A_{TM} \). \( S \) is constructed as follows:

- Input is \( \langle M, w \rangle \), where \( M \) is the code for a Turing machine and \( w \) is a string.
- Construct code for a new Turing machine \( M_w \) as follows:
  - Input is a string \( x \).
  - Simulate \( M \) on \( w \).
  - If \( M \) rejects \( w \), reject.
  - Otherwise, accept \( x \) exactly when \( x \) is one of the three strings Vassar, College, or Poughkeepsie.
- Feed \( \langle M_w \rangle \) to \( R \). If \( R \) accepts, accept. If \( R \) rejects, reject.

If \( M \) accepts \( w \), the language of \( M_w \) contains exactly three strings. If \( M \) doesn't accept \( w \), the language of \( M_w \) is the empty set. So \( R(\langle M_w \rangle) \) accepts exactly when \( M \) accepts \( w \). Thus, \( S \) decides \( A_{TM} \).

But we know that \( A_{TM} \) is undecidable, so \( S \) can't exist. Therefore we have a contradiction, and \( L_3 \) must have been undecidable. ■

**Acknowledgments**

This handout is based on material written by Nancy Ide.