Computability: Proof by Construction and Disproof by Contradiction

Oluwafunke Alliyu, Ethan Balcik, Paul John Balderston, Sen Zhu

April 2021

1 Introduction

In the age of digital communications, it is difficult to imagine how, in a world without digital computers, one might work toward the development of one. As a result, often overlooked are the initial developments which led to today's digital age. Nevertheless, the emergence of digital computers would not be possible without initial, groundbreaking developments in mathematical logic and information theory from significant engineers and mathematicians like Alan Turing and Claude Shannon. Throughout this paper, we discuss computability in a rigorous, self-contained manner - both its proof by construction and its disproof by contradiction, with examples of each. Furthermore, we aim to provide our readers with some historical insight into the development of these methods in order to build both an appreciation of their significance, and of the current challenges researchers face as attempts are made to further progress in theoretical computer science [**1**].

2 Background

Here we introduce the background section

2.1 Historical Background

Here we discuss the history behind computer science and its foundations in mathematics

2.2 Mathematical Logic and Set Theory

Here we discuss relevant concepts in mathematical logic and set theory

2.3 Finite State Machines

Here we discuss finite state machines, state diagrams, etc. to provide the necessary background to understand conceptual machines and understand Turing Machinces graphically

3 Turing Machines

An effective model for the general-purpose computer is the Turing Machine, developed by Alan Turing in 1936 [**2**]. The Turing Machine is a conceptual model of a general-purpose computing machine which involves the following conceptual components:

- A "control box" which stores a finitely-large program
- A tape with infinite spaces in which symbols can be stored, read, and written
- A read-write mechanism for the tape [**3**]

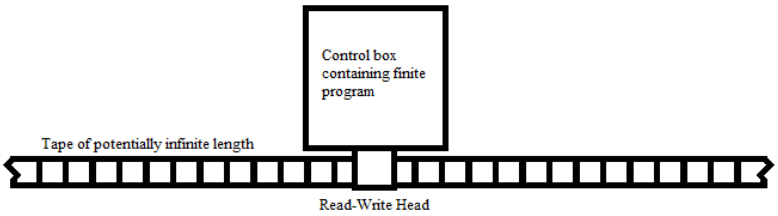

Figure 1: A simple visualization of a Turing machine. Note that spaces along the tape would be filled with symbols which can be read and written using the read-write head on the machine.

Definition 3.1. A **Turing Machine** is a 7-Tuple, $(Q, \Sigma, \Gamma, \delta, q_0, q_{accept}, q_{reject})$, where:

- Q is a finite set containing the states of the machine
- Σ is a finite set containing the machine's **input alphabet**
- Γ is the finite set containing th emachine's **tape alphabet** such that the **blank symbol** $\sqcup \in \Gamma$ and $\Sigma \subseteq \Gamma$
- δ is the **transition function** $\delta : Q \times \Gamma \to Q \times \Gamma \times \{L, R\}$
- q_0 is the **starting state** $q_0 \in Q$
- q_{accept} is the **accept state** $q_{accept} \in Q$
- q_{reject} is the **reject state** $q_{reject} \in Q$ such that $q_{reject} \neq q_{accept}$

A **configuration** represents the state of a Turing machine's read-write head along its tape, as well as the characters on the tape. For feasibly-sized tape inputs, a configuration is given as a string of the tape's characters listed starting from the left-most character and working right, with the state $q_n \in Q$ inserted to the left of the character currently being read by the read-write head of the machine. To exemplify this, we can introduce a new instance of a Turing Machine with a specific input, and an algorithm running on the input.

Example 3.1. Let's imagine a Turing machine running an algorithm which verifies whether or not a binary string of length n has an even weight (number of 1s in the binary string). It might achieve this by running the following algorithm:

1. Read each bit from left to right on the input string and cross off every other '1' character.
2. If in step 1 the tape contained no '1' characters, accept.
3. If in step 1 the tape contained a single '1' character, reject.
4. Return to the left-most character on the tape.
5. Return to step 1.

This particular Turing machine can be given formally as $M = (Q, \Sigma, \Gamma, \delta, q_1, q_{accept}, q_{reject})$ such that:

- $Q \coloneqq \{q_1, q_2, q_3, q_4, q_5, q_{accept}, q_{reject}\}$
- $\Sigma \coloneqq \{0, 1\}$
- $\Gamma \coloneqq \{0, 1, x, \textvisiblespace\}$
- The transition function δ is given as a state diagram (see figure 2)

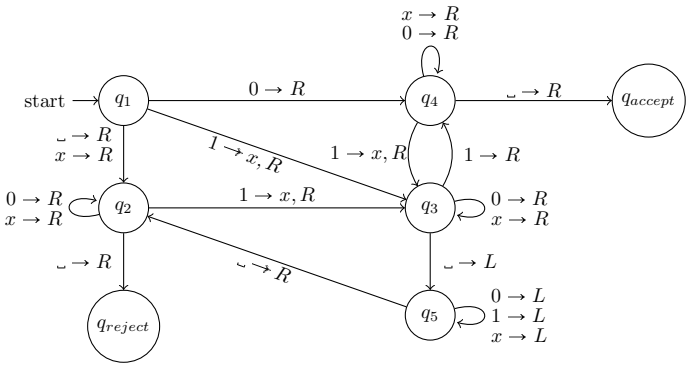

Figure 2: The transition function δ given as a finite state machine

Using the transition function δ as given by figure 2, we can show every configuration for a given input string. For the sake of the example, let's consider the string $\vec{x} = 1101$. We have the following configurations (read down each column, and then from left to right):

$q_1 1101$	$x1q_5 0x$	$xxq_3 0x$	$q_5 xx0x$	$xx0xq_{2\sqcup}$
$xq_3 101$	$xq_5 10x$	$xx0q_3 x$	$q_{5\sqcup} xx0x$	$xx0x_\sqcup q_{reject}$
$x1q_4 01$	$q_5 x10x$	$xx0xq_{3\sqcup}$	$q_2 xx0x$	
$x10q_4 1$	$q_{5\sqcup} x10x$	$xx0q_5 x$	$xq_2 x0x$	
$x10xq_{3\sqcup}$	$q_2 x10x$	$xxq_5 0x$	$xxq_2 0x$	
$x10q_5 x$	$xq_2 10x$	$xq_5 x0x$	$xx0q_2 x$	

We can clearly see that, since our input string has an odd number of '1' characters, our turing machine rejects it, signifying that it does not have an even weight. Next, let us walk through each configuration of the even-weighted input string $\vec{x} = 1001$. We have the following configurations:

$$q_1 1001$$
$$xq_3 001$$
$$x0q_3 01$$
$$x00q_3 1$$
$$x00xq_{4\sqcup}$$
$$x00x_\sqcup q_{accept}$$

Now, since our input string has an even number of '1' characters, our turing machine accepts it. [**2**]

4 Proof of Computability by Construction

The outcomes observed in **Example 3.1** are rather self-evident in the definition of a Turing machine, as two of its parameters are the accept state q_{accept} and the reject state q_{reject}. If a Turing machine ever reaches either of these states, then its algorithm will terminate. However, a third potential outcome when running an algorithm using a Turing machine is that the algorithm may never terminate. It is this possibility, the possibility that a Turing machine may run indefinitely for some input, from which much of the theory of computability emerges. In this section, we will build the definitions which found the theory of computability, and explore how we may prove that a function is computable.

Definition 4.1. An **alphabet** is a finite set of arbitrary characters which can be used in some code or language.

For example, the english alphabet (ignoring all punctuation and special characters) may define its alphabet as $A_{english} \coloneqq \{a, b, ..., z\}$

Definition 4.2. A **word** $\vec{x}$ is a string of characters, each of which belonging to some alphabet A.

Following from the previous example, we may construct words of varying lengths using the english alphabet, such as "the", "dog", "was", and "running". Each character composing each of these words belong to the alphabet $A_{english}$ defined above.

Definition 4.3. A **language** L is the set of all possible words $\vec{x} \in L$ of varying length, over some alphabet A.

Any combination of english characters imaginable will certainly be a member of the language $L_{english}$ which is defined on the alphabet $A_{english}$ mentioned previously.

Definition 4.4. A language L is **Turing-decidable** if there exists some Turing machine M such that, for each input word $\vec{x} \in L$, M either accepts or rejects it. [**2**]

This definition given is the definition which founds much of the theory of computability. It does so by use of the Church-Turing thesis, and the wealth of empirical evidence backing it, albeit there is no single, rigorous mathematical proof for this thesis. Essentially, one interpretation of the thesis states that if one wishes to prove that a certain operation is computable, one can do so by constructing a Turing machine which terminates for all possible inputs into that operation [**4**]. To display this, we will prove that the binary 'even weight verification' function introduced in **Example 3.1** is a computable function.

Proof 4.1. First, let us note that the input alphabet accepted by our Turing machine (its definition given in **Example 3.1**) $\Sigma \coloneqq \{0, 1\}$. This would imply that the **language** L emergent from this alphabet is simply the set of all binary strings (or **words**) of arbitrary length $n \geqslant 1$. Thus, our input language can be enumerated using $\mathbb{N}^2$. We must use $\mathbb{N}^2$ as opposed to simply $\mathbb{N}$ because we note that, for example, the strings $\vec{y} = 000101$ and $\vec{z} = 101$ are different inputs entirely, and will be handled differently by our Turing machine, even though their decimal values are identical. Therefore, we allow one degree of freedom to represent the length of the arbitrary input word $\vec{x}$, and the other to represent the decimal value of the arbitrary input word $\vec{x}$. Using this fact, we can partition our input language into four unique subsets, and engage in a 'proof by cases' on an arbitrary member of each such subset.

> **Case 1:** Let $\vec{x} \in L$ be an arbitrary-length input string with even weight, and starting with the '0' character. Our Turing machine will begin in state q_4. Since we know that there are an even number of '1' characters in $\vec{x}$, we can expect our Turing machine to 'bounce' back and forth between states q_4 and q_3 an even number of times, crossing off every other '1' character with an 'x' character, until ultimately producing some configuration $\ldots q_4 \sqcup$. This will finally yield the configuration $\ldots \sqcup q_{accept}$, and the Turing machine will terminate in state q_{accept} as expected.

Case 2: Let $\vec{x} \in L$ be an arbitrary-length input string with even weight, and starting with the '1' character. Our Turing machine will begin in state q_3 with the first '1' character crossed off. Since we know that there are an even number of '1' characters, and that we have already crossed off one of these characters, we can expect our Turing machine to 'bounce' back and forth between states q_3 and q_4 an odd number of times, crossing off every other '1' character with an 'x' character. Ultimately, this will produce the configuration $\ldots q_4 \sqcup$, which will finally yield the configuration $\ldots \sqcup q_{accept}$, and the Turing machine will terminate in state q_{accept} as expected.

Case 3: Let $\vec{x} \in L$ be an arbitrary-length input string with an odd number of '1' characters, and starting with the '1' character. Our Turing machine will begin in state q_3 with the first '1' character crossed off. Since we know that there are an odd number of '1' characters, and that we have already crossed off one of these characters, we can expect our Turing machine to 'bounce' back and forth between states q_3 and q_4 an even number of times, crossing off every other '1' character with an 'x' character. Ultimately, this will produce the configuration $\ldots q_3 \sqcup$, which will trigger the q_5 state, eventually returning the system to the q_2 state with the read-write head reading the first character of the string. Note that, since the input string had an odd weight, but had the first '1' character crossed off before the initial loop between states q_3 and q_4, it now has an odd number of '1' characters crossed off, and thus, an even number of '1' characters remaining. From here, the machine will proceed with this process recursively until it crosses off all '1' characters, and is left with the configuration $q_2 \ldots$, where q_2 will inevitably sweep through the entire string, producing the configuration $\ldots q_2 \sqcup$. As a result, the Turing machine will transition to the configuration $\ldots \sqcup q_{reject}$ as expected for our odd-weighted input string.

Case 4: Let $\vec{x} \in L$ be an arbitrary-length input string with odd weight, and starting with the '0' character. Our Turing machine will begin in state q_4. Since we know that there are an odd number of '1' characters, we can expect our Turing machine to 'bounce' back and forth between states q_4 and q_3, crossing off every other '1' character with an 'x' character. Ultimately, this will produce the configuration $\ldots q_3 \sqcup$, which will trigger the q_5 state, eventually returning the system to the q_2 state with the read-write head reading the first character of the string. Note that, since the input string had an odd weight, and since the transition between q_4 and q_3 took place an odd number of times starting with q_4, then in the current state with q_2 back at the beginning of the input string, we have the original input string, but with an odd number of '1' characters crossed off, and thus, an even number of '1' characters remaining. From here, our Turing machine will engage in an identical recursive process as given in **case 3**, meaning that it will terminate in state q_{reject} as expected.

Terefore, the binary 'even weight verification' function is computable, as it terminates for all input words $\vec{x} \in L$. $\square$

5 Disproof of Computability by Contradiction

Definitions/theorems to look into: The Halting Problem, Rice's Theorem; also provide at least one disproof of computability using Rice's Theorem

6 Conclusions

7 References

References

[1] National Research Council. 1999. Funding a Revolution: Government Support for Computing Research. Washington, DC: The National Academies Press. https://doi.org/10.17226/6323.

[2] Sipser, Michael. 2013. Introduction to the Theory of Computation. Cengage Learning. Third Edition. Print.

[3] Mainzer, Klaus. 2018. Proof of Computation: Digitization in Mathematics, Computer Science, and Philosophy. World Scientific. https://doi.org/10.1142/11005

[4] Evans, David. (2010). Church-Turing Thesis. University of Virginia. Web. http://www.cs.virginia.edu/ evans/cs3102-s10/classes/class15/class15.pdf