**CS120: Intro. to Algorithms and their Limitations** Hesterberg & Vadhan

# Lecture 17: The Church-Turing Thesis

*Harvard SEAS - Fall 2022* *2022-11-01*

## 1 Announcements

- MacCormick §5.6–5.7, §7.7–7.9
- Adam OH after class 11:15-12:15, SEC 2.122
- Lecture numbers updated.
- Sender-Receiver reflection at https://tinyurl.com/cs120sre4reflection .

## 2 Loose Ends: Assignment Extraction after Resolution

It turns out that closed sets of clauses that don't contain the empty clause are always satisfiable:

**Lemma 2.1.** *Let $\mathcal{C}$ be a closed set of clauses on $n$ variables, each of width at most $k$, such that $0 \notin \mathcal{C}$. Then an assignment that satisfies $\mathcal{C}$ exists and can be found in time $O(n + k \cdot |\mathcal{C}|)$.*

*Proof idea.* We generate our satisfying assignment one variable at a time. For each $v \in \{x_0, x_1, \ldots\}$ (in order):

1. If $\mathcal{C}$ contains a singleton clause $(v)$, then
2. If it contains $(\neg v)$ then
3. If it contains neither $(v)$ nor $(\neg v)$, then
4. $\mathcal{C}$ cannot contain both $(v)$ and $(\neg v)$, because

Once we have assigned a variable to a value, we set that variable's value in every clause and simplify. Crucially, we argue that even after assigning the variable, the set of clauses (a) does not contain 0, and (b) remains closed. (a) holds because of how we set $v$. Intuitively, (b) holds because assigning $v$ and then resolving two resulting clauses $C'$ and $D'$ is equivalent to first resolving the original clauses $C$ and $D$ and then assigning $v$. We know that $C \diamond D \in \mathcal{C}$ by closure of $\mathcal{C}$, so we have $C' \diamond D'$ after assigning $v$. $\square$

**Example:** Consider applying this procedure to the closed set of clauses below:

$$(\neg x_0 \vee x_3), (\neg x_1 \vee x_2), (x_1 \vee \neg x_2), (\neg x_0)$$

Lemma 2.1 and the lemma from last lecture that the output of the Resolution algorithm is a closed set of clauses imply that a satisfying assignment can be extracted from the final set $\mathcal{C}_{fin}$ of clauses it produces in time $O(n + k_{fin} \cdot |\mathcal{C}_{fin}|)$, where $k_{fin}$ is the maximum size among the clauses in $\mathcal{C}_{fin}$.

## 3 Introduction to Limits of Computation

Thus far in CS 120, we've focused on what algorithms can do, or what they can do efficiently. In the remainder of the course, we'll talk about what algorithms can't do, or can't do efficiently.

In particular, recall Lecture 3's lemma about reductions:

**Lemma 3.1.** *Let $\Pi$ and $\Gamma$ be computational problems such that $\Pi \leq \Gamma$. Then:*

1. *If there exists an algorithm solving $\Gamma$, then there exists an algorithm solving $\Pi$.*
2. *If there does not exist an algorithm solving $\Pi$, then there does not exist an algorithm solving $\Gamma$.*
3. *If there exists an algorithm solving $\Gamma$ with runtime $g(n)$, and $\Pi \leq_{T,f} \Gamma$, then there exists an algorithm solving $\Pi$ with runtime $O(T(n) + g(f(n)))$.*
4. *If there does not exists an algorithm solving $\Pi$ with runtime $O(T(n)+g(f(n))$, and $\Pi \leq_{T,f} \Gamma$, then there does not exist an algorithm solving $\Gamma$ with runtime $O(g(n))$.*

In the last unit of the course, we'll use the second lemma point: we'll find a problem $\Pi$ which we can prove is not solved by any Word-RAM algorithm, then reduce $\Pi$ to other problems $\Gamma$ to prove that no Word-RAM algorithm solves them.

Similarly, in the upcoming second-last unit of the course, we'll use the last lemma point: we'll assume that the problem $\Pi = SAT$ is not solved quickly by any Word-RAM algorithm, then reduce $SAT$ to other problems $\Gamma$ to prove that no Word-RAM algorithm solves them quickly.

Before we do so, let's consider how fundamental Word-RAM is to the statements above. That is, if we prove limitations of Word-RAM programs, are those limits specific to Word-RAM or are they more general/independent of technology? Could find substantially faster algorithms by choosing a different model of computation than Word RAM, like Python or Minecraft?

Unfortunately, the answer is conjectured to be “no”.

To explain why, we’ll first recall our simulation arguments that saying that the same problems are solvable by Word-RAM programs, Python programs, and so on.

## 4 The Church–Turing Thesis

**Theorem 4.1** (Turing-equivalent models)**.** *If a computational problem* $\Pi$ *is solvable in one of the following models of computation, then it is solvable in all of them:*

*Moreover, there is an algorithm (e.g. a RAM program) that can transform a program in any of these models of computation into an equivalent program in any of the others.*

**The Church–Turing Thesis:** The equivalence of many disparate models of computation leads to the Church–Turing Thesis, which has (at least) two different variants:

1.

2.

This is not a precise mathematical claim, and thus cannot be formally proven, but it has stood the test of time very well, even in the face of novel technologies like quantum computers (which have yet to be built in a scalable fashion); every problem that can be solved by a quantum algorithm can also be solved by a RAM program, albeit (as far as we know) much more slowly.

**Proof idea:**

**Simple and elegant models:**

**Input encodings:**

## 4.1 The Strong (or Extended) Church–Turing Thesis

The Church–Turing hypothesis only concerns problems solvable at all by these models of computation (Word-RAM programs, etc.). We haven't even seen any problems that are *not* solvable by Word-RAM programs—that will be a topic for the end of the course. There is, however, a stronger version of the Church–Turing hypothesis that also covers the efficiency with which we can solve problems.

Extended Church–Turing Thesis v1:

The Strong Church–Turing Thesis is not a precise mathematical claim, and thus cannot be formally proven. In fact, randomized algorithms, massively parallel computers, and quantum computers all could potentially provide an exponential savings in runtime. (For randomized algorithms, however, it is conjectured that they provide only a polynomial savings, as discussed in Lecture 8.)

If we modify the statement with some qualifiers, then these challenges no longer apply:

Extended Church–Turing Thesis v2:

"Deterministic" rules out both randomized and quantum computation, as both are inherently probabilistic. "Sequential" rules out parallel computation. This form of the Extended Church–Turing Thesis has stood the test of time for the approximately fifty years since it was formulated, even as computing technology has changed tremendously in that time.

Considering computational efficiency when comparing models of computation will be the subject of the next few lectures.