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 we assign $v = 1$.
2. If it contains $(\neg v)$ then assign $v = 0$.
3. If it contains neither (v) nor $(\neg v)$, then assign v arbitrarily.
4. $\mathcal{C}$ cannot contain both (v) and $(\neg v)$, because $\mathcal{C}$ is closed and does not contain 0.

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. □

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

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

Going through the variables in order, we set $x_0 = 0$ because we are forced to by the clause $(\neg x_0)$. After that, the clauses become:

$$(\neg 0 \vee x_3), (\neg x_1 \vee x_2), (\neg x_2 \vee x_1), (\neg 0)$$

which simplifies to

$$(\neg x_1 \vee x_2), (\neg x_2 \vee x_1).$$

These clauses don't include (x_1) or $(\neg x_1)$, so we can set x_1 as either 0 or 1. Arbitrarily choosing $x_1 = 1$, the clauses become:

$$(\neg 1 \vee x_2), (\neg x_2 \vee 1)$$

which simplifies to

$$(x_2).$$

Then we set $x_2 = 1$, and finally arbitrarily set $x_3 = 1$, yielding the satisfying assignment $(0, 1, 1, 1)$.

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 Π and Γ be computational problems such that $\Pi \leq \Gamma$. Then:*

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

In the last unit of the course, we'll use the second lemma point: we'll find a problem Π which we can prove is not solved by any Word-RAM algorithm, then reduce Π to other problems Γ 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 Γ 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* Π *is solvable in one of the following models of computation, then it is solvable in all of them:*

- *RAM programs*
- *Word-RAM programs*
- *XOR-extended RAM or Word-RAM programs*
- *%-extended RAM or Word-RAM programs*
- *Python programs*
- *OCaml programs*
- *C programs (modified to allow a variable/growing pointer size)*
- *Turing machines*
- *Lambda calculus*
- $\vdots$

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. The (equivalent) models of computation in Theorem 4.1 capture our intuitive notion of an algorithm.
2. Every physically realizable computation can be simulated by one of the models in Theorem 4.1.

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: A theorem like this is proven via "compilers" and simulation arguments like we have seen several times, giving a procedure to transform programs from one model to another (e.g. simulating XOR-extended Word-RAMs by ordinary Word-RAMs). Like we have seen, we can write simulators for RAM programs in high-level languages like Python and OCaml, and conversely those high-level languages are compiled down to assembly code, which is essentially Word-RAM code.

Simple and elegant models: The λ calculus and Turing machines are extremely simple (even moreso than the RAM model) and mathematically elegant models of computation, coming from the work of Church and Turing, respectively, in 1936, in their attempts to formalize the concept of an algorithm (prior to, and indeed inspiring, the development of general-purpose computer technology). We may describe Turing machines in more detail in a future lecture; they're similar

to the Word-RAM model, but with a fixed word size and memory access only at a pointer that moves in increments of ± 1. We won't have time to describe the lambda calculus, but it provided the foundation for future functional programming languages like OCaml, and one of the theorems in Turing's paper established the equivalence of Turing machines and the λ calculus.

Input encodings: One detail we are glossing over in Theorem 4.1 is that the different models have different ways of representing their inputs and outputs. For example, natural numbers can be represented directly in RAM programs, but in a Turing machine they need to be encoded as a string (e.g. using binary representation), and in the lambda calculus, they are represented as an operator on functions (which maps a function $f(x)$ to $f^{(n)}(x) = f(f(\cdots f(x)))$). So to be maximally precise, these models are equivalent up to the representation of input and output.

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: Every physically realizable model of computation can be simulated by a Word-RAM program (or Turing Machine, or Python program) with only a *polynomial* slowdown in runtime. Conversely, reality can simulate Word-RAM programs in real time only polynomially slower than their defined runtime.

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: Every physically realizable, deterministic, and sequential model of computation can be simulated by a Word-RAM program (or Turing Machine, or Python program) with only a polynomial slowdown in runtime. Conversely, reality can simulate Word-RAM programs in real time only polynomially slower than their defined runtime.

"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.

Note: in contrast to the above claims about Word-RAM, we had a pset where Word-RAM simulated RAM with an exponential slowdown, and our RAM to Word-RAM simulation theorem also has a slowdown factor that can get exponentially large (due to bitlength of numbers). So, the choice of base model (Word-RAM) is important here in a way it isn't for the regular Church–Turing Thesis.

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