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

Lecture 14: Logic

Harvard SEAS - Fall 2022 *2022-10-25*

1 Announcements

- Special 121.5 lecture: Minecraft in Minecraft, 1pm Friday in SEC 1.316
- Active Learning Exercise on Thursday. 3 more SREs, so everyone sender for 2/3.
- Ps7 (not out yet) deadline extended 1 week.

Recommended Reading:

- Lewis–Zax Ch. 9–10.
- Roughgarden IV, Sec. 21.5, Ch. 24.

2 Propositional Logic

Motivation: Logic is a fundamental building block of computation (e.g. digital circuits), and is also a very expressive language for encoding computational problems we want to solve.

Definition 2.1 (informal)**.** A *boolean formula* φ is a formula built up from a finite set of variables, say $x_0, \ldots, x_{n-1}$, using the logical operators $\wedge$ (AND), $\vee$ (OR), and $\neg$ (NOT), and parentheses.

Every boolean formula φ on n variables defines a boolean function, which we'll abuse notation and also denote by $\varphi : \{0,1\}^n \to \{0,1\}$, where we interpret 0 as false and 1 as true, and give $\wedge, \vee, \neg$ their usual semantics (meaning).

See the Lewis–Zax text for formal, inductive definitions of boolean formulas and the corresponding boolean functions.

Examples:

$$\varphi_{maj}(x_0, x_1, x_2) = (x_0 \wedge x_1) \vee (x_1 \wedge x_2) \vee (x_2 \wedge x_0)$$

is a boolean formula. It evaluates to 1 if at least two of its inputs are 1. For instance, $\phi_{maj}(1,1,0) = 1$ and $\phi_{maj}(1,0,0) = 0$.

$$\varphi_{pal}(x_0, x_1, x_2, x_3) = ((x_0 \wedge x_3) \vee (\neg x_0 \wedge \neg x_3)) \wedge ((x_1 \wedge x_2) \vee (\neg x_1 \wedge \neg x_2))$$

is a boolean formula. It evaluates to 1 if the input $x_0x_1x_2x_3$ is a palindrome.

Definition 2.2. A *literal* is a variable (e.g. x_i) or its negation ($\neg x_i$).

A boolean formula is in *disjunctive normal form (DNF)* if it is the OR of a sequence of *terms*, each of which is the AND of a sequence of literals.

A boolean formula is in *conjunctive normal form (CNF)* if it is the AND of a sequence of *clauses*, each of which is the OR of a sequence of literals.

Note terms and clauses may contain duplicate literals, but if a term or clause contains multiple copies of a variable x, it's equivalent to a term or clause with just one copy (since $x \vee x = x$ and $x \wedge x = x$). We can also remove any clause or term with both a variable x and its negation $\neg x$, as that clause or term will be always true (in the case of a clause) or always false (in the case of a term). We define a function Simplify which takes a clause and performs those simplifications: that is, given a clause B, Simplify(B) removes duplicates of literals from clause B, and returns 1 if B contains both a literal and its negation. Also, if we have an order on variables (e.g. x_0, x_1, $\dots$), Simplify(B) also sorts the literals in order of their variables.

Also by convention, an empty term is always true and an empty clause is always false.

Lemma 2.3. *For every boolean function $f : \{0,1\}^n \to \{0,1\}$, there are boolean formulas φ and ψ in DNF and CNF, respectively, such that $f \equiv \varphi$ and $f \equiv \psi$, where we use $\equiv$ to indicate equivalence as functions, i.e. $f \equiv g$ iff $\forall x : f(x) = g(x)$.*

Proof. For a function $f : \{0,1\}^n \to \{0,1\}$, we can define the DNF

$$\varphi(x_0, \dots, x_{n-1}) = \bigvee_{\alpha \in \{0,1\}^n : f(\alpha)=1} \left((x_0 = \alpha_0) \wedge (x_1 = \alpha_1) \wedge \cdots \wedge (x_{n-1} = \alpha_{n-1})\right).$$

Note that $x_i = \alpha_i$ can be rewritten as either x_i (with $\alpha_i = 1$) or $\neg x_i$ (with $\alpha_i = 0$). For example, applying to the palindrome function on 4 bits, we get

$$\varphi(x_0, x_1, x_2, x_3) = (x_0 \wedge x_1 \wedge x_2 \wedge x_3) \vee (x_0 \wedge \neg x_1 \wedge \neg x_2 \wedge x_3) \vee (\neg x_0 \wedge x_1 \wedge x_2 \wedge \neg x_3) \vee (\neg x_0 \wedge \neg x_1 \wedge \neg x_2 \wedge \neg x_3),$$

where the terms correspond to the satisfying assignments $(1,1,1,1)$, $(1,0,0,1)$, $(0,1,1,0)$, and $(1,1,1,1)$.

For the CNF, we define

$$\varphi(x_0, \dots, x_{n-1}) = \bigwedge_{\alpha \in \{0,1\}^n : f(\alpha)=0} \left((x_0 \neq \alpha_0) \vee (x_1 \neq \alpha_1) \vee \cdots \vee (x_{n-1} \neq \alpha_{n-1})\right).$$

For example, the majority function on 3 bits can be written as:

$$\psi(x_0, x_1, x_2) = (x_0 \vee x_1 \vee x_2) \wedge (\neg x_0 \vee x_1 \vee x_2) \wedge (x_0 \vee \neg x_1 \vee x_2) \wedge (x_0 \vee x_1 \vee \neg x_2),$$

with the clauses corresponding to the 4 non-satisfying assignments $(0,0,0), (1,0,0), (0,1,0), (1,1,1)$. This example shows that the DNF and CNF given by the general construction are not necessarily the smallest ones possible for a given function, as the majority function can also be expressed by the following simpler CNF formula:

$$(x_0 \vee x_1) \wedge (x_0 \vee x_2) \wedge (x_1 \vee x_2).$$

□

3 Computational Problems in Propositional Logic

Input : A boolean formula φ on n variables
Output : An $\alpha \in \{0,1\}^n$ such that $\varphi(\alpha) = 1$, or $\perp$ if no satisfying assignment exists

Computational Problem Satisfiability

It is common to restrict the boolean formulas to ones in CNF or DNF.

Input	**:** A CNF formula φ on n variables
Output	**:** An $\alpha \in \{0,1\}^n$ such that $\varphi(\alpha) = 1$, or $\perp$ if no satisfying assignment exists

Computational Problem CNF-Satisfiability

Input	**:** A DNF formula φ on n variables
Output	**:** An $\alpha \in \{0,1\}^n$ such that $\varphi(\alpha) = 1$, or $\perp$ if no satisfying assignment exists

Computational Problem DNF-Satisfiability

One of these problems is algorithmically very easy. Which one?

DNF satisfiability is easy - since we only need to satisfy a single term and then we are done, the only difficulties are when we have zero terms (in which case the problem is defined to be 0), or every term has a contradiction (both a variable and its negation).

4 Modelling using Satisfiability

One of the reasons for the importance of Satisfiability is its richness for encoding other problems. Thus any effort gone into optimizing algorithms for Satisfiability (aka "SAT Solvers") can be easily be applied to other problems we want to solve.

Theorem 4.1. *Graph k-Coloring on graphs with n nodes and m edges can be reduced in time $O(n + km)$ to CNF-Satisfiability on boolean formulas with kn variables and $n + km$ clauses.*

Proof.

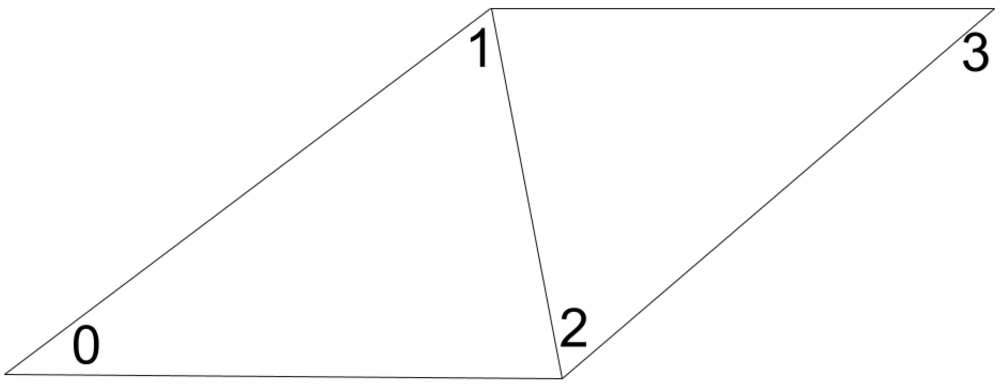
Given $G = (V, E)$ and $k \in \mathbb{N}$, we will construct a CNF ϕ_G that captures the graph coloring problem. In ϕ_G, we construct variables $x_{v,i}$ where $v \in V$ and $i \in [k]$. Intuitively, $x_{v,i}$ captures vertex v being assigned to color i. We then have a few types of clauses:

1. $(x_{v,0} \vee x_{v,1} \vee \cdots \vee x_{v,i})$ for all $v \in V$. (Each vertex must be assigned a color)

2. $(\neg x_{u,i} \vee \neg x_{v,i})$ for every edge $\{u, v\} \in E$ and every color $i \in [k]$. From De Morgan's Law, this is equivalent to the more intuitive $\neg(x_{u,i} \wedge x_{v,i})$. (The endpoints of an edge cannot be assigned the same color.)

3. In addition, we can require all vertices to be assigned at most one color (right now a valid solution could assign multiple colors). To avoid this, we can include clauses $(\neg x_{v,i} \vee \neg x_{v,j})$ for $i, j \in [k]$ where $i \neq j$. But we don't actually need to include these, and doing so would increase the number of clauses to nk^2.

For instance, if G is the graph below,



then we make the following SAT instance ϕ_G:

$$(x_{0,0} \vee x_{0,1} \vee x_{0,2}) \wedge (x_{1,0} \vee x_{1,1} \vee x_{1,2}) \wedge (x_{2,0} \vee x_{2,1} \vee x_{2,2}) \wedge (x_{3,0} \vee x_{3,1} \vee x_{3,2}) \wedge$$

$$(\neg x_{0,0} \vee \neg x_{1,0}) \wedge (\neg x_{0,1} \vee \neg x_{1,1}) \wedge (\neg x_{0,2} \vee \neg x_{1,2}) \wedge$$

$$(\neg x_{0,0} \vee \neg x_{2,0}) \wedge (\neg x_{0,1} \vee \neg x_{2,1}) \wedge (\neg x_{0,2} \vee \neg x_{2,2}) \wedge$$

$$(\neg x_{2,0} \vee \neg x_{1,0}) \wedge (\neg x_{2,1} \vee \neg x_{1,1}) \wedge (\neg x_{2,2} \vee \neg x_{1,2}) \wedge$$

$$(\neg x_{3,0} \vee \neg x_{1,0}) \wedge (\neg x_{3,1} \vee \neg x_{1,1}) \wedge (\neg x_{3,2} \vee \neg x_{1,2}) \wedge$$

$$(\neg x_{2,0} \vee \neg x_{3,0}) \wedge (\neg x_{2,1} \vee \neg x_{3,1}) \wedge (\neg x_{2,2} \vee \neg x_{3,2})$$

We then run the SAT oracle on ϕ_G and get an assignment α. If $\alpha = \perp$, we say G is not k-colorable. Otherwise, we construct and output the coloring

$$f_\alpha = \min\{i \in [k] : \alpha_{v,i} = 1\}.$$

(The minimum is just being used to pick out one of the colors i such that $\alpha_{v,i} = 1$ in case there are multiple, since we didn't include Clauses of Type 3.)

The runtime essentially follows from our description. If we start by removing isolated vertices (i.e. those with no adjacent edges), we have $n' \leq 2m$ actual vertices under consideration in our SAT clause, and so have a runtime of $O(n) + O(n'k) + O(mk) = O(n + km)$.

For correctness, we make two claims:

Claim 4.2. *If G has a valid k coloring, ϕ_G is satisfiable.*

$\implies$ don't incorrectly output $\perp$.

Claim 4.3. *If α satisfies ϕ_G, then f_α is a proper k-coloring of G.*

$\implies$ if we output a coloring, it will be proper.

Both of these claims are worth checking. Note that f_α is *well-defined* because α satisfies clauses of type 1 and is *proper* due to clauses of type 2.

□

Unfortunately, the fastest known algorithms for CNF-Satisfiability have worst-case runtime exponential in n, However, enormous effort has gone into designing heuristics that complete much more quickly on many real-world instances. In particular, SAT Solvers—with many additional optimizations—were used to solve large-scale graph coloring problems arising in the 2016 US Federal Communications Commission (FCC) auction to reallocate wireless spectrum. Roughly, those instances had $k = 23$ (corresponding to UHF channels 14–36), n in the thousands (corresponding to television stations being reassigned to one of the k channels), m in the tens of thousands (corresponding to pairs of stations with overlapping broadcast areas — similarly to how you are viewing interval scheduling on ps7). Over the course of the one-year auction, tens of thousands of coloring instances were produced, and roughly 99% of them were solved within a minute!

Thus motivated, we will now turn to algorithms for Satisfiability, to get a taste of some of the ideas that go into SAT Solvers.

5 Resolution (Preview)

SAT Solvers are algorithms to solve CNF-Satisfiability. Although they have worst-case exponential running time, on many "real-world" instances, they terminate more quickly with either (a) a satisfying assignment, or (b) a "proof" that the input formula is unsatisfiable.

The form of these unsatisfiability proofs is (implicitly) based on *resolution*. The idea is to repeatedly derive new clauses from the original clauses (using a valid deduction rule) until we either derive an empty clause (which is false, and a proof that the original formula is unsatisfiable) or we cannot derive any more clauses.

Definition 5.1 (resolution rule)**.** For clauses C and D, define

$$C \diamond D = \begin{cases} \text{Simplify}((C - \{\ell\}) \vee (D - \{\neg\ell\})) & \text{if } \ell \text{ is a literal s.t. } \ell \in C \text{ and } \neg\ell \in D \\ 1 & \text{if there is no such literal } \ell \end{cases}$$

Here $C - \{\ell\}$ means remove literal ℓ from clause C, 1 represents `true`. As noted last time, if C and D can be resolved with respect to more than one literal ℓ, then for all choices of ℓ we will have $\text{Simplify}((C - \{\ell\}) \vee (D - \{\neg\ell\})) = 1$, so $C \diamond D$ is well-defined.
Examples:

$$(x_0 \vee \neg x_1 \vee x_3 \vee \neg x_5) \diamond (x_1 \vee \neg x_4 \vee \neg x_5) = (x_0 \vee x_3 \vee \neg x_4 \vee \neg x_5)$$

For a singleton clause:

$$(x_0) \diamond (\neg x_0) = \emptyset = \text{FALSE}.$$

We could also have a clause that appears to be resolveable in two ways:

$$(x_0 \vee x_1 \vee \neg x_4) \diamond (\neg x_0 \vee x_2 \vee x_4) = (x_0 \vee \neg x_0 \vee x_1 \vee x_2) \text{ OR } = (x_1 \vee x_2 \vee \neg x_4 \vee x_4)$$

but both of these classes are equivalent, since they are tautologies. Thus, if there are multiple ways to resolve, all ways of resolving result in TRUE.

From now on, it will be useful to view a CNF formula as just a set $\mathcal{C}$ of clauses.

Definition 5.2. Let $\mathcal{C}$ be a set of clauses over variables $x_0, \ldots, x_{n-1}$. We say that an assignment $\alpha \in \{0,1\}^n$ *satisfies* $\mathcal{C}$ if α satisfies all of the clauses in $\mathcal{C}$, or equivalently α satisfies the CNF formula

$$\varphi(x_0, \ldots, x_{n-1}) = \bigwedge_{C \in \mathcal{C}} C(x_0, \ldots, x_{n-1}).$$

Lemma 5.3. *Let $\mathcal{C}$ be a set of clauses and let $C, D \in \mathcal{C}$. Then $\mathcal{C}$ and $\mathcal{C} \cup \{C \diamond D\}$ have the same set of satisfying assignments. In particular, if $C \diamond D$ is the empty clause, then $\mathcal{C}$ is unsatisfiable.*

Next time we'll see how repeated application of the resolution rule yields a correct algorithm for deciding satisfiability (and also how to extract a satisfying assignment at the end if the formula is satisfiable).