Holy Chapter 6

Emil Straschil

ETH Zurich

2025

Proof Systems

Proof System

A **proof system** is a quadruple $\Pi = (S, P, \tau, \phi)$

- S is a set of *statements*.
- P is a set of *proofs*.
- $\tau : S \to \{0, 1\}$ is the *truth function*. A statement $s \in S$ is *true* if $\tau(s) = 1$.
- $\phi : S \times P \to \{0, 1\}$ is the *verification function*. $p \in P$ is a *valid* proof for $s \in S$ if $\phi(s, p) = 1$.

Efficently Computable

τ does **not** need to be efficiently computable, but ϕ needs to be.
This means that you cannot use τ in your definition of ϕ.

Specifically, saying something like

$$\phi(s, p) = 1 \iff \tau(s) = 1$$

is **not** allowed.

Proof System Properties

Soundness

A proof system is *sound* if no false statement has a proof. This means that for some statement $s \in S$

$$\exists p \in P \text{ with } \phi(s, p) = 1 \implies \tau(s) = 1$$

Completeness

A proof system is *complete* if every true statement has a proof. This means that for all $s \in S$

$$\tau(s) = 1 \implies \exists p \in P \text{ with } \phi(s, p) = 1$$

You can use those statements to prove the properties.

Proof System Example

We define the proof system $MYSAT_k$

- S is the set of all prop. logic formulas with variables $X_0, X_1, \ldots, X_k$
- $P = \{0,1\}^k$ (the set of bitstrings of length $k+1$)
- $\tau(F) = 1$ if the formula is satisfiable
- $\phi(F,b) = 1$ if F is true under the interpretation $X_0 = b_0, X_1 = b_1, \ldots, X_k = b_k$

For example, for $MYSAT_2$: $F = X_0 \wedge (X_1 \vee X_2) \in S$ and $b = 101 \in P$ and we have $\phi(F,b) = 1$

Logic

Some words:

- *Syntax* is what symbols (and how) we can use
- *Semantics* is how the formula can be interpreted
- *Free* symbols need to be defined by the *interpretation*
- Semantics define if an interpretation has the truth value *true* of *false*. We write $\mathcal{A}(F) = 1/0$

Model

$\mathcal{A}$ is a *model* for F if it is suitable for F and $\mathcal{A}(F) = 1$.

Hello Chapter 2

Basically all logics contain the usual symbols and rules we know from Chapter 2. We also re-use the definitions.

- $\vee, \wedge, \neg, \rightarrow$
- tautology, satisfiable, ...
- distributivity, de-morgan, commutativity, ...
- ...

Useful Lemma

Lemma 6.3

The following statement are equivalent:

1. $\{F_1, F_2, \ldots, F_k\} \models G$
2. $(F_1 \wedge F_2 \wedge \cdots \wedge F_k) \rightarrow G$ is a tautology
3. $\{F_1, F_2, \ldots, F_k, \neg G\}$ is unsatisfiable.

This means instead of needing to prove (1) or (2) we can also show (3). You will learn about *resolution calculus* soon, which let's us prove statements of the form (3).

Calculi

Calculus

A *calculus* is a finite set of *derivation rules*.

For example, a derivation rule could be:

$$A \wedge B \vdash_R A$$

Derivations are purely syntactic. If the derivation rule $A \wedge B \vdash A$ does not exist in the calculus, you cannot use it.

Calculi Properties

Correctness

A derivation rule $\vdash_R$ is *correct* if

$$F \vdash_R G \implies F \models G$$

Soundness

A calculus K is *sound* if every derivation rule is correct:

$$F \vdash_K G \implies F \models G$$

Completeness

A calculus K is *complete* if every logical consequence can be derived.

$$F \models G \implies F \vdash_K G$$

Derivation Example

Say we have the rules:

$$F \vdash_1 F \wedge F$$
$$\{F, G\} \vdash_2 F \rightarrow G$$

Now we could derive from $\{A\}$:

$$A \vdash_1 A \wedge A$$
$$\{A, A \wedge A\} \vdash_2 A \rightarrow (A \wedge A)$$

Normal Forms

DNF

A formula is in *disjunctive normal form* if it is of the form

$$(X_{11} \wedge \cdots \wedge X_{1k}) \vee \cdots \vee (X_{m1} \wedge \cdots \wedge X_{ml})$$

CNF

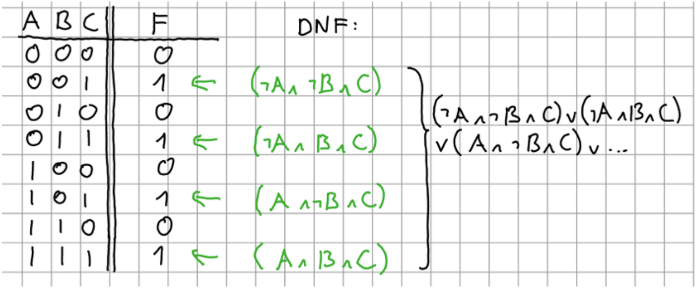
A

formula is in *conjunctive normal form* if it is of the form

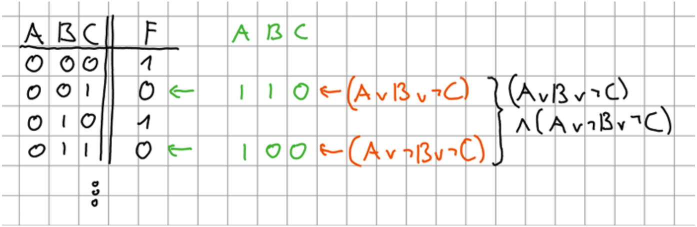
$$(X_{11} \vee \cdots \vee X_{1k}) \wedge \cdots \wedge (X_{m1} \vee \cdots \vee X_{ml})$$

Note that $(A \vee B) \equiv (A) \vee (B)$ is in CNF and DNF.

DNF


A B C
F
DNF:
0 0 0 0
0 0 1 1
0 1 0 0
0 1 1 1
1 0 0 0
1 0 1 1
1 1 0 0
1 1 1 1
(¬A ∧ ¬B ∧ C)
(¬A ∧ B ∧ C)
(A ∧ ¬B ∧ C)
(A ∧ B ∧ C)
(¬A ∧ ¬B ∧ C) ∨ (¬A ∧ B ∧ C)
∨ (A ∧ ¬B ∧ C) ∨ ...

CNF



Exercise 1 - Proof Systems

11.4 Combining Proof Systems ($\star$) ***(8 Points)***

Let

$$\Sigma = (\mathcal{S}, \mathcal{P}, \tau, \phi)$$

be a complete and sound proof system.

a) Define $\mathcal{P}'$ and ϕ' so that

$$\Sigma' = (\mathcal{S} \times \mathcal{S} \times \mathcal{S}, \mathcal{P}', \tau', \phi')$$

is a complete and sound proof system (and prove it!), where

$$\tau'\big((s_1, s_2, s_3)\big) = 1 \iff \text{at least 2 among } \tau(s_1), \tau(s_2), \tau(s_3) \text{ are equal to } 1.$$

b) Let

$$\overline{\Sigma} = \big(\mathcal{S}^2, \overline{\mathcal{P}}, \overline{\tau}, \overline{\phi}\big)$$

be a complete and sound proof system with

$$\overline{\tau}\big((s_1, s_2)\big) = 1 \iff \text{exactly 1 of the statements is true in } \Sigma, \text{ that is, } \tau(s_1) = 1 \text{ or } \tau(s_2) = 1, \text{but not both.} \tag{1}$$

Define $\mathcal{P}^*$ and ϕ^* so that $\Sigma^* = (\mathcal{S}, \mathcal{P}^*, \tau^*, \phi^*)$ is a complete and sound proof system (and prove it!), where

$$\tau^*(s) = 1 \iff \tau(s) = 0.$$

Solution 1a

a) Let $\mathcal{P}' = \{1,2,3\} \times \{1,2,3\} \times \mathcal{P} \times \mathcal{P}$ and let

$$\phi'\big((s_1,s_2,s_3),(i,j,p,p')\big) = 1 \iff i \neq j \text{ and } \phi(s_i,p) = 1 \text{ and } \phi(s_j,p') = 1.$$

To prove completeness, suppose that $\tau'(s_1,s_2,s_3) = 1$. This means that at least two s_i, s_j out of s_1,s_2,s_3 are true. By completeness of Σ there exist p and p' in $\mathcal{P}$ such that $\phi(s_i,p) = \phi(s_j,p') = 1$. This means that, with the given definition of ϕ', the 4-tuple (i,j,p,p') is a valid proof for (s_1,s_2,s_3) in Σ'.

To prove soundness, suppose that for some $(s_1,s_2,s_3) \in \mathcal{S}^3$ and some $(i,j,p,p') \in \mathcal{P}'$ we have

$$\phi'\big((s_1,s_2,s_3),(i,j,p,p')\big) = 1.$$

Then, by soundness of Σ, since $\phi(s_i,p) = 1$ and $\phi(s_j,p') = 1$ we get that s_i and s_j are true in Σ, which means that, since $i \neq j$, at least two out of s_1,s_2,s_3 are true in Σ, and by definition of τ' the statement (s_1,s_2,s_3) is true in Σ'.

Solution 1b

b) If there are no true statements in Σ, then the solution is trivial: simply define a proof set $\mathcal{P}^*$ with a single element, and the verification function ϕ^* evaluates to true for each statement in $\mathcal{S}$ and the only proof in $\mathcal{P}^*$. Therefore, we can assume that $\mathcal{S}$ contains at least one true statement. Let $\mathcal{P}^* = \mathcal{S} \times \mathcal{P} \times \overline{\mathcal{P}}$ and let

$$\phi^*\big(s, (s', p', \overline{p})\big) = 1 \iff \phi(s', p') = 1 \text{ and } \text{ and } \overline{\phi}\big((s', s), \overline{p}\big) = 1.$$

To prove completeness of Σ^*, suppose that $\tau^*(s) = 1$ which means $\tau(s) = 0$. By assumption, there exists an element $s' \in \mathcal{S}$ with $\tau(s) = 1$. By completeness of Σ we can find a proof $p' \in \mathcal{P}$ such that $\phi(s', p') = 1$. Furthermore, since $\tau(s) = 0$, this means that $\overline{\tau}(s', s) = 1$, because only s' is true in Σ. By completeness of $\overline{\Sigma}$ we find a proof $\overline{p}$ with $\overline{\phi}((s', s), \overline{p}) = 1$. Therefore $(s', p', \overline{p})$ is a valid proof of s in Σ^* with the above definition of ϕ^*. To prove soundness of Σ^*, suppose that $\phi^*\big(s, (s', p', \overline{p})\big) = 1$. This means 1) $\overline{\phi}((s', s), \overline{p}) = 1$, which by soundness of $\overline{\Sigma}$ this means that exactly one among s', s is true in Σ and 2) $\phi(s', p') = 1$, which by soundness of Σ implies that $\tau(s') = 1$. These two facts together imply that s is false in Σ. Therefore $\tau^*(s) = 1$.

Exercise 2 - CNF and DNF

You are given the following formula F (only as a function table).

1. Find an equivalent formula G in *disjunctive normal form*.
2. Find an equivalent formula H in *conjunctive normal form*.

A	B	C	F
0	0	0	1
0	0	1	0
0	1	0	0
0	1	1	1
1	0	0	0
1	0	1	0
1	1	0	0
1	1	1	1

Solution 2

We find the DNF by taking all the 1-rows. We "and" the variables and "or" those subformulas:

$$(\neg A \wedge \neg B \wedge \neg C) \vee (\neg A \wedge B \wedge C) \vee (A \wedge B \wedge C)$$

We find the CNF by taking all the 0-rows. For each row, we negate the variables, "or" them and "and" those subformulas:

$$(A \vee B \vee \neg C) \wedge (A \vee \neg B \vee C) \wedge (\neg A \vee B \vee C) \wedge (\neg A \vee B \vee \neg C) \wedge (\neg A \vee \neg B \vee C)$$

Exercise 3 - Deriving Formulas

Consider the following calculus:

$$\begin{aligned} \varnothing &\vdash_1 F \vee (F \rightarrow G) \\ \{F \vee G, \neg F\} &\vdash_2 G \\ \{F \rightarrow G, G \rightarrow H\} &\vdash_3 F \rightarrow H \\ \{F, \neg G\} &\vdash_4 F \rightarrow G \end{aligned}$$

Formally derive $A \rightarrow C$ from $\{A, \neg B\}$ in this calculus.
Hint: use every rule exactly once.

Solution 3

(1) A

(2) $\neg B$

(3) $\{(1),(2)\} \vdash_4 A \rightarrow B$

(4) $\varnothing \vdash_1 B \vee (B \rightarrow C)$

(5) $\{(4),(2)\} \vdash_2 B \rightarrow C$

(6) $\{(3),(5)\} \vdash_3 A \rightarrow C$