Propositional Resolution

A deductive system

Frédéric Prost

Université Grenoble Alpes

January 2023

Last course

- Important Equivalences
- Substitutions and replacement
- Normal Forms

John, Peter and Mary by simplification

$$(p \Rightarrow \neg j) \wedge (\neg p \Rightarrow j) \wedge (j \Rightarrow m) \Rightarrow m \vee p$$

John, Peter and Mary by simplification

$$(p \Rightarrow \neg j) \land (\neg p \Rightarrow j) \land (j \Rightarrow m) \Rightarrow m \lor p$$

$$\neg((p \Rightarrow \neg j) \land (\neg p \Rightarrow j) \land (j \Rightarrow m)) \lor m \lor p$$

John, Peter and Mary by simplification

$$(p \Rightarrow \neg j) \wedge (\neg p \Rightarrow j) \wedge (j \Rightarrow m) \Rightarrow m \vee p$$

$$\neg((p \Rightarrow \neg j) \wedge (\neg p \Rightarrow j) \wedge (j \Rightarrow m)) \vee m \vee p$$

$$\neg(p \Rightarrow \neg j) \vee \neg(\neg p \Rightarrow j) \vee \neg(j \Rightarrow m) \vee m \vee p$$

John, Peter and Mary by simplification

$$(p \Rightarrow \neg j) \wedge (\neg p \Rightarrow j) \wedge (j \Rightarrow m) \Rightarrow m \vee p$$

$$\neg((p \Rightarrow \neg j) \wedge (\neg p \Rightarrow j) \wedge (j \Rightarrow m)) \vee m \vee p$$

$$\neg(p \Rightarrow \neg j) \vee \neg(\neg p \Rightarrow j) \vee \neg(j \Rightarrow m) \vee m \vee p$$

$$(p \wedge \neg\neg j) \vee (\neg p \wedge \neg j) \vee (j \wedge \neg m) \vee m \vee p$$

John, Peter and Mary by simplification

$$(p \Rightarrow \neg j) \land (\neg p \Rightarrow j) \land (j \Rightarrow m) \Rightarrow m \lor p$$

$$\neg((p \Rightarrow \neg j) \land (\neg p \Rightarrow j) \land (j \Rightarrow m)) \lor m \lor p$$

$$\neg(p \Rightarrow \neg j) \lor \neg(\neg p \Rightarrow j) \lor \neg(j \Rightarrow m) \lor m \lor p$$

$$(p \land \neg\neg j) \lor (\neg p \land \neg j) \lor (j \land \neg m) \lor m \lor p$$

with $x \lor (x \land y) \equiv x$

$$(\neg p \land \neg j) \lor (j \land \neg m) \lor m \lor p$$

John, Peter and Mary by simplification

$$(p \Rightarrow \neg j) \wedge (\neg p \Rightarrow j) \wedge (j \Rightarrow m) \Rightarrow m \vee p$$

$$\neg((p \Rightarrow \neg j) \wedge (\neg p \Rightarrow j) \wedge (j \Rightarrow m)) \vee m \vee p$$

$$\neg(p \Rightarrow \neg j) \vee \neg(\neg p \Rightarrow j) \vee \neg(j \Rightarrow m) \vee m \vee p$$

$$(p \wedge \neg\neg j) \vee (\neg p \wedge \neg j) \vee (j \wedge \neg m) \vee m \vee p$$

with $x \vee (x \wedge y) \equiv x$

$$(\neg p \wedge \neg j) \vee (j \wedge \neg m) \vee m \vee p$$

with $x \vee (\neg x \wedge y) \equiv x \vee y$

$$\neg j \vee j \vee m \vee p = 1$$

Overview

Plan

Definition 1.5.1

A Boolean Algebra is a set of:

- at least two elements 0 and 1
- and three operations, complement ($\overline{x}$), sum ($+$) and product (.)

Definition 1.5.1

A Boolean Algebra is a set of:

- at least two elements 0 and 1
- and three operations, complement ($\overline{x}$), sum ($+$) and product (.)
- such that :

1. the sum is associative, commutative, with neutral element 0
2. the product is associative, commutative, with neutral element 1

Definition 1.5.1

A Boolean Algebra is a set of:

- at least two elements 0 and 1
- and three operations, complement ($\overline{x}$), sum ($+$) and product (.)
- such that :

1. the sum is associative, commutative, with neutral element 0
2. the product is associative, commutative, with neutral element 1
3. the product is distributive over the sum
4. the sum is distributive over the product

Definition 1.5.1

A Boolean Algebra is a set of:

- at least two elements 0 and 1
- and three operations, complement ($\overline{x}$), sum ($+$) and product (.)
- such that :

1. the sum is associative, commutative, with neutral element 0
2. the product is associative, commutative, with neutral element 1
3. the product is distributive over the sum
4. the sum is distributive over the product
5. negation laws:
    - $x + \overline{x} = 1$,
    - $x.\overline{x} = 0$.

Propositional logic is a Boolean Algebra

The axioms can be proven using the truth tables.

Propositional logic is a Boolean Algebra

The axioms can be proven using the truth tables.

Another example:

Boolean Algebra	$\mathcal{P}(X)$
1	X
0	$\emptyset$
$\overline{p}$	$X - p$
$p + q$	$p \cup q$
$p.q$	$p \cap q$

Properties of a Boolean Algebra

Property 1.5.3

- For any x, there is exactly one y such that $x + y = 1$ and $xy = 0$. In other words, the complement is unique.

Properties of a Boolean Algebra

Property 1.5.3

- For any x, there is exactly one y such that $x + y = 1$ and $xy = 0$. In other words, the complement is unique.
- 1. $\overline{1} = 0$
  2. $\overline{0} = 1$
  3. $\overline{\overline{x}} = x$
  4. $x.x = x$
  5. $x + x = x$
  6. $1 + x = 1$
  7. $0.x = 0$
  8. De Morgan laws:
     - $\overline{xy} = \bar{x} + \bar{y}$
     - $\overline{x + y} = \bar{x}.\bar{y}$

Proof

1. $\overline{1} = 0$.

2. $\overline{0} = 1$.

3. $\overline{\overline{x}} = x$.

Proof

1. $\overline{1} = 0$.

   By definition of negation, $x.\overline{x} = 0$. Hence, $1.\overline{1} = 0$.
   Since 1 is neutral for the product, $\overline{1} = 0$.

2. $\overline{0} = 1$.

3. $\overline{\overline{x}} = x$.

Proof

1. $\overline{1} = 0$.

   By definition of negation, $x.\overline{x} = 0$. Hence, $1.\overline{1} = 0$.
   Since 1 is neutral for the product, $\overline{1} = 0$.

2. $\overline{0} = 1$.

   Ditto : $x + \overline{x} = 1$ hence $0 + \overline{0} = 1$.
   Since 0 is neutral, $\overline{0} = 1$.

3. $\overline{\overline{x}} = x$.

Proof

1. $\overline{1} = 0$.

   By definition of negation, $x.\overline{x} = 0$. Hence, $1.\overline{1} = 0$.
   Since 1 is neutral for the product, $\overline{1} = 0$.

2. $\overline{0} = 1$.

   Ditto : $x + \overline{x} = 1$ hence $0 + \overline{0} = 1$.
   Since 0 is neutral, $\overline{0} = 1$.

3. $\overline{\overline{x}} = x$.

   By commutativity, $\overline{x} + x = 1$ and $\overline{x}.x = 0$.
   Because the complement of $\overline{x}$ is unique, $\overline{\overline{x}} = x$.

Proof

4. Product idempotence: $x.x = x$.

5. Sum idempotence: $x + x = x$

Proof

4. Product idempotence: $x.x = x$.

$$\begin{aligned} x &= x.1 \\ &= x.(x + \overline{x}) \\ &= x.x + x.\overline{x} \\ &= x.x + 0 \\ &= x.x \end{aligned}$$

5. Sum idempotence: $x + x = x$

Proof

4. Product idempotence: $x.x = x$.

$$\begin{aligned} x &= x.1 \\ &= x.(x+\overline{x}) \\ &= x.x + x.\overline{x} \\ &= x.x + 0 \\ &= x.x \end{aligned}$$

5. Sum idempotence: $x + x = x$

Ditto, starting from $x = x + 0$.

Proof

6. 1 is an absorbing element of the sum: $1 + x = 1$.

7. 0 is an absorbing element for the product: $0.x = 0$.

Proof

6. 1 is an absorbing element of the sum: $1 + x = 1$.

We use sum idempotence.

$$\begin{aligned} 1 + x &= (x + \overline{x}) + x \\ &= x + \overline{x} \\ &= 1 \end{aligned}$$

7. 0 is an absorbing element for the product: $0.x = 0$.

Proof

6. 1 is an absorbing element of the sum: $1 + x = 1$.

We use sum idempotence.

$$\begin{aligned} 1 + x &= (x + \overline{x}) + x \\ &= x + \overline{x} \\ &= 1 \end{aligned}$$

7. 0 is an absorbing element for the product: $0.x = 0$.

Ditto from $0.x = (x.\overline{x}).x$

Proof: De Morgan Law: $\overline{xy} = \bar{x} + \bar{y}$

Proof: De Morgan Law: $\overline{xy} = \bar{x} + \bar{y}$

We first show that $xy + (\bar{x} + \bar{y}) = 1$

$$\begin{aligned} x.y + (\overline{x} + \overline{y}) &= (x + \overline{x} + \overline{y}).(y + \overline{x} + \overline{y}) \\ &= (1 + \overline{y}).(1 + \overline{x}) \\ &= 1.1 \\ &= 1 \end{aligned}$$

Proof: De Morgan Law: $\overline{xy} = \bar{x} + \bar{y}$

We first show that $xy + (\bar{x} + \bar{y}) = 1$

$$\begin{aligned} x.y + (\overline{x} + \overline{y}) &= (x + \overline{x} + \overline{y}).(y + \overline{x} + \overline{y}) \\ &= (1 + \overline{y}).(1 + \overline{x}) \\ &= 1.1 \\ &= 1 \end{aligned}$$

Similarly $x.y.(\overline{x} + \overline{y}) = 0$.

Proof: De Morgan Law: $\overline{xy} = \bar{x} + \bar{y}$

We first show that $xy + (\bar{x} + \bar{y}) = 1$

$$\begin{aligned} x.y + (\overline{x} + \overline{y}) &= (x + \overline{x} + \overline{y}).(y + \overline{x} + \overline{y}) \\ &= (1 + \overline{y}).(1 + \overline{x}) \\ &= 1.1 \\ &= 1 \end{aligned}$$

Similarly $x.y.(\overline{x} + \overline{y}) = 0$.
Since negation is unique $\overline{x} + \overline{y}$ is the negation of xy.

Proof: De Morgan Law: $\overline{xy} = \bar{x} + \bar{y}$

We first show that $xy + (\bar{x} + \bar{y}) = 1$

$$\begin{aligned} x.y + (\overline{x} + \overline{y}) &= (x + \overline{x} + \overline{y}).(y + \overline{x} + \overline{y}) \\ &= (1 + \overline{y}).(1 + \overline{x}) \\ &= 1.1 \\ &= 1 \end{aligned}$$

Similarly $x.y.(\overline{x} + \overline{y}) = 0$.
Since negation is unique $\overline{x} + \overline{y}$ is the negation of xy.

Similarly we can prove that $\overline{x + y} = \overline{x}.\overline{y}$ by switching the uses of . and $+$ in this demonstration.

Plan

Definition 1.6.1: Boolean function

A boolean function is a function whose arguments and result belong to the set $\mathbb{B} = \{0, 1\}$.

Definition 1.6.1: Boolean function

A boolean function is a function whose arguments and result belong to the set $\mathbb{B} = \{0, 1\}$.

Example 1.6.2

Which of these functions are boolean ?

- The function $f : \mathbb{B} \to \mathbb{B} : f(x) = \neg x$
- The function $f : \mathbb{N} \to \mathbb{B} : f(x) = x \bmod 2$
- The function $f : \mathbb{B} \to \mathbb{N} : f(x) = x + 1$
- The function $f : \mathbb{B} \times \mathbb{B} \to \mathbb{B} : f(x, y) = \neg(x \wedge y)$

Definition 1.6.1: Boolean function

A boolean function is a function whose arguments and result belong to the set $\mathbb{B} = \{0, 1\}$.

Example 1.6.2

Which of these functions are boolean ?

- The function $f : \mathbb{B} \to \mathbb{B} : f(x) = \neg x$

  yes

- The function $f : \mathbb{N} \to \mathbb{B} : f(x) = x \text{ mod } 2$

  no

- The function $f : \mathbb{B} \to \mathbb{N} : f(x) = x + 1$

  no

- The function $f : \mathbb{B} \times \mathbb{B} \to \mathbb{B} : f(x, y) = \neg(x \wedge y)$

  yes

Boolean functions and monomial sums

Theorem 1.6.3

Let $x^0 = \bar{x}$ and $x^1 = x$.

Let f be a boolean function with n arguments, and let:

$$A = \sum_{f(a_1,\ldots,a_n)=1} x_1^{a_1} \ldots x_n^{a_n}.$$

A is the sum of the monomials $x_1^{a_1} \ldots x_n^{a_n}$ such that $f(a_1, \ldots, a_n) = 1$.

For any assignment v such that $v(x_1) = a_1, \ldots, v(x_n) = a_n$,
we have $f(a_1, \ldots, a_n) = [A]_v$.

Example 1.6.4

The function *maj* with 3 arguments yields 1 when at least 2 of its arguments equal 1.

Define the equivalent sum of monomials (theorem 1.6.3)

Example 1.6.4

The function *maj* with 3 arguments yields 1 when at least 2 of its arguments equal 1.

Define the equivalent sum of monomials (theorem 1.6.3)

x_1	x_2	x_3	$maj(x_1, x_2, x_3)$
0	0	0	0
0	0	1	0
0	1	0	0
0	1	1	1
1	0	0	0
1	0	1	1
1	1	0	1
1	1	1	1

Example 1.6.4

The function *maj* with 3 arguments yields 1 when at least 2 of its arguments equal 1.

Define the equivalent sum of monomials (theorem 1.6.3)

x_1	x_2	x_3	$maj(x_1, x_2, x_3)$
0	0	0	0
0	0	1	0
0	1	0	0
0	1	1	1
1	0	0	0
1	0	1	1
1	1	0	1
1	1	1	1

$\overline{x_1} x_2 x_3$

Example 1.6.4

The function *maj* with 3 arguments yields 1 when at least 2 of its arguments equal 1.

Define the equivalent sum of monomials (theorem 1.6.3)

x_1	x_2	x_3	$maj(x_1, x_2, x_3)$	
0	0	0	0	
0	0	1	0	
0	1	0	0	
0	1	1	1	$\overline{x_1} x_2 x_3$
1	0	0	0	
1	0	1	1	$x_1 \overline{x_2} x_3$
1	1	0	1	$x_1 x_2 \overline{x_3}$
1	1	1	1	$x_1 x_2 x_3$

$$maj(x_1, x_2, x_3) = \overline{x_1} x_2 x_3 + x_1 \overline{x_2} x_3 + x_1 x_2 \overline{x_3} + x_1 x_2 x_3$$

Let us verify the theorem 1.6.3 on example 1.6.4

x_1	x_2	x_3	$maj(x_1, x_2, x_3)$	$\overline{x_1} x_2 x_3$	$x_1 \overline{x_2} x_3$	$x_1 x_2 \overline{x_3}$	$x_1 x_2 x_3$	$\overline{x_1} x_2 x_3 + x_1 \overline{x_2} x_3 + x_1 x_2 \overline{x_3} + x_1 x_2 x_3$
0	0	0	0	0	0	0	0	0
0	0	1	0	0	0	0	0	0
0	1	0	0	0	0	0	0	0
0	1	1	1	1	0	0	0	1
1	0	0	0	0	0	0	0	0
1	0	1	1	0	1	0	0	1
1	1	0	1	0	0	1	0	1
1	1	1	1	0	0	0	1	1

$$maj(x_1, x_2, x_3) = \overline{x_1} x_2 x_3 + x_1 \overline{x_2} x_3 + x_1 x_2 \overline{x_3} + x_1 x_2 x_3$$

Proof of Theorem 1.6.3

Let v be any assignment.
Note that for all variable x, $v(x^a) = 1$ if and only if $v(x) = a$.

Proof of Theorem 1.6.3

Let v be any assignment.
Note that for all variable x, $v(x^a) = 1$ if and only if $v(x) = a$.
Thus:

$$[x_1^{a_1} \dots x_n^{a_n}]_v = 1 \quad \text{if and only if} \quad v(x_1) = a_1, \dots, v(x_n) = a_n. \tag{1}$$

Proof of Theorem 1.6.3

Let v be any assignment.
Note that for all variable x, $v(x^a) = 1$ if and only if $v(x) = a$.
Thus:

$$[x_1^{a_1} \ldots x_n^{a_n}]_v = 1 \quad \text{if and only if} \quad v(x_1) = a_1, \ldots, v(x_n) = a_n. \qquad (1)$$

Let v be an assignment such that $v(x_1) = a_1, \ldots v(x_n) = a_n$.
Consider the following two cases:

Proof of Theorem 1.6.3

Let v be any assignment.
Note that for all variable x, $v(x^a) = 1$ if and only if $v(x) = a$.
Thus:

$$[x_1^{a_1} \dots x_n^{a_n}]_v = 1 \quad \text{if and only if} \quad v(x_1) = a_1, \dots, v(x_n) = a_n. \tag{1}$$

Let v be an assignment such that $v(x_1) = a_1, \dots v(x_n) = a_n$.
Consider the following two cases:

1. $f(a_1, \dots, a_n) = 1$:
2. $f(a_1, \dots, a_n) = 0$:

Proof of Theorem 1.6.3

Let v be any assignment.
Note that for all variable x, $v(x^a) = 1$ if and only if $v(x) = a$.
Thus:

$$[x_1^{a_1} \dots x_n^{a_n}]_v = 1 \quad \text{if and only if} \quad v(x_1) = a_1, \dots, v(x_n) = a_n. \tag{1}$$

Let v be an assignment such that $v(x_1) = a_1, \dots v(x_n) = a_n$.
Consider the following two cases:

1. $f(a_1, \dots, a_n) = 1$: According to (1), we have $[x_1^{a_1} \dots x_n^{a_n}]_v = 1$.
   According to the definition of A, this monomial is the element of the sum A, so $[A]_v = 1$.
2. $f(a_1, \dots, a_n) = 0$:

Proof of Theorem 1.6.3

Let v be any assignment.
Note that for all variable x, $v(x^a) = 1$ if and only if $v(x) = a$.
Thus:

$$[x_1^{a_1} \dots x_n^{a_n}]_v = 1 \quad \text{if and only if} \quad v(x_1) = a_1, \dots, v(x_n) = a_n. \tag{1}$$

Let v be an assignment such that $v(x_1) = a_1, \dots v(x_n) = a_n$.
Consider the following two cases:

1. $f(a_1, \dots, a_n) = 1$: According to (1), we have $[x_1^{a_1} \dots x_n^{a_n}]_v = 1$.
   According to the definition of A, this monomial is the element of the sum A, so $[A]_v = 1$.
2. $f(a_1, \dots, a_n) = 0$: By definition of A, any monomial $x_1^{b_1} \dots x_n^{b_n}$ in A is such that $a_i \neq b_i$ for at least one subscript i.
   Consequently $v(x_i) \neq b_i$, so according to (1), $[x_1^{b_1} \dots, x_n^{b_n}]_v = 0$.

   Since this is true for every monomial in A, we conclude that $[A]_v = 0$.

Boolean functions and product of clauses

Theorem 1.6.5

Let f a boolean function with n arguments, and:

$$A = \prod_{f(a_1,\dots,a_n)=0} x_1^{\overline{a_1}} + \dots + x_n^{\overline{a_n}}.$$

A is the product of the clauses $x_1^{\overline{a_1}} + \dots + x_n^{\overline{a_n}}$ such that $f(a_1, \dots, a_n) = 0$.

For any assignment v such that $v(x_1) = a_1, \dots, v(x_n) = a_n$,
we have $f(a_1, \dots, a_n) = [A]_v$.

Proof of theorem 1.6.5

Similar proof:

- For every variable x, $v(x^a) = 0$ if and only if $v(x) \neq a$.
- From this remark, we deduce the following property:

$$[x_1^{\overline{a_1}} + \dots x_n^{\overline{a_n}}]_v = 0 \quad \Leftrightarrow \quad v(x_1) \neq \overline{a_1}, \dots v(x_n) \neq \overline{a_n} \qquad (2)$$
$$\Leftrightarrow \quad v(x_1) = a_1, \dots v(x_n) = a_n. \qquad (3)$$

- From the above properties, we deduce as before that $f(x_1, \dots x_n) = A$.

Example 1.6.6

The function *maj* of 3 arguments yields 1 if at least 2 of its arguments equal 1.

Define the equivalent product of clauses (theorem 1.6.5)

Example 1.6.6

The function *maj* of 3 arguments yields 1 if at least 2 of its arguments equal 1.

Define the equivalent product of clauses (theorem 1.6.5)

x_1	x_2	x_3	$maj(x_1, x_2, x_3)$
0	0	0	0
0	0	1	0
0	1	0	0
0	1	1	1
1	0	0	0
1	0	1	1
1	1	0	1
1	1	1	1

Example 1.6.6

The function *maj* of 3 arguments yields 1 if at least 2 of its arguments equal 1.

Define the equivalent product of clauses (theorem 1.6.5)

x_1	x_2	x_3	$maj(x_1, x_2, x_3)$
0	0	0	0
0	0	1	0
0	1	0	0
0	1	1	1
1	0	0	0
1	0	1	1
1	1	0	1
1	1	1	1

$x_1 + x_2 + x_3$

Example 1.6.6

The function *maj* of 3 arguments yields 1 if at least 2 of its arguments equal 1.

Define the equivalent product of clauses (theorem 1.6.5)

x_1	x_2	x_3	$maj(x_1, x_2, x_3)$
0	0	0	0
0	0	1	0
0	1	0	0
0	1	1	1
1	0	0	0
1	0	1	1
1	1	0	1
1	1	1	1

$x_1 + x_2 + x_3$

$x_1 + x_2 + \overline{x_3}$

$x_1 + \overline{x_2} + x_3$

$\overline{x_1} + x_2 + x_3$

$$maj(x_1, x_2, x_3) = (x_1 + x_2 + x_3)(x_1 + x_2 + \overline{x_3})(x_1 + \overline{x_2} + x_3)(\overline{x_1} + x_2 + x_3)$$

Let us verify theorem 1.6.5 on the example 1.6.6

x_1	x_2	x_3	$maj(x_1, x_2, x_3)$	$x_1 + x_2 + x_3$	$x_1 + x_2 + \overline{x_3}$	$x_1 + \overline{x_2} + x_3$	$\overline{x_1} + x_2 + x_3$	$(x_1 + x_2 + x_3)$ $(x_1 + x_2 + \overline{x_3})$ $(x_1 + \overline{x_2} + x_3)$ $(\overline{x_1} + x_2 + x_3)$
0	0	0	0	0	1	1	1	0
0	0	1	0	1	0	1	1	0
0	1	0	0	1	1	0	1	0
0	1	1	1	1	1	1	1	1
1	0	0	0	1	1	1	0	0
1	0	1	1	1	1	1	1	1
1	1	0	1	1	1	1	1	1
1	1	1	1	1	1	1	1	1

$$maj(x_1, x_2, x_3) = (x_1 + x_2 + x_3)(x_1 + x_2 + \overline{x_3})(x_1 + \overline{x_2} + x_3)(\overline{x_1} + x_2 + x_3)$$

Plan

BDDC (*Binary Decision Diagram based Calculator*)

BDDC is a tool for manipulating propositional formulae developed by Pascal Raymond and available at the following address:

`http://www-verimag.imag.fr/~raymond/home/tools/bddc/`

Plan of the Semester

- Propositional logic *
- Propositional resolution
- Natural propositional deduction

MIDTERM EXAM

- First order logic
- Basis for the automatic proof (“first order resolution”)
- First order natural deduction

EXAM

Plan

Deduction methods

- Is a formula valid?
- Is a reasoning correct?

Two methods:

Deduction methods

- Is a formula valid?
- Is a reasoning correct?

Two methods:

The truth tables and transformations

Deduction methods

- Is a formula valid?
- Is a reasoning correct?

Two methods:

The truth tables and transformations

Problem

If the number of variables increases, these methods are very long

Example

By a truth table, to verify
$a \Rightarrow b, b \Rightarrow c, c \Rightarrow d, d \Rightarrow e, e \Rightarrow f, f \Rightarrow g, g \Rightarrow h, h \Rightarrow i, i \Rightarrow j \models a \Rightarrow j$
we must test $2^{10} = 1024$ lines.

Example

By a truth table, to verify
$a \Rightarrow b, b \Rightarrow c, c \Rightarrow d, d \Rightarrow e, e \Rightarrow f, f \Rightarrow g, g \Rightarrow h, h \Rightarrow i, i \Rightarrow j \models a \Rightarrow j$
we must test $2^{10} = 1024$ lines.

Or, by deduction, this is a correct reasoning:

Example

By a truth table, to verify
$a \Rightarrow b, b \Rightarrow c, c \Rightarrow d, d \Rightarrow e, e \Rightarrow f, f \Rightarrow g, g \Rightarrow h, h \Rightarrow i, i \Rightarrow j \models a \Rightarrow j$
we must test $2^{10} = 1024$ lines.

Or, by deduction, this is a correct reasoning:

1. By transitivity of the implication, $a \Rightarrow j \models a \Rightarrow j$.
2. By definition, the formula $a \Rightarrow j$ is a consequence of its own.

Today

Today

- Formalisation of a deductive system (with 1 rule)

Today

- Formalisation of a deductive system (with 1 rule)
- How to prove a formula by resolution

Today

- Formalisation of a deductive system (with 1 rule)
- How to prove a formula by resolution
- Some properties of resolution

David Hilbert (1862-1943)

- Founder of the **formalism** school : mathematics can and should be formalized to be studied.
- Hilbert's program (1920):
  "*Wir müssen wissen. Wir werden wissen.*"
  as an answer to "*Ignoramus et ignorabimus*"
  - choose a finite set of axioms to express all of maths
  - prove it is consistent
  - design an algorithm that decides whether a proposition can be proved (*Entscheidungsproblem*)

- *Hilbert-style* deductive systems: axioms such as $\vdash p \Rightarrow (q \Rightarrow p)$
  and a few deduction rules such as $\dfrac{\vdash p \Rightarrow q \qquad \vdash p}{\vdash q}$
- proofs are thorough but hard to read and to check

Intuition

Formulas are put into CNF (conjunction of clauses), and then we use:

$$a + \overline{b},\ b + c \models a + c$$

Plan

Definitions

Definition 2.1.1

A clause is identified to the **set** of its literals, so we may say that:

Definitions

Definition 2.1.1

A clause is identified to the **set** of its literals, so we may say that:

- A literal is a member of a clause.
- A clause A is included in a clause B (or is a sub-clause of B).
- Two clauses are equal if they have the same set of literals.

Example 2.1.2

- The clauses $p+\overline{q}$, $\overline{q}+p$, and $p+\overline{q}+p$ are equal

Example 2.1.2

- The clauses $p + \overline{q}$, $\overline{q} + p$, and $p + \overline{q} + p$ are equal
- $p \in \overline{q} + p + r + p$
- $p + \overline{q} \subseteq \overline{q} + p + r + p$

Example 2.1.2

- The clauses $p+\overline{q}$, $\overline{q}+p$, and $p+\overline{q}+p$ are equal
- $p \in \overline{q}+p+r+p$
- $p+\overline{q} \subseteq \overline{q}+p+r+p$
- $\overline{q}+p+r+p - p = \overline{q}+r$
- $p+p+p - p = \perp$

Example 2.1.2

- The clauses $p+\overline{q}$, $\overline{q}+p$, and $p+\overline{q}+p$ are equal
- $p \in \overline{q}+p+r+p$
- $p+\overline{q} \subseteq \overline{q}+p+r+p$
- $\overline{q}+p+r+p - p = \overline{q}+r$
- $p+p+p - p = \bot$
- Adding the literal r to the clause p yields the clause $p+r$
- Adding the literal p to the clause $\bot$ yields the clause p

Notation

$s(A)$ the set of literals of the clause A.
By convention $\perp$ is the empty clause and $s(\perp) = \emptyset$.

Example 2.1.3

$s(\overline{q} + p + r + p + \overline{p}) =$

Notation

$s(A)$ the set of literals of the clause A.
By convention $\perp$ is the empty clause and $s(\perp) = \emptyset$.

Example 2.1.3

$s(\overline{q} + p + r + p + \overline{p}) =$

$\{\overline{q}, p, r, \overline{p}\}$

Complementary literal

Definition 2.1.4

We note L^c the complementary literal of a literal L :

If L is a variable, L^c is the negation of L.

If L is the negation of a variable, L^c is obtained by removing the negation of L.

Example 2.1.5

$x^c = \overline{x}$ and $\overline{x}^c = x$.

Resolvent

Definition 2.1.6

Let A and B be two clauses.

The clause C is a resolvent of A and B iff there exists a literal L such that

$$L \in A, \qquad L^c \in B, \qquad C = (A - \{L\}) \cup (B - \{L^c\})$$

Resolvent

Definition 2.1.6

Let A and B be two clauses.

The clause C is a resolvent of A and B iff there exists a literal L such that

$$L \in A, \qquad L^c \in B, \qquad C = (A - \{L\}) \cup (B - \{L^c\})$$

"C is a resolvent of A and B" is represented by:

$$\frac{A \qquad B}{C}$$

Resolvent

Definition 2.1.6

Let A and B be two clauses.

The clause C is a resolvent of A and B iff there exists a literal L such that

$$L \in A, \qquad L^c \in B, \qquad C = (A - \{L\}) \cup (B - \{L^c\})$$

"C is a resolvent of A and B" is represented by:

$$\frac{A \qquad B}{C}$$

C is generated by A and B
A and B are the parents of clause C.

Examples with resolution

Example 2.1.7

Give the resolvents of:

- $p + q + r$ and $p + \overline{q} + r$
- $p + \overline{q}$ and $\overline{p} + q + r$
- p and $\overline{p}$

Examples with resolution

Example 2.1.7

Give the resolvents of:

- $p+q+r$ and $p+\overline{q}+r$

$$\frac{p+q+r \qquad p+\overline{q}+r}{p+r}$$

- $p+\overline{q}$ and $\overline{p}+q+r$

- p and $\overline{p}$

Examples with resolution

Example 2.1.7

Give the resolvents of:

- $p+q+r$ and $p+\overline{q}+r$

$$\frac{p+q+r \qquad p+\overline{q}+r}{p+r}$$

- $p+\overline{q}$ and $\overline{p}+q+r$

$$\frac{p+\overline{q} \qquad \overline{p}+q+r}{\overline{p}+p+r} \qquad \frac{p+\overline{q} \qquad \overline{p}+q+r}{\overline{q}+q+r}$$

- p and $\overline{p}$

Examples with resolution

Example 2.1.7

Give the resolvents of:

- $p+q+r$ and $p+\overline{q}+r$

$$\frac{p+q+r \qquad p+\overline{q}+r}{p+r}$$

- $p+\overline{q}$ and $\overline{p}+q+r$

$$\frac{p+\overline{q} \qquad \overline{p}+q+r}{\overline{p}+p+r} \qquad \frac{p+\overline{q} \qquad \overline{p}+q+r}{\overline{q}+q+r}$$

- p and $\overline{p}$

$$\frac{p \qquad \overline{p}}{\perp}$$

Property

Property 2.1.8

If one of the parents of a resolvent is valid, the resolvent is valid or contains the other parent.

Proof.

See exercise 39. □

Property

Property 2.1.8

If one of the parents of a resolvent is valid, the resolvent is valid or contains the other parent.

Proof.

See exercise 39. □

Example

$$\frac{p+\bar{p}+q \qquad \bar{q}+r}{p+\bar{p}+r} \qquad\qquad \frac{p+\bar{p}+q \qquad \bar{p}+r}{\bar{p}+q+r}$$

Definition of a proof

Definition 2.1.11

Let Γ be a set of clauses and C a clause.

A proof of C starting from Γ is a list of clauses:

- where every clause of the proof is a member of Γ

Definition of a proof

Definition 2.1.11

Let Γ be a set of clauses and C a clause.

A proof of C starting from Γ is a list of clauses:

- where every clause of the proof is a member of Γ
- or is a resolvent of two clauses already obtained

Definition of a proof

Definition 2.1.11

Let Γ be a set of clauses and C a clause.

A proof of C starting from Γ is a list of clauses:

- where every clause of the proof is a member of Γ
- or is a resolvent of two clauses already obtained
- ending with C.

Definition of a proof

Definition 2.1.11

Let Γ be a set of clauses and C a clause.

A proof of C starting from Γ is a list of clauses:

- where every clause of the proof is a member of Γ
- or is a resolvent of two clauses already obtained
- ending with C.

The clause C is deduced from Γ (Γ yields C, or Γ proves C), denoted $\Gamma \vdash C$, if there is a proof of C starting from Γ.

The size of a proof is the number of lines in it.

Example

Example 2.1.12

Let Γ be the set of clauses $\overline{p}+q$, $p+\overline{q}$, $\overline{p}+\overline{q}$, $p+q$.

We show that $\Gamma \vdash \bot$:

Example

Example 2.1.12

Let Γ be the set of clauses $\overline{p}+q$, $p+\overline{q}$, $\overline{p}+\overline{q}$, $p+q$.

We show that $\Gamma \vdash \bot$:

1	$p+q$	Hypothesis

Example

Example 2.1.12

Let Γ be the set of clauses $\overline{p}+q$, $p+\overline{q}$, $\overline{p}+\overline{q}$, $p+q$.

We show that $\Gamma \vdash \perp$:

1	$p+q$	Hypothesis
2	$p+\overline{q}$	Hypothesis

Example

Example 2.1.12

Let Γ be the set of clauses $\overline{p}+q$, $p+\overline{q}$, $\overline{p}+\overline{q}$, $p+q$.

We show that $\Gamma \vdash \bot$:

1	$p+q$	Hypothesis
2	$p+\overline{q}$	Hypothesis
3	p	Resolvent of 1, 2

Example

Example 2.1.12

Let Γ be the set of clauses $\overline{p}+q$, $p+\overline{q}$, $\overline{p}+\overline{q}$, $p+q$.

We show that $\Gamma \vdash \perp$:

1	$p+q$	Hypothesis
2	$p+\overline{q}$	Hypothesis
3	p	Resolvent of 1, 2
4	$\overline{p}+q$	Hypothesis

Example

Example 2.1.12

Let Γ be the set of clauses $\overline{p}+q$, $p+\overline{q}$, $\overline{p}+\overline{q}$, $p+q$.

We show that $\Gamma \vdash \bot$:

1	$p+q$	Hypothesis
2	$p+\overline{q}$	Hypothesis
3	p	Resolvent of 1, 2
4	$\overline{p}+q$	Hypothesis
5	q	Resolvent of 3, 4

Example

Example 2.1.12

Let Γ be the set of clauses $\overline{p}+q$, $p+\overline{q}$, $\overline{p}+\overline{q}$, $p+q$.

We show that $\Gamma \vdash \perp$:

1	$p+q$	Hypothesis
2	$p+\overline{q}$	Hypothesis
3	p	Resolvent of 1, 2
4	$\overline{p}+q$	Hypothesis
5	q	Resolvent of 3, 4
6	$\overline{p}+\overline{q}$	Hypothesis

Example

Example 2.1.12

Let Γ be the set of clauses $\overline{p}+q$, $p+\overline{q}$, $\overline{p}+\overline{q}$, $p+q$.

We show that $\Gamma \vdash \bot$:

1	$p+q$	Hypothesis
2	$p+\overline{q}$	Hypothesis
3	p	Resolvent of 1, 2
4	$\overline{p}+q$	Hypothesis
5	q	Resolvent of 3, 4
6	$\overline{p}+\overline{q}$	Hypothesis
7	$\overline{p}$	Resolvent of 5, 6

Example

Example 2.1.12

Let Γ be the set of clauses $\overline{p}+q$, $p+\overline{q}$, $\overline{p}+\overline{q}$, $p+q$.
We show that $\Gamma \vdash \bot$:

1	$p+q$	Hypothesis
2	$p+\overline{q}$	Hypothesis
3	p	Resolvent of 1, 2
4	$\overline{p}+q$	Hypothesis
5	q	Resolvent of 3, 4
6	$\overline{p}+\overline{q}$	Hypothesis
7	$\overline{p}$	Resolvent of 5, 6
8	$\bot$	Resolvent of 3, 7

Proof tree

Example 2.1.12

Let Γ be the set of clauses $\overline{p}+q$, $p+\overline{q}$, $\overline{p}+\overline{q}$, $p+q$.

We show that $\Gamma \vdash \bot$:

$$\dfrac{\dfrac{\dfrac{\dfrac{p+q \quad p+\overline{q}}{p} \quad \overline{p}+q}{q} \quad \overline{p}+\overline{q}}{\overline{p}} \quad \dfrac{p+q \quad p+\overline{q}}{p}}{\bot}$$

Proof tree

Example 2.1.12

Let Γ be the set of clauses $\overline{p}+q$, $p+\overline{q}$, $\overline{p}+\overline{q}$, $p+q$.

We show that $\Gamma \vdash \bot$:

$$\dfrac{\dfrac{\dfrac{\dfrac{p+q \qquad p+\overline{q}}{p} \qquad \overline{p}+q}{q} \qquad \overline{p}+\overline{q}}{\overline{p}} \qquad \dfrac{p+q \qquad p+\overline{q}}{p}}{\bot}$$

Monotony and Composition

Property 2.1.14

1. Monotony: If $\Gamma \vdash A$ and if $\Gamma \subseteq \Delta$ then $\Delta \vdash A$
2. Composition: If $\Gamma \vdash A$ and $\Gamma \vdash B$ and if C is a resolvent of A and B then $\Gamma \vdash C$.

Proof.

Exercise 38 □

Plan

Today

- **Important equivalences** correspond to computation rules in a Boolean algebra
- Any boolean function can be represented by a (normal) formula

- A deductive system is given by a set of **formal rules**
- A proof is a sequence of applications of these rules starting from **hypotheses**.

Next course

- Correctness and Completeness of the system
- Comprehensive strategy
- Davis-Putnam

Homework

Hypotheses:

- (H1): If Peter is old, then John is not the son of Peter
- (H2): If Peter is not old, then John is the son of Peter
- (H3): If John is Peter's son then Mary is the sister of John

Conclusion (C): Either Mary is the sister of John or Peter is old.

Transform into clauses the premises and the negation of the conclusion.

What can you (or should you) **prove** using resolution ?