Equivalent replacement

Lemma Let I be an interpretation and $I \models F_1 \leftrightarrow F_2$. Then $I \models G[F_1] \leftrightarrow G[F_2]$.

Theorem (Equivalent Replacement) Let $F_1 \equiv F_2$. Then Then $G[F_1] \equiv G[F_2]$.

Monotonic replacement

Monotonic Replacement Lemma. Let $I \models F_1 \rightarrow F_2$. If $pol(G, \pi) = 1$, then $I \models G[F_1]_\pi \rightarrow G[F_2]_\pi$. Likewise, if $pol(G, \pi) = -1$, then $I \models G[F_2]_\pi \rightarrow G[F_1]_\pi$.

Monotonic Replacement Theorem. Let $F_1 \rightarrow F_2$ be valid. If $pol(G, \pi) = 1$, then $G[F_1]_\pi \rightarrow G[F_2]_\pi$ is valid too. Likewise, if $pol(G, \pi) = -1$, then $G[F_2]_\pi \rightarrow G[F_1]_\pi$ is valid too.

Substitutions for propositional formulas

Substitution: $(F)_p^G$

Example: $$((p \vee s) \wedge (q \rightarrow p))_p^{(l \wedge s)} =$$
$$(((l \wedge s) \vee s) \wedge (q \rightarrow (l \wedge s)))$$

Properties: If we apply any substitution to a valid formula then we also obtain a valid formula.

Substitution for quantified formulas

Some problems...

Consider $\exists q(\neg p \leftrightarrow q)$.

We cannot simply replace variables by formulas any more:

$\exists(r \rightarrow r)(\neg p \leftrightarrow r \rightarrow r)$???

Free variables are parameters.

We substitute only parameters.

But a variable can have both free and bound occurrences in a formula.

$(\forall p p \rightarrow q) \wedge (q \vee (q \rightarrow p))$

Renaming bound variables

Notation: $\exists\!\!\!\forall$: any of $\forall$, $\exists$.

$\wedge\!\!\!\vee$: any of $\wedge$, $\vee$.

Renaming bound variables in F:

Let $F[\,\exists\!\!\!\forall p G\,]$ and q be a variable not occurring in F then we replace all free occurrences of p in G by q obtaining G', and the result of renaming is $F[\,\exists\!\!\!\forall q G'\,]$.

Lemma. $F[\,\exists\!\!\!\forall p G\,] \equiv F[\,\exists\!\!\!\forall q G'\,]$.

Example:

$\exists q(\forall p((p \rightarrow q) \wedge p)) \vee p$

Then we can rename p by r.

$\exists q(\forall r((r \rightarrow q) \wedge r)) \vee p$

Rectified formulas

Rectified formula F:

- no variable appears both free and bound in F;
- for every variable p, the formula F contains at most one occurrence of quantifiers $\exists\forall p$.

Any formula can be transformed into a rectified formula by renaming bound variables.

Now we can use usual notation $(F)_p^G$ assuming that p occurs only free.

Rectification: Example

$$p \longrightarrow \exists p(p \wedge \forall p(p \vee r \longrightarrow \neg p)) \Rightarrow$$

$$p \longrightarrow \exists p_1(p_1 \wedge \forall p(p \vee r \longrightarrow \neg p)) \Rightarrow$$

$$p \longrightarrow \exists p_1(p_1 \wedge \forall p_2(p_2 \vee r \longrightarrow \neg p_2))$$

Another problem

$\exists q(\neg p \leftrightarrow q)$: there exists a truth value equivalent to $\neg p$.

Replace p by q.

$\exists q(\neg q \leftrightarrow q)$: there exists a truth value equivalent to its own negation.

Another restriction

Let we want to substitute $(F)_p^G$.

Then we require: no free variable in G become bound in $(F)_p^G$.

In previous example:

$\exists q(\neg p \leftrightarrow q)$

Substitute p by q. ($\exists q(\neg q \leftrightarrow q)$ does not satisfy above)

Uniform solution – renaming of bound variables

$\exists q(\neg p \leftrightarrow q) \equiv \exists r(\neg p \leftrightarrow r)$

Now we can substitute p by q: $\exists r(\neg q \leftrightarrow r)$

From now on we always assume that:

(1) formulas are rectified.

(2) all substitutions satisfy the requirement above

Prenex form

- ▷ Quantifier-free formula: no quantifiers (that is, propositional).
- ▷ Prenex formula has the form $\exists\!\!\!/\forall_1 p_1 \ldots \exists\!\!\!/\forall_n p_n G$, where G is quantifier-free.
- ▷ Outermost prefix of $\exists\!\!\!/\forall_1 p_1 \ldots \exists\!\!\!/\forall_n p_n G$: the longest subsequence $\exists\!\!\!/\forall_1 p_1 \ldots \exists\!\!\!/\forall_k p_k$ of $\exists\!\!\!/\forall_1 p_1 \ldots \exists\!\!\!/\forall_n p_n$ such that $\exists\!\!\!/\forall_1 = \ldots = \exists\!\!\!/\forall_k$.
- ▷ A formula F is a prenex form of a formula G if F is prenex and $F \equiv G$.

Prenexing rules

Prenexing rules:

$$\exists\!\!\!\forall p F_1 \wedge\!\!\!\!\vee \ldots \wedge\!\!\!\!\vee F_n \;\Rightarrow\; \exists\!\!\!\forall p (F_1 \wedge\!\!\!\!\vee \ldots \wedge\!\!\!\!\vee F_n)$$

$$\forall p F_1 \rightarrow F_2 \;\Rightarrow\; \exists p (F_1 \rightarrow F_2) \quad \exists p F_1 \rightarrow F_2 \;\Rightarrow\; \forall p (F_1 \rightarrow F_2)$$

$$F_1 \rightarrow \forall p F_2 \;\Rightarrow\; \forall p (F_1 \rightarrow F_2) \quad F_1 \rightarrow \exists p F_2 \;\Rightarrow\; \exists p (F_1 \rightarrow F_2)$$

$$\neg \forall p F \;\Rightarrow\; \exists p \neg F \qquad\qquad \neg \exists p F \;\Rightarrow\; \forall p \neg F$$

Prenexing. Example I

$$\exists q(q \rightarrow p) \rightarrow \neg\forall r(r \rightarrow p) \vee p \Rightarrow$$

$$\forall q((q \rightarrow p) \rightarrow \neg\forall r(r \rightarrow p) \vee p) \Rightarrow$$

$$\forall q((q \rightarrow p) \rightarrow \exists r\neg(r \rightarrow p) \vee p) \Rightarrow$$

$$\forall q((q \rightarrow p) \rightarrow \exists r(\neg(r \rightarrow p) \vee p)) \Rightarrow$$

$$\forall q\exists r((q \rightarrow p) \rightarrow \neg(r \rightarrow p) \vee p).$$

Prenexing. Example II

$$\exists q(q \rightarrow p) \rightarrow \neg\forall r(r \rightarrow p) \vee p \Rightarrow$$

$$\exists q(q \rightarrow p) \rightarrow \exists r\neg(r \rightarrow p) \vee p \Rightarrow$$

$$\exists q(q \rightarrow p) \rightarrow \exists r(\neg(r \rightarrow p) \vee p) \Rightarrow$$

$$\exists r(\exists q(q \rightarrow p) \rightarrow \neg(r \rightarrow p) \vee p) \Rightarrow$$

$$\exists r\forall q((q \rightarrow p) \rightarrow \neg(r \rightarrow p) \vee p).$$

What's next

Algorithms for satisfiability, validity of QBF:

- ▷ Splitting
- ▷ DLL

Reminder:

(i) $F(p_1, \ldots, p_n)$ is satisfiable iff $\exists p_1 \ldots \exists p_n F(p_1, \ldots, p_n)$ is true

(ii) $F(p_1, \ldots, p_n)$ is valid iff $\forall p_1 \ldots \forall p_n F(p_1, \ldots, p_n)$ is true

Algorithms will check truth/falsity of closed formulas.

Splitting: Foundations

Lemma

(i) A closed formula $\forall p F$ is

true if and only if the formulas $F_p^{\perp}$ and $F_p^{\top}$ are true.

(ii) A closed formula $\exists p F$ is

true if and only if at least one of the formulas $F_p^{\perp}$ or $F_p^{\top}$ is true.

Splitting

Simplification rules for $\top$:

$$\neg\top \;\Rightarrow\; \bot$$

$$\top \wedge F_1 \wedge \ldots \wedge F_n \;\Rightarrow\; F_1 \wedge \ldots \wedge F_n$$

$$\top \vee F_1 \vee \ldots \vee F_n \;\Rightarrow\; \top$$

$$F \rightarrow \top \;\Rightarrow\; \top \qquad \top \rightarrow F \;\Rightarrow\; F$$

$$F \leftrightarrow \top \;\Rightarrow\; F \qquad \top \leftrightarrow F \;\Rightarrow\; F$$

$$\forall p \top \;\Rightarrow\; \top$$

$$\exists p \top \;\Rightarrow\; \top$$

Simplification rules for $\bot$:

$$\neg\bot \;\Rightarrow\; \top$$

$$\bot \wedge F_1 \wedge \ldots \wedge F_n \;\Rightarrow\; \bot$$

$$\bot \vee F_1 \vee \ldots \vee F_n \;\Rightarrow\; F_1 \vee \ldots \vee F_n$$

$$F \rightarrow \bot \;\Rightarrow\; \neg F \qquad \bot \rightarrow F \;\Rightarrow\; \top$$

$$F \leftrightarrow \bot \;\Rightarrow\; \neg F \qquad \bot \leftrightarrow F \;\Rightarrow\; \neg F$$

$$\forall p \bot \;\Rightarrow\; \bot$$

$$\exists p \bot \;\Rightarrow\; \bot$$

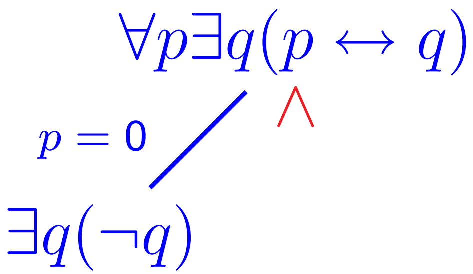
Splitting algorithm

procedure $splitting(F)$
input: closed rectified prenex formula F
output: 0 or 1
parameters: function $select\_signed\_atom$
begin
  F := $simplify(F)$
  if $F = \bot$ **then** **return** 0
  if $F = \top$ **then** **return** 1
  Let F have the form $\exists\forall p_1 \ldots \exists\forall p_k F_1$
  (p, b) := $select\_signed\_atom(F)$
  Let F' be obtained from F by deleting $\exists\forall p$ from its outermost prefix
  if $b = 0$ **then** (G_1, G_2) := $(\bot, \top)$
            else (G_1, G_2) := $(\top, \bot)$
  case $(splitting((F')_p^{G_1}), \exists\forall)$ **of**
    $(0, \forall) \Rightarrow$ **return** 0
    $(0, \exists) \Rightarrow$ **return** $splitting((F')_p^{G_2})$
    $(1, \forall) \Rightarrow$ **return** $splitting((F')_p^{G_2})$
    $(1, \exists) \Rightarrow$ **return** 1
end

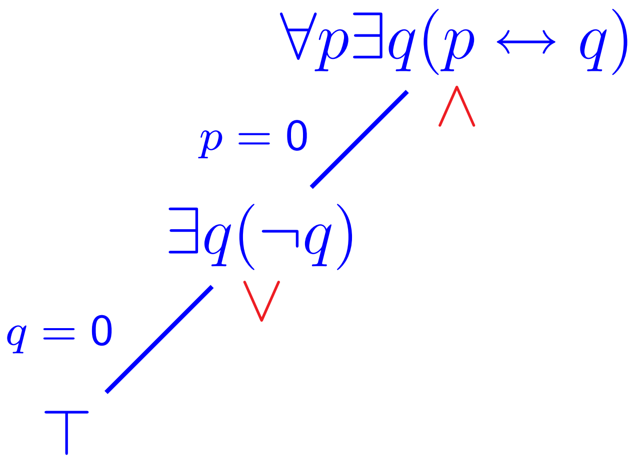
Splitting example

$$\forall p \exists q (p \leftrightarrow q)$$

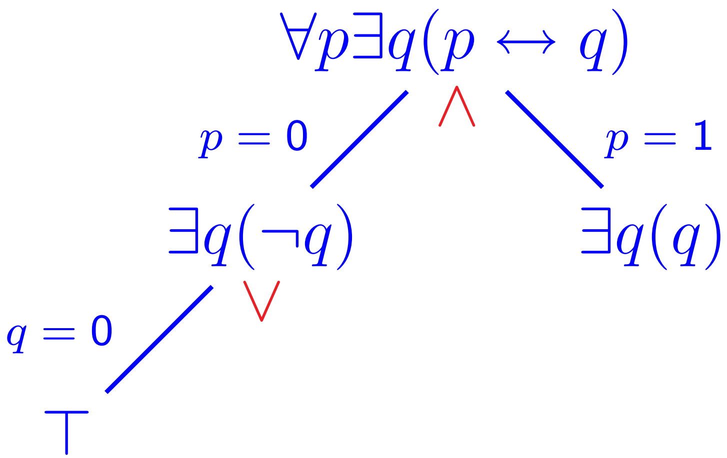
Splitting example



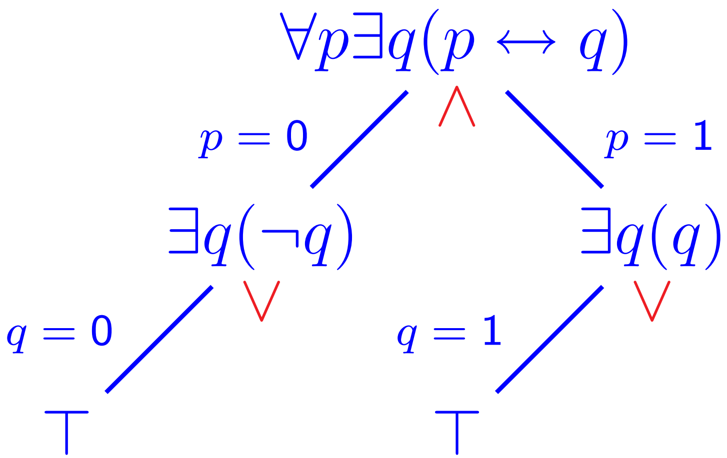
Splitting example



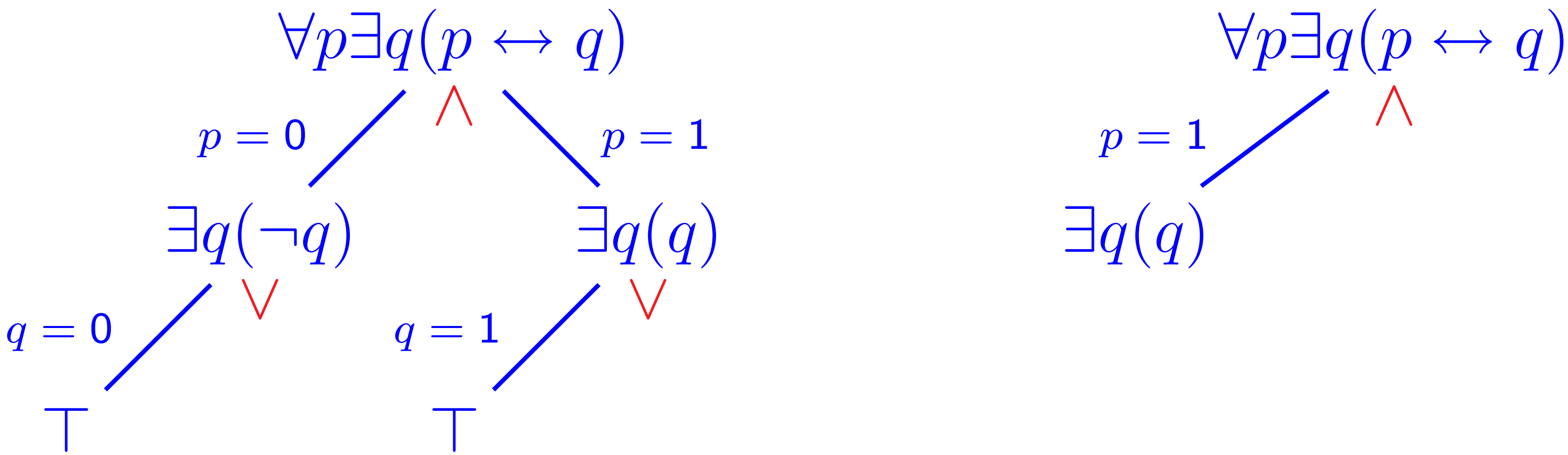
Splitting example



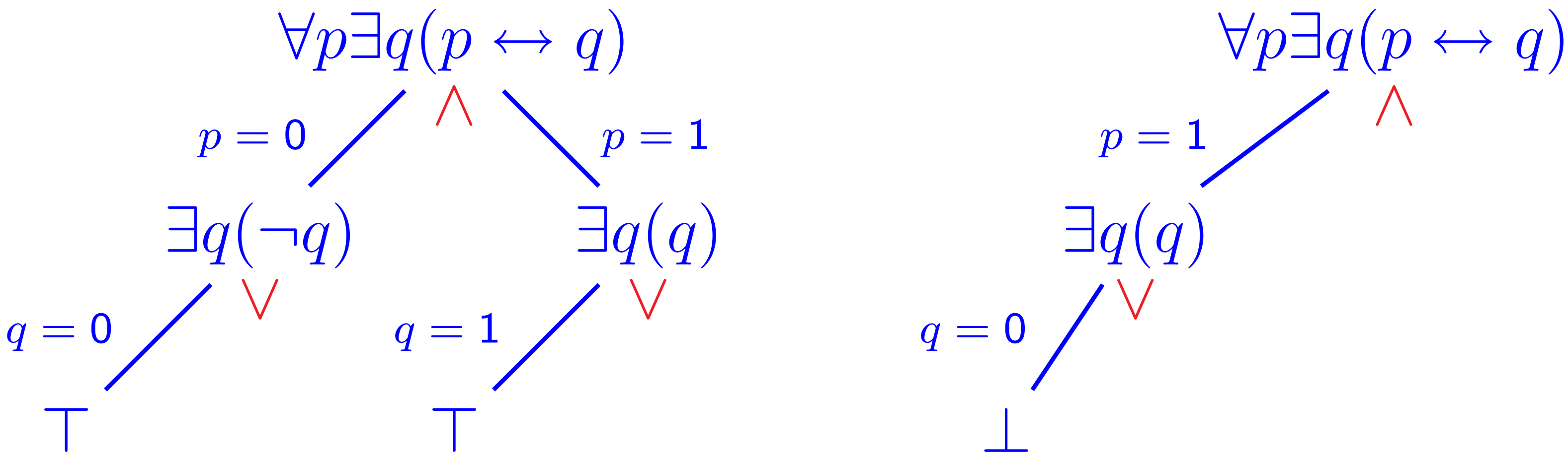
Splitting example



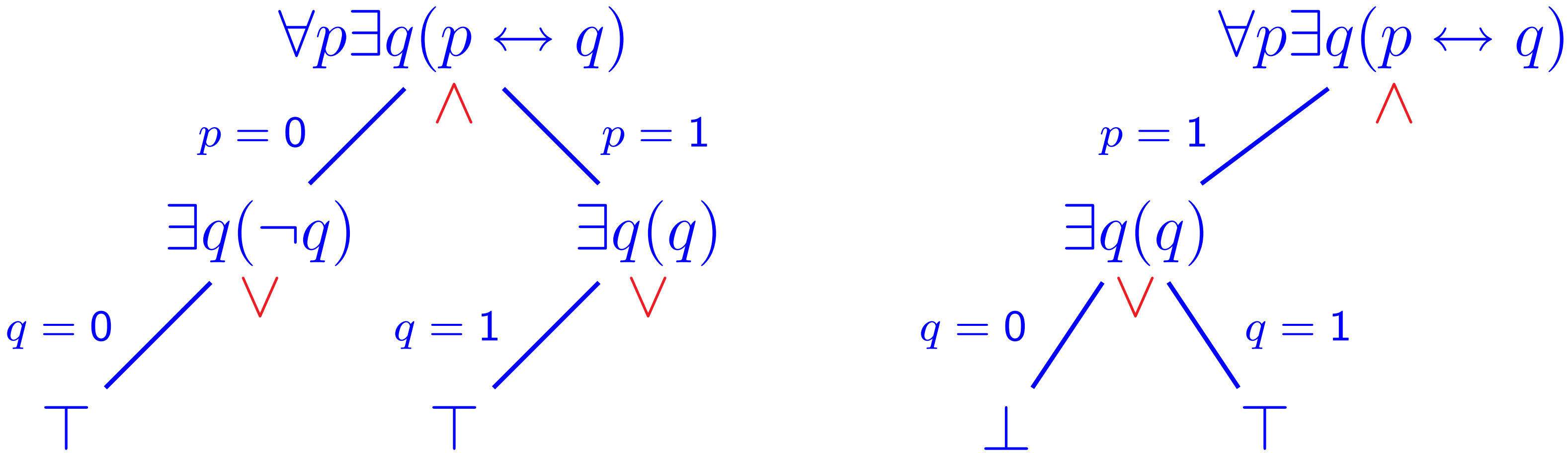
Splitting example



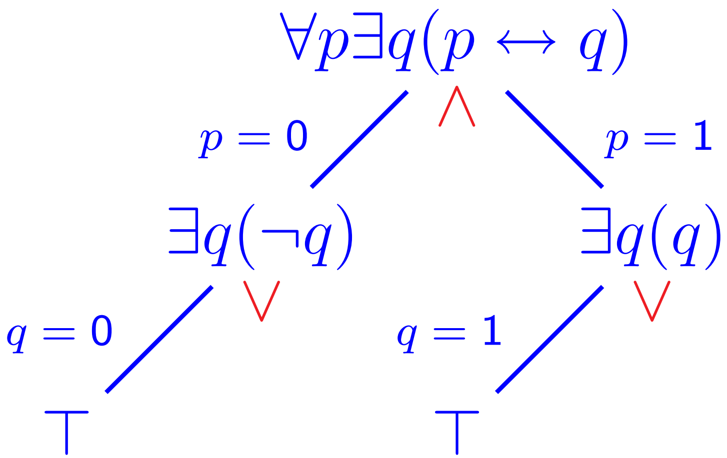
Splitting example

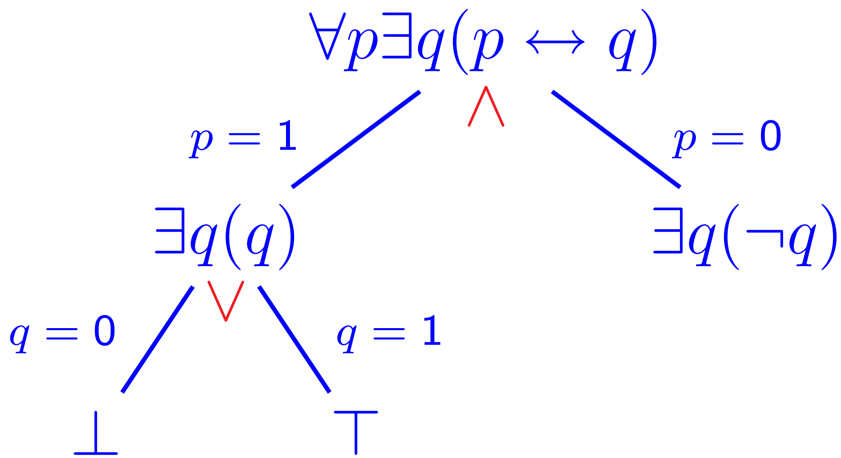


Splitting example

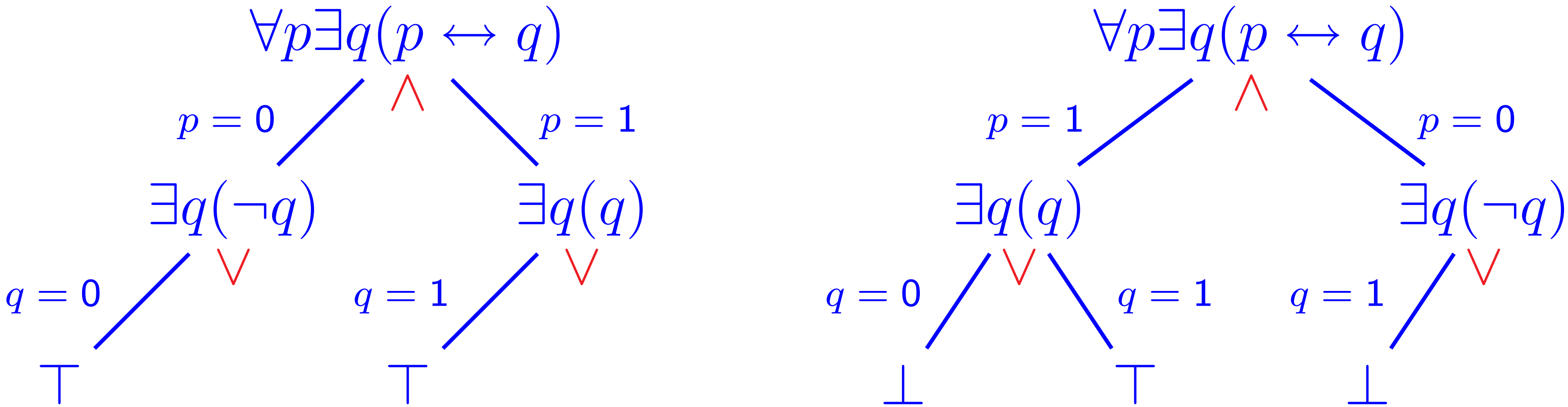


Splitting example





Splitting example



Splitting example