Monadic Logic

Monadic logic - Signature only monadic (unary) predicates.
Monadic logic - Signature only monadic (unary) predicates.

**Theorem.** The satisfiability problem for monadic logic is decidable.
Monadic logic - Signature only monadic (unary) predicates.

**Theorem.** The satisfiability problem for monadic logic is decidable.

Follows from

**Lemma (Small Model Property)** If a monadic formula \( \psi \) with \( k \) unary predicates is satisfiable then it is satisfiable in a structure with at most \( 2^k \) elements.
Monadic logic - Signature only monadic (unary) predicates.

**Theorem.** The satisfiability problem for monadic logic is decidable.

Follows from

**Lemma (Small Model Property)** If a monadic formula $\psi$ with $k$ unary predicates is satisfiable then it is satisfiable in a structure with at most $2^k$ elements.

and

**Theorem.** There is an algorithm that for a formula $\phi$ and a finite structure $M$ checks whether $\phi$ is satisfiable in $M$. 
Proof of small model property lemma
Proof of small model property lemma

Let $M$ be a structure for the signature $\{P_1, \ldots P_k\}$ - all $P_i$ are monadic predicate names.
Proof of small model property lemma

Let $M$ be a structure for the signature $\{P_1, \ldots P_k\}$ - all $P_i$ are monadic predicate names. Define an equivalence relation $\sim$ on the universe $|M|$ of $M$.

\[ a \sim b \text{ iff } a \in P_i^M \iff b \in P_i^M \text{ for } i = 1, \ldots, k \]
Proof of small model property lemma

Let $M$ be a structure for the signature $\{P_1, \ldots, P_k\}$ - all $P_i$ are monadic predicate names. Define an equivalence relation $\sim$ on the universe $|M|$ of $M$.

\[ a \sim b \text{ iff } \]

\[ a \in P_i^M \iff b \in P_i^M \text{ for } i = 1, \ldots, k \]

The equivalence class of $a$ is the set $\hat{a} = \{b : b \sim a\}$. 
Proof of small model property lemma

Let $M$ be a structure for the signature $\{P_1, \ldots, P_k\}$ - all $P_i$ are monadic predicate names. Define an equivalence relation $\sim$ on the universe $|M|$ of $M$.

\[ a \sim b \text{ iff } a \in P_i^M \iff b \in P_i^M \text{ for } i = 1, \ldots, k \]

The equivalence class of $a$ is the set $\hat{a} = \{b : b \sim a\}$. The number of the $\sim$ equivalence classes is finite.

How many?
Proof of small model property lemma

Let $M$ be a structure for the signature $\{P_1, \ldots P_k\}$ - all $P_i$ are monadic predicate names. Define an equivalence relation $\sim$ on the universe $|M|$ of $M$.

\[ a \sim b \text{ iff } a \in P_i^M \iff b \in P_i^M \text{ for } i = 1, \ldots, k \]

The equivalence class of $a$ is the set $\hat{a} = \{b : b \sim a\}$. The number of the $\sim$ equivalence classes is finite.

How many? at most $2^k$
The structure of equivalence classes

Given a structure $M$ for unary predicates.
We define a structure $\hat{M}$ of $\sim$ equivalence classes of $M$. 
The structure of equivalence classes

Given a structure $M$ for unary predicates.
We define a structure $\hat{M}$ of $\sim$ equivalence classes of $M$.

The Universe of $\hat{M}$: the set of $\sim$ equivalence classes of $M$. 
The structure of equivalence classes

Given a structure $\mathcal{M}$ for unary predicates.
We define a structure $\mathcal{\hat{M}}$ of $\sim$ equivalence classes of $\mathcal{M}$.
The Universe of $\mathcal{\hat{M}}$: the set of $\sim$ equivalence classes of $\mathcal{M}$.
Interpretation of predicates: $\hat{a} \in P_i^{\hat{M}}$ iff $a \in P_i^M$
The structure of equivalence classes

Given a structure \( M \) for unary predicates. We define a structure \( \hat{M} \) of \( \sim \) equivalence classes of \( M \).

The Universe of \( \hat{M} \): the set of \( \sim \) equivalence classes of \( M \).

Interpretation of predicates: \( \hat{a} \in P_i^{\hat{M}} \) iff \( a \in P_i^M \)

Lemma. Let \( \rho \) and \( \hat{\rho} \) be environments for \( M \) and \( \hat{M} \) such that \( \rho(x) \in \hat{\rho}(x) \) for all variables \( x \). Then for every formula \( \psi \)

\[
[|\psi|]^M \rho = [|\psi|]^{\hat{M}} \hat{\rho}
\]
The structure of equivalence classes

Given a structure $\mathcal{M}$ for unary predicates.
We define a structure $\hat{\mathcal{M}}$ of $\sim$ equivalence classes of $\mathcal{M}$.
The Universe of $\hat{\mathcal{M}}$: the set of $\sim$ equivalence classes of $\mathcal{M}$.
Interpretation of predicates: $\hat{a} \in P^\hat{\mathcal{M}}_i$ iff $a \in P^\mathcal{M}_i$

Lemma. Let $\rho$ and $\hat{\rho}$ be environments for $\mathcal{M}$ and $\hat{\mathcal{M}}$ such that $\rho(x) \in \hat{\rho}(x)$ for all variables $x$. Then for every formula $\psi$

\[ [\psi]^\mathcal{M} \rho = [\psi]^\hat{\mathcal{M}} \hat{\rho} \]

Proof: By structural inductions.
The structure of equivalence classes

Given a structure $\mathcal{M}$ for unary predicates.
We define a structure $\hat{\mathcal{M}}$ of $\sim$ equivalence classes of $\mathcal{M}$.

The Universe of $\hat{\mathcal{M}}$: the set of $\sim$ equivalence classes of $\mathcal{M}$.

Interpretation of predicates: $\hat{a} \in P_i^{\hat{\mathcal{M}}}$ iff $a \in P_i^\mathcal{M}$

Lemma. Let $\rho$ and $\hat{\rho}$ be environments for $\mathcal{M}$ and $\hat{\mathcal{M}}$ such that $\rho(x) \in \hat{\rho}(x)$ for all variables $x$. Then for every formula $\psi$

$$[|\psi|]^{\mathcal{M}} \rho = [|\psi|]^{\hat{\mathcal{M}}} \hat{\rho}$$

Proof: By structural inductions.

Corollary. $\psi$ is satisfiable in $\mathcal{M}$ iff $\psi$ is satisfiable in $\hat{\mathcal{M}}$. 
The structure of equivalence classes

Given a structure $\mathcal{M}$ for unary predicates. We define a structure $\hat{\mathcal{M}}$ of $\sim$ equivalence classes of $\mathcal{M}$.

The Universe of $\hat{\mathcal{M}}$: the set of $\sim$ equivalence classes of $\mathcal{M}$.

Interpretation of predicates: $\hat{a} \in P^\hat{\mathcal{M}}_i$ iff $a \in P^\mathcal{M}_i$

Lemma. Let $\rho$ and $\hat{\rho}$ be environments for $\mathcal{M}$ and $\hat{\mathcal{M}}$ such that $\rho(x) \in \hat{\rho}(x)$ for all variables $x$. Then for every formula $\psi$

\[ [\psi]^{\mathcal{M}} \rho = [\psi]^{\hat{\mathcal{M}}} \hat{\rho} \]

Proof: By structural inductions.

Corollary. $\psi$ is satisfiable in $\mathcal{M}$ iff $\psi$ is satisfiable in $\hat{\mathcal{M}}$.

Corollary. If $\psi$ is satisfiable then $\psi$ is satisfiable in a structure with at most $2^k$ elements.
**Quantifier Elimination**

**Theorem.** The satisfiability problem for formulas in the signature \{<, =\} over the rationals is decidable.
Quantifier Elimination

**Theorem.** The satisfiability problem for formulas in the signature \(<, =\) over the rationals is decidable. Follows from

**Lemma (Quantifier Elimination)**

1. Every formula is equivalent over Q to a quantifier free formula.
Theorem. The satisfiability problem for formulas in the signature \( \{<,=\} \) over the rationals is decidable. Follows from

Lemma (Quantifier Elimination)

1. Every formula is equivalent over \( \mathbb{Q} \) to a quantifier free formula.

2. There is an algorithm which for every \( \phi \) in the signature \( \{<,=\} \) constructs a quantifier free \( \psi \) such that \( \psi \) is equivalent to \( \phi \) over the rationals,
Quantifier Elimination

Theorem. The satisfiability problem for formulas in the signature $\{<,=\}$ over the rationals is decidable. Follows from Lemma (Quantifier Elimination)

1. Every formula is equivalent over $\mathbb{Q}$ to a quantifier free formula.

2. There is an algorithm which for every $\phi$ in the signature $\{<,=\}$ constructs a quantifier free $\psi$ such that $\psi$ is equivalent to $\phi$ over the rationals,
Quantifier Elimination

**Theorem.** The satisfiability problem for formulas in the signature \( \{<,=\} \) over the rationals is decidable.

Follows from

**Lemma (Quantifier Elimination)**

1. Every formula is equivalent over \( \mathbb{Q} \) to a quantifier free formula.

2. There is an algorithm which for every \( \phi \) in the signature \( \{<,=\} \) constructs a quantifier free \( \psi \) such that \( \psi \) is equivalent to \( \phi \) over the rationals,

and

**Lemma.** The satisfiability problem over \( \mathbb{Q} \) for quantifier free formulas is decidable.
How to check the satisfiability of Quantifier free formulas
How to check the satisfiability of Quantifier free formulas

Is $x_1 < x_2 \land x_3 < x_2$ satisfiable?
How to check the satisfiability of Quantifier free formulas

Is $x_1 < x_2 \land x_3 < x_2$ satisfiable? Yes.
How to check the satisfiability of Quantifier free formulas

Is \( x_1 < x_2 \land x_3 < x_2 \) satisfiable? Yes.
Is \( x_1 < x_2 \land x_3 < x_2 \land x_3 < x_1 \) satisfiable?
How to check the satisfiability of
Quantifier free formulas

Is $x_1 < x_2 \land x_3 < x_2$ satisfiable? Yes.
Is $x_1 < x_2 \land x_3 < x_2 \land x_3 < x_1$ satisfiable? Yes.
How to check the satisfiability of Quantifier free formulas

Is $x_1 < x_2 \land x_3 < x_2$ satisfiable? Yes.
Is $x_1 < x_2 \land x_3 < x_2 \land x_3 < x_1$ satisfiable? Yes.
Is $x_1 < x_2 \land x_2 < x_3 \land x_3 < x_1$ satisfiable?
How to check the satisfiability of Quantifier free formulas

Is $x_1 < x_2 \land x_3 < x_2$ satisfiable? Yes.
Is $x_1 < x_2 \land x_3 < x_2 \land x_3 < x_1$ satisfiable? Yes.
Is $x_1 < x_2 \land x_2 < x_3 \land x_3 < x_1$ satisfiable? No.
How to check the satisfiability of
Quantifier free formulas

Is \( x_1 < x_2 \land x_3 < x_2 \) satisfiable? Yes.
Is \( x_1 < x_2 \land x_3 < x_2 \land x_3 < x_1 \) satisfiable? Yes.
Is \( x_1 < x_2 \land x_2 < x_3 \land x_3 < x_1 \) satisfiable? No.
Is \( x_1 < x_2 \land x_2 = x_3 \land x_3 < x_1 \) satisfiable?
How to check the satisfiability of Quantifier free formulas

Is $x_1 < x_2 \land x_3 < x_2$ satisfiable? Yes.
Is $x_1 < x_2 \land x_3 < x_2 \land x_3 < x_1$ satisfiable? Yes.
Is $x_1 < x_2 \land x_2 < x_3 \land x_3 < x_1$ satisfiable? No.
Is $x_1 < x_2 \land x_2 = x_3 \land x_3 < x_1$ satisfiable? No.
How to check the satisfiability of Quantifier free formulas

Is \( x_1 < x_2 \land x_3 < x_2 \) satisfiable? Yes.
Is \( x_1 < x_2 \land x_3 < x_2 \land x_3 < x_1 \) satisfiable? Yes.
Is \( x_1 < x_2 \land x_2 < x_3 \land x_3 < x_1 \) satisfiable? No.
Is \( x_1 < x_2 \land x_2 = x_3 \land x_3 < x_1 \) satisfiable? No.

How to check whether a conjunction of formulas of the form \( x_i < x_j \) is satisfiable?
How to check the satisfiability of
Quantifier free formulas

Is $x_1 < x_2 \land x_3 < x_2$ satisfiable? Yes.
Is $x_1 < x_2 \land x_3 < x_2 \land x_3 < x_1$ satisfiable? Yes.
Is $x_1 < x_2 \land x_2 < x_3 \land x_3 < x_1$ satisfiable? No.
Is $x_1 < x_2 \land x_2 = x_3 \land x_3 < x_1$ satisfiable? No.

How to check whether a conjunction of formulas of the form $x_i < x_j$ is satisfiable?
Algorithm:

1. Construct graph:
   - Nodes - variables
   - Edges - put an edge from $x_i$ to $x_j$ if $x_i < x_j$. 
How to check the satisfiability of Quantifier free formulas

Is \( x_1 < x_2 \land x_3 < x_2 \) satisfiable? Yes.
Is \( x_1 < x_2 \land x_3 < x_2 \land x_3 < x_1 \) satisfiable? Yes.
Is \( x_1 < x_2 \land x_2 < x_3 \land x_3 < x_1 \) satisfiable? No.
Is \( x_1 < x_2 \land x_2 = x_3 \land x_3 < x_1 \) satisfiable? No.

How to check whether a conjunction of formulas of the form \( x_i < x_j \) is satisfiable?

**Algorithm:**

1. Construct graph:
   - Nodes - variables
   - Edges - put an edge from \( x_i \) to \( x_j \) if \( x_i < x_j \).
2. Check that the graph is cycle free.
How to check the satisfiability of
Quantifier free formulas

How to check whether a conjunction of formulas of the form $x_i < x_j$ and $x_m = x_l$ is satisfiable?
How to check the satisfiability of Quantifier free formulas

How to check whether a conjunction of formulas of the form $x_i < x_j$ and $x_m = x_l$ is satisfiable?
Reduce to the verification whether a conjunction of formulas of the form $x_i < x_j$ is satisfiable?
How to check the satisfiability of Quantifier free formulas

How to check whether a conjunction of formulas of the form \( x_i < x_j \) and \( x_m = x_l \) is satisfiable?

Reduce to the verification whether a conjunction of formulas of the form \( x_i < x_j \) is satisfiable?

Lemma. Let \( \phi \) be a conjunction of formulas of the form \( x_i < x_j \) and \( x_m = x_l \).
How to check whether a conjunction of formulas of the form $x_i < x_j$ and $x_m = x_l$ is satisfiable?

Reduce to the verification whether a conjunction of formulas of the form $x_i < x_j$ is satisfiable?

Lemma. Let $\phi$ be a conjunction of formulas of the form $x_i < x_j$ and $x_m = x_l$.

1. There is $\psi$ such that $\phi$ is satisfiable (over $\mathbb{Q}$) iff $\psi$ is, and $\psi$ is a conjunction of formulas of the form $x_i < x_j$. 
How to check whether a conjunction of formulas of the form $x_i < x_j$ and $x_m = x_l$ is satisfiable?

**Reduce** to the verification whether a conjunction of formulas of the form $x_i < x_j$ is satisfiable?

**Lemma.** Let $\phi$ be a conjunction of formulas of the form $x_i < x_j$ and $x_m = x_l$.

1. There is $\psi$ such that $\phi$ is satisfiable (over $\mathbb{Q}$) iff $\psi$ is, and $\psi$ is a conjunction of formulas of the form $x_i < x_j$.

2. Moreover, there is an algorithm that constructs $\psi$ from $\phi$. 
How to check the satisfiability of Quantifier free formulas

How to check whether a conjunction of formulas of the form \( x_i < x_j \) and \( x_m = x_l \) is satisfiable?

Reduce to the verification whether a conjunction of formulas of the form \( x_i < x_j \) is satisfiable?

**Lemma.** Let \( \phi \) be a conjunction of formulas of the form \( x_i < x_j \) and \( x_m = x_l \).

1. There is \( \psi \) such that \( \phi \) is satisfiable (over Q) iff \( \psi \) is, and \( \psi \) is a conjunction of formulas of the form \( x_i < x_j \).

2. Moreover, there is an algorithm that constructs \( \psi \) from \( \phi \).

**Algorithm.** If there is a conjunct \( x_m = x_l \) replace all occurrences of \( x_m \) by \( x_l \) and remove the conjunct \( x_m = x_l \).
How to check the satisfiability of Quantifier free formulas

1. Construct negation normal form (¬ appears only before atoms).
How to check the satisfiability of Quantifier free formulas

1. Construct negation normal form (¬ appears only before atoms).
2. Eliminate Negations: (a) replace ¬\( x_i < x_j \) by 
\[ x_i = x_j \lor x_i > x_j \]; (b) replace ¬\( x_i = x_j \) by \( x_i < x_j \lor x_j < x_i \).
How to check the satisfiability of Quantifier free formulas

1. Construct negation normal form (¬ appears only before atoms).
2. Eliminate Negations: (a) replace ¬\(x_i < x_j\) by \(x_i = x_j \lor x_i > x_j\); (b) replace ¬\(x_i = x_j\) by \(x_i < x_j \lor x_j < x_i\).
3. Construct DNF: \(\bigvee_i \bigwedge_j c_{i,j}\) where \(c_{i,j}\) is of the form \(x_m < x_l\) or \(x_m = x_l\).
How to check the satisfiability of Quantifier free formulas

1. Construct negation normal form (¬ appears only before atoms).
2. Eliminate Negations: (a) replace \( \neg x_i < x_j \) by \( x_i = x_j \lor x_i > x_j \); (b) replace \( \neg x_i = x_j \) by \( x_i < x_j \lor x_j < x_i \).
3. Construct DNF: \( \bigvee_i \bigwedge_j c_{i,j} \) where \( c_{i,j} \) is of the form \( x_m < x_l \) or \( x_m = x_l \).
4. Check if there is \( i \) such that \( \bigwedge_j c_{i,j} \) is satisfiable
How to check the satisfiability of Quantifier free formulas

1. Construct negation normal form (¬ appears only before atoms).
2. Eliminate Negations: (a) replace ¬\(x_i < x_j\) by \(x_i = x_j \lor x_i > x_j\); (b) replace ¬\(x_i = x_j\) by \(x_i < x_j \lor x_j < x_i\).
3. Construct DNF: \(\bigvee_i \bigwedge_j c_{i,j}\) where \(c_{i,j}\) is of the form \(x_m < x_l\) or \(x_m = x_l\).
4. Check if there is \(i\) such that \(\bigwedge_j c_{i,j}\) is satisfiable

Hence

**Lemma.** The satisfiability problem over \(Q\) for quantifier free formulas is decidable.
Quantifier Elimination

**Lemma.** Every quantifier free formula is equivalent over linear orders to a formula of the form

$$\forall \bigwedge_i \forall j c_{i,j},$$

where $c_{i,j}$ is of the form $x_m < x_l$ or $x_m = x_l$. 
Lemma. Every quantifier free formula is equivalent over linear orders to a formula of the form

$$
\bigvee_{i} \bigwedge_{j} c_{i,j},
$$

where $c_{i,j}$ is of the form $x_m < x_l$ or $x_m = x_l$.

Theorem (Quantifier Elimination)
Quantifier Elimination

Lemma. Every quantifier free formula is equivalent over linear orders to a formula of the form

$$\bigvee_i \bigwedge_j c_{i,j},$$

where $c_{i,j}$ is of the form $x_m < x_l$ or $x_m = x_l$.

Theorem (Quantifier Elimination)

1. Every formula is equivalent over $Q$ to a quantifier free formula.
Lemma. Every quantifier free formula is equivalent over linear orders to a formula of the form

$$\bigvee_i \bigwedge_j c_{i,j},$$

where $c_{i,j}$ is of the form $x_m < x_l$ or $x_m = x_l$.

Theorem (Quantifier Elimination)

1. Every formula is equivalent over $\mathbb{Q}$ to a quantifier free formula.

2. There is an algorithm which for every $\phi$ in the signature $\{<,=\}$ constructs a quantifier free $\psi$ such that $\psi$ is equivalent to $\phi$ over the rationals,
Lemma. Every quantifier free formula is equivalent over linear orders to a formula of the form

$$\bigvee_{i} \bigwedge_{j} c_{i,j},$$

where $c_{i,j}$ is of the form $x_{m} < x_{l}$ or $x_{m} = x_{l}$.

Theorem (Quantifier Elimination)

1. Every formula is equivalent over $\mathbb{Q}$ to a quantifier free formula.

2. There is an algorithm which for every $\phi$ in the signature $\{<,=\}$ constructs a quantifier free $\psi$ such that $\psi$ is equivalent to $\phi$ over the rationals,

Proof by induction on the number of quantifiers.
Proof of Quantifier Elimination

Basis is trivial
Proof of Quantifier Elimination

Basis is trivial
Inductive step it is enough to show
Lemma. \( \exists x_k \bigvee_i \bigwedge_j c_{i,j} \), where \( c_{i,j} \) is of the form \( x_m < x_l \) or \( x_m = x_l \) is equivalent to a quantifier free formula.
Proof of Quantifier Elimination

Basis is trivial
Inductive step it is enough to show
Lemma. \( \exists x_k \bigvee_i \bigwedge_j c_{i,j} \), where \( c_{i,j} \) is of the form \( x_m < x_l \) or \( x_m = x_l \) is equivalent to a quantifier free formula.

\[ \exists x_k \bigvee_i \bigwedge_j c_{i,j} \text{ equivalent to } \bigvee_i \exists x_k \bigwedge_j c_{i,j} \]
Proof of Quantifier Elimination

Basis is trivial
Inductive step it is enough to show
Lemma. \( \exists x_k \bigvee_i \bigwedge_j c_{i,j} \), where \( c_{i,j} \) is of the form \( x_m < x_l \) or \( x_m = x_l \) is equivalent to a quantifier free formula.

\[ \exists x_k \bigvee_i \bigwedge_j c_{i,j} \text{ equivalent to } \bigvee_i \exists x_k \bigwedge_j c_{i,j} \]

\[ \exists x_k \bigwedge_j c_j \text{ is equivalent to } \bigwedge_{j \notin M} c_j \land \exists x_k \bigwedge_{j \in M} c_j, \text{ where } M = \{ i : x_k \text{ occurs in } c_i \} \]
Proof of Quantifier Elimination

**Basis** is trivial

**Inductive step** it is enough to show

**Lemma.** $\exists x_k \bigvee_i \bigwedge_j c_{i,j}$, where $c_{i,j}$ is of the form $x_m < x_l$ or $x_m = x_l$ is equivalent to a quantifier free formula.

$$\exists x_k \bigvee_i \bigwedge_j c_{i,j} \text{ equivalent to } \bigvee_i \exists x_k \bigwedge_j c_{i,j}$$

$$\exists x_k \bigwedge_j c_j \text{ is equivalent to } \bigwedge_{j \notin M} c_j \land \exists x_k \bigwedge_{j \in M} c_j$$, where $M = \{i : x_k \text{ occurs in } c_i\}$. If $x_k = x_l$ is one of the conjuncts in $\exists x_k \bigwedge_{j \in M} c_j$ then this formula is equivalent to

$$\bigwedge_{j \in M} c_j \{x_l/x_k\}$$
Proof of Quantifier Elimination

The last case to consider:

$$\exists x_k \bigwedge_{j} c_j$$

where every $c_j$ is of the form $x_l < x_k$ or $x_k < x_l$ or $x_k < x_l$. 
Proof of Quantifier Elimination

The last case to consider:

\[ \exists x_k \bigwedge_j c_j \]

where every \( c_j \) is of the form \( x_l < x_k \) or \( x_k < x_l \) or \( x_k < x_k \).

If \( x_k < x_k \) is one of the conjunct replace the formula by \( x_k < x_k \).
Proof of Quantifier Elimination

The last case to consider:

$$\exists x_k \bigwedge_{j} c_j$$

where every $c_j$ is of the form $x_l < x_k$ or $x_k < x_l$ or $x_k < x_k$.

If $x_k < x_k$ is one of the conjunct replace the formula by $x_k < x_k$

Otherwise replace it by $\bigwedge_{l \in L, r \in R} x_l < x_r$ where $l \in L$ iff $x_l < x_k$ is one of the conjuncts and $r \in R$ iff $x_k < x_r$ is one of the conjuncts.

Example:

$\exists x_1(x_1 < x_2 \land x_1 < x_3 \land x_4 < x_1 \land x_5 < x_1)$ is equivalent to

$$x_4 < x_2 \land x_4 < x_3 \land x_5 < x_2 \land x_5 < x_3$$
Validity Problem

Instance: a formula $\psi$
Question: Is $\psi$ valid?
Validity Problem

Instance: a formula $\psi$

Question: Is $\psi$ valid?

Theorem (Church) The validity problem is undecidable. (i.e., there is no algorithm for the validity problem).
How to show undecidability
1. Deep analysis of the notion of \textit{algorithm}.
How to show undecidability

1. Deep analysis of the notion of algorithm.

The analysis is done in the course of Automata and Computability
How to show undecidability

1. Deep analysis of the notion of algorithm.

The analysis is done in the course of Automata and Computability

The halting problem is undecidable

Instance: a Turing machine M
Question: Does M stops on all inputs.
How to show undecidability

1. Deep analysis of the notion of algorithm.
   
The analysis is done in the course of Automata and Computability.
   
The halting problem is undecidable.
   
   **Instance:** a Turing machine M
   
   **Question:** Does M stops on all inputs.

2. Reduction techniques
Reduction Technique - an Example
Reduction Technique - an Example

Satisfiability Problem
Instance: a sentence $\psi$
Question: Is $\psi$ satisfiable?
Reduction Technique - an Example

Satisfiability Problem
Instance: a sentence \( \psi \)
Question: Is \( \psi \) satisfiable?

Reduction from Validity to satisfiability.
\( \phi \) is valid iff \( \neg \phi \) is unsatisfiable.

Since Validity problem is undecidable we obtain that satisfiability problem is undecidable.
Assume that $P_1$ and $P_2$ are two decision problems.

**Def.** An algorithm $f$ is a reduction from $P_1$ to $P_2$ if it maps every Yes-instance of $P_1$ to a Yes-instance of $P_2$ and every No-instance of $P_1$ to a No-instance of $P_2$.
Assume that $P_1$ and $P_2$ are two decision problems

**Def.** An algorithm $f$ is a reduction from $P_1$ to $P_2$ if it maps every Yes-instance of $P_1$ to a Yes-instance of $P_2$ and every No-instance of $P_1$ to a No-instance of $P_2$

**Theorem.** If $P_1$ is undecidable and there is a reduction from $P_1$ to $P_2$ then $P_2$ is undecidable.
Post Correspondence Problem

Post Problem

Instance: a sequence \( \langle a_1, b_1 \rangle \langle a_2, b_2 \rangle \ldots \langle a_k, b_k \rangle \) of pairs of strings over \( \{0, 1\} \).
Post Correspondence Problem

Post Problem

Instance: a sequence \( \langle a_1, b_1 \rangle \langle a_2, b_2 \rangle \ldots \langle a_k, b_k \rangle \) of pairs of strings over \( \{0, 1\} \).

A sequence \( i_1 i_2 \ldots i_m \) (for \( i_l \in \{1, \ldots k\} \)) is a solution for this instance if the string \( a_{i_1} a_{i_2} \ldots a_{i_m} \) is the same as the string \( b_{i_1} b_{i_2} \ldots b_{i_m} \).
Post Correspondence Problem

Post Problem
Instance: a sequence \( \langle a_1, b_1 \rangle \langle a_2, b_2 \rangle \ldots \langle a_k, b_k \rangle \) of pairs of strings over \( \{0, 1\} \).
A sequence \( i_1 i_2 \ldots i_m \) (for \( i_l \in \{1, \ldots k\} \)) is a solution for this instance if the string \( a_{i_1} a_{i_2} \ldots a_{i_m} \) is the same as the string \( b_{i_1} b_{i_2} \ldots b_{i_m} \).
Decision Question: Does an instance has a solution.
**Post Correspondence Problem**

**Post Problem**

**Instance:** a sequence \(\langle a_1, b_1 \rangle \langle a_2, b_2 \rangle \ldots \langle a_k, b_k \rangle\) of pairs of strings over \(\{0, 1\}\).

A sequence \(i_1 i_2 \ldots i_m\) (for \(i_l \in \{1, \ldots k\}\)) is a solution for this instance if the string \(a_{i_1} a_{i_2} \ldots a_{i_m}\) is the same as the string \(b_{i_1} b_{i_2} \ldots b_{i_m}\).

**Decision Question:** Does an instance has a solution.

**Theorem(Post)** The Post problem is undecidable.
Reduction of Post Problem to Validity Problem
Reduction of Post Problem to Validity

Problem

Signature a constant \( c \), two unary function \( f_0, f_1 \) and a binary predicate \( R \)
Reduction of Post Problem to Validity

Problem

Signature a constant $c$, two unary function $f_0, f_1$ and a binary predicate $R$

For every instance $I$ of the Post Problem we construct a formula $\psi^I$ such that $I$ has a solution iff $\psi^I$ is valid.
Reduction of Post Problem to Validity Problem

Signature a constant $c$, two unary function $f_0, f_1$ and a binary predicate $R$

For every instance $I$ of the Post Problem we construct a formula $\psi^I$ such that $I$ has a solution iff $\psi^I$ is valid.

Notations For a string $u = \alpha_1, \ldots, \alpha_m$ over $\{0, 1\}$ we write $f_u(x)$ as a shorthand for $f_{\alpha_1}(f_{\alpha_2}(\ldots(f_{\alpha_m}(x)))\ldots)$. 
Reduction of Post Problem to Validity Problem
Reduction of Post Problem to Validity Problem

Construction of $\psi^I$ for an instance
$I = \langle a_1, b_1 \rangle \langle a_2, b_2 \rangle \ldots \langle a_k, b_k \rangle$ of Post problem

Let $\phi_1^I$ be

$$R(f_{a_1}(c), f_{b_1}(c)) \land \cdots \land R(f_{a_k}(c), f_{b_k}(c))$$
Reduction of Post Problem to Validity Problem

Construction of $\psi^I$ for an instance $I = \langle a_1, b_1 \rangle \langle a_2, b_2 \rangle \cdots \langle a_k, b_k \rangle$ of Post problem

Let $\phi_1^I$ be

$$R(f_{a_1}(c), f_{b_1}(c)) \land \cdots \land R(f_{a_k}(c), f_{b_k}(c))$$

Let $\phi_2^I$ be

$$\forall x \forall y R(x, y) \rightarrow (R(f_{a_1}(x), f_{b_1}(y)) \land \cdots \land R(f_{a_k}(x), f_{b_k}(y)))$$
Construction of $\psi^I$ for an instance
$I = \langle a_1, b_1 \rangle \langle a_2, b_2 \rangle \ldots \langle a_k, b_k \rangle$ of Post problem

Let $\phi_1^I$ be

$$R(f_{a_1}(c), f_{b_1}(c)) \land \cdots \land R(f_{a_k}(c), f_{b_k}(c))$$

Let $\phi_2^I$ be

$$\forall x \forall y R(x, y) \rightarrow (R(f_{a_1}(x), f_{b_1}(y)) \land \cdots \land R(f_{a_k}(x), f_{b_k}(y)))$$

Let $\psi^I$ be $\phi_1^I \land \phi_2^I \rightarrow \exists x R(x, x)$
Correctness of the Reduction
Correctness of the Reduction

Theorem (Correctness of the reduction) An instance $I$ of the Post problem has a solution if and only if $\psi^I$ is a valid formula.
Correctness of the Reduction

Theorem (Correctness of the reduction) An instance $I$ of the Post problem has a solution if and only if $\psi^I$ is a valid formula.

The $\Rightarrow$ direction of the Theorem follows from the Lemma. Let $i_1, \ldots, i_n$ be a sequence over $\{1, \ldots, k\}$. Then

$$\phi^I_1 \land \phi^I_2 \models R(f_{a_{i_1}a_{i_2}\ldots a_{i_n}}(c), f_{b_{i_1}b_{i_2}\ldots b_{i_n}}(c))$$
Correctness of the Reduction

Theorem (Correctness of the reduction) An instance $I$ of the Post problem has a solution if and only if $\psi^I$ is a valid formula.

The $\Rightarrow$ direction of the Theorem follows from
Lemma Let $i_1, \ldots, i_n$ be a sequence over $\{1, \ldots, k\}$. Then

$$\phi_1^I \land \phi_2^I \models R(f_{a_i_1 a_i_2 \ldots a_i_n}(c), f_{b_i_1 b_i_2 \ldots b_i_n}(c))$$

Proof By induction on $n$.
Basis $n = 1$ - follows from $\phi_1^I$
Correctness of the Reduction

Theorem (Correctness of the reduction) An instance $I$ of the Post problem has a solution if and only if $\psi^I$ is a valid formula.

The $\Rightarrow$ direction of the Theorem follows from Lemma Let $i_1, \ldots, i_n$ be a sequence over $\{1, \ldots, k\}$. Then

$$\phi^I_1 \land \phi^I_2 \models R(f_{a_{i_1} a_{i_2} \ldots a_{i_n}}(c), f_{b_{i_1} b_{i_2} \ldots b_{i_n}}(c))$$

Proof By induction on $n$.

Basis $n = 1$ - follows from $\phi^I_1$

Inductive Step $n \rightarrow n + 1$ - use $\phi^I_2$. 
The $\iff$ direction of the Correctness Theorem.
The direction of the Correctness Theorem.

Let $\mathcal{M}$ be the structure defined as follows:
The direction of the Correctness Theorem.

Let $M$ be the structure defined as follows: The Universe all strings over $\{0, 1\}$.
The \iff direction of the Correctness Theorem.

Let $M$ be the structure defined as follows:
The Universe all strings over $\{0, 1\}$.
The interpretation of $f_1 : f_1^M(u) = 1u$ (put 1 in the front of the string $u$).
The $\iff$ direction of the Correctness Theorem.

Let $M$ be the structure defined as follows:
The Universe all strings over $\{0, 1\}$.
The interpretation of $f_1$: $f_1^M(u) = 1u$ (put 1 in the front of the string $u$).
The interpretation of $f_0$: $f_0^M(u) = 0u$
Let $M$ be the structure defined as follows: The Universe all strings over $\{0, 1\}$. The interpretation of $f_1: f_1^M(u) = 1u$ (put 1 in the front of the string $u$). The interpretation of $f_0: f_0^M(u) = 0u$ The interpretation of $c$: the empty string $\epsilon$. 

The $\iff$ direction of the Correctness Theorem.
The \( \Leftrightarrow \) direction of the Correctness Theorem.

Let \( M \) be the structure defined as follows:

- The Universe all strings over \( \{0, 1\} \).
- The interpretation of \( f_1: f_1^M(u) = 1u \) (put 1 in the front of the string \( u \)).
- The interpretation of \( f_0: f_0^M(u) = 0u \)
- The interpretation of \( c: \) the empty string \( \epsilon \).
- The interpretation of \( R: R^M(u, v) \) iff there is a sequence \( i_1, \ldots, i_n \) such that \( u \equiv a_{i_1} a_{i_2} \cdots a_{i_n} \) and \( v \equiv b_{i_1} b_{i_2} \cdots b_{i_n} \).
Let $M$ be the structure defined as follows:
The Universe all strings over $\{0, 1\}$.
The interpretation of $f_1: f_1^M(u) = 1u$ (put 1 in the front of the string $u$).
The interpretation of $f_0: f_0^M(u) = 0u$
The interpretation of $c$: the empty string $\epsilon$.
The interpretation of $R: R^M(u, v)$ iff there is a sequence $i_1, \ldots, i_n$ such that $u \equiv a_{i_1}a_{i_2}\cdots a_{i_n}$ and $v \equiv b_{i_1}b_{i_2}\cdots b_{i_n}$.
Observation $\phi_1^I$ and $\phi_2^I$ hold in $M$. 

The $\iff$ direction of the Correctness
Theorem.
Let $M$ be the structure defined as follows:
The Universe all strings over $\{0, 1\}$.
The interpretation of $f_1: f_1^M(u) = 1u$ (put 1 in the front of 
the string $u$).
The interpretation of $f_0: f_0^M(u) = 0u$
The interpretation of $c$: the empty string $\epsilon$.
The interpretation of $R$: $R^M(u, v)$ iff there is a sequence 
$i_1, \ldots, i_n$ such that $u \equiv a_{i_1}a_{i_2}\cdots a_{i_n}$ and $v \equiv b_{i_1}b_{i_2}\cdots b_{i_n}$.
Observation $\phi_1^I$ and $\phi_2^I$ hold in $M$.
Therefore, if $\psi^I$ is valid then there is a string $u$ such that 
$R^M(u, u)$.
The direction of the Correctness Theorem.

Let $M$ be the structure defined as follows:
The Universe all strings over $\{0, 1\}$.
The interpretation of $f_1: f_1^M(u) = 1u$ (put 1 in the front of the string $u$).
The interpretation of $f_0: f_0^M(u) = 0u$
The interpretation of $c$: the empty string $\epsilon$.
The interpretation of $R: R^M(u, v)$ iff there is a sequence $i_1, \ldots, i_n$ such that $u \equiv a_{i_1}a_{i_2}\cdots a_{i_n}$ and $v \equiv b_{i_1}b_{i_2}\cdots b_{i_n}$.
Observation $\phi^I_1$ and $\phi^I_2$ hold in $M$.
Therefore, if $\psi^I$ is valid then there is a string $u$ such that $R^M(u, u)$.

Hence, (by the definition of $R^M$) the $I$ instance of the Post problem has a solution.