Chapter 2

Quantified Propositional Logic (QPL)

We can prove Compactness for *quantified propositional logic* (QPL) by reducing it to Compactness for *propositional logic* (PL). We have already done much of the preliminary work in Chapter 1. We write $\mathsf{WFF}_{\mathsf{QPL}}(\mathcal{P})$ for the set of all wff's of QPL over the set $\mathcal{P}$ of propositional variables.

Lemma 36. *Let Γ be a subset, finite or infinite, of $\mathsf{WFF}_{\mathsf{QPL}}(\mathcal{P})$. We can construct a set Γ' of quantifier-free formulas in $\mathsf{WFF}_{\mathsf{PL}}(\mathcal{P})$ such that:*

1. *Γ is finitely satisfiable iff Γ' is finitely satisfiable.*
2. *Γ is satisfiable iff Γ' is satisfiable.*

The construction in the proof below establishes a stronger result: Γ and Γ' are more than *finitely equisatisfiable* and *equisatisfiable*; they are in fact *equivalent* (informally, "they say the same thing"): For every QPL wff $\varphi \in \Gamma$ there is a PL wff $\varphi' \in \Gamma'$ such that φ and φ' are equivalent, and for every PL wff $\varphi' \in \Gamma'$ there is a QPL wff $\varphi \in \Gamma$ such that φ and φ' are equivalent.[15]

Proof. If φ is a propositional wff, we write "$\varphi[p := \bot]$" and "$\varphi[p := \top]$" to denote the substitution of the symbols $\bot$ and $\top$, respectively, for every occurrence of variable p in φ. We define a translation from QPL to PL, named "$\boxed{\mathsf{QPL} \mapsto \mathsf{PL}}$" by structural induction:[16]

1. $\boxed{\mathsf{QPL} \mapsto \mathsf{PL}}(p) \overset{\text{def}}{=} p \qquad \text{(for every variable } p\text{)}$
2. $\boxed{\mathsf{QPL} \mapsto \mathsf{PL}}(\neg\varphi) \overset{\text{def}}{=} \neg \boxed{\mathsf{QPL} \mapsto \mathsf{PL}}(\varphi)$
3. $\boxed{\mathsf{QPL} \mapsto \mathsf{PL}}(\varphi \wedge \psi) \overset{\text{def}}{=} \boxed{\mathsf{QPL} \mapsto \mathsf{PL}}(\varphi) \wedge \boxed{\mathsf{QPL} \mapsto \mathsf{PL}}(\psi)$
4. $\boxed{\mathsf{QPL} \mapsto \mathsf{PL}}(\varphi \vee \psi) \overset{\text{def}}{=} \boxed{\mathsf{QPL} \mapsto \mathsf{PL}}(\varphi) \vee \boxed{\mathsf{QPL} \mapsto \mathsf{PL}}(\psi)$
5. $\boxed{\mathsf{QPL} \mapsto \mathsf{PL}}(\varphi \to \psi) \overset{\text{def}}{=} \boxed{\mathsf{QPL} \mapsto \mathsf{PL}}(\varphi) \to \boxed{\mathsf{QPL} \mapsto \mathsf{PL}}(\psi)$
6. $\boxed{\mathsf{QPL} \mapsto \mathsf{PL}}(\forall p\ \varphi) \overset{\text{def}}{=} \Big(\boxed{\mathsf{QPL} \mapsto \mathsf{PL}}(\varphi)\Big)[p := \bot] \ \wedge\ \Big(\boxed{\mathsf{QPL} \mapsto \mathsf{PL}}(\varphi)\Big)[p := \top]$
7. $\boxed{\mathsf{QPL} \mapsto \mathsf{PL}}(\exists p\ \varphi) \overset{\text{def}}{=} \Big(\boxed{\mathsf{QPL} \mapsto \mathsf{PL}}(\varphi)\Big)[p := \bot] \ \vee\ \Big(\boxed{\mathsf{QPL} \mapsto \mathsf{PL}}(\varphi)\Big)[p := \top]$

[15] If so, why use QPL instead of PL? Applications and exercises in Section 2.2 illustrate some of the advantages – just a few out of many – of using QPL rather than PL. In particular, QPL is central in the study of what is called the *polynomial-time hierarchy* in computational complexity, something outside the scope of these notes.

[16] I quickly run out of notation. To simplify my task, I denote translations of syntax in a particular way: Each is denoted by a framed box and what is inside the box, here "QPL $\mapsto$ PL", suggests what the translation does. The box and its contents is a single name.

Claim: For every QPL wff φ, the transformation $\boxed{\mathsf{QPL} \mapsto \mathsf{PL}}(\varphi)$ satisfies the following properties:

(a) $\boxed{\mathsf{QPL} \mapsto \mathsf{PL}}(\varphi)$ is a propositional wff,

(b) the set of free variables $\mathrm{FV}(\varphi)$ in φ are exactly all the variables occurring in $\boxed{\mathsf{QPL} \mapsto \mathsf{PL}}(\varphi)$, and

(c) if $X = \mathrm{FV}(\varphi)$, then for every truth assignment σ to the members of X, it holds that σ satisfies φ iff σ satisfies $\boxed{\mathsf{QPL} \mapsto \mathsf{PL}}(\varphi)$.

Part (c) in this claim shows that φ and $\boxed{\mathsf{QPL} \mapsto \mathsf{PL}}(\varphi)$ are not only equisatisfiable, but also equivalent. We leave the proof of this claim as an exercise. Given a subset $\Gamma \subseteq \mathsf{WFF}_{\mathsf{QPL}}(\mathcal{P})$, we now define Γ' by:

$$\Gamma' \stackrel{\text{def}}{=} \left\{ \boxed{\mathsf{QPL} \mapsto \mathsf{PL}}(\varphi) \;\middle|\; \varphi \in \Gamma \right\}$$

By the preceding claim, we conclude that for every truth assignment σ to $\mathcal{P}$:

- for every finite $\Delta \subseteq \Gamma$ there is a finite $\Delta' \subseteq \Gamma'$ s.t. σ satisfies Δ iff σ satisfies Δ',
- for every finite $\Delta' \subseteq \Gamma'$ there is a finite $\Delta \subseteq \Gamma$ s.t. σ satisfies Δ iff σ satisfies Δ',
- σ satisfies Γ iff σ satisfies Γ'.

We leave the missing details in the proof of the preceding three bullet points as an exercise. □

Exercise 37. Prove the **claim** in the proof of Lemma 36. *Hint*: Use structural induction on wff's of QPL, following the seven steps in the definition of the transformation $\boxed{\mathsf{QPL} \mapsto \mathsf{PL}}$. □

Exercise 38. In the statement of Lemma 36 and its proof, the set Γ of quantified propositional wff's and the set Γ' of propositional wff's are equivalent. Specify:

1. Conditions under which $\lvert\Gamma\rvert = \lvert\Gamma'\rvert$, and
2. Conditions under which $\lvert\Gamma\rvert > \lvert\Gamma'\rvert$,

where $\lvert\Gamma\rvert$ is the cardinality of the set Γ. *Hint*: Consider, for example, the case when all the quantified propositional wff's in Γ are *closed*; what is Γ' in this case? □

Exercise 39. Supply the details in the proof of the three bullet points at the end of the proof of Lemma 36. *Hint*: This is subtler than at first blush; do Exercise 38 before this one. □

2.1 Compactness and Completeness in QPL

Theorem 40 (Compactness for QPL, Version I)**.** *Let $\Gamma \subseteq \mathsf{WFF}_{\mathsf{QPL}}(\mathcal{P})$. It then holds that Γ is satisfiable iff Γ is finitely satisfiable.*

Proof. The left-to-right implication is immediate. The non-trivial is the right-to-left implication, *i.e.*, we have to prove that if Γ is finitely satisfiable, then Γ is satisfiable. Let Γ' be the set of propositional wff's defined from Γ according to Lemma 36.

By Lemma 36, Γ is finitely satisfiable iff Γ' is finitely satisfiable. By Theorem 2, Γ' is finitely satisfiable iff Γ' is satisfiable. By Lemma 36 once more, Γ' is satisfiable iff Γ is satisfiable. Hence, if Γ is finitely satisfiable, then Γ is satisfiable, as desired. □

For the next lemma and its corollary, review the formal semantics of quantified propositional wff's in Appendix B.

Lemma 41. *Let* $\Gamma \subseteq \mathsf{WFF}_{\mathsf{QPL}}(\mathcal{P})$ *and* $\varphi \in \mathsf{WFF}_{\mathsf{QPL}}(\mathcal{P})$*, both arbitrary. It then holds that* $\Gamma \models \varphi$ *iff* $\Gamma \cup \{\neg\varphi\}$ *is unsatisfiable – or, equivalently,* $\Gamma \not\models \varphi$ *iff* $\Gamma \cup \{\neg\varphi\}$ *is satisfiable.*

Proof. Identical to the proof of Lemma 6, except that here Γ is a set of quantified propositional wff's and φ is a quantified propositional wff. □

Corollary 42 (Compactness for QPL, Version II)**.** *Let* $\Gamma \subseteq \mathsf{WFF}_{\mathsf{QPL}}(\mathcal{P})$ *and* $\varphi \in \mathsf{WFF}_{\mathsf{QPL}}(\mathcal{P})$*. It then holds that* $\Gamma \models \varphi$ *iff there is a finite subset* $\Gamma_0 \subseteq \Gamma$ *such that* $\Gamma_0 \models \varphi$*.*

Proof. Identical to the proof of Corollary 7, except that here Γ is a set of quantified propositional wff's and φ is a quantified propositional wff. Moreover, here we invoke Lemma 41 instead of Lemma 6, and Theorem 40 instead of Theorem 2. □

The statements of Lemma 10 (the *Deduction Theorem*) and Lemma 12, as well as their respective proofs, hold verbatim for the logic of quantified propositional wff's – except that "$\mathsf{WFF}_{\mathsf{PL}}(\mathcal{P})$" has to be replaced by "$\mathsf{WFF}_{\mathsf{QPL}}(\mathcal{P})$" throughout.

Theorem 43 (Completeness for the Logic QPL)**.** *Let* $\Gamma \subseteq \mathsf{WFF}_{\mathsf{QPL}}(\mathcal{P})$ *and* $\psi \in \mathsf{WFF}_{\mathsf{QPL}}(\mathcal{P})$*, both arbitrary. If* $\Gamma \models \psi$*, then* $\Gamma \vdash \psi$*.*

Proof. This proof is identical to the proof of Theorem 13, except that all formulas are now quantified propositional wff's, not just propositional wff's. □

2.2 Applications and Exercises

Example 44 (*Cliques in Simple Graphs*)**.** You need to consult Example 15 as you read through this example. We are given a finite simple graph G whose set of vertices is $\{1, 2, \ldots, n\}$ and we want to test the presence or absence of a k-clique in G with a wff of QPL, for some fixed integer $k \geqslant 1$. We use the same set X of propositional variables as in Example 15:

$$X \stackrel{\text{def}}{=} \Big\{ x_{i,j} \;\Big|\; 1 \leqslant i < j \leqslant n \Big\},$$

together with an additional set of auxiliary variables $\mathcal{Q}$, introduced below. We want to define a wff $\varphi \in \mathsf{WFF}_{\mathsf{QPL}}(X \cup \mathcal{Q})$ such that:

- $\mathrm{FV}(\varphi) \subseteq X$, *i.e.*, the free variables of φ are in X and its bound variables are in $\mathcal{Q}$, and
- φ is satisfied by G iff G contains a k-clique.

We say φ *is satisfied by* G iff φ is satisfied by the truth assignment induced by G, which is defined as in Example 15 and is of the form $\sigma : X \to \{\mathit{true}, \mathit{false}\}$. Our analysis is in two stages:

Stage 1. We introduce a fresh set of variables $\mathcal{Q} \stackrel{\text{def}}{=} \{\, q_{i,\ell} \mid 1 \leqslant i \leqslant n \text{ and } 1 \leqslant \ell \leqslant k \,\}$, and define a propositional wff ψ over $\mathcal{Q}$ satisfied by a truth assignment $\zeta : \mathcal{Q} \to \{\mathit{true}, \mathit{false}\}$ iff:

- for every $i \in \{1, \ldots, n\}$ there is at most one $\ell \in \{1, \ldots, k\}$ such that $\zeta(q_{i,\ell}) = \mathit{true}$,
- for every $\ell \in \{1, \ldots, k\}$ there is exactly one $i \in \{1, \ldots, n\}$ such that $\zeta(q_{i,\ell}) = \mathit{true}$.

Think of an assignment ζ for $\mathcal{Q}$ as defining a relation between $\{1, \ldots, n\}$ and $\{1, \ldots, k\}$. Moreover, if ψ is defined so that a ζ satisfying it satisfies the two preceding conditions, then such a ζ can be viewed as an injective map from $\{1, \ldots, k\}$ to $\{1, \ldots, n\}$ – or, put differently, such a ζ selects exactly k entries out of the set $\{1, \ldots, n\}$, *i.e.*, a subset of size k from $\{1, \ldots, n\}$. To emphasize that all the variables occurring in ψ are in $\mathcal{Q}$ and disjoint from X, let's write $\psi(\mathcal{Q})$ instead of just ψ.

Here is an appropriate definition of the desired $\psi(\mathcal{Q})$ where, to the right of every line below, we include an informal justification in plain text:

$$\begin{aligned}
\psi(\mathcal{Q}) \ \stackrel{\text{def}}{=}\ & \bigwedge \left\{ \neg(q_{i,\ell} \wedge q_{i,\ell'}) \,\middle|\, 1 \leqslant i \leqslant n,\ 1 \leqslant \ell < \ell' \leqslant k \right\} \wedge \quad & \text{(at most one } \ell \text{ for every } i\text{)} \\
& \bigwedge \left\{ \neg(q_{i,\ell} \wedge q_{i',\ell}) \,\middle|\, 1 \leqslant i < i' \leqslant n,\ 1 \leqslant \ell \leqslant k \right\} \wedge \quad & \text{(at most one } i \text{ for every } \ell\text{)} \\
& \bigwedge \left\{ \bigvee \left\{ q_{i,\ell} \,\middle|\, 1 \leqslant i \leqslant n \right\} \,\middle|\, 1 \leqslant \ell \leqslant k \right\} & \text{(at least one } i \text{ for every } \ell\text{)}
\end{aligned}$$

Stage 2. We are ready to define the desired wff φ, where we write $\exists\overrightarrow{\mathcal{Q}}$ to mean the existential quantification of all the variables in $\mathcal{Q}$:

$$\begin{aligned}
\varphi \stackrel{\text{def}}{=}\ & \exists\overrightarrow{\mathcal{Q}}.\ \psi(\mathcal{Q}) \wedge \\
& \qquad \bigwedge \left\{ (q_{i,\ell} \wedge q_{i',\ell'}) \to x_{i,i'} \,\middle|\, 1 \leqslant i < i' \leqslant n \text{ and } 1 \leqslant \ell, \ell' \leqslant k \text{ with } \ell \neq \ell' \right\}.
\end{aligned}$$

Informally, the first line of φ says: There exists a k-subset of the n vertices of G such that the second line in φ holds. And the second line says: If there exists a truth assignment to the variables in $\mathcal{Q}$ so that $(q_{i,\ell} \wedge q_{i',\ell'})$ is true, *i.e.*, vertices i and i' are selected, then $x_{i,i'}$ is true, *i.e.*, there is an edge between i and i'. It follows that φ is satisfied by G iff G contains a k-clique. Note carefully that our definition of φ specifies ℓ and ℓ' according to "$1 \leqslant \ell, \ell' \leqslant k$ with $\ell \neq \ell'$" and not "$1 \leqslant \ell < \ell' \leqslant k$" (why?). □

Exercise 45 (*Dominating Sets in Simple Graphs*)**.** Read and understand Example 44 before you embark on this exercise. Review the definition of *dominating sets in simple graphs* in Exercise 18.

Your task is to define a wff $\varphi \in \mathsf{WFF}_{\mathsf{QPL}}(X \cup \mathcal{Q})$, and then justify its correctness, such that: Given a simple graph G with $n \geqslant 1$ vertices and an integer $1 \leqslant k \leqslant n$, it holds that: *$\varphi$ is satisfied by G iff G contains a k-dominating set.*

Hint: You only need to modify Stage 2 in Example 44. □

Example 46 (*Transition Systems*)**.** A *transition system* (sometime called a *state-transition system*) is specified as a structure $\mathcal{M} \stackrel{\text{def}}{=} (\mathsf{States}, R, \mathsf{Init}, \mathsf{End})$ where States is a finite or infinite set, $R \subseteq \mathsf{States} \times \mathsf{States}$ is a binary relation (*the transition relation*), and $\mathsf{Init} \subseteq \mathsf{States}$ and $\mathsf{End} \subseteq \mathsf{States}$ are the subsets of *initial states* and *end states*, respectively.

When States is a finite set, $\mathcal{M}$ is conveniently represented by a finite directed graph; an example is shown in Figure 2.1. Each state of the system is a *node* in the graph and each possible transition from a state to another is a directed *edge*.

We can uniquely identify each state by a bit vector, with $B = \{\bot, \top\}$ as the set of bits. For the system in Figure 2.1 with 4 states, 2-bit vectors suffice for this encoding; in this case, we can model the *transition relation* by a propositional wff θ with propositional variables $\{p_1, p_2, p_3, p_4\}$ where we use the pairs (p_1, p_2) and (p_3, p_4) to encode the *from-state* and *to-state* of a transition, respectively. The setup in full generality is thus:

$$\begin{aligned}
\mathsf{encode} &: \mathsf{States} \to B^n & & \text{(where } n = \lceil \log_2 \mathsf{size}(\mathsf{States}) \rceil\text{)}, \\
\mathsf{init} &: B^n \to \{\mathit{false}, \mathit{true}\} & & \text{(the set of initial states)}, \\
\mathsf{end} &: B^n \to \{\mathit{false}, \mathit{true}\} & & \text{(the set of end states)}, \\
\theta &: B^n \times B^n \to \{\mathit{false}, \mathit{true}\} & & \text{(the transition relation)}.
\end{aligned}$$

Whichever is more convenient, we write $\{\mathsf{init}, \mathsf{end}, \theta\}$ as functions (as above) or sometimes as unary and binary relations; either way, they are translated into propositional wff's whose interpretations are values in $\{\mathit{false}, \mathit{true}\}$. Note that the symbol "$R$", "$\mathsf{Init}$", and "$\mathsf{End}$", are not part of the vocabulary of PL and QPL, which is why we need to write three wff's $\{\,\theta,\ \mathsf{init},\ \mathsf{end}\,\}$ in the syntax of PL and QPL to formally model these relations.

For the particular transition system in Figure 2.1 where $n = \log_2 4 = 2$, the setup is thus:

$$
\begin{aligned}
\mathsf{encode}(\mathsf{States}) &\stackrel{\text{def}}{=} \Big\{(\bot,\bot),(\bot,\top),(\top,\bot),(\top,\top)\Big\},\\
\mathsf{init}(p_1,p_2) &\stackrel{\text{def}}{=} (p_1 \leftrightarrow \bot)\wedge(p_2 \leftrightarrow \bot) = (\neg p_1 \wedge \neg p_2) \quad \text{or also } \ \mathsf{init} \stackrel{\text{def}}{=} \{(\bot,\bot)\},\\
\mathsf{end}(p_1,p_2) &\stackrel{\text{def}}{=} (p_1 \leftrightarrow \top)\wedge(p_2 \leftrightarrow \top) = (p_1 \wedge p_2) \quad \text{or also } \ \mathsf{end} \stackrel{\text{def}}{=} \{(\top,\top)\},\\
\theta(p_1,p_2,p_3,p_4) &\stackrel{\text{def}}{=} \big((\neg p_1 \wedge \neg p_2) \ \to\ (\neg p_3 \wedge \neg p_4)\vee(\neg p_3 \wedge p_4)\big) && \text{(from } s_1)\\
&\quad \wedge\ \big((\neg p_1 \wedge p_2) \ \to\ (\neg p_3 \wedge p_4)\vee(p_3 \wedge \neg p_4)\big) && \text{(from } s_2)\\
&\quad \wedge\ \big((p_1 \wedge \neg p_2) \ \to\ (\neg p_3 \wedge p_4)\vee(\neg p_3 \wedge \neg p_4)\vee(p_3 \wedge p_4)\big) && \text{(from } s_3)\\
&\quad \wedge\ \big((\neg p_3 \wedge \neg p_4) \ \to\ (\neg p_1 \wedge \neg p_2)\vee(p_1 \wedge \neg p_2)\big) && \text{(to } s_1)\\
&\quad \wedge\ \big((\neg p_3 \wedge p_4) \ \to\ (\neg p_1 \wedge \neg p_2)\vee(\neg p_1 \wedge p_2)\vee(p_1 \wedge \neg p_2)\big) && \text{(to } s_2)\\
&\quad \wedge\ \big((p_3 \wedge \neg p_4) \ \to\ (\neg p_1 \wedge p_2)\big) && \text{(to } s_3)\\
&\quad \wedge\ \big((p_3 \wedge p_4) \ \to\ (p_1 \wedge \neg p_2)\big) && \text{(to } s_4)
\end{aligned}
$$

Note how we write θ: it is a conjunction of seven implications, three implications for the *from-state* part of transitions (or the *tail* end of edges) and four implications for the *to-state* part of transitions (or the *head* end of edges). Convince yourself that θ faithfully models the behavior of the relation R (a little painstaking task!).

With the preceding we can now express problems of *reachability* in the transition system, namely, whether some states are reachable from other states. Consider the following wff's as an example, where we purposely use a different set of propositional variables $\{q_1, q_2, \ldots\}$:

$$
\begin{aligned}
\varphi_1(q_1,\ldots,q_4) &\stackrel{\text{def}}{=} \mathsf{init}(q_1,q_2)\wedge\theta(q_1,q_2,q_3,q_4)\wedge\mathsf{end}(q_3,q_4),\\
\varphi_2(q_1,\ldots,q_6) &\stackrel{\text{def}}{=} \mathsf{init}(q_1,q_2)\wedge\theta(q_1,q_2,q_3,q_4)\wedge\theta(q_3,q_4,q_5,q_6)\wedge\mathsf{end}(q_5,q_6),\\
\varphi_3(q_1,\ldots,q_8) &\stackrel{\text{def}}{=} \mathsf{init}(q_1,q_2)\wedge\theta(q_1,q_2,q_3,q_4)\wedge\theta(q_3,q_4,q_5,q_6)\wedge\theta(q_5,q_6,q_7,q_8)\wedge\mathsf{end}(q_7,q_8).
\end{aligned}
$$

The wff φ_1 (resp. φ_2, resp. φ_3) encodes the problem of whether it is possible to go from *initial state* s_1 to *end state* s_4 in one step (resp. two steps, resp. three steps). By inspection, the transition system $\mathcal{M}$ in Figure 2.1 does not satisfy φ_1 and φ_2, while $\mathcal{M}$ does satisfy φ_3. More succintly, using quantifiers allowed by the syntax of QPL, it holds that:[17]

$$
\begin{aligned}
&\Gamma\ \not\models\ (\exists\, q_1\cdots q_4.\ \varphi_1),\quad \Gamma\ \not\models\ (\exists\, q_1\cdots q_6.\ \varphi_2),\quad \text{and } \Gamma\ \models\ (\exists\, q_1\cdots q_8.\ \varphi_3),\\
&\text{where}\quad \Gamma \stackrel{\text{def}}{=} \Big\{\ \forall\, p_1\, p_2.\, \mathsf{init}(p_1,p_2)\,, \forall\, p_1\, p_2.\, \mathsf{end}(p_1,p_2)\,, \forall\, p_1\cdots p_4.\ \theta(p_1,p_2,p_3,p_4)\ \Big\}.
\end{aligned}
$$

Things become more complicated when the transition relation expressed by θ has to account for many more states than only four in this example, or when the path from an *initial state* to an *end state* must satisfy some restriction. Exercises 47 and 48 pursue the analysis started in this example further.

Exercise 47 (*Reachability in Transition Systems*)**.** This is a continuation of the analysis in Example 46 in relation to the particular transition system in Figure 2.1. If we want to model reachability of s_4 from s_1 for some large number k of steps, the resulting wff will be unwieldy

[17] It is tempting to replace "$\Gamma \not\models \ldots$" and "$\Gamma \models \ldots$" by "$\mathcal{M} \not\models \ldots$" and "$\mathcal{M} \models \ldots$", respectively. Although the intent is clear, the latter notation is not permitted by the definition of "$\models$" in the semantics of QPL. $\mathcal{M}$ is not a model in quantified propositional logic. The set of wff's Γ completely captures the behavior of the transition system.

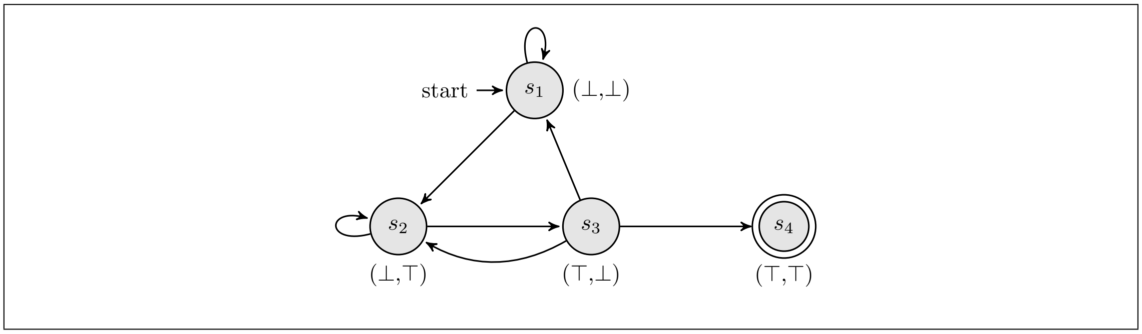

Figure 2.1: Graphical representation of a transition system with 4 states $\{s_1, s_2, s_3, s_4\}$ in Example 46, which can be encoded by 2-bit vectors $\{(\bot,\bot),(\bot,\top),(\top,\bot),(\top,\top)\}$, where s_1 is an *initial state* and s_4 is an *end state.*

with k copies of θ as sub-wff's. A way out is to resort to a wff φ_k involving quantifiers and a single copy of θ, as follows:

$$\varphi_k \stackrel{\text{def}}{=} \exists\, q_1\, q_2 \;\cdots\; q_{2k+1}\, q_{2k+2} \,.\, \mathsf{init}(q_1, q_2) \;\wedge\; \mathsf{end}(q_{2k+1}, q_{2k+2}) \;\wedge$$
$$\forall\, r_1\, r_2\, r_3\, r_4 \,.\Big(\Big(\bigvee\nolimits_{0\leqslant i\leqslant k-1} r_1 = q_{2i+1} \wedge r_2 = q_{2i+2} \wedge r_3 = q_{2i+3} \wedge r_4 = q_{2i+4}\Big) \;\to\; \theta(r_1, r_2, r_3, r_4)\Big)$$

where "$p = q$" abbreviates "$p \leftrightarrow q$", and "$p \leftrightarrow q$" abbreviates "$(p \to q) \wedge (q \to p)$". Give a precise argument showing that φ_k correctly models reachability of s_4 from s_1 in k steps. □

Exercise 48 (*The Unwind Property in Transition Systems*)**.** A finite transition system $\mathcal{M}$ is said to have the *unwind property* if there is a natural number n such that every execution path from an *initial state* to an *end state* halts within at most n steps (or n single-edge transitions in the graph representation of $\mathcal{M}$).

As it stands, the system in Figure 2.1 does not have the unwind property. From the *initial state* s_1 to the *end state* s_4, there are arbitrarily long executions paths, thus preventing any "unwinding" or "unrolling" of the system into an equivalent and finite loop-free transition system.

We now consider operating the system under two separate restrictions (assumed to be enforced by mechanisms not mentioned in our definitions here):

(a) An execution path from s_1 to s_4 is *valid* provided each of the states in $\{s_1, s_2, s_3\}$ is visited an equal number $n \geqslant 1$ of times.

(b) An execution path from s_1 to s_4 is *valid* provided s_1 is visited at most $n \leqslant 2$ times, and each of s_2 and s_3 is visited $2n$ times.

There are four parts in this exercise. For the last two parts, you may find it helpful to do Exercise 47 first, taking advantage of the succintness that quantifiers allow in writing wff's:

1. Write the propositional wff θ_a which models the transition relation when the system operates under restriction (a).

   Hint: θ_a is a restriction of θ defined in Example 46. The requirement that all the states in $\{s_1, s_2, s_3\}$ are visited an equal number of times precludes the use of the self-loops around s_1 and s_2, as well as the loop "$s_2 \to s_3 \to s_2$", but not the loop "$s_1 \to s_2 \to s_3 \to s_1$".

2. Write the propositional wff θ_b which models the transition relation when the system operates under restriction (b).

   Hint: The requirement that s_2 and s_3 are visited an equal number times precludes the use of the self-loop around s_2, but not the use of the other loops.

3. Give a formal logic-based argument (no "hand waving") showing the transition system under restriction (a) does not have the *unwind property.* Thus, under restriction (a), the existence of arbitrarily long (finite) valid executions implies the system does not always halt, *i.e.*, there are non-terminating valid executions.

Hint: Exhibit an infinite set Δ of QPL wff's expressing the existence of an infinite path starting at s_1 with infinitely many valid finite prefixes. Show that Δ is finitely satisfiable and invoke Compactness.

4. Give a precise argument showing that the transition system under restriction (b) does have the *unwind property*. Thus, under restriction (b), the system always halts and all valid execution paths are finite.

   Hint: This will be (mostly) a counting argument based on what restriction (b) entails. $\square$