An Effective Environment for Software Development

4C－6

富樫 敦　金指 文明　陸 暁松*

静岡大学 情報学部 情報科学科: togashi@cs.inf.shizuoka.ac.jp

1. Introduction

This paper proposes new methodologies for the description of system requirements and the synthesis of formal specifications from user requirements. The formal specifications can be taken as models of the system requirements. More generally, the main objective is to be able to derive an implementable or operational system description from a given high-level description on system functions. The proposed methodology can be fully automated, hence may/can improve both productivity and quality of system development. We have implemented a support system based on our approach and applied several practical system designs such as a telephone service, a communication protocol, a CATV system, etc.

2. Requirements & Specifications

Let $\mathcal{P}$ be a set of *atomic propositions*. Each atomic proposition describes a specific property of the intended system under the target of design. A system can be essentially specified by its fundamental functions and their related constraints for execution. To be more precise, a system function may be invoked by a specific input provided that its pre-condition to be satisfied before execution can hold in the current state. Then, the function is executed, possibly producing some appropriate output. After the execution the current state is changed into the new one. In the new state, another functions (including the same function as well) can be applicable. Taking account of this intuition of system specifications, a function requirement is formally defined in the next definition.

Definition A *function requirement* is a tuple $\rho = \langle id, a, f_{in}, o, f_{out} \rangle$, where

(1) id is a *name* of the function;
(2) a is an *input symbol* of the function;
(3) f_{in} is a *pre-condition* of the function to be satisfied before execution, which is represented as a consistent proposition using atomic propositions in $\mathcal{P}$;
(4) o is an *output symbol* of the function;
(5) f_{out} is a *post-condition* of the function to be satisfied after execution, which is represented as a consistent conjunction of literals by atomic propositions in $\mathcal{P}$. □

For simplicity, in what follows we omit the names and the output symbols from the description of function requirements because they do not play the central roles on the theoretical treatment in this paper. A function requirement $\rho = \langle a, f_{in}, f_{out} \rangle$ is often abbreviated as $\rho : f_{in} \stackrel{a}{\Rightarrow} f_{out}$.

Definition A *system requirement* is a pair $\mathcal{R} = \langle R, \gamma_0 \rangle$, where R is a set of function requirements and γ_0 is an *initial condition* represented as a consistent conjunction of literals in $\mathcal{P}$. □

In this paper, state transition systems are considered as formal specifications. A *state transition system* is a quadruple $M = \langle Q, \Sigma, \rightarrow, q_0 \rangle$, where Q is a set of *states*, Σ is a set of input symbols, $\rightarrow$ is a *transition relation* defined as $\rightarrow \subset Q \times \Sigma \times Q$, and q_0 is an *initial state*.

3. Soundness and Completeness

A state transition $t = \langle p \stackrel{a}{\rightarrow} q \rangle$ *satisfies* (is *correct w.r.t.*) a function requirement $\rho : f_{in} \stackrel{b}{\Rightarrow} f_{out}$, denoted as $t \models \rho$, if the following conditions hold:

(1) $p \models f_{in}$, $a = b$, and $q \models f_{out}$.
(2) The partial interpretations $I(p)$ and $I(q)$ are identical if atomic propositions independent of f_{out} are only concerned. □

The condition (1) means the precondition and the postcondition must hold in the current state and the next state, respectively. The condition (2) states that for an atomic proposition A independent of f_{out}, $p \models A \iff q \models A$. This means that the truth value of independent atomic propositions *w.r.t.* the postcondition remain unchanged

*Atsushi Togashi, Fumiaki Kanezashi, Xiaosong Lu, Department of Computer Science, Faculty of Information, Shizuoka University, 3-5-1 Johoku, Hamamatsu, 432, Japan

through the transition.

A state transition system $M = \langle Q, \Sigma, \rightarrow, q_0 \rangle$ is *sound* with respect to a requirement description $\mathcal{R} = \langle R, \gamma_0 \rangle$ if the following conditions are satisfied:

(1) $I(q_0) = I(\gamma_0)$;
(2) for any transition t in M there exists a function requirement $\rho \in R$ such that $t \models \rho$. □

The transition systems M_1 and M_2 are sound with respect to the requirement description $\mathcal{R}_1$ and $\mathcal{R}_2$, respectively. Let $M = \langle Q, \Sigma, \rightarrow, q_0 \rangle$,, $M' = \langle Q', \Sigma, \rightarrow', q_0' \rangle$ be state transition systems in common input symbols. A *homomorphism* from M into M' is a mapping $\xi : Q \rightarrow Q'$ such that

(1) $\xi(q_0) = q_0'$.
(2) if $p \xrightarrow{a} q$ in M, then $\xi(p) \xrightarrow{a} \xi(q)$ in M'.
(3) $p \models f$ implies $\xi(p) \models f$ for all states p in M and propositions f. □

If a homomorphism $\xi : M \rightarrow M'$ is a bijection and the inverse function ξ^{-1} is a homomorphism from M' to M, then ξ is called an *isomorphism.* If there is an isomorphism from M to M', then M and M' are *isomorphic.* Let M be a sound state transition system with respect to $\mathcal{R}$. M is called *complete* with respect to $\mathcal{R}$ if, there is a homomorphism $\xi : M' \rightarrow M$ for every sound state transition system M' with respect to $\mathcal{R}$. A sound and complete transition system with respect to $\mathcal{R}$ is called a *standard system* (*model*) of $\mathcal{R}$.

Theorem Let M, M' be standard systems of $\mathcal{R}$, then M and M' are isomorphic [?]. □

Let $M(\mathcal{R})$ denote a unique standard system of $\mathcal{R}$ up to isomorphism.

4. Synthesis of Specification

Our target is to derive a sound and complete state transition system M from a given requirement description $\mathcal{R} = \langle R, \gamma_0 \rangle$. Now, we state a transformation $\mathcal{T}$ from $\mathcal{R}$ into M. Let define a transition system $\mathcal{T}(\mathcal{R}) = \langle \Gamma, \Sigma, \rightarrow, q_0 \rangle$, where

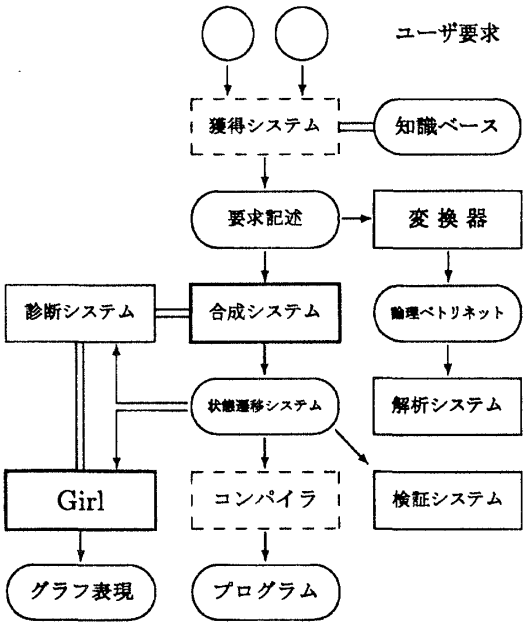
(1) Γ is a consistent conjunction of literals in $\mathcal{P}$
(2) $\Sigma = \{a \mid \rho : f_{in} \overset{a}{\Rightarrow} f_{out} \in R\}$
(3) $\gamma \xrightarrow{a} \gamma'$ iff there exists a function requirement $\rho : f_{in} \overset{a}{\Rightarrow} f_{out} \in R$ such that
   (a) $I(\gamma) \models f_{in}$.
   (b) $I(\gamma') \models f_{out}$.
   (c) If an atomic proposition A is independent of f_{out}, then $I(\gamma) \models A$ iff $I(\gamma') \models A$.
(4) $q_o = \gamma_0$.

The partial interpretation associated with a state γ in $\mathcal{T}(\mathcal{R})$ is defined as $I(\gamma)$. In other words, the states correspond possible partial interpretations for all atomic propositions in $\mathcal{P}$. It is trivial from the construction that $\mathcal{T}(\mathcal{R})$ is irreducible.

Theorem The state transition system $\mathcal{T}(\mathcal{R})$ derived from a requirement description $\mathcal{R} = \langle R, \gamma_0 \rangle$ by $\mathcal{T}$ is a standard system of $\mathcal{R}$.

5. Environment

An effective environment for software development is given as follows:



6. Conclusion

A formal methodology for the description of system requirements and the synthesis of formal specifications from user requirements have been presented.

参考文献

[1] Song, K., Togashi, A., Shiratori, N., Verification and refinement for system requirements, IEICE Trans. on Fundamentals of Elec., Comm. and Comp. Sci., Vol.E78-A, No.11, pp.1468–1478, 1995.

[2] Song, K., Togashi, A., Shiratori, N., A requirement description method based on propositional logic and its semantic description by state transition system, Trans. of Information Processing Society of Japan, Vol.37, No.4, pp.511–519, 1996 (in Japanese).

[3] Togashi, A., Usui, N., Song, K., Shiratori, N. A derivation of System Specifications based on a Partial Logical Petri Net, Proc. of ISCAS95, 1995.