



UNIVERSIDAD DE BUENOS AIRES

FACULTAD DE CIENCIAS EXACTAS Y NATURALES

DEPARTAMENTO DE COMPUTACIÓN

Síntesis de Controladores Actualizables Dinámicamente: Herramienta MTSA

Tesis presentada para optar al título de
Licenciado en Ciencias de la Computación

Leandro Ezequiel Nahabedian

Director: Nicolás Roque D'Ippolito

Buenos Aires, Argentina 2014

SÍNTESIS DE CONTROLADORES ACTUALIZABLES DINÁMICAMENTE

Es esperado que muchos sistemas corran continuamente mientras el ambiente cambia y los requerimientos evolucionan, por lo tanto las implementaciones de dichos sistemas deben ser actualizados dinámicamente para satisfacer los cambios de requerimientos, respetando los cambios del ambiente. Lo complejo de este paso, es poder determinar en que puntos de la ejecución previa es seguro hacer la actualización, y si es seguro, como deberá seguir ejecutando el nuevo sistema. Tanto la máquina, como el ambiente y los requerimientos, pueden ser interpretados por modelos de comportamiento que son estructuras formales que definen acciones que pueden suceder. Mediante la síntesis de controladores podremos obtener modelos de forma correcta debido a que son obtenidos mediante construcciones.

El enfoque de esta tesis es definir y plantear formalmente mediante síntesis de controladores el problema de la actualización dinámica, detallando un conjunto de inputs necesarios para la solución del mismo. A su vez, desarrollaremos varios casos de test utilizando la herramienta MTSA (Modal Transition System Analyser) dejando constancia de que los inputs definidos son suficientes para obtener el controlador buscado.

Palabras claves: *Ingeniería de requerimientos; Síntesis de controladores; Actualización dinámica; Especificación basada en eventos; MTSA framework; Concurrencia, LTS; Fluent; LTL.*

AGRADECIMIENTOS

Quiero aprovechar este espacio para agradecer

A mi familia con todo mi amor.

Índice general

1..	Introducción	1
1.1.	Motivación	1
1.2.	Resumen de la contribución	2
1.3.	Esquema de tesis	3
2..	Fundamentos teóricos	5
2.1.	El Mundo y la Máquina	5
2.2.	Sistema de Transición Etiquetados (Labelled Transition System)	7
2.3.	Lógica Lineal Temporal de Flujos (Fluent Linear Temporal Logic)	8
2.4.	Problemas de síntesis de controladores	9
2.5.	Juegos de dos jugadores	10
2.6.	Procesos de estados Finitos (Finite State Process)	11
3..	MTSA como herramienta de modelado y síntesis	13
4..	Problema de actualización de controladores dinámicamente	15
5..	Validando los algoritmos	17
5.1.	Casos de Estudio	17
5.2.	Resultados	17
6..	Conclusiones y trabajos futuros	19
6.1.	Conclusiones	19
6.2.	Trabajo futuro	19

1. INTRODUCCIÓN

1.1. Motivación

Cuando trabajamos en ingeniería de requerimientos, nuestra tarea es relevar y documentar los objetivos y el funcionamiento del ambiente, para elaborar un conjunto de requerimientos cuya máquina a construir debe cumplir. Teniendo estas tres componentes, podemos formular la siguiente ecuación: $R, D \models G$. Donde R son los Requerimientos de la máquina, D las asunciones del dominio y G los objetivos que la máquina deberá satisfacer.

Entonces, un problema clave de la ingeniería de requerimientos puede ser visto como un problema de síntesis, tal que dado un modelo de la máquina, un modelo del mundo y un conjunto de objetivos del sistema, permite construir un modelo operacional el cual satisface los objetivos. La técnica que resuelve esta ecuación mediante los modelos mencionados es llamada síntesis de controladores y esta siendo estudiada exhaustivamente en varios aspectos de la ingeniería de los requerimientos.

La construcción de dichos modelos son una de las principales herramientas en el diseño de sistemas concurrentes, debido a que nos facilita la detección de errores de diseño en las primeras etapas de desarrollo. Por otro lado, estos modelos de comportamiento pueden resultar complejos de construir. Utilizar la técnica de síntesis anteriormente mencionada facilita la construcción tomando modelos pequeños y propiedades lógicas, que suelen ser más sencillas de especificar y de validar.

Por lo tanto, un problema de control consiste en generar automáticamente una máquina que restrinja la ocurrencia de eventos controlables basado en los eventos del mundo que se producen. Es decir, teniendo la especificación de un ambiente, asunciones, objetivos y un conjunto de acciones controlables, podemos definir una máquina cuyo comportamiento concurrente con el ambiente satisfaga las asunciones y los objetivos del sistema.

Este problema está siendo ampliamente estudiado en diferentes contextos, desde sistemas autoadaptativos hasta composición automática de web-services. Para diseñar softwa-

res autoadaptativos los más evolucionados fueron los basados en arquitectura y los basados en requerimientos. El primero de estos utiliza reglas de adaptación que serán utilizadas para monitorear condiciones del conjunto de operaciones del sistema y definir acciones en run-time si las condiciones son desfavorables. Por otro lado, los basados en requerimientos extienden las técnicas de ingeniería de los requerimientos con el fin de representar a los requisitos de adaptación y/o la incertidumbre inherente del medio ambiente en el que opera el sistema. El modelo más utilizado en la comunidad, hoy en día, para definir sistemas autoadaptables es el modelo arquitectural.

Actualmente, trabajos recientes en el área de sistemas auto adaptativos definen una técnica para lograr encontrar estados de la ejecución del controlador en los cuales es seguro realizar una actualización y seguir ejecutando el nuevo controlador sin tener que apagar y prender el primero. Sin embargo, dicho problema no ha sido estudiado en el marco de síntesis de controladores.

1.2. Resumen de la contribución

Trabajos previos en el área de ingeniería de los requerimientos han estudiado la utilidad de diversas técnicas de sistemas adaptativos, debido a la necesidad de cambiar el ambiente o los requerimientos de un sistema sin frenar o interrumpir su ejecución.

La contribución central de esta tesis es la presentación de una técnica que produce la actualización automática de sistemas. Dicha técnica, propone mejorar ciertos problemas que las anteriores estrategias padecían, como la necesidad de conocer estados de la ejecución en los cuales es "seguro" actualizar, y si lo es, detectaremos cual es el estado equivalente en el sistema actualizado. Detallaremos en el capítulo BLA por qué y cómo resolvemos dichas complicaciones.

Por otro lado, lo novedoso del trabajo presentado es el enfoque usado. La actualización automática de sistemas ha sido estudiado en diversos enfoques pero no bajo el marco de síntesis de controladores. Al presentar dicha técnica bajo un marco no explorado abrimos a la comunidad científica un nuevo paradigma que podría potencialmente solucionar problemas en otras áreas relacionadas con la ingeniería de los requerimientos.

1.3. Esquema de tesis

2. FUNDAMENTOS TEÓRICOS

2.1. El Mundo y la Máquina

Los primeros conceptos que detallaré estarán involucrados con la ingeniería de los requerimientos. Los puntos de vista mas relevantes son los de Zave y Jackson ([11, 2, 3]) por un lado, y los de Letier y Van Lamsweerde ([10, 8]) por el otro. Ambos puntos de vista distinguen a los problemas del *Mundo* y las soluciones de la *Máquina* como fundamentales para reconocer si las operaciones de la máquina solucionan los problemas planteados en el mundo. De hecho, el efecto de la máquina en el mundo y las suposiciones que hacemos acerca de este mundo son fundamentales para el proceso de toma de requerimientos. En el lado del mundo definimos una serie de problemas que existen en el mundo real que serán solucionados al construir una máquina. Fácilmente podremos notar que existen componentes en la máquina que interactúan directamente con el mundo siguiendo normas y procesos conocidos. Estas, forman parte de la intersección entre el mundo y la máquina. Por ejemplo un taladro, un brazo robótico o las reglas de procesamiento para cada elemento que entra en una linea de producción (véase la Fig. 2.1).

Así mismo, es esperado que la máquina proponga una solución al problema. Por ejemplo, en la Fig. 2.1 podemos ver que la célula de producción debe procesar cada producto, solo si están disponible en la bandeja de entrada en ese momento. Con la senten-

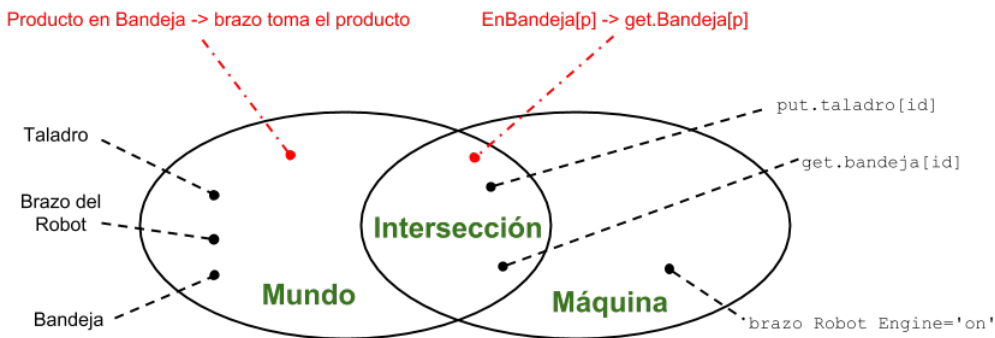


Fig. 2.1: El Mundo y la Máquina

cia $EnBandeja[p] \rightarrow get.Bandeja[p]$ muestro que se espera que el brazo del robot solo podrá tomar los productos de la bandeja cuando estén listos. Finalizando, los fenómenos compartidos entre el mundo y máquina, es decir, los que se encuentran en la intersección, representa a la *interfaz*, donde la máquina interactúa con el mundo. También, podemos definir a los fenómenos del mundo como el *modelo del entorno* ya que el conjunto de estos describen los eventos que suceden en el mundo real.

Las sentencias que detallan los distintos fenómenos, tanto en el mundo como en la máquina pueden variar en *alcance* y en *forma* [7, 2]. Además, estas pueden estar en modo *indicativo* u *optativo*. En otros trabajos, como en [9], las sentencias utilizadas son *descriptivas* y *prescriptivas*.

- Sentencias descriptivas: representan propiedades que son independientes de cómo se comporta el sistema. Se usan en modo *indicativo*. No pueden ser cambiadas ni removidas.
- Sentencia prescriptivas: afirman propiedades deseables que pueden estar presentes o no. Deben estar aplicadas por los componentes del sistema. Normalmente, pueden cambiar fortaleciéndose o debilitándose, o incluso pueden ser eliminadas.

Anteriormente, fue mencionado que los estados pueden variar en su alcance. Ambos tipos de sentencias pueden referirse a características de la máquina que no son compartidas por el mundo. En otras ocasiones, sentencias pueden referirse a fenómenos compartidos por el mundo y la máquina. Más precisamente, una *propiedad de dominio* es una sentencia descriptiva sobre el mundo. Durante todo este trabajo, vamos a llamar *modelo ambiente*, al conjunto de propiedades del dominio de un problema particular.

Por otro lado, un *supuesto de ambiente* es una sentencia que podría no suceder y debe ser satisfecha por el ambiente. Un requisito de software, o *requisito* de forma abreviada, es una sentencia prescriptiva que la máquina deberá satisfacer independientemente de cómo se comporta el problema detallado en el mundo y deben ser elaboradas en términos de fenómenos compartidos entre el mundo y la máquina.

Para finalizar y siguiendo lo publicado en [8, 10] podremos determinar a una acción como supervisada / controlable si dicha acción es supervisada / controlable por la máquina. En este trabajo, llamaremos a las acciones supervisadas como acciones no controlables, ya

que están controladas por el ambiente.

2.2. Sistema de Transición Etiquetados (Labelled Transition System)

En esta sección vamos a dar una notación para los sistemas de transiciones etiquetados o Labelled Transition System (LTS), la cual usaremos durante este trabajo. Dichos sistemas, son muy usados actualmente para modelar y analizar comportamiento en sistemas concurrentes y distribuidos. Un LTS es un sistema de transiciones de estados donde cada una de ellas esta etiquetada con una acción. El conjunto de todas las acciones que posee un LTS es llamado alfabeto.

Definición 2.2.1. *(Sistema de Transición Etiquetado)[5] Sea States un conjunto universal de estados, Act un conjunto universal de etiquetas. Un Sistema de Transición Etiquetado (LTS) es una tupla $E = (S_E, A_E, \Delta_E, s_{E_0})$, donde $S_E \subseteq \text{States}$ es un conjunto finito de estados, $A_E \subseteq \text{Act}$ es un alfabeto finito, $\Delta_E \subseteq (S_E \times A_E \times S_E)$ es una relación, y $s_0 \in S_E$ es el estado inicial.*

Si $(s, l, s') \in \Delta_E$ diremos que l está activo desde s en E . Diremos también que un LTS E es *determinístico* si $\forall_{(s,l,s'),(s,l,s'') \in \Delta_E}$ implica $s' = s''$. Para un estado s definiremos $\Delta_E(s) = \{l \mid (s, l, s') \in \Delta_E\}$. Dado un LTS E , vamos a referirnos a su alfabeto como αE .

Definición 2.2.2. *(Composición en Paralelo) Sean $M = (S_M, A_M, \Delta_M, s_{M_0})$ y $E = (S_E, A_E, \Delta_E, s_{E_0})$ LTSs. Una Composición en Paralelo(\parallel) es un operador simétrico tal que $E \parallel M$ es el LTS definido de la siguiente manera $E \parallel M = (S_E \times S_M, A_E \cup A_M, \Delta, (s_{E_0}, s_{M_0}))$, donde Δ es la relación mas pequeña que satisface las siguientes reglas, donde $l \in A_E \cup A_M$:*

ESCRIBIR GARCHA DE LOGICA

Definición 2.2.3. *(LTS Legal) Dado $E = (S_E, A_E, \Delta_E, s_{E_0})$, $M = (S_M, A_M, \Delta_M, s_{M_0})$ LTSs, y $A_{E_u} \in A_E$. Decimos que M es un LTS Legal par E con respecto a A_{E_u} si para todos $(s_E, s_M) \in E \parallel M$ sucede lo siguiente: $\Delta_{E \parallel M}((s_E, s_M)) \cap A_{E_u} = \Delta_E(s_E) \cap A_{E_u}$.*

Intuitivamente, un LTS M es un LTS *Legal* para el LTS E con respecto a A_{E_u} , si para todos los estados en la composición $(s_E, s_M) \in S_{E \parallel M}$ se cumple que, una acción $l \in A_{E_u}$ es deshabilitada en (s_E, s_M) si y solo si también esta deshabilitada en $s_E \in E$. En otras palabras, M no restringe a E con respecto a A_{E_u} .

Definición 2.2.4. (*Tranzas*) Sea un LTS $E = (S, A, \Delta, s_0)$. Una secuencia $\pi = l_0, l_1, \dots$ es una traza en E si existe una secuencia $s_0, l_0, s_1, l_1, \dots$ donde para todo i tenemos $(s_i, l_i, s_{i+1}) \in \Delta$.

Definición 2.2.5. (*Estados Alcanzables*) Sea un LTS $E = (S_E, A_E, \Delta_E, s_0)$. Un estado $s \in S_E$ es alcanzable (desde el estado inicial) en E si existe una secuencia $s_0, l_0, s_1, l_1, \dots$ donde para cada i tenemos $(s_i, l_i, s_{i+1}) \in \Delta$ y $s = s_{i+1}$. Nos referimos a el conjunto de todos los estados alcanzables en E como $\text{Reach}(E)$.

En el transcurso de esta tesis, vamos a estudiar solo aquellos LTSs E donde todos sus estados $s \in S_E$ son alcanzables.

2.3. Lógica Lineal Temporal de Flujos (Fluent Linear Temporal Logic)

La Lógica Lineal Temporal (LTL) esta siendo ampliamente usada en la ingeniería de los requerimientos [4, 1, 10, 6]. La motivación para escoger a las LTL de flujos es que estas proveen un framework uniforme para especificar propiedades basados en estados sobre modelos basados en eventos [1]. Fluent Linear Temporal Logic (FLTL) [1] es una lógica de tiempo lineal, temporal, para razonar acerca de flujos. Un *flujo* Fl es definido por un par de conjuntos y un valor booleano: $Fl = \langle I_{Fl}, T_{Fl}, \text{Init}_{Fl} \rangle$, donde $I_{Fl} \subseteq \text{Act}$ es el conjunto de acciones iniciadoras, $T_{Fl} \subseteq \text{Act}$ es el conjunto de acciones finalizadoras y $I_{Fl} \cap T_{Fl} = \emptyset$. Un flujo puede ser inicializado con valor true o false indicado por Init_{Fl} . Toda acción $l \in \text{Act}$ induce un flujo, que notaremos $\hat{l} = \langle l, \text{Act} \setminus \{l\}, \text{false} \rangle$. Por último, el alfabeto de un flujo es el que se obtiene mediante la unión del conjunto de acciones iniciadoras y el conjunto de acciones finalizadoras.

Sea \mathcal{F} el conjunto de todas las posibles flujos sobre Act . Una formula FLTL esta se define inductivamente utilizando los conectores booleanos estandar y operadores temporales como el **X** (próximo), **U** (antes fuerte) de la siguiente manera:

$$\varphi ::= Fl \mid \neg\varphi \mid \varphi \vee \psi \mid \mathbf{X}\varphi \mid \varphi \mathbf{U} \psi$$

donde $Fl \in \mathcal{F}$. Para comodidad sintáctica, vamos a introducir las operaciones de \wedge , \diamond (eventualmente) y \square (siempre). Sea Π el conjunto de trazas infinitas sobre Act , diremos que la traza $\pi = l_0, l_1, \dots$ satisface un flujo Fl en la posición i , notado $\pi, i \models Fl$, si y solo

si una de las siguientes condiciones es válida:

- $Init_{Fl} \wedge (\forall j \in \mathbb{N} : 0 \leq j \leq i \rightarrow l_k \notin T_{Fl})$
- $\exists j \in \mathbb{N} : (j \leq i \wedge l_j \in I_{Fl}) \wedge (\forall k \in \mathbb{N} : j < k \leq i \rightarrow l_k \notin T_{Fl})$

Dada una traza infinita π , la fórmula que satisface φ en la posición i , denotada como $\pi, i \models \varphi$, es definida a continuación como se muestra en la semántica para el operador de satisfacción:

$$\begin{aligned}
 \pi, i \models Fl & \triangleq \pi, i \models Fl \\
 \pi, i \models \neg \varphi & \triangleq \neg(\pi, i \models \varphi) \\
 \pi, i \models \varphi \vee \psi & \triangleq (\pi, i \models \varphi) \vee (\pi, i \models \psi) \\
 \pi, i \models \mathbf{X}\varphi & \triangleq \pi, 1 \models \varphi \\
 \pi, i \models \varphi \mathbf{U} \psi & \triangleq \exists j \geq i : \pi, j \models \psi \wedge \forall i \leq k < j : \pi, k \models \varphi
 \end{aligned}$$

Diremos que φ se cumple en π , denotado como $\pi \models \varphi$, si $\pi, 0 \models \varphi$. Una fórmula $\varphi \in \text{FLTL}$ es cierta si un LTS E (denotado como $E \models \varphi$) si éste es cierto en toda traza infinita producida por E .

2.4. Problemas de síntesis de controladores

Los problemas de síntesis de controladores son aquellos que producen una máquina, la cual, restringe las ocurrencias de los eventos controlables, basado en las observaciones, de los eventos no controlables que han ocurrido. Dicha máquina, al ser desplegada con un ambiente adecuando logramos satisfacer el conjunto de objetivos del sistema. Cabe destacar, que estos objetivos se cumplirán si se satisfacen las asunciones que se hacen sobre el ambiente. Resumiendo, tendremos una especificación del ambiente, asunciones, objetivos, y un conjunto de acciones controlables. Resolver el *problema de síntesis de control* es hallar una máquina, que al trabajar concurrentemente con el ambiente, que satisface las asunciones del dominio, satisfacemos el conjunto de objetivos del sistema.

Hecha esta introducción definiremos el problema de síntesis de control para modelos basados en eventos de la siguiente manera. Dada una LTS que detalla el comportamiento del ambiente, un conjunto de eventos controlables, un conjunto de formulas FLTL que describen los objetivos del sistema, el problema de control LTS consiste en encontrar una

LTS que restringe solamente la ocurrencia de acciones controlables y garantiza que la composición paralela del ambiente con la LTS recién descrita estará libre de deadlocks y que, si las presunciones del ambiente valen, satisfecerá también los objetivos del sistema.

Definición 2.4.1. (*Control LTS*) Dada una especificación de un entorno en forma de una LTS E , un conjunto de acciones controlables $A_c \in \text{Act}$ y un conjunto H de pares (A_{s_i}, G_i) donde A_{s_i} y G_i son fórmulas FLTL especificando presunciones y objetivos del sistema respectivamente, la solución al problema de control LTS $\mathcal{E} = \langle E, H, A_c \rangle$ consiste en encontrar una LTS M de forma que M es legal a E sobre el conjunto de acciones no controlables $A_U = \overline{A_c}$, $E || M$ se encuentra libre de deadlocks, y para cada par $(A_{s_i}, G_i) \in H$ y para cada traza π en $E || M$ se cumple que si $\pi \models A_{s_i}$ entonces $\pi \models G_i$.

Ahora pasaremos a definir un subconjunto de problemas de control LTS que esta determinado por aquellos problemas de control que son computables en tiempo polinómico. Identificaremos estos problemas como problemas de control LTS SGR(1) (Safe Generalised Reactivity(1)). Estos se construyen a partir de GR(1) y problemas de seguridad pero en modelos basados en eventos. Dichos problemas, constan de un modelo del ambiente E que será un LTS determinístico para asegurar que el controlador tenga una visión completa de los estados del ambiente. Requerimos que H sea $\{(\emptyset, I), (A_s, G)\}$, donde I es un invariante de seguridad de la pinta $\Box \rho$, las asunciones A_s son una conjunción de sub-fórmulas FLTL de la pinta $\Box \Diamond \phi$, y el objetivo G una conjunción de sub-fórmulas FLTL de la pinta $\Box \Diamond \gamma$ donde ρ, ϕ y γ son combinación booleana de flujos.

Definición 2.4.2. (*Control LTS SGR(1)*) un problema de control LTS $\mathcal{E} = \langle E, H, A_c \rangle$ es SGR(1) si E es determinístico, y $H = \{(\emptyset, I), (A_s, G)\}$, donde $I = \Box \rho$, $A_s = \bigwedge_{i=1}^n \Box \Diamond \phi_i$, $G = \bigwedge_{j=1}^m \Box \Diamond \gamma_j$, y ϕ_i, ρ y γ_j son combinación booleana de flujos.

2.5. Juegos de dos jugadores

Llamaremos juegos de dos jugadores a aquellos que consisten en dos jugadores, jugador 1 y jugador 2, donde el objetivo del jugador 1 es satisfacer una especificación independientemente de las acciones que el jugador 2 ejecute.

2.6. Procesos de estados Finitos (Finite State Process)

3. MTSA COMO HERRAMIENTA DE MODELADO Y SÍNTESIS

4. PROBLEMA DE ACTUALIZACIÓN DE CONTROLADORES DINÁMICAMENTE

5. VALIDANDO LOS ALGORITMOS

5.1. Casos de Estudio

5.2. Resultados

6. CONCLUSIONES Y TRABAJOS FUTUROS

6.1. Conclusiones

6.2. Trabajo futuro

Bibliografía

- [1] D. Giannakopoulou and J. Magee. Fluent model checking for event-based systems. In *Proceedings of the 9th European Software Engineering Conference Held Jointly with 11th ACM SIGSOFT International Symposium on Foundations of Software Engineering*, ESEC/FSE-11, pages 257–266, New York, NY, USA, 2003. ACM.
- [2] M. Jackson. *Software Requirements & Specifications: A Lexicon of Practice, Principles and Prejudices*. ACM Press/Addison-Wesley Publishing Co., New York, NY, USA, 1995.
- [3] M. Jackson. The world and the machine. In *Software Engineering, 1995. ICSE 1995. 17th International Conference on*, pages 283–283, April 1995.
- [4] R. Kazhamiakin, M. Pistore, and M. Roveri. Formal verification of requirements using spin: a case study on web services. In *Software Engineering and Formal Methods, 2004. SEFM 2004. Proceedings of the Second International Conference on*, pages 406–415, Sept 2004.
- [5] R. M. Keller. Formal verification of parallel programs. *Commun. ACM*, 19(7):371–384, July 1976.
- [6] E. Letier and A. van Lamsweerde. Agent-based tactics for goal-oriented requirements elaboration. In *Proceedings of the 24th International Conference on Software Engineering*, ICSE '02, pages 83–93, New York, NY, USA, 2002. ACM.
- [7] D. L. Parnas and J. Madey. Functional documents for computer systems. *Science of Computer Programming*, 25:41–61, 1995.
- [8] A. Van Lamsweerde. Goal-oriented requirements engineering: A guided tour. In *Proceedings of the Fifth IEEE International Symposium on Requirements Engineering*, RE '01, pages 249–, Washington, DC, USA, 2001. IEEE Computer Society.
- [9] A. van Lamsweerde. *Requirements Engineering: From System Goals to UML Models to Software Specifications*. Wiley, 2009.

- [10] A. Van Lamsweerde and E. Letier. Handling obstacles in goal-oriented requirements engineering. *Software Engineering, IEEE Transactions on*, 26(10):978–1005, Oct 2000.
- [11] P. Zave and M. Jackson. Four dark corners of requirements engineering. *ACM Transactions on Software Engineering and Methodology*, 6:1–30, 1997.