

Curso: Model checking probabilista

Docente: Pedro R. D'Argenio

Resumen

Los sistemas concurrentes de estados finitos aparecen naturalmente en varias áreas de las Ciencias de la Computación, particularmente en el diseño de circuitos digitales y protocolos de comunicación. Los errores lógicos encontrados tarde en la fase de diseño de estos sistemas son un problema extremadamente importante ya que pueden ocasionar retrasos en la liberación de un nuevo producto o causar fallas de dispositivos de sistemas críticos en funcionamiento.

Los algoritmos aleatorios concurrentes y/o distribuidos, en particular, presentan, muchas veces, soluciones más veloces que los algoritmos tradicionales y, en otros casos, soluciones que no serían posible dentro del dominio de los algoritmos tradicionales. Como ejemplo tenemos los protocolos de elección de líder o los de acuerdo bizantino donde la componente no-determinista se mezcla con la aleatoria. Otro factor que contribuye a la aleatoriedad del sistema es el entorno o medio con el cual las distintas componentes del programa deben interactuar. Este factor se presentaría en situaciones tales como la pérdida de un mensaje en la red, la falla de una componente de un sistema, o la disponibilidad de un recurso.

El hecho de considerar probabilidades dentro del comportamiento de los sistemas implica que el conjunto de propiedades asociadas a estos sistemas se sale de la lógica usual. Un ejemplo característico en este sentido se presenta en protocolos con retransmisión limitada donde es imposible establecer que todo mensaje enviado se recibe. A cambio uno podría analizar la validez de lo siguiente: "todo mensaje enviado se recibe con probabilidad 0.99". A este tipo de propiedades se las denomina propiedades cuantitativas.

Model checking es una técnica de verificación que, dado el modelo del sistema bajo estudio y la propiedad requerida, permite decidir automáticamente si la propiedad es satisfecha o no. Las técnicas de model checking sobre programas probabilísticos concurrentes comenzaron a estudiarse a mediados de los 80 pero el análisis cuantitativo se impuso recién hacia finales de los 90. Basado en estas técnicas, se han desarrollado una diversidad de algoritmos y herramientas.

En esta materia se estudiarán los fundamentos del model checking probabilista así como las técnicas, algoritmos y fundamentos de las herramientas que lo implementan.

Contenido

- (I) **Conceptos básicos de teoría de la medida:** (1) σ -álgebras y σ -álgebras generadas. (2) Semi-anillos y anillos. (3) Medida y medida de probabilidad. (4) Extensión de Caratheodory. (5) Funciones medibles. (6) Espacios de medida productos y espacios de medida sobre secuencias infinitas.
- (II) **Lenguajes ω -regulares:** (1) Definición. (2) Autómatas de Büchi. (3) Autómatas de Rabin. (4) Determinización de autómatas de Rabin. (5) Equivalencia entre los lenguajes ω -regulares y los lenguajes inducidos por los autómatas de Büchi y los autómatas de Rabin. (6) Medibilidad de los lenguajes ω -regulares.
- (III) **Lógica temporal lineal (LTL):** (1) Sintaxis. (2) Semántica. (3) Traducción a un autómata de Rabin determinista.

- (IV) **Cadenas de Markov de tiempo discreto (DTMC):** (1) Definición. (2) Espacio de probabilidades inducido por una DTMC. (3) Verificación de propiedades de alcanzabilidad. (4) Verificación de propiedades cualitativas. (5) Verificación de propiedades LTL. (6) Métodos de solución iterativo.
- (V) **Lógicas sobre árboles computacionales – PCTL y PCTL*:** (1) Sintaxis y semántica de PCTL. (2) Verificación de propiedades PCTL. (3) El fragmento cualitativo de PCTL y la lógica CTL. (4) Sintaxis y semántica de PCTL*. (5) Verificación de propiedades PCTL*.
- (VI) ^(†)**Modelos de Markov con recompensa:** (1) Definición. (2) Alcanzabilidad con costo acotado. (3) La lógica PRCTL: sintaxis y semántica. (4) Propiedades de ejecuciones largas (estado estable). (5) Verificación de propiedades PRCTL.
- (VII) **Procesos de decisión de Markov (MDP):** (1) Definición. (2) Estrategias (*schedulers*). (3) Tipos de estrategias. (4) Semántica de LTL, PCTL y PCTL* en MDP. (5) Verificación de propiedades de alcanzabilidad. (6) Existencia de la estrategia óptima. (7) Reducción del problema de model checking a un problema de programación lineal. (8) Análisis cualitativo. (9) Verificación de propiedades LTL, PCTL y PCTL* sobre MDP. (10) Fairness. (11) Métodos de solución iterativos.
- (VIII) **Diagramas de decisión binaria con terminales múltiples (MTBDD):** (1) Definición de BDD y MTBDD. (2) Operaciones. (3) Representación de vectores y matrices. (4) Representación de DTMC. (5) Representación de MDP. (6) Construcción y alcanzabilidad.
- (IX) **Model checking utilizando MTBDD:** (1) El algoritmo principal. (2) Algoritmos de precómputo. (3) Cómputo numérico. (4) El operador *until* en DTMC. (5) El operador *until* en MDP. (6) Otros operadores.
- (X) **Model checking utilizando técnicas híbridas:** (1) Interconexión entre MTBDD y arreglos. (2) El proceso de construcción. (3) Optimizaciones. (4) Extensión sobre MDP.
- (XI) ^(†)**Otras técnicas asociadas al model checking probabilista:** (1) Técnicas de reducción de espacio de estado I: Abstracción y refinamiento basado en simulación. (2) Técnicas de reducción de espacio de estado II: Abstracción y refinamiento basado en teoría de juegos. (3) Técnicas de reducción de espacio de estado III: Reducción de orden parcial. (4) Derivación de contraejemplos. (5) Model checking de sistemas probabilistas con observación parcial: Indecibilidad en sistemas de estados finitos y algoritmos para propiedades de tiempo acotado.

El dictado de las unidades indicadas con ^(†) está sujeto a la disponibilidad de tiempo.

Modalidad del dictado y carga horaria

El curso comprende 60 horas de dictado del teórico de la materia. El curso comprenderá también la realización de diversos trabajos prácticos complementarios al teórico. Los alumnos deberán invertir horas de estudio de manera independiente aparte de las horas del dictado de clases para la realización de dichos trabajos prácticos. El curso se evaluará mediante la realización de diversos ejercicios en la modalidad “*take-home*”.

Bibliografia

- [1] Christel Baier and Joost-Pieter Katoen. *Principles of Model Checking*. MIT press, 2008.
- [2] David Parker. *Implementation of Symbolic Model Checking for Probabilistic Systems*. PhD thesis, University of Birmingham, 2002.
- [3] Noel Valiant. *Probability Tutorials*. www.probability.net, 1999.
- [4] P. Billingsley. *Probability and Measure*. Wiley-Interscience, 1995.
- [5] Martin L. Puterman. *Markov Decision Processes: Discrete Stochastic Dynamic Programming*. Wiley, 2005.
- [6] D.J. White. *Markov Decision*. Wiley, 1993.
- [7] Michael Huth and Mark Ryan. *Logic in Computer Science: Modelling and Reasoning about Systems (2nd ed)*. Cambridge University Press, 2004.
- [8] Andrea Bianco, Luca de Alfaro. Model checking of probabilistic and nondeterministic systems. In *Procs. of FST&TCS'95*, volume 1026 of *LNCS*, pages 499–513. Springer, 1995.
- [9] C. Baier and M. Kwiatkowska. Model checking for a probabilistic branching time logic with fairness. *Distr. Computing*, 11(3):125–155, 1998.
- [10] M.Y. Vardi. Automatic verification of probabilistic concurrent finite state programs. In *26th Annual Symposium on Foundations of Computer Science*, pages 327–338. IEEE press, 1985.
- [11] C. Courcoubetis and M. Yannakakis. Verifying temporal properties of finite-state probabilistic processes. In *Procs. of 29th Annual Symposium on Foundations of Computer Science*, pages 338–345. IEEE press, 1988.
- [12] Pedro R. D’Argenio, Bertrand Jeannet, Henrik E. Jensen, and Kim G. Larsen. Reachability analysis of probabilistic systems by successive refinements. In *Proc. of PAPM/PROBMIV 2001*, volume 2165 of *LNCS*, pages 39–56. Springer, 2001.
- [13] Marta Z. Kwiatkowska, Gethin Norman, and David Parker. Game-based Abstraction for Markov Decision Processes. In *QEST 2006*, pages 157–166. IEEE Computer Society, 2006.
- [14] Christel Baier, Marcus Größer, and Frank Ciesinski. Partial order reduction for probabilistic systems. In *QEST '04*, pages 230–239. IEEE CS, 2004.
- [15] Pedro R. D’Argenio and Peter Niebert. Partial order reduction on concurrent probabilistic programs. In *QEST '04*, pages 240–249. IEEE CS, 2004.
- [16] Christel Baier, Pedro R. D’Argenio, and Marcus Größer. Partial Order Reduction for Probabilistic Branching Time. *Electr. Notes Theor. Comput. Sci.* 153(2):97–116. 2006.
- [17] T. Han and J.-P. Katoen. Counterexamples in probabilistic model checking. In *Proceedings of TACAS '07*, volume 4424 of *LNCS*, pages 60–75. Springer, 2007.

- [18] B. Damman, T. Han, and J.-P. Katoen. Regular expressions for PCTL counterexamples. in quantitative evaluation of systems. In *Proceedings of QEST '08*. IEEE press, 2008.
- [19] M. Andrés, P.R. D'Argenio, and P. van Rossum. Significant diagnostic counterexamples in probabilistic model checking. In *Haifa Verification Conference*. LNCS 5394, pages 129/-148. Springer, 2009.
- [20] S. Giro and P.R. D'Argenio. Quantitative model checking revisited: neither decidable nor approximable. In *FORMATS'07*, LNCS 4763, pages 179–194. Springer, 2007.
- [21] S. Giro and P.R. D'Argenio. On the expressive power of schedulers in distributed probabilistic systems. In *Proc. of QAPL 2009*. York, UK, March 28-29 2009. Extended version available at cs.famaf.unc.edu.ar/~sgiro/QAPL09-ext.pdf.
- [22] Sergio Giro. Undecidability Results for Distributed Probabilistic Systems. In *SBMF 2009*, LNCS 5902, pages 220–235. Springer, 2009.
- [23] Georget Calin, Pepijn Crouzen, Pedro R. D'Argenio, Ernst Moritz Hahn, and Lijun Zhang. Time-Bounded Reachability in Distributed Input/Output Interactive Probabilistic Chains. In *Procs. of SPIN Workshop 2010*. LNCS 6349, pages 193–211. Springer, 2010.