Simulación en estado transitorio de sistemas altamente confiables [†]

Héctor Cancela Bosi
cancela@fing.edu.uy
Investigación Operativa, InCo - Pedeciba Informática
Facultad de Ingeniería, Universidad de la República
Montevideo, Uruguay

Reporte Técnico INCO 98.04

23 Abril 1998

Resumen

La evaluación de medidas de seguridad de funcionamiento es un aspecto importante dentro del diseño de sistemas informáticos y de comunicaciones complejos. Una de las herramientas más flexibles es el modelado a través de cadenas de Markov, que permiten la representación del comportamiento dinámico y la interacción entre los distintos componentes de un sistema.

Este trabajo se concentra en la evaluación por simulación (Monte Carlo) de la confiabilidad instantánea R_t de estos sistemas, y presenta un método basado en técnicas de reducción recursiva de la varianza que garantiza mayor eficiencia respecto al método Monte Carlo estándar.

1 Introducción

En la actualidad, el modelado y la evaluación de medidas de seguridad de funcionamiento es un aspecto importante dentro del diseño de sistemas informáticos y de comunicaciones complejos. Una de las herramientas más

[†]Este trabajo fue financiado por la Acción U93E03 del Programa ECOS de Cooperación Científica Francia-Uruguay, y por el CONICYT y la CSIC (Uruguay).

flexibles es el modelado a través de cadenas de Markov, que permiten la representación del comportamiento dinámico y la interacción entre los distintos componentes de un sistema [1, 13]. Cuando el sistema es pequeño, es posible también evaluar analíticamente las medidas de interés; pero a medida que el número de componentes crece, los métodos analíticos dejan de ser factibles, debido al incremento exponencial del tiempo de cálculo.

Una alternativa es el empleo de técnicas de simulación Monte Carlo, que proporcionan estimaciones (con un cierto intervalo de confianza) de las medidas de seguridad de funcionamiento. El método Monte Carlo estándar (o "crudo") también sufre de inconvenientes cuando los eventos de interés son raros (ocurren con muy baja probabilidad), lo que es común en los sistemas actuales, altamente confiables. Es necesario entonces recurrir a técnicas de reducción de la varianza, que pueden calcular estimadores más precisos utilizando muestras del mismo tamaño [8, 10]. En el caso de las medidas en régimen estacionario, una familia de esquemas de muestreo según importancia (que reciben en forma amplia el número de métodos de "failure biasing") han demostrado ser apropiados [5, 6, 9, 11, 12]. Estos esquemas no son tan eficientes en el caso de la evaluación de medidas en régimen transitorio; en este caso, otras técnicas deben ser utilizadas, ya sea solas o combinadas con muestreo según importancia.

Este trabajo se concentra en la confiabilidad R_t, que es una de las medidas de seguridad de funcionamiento más importantes y utilizadas, y propone una técnica Monte Carlo para su evaluación que garantiza reducción de la varianza respecto a Monte Carlo estándar. Esta técnica pertenece a la familia de métodos de reducción recursiva de la varianza [2, 4, 3], y emplea el uso de un procedimiento de particionamiento del espacio de estado en forma recursiva, que en este caso particular puede obtenerse mediante el uso de cotas de la confiabilidad basadas en pathsets del sistema.

El resto del trabajo está organizado de la forma siguiente. La sección 2 presenta brevemente los modelos markovianos de seguridad de funcionamiento de sistemas multi-componentes, así como su evaluación por el método Monte Carlo estándar. La sección 3 describe en forma genérica la adaptación de la técnica de reducción recursiva de la variancia a la evaluación de la confiabilidad R_t. Esta técnica es paramétrica respecto al método de particionamiento empleado; en la sección 4 se presenta uno de los particionamientos pasibles de ser empleados. Este método particular está basado en los pathsets del sistema, y resulta de fácil implementación.

La sección 5 presenta un ejemplo concreto de aplicación del método propuesto, junto con algunos resultados numéricos. Por último, la sección 6 presenta algunas conclusiones y perspectivas de trabajo futuro.

2 Descripción del modelo

Consideremos un sistema multi-componente con fallas y reparaciones, cuyo espacio de estados se divide en dos conjuntos disjuntos U y D, siendo U el conjunto de los estados en los cuales el sistema está operacional (suministrando el servicio deseado), y D el conjunto de los estados en los cuales el sistema está en falla (el servicio suministrado no conforma las especificaciones).

El sistema se representa a través de una cadena de Markov de tiempo continuo homogénea e irreductible $X = \{X_t, t \geq 0\}$. Denotamos por S el espacio de estado de X, y supondremos que $1 \ll |S|\ (< +\infty)$.

Las principales medidas de seguridad de funcionamiento en régimen transitorio de los sistemas multi-componentes son:

- La *disponibilidad instantánea* A_t: probabilidad que el sistema se encuentre en estado operativo en el instante t:

$$A_t = I\!P\left\{X_t \in U\right\} = \mathrm{E}\left\{\mathbf{1}_{(X_t \in U)}\right\}.$$

- La *disponibilidad* D_t en el intervalo $[0,t]$: variable aleatoria definida comme la fracción del intervalo $[0,t]$ en la cual el sistema se encuentra operativo:

$$D_t = \frac{1}{t}\int_0^t \mathbf{1}_{(X_s \in U)} ds.$$

  La *disponibilidad esperada* verifica:

$$\mathrm{E}\left\{D_t\right\} = \frac{1}{t}\int_0^t A_s ds.$$

- La *confiabilidad* R_t en el instante t: probabilidad que el sistema esté operativo durante todo el período $[0,t]$, es decir:

$$R_t = I\!P\left\{X_s \in U, \forall s \in [0,t]\right\}.$$

Para mejor centrar la discusión, nos restringiremos a la evaluación de la confiabilidad R_t, aunque el caso de las otras medidas puede ser tratado con las mismas herramientas que presentaremos.

Para estimar la confiabilidad R_t consideremos une simulación del tipo Monte Carlo estándar de la cadena X. Una realización comienza siempre en el estado inicial del sistema y finaliza cuando se alcanza algún estado perteneciente a D o cuando el tiempo de estadía acumulado en los diversos estados supera el valor de t. En el primer caso el valor de la realización es 0, en el segundo es 1. Llamaremos $Y(t)$ el procedimiento de sorteo del método Monte Carlo estándar. En el caso de la simulación de los modelos altamente confiables, el problema está ocasionado fundamentalmente por el hecho de que el tiempo de estadía en el estado inicial del sistema suele ser mayor que el intervalo considerado $[0,t]$. Entonces, la cadena X permanecerá en el estado inicial durante todo el intervalo $[0,t]$. Esto significa que para que la simulación proporcione estimaciones aceptables al cabo de un número razonable de transiciones t debe ser más grande que el tiempo medio de estadía en el estado inicial.

3 Métodos de reducción recursiva de la varianza

El objetivo de esta sección es estudiar la familia de técnicas de reducción recursiva de la varianza para su adaptación al caso de la evaluación de las medidas en estado transitorio de los sistemas markovianos. Esta familia de técnicas (introducida en el contexto de la evaluación de sistemas combinatorios [2, 4]) garantiza une varianza menor a la del método Monte Carlo estándar, y está basada en el uso recursivo de un procedimiento de particionamiento.

Definimos un espacio de muestreo $\Omega(t) = \ x : [0,t] \rightarrow S\}$ que contiene todas las trayectorias sobre $[0,t]$ posibles de la cadena X; la medida μ_X es la medida de probabilidad de X en $\Omega(t)$.

Sea una familia $\mathcal{B}$ de sub-conjuntos de $\Omega(t)$ compatibles con la medida μ_X; notaremos $R(t|B) = I\!P\{\forall s \in [0,t], X_s \in U | X \in B\}$ la confiabilidad $[0,t]$ del sistema condicionado al evento B, para todo $B \in \mathcal{B}$. Sea un procedimiento $Y()$ de simulación estándar ("cruda") de la cadena X condicionado a un evento $B \in \mathcal{B}$: entonces $Y(t,B)$ es un variable aleatoria de Bernoulli, con $\mathrm{E}\{Y(t,B)\} = R(t|B)$, $\forall B \in \mathcal{B}$;

Para aplicar la técnica de reducción recursiva de la variancia, es necesario utilizar un método **PART** de particionamiento genérico, que descompone un elemento de $\mathcal{B}$ en sub-conjuntos que pertenecen a $\mathcal{B}$. Más específicamente, para cualquier conjunto $B \in \mathcal{B}$, el procedimiento **PART** devuelve (en un tiempo polinomial en el número de componentes del sistema) una partición $\mathcal{P} = \{A_O, A_P, B_w, w \in \mathcal{W}\}$ de B tal que:

- todos los elementos que pertenecen a A_O corresponden a trayectorias de buen funcionamiento del sistema en todo el intervalo $[0,t]$:

$$\forall \bar{x} \in A_O, \forall s \in [0,t], \bar{x}(s) \in U. \tag{1}$$

- todos los elementos que pertenecen a A_P corresponden a trayectorias de rotura del sistema antes del final del intervalo $[0,t]$:

$$\forall \bar{x} \in A_P, \exists s \in [0,t] \text{ tal que } \bar{x}(s) \in D. \tag{2}$$

- Existe une variable aleatoria W que toma valores en $\mathcal{W}$, definida por la medida $\mu_W(A) = \mu_{X|X\in(B-A_O-A_P)}(\bigcup_{w\in A} B_w)$;

- la aplicación recursiva del procedimiento **PART** sobre cualquier conjunto B lleva en un número finito de pasos a una partición tal que $|\mathcal{P}| = 1$.

Emplearemos las notaciones siguientes: $\mu_{X|B}(A_O) = P_O$, $\mu_{X|B}(A_P) = P_P$. De las definiciones precedentes, es claro que si $P_O > 0$ entonces $R(t|A_O) = 1$, y si $P_P > 0$ entonces $R(t|A_P) = 0$.

Definimos la variable aleatoria $Z(t,B)$ de la manera siguiente:

$$Z(t,B) = \begin{cases} Y(t,B) & \text{si } \mathcal{P} = \{B\}; \\ P_O & \text{si } \mathcal{P} = \{A_P, A_O\}; \\ P_O + (1 - P_O - P_P) Z(t, B_W) & \text{sinon}; \end{cases} \tag{3}$$

donde $\mathcal{P} = \{A_O, A_P, B_w, w \in \mathcal{W}\}$ es el resultado del método **PART** aplicado a B, y W es la v.a. definida antes.

De manera análoga al caso combinatorio [2], es posible probar que

$$\mathrm{E}\{Z(t,B)\} = R(t|B), \tag{4}$$

y

$$\begin{aligned} \mathrm{Var}\{Z(t,B)\} &\leq (R(t|B) - P_O)(1 - R(t|B) - P_P) \qquad (5) \\ &\leq R(t|B)(1 - R(t|B)) = Y(t,B). \qquad (6) \end{aligned}$$

Entonces $\mathrm{E}\{Z(t,\Omega(t)\} = R_t$ y $\mathrm{Var}\{Z(t,\Omega(t)\} \leq R_t(1-R_t)$, por lo que el estimador Z es más eficiente (en terminos de varianza) que el estimador Monte Carlo estándar.

4 Método de particionamiento basado en pathsets

La técnica que hemos descrito en la sección precedente es en realidad una "meta-técnica", en cuanto su implementación concreta y su performance depende de la definición del método de particionamiento **PART** a ser aplicado.

Es posible definir diversos métodos de particionamiento adaptados a los sistemas multi-componentes; entre los más intuitivos, encontramos aquellos basados en los pathsets y en los cutsets del sistema (recordamos que un pathset es un conjunto de componentes tales que su funcionamiento correcto asegura el buen funcionamiento del sistema; en un sistema de función de estructura coherente, todo super conjunto de un pathset es un pathset [7]).

En esta sección presentaremos un método sencillo de particionamiento basado en los pathsets del sistema. Haremos un cierto número de hipótesis sobre la naturaleza de los sistemas modelados, que simplificará nuestra tarea:

- las tasas de falla de los componentes no dependen del estado del sistema ($\lambda_i = a_i \varepsilon^{b_i}$, con $a_i \geq 0$ y $b_i \geq 1$ independientes del estado del sistema);
- es posible identificar cada componente de manera individual;
- no hay propagación de fallas;
- existe un método eficiente para encontrar un pathset del sistema cuando el estado de un cierto número de componentes ya ha sido fijado.

La mayor parte de estas hipótesis pueden ser relajadas, al costo de una formalización más engorrosa (y en algunos casos de una eficiencia reducida).

Definimos los elementos siguientes:

- tp_i = tiempo de la primer falla del componente i;
- la familia $\mathcal{B}$ está compuesta por conjuntos de la forma $\bigcap_{i \in I}(tp_i = s_i)$; para $B \in \mathcal{B}$, definimos el conjunto $I_1(B)$ como el conjunto de los componentes del sistema cuyo primer tiempo de falla ya ha sido fijado en B, y es menor o igual a t; y el conjunto $I_2(B)$ como el conjunto de los componentes del sistema cuyo primer tiempo de falla ya ha sido fijado en B, y es mayor que t;
- el seudo-código del procedimiento $Z(t, B)$ (que incluye el procedimiento de particionamiento según pathsets) es el siguiente:
  Entrada: conjunto B;
  Buscar un pathset $C = \{c_1, \ldots, c_{|C|}\}$ que no contenga ningún componente de $I_1(B)$;
  si no existe tal pathset C **entonces**
      resultado: sorteo Monte Carlo estándar $Y(t, B)$;
  de otro modo
  $$A_O = \left(\bigcap_{c \in C} (tp_c > t) \right) \cap B;$$

$P_O = \prod_{c \in C - I_2(B)} I\!P\{tp_c > t\} = \prod_{c \in C - I_2(B)} e^{-\lambda_c t};$

$A_F = \emptyset;$

$P_F = 0;$

Efectuar un sorteo de B_W (ver procedimiento abajo);

resultado: $P_O + (1 - P_O)Z(t, B_W);$

fin_si

- el sorteo de la variable B_W se efectúa de la manera siguiente:

  $B_W = B;$

  $D = C - I_2(B);$

  repetir hasta que $D = \emptyset$

  Elegir un componente $i \in D$;

  Realizar un sorteo s_i de tp_i condicionado a $\min_{c \in C} tp_c \leq t$:

  $B_W = B_W \cap (tp_i = s_i);$

  si $(s_i \leq t)$ **entonces**

  resultado: $B_W;$

  fin_si

  $D = D - \{i\};$

  fin_repetir

- el estimador de Monte Carlo estándar condicionado a un evento B, $Y(t, B)$ no plantea problemas para su implementación, dado que B es la intersección de eventos de tipo $(tp_i = s_i)$; alcanza con fijar los tiempos de falla de los componentes condicionados, y simular de manera estándar el comportamiento de los otros componentes.

5 Resultados numéricos

Ilustramos con un ejemplo la aplicación del método definido en la sección anterior para la evaluación de la confiabilidad R_t.

El sistema estudiado posee 30 componentes, 16 de tipo A, y 14 de tipo B. Todos los componentes tienen las mismas tasas de falla $\lambda = 1$ falla/hora; hay dos reparadores, uno para cada tipo de componente; las tasas de reparación para los componentes de tipo A es $\mu_A = 100$ reparaciónes/hora, y para los componentes de tipo B es $\mu_B = 1000$ reparaciónes/hora. La función de estructura del sistema está dada por el grafo representado en la figura 1. Los componentes del sistema están representados por las aristas del grafo: los componentes de tipo A marcados con línea punteada, aquellos de tipo B con línea continua. El sistema funciona correctamente si hay un camino operativo (un conjunto de aristas en funcionamiento) entre los nodos 1 y 20. El tamaño del espacio de estados de este sistema es de más de mil millones de estados.

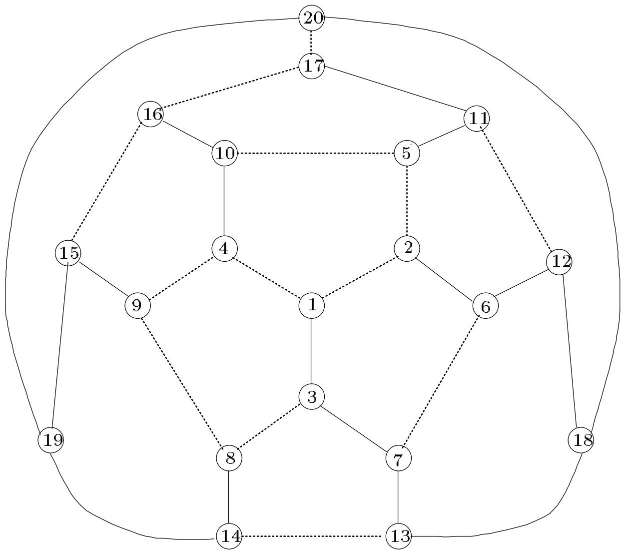

Figura 1: El sistema "dodecaedro"

Hemos implementado el método de reducción recursiva de la varianza basada en pathsets descrita precedentemente (subsección 4), y un método de Monte Carlo estándar. Los experimentos fueron efectuados en una estación de trabajo SUN SPARCstation 10 Model 602.

	$\widehat{Z}(t)$	$\dfrac{V\{Y\}}{\widehat{V}\{Z\}}$	$\dfrac{T_Y}{T_Z}$	$\dfrac{W_Y}{W_Z}$
$t = 0.001$	1.51×10^{-9}	0.99×10^{7}	2.65×10^{-1}	2.62×10^{6}
$t = 0.01$	5.63×10^{-7}	1.11×10^{4}	2.73×10^{-1}	3.03×10^{3}
$t = 0.1$	4.35×10^{-5}	2.53×10^{1}	3.17×10^{-1}	8.02×10^{0}
$t = 1$	5.01×10^{-4}	1.05×10^{0}	7.71×10^{-1}	8.10×10^{-1}

Tabla 1: Estimaciones de R_t para un método de reducción recursiva de la varianza

En la tabla 1 presentamos los resultados de simulación de la confiabilidad R_t, calculada para cuatro valores diferentes de t: $t = 0.001$, 0.01, 0.1 y 1 horas. El tamaño de la muestra utilizada es de 10^6 experimentos para cada valor de t. En la primer columna indicamos los valores del parámetro

t. La columna $\widehat{Z}(t)$ presenta los valores estimados por el método de reducción recursiva de la varianza para la confiabilidad R_t. La tercer columna contiene una estimación de los cocientes de las varianzas (calculados como los cocientes de la varianza de Monte Carlo estándar, $V\{Y\} = R_t(1 - R_t)$, y la varianza estimada del método de reducción recursiva de la varianza). Las columnas siguientes presentan el cociente de los tiempos de ejecución, y la eficiencia relativa del método de reducción recursiva de la varianza en relación al método estándar.

Podemos ver que el método propuesto posee une varianza que es siempre más pequeña que aquella del método de Monte Carlo estándar; pero esta reducción de la varianza depende en gran medida del valor de t estudiado. Para los valores más pequeños, se obtienen aceleraciones muy importantes, pero para valores de t más grandes las aceleraciones son menores. Este resultado podía esperarse observando que la varianza de Z está acotada por $(R_t - P_O)(1 - R_t)$ (de acuerdo a la ecuación 5), siendo $P_O = \prod_{c \in C} \mathbb{P}\{tp_c > t\} = \prod_{c \in C} e^{-\lambda_c t}$ una función decreciente de t; cuando t es pequeño, la varianza también lo será, pero al crecer t, P_O tiende a 0, y la cota se aproxima al valor de la varianza del método Monte Carlo estándar.

El tiempo de ejecución del método propuesto (que aparece en la columna 4) es un poco mayor que el del método estándar, especialmente para los valores más pequeños de t, lo que se explica por la necesidad de buscar los pathsets del sistema y un procedimiento de sorteo más complejo (que además es ejecutado en forma recursiva). El efecto combinado reducción de la varianza-tiempo de ejecución se aprecia en la eficiencia relativa W_Y/W_Z. Podemos ver que en general el balance es satisfactorio, exceptuando el caso $t = 1$, en el que la penalización en tiempo de ejecución es más importante que la reducción de la varianza obtenida. Para los valores de t más pequeños, la ganancia en eficiencia es realmente muy importante, y permite evaluar en un tiempo razonable sistemas que no eran abordables con el método estándar.

6 Conclusiones

En este trabajo hemos presentado la adaptación de la familia de técnicas de reducción recursiva de la varianza para la evaluación de medidas transitorias de seguridad de funcionamiento. Hemos implementado un método de esta familia, utilizando un método de particionamiento basado en los pathsets del sistema estudiado. Los resultados obtenidos sobre un ejemplo concreto muestran el interés de la propuesta, ilustrando las aceleraciones que pueden obtenerse, especialmente en el caso de sistemas muy confiables y ventanas de tiempo relativamente ajustadas.

Entre las perspectivas de trabajo futuro, se encuentra el desarrollo de otros métodos de particionamiento, de forma de ampliar la clase de sistemas susceptibles de ser evaluados con este enfoque. Es también interesante comparar las aceleraciones que pueden ser obtenidas en cada caso, y en particular buscar métodos que permitan mejorar los resultados en el caso de ventanas de tiempo mayores.

Referencias

[1] M. Ajmone Marsan, G. Balbo, and G. Conte. *Performance Models of Multiprocessor Systems*. The MIT Press, 1988.

[2] H. Cancela and M. El Khadiri. A recursive variance-reduction algorithm for estimating communication-network reliability. *IEEE Transactions on Reliability*, 44(4):595–602, December 1995.

[3] H. Cancela and M. El Khadiri. An improvement to the total hazard method for system reliability simulation. *Probability in the Engineering and Informational Sciences*, 10(2):187–196, 1996.

[4] H. Cancela and M. El Khadiri. A simulation algorithm for source-terminal communication network reliability. In *Proceedings of the 29th Annual Simulation Symposium*, pages 155–161, New Orleans, Louisiana, April 1996. IEEE Computer Society Press.

[5] H. Cancela, G. Rubino, and B. Tuffin. Fast Monte Carlo methods for evaluating highly dependable Markovian systems. In *2nd International Conference on Monte Carlo and Quasi-Monte Carlo Methods in Scientific Computing*, Salzburg, Austria, July 1996.

[6] J. A. Carrasco. Failure distance based simulation of repairable fault tolerant systems. In *Proceedings of the 5th International Conference on Modelling Techniques and Tools for Computer Performance Evaluation*, pages 351–365, 1991.

[7] C.J. Colbourn. *The Combinatorics of Network Reliability*. Oxford University Press, New York, 1987.

[8] George S. Fishman. *Monte Carlo: Concepts, algorithms and applications*. Springer, 1997.

[9] A. Goyal, P. Shahabuddin, P. Heidelberger, V. F. Nicola, and P. W. Glynn. A unified framework for simulating Markovian models of highly dependable systems. *IEEE Transactions on Computers*, 41(1):36–51, January 1992.

[10] Sheldon M. Ross. *Simulation.* Academic Press, 1996.

[11] P. Shahabuddin. Importance Sampling for the Simulation of Highly Reliable Markovian Systems. *Management Science*, 40(3):333–352, March 1994.

[12] B. Tuffin. Variance reduction applied to product form multiclass queuing networks. *ACM Transactions on Modeling and Computer Simulation*, 7(4):478–500, October 1997.

[13] J. Walrand and P. Varaiya. *High Performance Communication Networks.* Morgan Kaufmann Publishers, 1996.