Proceeding Series of the Brazilian Society of Computational and Applied Mathematics

Um modelo parcial de formação das classes de reversibilidade em autômatos celulares elementares

Ronaldo de Castro Corrêa[1]

Programa de Pós-Graduação em Engenharia Elétrica e Computação

Pedro Paulo B. de Oliveira[2]

Faculdade de Computação e Informática & Programa de Pós-Graduação em Engenharia Elétrica e Computação, Universidade Presbiteriana Mackenzie, São Paulo, SP

Resumo. O custoso processo de determinar computacionalmente o padrão de pré-imagens de regras de autômatos celulares permite particioná-las em diferentes níveis de reversibilidade. Visando simplificá-lo, apresentamos uma operação alternativa, definida diretamente das transições de estado, e a avaliamos no espaço elementar. Das 45 classes prováveis, 3 sofreram particionamento adicional, e a análise dos grafos de De Bruijn associados evidenciou importantes aspectos conceituais envolvidos.

Palavras-chave. Autômatos celulares, espaço elementar, regras reversíveis, regras parcialmente reversíveis, grafo de De Bruijn.

1 Introdução

Algumas regras dos autômatos celulares (ACs) possuem uma característica que permite que uma evolução temporal seja refeita independente da configuração inicial por meio de sua regra inversa correspondente; essa propriedade é chamada de reversibilidade. A reversibilidade de regras em autômatos celulares pode ter algumas aplicações, tais como criptografia, preservação de informação, modelos reversíveis de computação, etc [9].

Vários estudos sobre a reversibilidade de autômatos celulares têm sido realizados, tanto visando compreender as propriedades dessas regras, quanto para criar algoritmos para detectar ou construir autômatos celulares reversíveis. Por exemplo, [6], [1] propõem algoritmos para construir regras reversíveis, o primeiro usando um método baseado em grafos, e o segundo um sofisticado modelo algébrico. Por outro lado, [5] apresenta um algoritmo para verificar se uma regra de AC é reversível ou não.

Estendendo o conceito original de reversibilidade, em [7] foi introduzida a noção da *reversibilidade parcial*, que consiste em classificar regras que sejam mais ou menos reversíveis; com isso torna-se possível agrupá-las em classes de regras com o mesmo nível

[1]ronaldo.c.correa@gmail.com
[2]pedrob@mackenzie.br

DOI: 10.5540/03.2016.004.01.0019

de reversibilidade. Nesta classificação estão os conjuntos de regras reversíveis em um extremo, e as menos reversíveis no outro; tal classificação é obtida por meio da ordenação lexicográfica dos *padrões de pré-imagens*. Um padrão de pré-imagem é uma representação das quantidades de pré-imagens de todas as configurações possíveis de um reticulado, até um tamanho máximo L_{max} dado; a representação se dá ordenando as quantidades obtidas de cada configuração, independentemente dos tamanhos de reticulado considerados (este e outros detalhes em [7]). Para obter a classificação é necessário calcular o padrão de pré-imagem o que, dependendo do tamanho do reticulado, demanda alto tempo de processamento. Nosso objetivo é verificar se existe alguma forma de obter regras que possuam o mesmo grau de reversibilidade, porém sem calcular o padrão de pré-imagem, ou seja analisando somente a definição das próprias regras.

Restringe-se aqui a ACs unidimensionais, em parte devido à demonstração em [3] de que não existe um algoritmo que determine se uma regra é reversível para reticulados com dimensões superiores a 1, para qualquer quantidade de estados. Outro motivo da restrição metodológica que adotamos é simplesmente tomar o caso mais simples inicialmente, qual seja, a dos autômatos celulares elementares com condição de contorno cíclica, os quais possuem apenas 2 estados e 3 células na vizinhança.

No restante do artigo, a Seção 2 introduz o referencial teórico do trabalho, a Seção 3 apresenta os experimentos realizados, os resultados obtidos, e compara-os com os dados obtidos em [7]. A Seção 4 conclui o artigo com considerações finais.

2 Referencial Teórico

Autômatos celulares (ACs) são sistemas dinâmicos discretos definidos ([3]) pela *tripla* (S, N, f), onde S é o conjunto finito de estados $S = \{s_0, s_1, \ldots, s_{k-1}\}$, $N \in S^m$ é a vizinhança de uma célula c, onde m é o tamanho (em quantidade de células) da vizinhança e $f : S^m \longrightarrow S$ é a função de transição de estado local de uma célula. O reticulado é denotado por $C \in Z^d$, onde d é o número de dimensões e $d > 0$. O reticulado é composto por células que podem assumir os estados definidos por S. Neste trabalho são utilizados os ACs binários unidimensionais, $S = \{0, 1\}$ e $m = 3$, parâmetros estes que definem o espaço elementar de ACs. A função de transição de estados f recebe como parâmetro os estados das células vizinhas e da própria célula c e retorna seu novo estado, ou seja $f : S^m \longrightarrow S$. Ao definir f para todas as S^m configurações possíveis de vizinhança tem-se uma regra de um autômato celular; por exemplo, no caso elementar, uma regra pode ser definida como: $111 \rightarrow 0$, $110 \rightarrow 1$, $101 \rightarrow 1$, $100 \rightarrow 0$, $011 \rightarrow 0$, $010 \rightarrow 1$, $001 \rightarrow 1$, $000 \rightarrow 0$.

Uma regra é aplicada em todas as células do reticulado, sincronamente, a cada passo de tempo t. O reticulado unidimensional pode ser representado por um array de células, por exemplo $C = \{0, 1, 0, 1, 1, 1, 0\}$, para $t = 0$ e ao executar uma regra em C, a configuração é atualizada e o passo t incrementado. No caso de ACs binários, onde $S = \{0, 1\}$ cada regra é representada por um número inteiro R decorrente da conversão dos bits de saída de cada vizinhança; por exemplo, convertendo o número binário 01100110 (regra descrita acima) em um número decimal, é obtido o número 102. As regras de qualquer reticulado unidimensional finito ou infinito, com conjunto de estados $S = \{0, 1\}$ e tamanho de vizi-

DOI: 10.5540/03.2016.004.01.0019

nhança $m = 3$, são chamados de regras do espaço elementar. Como existem $2^m = 2^3 = 8$ configurações de vizinhança possíveis, e cada uma delas pode levar a um estado 0 ou 1, então existem $2^8 = 256$ regras possíveis, que definem o espaço elementar de autômatos celulares [10].

Existem regras que são equivalentes entre si, ou seja, possuem o mesmo comportamento dinâmico. As regras equivalentes são obtidas por meio de três operações: conjugação, reflexão e conjugação-reflexão, esta última uma das operações anteriores seguida da outra, ou seja, a composição das operações individuais [10]. No caso de ACs binários, a operação de conjugação consiste em inverter os bits das vizinhanças e os bits de saída, a operação de reflexão consiste em inverter as vizinhanças (por exemplo, $001 \rightarrow 100$) mantendo-se os bits de saída, e a operação conjugação-reflexão é a composição de uma das anteriores com a outra, em qualquer ordem. Cada grupo de regras formado por estas três operações define uma classe de equivalência dinâmica, sendo que, por convenção, a regra de menor valor de cada classe é tomada como a representante da classe; por exemplo, a regra 45 é a representante da classe formada pelas regras 45, 75, 101 e 89 (detalhes da formação dessa classe podem ser observados na Tabela 2).

2.1 Reversibilidade Parcial

Pré-imagens em autômatos celulares são todas as possíveis configurações anteriores de um reticulado no passo $t-1$ que levam a uma configuração no passo t. Para uma regra ser reversível todas as configurações iniciais possíveis de um reticulado podem possuir somente uma pré-imagem [8]. Configurações iniciais que não possuam pré-imagens são definidas como *Garden of Eden* ou *GoE*. Caso uma regra possua pelo menos uma configuração do tipo *GoE* consequentemente a regra também possui alguma configuração que tenha mais de uma pré-imagem; logo, a regra não é reversível [8]. Autômatos celulares reversíveis são exceções, pois a maioria dos autômatos celulares possuem alguma configuração que seja *GoE*. No grupo dos autômatos celulares elementares somente as regras 15, 85, 51, 170, 240 e 204 são reversíveis.

A noção de reversibilidade parcial proposta em [7] fundamentou-se no fato de que regras diferentes podem apresentar o mesmo padrão de pré-imagens, o que, em última instância, é o que define o comportamento de uma regra, quanto às suas possibilidades de admitir o percorrimento reverso de seu espaço de estados. Como consequência, o espaço de regras pode ser particionado em classes de mesmo nível de reversibilidade, a partir de seus padrões de pré-imagens, o que dá origem às *Classes de Reversibilidade Parcial* ou PRCs (*Partial Reversibility Classes*). Cada PRC é denotada pelo conjunto das regras representantes de cada classe de equivalência dinâmica compreendida na PRC; por exemplo, a regra 45 da PRC {45, 154} (Tabela 1) possui o mesmo padrão de pré-imagem de suas equivalentes dinâmicas, as regras 75, 101 e 89; o mesmo ocorre com a regra 154, que possui o mesmo padrão de pré-imagem de suas equivalentes dinâmicas, as regras 210, 166 e 154. A Tabela 1 abaixo é o resultado para reticulados de tamanho 33, com as classes agrupadas pelo tamanho de cada PRC, gerando três subconjuntos, PRC_i, $i \in \{1, 2, 4\}$, significando que $|PRC| = i$, onde na PRC {15, 51, 170, 204} estão as regras reversíveis e na PRC {0} estão as regras menos reversíveis.

DOI: 10.5540/03.2016.004.01.0019

Tabela 1: PRCs do espaço elementar agrupadas pelo tamanho.

PRC_1	{10},{60},{90},{126},{36},{24},{46},{0}
PRC_2	{45, 154},{30, 106},{105, 150},{37, 164},{22, 104},{62, 110},{25, 152}, {41, 134},{73, 146},{26, 74},{57, 156},{94, 122},{7, 168},{58, 78},{54, 108}, {14, 42},{38, 44},{35, 140},{33, 132},{77, 178},{23, 232},{6, 40},{9, 130}, {5, 160},{27, 172},{13, 162},{18, 72},{43, 142},{29, 184},{1, 128},{4, 32}, {11, 138},{12, 34},{2, 8}
PRC_4	{15, 51, 170, 204},{28, 50, 56, 76},{3, 19, 136, 200}

O padrão de pré-imagem é o multi-conjunto ordenado das quantidades de pré-imagens que todas as configurações iniciais possíveis de C com L de 1 até L_{max} possui; as configurações iniciais que não possuam pré-imagens não são adicionadas, e portanto o tamanho máximo de um padrão de pré-imagem é dado por $\sum_{i=1}^{L_{max}} |S|^i$, o qual pode variar de acordo com o nível de reversibilidade. Para fins de comparação, eis a ordenação lexicográfica dos padrões de pré-imagens de quatro regras elementares, para $L = 1$ até $L_{max} = 4$: **0**: {2, 4, 8, 16}; **1**: {1, 1, 1, 1, 1, 1, 1, 1, 1, 3, 7, 11}; **11**: {1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 2, 2, 2, 2, 2, 2, 2, 3, 3}; **15**: {1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1}. Observa-se no exemplo que a regra 15 é a mais reversível já que todas as 30 configurações iniciais possuem uma única pré-imagem; logo, se $L_{max} = 4$ o padrão de pré-imagem possui tamanho igual a 30 porque não existem configurações iniciais do tipo *GoE*. A regra 0 é a menos reversível já que para cada tamanho de reticulado $L = 1$ até $L_{max} = 4$ existe uma configuração inicial que possui todas as outras configurações iniciais como pré-imagem. O algoritmo utilizado para gerar o padrão de pré-imagem é o algoritmo proposto por [4].

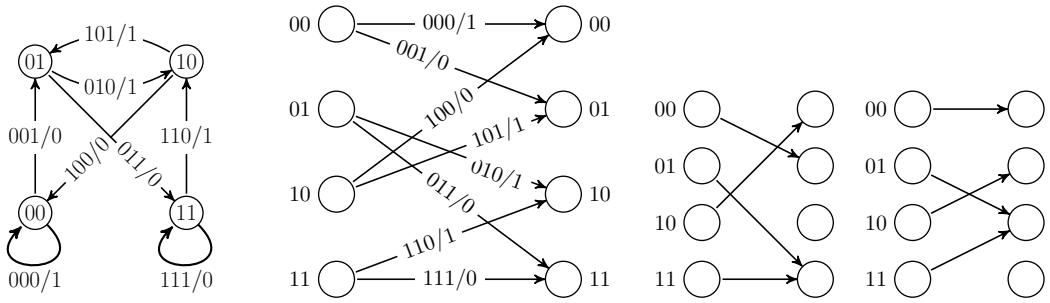
2.2 Grafo de De Bruijn modificado

Grafos de De Bruijn (GDB) são utilizados para representar as transições de estados de um AC unidimensional; a Figura 1(a) ilustra o grafo de De Bruijn da regra elementar 101. Em [2] apresenta-se um algoritmo para listar as pré-imagens de uma configuração de reticulado, o qual utiliza uma versão modificada do grafo de De Bruijn, ao qual nos referimos aqui como GDBm ou $GDBm^{(R)}$, onde R é o número da regra

Note que o grafo de De Bruijn da Figura 1(a) indica que seus nós estão rotulados com todas as permutações possíveis de tamanho k do conjunto S. Para obter os GDBm's correspondentes (Figura 1(c)), os vértices são organizados em duas colunas, e conectados de maneira que a sobreposição de seus rótulos formem as vizinhanças da regra e suas transições de estados associadas; tem-se então o grafo da Figura 1(b). Finalmente, decompõe-se o grafo anterior para cada estado do conjunto S. Os grafos obtidos para cada transição de estado são representados por $D^{(R)}(s_i)$, $i = 0, 1, \ldots k-1$. A Figura 1(c) ilustra o resultado da última etapa.

3 Operação de conjugação da vizinhança

Para cada PRC da Tabela 1 com mais que uma regra verificou-se que as regras da classe não são equivalentes dinâmicas entre si. Após tal verificação, para cada regra de



(a) Grafo de De Bruijn. (b) Grafo de De Bruijn alterado. (c) $D^{(101)}(0)$ e $D^{(101)}(1)$.

Figura 1: Passos para construção do grafo de De Bruijn modificado da regra elementar 101.

cada PRC listou-se suas respectivas equivalentes dinâmicas e suas transições de estado. A Tabela 2 ilustra para a PRC {45,154} a análise realizada em seguida.

Tabela 2: Equivalentes dinâmicas e transições de estados para a PRC {45,154}.

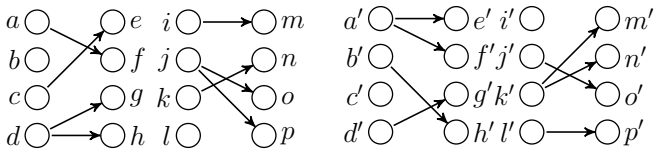
PRC	45				154			
EDs	45	75^1	89^2	101^3	154	166^1	180^2	210^3
Transições de Estado	$111 \to 0$	$111 \to 0$	$111 \to 0$	$111 \to 0$	$111 \to 1$	$111 \to 1$	$111 \to 1$	$111 \to 1$
	$110 \to 0$	$110 \to 1$	$110 \to 1$	$110 \to 1$	$110 \to 0$	$110 \to 0$	$110 \to 0$	$110 \to 1$
	$101 \to 1$	$101 \to 0$	$101 \to 0$	$101 \to 1$	$101 \to 0$	$101 \to 1$	$101 \to 1$	$101 \to 0$
	$100 \to 0$	$100 \to 0$	$100 \to 1$	$100 \to 0$	$100 \to 1$	$100 \to 0$	$100 \to 1$	$100 \to 1$
	$011 \to 1$	$011 \to 1$	$011 \to 1$	$011 \to 0$	$011 \to 1$	$011 \to 0$	$011 \to 0$	$011 \to 0$
	$010 \to 1$	$010 \to 0$	$010 \to 0$	$010 \to 1$	$010 \to 0$	$010 \to 1$	$010 \to 1$	$010 \to 0$
	$001 \to 0$	$001 \to 1$	$001 \to 0$	$001 \to 0$	$001 \to 1$	$001 \to 1$	$001 \to 0$	$001 \to 1$
	$000 \to 1$	$000 \to 1$	$000 \to 1$	$000 \to 1$	$100 \to 0$	$000 \to 0$	$000 \to 0$	$000 \to 0$
*EDs = Equivalentes dinâmicas por conjugação (1), conjugação-reflexão (2) e reflexão (3).								

Na Tabela 2 é possível identificar a existência de uma relação entre as regras 45 e 154. Ao inverter os bits das vizinhanças ($0 \to 1$ e $1 \to 0$) da regra 45, mantendo o próximo estado e, em seguida, ordenando novamente as vizinhanças em ordem lexicográfica, obtém-se a regra 180. Como a regra 180 é equivalente dinâmica da regra 154, basta obter a menor equivalente dinâmica da regra 180 para formar a classe de reversibilidade parcial {45,154}. Essa operação estabelece uma relação entre as regras de uma PRC, aqui chamada de *conjugação da vizinhança*, a operação é definida como $NC : R \to R$.

Para validar a operação *NC*, é realizada a análise dos GDBm's das regras; essa análise é válida devido ao algoritmo de listagem de pré-imagem apresentado por [2] ser equivalente ao algoritmo de contagem pré-imagem utilizado para calcular o padrão de pré-imagem. As Figuras 2(a) e 2(b) ilustram os GDBm's das regras 45 e 180.

Analisando os grafos das regras 45 e 180, observa-se que o GDBm $D^{(45)}(0)$ é exatamente o inverso de $D^{(180)}(0)$ e o mesmo acontece com $D^{(45)}(1)$ e $D^{(180)}(1)$; portanto, há isomorfismo entre os GDBm's das regras. Se todas as condições iniciais para um reticulado C de tamanho L forem testadas, a quantidade de pré-imagens obtidas pelo algoritmo será exatamente a mesma para as duas regras. Para existir isomorfismo entre duas regras R_1

DOI: 10.5540/03.2016.004.01.0019



(a) $D^{(45)}(0)$ e $D^{(45)}(1)$. (b) $D^{(180)}(0)$ e $D^{(180)}(1)$.

Figura 2: GDBm's das regras 45 e 180.

e R_2 deve existir isomorfismo entre os GDBm's $D^{(R_1)}(s_i)$ e $D^{(R_2)}(s_i)$:

$$GDBm^{(R_1)} \equiv GDBm^{(R_2)} \longrightarrow \begin{cases} \exists \text{ isomorfismo} & D^{(R_1)}(0) \equiv D^{(R_2)}(0) \text{ e } D^{(R_1)}(1) \equiv D^{(R_2)}(1) \\ & \text{ou} \\ & D^{(R_1)}(0) \equiv D^{(R_2)}(1) \text{ e } D^{(R_1)}(1) \equiv D^{(R_2)}(0); \\ \nexists \text{ isomorfismo} & \text{caso contrário.} \end{cases}$$

O isomorfismo entre $GDBm^{(45)} \equiv GDBm^{(180)} \rightarrow \{D^{(45)}(0) \equiv D^{(180)}(0) \text{ e } D^{(45)}(1) \equiv D^{(180)}(1)\}$ demonstra que por meio da operação NC é obtida uma regra que possui o mesmo padrão de pré-imagem. Entretanto, o isomorfismo é uma condição suficiente mas não necessária para que duas regras possuam o mesmo padrão de pré-imagem, o que pode ser observado analisando a regra 45 e sua equivalente dinâmica por reflexão a regra 101, conforme a Figura 1(c). Os GDBm's da regra 45 e a regra 101 não são isomorfos já que $D^{(45)}(0) \not\equiv D^{(101)}(0)$, $D^{(45)}(0) \not\equiv D^{(101)}(1)$, $D^{(45)}(1) \not\equiv D^{(101)}(1)$ e $D^{(45)}(1) \not\equiv D^{(101)}(0)$.

A aplicação da operação NC em cada representante das classes de equivalência dinâmica do espaço elementar, levou ao particionamento mostrado na Tabela 3. Observa-se, portanto, concordância entre nossos resultados com a Tabela 1, no que diz respeito às classes da PRC_1. Observa-se ainda que o grupo PRC_2 que obtivemos contêm o grupo correspondente da Tabela 1, e que o grupo PRC_4 da Tabela 3 difere da PRC_4 da Tabela 1.

As classes da Tabela 1 que não se agruparam corretamente foram {15, 51, 170, 204}, {28, 50, 56, 76} e {3, 19, 136, 200}, uma vez que sofreram um particionamento adicional, em blocos iguais, tendo gerado as classes, {15, 170}, {51, 204}, {28, 56}, {50, 76}, {3, 136} e {19, 200}. A razão para tanto está sendo investigada e representaria o critério necessário a complementar o critério suficiente representado pela operação de conjugação da vizinhança.

Tabela 3: PRCs do espaço elementar obtidas através da operação NC.

PRC_1	{10},{60},{90},{126},{36},{24},{46},{0}
PRC_2	{15, 170}, {51, 204},{28, 56},{50, 76},{3, 136},{19, 200},...,{12, 34},{2, 8}
PRC_4	

4 Conclusão

Ao aplicar a operação NC em cada representante das equivalentes dinâmicas do espaço elementar, o resultado obtido foi similar ao resultado apresentado por [7], visto que somente

DOI: 10.5540/03.2016.004.01.0019

as classes, {15, 51, 170, 204}, {28, 50, 56, 76} e {3, 19, 136, 200}, não se agruparam corretamente. Apesar do resultado obtido com a operação NC não gerar corretamente as PRCs da Tabela 1, as classes obtidas possuem o mesmo padrão de pré-imagem. Para se obter a classificação das regras para reticulados de tamanho até aproximadamente $L_{max} = 25$ o tempo de processamento é razoável; porém estender o tamanho do reticulado além desse patamar o processamento vai se inviabilizando, dado o crescimento exponencial da quantidade de configurações. A vantagem da operação NC é que não há necessidade de calcular os padrões de pré-imagens para saber quais regras estão na mesma classe de reversibilidade parcial, ou seja, apenas com a operação NC sabe-se quais regras possuem o mesmo nível de reversibilidade independente do tamanho do reticulado. Também foi visto que o isomorfismo dos grafos de De Bruijn modificados é uma condição suficiente, mas não necessária, para que as regras possuam o mesmo nível de reversibilidade parcial.

Agradecimentos: Nós agradecemos o IPM (Instituto Presbiteriano Mackenzie), e PPBO agradece o suporte financeiro MackPesquisa (Fundo Mackenzie de Pesquisa), FAPESP (Fundação de Amparo à Pesquisa do Estado de São Paulo) e CNPq (Conselho Nacional de Desenvolvimento Científico e Tecnológico)

Referências

[1] T. Boykett, Efficient exhaustive listings of reversible one dimensional cellular automata, *Theoretical Computer Science*, 325:215–247, (2004).

[2] I. Jeras and A. Dobnikar, Algorithms for computing preimages of cellular automata configurations, *Physica D*, 233:95–111 (2007).

[3] J. Kari, Theory of Cellular Automata: A Survey, *Theoretical Computer Science*, 334:3–33 (2005).

[4] H. V. McIntosh, *Linear Cellular Automata via DeBruijn Diagrams*, Depto. de Aplicación de Microcomputadoras, Inst. de Ciencias, Univ. Autónoma de Puebla (1991).

[5] J. C. S. T. Mora and S. V. C. Vergara and G. J. Martínez and H. V. McIntosh, Procedures for calculating reversible one-dimensional cellular automata, *Physica D*, 202:134–141 (2005).

[6] H. Moraal, Graph-theoretical characterization of invertible cellular automata, *Physica D*, 141:1–18 (2000).

[7] P. P. B. de Oliveira and R. Freitas, Relative partial reversibility of elementary cellular automata, In J. Kari, N. Fatés, T. Worsh, eds, *Proc. of Automata 2010:* 16^{th} *Int. Workshop on Cellular Automata and Discrete Complex Systems*, LORIA-INRIA, Nancy, France, 195–208 (2010).

[8] E. J. Powley, *Global properties of cellular automata*, Tese de Doutorado, University of York, Department of Computer Science (2009).

[9] T. Toffoli and N. Margolus, Invertible Cellular Automata: A Review, *Physica D*, 45:229–253, (1994).

[10] S. Wolfram, *A New kind of Science*, Wolfram Media, (2002).

