GRUPOS LIVRES E AUTÓMATOS CELULARES

Alberto Martins Teixeira

Tese de Mestrado

FCUP - 1995/1996

ÍNDICE

PREFÁCIO

Leibnitz, deverá ter sido um dos primeiros matemáticos a pensar em termos *Booleanos*. Nas suas teses de 1714 acerca de Monadologia afirma que "Se há compostos, é necessário haver substâncias simples, pois o composto é apenas reunião ou *aggregatum* dos simples". Se este grande filósofo tem razão então este trabalho pretende ser uma achega ao *aggregatum* dos 256 autómatos celulares de mais simples definição. Na bibliografia mencionada estão algumas das proposições e teoremas que inspiraram e guiaram este trabalho. Não posso ainda deixar de acrescentar à bibliografia os conselhos e sugestões do meu amigo João Carvalho com quem divaguei muitas vezes as minhas ideias.

1. INTRODUÇÃO

1.1. Definição de um Autómato Celular

Um automato celular pode ser encarado como um conjunto de células ou sítios, cada um dos quais podendo assumir diversos estados, com uma determinada evolução temporal. Desta forma o autómato celular não é mais do que um sistema completamente discreto: discreto no espaço porque é formado por um conjunto de células individuais, discreto no tempo porque consideramos a sua evolução por étapas sequênciais e finalmente discreto em magnitude porque cada célula só pode assumir um número finito de estados.

O instrumento a que nos habituamos para descrever o mundo físico, que nos rodeia, tem sido as equações diferenciais que descrevem a mudança de quantidades através duma função contínua do espaço e do tempo. Neste contexto os autómatos celulares desempenham um papel de aproximação discreto aos sistemas dinâmicos, isto é qualquer sistema físico descrito através de equações diferenciais poderá ser aproximado por um autómato celular introduzindo diferenças finitas e variáveis discretas.

Para descrever um autómato celular, convenientemente, precisamos de caracterizar quatro propriedades: a geometria do autómato, a vizinhança da célula, o número de estados de cada célula e finanlmente a regra de evolução do autómato.

1.2. Geometria dum Autómato Celular

O conjunto das células ou sítios constituem o autómato celular pode dispor-se de várias formas, segundo uma linha, no plano, no espaço tridimensional ou num espaço com mais de três dimensões. Esta disposição conduzirá a autómatos unidimensionais, bidimensionais, tridimensionais e pluridimensionais. A razão porque isso acontece dependerá em cada caso da aplicação concreta que é feita do autómato celular. Para o estudo do crescimento dum floco de neve poderá ser apropriado tomar como modelo uma matriz bidimensional.

De alguma forma, se bem que convenientemente caracterizados, autómatos celulares em espaços com três ou mais dimensões são de difícil visualização. Por outro lado, o comportamento dos autómatos mais simples, deste ponto de vista, os unidimensionais poderá apresentar factores complexos, como se verá.

1.3 Vizinhança duma Célula

Esta noção topológica introduz um grau de complexidade na estrutura dos autómatos celulares de cada dimensão. Entende-se como vizinho dum sítio, outro que para os efeitos considerados se possa considerar "perto" e portanto possa influenciar esse sítio. Num autómato celular consideramos que cada sítio evoluiu em função do estado desse próprio sítio e de todos os que estando perto o possam influenciar, ou sejam, os seus vizinhos.

No caso unidimensional, a situação mais simples é tomar como vizinhança dum ponto (célula) x_i as células adjacentes, os sítios x_{i-1} e x_{i+1}. Se considerarmos o agregado de células

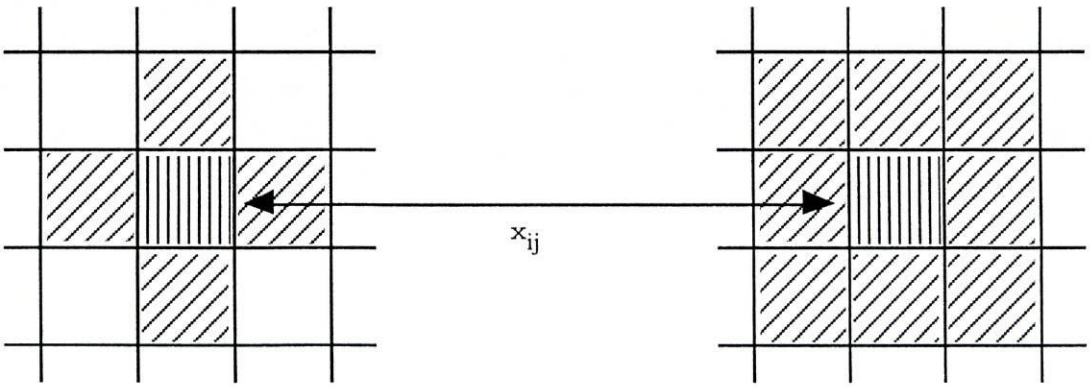
unidimensionais infinito, esta definição não conduz a quaisquer problema, no entanto se o agregado for finito a primeira célula x_1 não tem vizinho à esquerda assim a última célula x_n não tem vizinho à direita. Para ultrapassar esta dificuldade podemos optar entre duas soluções, que não são relevantes para a evolução do autómato:

1°) Considerar o vizinho esquerdo da célula x_1 com sendo uma célula num determinado estado, o nulo, que definiremos a seguir e tomar para vizinho direito da célula x_n uma célula virtual nas mesmas condições que o vizinho direito de x_1.

2°) Considerar que o vizinho esquerdo de x_1 é a célula x_n e considerar que o vizinho direito de x_n é a célula x_1. Isto corresponde, em termos topológicos, a considerar o segmento, onde se situam as células $x_1, x_2, \ldots, x_n$, com os extremos identificados, que é o mesmo que considerar as células dispostas segundo um círculo.

No caso bidimensional, que de certa forma inspiram toda a teoria dos autómatos celulares é costume considerar para cada célula x_{ij} duas vizinhanças típicas: a vizinhança de *von-Neumann*, constituida pela célula x_{ij} e pelas situados respectivamente, a norte, a sul, a este e a oeste, simbolicamente $x_{i-1,j}$; $x_{i+1,j}$; $x_{i,j-1}$ e $x_{i,j+1}$ ou então a chamada vizinhança de *Moore* constituida pela célula e por todas as que a rodeiam.

Geometricamente, teremos:



Vizinhança de *von Neumann* Vizinhança de *Moore*

Um dos autómatos celulares mais conhecidos e mais divulgados devido a *Martin Gardner*, é o "jogo da vida", autómato criado por *John Conway* em 1970 e que pretende simular a evolução da vida: uma célula nasce permanece viva ou morre dependendo do número de células vizinhas.

1.4. Número de Estados duma Célula

Cada célula poderá apresentar-se segundo um número finito de estados. Naturalmente no caso mais simples a célula poderá ter apenas dois estados que representaremos por 0 e 1, são os chamados autómatos celulares Booleanos. No caso do "jogo da vida" diriamos que a célula estaria "morta" (0) ou "viva" (1).

Está mais ou menos definido que o número de estados duma célula deverá ser um número primo, por razões de cálculo algébrico.

Torna-se agora claro que na evolução de autómatos celulares unidimensionais finitos, podemos considerar como vizinhas das células das extremidades células virtuais em estado nulo (zero) em alternativa a condições de fronteira circulares.

1.5. Regras de Evolução

Entendemos por regras de evolução dum autómato celular como sendo a aplicação que nos indica o estado futuro duma célula x_i^t, situada no ponto i no tempo t, quando o tempo evolui de uma unidade, ou seja o estado da célula x_i^{t+1}:

$$x_i^t \xrightarrow[\substack{regra\ de\\ evolução}]{} x_i^{t+1}$$

Como já foi dito a evolução do estado duma célula depende não só do estado em que ela se encontra mas também dos estados em que se encontram as células vizinhas, isto é:

$$x_i^{t+1} = f\left(x_{i-r}^t,\ldots,x_i^t,\ldots x_{i+r}^t\right)$$

o estado de x_i^{t+1} depende dos estados das $2r+1$ células que constituem a vizinhança de "raio r" da célula x_i no tempo t. Se considerarmos que os estados possíveis para cada célula pertencem a um conjunto finito $S\,(\#S=s)$ a aplicação anterior f pode-se caracterizar como

$$f: S^{2r+1} \to S$$

ou seja uma aplicação da potência cartesiana de ordem $2r+1$ de S nele próprio .

No caso unidimensional, caso que será daqui para a frente o único considerado, o número de autómatos celulares diferentes considerando vizinhanças de n sítios e k estados para cada célula é:

$$K^{K^n}$$

De todos estes, os autómatos mais simples e os mais estudados, são os autómatos em que $n=3$ (os vizinhos dum ponto são os seus adjacentes) e $K=2$ (cada autómato só tem dois estados possíveis: 0 e 1). Temos para este caso $2^{2^3}=2^8=256$ possibilidades de estabelecermos regras evolutivas, sendo cada regra uma aplicação de B^3 em B onde $B=\{0,1\}$

$$\begin{aligned} f:&\ B^3 \to B \\ &(x,y,z) \to f(x,y,z) \end{aligned}$$

Sendo Y a célula considerada no tempo t e X, Z os seus vizinhos. Isto é:

$$\begin{aligned} f:&\ B^3 \to B \\ &(x^t,y^t,z^t) \to y^{t+1} \end{aligned}$$

Neste caso em que $K=2$ e $n=3$, as vizinhanças dos pontos 1 e 0 são descritas facilmente:

$$V_1 = \{111, 110, 011, 010\}$$
$$V_0 = \{101, 100, 001, 000\}$$

Só temos que atribuir a cada um destes termos de números os valores 1 ou 0, que é equivalente a preencher a seguinte tabela,

X	Y	Z	
1	1	1	
1	1	0	
1	0	1	
1	0	0	
0	1	1	
0	1	0	
0	0	1	
0	0	0	

que traduz o número total de funções booleanas de três argumentos.

É sabido que cada função booleana se pode representar por forma canónica ou forma normal disjuntiva da seguinte maneira:

$$f(x_1, x_2, \ldots x_n) = \sum f(\alpha_1, \ldots \alpha_n) X_1^{(\alpha_1)} X_2^{(\alpha_2)} \ldots X_n^{(\alpha_n)} \qquad \alpha_i \in \{0,1\} \forall_i$$

onde

$$X_i^{(\alpha_1)} = \begin{cases} X_i & \text{se} \quad \alpha_i = 1 \\ \overline{X}_i & \text{se} \quad \alpha_i = 0 \end{cases} \qquad (\overline{X}_i \text{ é o complementar ou negação de } X_i)$$

a soma $\sum$ é entendido no sentida da disjunção inclusiva e o produto $X_i X_j$ como a conjunção.

Cada um dos termos $X_1^{(\alpha_1)} \ldots X_n^{(\alpha_n)}$ é chamado um minitermo.

No nosso caso, de três argumentos, a expansão representa-se por

$$f(X,Y,Z) = \sum f(\alpha_1, \alpha_2, \alpha_3) X^{(\alpha_1)} Y^{(\alpha_2)} Z^{(\alpha_3)} \qquad (F1)$$

e os únicos e efectivos termos são aqueles em que $\sum f(\alpha_1, \alpha_2, \alpha_3) = 1$. Quando nos é dada uma tabela a forma normal disjuntiva é imediatamente calculada. Ex.:

X	Y	Z	
1	1	1	0
1	1	0	0
1	0	1	1
1	0	0	1
0	1	1	0
0	1	0	0
0	0	1	1
0	0	0	0

este autómato celular é conhecido como Regra 50 (já de seguida se verá porquê) e a sua expressão como função booleana de três argumentos é

$$f(X,Y,Z) = f(1,0,1)X^{(1)}Y^{(0)}Z^{(1)} + f(1,0,0)X^{(1)}Y^{(0)}Z^{(0)} + f(0,0,1)X^{(0)}Y^{(0)}Z^{(1)}$$

ou seja

$$f(X,Y,Z) = X\overline{Y}Z + X\overline{Y}\overline{Z} + \overline{X}\overline{Y}Z$$

Quando consideramos o anel Booleano $(Z_2, \oplus, \bullet)$, a operação $\oplus$ corresponde à disjunção exclusiva e as relações:

$$X + Y = XY \oplus x + Y \quad \text{e também } \overline{X} = X \oplus 1$$

Isso quer dizer que podemos escrever a expressão (F1) apenas com operações neste anel:

Por exemplo, para a Regra 50:

$$\begin{aligned}
&X\overline{Y}Z + X\overline{Y}\overline{Z} + \overline{X}\overline{Y}Z \qquad (F2)\\
&= X\overline{Y}Z \cdot X\overline{Y}\overline{Z} \oplus X\overline{Y}Z \oplus X\overline{Y}\overline{Z} + \overline{X}\overline{Y}Z\\
&= X\overline{Y}Z \oplus X\overline{Y}\overline{Z} + \overline{X}\overline{Y}Z\\
&= \left(X\overline{Y}Z \oplus X\overline{Y}\overline{Z}\right)\overline{X}\overline{Y}Z \oplus X\overline{Y}Z \oplus X\overline{Y}\overline{Z} \oplus \overline{X}\overline{Y}Z\\
&= X\overline{Y}Z \cdot \overline{X}\overline{Y}Z \oplus X\overline{Y}\overline{Z} \cdot \overline{X}\overline{Y}Z \oplus X\overline{Y}Z \oplus X\overline{Y}\overline{Z} \oplus \overline{X}\overline{Y}Z\\
&= X\overline{Y}Z \oplus X\overline{Y}\overline{Z} \oplus \overline{X}\overline{Y}Z \qquad (F3)
\end{aligned}$$

Utilizamos nesta simpificação algumas propriedades booleanas tais como:

$$XX = X^2 = X \qquad X \cdot \overline{X} = 0 \qquad X \cdot 0 = 0 \qquad X \oplus 0 = X$$

Olhando para as expressões (F2) e (F3) parece que tudo se resumiu a mudar os + pelos $\oplus$. Assim, é, de facto, se bem que existe uma explicação para isso.

Considerem-se dois minitermos:

$$M_\alpha = X_1^{(\alpha_1)}X_2^{(\alpha_2)}X_3^{(\alpha_3)} \qquad \text{e} \qquad M_\beta = X_1^{(\beta_1)}X_2^{(\beta_2)}X_3^{(\beta_3)}$$

não podemos ter $\alpha_i = \beta_i \quad \forall_i \in \{1,2,3\}$ porque então, $M_\alpha = M_\beta$ o que é impossível acontecer nos minitermos. Portanto

$$I_i \in \{1,2,3\}: \alpha_i \neq \beta_i$$

sem perdas de generalidades podemos considerar $\alpha_i = 1$ e $\beta_i = 0$ donde $X_i^{(\alpha_i)} = X_i$ e $X_i^{(\beta_i)} = \overline{X}$ seja $M_\alpha + M_\beta = M_\alpha M_\beta \oplus M_\alpha \oplus M_\beta$ em $M_\alpha M_\beta$ vai aparecer o factor $X_i^{(\alpha_i)} X_i^{(\beta_i)} = X_i \cdot \overline{X}_i = 0$ donde $M_\alpha M_\beta = 0$, daí a razão de termos para os minitermos da expansão disjuntiva $M_\alpha + M_\beta = M_\alpha \oplus M_\beta$, igualdade que permite escrever a expressão (F1) da seguinte forma

$$f(X,Y,Z) = \sum f(\cdot\alpha_1, \alpha_2, \alpha_3) \cdot X^{(\alpha_1)} Y^{(\alpha_2)} Z^{(\alpha_3)} \qquad (F4)$$

onde $\sum$ se refere à soma lógica entendida como disjunção exclusiva podemos ir um pouco mais longe. Sabemos que $\overline{X} = X \oplus 1$, igualdade que podemos utilizar para simplificar a expressão (F4).

Tomando como exemplo a expressão (F3) obtido da Regra 50:

$$\begin{aligned} & X\overline{Y}Z \oplus X\overline{Y}\overline{Z} \oplus \overline{X}\overline{Y}Z \qquad (F3) \\ &= X(Y \oplus 1)Z \oplus X(Y \oplus 1)(Z \oplus 1) \oplus (X \oplus 1)(Y \oplus 1)Z \\ &= XYZ \oplus XZ \oplus XYZ \oplus XY \oplus X \oplus XYZ \oplus XZ \oplus YZ \oplus Z \\ &= XYZ \oplus XY \oplus XZ \oplus YZ \oplus X \oplus Z \qquad (F5) \end{aligned}$$

A expressão que obtivemos em (F5) a partir de (F3) poderá ser feita para qualquer outra expressão que resulte de expandir a regra do autómato celular no anel. Ou seja qualquer expressão do tipo (F4) pode ser escrito na forma

$$f(X,Y,Z) = \sum g(\alpha_1, \alpha_2, \alpha_3) X^{\alpha_1} Y^{\alpha_2} Z^{\alpha_3} \qquad (F6)$$

onde $g(\alpha_1, \alpha_2, \alpha_3) \in \{0,1\}$ e $X_i^{\alpha_i} = \begin{cases} X_i & \text{se} \quad \alpha_i = 1 \\ 1 & \text{se} \quad \alpha_i = 0 \end{cases}$

Daqui para a frente o símbolo $\sum$ referir-se-á sempre à disjunção exclusiva que temos vindo a representar por $\oplus$.Falta-no agora falar da forma como podemos atribuir um número a cada regra.

Tomemos, ainda como exemplo, a dita regra 50 cuja tabela é:

X	Y	Z	
1	1	1	0
1	1	0	0
1	0	1	1
1	0	0	1
0	1	1	0
0	1	0	0
0	0	1	1
0	0	0	0

se considerarmos cada linha como sendo uma potência de base 2, desde 2^0 (a linha inferior) até 2^7 (linha superior), os expostos das potências em numeração binária representam os termos ordenados XYZ. Temos sucessivamente

$$2^0 = 2^{000} = 1 \qquad 2^4 = 2^{100} = 16$$
$$2^1 = 2^{001} = 2 \qquad 2^5 = 2^{101} = 32$$
$$2^2 = 2^{010} = 4 \qquad 2^6 = 2^{110} = 64$$
$$2^3 = 2^{011} = 8 \qquad 2^7 = 2^{111} = 128$$

Numeramos cada regra considerando as somas das potências cujos exponentes em binário (identificados com as vizinhanças) são aplicadas em 1. Ainda no exemplo que temos vindo a tratar, vemos que

$$101 \rightarrow 1 \qquad 100 \rightarrow 1 \qquad 001 \rightarrow 1$$

portanto a nossa regra será

Regra = 32+16+2 = 50 ou seja Regra 50

Com este processo podemos numerar os 256 autómatos celulares Booleanos unidimensionais de vizinhança 3, de 0 correspondente ao autómato cuja matriz é (00000000) e que transforma tudo em zero até ao autómato 255 a que corresponde a matriz (11111111) e que transforma tudo em 1. Entre um e outro estão todos os restantes autómatos.

Por exemplo, qual será o autómato celular correspondente à Regra 104?

Comecemos por decompor 104 em potências de base 2:

$$104 = 64 + 32 + 8 = 2^6 + 2^5 + 2^3$$

ficamos portanto a saber que os únicos ternos ordenados que têm por imagem 1 são:

6: 110 5: 101 e 3: 011

daqui facilmente construimos a tabela de aplicações:

X	Y	Z	
1	1	1	0
1	1	0	1
1	0	1	1
1	0	0	0
0	1	1	1
0	1	0	0
0	0	1	0
0	0	0	0

← 6
← 5
← 3

Este é o autómato celular $R_{104} = (01101000)$

2. BREVES REFERÊNCIAS A ALGUMAS PROPRIEDADES ELEMENTARES E GLOBAIS DOS AUTÓMATOS CELULARES

Como ficou visto os autómatos celulares unidimensionais binários com vizinhança mínima são de fácil definição. No entanto a evolução destes autómatos a partir dum sítio único ou duma sequência aleatória de sítios em estados 0 e 1 poderá conduzir a padrões de alta complexidade.

Em primeiro lugar podemos estabelecer algumas condicionantes para estas regras. Podemos por exemplo proibir que $000 \rightarrow 1$, isto é que uma ocupação seja criada a partir do nada, ou ainda que as regras produzam simetria, isto é que 011 e 110 conduzam ao mesmo valor (bem como 001 e 100). Com estas restrições temos aquilo que se designa por regras legais. Têm por matriz:

$$(a_1, a_2, a_3, a_4, a_2, a_5, a_4, 0)$$

Por outro lado existem regras que exibem propriedades simplificadoras. É o caso das regras ditas aditivas, que além de serem legais exibem a propriedade de sobreposição aditiva ou seja a evolução duma sequência de uns e zeros pode ser obtida pela sobreposição (somar módulo 2) da evolução de cada um dos sítios uns, feita isoladamente. Estas regras caracterizam-se pela matriz

$$(a_1 a_2 0 a_3 a_2 a_1 a_3 0) \qquad \text{com} \qquad a_3 = a_1 \oplus a_2$$

correspondentes às regras 0, 90, 150 e 204, de fácil caracterização

$R_0 = 0$ transforma tudo em zeros, anula qualquer situação inicial.

$R_{204} = Y$ mantém qualquer situação inicial inalterável.

$R_{90} = X \oplus Z$ representa a adição (módulo 2) dos sítos vizinhos do sítio considerado. Se fizermos a evolução a partir do sítio único não há evolução, uma vez que os vizinhos do síto único são zeros.

$R_{150} = X \oplus Y \oplus Z$ corresponde à adição (módulo 2) dum sítio com os seus vizinhos.

Outras considerações poderão ser feitas analisando outras características. Se em vez da sobreposição aditiva pensarmos na sobreposição multiplicativa ou conjuntiva teremos as regras

$$R_0 = 0$$
$$R_4 = XYZ \oplus XY \oplus YZ \oplus Y$$
$$R_{50} = XYZ \oplus XY \oplus XZ \oplus YZ \oplus X \oplus Z$$
$$R_{254} = XYZ \oplus XY \oplus XZ \oplus YZ \oplus X \oplus Y \oplus Z$$

Também considerando o princípio da sobreposição disjuntiva inclusiva, teremos as regras

$$R_0 = 0$$
$$R_{204} = Y$$
$$R_{250} = XZ \oplus Z$$
$$R_{254} = XYZ \oplus XY \oplus XZ \oplus YZ \oplus Z \oplus Y$$

Noutra perspectiva as regras poderão considerar-se periféricas se a evolução dum sítio depende não desse sítio mas da periferia do sítio, isto é dos seus vizinhos. Estes autómatos traduzem-se pela matriz:

$$(a_1 a_2 a_1 a_2 a_2 0 a_2 0)$$

Se atendermos à evolução do sítio único ocupado, várias situações podem ocorrer: esse sítio é imediatamente apagado (por exemplo regras 0 e 160), é mantido para sempre (regras 4 e 36) ou esse 1 mantem-se mas em cada evolução temporal dois novos sítios são ocupados, um em cada direcção, criando-se uma estrutura uniforme de sítos ocupados que vai crescendo no tempo numa forma triangular. Qualquer uma destas regras é considerada simples a contrário das regras do tipo 18, 22 ou 90 que conduzem a padrões não-triviais e são denominadas complexas. Nestas regras a característica principal é o aparecimento de formas triangulares formadas pela ausência de sítios ocupados. A regra 90, por exemplo, manifesta auto-semelhança nos seus triângulos criando assim uma estrutura do tipo fractal semelhante ao triângulo de *Sierpinski*.

Quando o estudo é feito considerando sequências iniciais finitas de zeros e uns (com condições de fronteira periódica ou não) os padrões observados diferem quer se trate de regras ditas simples ou das regras complexas. À semelhança do que se passa com sistemas

dinâmicos as regras simples apresentam pontos limtes ou circulos limites, isto é uma dada configuração aparece, mantendo-se indefinidamente, ou o autómato evolui a partir de certa altura percorrendo periodicamente um ciclo de estados. Por outro lado as regras complexas exibem uma fenomenologia semelhante aos atratactores estranhos.

Stephen Wolfram divide os autómatos celulares em 4 classes, analisando a forma como evoluem a partir duma sequência finita aleatória de zeros e uns. Na classe 1 são incluidos os autómatos celulares para os quais o padrão estabiliza homogeneamente, por exemplo todas as células permanecem com uns, ou então com zeros. A segunda classe é constituida por autómatos em que os padrões degeneram em estruturas periódicas, os chamados ciclos limites. São da classe 3 os autómatos que criam padrões caóticos embora não aleatórios. Finalmente *Wolfram* inclui na classe 4 todos os autómatos que criam padrões complexos. O comportamento dos autómatos de cada uma destas classes tem consequências imediatas Podemos pensar no que acontecerá se modificarmos ligeiramente a configuração inicial. Para os autómatos da classe 1 isso é irrelevante o estado final a atingir será o mesmo, para a classe 2 o efeito é visível mas localiza-se junto à área onde a mudança ocorreu. Apenas nas classes 3 e 4 podemos ver a propagação da mudança através da evolução, sendo os autómatos da classe 4 mais sensíveis a pequenas perturbações que os da classe 3. Conjectura-se, por isso, que para autómatos da classe 4 qualquer conjectura sobre a evolução futura só poderá ser decidida atavés da própria evolução. Por esta razão apresentam-se estes autómatos como candidatos a estruturas mais simples capazes de computação universal.

Outra questão que se prende com os autómatos celulares é a possibilidade de serem ou não capazes de reversibilidade, isto é de serem ou não invertiveis. Sabemos que uma dada configuração terá na sua evolução temporal uma e uma só sucessora. No entanto existem autómatos para os quais uma dada configuração pode ser atingida a partir de diferentes configurações antecessoras no tempo. Uma condição necessária para a reversibilidade é pois que a lei de transição possa ser determinista nos dois sentidos (para a frente e para trás), só podendo haver um sucessor e um antecessor para cada configuração. Uma forma de criar reversibilidade nas regras foi inventada por *Fredkin* e aplicada por *Margolus*, a ideia chave é deixar que o próximo estado duma célula dependa apenas dos dois prévios estados no tempo dos seus vizinhos. O estado no tempo $(t+1)$ é portanto a diferença do estado no tempo t pelo estado no tempo $(t-1)$ e vice-versa o estado no tempo $(t-1)$ é a diferença entre os estados no tempo (t) e $(t+1)$. Nestes autómatos e por causa do determinismo bidireccional não poderão existir atractores.

Seguem-se imagens de evolução de alguns autómatos celulares mencionados.

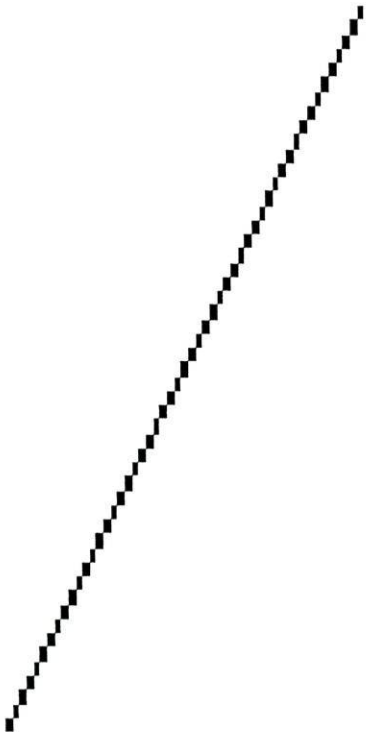
Comecemos pelas regras 128, 136, 160, 170, 192, 204, 240 e 250, regras que são de grande importância para o que vai seguir-se.

As primeiras imagens foram obtidas a partir dum ponto único e podemos varificar que todos eles ou "morrem" ou criam estruturas simples e estáveis, usando 50 iterações.

R=128

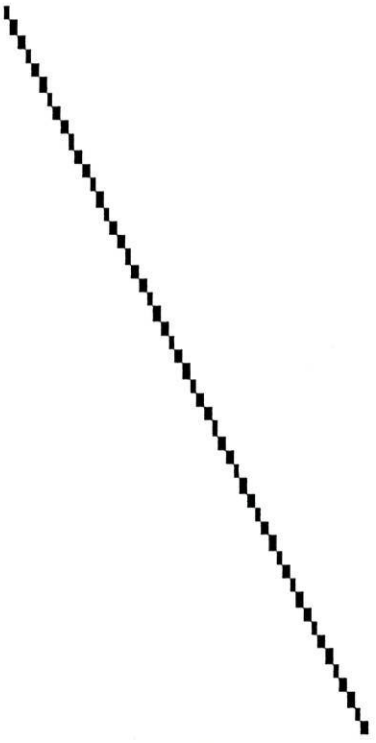
R=136

R=160

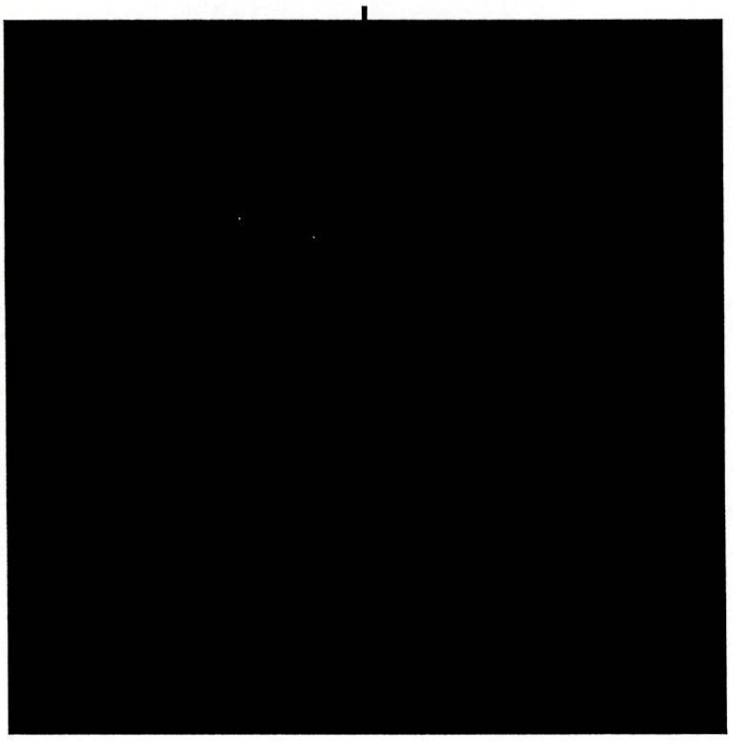


R=170

R=192
R=204



R=240



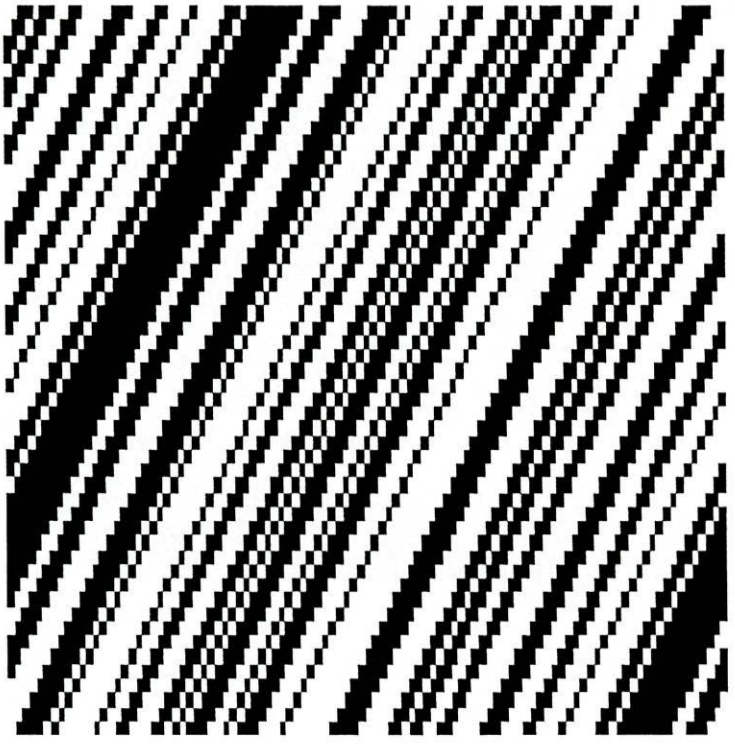
R=255

As imagens seguintes foram obtidos com os mesmos autómatos mas a partir duma sequência aleatória de zeros e uns. Apresentam estruturalmente o mesmo tipo de comportamento, ao fim do mesmo número de iteração.

R=128

R=136

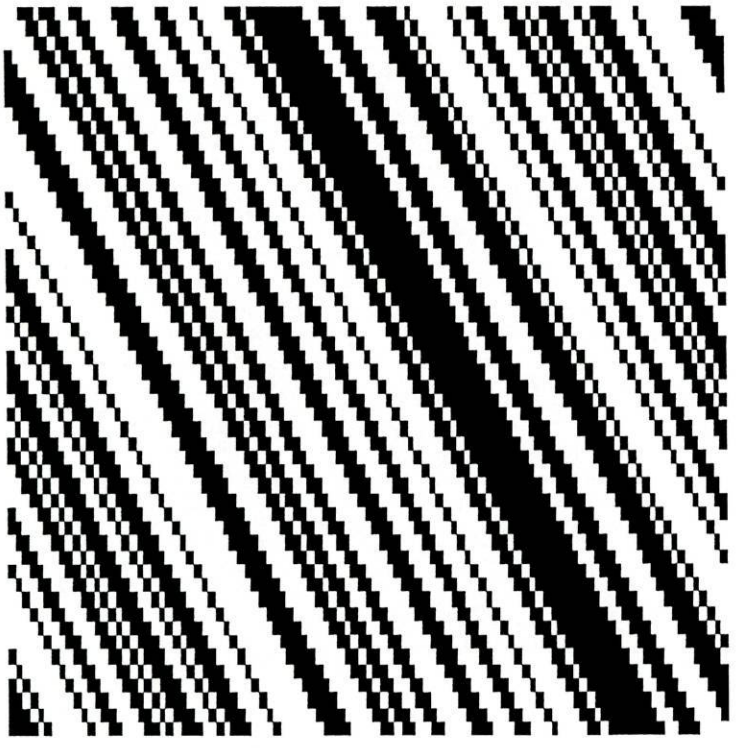
R=160



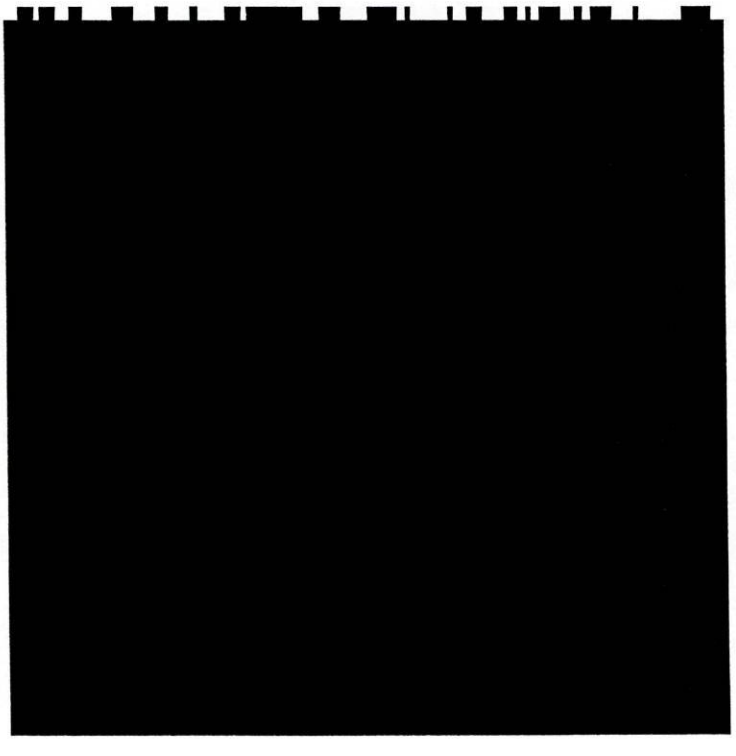
R=170

R=192

R=204

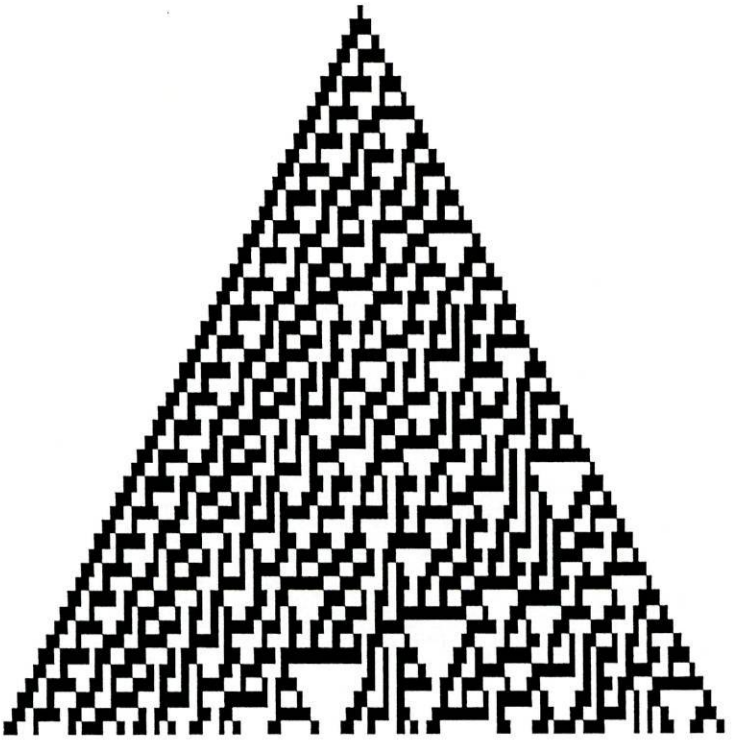


R=240

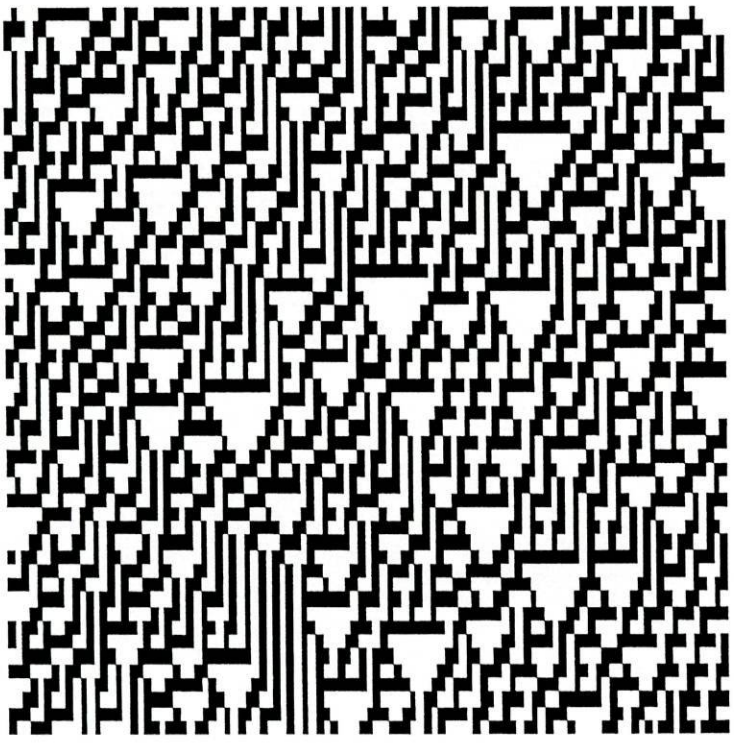


R=255

Por fim podemos ver a imagem do autómato celular 30 que pertence à classe 3 e tem a aparente inexplicável capacidade de gerar números pseudo-aleatórios. Começaremos com um ponto único e depois com a nossa sequência aleatória usada anteriormente.



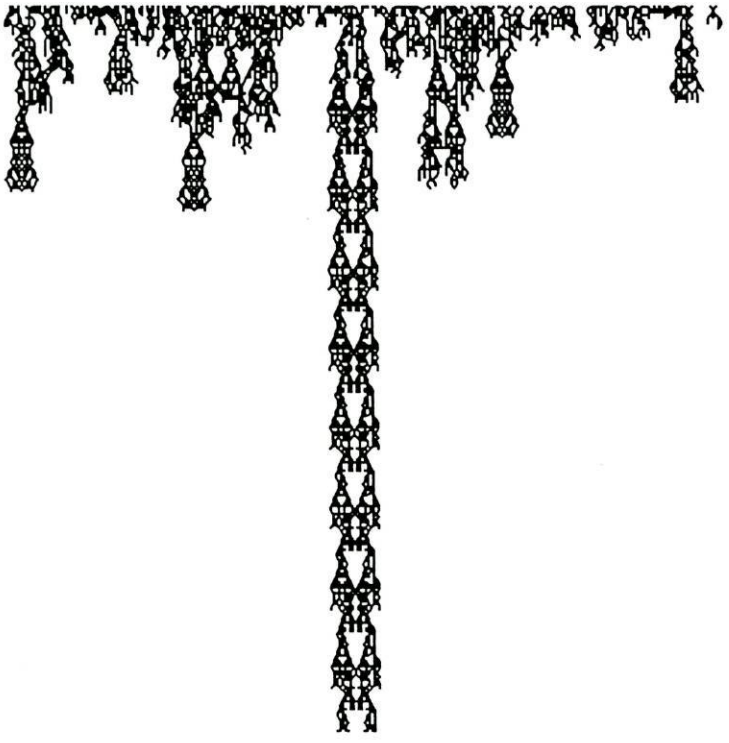
R=30



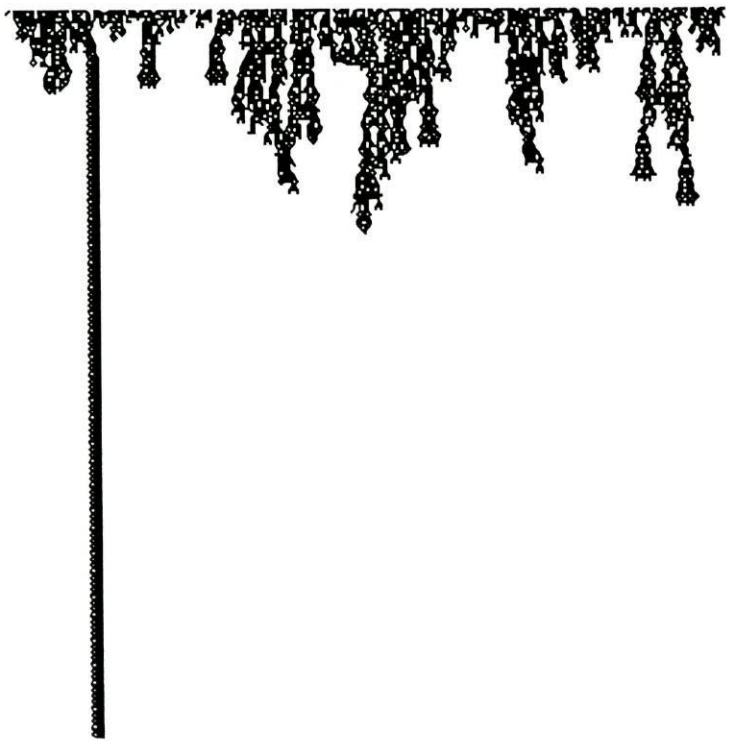
R=30

Para ilustrar a classe 4 escolhemos um autómato celular Booleano com comprimento de vizinhança 5 e assim definido; o centro da vizinhança evolui para 1 ou para zero dependendo de existirem 3 ou 4 células na sua vizinhança iguais a 1 ou não. É na regra totalista e podemos ver os padrões complexos que se geram a partir duma sequência aleatória.

Classe 4



Classe 4 (401 x 200)



Classe 4 (601 x 300)

3. GRUPOS LIVRES E AUTÓMATOS CELULARES

3.1. Introdução

No que se seguirá designaremos por AC(2,3) os 256 autómatos celulares unidimensionais Booleanos (cada célula apresenta-se sob dois estados, 0 e 1) e de vizinhança simétrica mínima (ou seja a célula x_i, situada no sítio i tem como vizinhança ela própria, e as células adjacentes x_{i-1} e x_{i+1}).

É nossa pretensão mostrar que AC(2,3) é um grupo livre abeliano com relações. O propósito da construção é tentar reduzir o estudo de AC(2,3) ao estudo dum conjunto mínimo de autómatos que de certa forma representam AC(2,3).

3.2. Alguns Resultados Relativos a Grupos Livres

Um grupo livre é uma estrutura que é construida a partir dum conjunto de elementos $\{a,b,c,\ldots\} \in \mathcal{A}$ chamadas as letras dum certo alfabeto. Quando juntamos várias letras por exemplo $aaa\ldots a$ obtemos uma sílaba que se representa por a^n (sendo n o número de vezes que "a" se repete. As palavras deste alfabeto são as sequências ordenadas de sílabas obtidas por simples concatenação. Para efeito de construção designa-se por a^0 a palavra vazia (sem sílabas) a que também daremos a representação 1. Neste conjunto de palavas define-se o produto de palavras como a concatenação de palavras, à semelhança do que se faz com as sílabas para obter a palavra.

Ex:

sejam $p = a^n b^m c^n$ e $q = b^s c^t$ duas palavras. O seu produto $p \bullet q$ será $p \bullet q = a^n b^m c^n b^s c^t$.

Este conjunto representado por $W(\mathcal{A})$ tem a estrutura de semi-grupo. Se definirmos em $W(\mathcal{A})$ as duas seguintes relações:
sejam W_1 e W_2 duas palavras

$$(1) \quad W_1 a^0 W_2 = W_1 W_2$$

$$(2) \quad W_1 a^n a^m W_2 = W_1 a^{n+m} W_2$$

Verificamos que definem em $W(\mathcal{A})$ uma relação de equivalência R. O conjunto cociente $W(\mathcal{A})/R = F(\mathcal{A})$ herda a multiplicação nas classes equivalentes, isto é:
sendo $[u]$ e $[v]$ duas classes de palavras equivalentes respectivamente a "u" e a "v" então $[u]\cdot[v]=[u\cdot v]$.

$F(\mathcal{A})$ é assim um grupo. A razão desta afirmação está no facto de ser possível definir para cada classe $[u]$ na classe inversa $[u]^{-1}$ de modo que $[u]\cdot[u]^{-1}=[1]$, $[u]^{-1}$ é simplesmente a classe das palavras equivalentes obtidas da palavra u por ordem inversa das sílabas de u e troca do sinal do expoente em cada sílaba, isto é, sendo $[u]=a^3b^{-5}c^0d^{-2}$ $[u]^{-1}=d^2c^0b^5a^{-3}$. A este grupo cociente $F(\mathcal{A})$ designamos por grupo livre de base $\mathcal{A}$.

Se considerarmos um grupo qualquer G e um subconjunto $E \subset G$ à intersecção de todos os sub-grupos de G que contém E chamamos o grupo livre gerado por E que é necessariamente um sub-grupo de G. Os elementos deste grupo são os produtos da forma

$$g_1^{n_1} g_2^{n_2} \ldots g_k^{n_k} \quad \text{onde} \quad g_i \in E \quad \forall_i = 1,k \quad \text{e} \quad n_i \in Z \quad \forall_i = 1,k$$

Quando este grupo coincide com o próprio G, dizemos que E é o conjunto de geradores de G e podemos apresentar um resultado importante:

- Qualquer homomorfismo de G num grupo qualquer H fica determinado se conhecermos a sua expressão no conjunto E. A razão é trivial. Sendo f esse homomorfismo

$$f\left(g_1^{n_1} g_2^{n_2} \ldots g_k^{n_k}\right) = f^{n_1}(g_1) \bullet f^{n_2}(g_2) \ldots f^{n_k}(g_k)$$

dito de forma mais poderosa, qualquer aplicação $\varnothing: E \to M$ extende-se a um homomorfismo de $G \to M$.

Daqui resulta o facto mais importante da teoria de grupos livres:

Proposição 1: qualquer grupo é imagem homomorfica dalgum grupo livre.

Esta proposição corresponde, dentro da teoria dos grupos, ao que os sistemas de coordenadas representam na Geometria Cartesiana. Qualquer grupo pode ser estudado à custa dum certo "referencial" que é um grupo livre.

A veracidade da proposição resulta imediatamente do seguinte: seja E um conjunto de G e seja $F(\mathcal{A})$ o grupo livre no alfabeto $\mathcal{A}$ cuja cardinalidade é igual ou superior à cardinalidade de E $\left(\#E \leq \#\mathcal{A}\right)$. Seja $\lambda: \mathcal{A} \to E$ uma aplicação qualquer cuja imagem é E. Como $\mathcal{A}$ é uma base livre para $F(\mathcal{A})$, λ extende-se a um homomorfismo de $F(\mathcal{A})$ em G ou seja

$$\begin{array}{ccccc} & & \lambda & & \\ & \mathcal{A} & \rightarrow & E & \\ p & \downarrow & & \downarrow & i \\ & F(\mathcal{A}) & \rightarrow & G & \\ & & \varphi & & \end{array}$$

onde

p é a projecção canónica no grupo cociente $F(\mathcal{A})$;

i é a inclusão;

λ a aplicação considerada;

φ fica definido pela comutatividade do rectângulo

$$\varphi op = io\lambda$$

De fato, para um dado grupo, não são só os geradores os elementos importantes para a sua descrição. Por exemplo se tomarmos o grupo gerado pelos elementos $\{a,b\}$ com a seguinte operação, definida pela tabela

	1	a	b
1	1	a	b
a	a	b	1
b	b	1	a

facilmente reparamos que $b = a^2$ e portanto $a^3 = 1$, ou seja, este grupo só tem um gerador $\{a\}$, ou ainda este grupo é um grupo ciclo de ordem três $\{a, a^2, 1\}$. Dizer isso ou dizer que este grupo é o grupo com dois geradores $\{a,b\}$ e a relação $a^2 = b$ é basicamente a mesma coisa. Repare-se que este grupo não é um grupo de base $\{a\}$, esse grupo seria simplesmente o grupo das potências inteiras de base a ou seja $\{a^n, n \in Z\}$. Este exemplo levou a que para além dos geradores dum grupo $\{g_1, \ldots g_k\}$ se considerem possíveis relações existentes entre estes geradores, que são equações do tipo

$$f_1(g_1 \ldots g_k) = 1, \quad f_2(g_1, \ldots g_k) = 1, \quad \ldots, f_l(g_1 \ldots g_k) = 1$$

Voltemos aos grupos livres. Seja então um grupo F, grupo de base $x_1, x_2, x_3, \ldots x_e$ (os geradores poderão não ser finitos, embora nesta exposição se presuma que sim dado o fim que temos em vista) e aplicação φ injectiva aplica os $x_1, x_2, \ldots$ nos geradores de $G, g_1, g_2, \ldots g_k$.

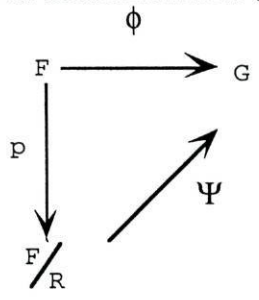
Sabemos já que esta aplicação φ se prolonga a um homomorfismo Ø de F em G definido por

$$g_i = \varnothing x_i \quad \forall_i.$$

A cada relação $f_j(g_1,g_2,\ldots)=1$ corresponde na relação do tipo $f_j(x_1,x_2,\ldots)=r_j$ obtida simplesmente substituindo cada g_i por $\varnothing x_i$ (deveriamos usar dois simbolos diferentes para os f_j. Não o fazemos para não sobrecarregar a notação, de facto são aplicações distintas (pois o domínio é distinto).

Aos elementos $r_1,r_2,r_3,\ldots$ chamamos os relatores do grupo. Estes relatores geram um subgrupo normal de F, R, denominado a consequência dos r_j.

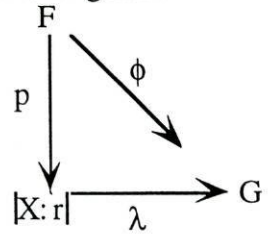
Retomando ao homomorfismo Ø fica claro que no triângulo



Ψ é um isomorfismo de F/R em G, simplesmente porque com as devidas identificações R é o núcleo do homomorfismo Ø

Este grupo cociente F/R representa-se habitualmente por $|X:r|$ onde X são os geradores e r os relatores.

Chamamos uma pré-representação do grupo G ao par $|X:r|$ e isomorfismo λ, de tal forma que comute o diagrama



onde F é um grupo livre G a sua imagem homomorfa e $|X:r|$ o grupo cociente atrás definido.

Utilizamos as designações de finitamente gerado se o conjunto de geradores é finito e finitamente relacionado se o conjunto dos relatores é finito.

Apenas uma observação. No exemplo anterior do grupo gerado por $\{a,b\}$ falamos da relação $a^2=b$ que não é de forma alguma do tipo $f_1(g_1\ldots g_k)=1$, no entanto se considerarmos $a^2=b \Leftrightarrow a^2b^{-1}=1$ fica claro que a relação é do tipo $f(a,b)=1$ com $f(a,b)=a^2b^{-1}$.

Quando tomamos a operação, no grupo livre, comutativa podemos falar em grupos abelianos livres, embora se deveria entender por grupo abeliano livre o abelianizado dum grupo livre, isto é um grupo F/R obtido do grupo livre e onde o sub-grupo dos relatores é o comutador do grupo, isto é as consequências das relações do tipo

$$g_ig_j=g_jg_i \;\forall_{i,j} \quad \Leftrightarrow \quad g_i^{-1}g_j^{-1}g_ig_j=1 \;\forall_{i,j}$$

Na nossa construção usaremos um subterfúgio para escapar a este pesado formalismo, que se baseia na proposição.

Proposição 2: Se num grupo G, $a^2 = 1$ para qualquer elemento G, então o grupo é abeliano (ou seja a operação é comutativa).

É imediato:

$$a^2 = 1 \,\forall_{a \in G} \Rightarrow (a,b)^2 = 1 \,\forall_{a,b \in G} \Rightarrow abab = 1$$

como também $a^2 = 1 \Rightarrow a = a^{-1}$ teremos

$$abab = 1 \Leftrightarrow aba^{-1}b^{-1} = 1 \Leftrightarrow ab = ba \,\forall_{a,b \in G}$$

3.3. Construção dum Grupo Livre com Relatores em AC(2,3)

Ficou já visto que para qualquer autómato celular, entendido como aplicação do cubo cartesiano de $B = \{0,1\}$ em B, essa aplicação se representa univocamente na forma:

$$f(X,Y,Z) = \sum g(\alpha_1,\alpha_2,\alpha_3) X^{\alpha_1} Y^{\alpha_2} Z^{\alpha_3}$$

onde $g(\alpha_1,\alpha_2,\alpha_3) \in \{0,1\}$ e $X^{\alpha_i} = \begin{cases} X & \text{se} \quad \alpha_i = 1 \\ 1 & \text{se} \quad \alpha_i = 0 \end{cases}$ por exemplo a regra 146 representa-se por $f_{146}(X,Y,Z) = XYZ \oplus XY \oplus YZ \oplus X \oplus Z$

Se considerarmos as regras

$$\begin{array}{lll} R_{255} = 1 & R_{170} = Z & R_{136} = YZ \\ R_{240} = X & R_{192} = XY & R_{128} = XYZ \\ R_{204} = Y & R_{160} = XZ & \end{array}$$

aquilo que foi anteriormente dito reduz-se a afirmar que uma dada regra pode ser obtida por soma Booleana ($\oplus$) dum número de parcelas que é um subconjunto destas 8 regras, ou ainda, na linguagem que estamos a adoptar que estas 8 regras geram um grupo livre.

Designando por

$$\begin{array}{lll} g_1 = R_{255} = 1 & g_4 = R_{170} = Z & g_7 = R_{136} = YZ \\ g_2 = R_{240} = X & g_5 = R_{192} = XY & g_8 = R_{128} = XYZ \\ g_3 = R_{204} = Y & g_6 = R_{160} = XZ & \end{array}$$

e ainda por $1 = R_0 = 0$ e por

$$g_i g_j = g_i \oplus g_j$$

Obtemos um grupo livre F de base

$$\{g_1, g_2, g_3, g_4, g_5, g_6, g_7, g_8\}$$

Sabemos da algebra Booleana que $a \oplus a = 0 \quad \forall_a$. esta relação induz neste grupo livre um conjunto de relatores:

$$r_1 = g_1 g_1 \quad r_4 = g_4 g_4 \quad r_7 = g_7 g_7$$
$$r_2 = g_2 g_2 \quad r_5 = g_5 g_5 \quad r_8 = g_8 g_8$$
$$r_3 = g_3 g_3 \quad r_6 = g_6 g_6$$

cuja consequência R origina o grupo cociente $F/R = G$ grupo abliano livre com relatores

$$G = |g_i : r_i| \quad i = 1,8$$

De facto estes relatores, pelo que foi dito na proposição 2, induzem um grupo abeliano. Para efeitos da exposição omitiremos que o grupo é abeliano livre pelo simples facto que é a propriedade de ser grupo livre que nos interessa mais.

3.4. Anel dum grupo

A cada grupo G é possível associar um anel KG, à custa dum anel K de inteiros, com a seguinte definição

$$KG = \{v: G \to k \quad \text{com} \quad v(g) = 0 \; g \in G, \quad \text{excepto para uma número finito de elementos de } G\}$$

$$v_1 + v_2: \quad G \to k$$
$$g \to v_1(g) + v_2(g)$$

$$v_i \cdot v_2 : G \to k$$
$$g \to \sum_{h \in G} (v_1 h) \cdot \left(v_2 h^{-1} g\right)$$

esta soma não traz problemas porque o número de parcelas não nulas é finito.

É trivial que $(KG, +.0)$ é um anel. Em relação ao par (KG,+)

$$0v : G \to k \qquad \text{funcionar como elemento n}$$
$$g \to 0 \quad \text{(zero do anel)}$$

e

$$-v : G \to k \qquad \text{como o inverso aditivo do}$$
$$g \to -v(g)$$
elemento $v : G \to k$
$$g \to v(g)$$

trivialmente se verifica que $v_1 + v_2 = v_2 + v_1$ e $(v_1 + v_2) + v_3 = v_1 + (v_2 + v_3)$

KG é portanto um grupo abeliano. A associatividade de $(KG, \bullet)$ é uma questão técnica. $(v_1 \bullet v_2) \bullet v_3 = v_1 \bullet (v_2 \bullet v_3)$.

Basta notar que $(v_1v_2)v_3g = v_1(v_2v_3)g \quad \forall_{g\in G}$.

Calculemos o primeiro membro

$$(v_1v_2)v_3g = \sum_{h\in G}(v_1v_2h)\cdot\left(v_3h^{-1}g\right)$$

$$= \sum_{h\in G}\left[\sum_{f\in G}(v_1f)\cdot\left(v_2f^{-1}h\right)\right]\left(v_3h^{-1}g\right)$$

$$= \sum_{h,f\in G}(v_1f)\left(v_2f^{-1}h\right)\left(v_3h^{-1}g\right)$$

quanto ao segundo membro

$$v_1(v_2v_3)g = \sum_{h_1\in G}(v_1h_1)\left(v_2v_3h_1^{-1}g\right)$$

$$= \sum_{h_1\in G}(v_1h_1)\left[\sum_{f_1\in G}(v_2h_1)\left(v_3f_1^{-1}h_1^{-1}g\right)\right]$$

$$= \sum_{h_1,f_1\in G}(v_1h_1)(v_2h_1)\left(v_3f_1^{-1}h_1^{-1}g\right)$$

Como h e f percorrem G bem como h_1 e f_1, fazendo

$$\begin{cases} f = h_1 \\ f^{-1}h = f_1 \end{cases} \qquad \text{temos} \qquad \begin{cases} f = h_1 \\ h = h_1f_1 \end{cases}$$

donde

$$f_1^{-1}h_1^{-1}g = (h_1f_1)^{-1}g = \left(f^{-1}h\right)^{-1}g = h^{-1}g$$

e a propriedade fica verificada. KG é de facto um anel. De acordo com as convenções utilizadas num anel, fica bem definido o termo nv com $n \in Z$ será a aplicação

$$(nv)g = n(vg)$$
$$= (v + v + v \ldots + v)g \qquad (n \text{ parcelas})$$
$$= vg + vg + \ldots + vg \qquad (n \text{ parcelas})$$

Consideremos agora um homomorfismo assim definido

$$G \xrightarrow{\Psi} KG$$
$$g \to g^*$$

onde

$$g^*: G \to K$$

$$h \to \begin{cases} 1 & \text{se} \quad h = g \\ 0 & \text{se} \quad h \neq g \end{cases}$$

(1º) Ψ está bem definida

se $g = \overline{g}$ temos atendendo à definição g^*

$$g * h = 1 \quad \text{se} \quad h = g$$
$$g * h = 0 \quad \text{se} \quad h \neq g$$

como $g = \overline{g}$

$$g * h = 1 \quad \text{se} \quad h = \overline{g} \qquad \text{portanto} \qquad g^* = \overline{g}\,^*$$
$$g * h = 0 \quad \text{se} \quad h \neq \overline{g}$$

(2º) Ψ é injectiva

$$\Psi(g) = \Psi(\overline{g}) \Rightarrow g^* = \overline{g}\,^*$$

ou seja $g * h = \overline{g} * h \quad \forall_{h \in G}$

para $g * h = 1$ e $\overline{g} * h = 1$ temos $g = h$ e $\overline{g} = h$ donde $g = \overline{g}$

(3º) Ψ preserva produtos, isto é Ψ é um homomorfismo de G em KG

$$\Psi(g \cdot \overline{g}) = (g \cdot \overline{g})^*$$

onde

$$(g\overline{g})^*: G \to K$$

$$h \to \begin{cases} 1 & \text{se} \quad h = g \cdot \overline{g} \\ 0 & \text{se} \quad h \neq g \cdot \overline{g} \end{cases}$$

$$\Psi(g) = g^* \qquad g^*: G \to K$$

$$h \to \begin{cases} 1 & \text{se} \quad h = g \\ 0 & \text{se} \quad h \neq g \end{cases}$$

$$\Psi(\overline{g}) = \overline{g}\,^* \qquad \overline{g}^*: G \to K$$

$$h \to \begin{cases} 1 & \text{se} \quad h = \overline{g} \\ 0 & \text{se} \quad h \neq \overline{g} \end{cases}$$

se fizermos o produto $g^* \cdot \overline{g}\,^*$ teremos

$$(g^* \cdot \overline{g}\,^*)h = \sum_{f \in G} (g^* f)\left(\overline{g}^* f^{-1} h\right)$$

este somatório só é igual quando

$$g * f = 1 \text{ e } \overline{g} * f^{-1}h = 1 \text{ ou seja } f = g \text{ e } f^{-1}h = \overline{g}$$

"multiplicando" ambos os membros

$$f^{-1}h = g\overline{g} \Rightarrow h = g\overline{g}$$

portanto

$$g * \cdot \overline{g} *: G \to K$$

$$h \to \begin{cases} 1 & \text{se } h = g\overline{g} \\ 0 & \text{se } h \neq g\overline{g} \end{cases}$$

comparando as definições de $(g\overline{g})*$ e $g * \cdot \overline{g} *$ verificamos que são aplicações idênticas, portanto

$$\Psi(g \cdot \overline{g}) = \Psi(g) \cdot \Psi(\overline{g})$$

Das afirmações (1°), (2°) e (3°) fica provado que

$g \to g *$ é um isomorfismo sobre a imagem

Ao elemento neutro $e \in G$ corresponderá por este isomorfismo o elemento $e*$ que é o elemento unidade do anel KG.

A importância deste isomorfismo reside no facto de ser possível fazer uma representação mais objectiva e mais manejável dos elementos de KG.

Seja $v \in KG$ um elemento não nulo e sejam $g_1 g_2, \ldots g_k \quad k \geq 1$ elementos de G para os quais $v(g_i) \neq 0$, seja $n_i = v(g_i) \quad i = 1,k$ então

$$v = n_i g_i * + \ldots + n_k g_k *$$

basta calcular as aplicações de cada membro nos elementos $g_1, g_2, \ldots g_k$.

É deste facto que resulta a afirmação anterior que traduz o facto da imagem de g pelo homomorfismo $g \to g *$ gerar o grupo aditivo KG. Assim é possível escrever os elementos de KG como combinações inteiros finitos de elementos de G.

Uma consequência imediata é que sendo G um grupo comutativo também KG o é e vice-versa.

Com esta identificação é possível estabelecer a seguinte proposição, de grande importância.

Proposição 3: Qualquer homomorfismo de G num grupo abeliano$A$ tem uma única extensão como homomorfismo ao anel KG

$$\varnothing: KG \to A$$

É quase uma consequência imediata de tudo o que foi dito até aqui.

Em primeiro lugar estabeleça-se que $\varnothing 0 = 0$

Como cada elemento não nulo de KG tem uma expressão única do tipo

$$n_1g_1+\ldots+n_kg_k \quad n_i \neq 0 \quad i=1,k \text{ para } g_i \neq g_j \quad \forall_{i,j}$$

para obter a extensão basta que

$$\varnothing\left(n_1g_1+\ldots+n_kg_k\right)=n_1\varnothing g_1+\ldots+n_k\varnothing g_k$$

Se queremos uma extensão de $\varnothing$ que seja homomorfismo esta igualdade terá que ser válida para quaisquer g_i e quaisquer n_i donde a unicidade fica garantida. Resta-nos verificar que $\varnothing$ assim definida preserva os produtos nos respectivos aneis. Também isso é imediato

$$\varnothing\left(\sum_i n_ig_i \cdot \sum_j n_j'g_j'\right)$$

$$=\varnothing\left(\sum_{i,j} n_in_j'g_ig_j'\right)$$

$$=\sum_{i,j} n_in_j'\varnothing\left(g_ig_j'\right) \qquad \text{por definição de } \varnothing$$

$$=\sum_{i,j} n_in_j'\varnothing(g_i)\varnothing\left(g_j'\right) \qquad \text{porque } \varnothing \text{ é homomorfismo em G}$$

$$=\sum_i n_i\varnothing g_i \cdot \sum_j n_j'\varnothing g_j'$$

$$=\varnothing\left(\sum_i n_ig_i\right)\cdot\varnothing\left(\sum_j n_j'g_j'\right) \qquad \text{novamente por definição}$$

Um corolário imediato desta proposição é o seguinte

Corolário: Qualquer homomorfismo entre grupos G e G'

$$\varnothing: G \to G'$$

tem uma extensão única as respectivos aneís de grupo KG e KG'

$$\tilde{\varnothing}: KG \to KG'$$

Estamos em condições de definir dois homomorfismo de grande importância.

O Abelianizador:

Considerando $a: G \to {}^{G}\!/_{[G,G]}$ onde $[G,G]$ é o comutador de G.

O abelianizador será a extensão de G a KG.

O Trivializador:

Consideremos para cada grupo G o homomorfismo $t: G \to K$ definido por $t(g)=1 \quad \forall_{g\in G}$.

O trivializador é a única extensão de G ao anel KG

$$t: KG \to K$$

por definição $t\left(\sum n_i g_i\right) = \sum n_i t(g_i) = \sum n_i$

3.5. Construção do Anel de Grupo em AC(2,3)

Foi definido AC(2,3) como o grupo $G = |g_i : r_i| \quad i = 1,8$. Uma vez que estamos a tratar de autómatos celulares Booleanos o natural é tomarmos para anel K o anel $(Z_2, +, \bullet)$ anel cociente $Z/2'Z$ com as operações + e • tomadas módulo 2.

$Z_2 G$ define-se de modo natural como sendo o conjunto

$$\left\{v: G \to Z_2 \quad \text{com} \quad vg_i = 0 \quad \text{ou} \quad vg_i = 1 \quad \forall_{g_i \in G}\right\}$$

Como este conjunto é finito é trivial garantir que $vg = 0$ exepto para um número finito de elementos de G.

A adição $v_1 + v_2$ não carece de observações particulares. Relativamente ao produto $v_1 v_2$ uma simplificação pode ser feita

$$v_1 \cdot v_2 : G \to Z_2$$

$$g \to \sum_{\substack{i=1 \\ h_i \in G}}^{8} (v_1 h_i)\left(v_2 h_i^{-1} g\right)$$

Como $h_i^{-1} = h_i \quad \forall_{h_i \in G}$ a expressão do produto vem

$$\sum_{i=1}^{8} (v_1 h_i)(v_2 h_i g)$$

4. CÁLCULO EM GRUPOS LIVRES E SUA APLICAÇÃO AO GRUPO AC(2,3)

4.1. Introdução

Nas páginas que vão seguir-se, será desenvolvida uma técnica com vista ao cálculo de invariantes num grupo livre e sua consequente aplicação ao grupo AC(2,3). O interesse desses invariantes, que no caso concreto é uma sequência de Ideais principais do anel de grupo, reside no facto dessas invariantes caracterizarem o grupo a menos dum isomorfismo. Qualquer outro grupo com a mesma sequência de Ideais principais de KG poderá ser tomado como uma interpretação de AC(2,3).

4.2. Definição de Derivada

Dá-se o nome de derivada num anel de grupo a toda a aplicação $D: KG \to KG$ com as seguintes propriedades

1°) $D(v_1 + v_2) = Dv_1 + Dv_2$

2°) $D(v_1 v_2) = Dv_1 t(v_2) + v_1 Dv_2$

onde t é o trivializador

O reflexo de D nos geradores de G é

$$D(g_1g_2) = Dg_1 + g_1Dg_2 \text{ uma vez que } t(g_i) = 1 \quad \forall_{g_i \in G}$$

Por este facto é também possível definir a derivada em KG com a única extensão linear a KG da aplicação em G assim definida

$$G \to G$$
$$g \to Dg \qquad \text{com a propriedade} \qquad D(g_1g_2) = Dg_1 + g_1Dg_2$$

Sabemos que esta extensão existe e fica completamente caracterizada pelos valores que toma nos elementos de G.

Como exemplo trivial de derivada temos a aplicação constante nula

$$JG \to JG$$
$$g \to 0 \quad (g \in G)$$

também a aplicação $G \to G$ induz uma derivada, dado que $D(g_1g_2) = g_1g_2 - 1$
$g \to g - 1$

$$Dg_1 + g_1Dg_2 = g_1 - 1 + g_1(g_2 - 1) = g_1 - 1 + g_1g_2 - g_1 = g_1g_2 - 1$$

Temos ainda possibilidade de construir novas derivadas a partir de derivadas já conhecidas. Por exemplo, sendo D e D' duas derivadas em KG e v_0 um elemento qualquer de KG então

(1) $(D + D')v = Dv + D'v$

e

(2) $(D_0v_0)v = (Dv)v_0$

são duas novas derivadas. A justificação resume-se a meros, calculos todos eles imediatos

$$\begin{aligned}(1)\quad (D + D')(v_1 + v_2) &= D(v_1 + v_2) + D'(v_1 + v_2)\\ &= Dv_1 + Dv_2 + D'v_1 + D'v_2\\ &= (D + D')v_1 + (D + D')v_2\end{aligned}$$

e também

$$\begin{aligned}(D + D')(v_1v_2) &= Dv_1v_2 + D'v_1v_2\\ &= (Dv_1tv_2 + v_1Dv_2) + (Dv_1 + tv_2 + v_1D'v_2)\\ &= Dv_1tv_2 + D'v_1tv_2 + v_1(D + D')v_2\\ &= (D + D')v_1tv_2 + v_1(D + D')v_2\end{aligned}$$

Para a outra derivada

$$(2)\quad (D_0v_0)(v_1+v_2)=\left[D(v_1+v_2)\right]v_0$$
$$=(Dv_1+Dv_2)v_0=(Dv_1)v_0+(Dv_2)v_0$$
$$=(D_0v_0)v_1+(D_0v_0)v_2$$

e também

$$(D_0v_0)(v_1v_2)=(Dv_1v_2)v_0$$
$$=\left[Dv_1tv_2+v_1Dv_2\right]v_0$$
$$=(Dv_1tv_2)v_0+(v_1Dv_2)v_0$$
$$=(Dv_1)v_0tv_2+v_1(Dv_2)v_0$$
$$=(D_0v_0)v_1tv_2+v_1(D_0v_0)v_2$$

Para aspectos práticos de cálculo apresentemos de seguida quatro propriedades de que gozam as derivadas.

Propriedade 1 $D\left(\sum ng_i\right)=\sum nDg_i$

A justificação assenta inteiramente na linearidade aditiva de D e na definição de ng_i como sendo uma soma de n parcelas todas iguais.

Propriedade 2 $Dn=0$

Na verdade esta igualdade poderá causar alguma perplexidade uma vez que "n" não é um elemento de KG. Entenda-se "n" como sendo a soma

$$n=1+1+\ldots+1$$

"1" o elemento unidade com n parcelas e do anel KG.

Em primeiro lugar vejamos que $D1=0$:

como $1=1.1$

$$D1=D1\cdot 1$$
$$D1=D1t(1)+1D1$$
$$D1=D1t(1)+D1$$

donde $D1t(1)=0$ e como $t(1)=1$ vem $D1=0$ usando este facto e a propriedade anterior

$$Dn=D(1+1+\ldots+1)=D1+D1+\ldots+D1=0+0\ldots+0=0$$

Propriedade 3 $Dg^{-1}=-g^{1}Dg \quad \forall_{g\in G}$

resulta de $g\bullet g^{-1}=1$

$$D\left(gg^{-1}\right)=D_1\Leftrightarrow Dg+gDg^{-1}=0$$

donde $gDg^{-1}=-Dg\Leftrightarrow Dg^{-1}=-g^{-1}Dg$

Propriedade 4 Diz-nos como derivar $g^n(n\in Z)$

Antes disso definemos o elemento de G

$$\frac{g^n-1}{g-1}=\begin{cases}0 & \text{se} \quad n=0\\ \sum_{i=0}^{n-1} g^i & \text{se} \quad n>0\\ -\sum_{i=n}^{-1} g^i & \text{se} \quad n<0\end{cases}$$

com esta definição

$$Dg^n=\frac{g^n-1}{g-1}Dg \quad (g\neq 1) \quad \forall_{g\in G}$$

$$\forall_{n\in Z}$$

A justificação é feita para $n \in N$ por indução matemática:

para $n=1$

$$Dg^1=Dg \quad \frac{g^1-1}{g-1}Dg=\frac{g-1}{g-1}Dg=1\cdot Dg=Dg$$

está verificado

para $n+1$

$$\begin{aligned}Dg^{n+1}&=Dg^n\cdot g=Dg^n+g^nDg\\ &=\frac{g^n-1}{g-1}Dg+g^nDg \qquad \text{por hipótese de indução}\\ &=\sum_{i=1}^{n-1}g^iDg+g^nDg \qquad \text{por definição de } \frac{g^n-1}{g-1}\\ &=\sum_{i=1}^{n}g_iDg=\frac{g^{n+1}-1}{g-1}Dg\end{aligned}$$

e temos assim provada a formula da derivada para potências de expoente inteiro positivo. Para $n=0$ resulta imediatamente que, $Dg^0=D1=0$ e

$$\frac{g^0-1}{g-1}Dg=\frac{1-1}{g-1}Dg=\frac{0}{g-1}Dg=0Dg=0,$$

para $n-1 \quad Dg^{-1}=-g^{-1}Dg$

$$\frac{g^{-1}-1}{g-1}Dg=-\sum_{i=-1}^{-1}g^iDg=-g^{-1}DG$$

finalmente para $n<0$ basta reparar que $n=-m$ com $m\in N$ e portanto

$$Dg^n = Dg^{-m} = D\left(g^m\right)^{-1}$$

$$= -\left(g^m\right)^{-1} \cdot Dg^m \qquad \text{propriedade 3}$$

$$= -g^{-m} \cdot \frac{g^m - 1}{g-1} Dg \qquad \text{propriedade 4 para expoentes inteiros positivos}$$

$$= \frac{-g^{-m} \cdot g^m + g^{-m}}{g-1} Dg = \frac{g^{-m} - 1}{g-1} Dg = \frac{g^n - 1}{g-1} Dg$$

e fica a propriedade 4 provada para qualquer expoente inteiro.

Como qualquer derivada em KG é determinada pelos valores que toma nos geradores de G estas quatro propriedades bastam para o cálculo de derivadas no anel KG.

Com alguma semelhança entre o que acontece em R^n, onde se pode definir o que se entende por função derivada e depois por derivada parcial, num grupo livre existe uma única derivada D_j que se representará por $\frac{\partial}{\partial x_j}$ com a propriedade de $\frac{\partial x_i}{\partial x_j} = \delta_{i_j}$ (simbolo de *Kronecker*) onde x_i e x_j são os geradores do grupo livre.

4.3. Construção de Derivadas num Grupo Livre Usando os Geradores

Consideramos um grupo livre designado por F cuja base de geradores é o conjunto $\{x_1, x_2, \ldots\}$.

Sendo K um anel, sabemos já que os elementos de KF (anel de grupos) são as somas finitas de produtos finitos dos elementos $x_1, x_2, \ldots$.

É nossa intenção associar a cada x_i (gerador) uma derivada $\frac{\partial}{\partial x_i}$ com a propriedade atrás mencionada. A unicidade resultará do facto de conhecidos os resultados de $\frac{\partial}{\partial x_i}$ no conjunto de geradores de F ficar completamente determinado o comportamento de $\frac{\partial}{\partial x_i}$ no anel KF.

Vamos agora proceder à sua construção. Para isso tomemos um conjunto qualquer $A = \{a_1, a_2, \ldots\}$ em correspondência unívoca com os geradores $x_1, x_2, \ldots$ através duma aplicação θ:

$$a_i \xrightarrow{\theta} x_i$$

Do que já sabemos é possível estender θ a uma aplicação do semi-grupo $W(A)$ das palavras do alfabeto A, no grupo livre F, de forma a preservar os "produtos".

Tomando um elemento x_j qualquer definamos na aplicação

$$\Lambda_j : W(A) \to KF$$

da seguinte forma

$$\begin{cases} \Lambda_j 1 = 0 \qquad (1 \text{ é a palavra vazia}) \\ \Lambda_j a_i^n = \dfrac{x_i^n - 1}{x_i - 1}\delta_{ij} \\ \Lambda_j\left(a_i^n \cdot a\right) = \Lambda_j a_i^n + x_i^n \Lambda_j a \qquad (a \in W(A)) \end{cases}$$

Esta aplicação induzirá em KF uma derivada que designaremos por D_j ou $\dfrac{\partial}{\partial x_j}$.

A nossa primeira observação é que

$$(E_1) \quad \Lambda_j(ab) = \Lambda_j a + \theta a \cdot \Lambda_j b, \quad a,b \in W(A)$$

A demonstração é feita por indução sobre o número de sílabas em ab.

Sendo a a palavra vazia, o resultado é imediato

$$\Lambda_j(1 \cdot b) = \Lambda_j(1) + \theta 1 \cdot \Lambda_j b$$

em qualquer dos membros o resultado é $\Lambda_j b$.

Consideremos agora que "a" contém pelo menos uma sílaba, ou seja $a = a_i^n c$

$$\begin{aligned} &\Lambda_j(a,b) = \Lambda_j\left(a_i^n \cdot cb\right) \\ &= \Lambda_j a_i^n + x_i^n \Lambda_j(c,b) \qquad \text{pela definição de } \Lambda_j \\ &= \Lambda_j a_i^n + x_i^n\left[\Lambda_j c + \theta c \cdot \Lambda_j b\right] \qquad \text{por hipótese de indução} \\ &= \Lambda_j a_i^n + x_i^n \Lambda_j c + x_i^n \theta c \Lambda_j b \\ &= \Lambda_j\left(a_i^n \cdot c\right) + x_i^n \theta c \Lambda_j b \qquad \text{novamente por definição de } \Lambda_j \\ &= \Lambda_j(a) + \theta(a)\Lambda_j(b) \qquad \text{porque } a_i^n c = a \quad \text{e} \\ &\qquad\qquad\qquad\qquad \theta\left(a_i^n c\right) = \theta a_i^n \theta c = x_i^n \theta c \end{aligned}$$

temos concluido a prova que (E_1) é verdadeira

Falta-nos ver que as imagens por Λ_j, de duas palavras equivalentes, são iguais. Ou seja

$$(E_2) \quad \Lambda_j\left(aa_i^0 b\right) = \Lambda_j(ab)$$

$$(E_3) \quad \Lambda_j\left(aa_i^{m+m} b\right) = \Lambda_j\left(aa_i^m a_i^n b\right)$$

pois são estas as duas transformações de equivalência que definimos no semi-grupo das palavras.

Relativamente a (E_1) temos

$$\begin{aligned}\Lambda_j\left(aa_i^0 b\right) &= \Lambda_j\left(aa_i^0\right) + \theta\left(aa_i^0\right)\cdot \Lambda_j b \\ &= \Lambda_j(a) + \theta(a)\cdot \Lambda_j b \\ &= \Lambda_j(ab)\end{aligned}$$

utilizamos dois factos já provados

$$\Lambda_j\left(aa_i^0\right) = \Lambda_j(a\cdot 1) = \Lambda_j(a) \quad \text{e}$$

$$\theta\left(aa_i^0\right) = \theta a\cdot \theta a_i^0 = \theta a\cdot x_i^0 = \theta a\cdot 1 = \theta a$$

Quanto a (E_2) comecemos por reparar que

$$\frac{x_i^{m+n}-1}{x_i-1} = \frac{x_i^m-1}{x_i-1} + x_i^m\,\frac{x_i^n-1}{x_i-1}$$

resultante do uso da propriedade distributiva do produto em relação à soma e da propriedade associativa da soma

$$\begin{aligned}&\frac{x_i^{m+n}-1}{x_i-1} = 1 + x_i + x_i^2 + \ldots + x_i^{m+n-1} \\ &= \left(1 + x_i + x_i^2 + \ldots + x_i^{m-1}\right) + \left(x_i^m + x_i^{m+1} + \ldots x_i^{m+n-1}\right) \\ &= \left(1 + x_i + x_i^2 + \ldots + x_i^{m-1}\right) + x_i^m\left(1 + x_i + \ldots + x_i^{n-1}\right) \\ &= \frac{x_i^m-1}{x_i-1} + x_i^m\cdot\frac{x_i^n-1}{x_i-1}\end{aligned}$$

Tendo em atenção esta igualdade vamos ver que

$$\Lambda_j\left(a_i^{m+n}\right) = \Lambda_j\left(a_i^m\cdot a_i^n\right)$$

$$\Lambda_j\left(a_i^{m+n}\right) = \frac{x_i^{m+n}-1}{x_i-1}\delta_{ij} \qquad \text{por definição}$$

$$= \frac{x_i^m-1}{x_i-1}\delta_{ij} + x_i^m\,\frac{x_i^n-1}{x_i-1}\delta_{ij} \qquad \text{usando a igualdade mostrada anteriormente}$$

$$= \Lambda_j a_i^m + x_i^m \Lambda_j a_i^n$$

$$= \Lambda_j\left(a_i^m\cdot a_i^n\right) \qquad (\text{usando } \mathrm{E}_1)$$

Estamos agora em condições de provar (E_3)

$$\Lambda_j\left(aa_i^{m+n}b\right) = \Lambda_j\left(aa_i^{m+n}\right) + \theta\left(aa_i^{m+n}\right)\Lambda_j b$$

$$= \Lambda_j(a) + \theta(a)\Lambda_j\left(a_i^{m+n}\right) + \theta\left(aa_i^{m+n}\right)\Lambda_j b$$

$$= \Lambda_j(a) + \theta a\Lambda_j\left(a_i^m a_i^n\right) + \theta\left(aa_i^m a_i^n\right)\Lambda_j b$$

$$= \Lambda_j\left(aa_i^m a_i^n\right) + \theta\left(aa_i^m a_i^n\right)\Lambda_j b$$

$$= \Lambda_j\left(aa_i^m a_i^n b\right)$$

Com estes ingredientes torna-se possível definir a aplicação

$$\frac{\partial}{\partial x_j}: F \to KF$$

$$x = \theta a \to \Lambda_j(a) \qquad \text{com } a \in W(A)$$

Esta aplicação está bem definida porque se tivermos $\theta a = \theta b$ isto quer dizer que "a" e "b" são palavras equivalentes e já vimos que para palavras equivalentes

$$\Lambda_j a = \Lambda_j b$$

Do modo como já foi definido $\frac{\partial}{\partial x_j}$, resulta a propriedade de que $\frac{\partial x_i}{\partial x_j} = \delta_{ij}$.

É imediato:

$$\frac{\partial x_i}{\partial x_j} = \frac{\partial}{\partial x_j}(\theta a_i) = \Lambda_j a_i = \frac{x_i^1 - 1}{x_i - 1}\delta_{ij} = 1 \cdot \delta_{ij} = \delta_{ij}$$

Só nos resta ver que se trata de facto duma derivada em KF. Tomemos dois elementos x, y em F

$$x = \theta a \quad y = \theta b$$

$$\frac{\partial}{\partial x_j}(x, y) = \frac{\partial}{\partial x_j}(\theta ab) = \Lambda_j ab$$

$$= \Lambda_j a + \theta a\Lambda_j b$$

$$= \frac{\partial}{\partial x_j}\theta a + \theta a\frac{\partial}{\partial x_j}\theta b$$

$$= \frac{\partial}{\partial x_j}x + x \cdot \frac{\partial}{\partial x_j}y$$

Como uma derivação em F induz uma derivação em KF temos a construção justificada.

A utilização de derivadas num grupo livre resulta de grande importância pelo facto da estrutura desse grupo ficar determinada pelo conjunto das derivadas num seu anel de grupo livre como se pode ver pelo seguinte teorema.

Teorema:

Para quaisquer polinómios livres $h_1(x), h_2(x)\ldots$ existe uma e uma só derivada D em KF tal que

$$Dx_j = h_j(x) \quad \forall_{j=1,2,\ldots}$$

Além disso para qualquer $f(x) \in KF$ temos

$$Df(x) = \sum_j \frac{\partial f}{\partial x_j} h_j(x)$$

Demonstração:

A existência está garantida se ficar provado que $f(x) \mapsto \sum_j \frac{\partial f}{\partial x_j} h_j(x)$ é uma derivada

Observemos primeiro que se x_j não ocorre no polinómio $f(x)$ então

$$\frac{\partial f}{\partial x_j} = 0$$

Como o polinómio $f(x)$ é de forma

$$f(x) = \sum m_{i_1, i_2, \ldots i_k} x_{i_1}^{n_{1_i}} x_{i_2}^{n_{i_2}} \ldots x_{i_k}^{n_{i_k}}$$

dada a aditividade da derivada

$$\frac{\partial f}{\partial x_j} = \sum m_{i_1, i_2, \ldots i_k} \frac{\partial}{\partial x_j} \left(x_{i_1}^{n_{i_1}} x_{i_2}^{n_{i_2}} \ldots x_{i_k}^{n_{i_k}} \right)$$

para analisar se $\frac{\partial f}{\partial x_j}$ é ou não zero basta ver que se passa para produtos de dois momómios e concluir por indução:

$$\frac{\partial}{\partial x_j} \left(x_{i_e}^{n_{i_e}} x_{i_s}^{n_{i_s}} \right) = \frac{\partial}{\partial x_j} x_{i_e}^{n_{i_e}} + x_{i_e}^{n_{i_e}} \frac{\partial}{\partial x_j} x_{i_s}^{n_{i_s}}$$

$$= \frac{x_{i_e}^{n_{i_e}} - 1}{x_{i_e} - 1} \delta_{i_e j} + x_{i_e}^{n_{i_e}} \frac{x_{i_s}^{n_{i_s}} - 1}{x_{i_s} - 1} \delta_{i_s j}$$

se $i_e \neq j$ e $i_s \neq j$ a derivada é nula, porque

$$\delta_{i_e j} = \delta_{i_s j} = 0$$

Como a derivada de cada momómio $x_{i_1}^{n_{i_1}} \ldots x_{i_k}^{n_{i_k}}$ se reduz ao cálculo de derivadas do tipo $\frac{\partial}{\partial x_j} x_{i_s}^{n_{i_s}}$, se x_j nunca aparecer na formação deste monómio as suas derivadas são nulas e portanto $\frac{\partial f}{\partial x_j} = 0$

Este resultado permite-nos concluir que a aplicação

$$f(x) \xrightarrow{D} \sum \frac{\partial f}{\partial x_j} h_j(x)$$

está bem definida porque o número das suas parcelas nunca será infinito.

Calculemos as imagens dos geradores do grupo livre por esta aplicação

$$x_i \xrightarrow{D} \sum \frac{\partial x_i}{\partial x_j} h_j(x) = 1 \cdot h_i(x) = h_i(x)$$

portanto $Dx_j = h_j(x) \quad \forall_j$

Mostremos por fim que D se comporta como uma derivada nos geradores

$$D(x_i x_k) = \sum_j \frac{\partial (x_i x_k)}{\partial x_j} h_j(x)$$

reparemos, usando a observação anterior que as duas únicas parcelas não nulas são

$$\begin{aligned}
&\frac{\partial}{\partial x_i}(x_i x_k) h_i(x) + \frac{\partial}{\partial x_k}(x_i x_k) h_k(x) \\
&= \left(\frac{\partial x_i}{\partial x_i} + x_i \frac{\partial x_k}{\partial x_i} \right) h_i(x) + \left(\frac{\partial x_i}{\partial x_k} + x_i \frac{\partial x_k}{\partial x_k} \right) h_k(x) \\
&= \frac{\partial x_i}{\partial x_i} h_i(x) + x_i \frac{\partial x_k}{\partial x_k} h_k(x) \\
&= h_i(x) + x_i h_k(x) = D(x_i) + x_i D(x_k)
\end{aligned}$$

Portanto como nos geradores $x_1, x_2, \ldots, D$ actua como uma derivada, é possível extendê-la ao anel de grupo livre KF, mantendo as propriedades pretendidas. Como a extensão é, única tudo fica provado.

Como também já foi visto $f(x) \mapsto f(x) - f(1)$ é uma derivada em KF. Daqui podemos como corolário deste teorema, obter a formula fundamental.

$$f(x) - f(1) = \sum_j \frac{\partial f}{\partial x_j}(x_j - 1) \qquad (E_4)$$

Basta fazer $g(x)=f(x)-f(1)$ e $h_j(x)=x_j-1$. Como $\frac{\partial g(x)}{\partial x_j}=\frac{\partial f(x)}{\partial x_j}$ aplicando o teorema anterior a $g(x)$ resulta a expressão (E_4).

4.4. A Matriz de *Alexander* e os Ideais Elementares dum Anel

Temos vindo a sugerir que o cálculo livre é uma ferramenta imprescindível na construção de invariantes importantes da pré-representação de grupos. Vejamos quais são esses invariantes.

Foi já dito que a partir dum conjunto de geradores $X=(x_1,x_2,\ldots)$ podemos definir um grupo livre F de base X com eventuais relatores $r_1,r_2,\ldots$.

Chamando R à consequência de $(r_1,r_2,\ldots)$ a pré-apresentação do grupo é a aplicação

$$F \xrightarrow{P} F/R = |x_i : r_i|$$

onde p é o homomofismo cnónico. Estabelecendo a seguinte cadeia de aplicações

$$KF \xrightarrow{\frac{\partial}{\partial x_i}} KF \xrightarrow{\gamma} K|X:r| \xrightarrow{\alpha} JH$$

onde γ é a extensão de p e α o abelianizador já atrás definido, podemos introduzir a *matriz de Alexander* de $|X:r|$, grupo livre de base X como sendo a matriz A cujo elemento genérico a_{ij} é

$$a_{ij}=\alpha\gamma\left(\frac{\partial r_i}{\partial x_j}\right)$$

A importância de γ e α na definição está no facto de γ aplicar qualquer relator r_i em 1 e α transportar o cálculo para um anel comutativo onde é possível definir determinantes.

Em qualquer anel comutativo com unidade é possível considerar o conjunto das matrizes A, $m\times n$ cujo elemento genérico $a_{ij}\in A$.

Nesse conjunto de matrizes pode definir-se para $\forall_{K\in N}$ o K ésimo **ideal elementar** $E_K(A)$ da matriz A como sendo:

(1°) Para $0<n-k\leq m$, o ideal gerado pelos determinantes das $(n-k)\times(n-k)$ sub-matrizes de A.

(2°) Para $n-k>m$, $E_k(A)=0$

(3°) Para $n-k\leq 0$, $E_k(A)=R$ (anel considerado)

O determinante duma matriz pode ser expandido como combinação de cofactores dos elementos de qualquer linha ou coluna, daí resulta que os ideais elementares de A formam uma cadeia ascendente

$$E_0(A)\ C\ E_1(A)\ C \ldots C\ E_n(A) = E_{n+1}(A) = \ldots = R$$

A importância dos ideais elementares fica estabelecida pelo seguinte teorema cuja demonstração se baseia apenas em propriedades básicas de homomorfismo e grupos cociente.

Teorema:

Os ideais elementares formam um invariante numa pré-representação dum qualquer grupo finito, isto é duas pré-representações dum grupo G tem forçosamente a mesma cadeia de ideais elementares.

4.5. Construção dos Ideais Elementares de AC(2,3)

Os geradores de AC(2,3) são os autómatos celulares, já mencionados, a que atribuimos por comodidade um simbolo constituido por uma letra(g) e um índice. Relembremos:

$$g_1 = R_{255} \quad g_4 = R_{170} \quad g_7 = R_{136}$$
$$g_2 = R_{240} \quad g_5 = R_{192} \quad g_8 = R_{128}$$
$$g_3 = R_{204} \quad g_6 = R_{160}$$

designamos por $g_0 = 1 = R_0$, o elemento neutro do grupo livre gerado pelos $g_i \quad i = 1,8$. Sabemos que este grupo possui relatores r_i e que

$$r_i = g_i^2 \quad \forall_{i=1,8}$$

Como este grupo livre é comutativo o seu anel de grupo também é e portanto coincide com o Abelianizado. Dito doutro modo estamos perante um grupo comutativo livre.

Nas nossas notações, o elemento genérico da matriz de *Alexander* foi definido como,

$$a_{ij} = \alpha \cdot p\left(\frac{\partial r_i}{\partial g_j}\right)$$

onde p é a projecção canónica do grupo no grupo cociente e α o Abelianizador. No nosso caso p tem o efeito de estabelecer as identificações $g_i^2 = 1$ e α é pura e simplesmente a identidade, portanto $a_{ij} = \frac{\partial r_i}{\partial g_j}$. Efectuemos as derivadas:

$$a_{ij} = \frac{\partial r_i}{\partial g_j} = \frac{\partial g_i^2}{\partial g_j}$$

Para $i \neq j$

$$\frac{\partial g_i^2}{\partial g_j} = \frac{\partial}{\partial g_j}\left(g_i^2\right) = \frac{g_i^2 - 1}{g_i - 1} \cdot \frac{\partial g_i}{\partial g_j} = \frac{g_i^2 - 1}{g_i - 1} \cdot 0 = 0$$

Para $i = j$

$$\frac{\partial g_i^2}{\partial g_i} = \frac{\partial}{\partial g_i}\left(g_i^2\right) = \frac{g_i^2 - 1}{g_i - 1} \cdot \frac{\partial g_i}{\partial g_i} = \frac{g_i^2 - 1}{g_i - 1} \cdot 1 = \frac{g_i^2 - 1}{g_i - 1} = g_i + 1$$

Concluimos assim que a matriz de *Alexander* de AC(2,3) é a matriz diagonal:

$$A = \begin{pmatrix} g_1+1 & 0 & \cdots & \cdots & \cdots & \cdots & \cdots & 0 \\ 0 & g_2+1 & & & & & & \vdots \\ \vdots & & g_3+1 & & & & & \vdots \\ \vdots & & & g_4+1 & & & & \vdots \\ \vdots & & & & g_5+1 & & & \vdots \\ \vdots & & & & & g_6+1 & & \vdots \\ \vdots & & & & & & g_7+1 & \vdots \\ 0 & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & g_8+1 \end{pmatrix}$$

O cálculo das ideias elementares fica extremamente simplificado:

Como $m = n$, temos que $E_k(A)$, para $0 < n-k \leq n$, será o ideal gerado pelos determinantes de todas as $(n-k)\times(n-k)$ sub-matrizes de A. É importante referir que apenas os determinantes das sub-matrizes $(n-k)\times(n-k)$ diagonais são não-nulos, ou seja na determinação do ideal $E_k(A)$ apenas nos teremos que preocupar com essas sub-matrizes. A razão é a que em termos práticos para formarmos uma sub-matriz $(n-k)\times(n-k)$ teremos que eleminar k linhas e k colunas da matriz. Quando aas k linhas têm exactamente os mesmos índices que as k linhas que vão ser excluidos então a sub-matriz $(n-k)\times(n-k)$ é uma matriz diagonal e no nosso caso com todos os elementos $a_{ii} \neq 0$. Quando um dos índices das linhas a excluir não coincidir com quaisquer dos índices das colunas a excluir então existirá um elemento $a_{ji} = 0$ e portanto o determinante dessa matriz, assim obtida, será nulo.

Para $k = 1$ teremos $E_1(A)$ gerado pelas sub-matrizes 7×7 das quais apenas nos teremos que preocupar com as únicas 8 que têm elementos diagonais não nulos.

Cada determinante D_j com $j = 1,8$ é da forma

$$D_j = \prod_{i=1}^{7}\left(g_{ij}+1\right) \quad \text{com}$$

$$\left\{1_j, 2_j, 3_j, 4_j, 5_j, 6_j, 7_j\right\} \quad C \quad \{1,2,3,4,5,6,7,8\}$$

ou seja o conjunto $\left\{i_j;\ \ i = 1,7\right\}$ para um dado j é um sub-conjunto de $N_8 = \{n \in N : n \leq 8\}$ com 7 elementos.

Utilizando as operações definidas no anel Z_2G é possível escrever D_j como um somatório

$$D_j = \sum g_1^{\alpha_1} g_2^{\alpha} \cdots g_8^{\alpha_8}$$

onde pelo menos um dos α_i é nulo e

$$g_i^{\alpha_i} = \begin{cases} g_i & \text{se} \quad \alpha_i = 1 \\ 1 & \text{se} \quad \alpha_i = 0 \end{cases}$$

Vamos agora concluir que $E_1(A)$ é o próprio anel Z_2G.

Observemos antes de mais que dado um anel R e dados $\alpha_1, \alpha_2, \ldots \alpha_n$ elementos desse anel o ideal I, gerado pelos elementos de R são da forma

$$\sum r_i a_i + \sum n_j a_j \quad \text{com} \quad r_i \in R \quad \text{e} \quad n_j \in Z$$

No nosso caso os geradores são $D_1, D_2, \ldots D_8$. O ideal $E_1(A)$ sem o conjunto dos elementos da forma

$$\sum g_i D_i + \sum n_j D_j \quad \text{onde} \quad g_i \in G \quad \text{e} \quad n_j \in Z_2$$

ou seja $E_1(A) = Z_2G$ dada a forma dos D_i. Foi também dito que os ideais elementares constituiam uma sucessão ascendente. por este facto fica também concluido que

$$E_2(A) = E_3(A) = \ldots = E_8(A) = Z_2G$$

A conclusão é também imediata fazendo um raciocínio directo como fizemos para $E_1(A)$. Seja por exemplo o cálculo de $E_k(A)$ para um k genérico. Como já observamos apenas nos teremos que preocupar com C_k^n matrizes quadradas $(n-k)\times(n-k)$ com elementos na diagonal todas diferentes de zero. Esses C_k^n determinantes são assim definidos

$$D_j = \prod_{i=1}^{n-k} \left(g_{ij} + 1 \right) \quad \text{com} \quad j = 1,\ C_k^n$$

e onde $\left\{ 1_j, 2_j, \ldots (n-k)_j \right\} \quad C \quad N_8$ são todos os sub-conjuntos de N_8 com $n-k$ elementos.

Exactamente como no caso anterior D_j pode ser escrito na forma

$$D_j = \sum g_1^{\alpha_1} \ldots g_8^{\alpha_8}$$

onde pelo menos K dos α_i são nulos. Resulta também que os elementos da forma

$$\sum r_j D_j + \sum D_i$$

são elementos tanto do ideal $E_k(A)$ como do anel Z_2G e por isso $E_k(A) = Z_2G$. Portanto $E_0(A) = 0$ e $E_k(A) = Z_2G$ para $k > 1$.

A conclusão de tudo isto é que Z_2G não apresenta ideais próprios. Em termos do nosso objectivo inicial que era dar, para além duma pré-representação do grupo livre G, um estudo que permitisse localizar dentro do grupo, sub-grupos estruturalmente respresentativos, por exemplo apontar que autómatos da classe 3 pudessem ser estruturalmente estáveis, concluimos pela impossibilidade de garantir por métodos algébricos que isso seja verdade.

5. UMA ABORDAGEM DE AC(2,3) EM TERMOS DE DERIVADAS *BOOLEANAS*

5.1. Introdução

Vimos até aqui que no grupo livre AC(2,3) os autómatos geradores agem como uma base de representação de todo o grupo. Num artigo publicado em 1984 na *"Communications in Mathematical Physics" pp. 51, Oliver Martin, Andrew Odlyzko e Stephen Wolfram*, analisam os autómatos aqui designados por X, Y, Z, $X \oplus Y$, $X \oplus Z$, $Y \oplus Z$ e $X \oplus Y \oplus Z$ em grande detalhe. Estes autómatos formam como se pode facilmente verificar um sub-grupo de AC(2,3) gerado para X,Y e Z.

A sua apresentação gráfica foi feita no capítulo 2 e representam respectivamente um deslocamento para a direita, a identidade e, um deslocamento para a esquerda, quando aplicados a uma qualquer configuração inicial. No citado artigo a cada um destes autómatos é associado um monómio generalizado (com expoentes em Z), respectivamente; x, 1 e x^{-1}.

Representando cada configuração inicial de N sítios dispostos circularmente pelo polinómio

$$A_{(x)}^{(t)} = \sum_{i=0}^{N-1} a_i^{(t)} x^i$$

onde x^i representa o sítio "i", $a_i^{(t)}$ a grandeza do sítio "i" no tempo "t" e $A^{(t)}$ a configuração no tempo "t" a evolução segundo cada um dos autómatos mencionados pode ser obtida pela mutiplicação dum polinómio generalizado $T(x)$ pelo polinómio $A^t(x)$, produto feito módulo $x^N - 1$ (resultante das condições de fronteira onde o sítio "0" se identifica ao sítio "N"). Os autómatos mencionados são, nesta perspectiva, representados pelos polinómios seguintes:

$$X = x \qquad Y \oplus Z = 1 + x^{-1}$$
$$Y = 1 \qquad X \oplus Y \oplus Z = x + 1 + x^{-1}$$
$$Z = x^{-1}$$
$$X \oplus Y = x + 1$$
$$X \oplus Z = x + x^{-1}$$

Usando técnicas da análise polinominal os autores fazem um estudo exaustivo destes autómatos (ditos aditivos) generalizando os resultados a vizinhanças maiores que 3 e a número de estados por sítio superiores a 2. Para as outras regras, de maior complexidade conjucturaram que a ausência de aditividade impede em geral o uso de técnicas algébricas.

Nesta nossa perspectiva de encarar AC(2,3) como um grupo livre comutativo pretendemos dar um contributo no sentido dessa aditividade em falta.

O sub-grupo anterior foi obtido apenas com os elementos: dois deslocamentos, uma identidade e uma operação. Dito doutro modo a evolução, por exemplo, duma configuração qualquer com o autómato $X \oplus Z$ resulta da adição do deslocamento para a esquerda com o deslocamento para a direita. Se quisermos falar dos autómatos celulares representados por

regras legais, temos que dar uma interpretação aos geradores XYZ, XY, XZ e YZ. Comecemos por reparar que todos eles são produtos de deslocamentos e da identidade. Tomemos por exemplo o autómato $XY \oplus X \oplus Z$. Este autómato tem uma parte aditiva $X \oplus Z$ que já sabemos interpretar, quer em termos de polinómios generalizados, quer em termos de deslocamentos básicos (para a direita, para a esquerda e identidade). Falta-nos a parte XY que é o produto da identidade com o deslocamento para a esquerda. A aditividade permanece entre os três geradores da regra. Resta-nos dizer que AC(2,3) fica completamente caracterizado se juntarmos a estes deslocamentos básicos o "1" que corresponde aos sítios todos ocupados, ou ainda ao polinómio

$$\sum_{i=0}^{N-1} x^i$$

Nesta perspectiva bastariam seis elementos para gerarem o conjunto AC(2,3): três deslocamentos (X,Y,Z) um preenchimento de sítios (1) e duas operações $(\oplus,\bullet)$.

Vamos seguidamente tentar reinterpretar os geradores de AC(2,3) em termos de derivadas Booleanas.

5.2. Definição de Derivada Booleana

Toma-se habitualmente como definição de derivada em R o limite

$$\lim_{\Delta x \to 0} \frac{\Delta f(x)}{\Delta x} = \lim_{\Delta x \to 0} \frac{f(x+\Delta x) f(x)}{\Delta x}$$

É possível usando as mesmas motivações da análise real, definir para funções Booleanas uma derivada. Como no cálculo só existem dois valores possíveis "0" e "1", Δx definido como acréscimo da variável independente, só poderá ser a constante "1" isto é

$$\Delta x = x \oplus \bar{x} = x \oplus (x \oplus 1) = 1$$

isto é $x \oplus \Delta x = \bar{x}$ (note-se que a operação inversa de $\oplus$ é ela própria).

Portanto $f(x) = f(x \oplus \Delta x) \oplus f(x)$

ou seja $f(x) = f(\bar{x}) \oplus f(x)$

Desta definição resultam algumas propriedades em tudo semelhante às das derivadas reais

(1°) Sendo "a" uma constante, a sua derivada é zero

$$\text{Se } f(x) = a, \quad f(\bar{x}) = a \qquad f'(x) = a \oplus a = 0$$

(2°) A derivada é linear relativamente à adição

$$[f(x)\oplus g(x)]' = f'(x)\oplus g'(x)$$

$$\begin{aligned}[f(x)\oplus g(x)]' &= [f(\bar{x})\oplus g(\bar{x})]\oplus[f(x)\oplus g(x)]\\ &= [f(\bar{x})\oplus f(x)]\oplus[g(\bar{x})\oplus g(x)]\\ &= f'(x)\oplus g'(x)\end{aligned}$$

(3º) Se $f(x)=ag(x)$, com "a" constante, então

$$f'(x)=ag'(x)$$

$$f'(x)=ag(\bar{x})\oplus ag(x)=a[g(\bar{x})\oplus g(x)]=ag'(x)$$

(4º) $[f(x)\cdot g(x)]' = f'(x)\cdot g(x)\oplus f(x)g'(x)\oplus f'(x)g'(x)$

Esta é a única regra que se apresenta apenas parcialmente semelhante à sua homóloga real. Justifiquemos

$$\begin{aligned}&[f(x)\cdot g(x)]' = f(\bar{x})g(\bar{x})\oplus f(x)g(x)\\ &= f(\bar{x})g(\bar{x})\oplus f(x)g(\bar{x})\oplus f(x)g(\bar{x})\\ &\oplus f(\bar{x})g(x)\oplus f(\bar{x})g(x)\oplus f(x)g(x)\\ &= [f(\bar{x})g(\bar{x})\oplus f(x)g(\bar{x})\oplus f(\bar{x})g(x)\oplus f(x)g(x)]\\ &\oplus f(x)g(\bar{x})\oplus f(\bar{x})g(x)\\ &= [f(\bar{x})\oplus f(x)][g(\bar{x})\oplus g(x)]\oplus f(x)g(\bar{x})\oplus f(\bar{x})g(x)\\ &\oplus f(x)g(x)\oplus f(x)g(x)\\ &= f'(x)\cdot g'(x)\oplus f(x)[g(\bar{x})\oplus g(x)]\oplus[f(\bar{x})\oplus f(x)]g(x)\\ &= f'(x)\cdot g'(x)\oplus f(x)\cdot g'(x)\oplus f'(x)\cdot g(x)\end{aligned}$$

Usaremos daqui para a frente a notação de *Leibnitz* $\dfrac{\partial f(x)}{\partial x}$ em vez de $f'(x)$ por razões de simplificação quando falarmos de derivação parcial.

Também à semelhança das derivadas em R^n é possível definir o que se entende por derivação parcial, para funções Booleanas de várias variáveis.

Por definição

$$\frac{\partial f(x_1,\ldots x_n)}{\partial x_i} = f(x_1,\ldots x_i\oplus 1,\ldots x_n)\oplus f(x_1,\ldots x_i\ldots x_n)$$

Formalmente ao derivar $f(x_1,\ldots x_n)$ em ordem a x_i usamos as regras de derivação atrás enunciados considerando com variável independente a variável x_i e considerando as variáveis $x_1\ldots x_{i-1},x_{i+1},\ldots x_n$ como constantes, ex:

$$\frac{\partial(xy\oplus y)}{\partial y}=\frac{\partial(xy)}{\partial y}\oplus\frac{\partial y}{\partial y}=x\frac{\partial y}{\partial y}\oplus 1=x\oplus 1$$

$$\frac{\partial(xy\oplus y)}{\partial x}=\frac{\partial(xy)}{\partial x}\oplus\frac{\partial y}{\partial x}=y\frac{\partial x}{\partial x}\oplus 0=y$$

Definição

$$\frac{\partial^n f}{\partial x_1 \partial x_2 \ldots \partial x_n} = \frac{\partial}{\partial x_1}\left(\frac{\partial}{\partial x_2}\left(\ldots\left(\frac{\partial f}{\partial x_m}\right)\ldots\right)\right)$$

esta definição é identica aquela que usamos na análise real e também existe uma propriedade que nos permite trocar a ordem de derivação.

Propriedade

$$\frac{\partial^2 f(x_1 \ldots x_n)}{\partial x_i \partial x_j} = \frac{\partial^2 f(x_1 \ldots x_n)}{\partial x_j \partial x_i}$$

ao contrário do campo real esta propriedade é universal para qualquer função Booleana. A demonstração é imediata e baseia-se nas propriedades associativa e comutativa da adição

$$\frac{\partial^2 f(x_1 \ldots x_n)}{\partial x_i \partial x_j} = \frac{\partial}{\partial x_i}\left(\frac{\partial f(x_1 \ldots x_n)}{\partial x_j}\right)$$

$$= \frac{\partial}{\partial x_i}\left[f(x_1 \ldots \bar{x}_j, \ldots x_n) \oplus f(x_1 \ldots x_j, \ldots x_n)\right]$$

$$= \frac{\partial}{\partial x_i} f(x_1 \ldots \bar{x}_j, \ldots x_n) \oplus \frac{\partial}{\partial x_i} f(x_1 \ldots x_j, \ldots x_n)$$

$$= \left[f(x_1 \ldots \bar{x}_i, \ldots \bar{x}_j, \ldots x_n) \oplus f(x_1 \ldots x_i \ldots \bar{x}_j \ldots x_n)\right]$$

$$\oplus\left[f(x_1 \ldots \bar{x}_i \ldots x_j \ldots x_n) \oplus f(x_1 \ldots x_i \ldots x_j \ldots x_n)\right]$$

$$= \left[f(x_1 \ldots \bar{x}_i \ldots \bar{x}_j \ldots x_n) \oplus f(x_1 \ldots \bar{x}_i \ldots x_j \ldots x_n)\right]$$

$$\oplus\left[f(x_1 \ldots x_i \ldots \bar{x}_j \ldots x_n) \oplus f(x_1 \ldots x_i \ldots x_j \ldots x_n)\right]$$

$$= \frac{\partial}{\partial x_j} f(x_1 \ldots \bar{x}_i \ldots x_n) \oplus \frac{\partial}{\partial x_j} f(x_1 \ldots x_i \ldots x_n)$$

$$= \frac{\partial}{\partial x_j}\left[f(x_1 \ldots \bar{x}_i \ldots x_n) \oplus f(x_1 \ldots x_i \ldots x_n)\right]$$

$$= \frac{\partial}{\partial x_j}\left(\frac{\partial f}{\partial x_i}\right) = \frac{\partial^2 f}{\partial x_j \partial x_i}$$

A generalização por indução matemática é imediata e permite-nos escrever

$$\frac{\partial^n f}{\partial x_1 \partial x_2 \ldots \partial x_n} = \frac{\partial^n f}{\partial x_{\sigma(1)} \partial x_{\sigma(2)} \ldots \partial x_{\sigma(n)}}$$

onde $\{\sigma(1), \sigma(2) \ldots, \sigma(n)\}$ representa uma permutação do conjunto $\{1,2,\ldots,n\}$

5.3. Expansão Booleana em Série de *MacLaurin*

À semelhança das funções reais de variável real podemos expandir qualquer função Booleana em série. De facto o termo série não está correctamente aplicado, uma vez que a soma que a seguir definiremos é sempre necessariamente finita. Manteremos a designação por uma questão de semelhança formal.

Vimos já nos capítulos anteriores que qualquer regra respeitante a um autómato celular Booleano poderá ser escrita como

$$f(X,Y,Z) = \sum_{(\alpha_1,\alpha_2,\alpha_3)=(0,0,0)}^{(1,1,1)} g(\alpha_1,\alpha_2,\alpha_3) X^{\alpha_1} Y^{\alpha_2} Z^{\alpha_3}$$

Uma vez que $\alpha_i \in \{0,1\}$ $\forall_i$ aquela soma é formalmente equivalente a

$$f(X,Y,Z) = \lambda_0 \cdot 1 \oplus \lambda_1 X \oplus \lambda_2 Y \oplus \lambda_3 Z \oplus \lambda_4 XY \oplus \lambda_5 XZ \oplus \lambda_6 YZ \oplus \lambda_7 XYZ \qquad (D_1)$$

com $\lambda_i \in \{0,1\}$ $\forall_i$. Comecemos por observar que $f(0,0,0) = \lambda_0$.

Calculemos todas as possíveis derivadas até à terceira ordem e apliquemos essas derivadas no ponto $(0,0,0)$. Teremos:

$$\frac{\partial f}{\partial X} = \lambda_1 \oplus \lambda_4 Y \oplus \lambda_5 Z \oplus \lambda_7 YZ$$

$$\left.\frac{\partial f}{\partial X}\right|_{(0,0,0)} = \lambda_1$$

$$\frac{\partial f}{\partial Y} = \lambda_2 \oplus \lambda_4 X \oplus \lambda_6 Z \oplus \lambda_7 XZ$$

$$\left.\frac{\partial f}{\partial Y}\right|_{(0,0,0)} = \lambda_2$$

$$\frac{\partial f}{\partial Z} = \lambda_3 \oplus \lambda_5 X \oplus \lambda_6 Y \oplus \lambda_7 XY$$

$$\left.\frac{\partial f}{\partial Z}\right|_{(0,0,0)} = \lambda_3$$

$$\frac{\partial f}{\partial X \partial Y} = \frac{\partial f}{\partial Y \partial X} = \lambda_4 \oplus \lambda_7 Z$$

$$\left.\frac{\partial f}{\partial X \partial Y}\right|_{(0,0,0)} = \lambda_4$$

$$\frac{\partial^2 f}{\partial X \partial Z} = \frac{\partial f}{\partial Z \partial X} = \lambda_5 \oplus \lambda_7 Y$$

$$\left.\frac{\partial f}{\partial X \partial Z}\right|_{(0,0,0)} = \lambda_5$$

$$\frac{\partial^2 f}{\partial Y \partial Z} = \frac{\partial^2 f}{\partial Z \partial Y} = \lambda_6 \oplus \lambda_7 X$$

$$\left.\frac{\partial^2 f}{\partial Y \partial Z}\right|_{(0,0,0)} = \lambda_6$$

$$\frac{\partial^3 f}{\partial X \partial Y \partial Z} = \frac{\partial^3 f}{\partial Y \partial X \partial Z} = \frac{\partial^3 f}{\partial Z \partial Y \partial X} = \ldots = \lambda_7$$

$$\left.\frac{\partial^3 f}{\partial X \partial Y \partial Z}\right|_{(0,0,0)} = \lambda_7$$

fica claro porque terminamos na ordem 3. As derivadas de 4ª ordem e seguintes são nulas. Para $n > 3$

$$\frac{\partial^n f}{\partial X^{n_1} \partial Y^{n_2} \partial Z^{n_3}} = 0 \quad \text{com} \quad n_1 + n_2 + n_3 = n$$

Designando por $\mathbf{X} = (X, Y, Z)$ e por I o número "i" em binário entendido como um termo (i_1, i_2, i_3) podemos compactificar a expressão (D_1) da seguinte forma

$$f(\mathbf{X}) = \sum_{I=0}^{7} \left.\frac{\partial^I f}{\partial X^I}\right|_{(0,0,0)} \cdot X^I \qquad (D_2)$$

onde

$$\lambda_i = \frac{\partial^I f(\mathbf{X})}{\partial \mathbf{X}^I}$$

por exemplo $\lambda_5 = \dfrac{\partial^5 f}{\partial X^5}$ (como $5 = 4 + 1$) $5 = (1,0,1)$ $1 + 0 + 1 = 2$ e daí que

$$\frac{\partial^5 f(\mathbf{X})}{\partial X^5} = \frac{\partial^2 f(X, Y, Z)}{\partial X \partial Z}$$

Convencionando que $\lambda_0 = \dfrac{\partial^0 f(\mathbf{X})}{\partial \mathbf{X}^0} = f(0,0,0)$ a expressão (D_2) pela sua semelhança com o desenvolvimento em série de *MacLaurin* para funções reais designa-se por expansão Booleana em série de *MacLaurin*.

5.4. O Grupo Livre AC(2,3) em Termos de Derivadas Booleanas

A expansão (D_2) que se escreve também como

$$f(Z,Y,Z) = f(0,0,0)\cdot 1 \oplus \left.\frac{\partial f}{\partial X}\right|_{(0,0,0)} \cdot X \oplus \left.\frac{\partial f}{\partial Y}\right|_{(0,0,0)} Y$$
$$\oplus \left.\frac{\partial f}{\partial Z}\right|_{(0,0,0)} \cdot Z \oplus \left.\frac{\partial^2 f}{\partial X \partial Y}\right|_{(0,0,0)} XY \oplus \left.\frac{\partial^2 f}{\partial X \partial Z}\right|_{(0,0,0)} XZ$$
$$\oplus \left.\frac{\partial^2 f}{\partial Y \partial Z}\right|_{(0,0,0)} YZ \oplus \left.\frac{\partial^3 f}{\partial X \partial Y \partial Z}\right|_{(0,0,0)} XYZ \qquad (D_3)$$

não é mais do que a expressão do elemento genérico do grupo livre AC(2,3) construido no capítulo 3.

Formalizando um pouco mais é possível com o auxílio das derivadas reduzir os geradores do grupo AC(2,3) formalmente a um, a regra 128 correspondente ao autómato XYZ. Basta repara que

$$X = \frac{\partial^2 (XYZ)}{\partial Y \partial Z} \quad XY = \frac{\partial (XYZ)}{\partial Z}$$
$$Y = \frac{\partial^2 (XYZ)}{\partial X \partial Z} \quad XZ = \frac{\partial (XYZ)}{\partial Y}$$
$$Z = \frac{\partial^2 (XYZ)}{\partial X \partial Y} \quad YZ = \frac{\partial (XYZ)}{\partial X}$$
$$1 = \frac{\partial^3 (XYZ)}{\partial X \partial Y \partial Z} \quad XYZ = \frac{\partial^0 (XYZ)}{\partial X \partial Y \partial Z}$$

Com estas novas rotações (D_3) escreve-se na forma:

$$f(X,Y,Z) = f(0,0,0)\cdot \frac{\partial^3 (XYZ)}{\partial X \partial Y \partial Z} \oplus \left.\frac{\partial f}{\partial X}\right|_{(0,0,0)} \cdot \frac{\partial^2 (X,Y,Z)}{\partial Y \partial Z}$$
$$\oplus \left.\frac{\partial f}{\partial Y}\right|_{(0,0,0)} \cdot \frac{\partial^2 (XYZ)}{\partial X \partial Z} \oplus \left.\frac{\partial f}{\partial Z}\right|_{(0,0,0)} \cdot \frac{\partial^2 (XYZ)}{\partial X \partial Y}$$
$$\oplus \left.\frac{\partial^2 f}{\partial X \partial Y}\right|_{(0,0,0)} \cdot \frac{\partial (XYZ)}{\partial Z} \oplus \left.\frac{\partial^2 f}{\partial X \partial Z}\right|_{(0,0,0)} \cdot \frac{\partial (XYZ)}{\partial Y}$$
$$\oplus \left.\frac{\partial^2 f}{\partial Y \partial Z}\right|_{(0,0,0)} \cdot \frac{\partial (XYZ)}{\partial X} \oplus \left.\frac{\partial^3 f}{\partial X \partial Y \partial Z}\right|_{(0,0,0)} \cdot \frac{\partial^0 (XYZ)}{\partial X \partial Y \partial Z}$$

introduzindo a notação $\frac{\partial^I (XYZ)}{\partial X^I}$ como sendo $\frac{\partial^{i_1+i_2+i_3}}{\partial X^{i_1} \partial Y^{i_2} \partial Z^{i_3}}$ onde (i_1, i_2, i_3) é a representação de $I = 1,7$ em binário, escrevemos (D_2) como

$$f(\mathbf{X}) = \sum_{I=0}^{7} \frac{\partial^I f}{\partial \mathbf{X}^I}\bigg|_{(0,0,0)} \cdot \frac{\partial^{7-I}(XYZ)}{\partial \mathbf{X}^{(7-1)}} \qquad (D_4)$$

Esta última expressão permite olhar o grupo AC(2,3) como sendo o grupo livre gerado pelas derivadas do autómato *XYZ*.

Se entendermos as derivadas como uma taxa de variação, qualquer regra incorpora em si as diferentes variações da regra 128.

Por outro lado a expressão D_4 é útil em termos de implementação de sistemas dinâmicos associados aos autómatos celulares, porque reduz o número de componentes.

6. GENERALIZAÇÕES

A generalização de AC(2,3) para outros grupos AC(k,n) em termos de grupos livres está garantida. O aumento da vizinhança, resulta num aumento no número de variáveis.Com vizinhanças de tamanho "*n*" teremos funções do tipo $f(X_1, X_2, \ldots X_n)$

Se aumentarmos o número de estados de cada sítio, modificamos os relatores do grupo livre. Com k estados trabalhamos em Z_k e os relatores seriam da forma $X_i^k = 0$

Resulta claro porque é preferível ter um número de estados primos. $(Z_K, \oplus_K, \bullet_K)$ é um corpo para k primo.

BIBLIOGRFIA

[1] Stephan Wolfran, "Theory and Applications of Cellular Automata", World Scientific Publishing Co. Pte. Ltd. (1986)

[2] John B. Fraleigh, "A first Course in Abstract Algebra", Addison-Wesley Publishing Company (1981)

[3] B.L. Van der Waerden, "Álgebra Moderna", publicações da Sociedade Portuguesa de Matemática (1956)

[4] Richard H. Crowell, Ralph M. Fox, "Introduction to Knot Theory", Springer Verlag (1963)

[5] Adilson Gonçalves, "Introdução à Álgebra", projecto Euclides (1979)

[6] Gérard Y. Vichniac, "Boolean Derivatives on Cellular Automata" (1990)

[7] A. Thayse "Boolean Calcules of Differences ", Springer (1981)