Trabalho apresentado no XXXVII CNMAC, S.J. dos Campos - SP, 2017.

Proceeding Series of the Brazilian Society of Computational and Applied Mathematics

Loops de Código

Rosemary Miguel Pires[1]
Departamento de Matemática, Instituto de Ciências Exatas, UFF, Volta Redonda, RJ

Resumo. Robert L. Griess (1986) introduziu a teoria de Loops de Código que tem aplicabilidade no estudo das Álgebras Não Associativas. Griess demonstrou que um loop de código é um loop de Moufang [5] e Orin Chein e Edgar G. Goodaire (1990) demonstraram que loops de código tem um único comutador não-trivial, um único associador não-trivial e um único quadrado não-trivial. Em [7], classificamos todos os loops de códigos de posto 3 e 4 e determinamos todas as representações básicas destes loops. Neste trabalho apresentamos uma introdução à Teoria de Loops de Código. De modo mais específico, apresentamos alguns resultados essenciais sobre códigos pares, loops de Moufang e loops de código e apresentamos uma caracterização dos loops de código.

Palavras-chave. Loops de Moufang, Códigos Pares, Loops de Código.

1 Introdução

Nesta seção apresentamos algumas definições e resultados preliminares sobre loops. Para mais detalhes e demonstrações ver [3] e [6].

Um **loop** é um conjunto L, munido com uma operação binária (denotada por justaposição ou por .) tal que, dados quaisquer elementos x, y, z, a equação $x.y = z$ determina o terceiro elemento de modo único e tal que existe um elemento identidade (denotado por 1).

Um loop L é um loop com a propriedade inversa (denotado por loop P.I.) se cada $x \in L$ tem um único inverso bilateral, que denotamos por x^{-1}, e se, $\forall\ x, y \in L$, o loop satisfaz $x^{-1}(xy) = y$ e $(yx)x^{-1} = y$, ou seja, as propriedades de inverso à esquerda e inverso à direita, respectivamente.

Teorema 1.1. *Em qualquer loop L, para quaisquer elementos x, y, z de L, as seguintes identidades (chamadas identidades de Moufang) são equivalentes:*

$$((xy)x)z = x(y(xz)), \tag{1}$$
$$((xy)z)y = x(y(zy)), \tag{2}$$
$$(xy)(zx) = (x(yz))x. \tag{3}$$

Se L é um loop satisfazendo qualquer uma dessas identidades, então L é um loop P.I. que também satisfaz

$$(yx)x = yx^2, \ \ x(xy) = x^2y, \ \ (xy)x = x(yx). \tag{4}$$

[1]rosemarypires@id.uff.br

Um loop L é chamado um **loop de Moufang** se ele satisfaz qualquer uma das três identidades de Moufang.

Com o objetivo de enunciar um teorema, que é bastante útil para decidirmos se um determinado conjunto não-vazio munido de uma operação binária é um loop, vamos definir a noção de quasigrupo. Seja G um conjunto não-vazio munido de uma operação binária "."(denotado por $(G, .)$ e chamado de grupóide) e seja a qualquer elemento fixado em G. As aplicações de translação $L_a : G \longrightarrow G$ e $R_a : G \longrightarrow G$, são definidas respectivamente por $L_a(x) = a.x$ e $R_a(x) = x.a$, $\forall x \in G$.

Um grupóide $(G, .)$ é chamado um quasigrupo se as aplicações $L_a : G \longrightarrow G$ e $R_a : G \longrightarrow G$ são bijeções para todo $a \in G$.

A definição de quasigrupo é equivalente a dizermos que dados quaisquer dois elementos de x, y, z em G o terceiro pode ser unicamente selecionado em G de modo que $x.y = z$. Logo, temos que um loop $(L, .)$ é um quasigrupo com elemento identidade (bilateral) 1.

Teorema 1.2. *Seja $(G, .)$ um grupóide finito. São equivalentes:*

(i) *$(G, .)$ é um quasigrupo.*

(ii) *$L_a : G \longrightarrow G$ e $R_a : G \longrightarrow G$ são injetoras para todo $a \in G$.*

(iii) *$L_a : G \longrightarrow G$ e $R_a : G \longrightarrow G$ são sobrejetoras para todo $a \in G$.*

(iv) *As leis de cancelamento à esquerda e à direita valem para $(G, .)$.*

(v) *Cada elemento em G aparece somente uma vez em cada linha e em cada coluna da tabela de multiplicação para $(G, .)$.*

Definição 1.1. *Sejam x, y e z três elementos de um loop L. O comutador de x e y é o único elemento $[x, y]$ de L que satisfaz $xy = (yx)[x, y]$ e o associador de x, y e z é o único elemento (x, y, z) de L que satisfaz $(xy)z = (x(yz))(x, y, z)$.*

O núcleo à esquerda de um loop L é o conjunto $\mathcal{N}_l = \{a \in L | (a, x, y) = 1, \forall x, y \in L\}$, o núcleo à direita é o conjunto $\mathcal{N}_r = \{a \in L | (x, y, a) = 1, \forall x, y \in L\}$, o núcleo do meio é $\mathcal{N}_m = \{a \in L | (x, a, y) = 1, \forall x, y \in L\}$ e o núcleo de L é $\mathcal{N}(L) = \mathcal{N}_l \cap \mathcal{N}_r \cap \mathcal{N}_m$. O centro de L é $\mathcal{Z}(L) = \{x \in \mathcal{N}(L) | [a, x] = 1, \forall a \in L\}$.

Proposição 1.1. *Todo núcleo de um loop é um subloop associativo e portanto um grupo. O centro de um loop é um grupo abeliano.*

As demonstrações do Lema 1.1, Corolário 1.1 e dos Teoremas 1.3 e 1.4 a seguir podem ser encontradas em [2].

Lema 1.1. *Se L é um loop de Moufang, $z \in L$ um elemento que comuta com todo elemento de L, e $z^2 \in \mathcal{N}(L)$, então $z \in \mathcal{Z}(L)$.*

Corolário 1.1. *Se L é um loop de Moufang, $z \in L$ um elemento que comuta com todo elemento de L, e $z^2 = 1$, então $z \in \mathcal{Z}(L)$.*

DOI: 10.5540/03.2018.006.01.0383

Teorema 1.3. *Se L é um loop de Moufang com um único quadrado não trivial, e, então $e^2 = 1$ e L é um grupo abeliano ou $[L, L] = (L, L, L) = L^2 = \{1, e\} \subseteq \mathcal{Z}(L)$.*

Teorema 1.4. *Se L é um loop de Moufang com $L^2 = \{1, e\}$, então, para todo $w, x, y, z \in L$,*

1. $[xy, z] = [x, z][y, z](x, y, z)$
2. $(wx, y, z) = (w, y, z)(x, y, z)$.

Teorema 1.5. *(Moufang) Se a, b, c são elementos de um loop de Moufang e $ab.c = a.bc$, o subloop gerado por $\{a, b, c\}$ é um grupo.*

Para a demonstração do Teorema de Moufang ver Bruck [1]. Por este teorema, se $(x, y, z) \neq 1$, então $(x', y', z') \neq 1$ para qualquer permutação x', y', z' de x, y, z. Portanto se L tem um único quadrado não trivial e desta forma, um único associador não trivial, então $(x', y', z') = (x, y, z)$. Em outras palavras, o associador de três elementos é independente da ordem de seus elementos. Assim, a propriedade (2) do Teorema 1.4 também é válida para (x, wy, z) e (x, y, wz).

Proposição 1.2. *([2], Teorema 2) Seja F um loop de Moufang.*

1. *Se $(x, y, z)^2 = 1$ e todos os comutadores e associadores de F são centrais então*

$$[xy, z] = [x, z][y, z](x, y, z). \tag{5}$$

2. *Se os comutadores e associadores de F são centrais então*

$$(wx, y, z) = (w, y, z)(x, y, z). \tag{6}$$

Usando a proposição anterior se prova que $(x, wy, z) = (x, w, z)(x, y, z)$ e $(x, y, wz) = (x, y, w)(x, y, z)$. De fato, observe que $[xy, z] = [z, xy]$. Daí, $(x, y, z) = (z, x, y)$. Logo, $(x, y, wz) = (wz, x, y) = (w, x, y)(z, x, y) = (y, w, x)(y, z, x) = (x, y, w)(x, y, z)$. Analogamente temos o outro caso. Claramente obtemos o próximo resultado:

Proposição 1.3. *Se os quadrados e comutadores de um loop de Moufang F são centrais então temos*

$$(xy)^2 = x^2 y^2 [x, y].$$

2 Loops de Código

Nesta seção apresentamos uma introdução da Teoria de Loops de Código. Para isto, consideremos $\mathbf{F}_2^n$ como um espaço vetorial n-dimensional sobre o corpo de 2 elementos $\mathbf{F}_2 = \{0, 1\}$. Para vetores u e v em $\mathbf{F}_2^n$, $|v|$ (o peso de v) denota o número de coordenadas não-nulas de v e $|u \cap v|$ (peso de u intersecção v) denota o número de posições nas quais as coordenadas de u e v são ambas não-nulas, ou seja, se $u = (u_1, ..., u_n)$ e $v = (v_1, ..., v_n)$, com $u_i, v_i \in \mathbf{F}_2$ $\forall i = 1, \ldots, n$, então $|v| = |\{i | v_i = 1\}|$ e $|u \cap v| = |\{i | u_i = v_i = 1\}|$.

DOI: 10.5540/03.2018.006.01.0383

Definição 2.1. *Um código par é um subespaço $V \subseteq \boldsymbol{F}_2^n$ tal que $|v| \equiv 0 \ (mod\ 4)$ e $|u \cap v| \equiv 0 \ (mod\ 2)$ para quaisquer $u, v \in V$.*

Como exemplo de código par, considere o subespaço $V \subseteq \mathbf{F}_2^7$ com base $B = \{v_1, v_2, v_3\}$ onde

$$v_1 = (1,1,1,1,0,0,0), \ \ v_2 = (1,1,0,0,1,1,0), \ \ v_3 = (1,0,1,0,1,0,1).$$

Seja V um código par. Denotemos por $L(V)$ o conjunto $V \cup (-V)$. Definimos uma função $\phi : V \times V \to \{1, -1\}$ para todo $u, v, w \in V$, (chamada fator de conjunto) do seguinte modo:

1. $\phi(v, v) = (-1)^{\frac{|v|}{4}}$.
2. $\phi(v, w) = (-1)^{\frac{|v \cap w|}{2}} \phi(w, v)$.
3. $\phi(0, v) = \phi(v, 0) = 1$.
4. $\phi(v + w, u) = \phi(v, w + u)\phi(v, w)\phi(w, u)(-1)^{|v \cap w \cap u|}$.

Vamos definir uma operação binária $'.'$ sobre $L(V)$, chamada de produto e denotada, quando conveniente, por justaposição. Sejam $v, w \in V$, definimos

$$\begin{array}{l} v.w = \phi(v, w)(v + w), \ \text{ onde } \ \phi(v, w) \in \{1, -1\}, \\ v.(-w) = (-v).w = -(v.w), \\ (-v).(-w) = v.w. \end{array} \tag{7}$$

Logo, com o produto definido, temos que $(L(V), .)$, ou simplesmente $L(V)$, tem uma estrutura de loop. Para provarmos que $L(V)$ é loop devemos definir a igualdade de dois elementos. Como podemos pensar em $L(V)$ como o produto cartesiano de $\{1, -1\} \times V$, identificando v com $(1, v)$ e $-v$ com $(-1, v)$, e como a igualdade de dois pares ordenados é dada pela igualdade componente a componente, definimos que dois elementos x, y de $L(V)$ da forma $x = au$ e $y = bv$, com $a, b \in \{1, -1\}$, são iguais se $a = b$ e $u = v$. Sempre que denotarmos um elemento de $L(V)$ da forma $x = av$ significa que $a \in \{1, -1\}$ e $v \in V$. É bom observar também que podemos representar o produto de dois elementos quaisquer $x = au$ e $y = bv$ de $L(V)$ da forma $xy = (ab\phi(u, v))(u + v)$.

Observemos que $L(V)$ é finito. Logo, para provar que $L(V)$ é loop basta provar que para todo $a \in L(V)$ que as aplicações de translação $L_a : G \longrightarrow G$ e $R_a : G \longrightarrow G$, definidas respectivamente por $L_a(x) = a.x$ e $R_a(x) = x.a$, $\forall x \in G$ são injetoras (pelo Teorema 1.2) e que $L(V)$ tem elemento identidade.

Consideraremos através do lema abaixo algumas propriedades relativas ao código par V, que podem ser encontradas no artigo de Griess [5].

Lema 2.1. *Sejam x, y, z quaisquer elementos do código par V. Então:*

a) $|x \cap y \cap (z + x)| = |x \cap y \cap z|$;

b) $\frac{1}{2}|x \cap (x + y + z)| = \frac{1}{2}|x \cap y| + \frac{1}{2}|x \cap z| + |x \cap y \cap z|$;

DOI: 10.5540/03.2018.006.01.0383

c) $\frac{1}{2}|y \cap (x+z)| = \frac{1}{2}|y \cap x| + \frac{1}{2}|y \cap z| + |y \cap x \cap z|$.

Robert L. Griess Jr. demonstrou em [5] que um loop de código é um loop de Moufang e em [2], Orin Chein e Edgar G. Goodaire demonstraram que um loop de código satisfaz as propriedades do próximo teorema. Com base nas ideias destes artigos demonstramos de forma mais detalhada o próximo teorema.

Teorema 2.1. *O loop $L(V)$ é loop de Moufang e valem as seguintes propriedades, para quaisquer $u, v, w \in V$:*

$$\begin{aligned} &i)\ \ v^2 = (-1)^{\frac{|v|}{4}}0, \\ &ii)\ \ [u,v] = u^{-1}v^{-1}uv = (-1)^{\frac{|u\cap v|}{2}}0, \\ &iii)\ (u,v,w) = ((uv)w)((u(vw))^{-1}) = (-1)^{|u\cap v\cap w|}0. \end{aligned}$$

Demonstração. Seja $L(V) = V \cup (-V)$, onde V é um código par. Temos que provar que $L(V)$ satisfaz qualquer uma das identidades de Moufang. Vamos provar então que

$$(ax)(by).(cz)(ax) = [(ax).(by)(cz)]\,(ax), \ \ \forall\ \ ax, by, cz \in L(V) \tag{8}$$

Pela definição do produto em $L(V)$ para obtermos (8) basta provarmos que

$$\phi(x,y)\phi(z,x)\phi(x+y,z+x) = \phi(y,z)\phi(x,y+z)\phi(x+y+z,x), \tag{9}$$

onde $\phi : V\times V \to \{1,-1\}$ é a função fator de conjunto.

De fato, por um lado $(ax)(by).(cz)(ax) = (abac\phi(x,y)\phi(z,x)\phi(x+y,z+x))(y+z)$. Por outro lado, $[(ax).(by)(cz)]\,(ax) = (abac\phi(y,z)\phi(x,y+z)\phi(x+y+z,x))(y+z)$.

Relembremos duas propriedades da função fator de conjunto $\phi : V\times V \to \{1,-1\}$:

$$\begin{aligned} \phi(v,w) &= (-1)^{\frac{v\cap w}{2}}\phi(w,v); & (10)\\ \phi(v+w,u) &= \phi(v,w+u)\phi(v,w)\phi(w,u)(-1)^{|v\cap w\cap u|}. & (11) \end{aligned}$$

Pelo Lema 2.1a) e pela equação (11),

$$\begin{aligned} \phi(x,y)\phi(x+y,z+x) &= \phi(y,z+x)\phi(x,x+y+z)(-1)^{|x\cap y\cap z|} \overset{\text{eq.10 e lema 2.1}b)}{=} \\ &= \phi(y,z+x)\phi(x+y+z,x)(-1)^{\frac{|x\cap y|}{2}+\frac{|x\cap z|}{2}}. \end{aligned}$$

Em (10) ficamos com

$$\phi(y,z+x)\phi(x+y+z,x)\phi(z,x)(-1)^{\frac{|x\cap y|}{2}+\frac{|x\cap z|}{2}} = \phi(y,z)\phi(x,y+z)\phi(x+y+z,x).$$

Logo a equação (10) é equivalente à:

$$\phi(z,x)\phi(y,z)\phi(x,y+z)\phi(y,z+x)(-1)^{\frac{|x\cap y|}{2}+\frac{|x\cap z|}{2}} = 1.$$

Mas $\phi(z,x) = (-1)^{\frac{|x\cap z|}{2}}\phi(x,z)$ por (10). Assim, (9) é equivalente à

$$\phi(x,z)\phi(y,z)\phi(x,y+z)\phi(y,z+x)(-1)^{\frac{|x\cap y|}{2}} = 1. \tag{12}$$

DOI: 10.5540/03.2018.006.01.0383

Agora para provarmos a equação (12) basta observarmos que pelo Lema 2.1c) e pelas equações (10) e (11) temos:

$$\begin{aligned}\phi(x,z)\phi(x,z+y) &= \phi(x+z,y)\phi(z,y)(-1)^{|x\cap y\cap z|};\\ \phi(y,x+z) &= \phi(x+z,y)(-1)^{\frac{y\cap x}{2}+\frac{y\cap z}{2}+|y\cap x\cap z|};\\ \phi(y,z) &= (-1)^{\frac{|y\cap z|}{2}}\phi(z,y).\end{aligned}$$

Portanto $L(V)$ é loop de Moufang. Agora provaremos as propriedades mencionadas no Teorema.

i) Como $v^2 = \phi(v,v)(v+v)$, e por definição $\phi(v,v) = (-1)^{\frac{|v|}{4}}$, logo $v^2 = (-1)^{\frac{|v|}{4}}0$.

ii) Por definição,

$$\begin{aligned}u.v = \phi(u,v)(u+v) = (-1)^{\frac{|u\cap v|}{2}}\phi(v,u)(v+u) =\\ = (-1)^{\frac{|u\cap v|}{2}}0.\phi(v,u)(v+u) = (-1)^{\frac{|u\cap v|}{2}}0.(v.u).\end{aligned}$$

Portanto, pela unicidade do comutador, temos que $[u,v] = (-1)^{\frac{|u\cap v|}{2}}0$.

iii) Por definição, por um lado
$(uv)w = \phi(u,v)\phi(u+v,w)(u+v+w) == (-1)^{|u\cap v\cap w|}\phi(v,w)\phi(u,v+w)(u+v+w)$. Por outro lado,

$$\begin{aligned}(-1)^{|u\cap v\cap w|}0.(u(vw)) &= (-1)^{|u\cap v\cap w|}0.(\phi(v,w)\phi(u,v+w)(u+v+w)) =\\ &= (-1)^{|u\cap v\cap w|}\phi(v,w)\phi(u,v+w)\phi(0,u+v+w)(u+v+w) =\\ &= (uv)w.\end{aligned}$$

Portanto, pela unicidade do associador, temos que $(u,v,w) = (-1)^{|u\cap v\cap w|}0$. □

Definição 2.2. *O loop de Moufang $L(V)$ é chamado de loop de código. Dizemos que $L(V)$ tem posto m, se dim $_{\boldsymbol{F}_2}V = m$.*

Como exemplo, considere V o código par do exemplo anterior e $L(V) = V\cup(-V)$, com a operação de multiplicação definida como acima. Claramente temos que $L(V)$ é um loop de código de posto 3 com 16 elementos.

Definição 2.3. *Um loop de Moufang L é chamado E-loop se existe um subloop central Z de 2 elementos tal que $L/Z \in A$, onde A é a variedade de grupos com identidade $x^2 = 1$.*

O resultado principal desta seção relaciona loops de código e E-loops. Para demonstrarmos este resultado precisamos do próximo lema e do teorema principal demonstrado por Chein e Goodaire em [2].

Lema 2.2. *Seja L um loop de Moufang finito. O loop L é um E-loop se, e somente se, $|L^2| \leq 2$.*

Demonstração. Seja L um E-loop. Então existe um subloop central $Z = \{1, x\}$ tal que $\overline{y}^2 = \overline{1}$, $\forall \overline{y} \in L/Z$. Vamos mostrar que $L^2 \subseteq Z$. Se supormos que $e \in L^2$ seja tal que $e \neq 1, x$, então existirá $u \in L$ tal que $u^2 = e$. Daí teremos $\overline{u}^2 \neq 1$, contradizendo a definição de L. Logo $u^2 = 1$ ou $u^2 = x$, ou seja $L^2 \subseteq Z$. Portanto, $|L^2| \leq 2$.

Reciprocamente, suponhamos que $|L^2| \leq 2$. Caso $|L^2| = 1$, então L é um loop de Moufang comutativo. De fato, para quaisquer $x, y \in L$, $[x, y] = x^{-2}(xy^{-1})^2y^2 = 1$. Logo, pelo Corolário 1.1, qualquer elemento de L está no centro de L. Considere então um subloop central qualquer de dois elementos, digamos $Z(L) = \{1, x\}$, onde $x \in L$ é qualquer. Assim, $L/Z(L) \in A$, onde A é a variedade de grupos tais que $y^2 = 1$, $\forall y$. Agora suponhamos que $L^2 = \{1, e\}$ e que $L^2 = Z$. Pelo Teorema 1.3, L^2 é um subloop central e assim, podemos ver com simples cálculos que $\overline{y}^2 = \overline{1}$, $\forall \overline{y} \in L/Z$. □

Teorema 2.2. *(Chein e Goodaire, [2]) Um loop finito L é isomorfo a um loop de código se, e somente se, L é um loop de Moufang com $|L^2| \leq 2$.*

Teorema 2.3. *Um loop de Moufang L é um loop de código se, e somente se, L é um E-loop.*

Demonstração. A demonstração sai diretamente do Lema 2.2 e do Teorema 2.2. □

3 Conclusões

Neste trabalho introduzimos os loops de código a partir de códigos pares e mostramos com detalhes que loops de código são loops de Moufang com um único comutador não-trivial, um único associador não-trivial e um único quadrado não-trivial. Além disso, definimos E-loops e mostramos a relação existente entre E-loops e loops de código.

Referências

[1] R.H. Bruck, A survey of binary systems, Springer-Verlag, Berlin, 1958.

[2] O. Chein and E.G. Goodaire, Moufang Loops with a Unique Nonidentity Commutator (Associator, Square), *J. Algebra* 130, 369−384, 1990.

[3] E.G. Goodaire, E. Jaspers and C. Polcino, *Alternative Loop Rings*, North Holland Math, Studies N.184, Elsevier, Amsterdam, 1996.

[4] A. Grichkov and R. M. Pires, Code loops: automorphisms and representations, preprint. Available in: http://arxiv.org/abs/1412.2185

[5] R.L. Griess Jr., Code loops, *J.Algebra* 100, 224−234, 1986.

[6] H.O. Pflugfelder, *Quasigroups and Loops: Introduction*, Berlin, 1990.

[7] R. M. Pires, Loops de código: automorfismos e representações, Tese de Doutorado, IME/USP, São Paulo, 2011.

DOI: 10.5540/03.2018.006.01.0383