Arquitetura para o Multiplicador de Mastrovito Utilizando Circuitos de Limiar Linear

Andresso da Silva, Francisco M. de Assis, Marlo A. Santos

***Resumo*— Neste artigo é apresentada uma arquitetura para o multiplicador de Mastrovito usando circuitos de limiar linear. São determinados os polinômios irredutíveis ótimos para a construção do multiplicador de Mastrovito em corpos finitos $GF(2^m)$, para $2 \leq m \leq 16$. A arquitetura proposta fornece menor complexidade espacial teórica em relação às outras arquiteturas do multiplicador de Mastrovito. Quando há a utilização de polinômios irredutíveis ótimos, observa-se uma redução da complexidade espacial para $m > 11$.**

***Palavras-Chave*— Multiplicador de Mastrovito, Circuitos de Limiar Linear, Corpos Finitos, Função de Paridade**

***Abstract*— This paper presents an architecture for the Mastrovito multiplier using linear threshold circuits. Optimal irreducible polynomials are determined for the construction of the Mastrovito multiplier in finite field $GF(2^m)$, for $2 \leq m \leq 16$. The proposed architecture provides minor theoretical spatial complexity. However, when using the optimal irreducible polynomials, the proposed architecture will present minor spatial complexity for $m > 11$ when compared to other architectures that use linear threshold circuits.**

***Keywords*— Mastrovito Multiplier, Linear Threshold Circuits, Finite Fields, Parity Function**

I. Introdução

Operações em corpos finitos são fundamentais em códigos corretores de erro, teoria da codificação, processamento digital de sinais e criptografia moderna [2], [3], [4], [11]. Como a multiplicação é a operação mais complexa, é a que possui maior complexidade espacial e temporal [9]. Desta forma, o desenvolvimento de multiplicadores mais eficientes em termos de tempo e espaço é fundamental [11].

Mastrovito [5], [6] propôs uma arquitetura para multiplicação na base canônica em $GF(2^m)$. A multiplicação polinomial e redução por módulo é feita por meio da matriz $\mathbf{Z}$ que é função de um polinômio irredutível $P(x) \in GF(2)[x]$. Polinômios $P(x)$ com menor peso de Hamming, w_p, produzem circuitos com menores complexidades espaciais (i.e., menor número de portas), sendo os trinômios ($w_p = 3$) os que geram menores complexidades espaciais [5]. Entretanto, não existem trinômios para todos os valores de m [5].

O uso de portas de limiar linear (TG) para a multiplicação sobre corpos finitos foi apresentado por Lidiano [7], [8]. Foi demonstrado em [7] que a utilização de TGs reduz a complexidade espacial do multiplicador de Mastrovito e proporciona um atraso temporal fixo (i.e., o tempo que o circuito leva para gerar a saída). Em [8], a cota superior para a complexidade espacial do circuito foi deduzida para o caso de $P(x)$ ser um trinômio.

Neste artigo é apresentada uma arquitetura para o multiplicador de Mastrovito utilizando portas de limiar linear (TG). O desenvolvimento da arquitetura proposta buscou reduzir a complexidade espacial em comparação com a arquitetura apresentada por [8]. As cotas superiores para complexidade espacial da arquitetura de [8] e da arquitetura proposta aqui foram deduzidas para qualquer polinômio irredutível $P(x)$. Além disso, são investigados os polinômios $P(x)$ que geram as menores complexidades espaciais.

O trabalho está organizado como se segue. Na Seção I são apresentados os conceitos básicos relacionados às portas de limiar linear e a construção de circuitos utilizando tais portas. Na Seção II é apresentada a arquitetura proposta por Mastrovito. A arquitetura proposta neste artigo é apresentada na Seção III. Os resultados e discussões são apresentados na Seção IV e as conclusões são apresentadas na Seção V.

A. Portas e Circuitos de Limiar Linear

Uma porta de limiar linear (TG) é um elemento que computa uma função de limiar linear $f(X)$, em que $X = (x_1, ..., x_n, x_v)$, e é caracterizada por um vetor de pesos $\mathbf{w} = [w_1, \ldots, w_n, w_v]$ e um limiar t.

$$f(X) = \text{sgn}\left(\sum_{i=1}^{n} w_i \cdot x_i - w_v \cdot x_v - t\right) \tag{1}$$

em que $\text{sgn}(\cdot)$ é a função degrau unitário, definida por

$$\text{sgn}(k) = \begin{cases} 1 & \text{, se } k \geq 0 \\ 0 & \text{, se } k < 0 \end{cases} \tag{2}$$

e x_v é chamado de viés.

Uma porta de limiar linear genérica é exibida na Fig. 1.

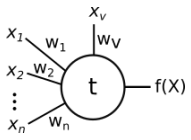

Fig. 1. Porta de limiar linear genérica.

Portas de limiar linear podem ser empregadas para implementar funções booleanas convencionais como AND, OR ou NOT, doravante chamadas de portas AON. Na Fig. 2 são apresentadas a construção da porta AND e da porta OR utilizando portas de limiar linear. Os pesos unitários serão omitidos.

Andresso da Silva, Universidade Federal de Campina Grande, e-mail: andresso.silva@ee.ufcg.edu.br; Francisco Marcos de Assis, Universidade Federal de Campina Grande, e-mail: fmarcos@dee.ufcg.edu.br.; Marlo A. Santos, Instituto Federal de Pernambuco, e-mail: marlo.santos@ee.ufcg.edu.br

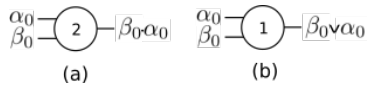

Fig. 2. (a) Porta AND de duas entradas utilizando porta de limiar linear. (b) Porta OR de duas entradas utilizando porta de limiar linear.

Circuitos de limiar linear são circuitos compostos exclusivamente por TGs. A complexidade espacial de um circuito de limiar linear é a quantidade de TGs que o circuito utiliza. A profundidade ou quantidade de camadas do circuito é o número máximo de portas que se percorre na propagação direta da entrada até a saída do circuito. O atraso total do circuito é a soma dos tempos que se leva para cada uma das camadas processar a entrada e gerar uma saída.

B. Implementação de funções simétricas usando circuitos de limiar linear

A função de paridade pode ser definida como

Definição 1: [Função de Paridade]

$$PAR_n(X) = \begin{cases} 1 & \text{, se } \sum_{i=1}^{n} x_i \text{ é par} \\ 0 & \text{, caso contrário} \end{cases} \tag{3}$$

em que $X = (x_1, \ldots, x_n) \in \{0,1\}^n$. $PAR_n(X)$ é equivalente a $PAR_n(X) = x_1 \oplus x_2 \oplus \ldots \oplus x_n$, em que $\oplus$ denota a operação XOR.

A função de paridade pertence a uma classe de funções chamadas de simétricas, definidas como:

Definição 2: [Funções Simétricas] Uma função booleana $f : \{0,1\}^n \rightarrow \{0,1\}$ é dita simétrica se f depende somente da soma dos valores de entrada, $\sum_{i=1}^{n} x_i$

Alguns resultados envolvendo funções simétricas são apresentados nos teoremas a seguir.

Teorema 1: [Construção com duas camadas] Qualquer função simétrica de n variáveis pode ser computada por um circuito de limiar linear de duas camadas usando pelo menos $\lceil \frac{n}{2} \rceil + 1$ portas.

Teorema 2: [Construção com três camadas] Qualquer função simétrica de n variáveis pode ser computada por um circuito de limiar linear de três camadas usando $\lceil 2\sqrt{n} \rceil + 1$ portas.

As provas do Teoremas 1 e do Teorema 2 podem ser encontradas em [10, p. 119] e [10, p. 120], respectivamente. A prova do Teorema 2 será apresentada aqui com algumas modificações e correções.

Demonstração: [Construção com três camadas] Uma função simétrica f pode ser definida a partir de um conjunto de inteiros s_i e S_i, $i = 1, \ldots, r$, com $s_i \leq S_i < s_{i+1}$ tal que $f(X) = 1$, $X = (x_1, \ldots x_n)$, se e, somente se, para algum i, $s_i \leq \sum_{j=1}^{n} x_j \leq S_i$.

O intervalo $[0, n]$ pode sempre ser dividido em d subintervalos consecutivos, $[s_{1_1}, s_{2_1} - 1], [s_{2_1}, s_{3_1} - 1], \ldots, [s_{d_1}, n]$, de forma que cada subintervalo (exceto possivelmente o último) contém o mesmo número l de inteiros s_i e S_i, em que $l \leq \lceil \frac{n}{2d_1} \rceil$. O i-ésimo subintervalo conterá os inteiros $s_{i_1} \leq S_{i_1} < s_{i_2} \leq S_{i_2} < \cdots < s_{i_l} \leq S_{i_l}$.

A primeira camada do circuito contém d portas de limiar linear, cada uma computando o valor z_i

$$z_i = \text{sgn}\left(\sum_{j=1}^{n} x_j - s_{i_1} + 1 \right), \text{ para } i = 1, \ldots, d. \tag{4}$$

Para cada $k = 1, \ldots, l$, define-se duas somas telescópicas como

$$T_k = S_{1_k} z_1 + \sum_{j=2}^{d} \left(S_{j_k} - S_{j-1_k} \right) z_j \tag{5}$$

$$t_k = s_{1_k} z_1 + \sum_{j=2}^{d} \left(s_{j_k} - s_{j-1_k} \right) z_j \tag{6}$$

de forma que T_k e t_k são combinações lineares das saídas da primeira camada.

A segunda camada contém $2l$ portas de limiar linear que computam Q_k ou q_k e que utilizam o inteiro T_k ou t_k como um tipo de valor de limiar, em que

$$Q_k = \text{sgn}\left(T_k - \sum_{j=1}^{n} x_j \right), \text{ e } \quad q_k = \text{sgn}\left(\sum_{j=1}^{n} x_j - t_k \right) \tag{7, 8}$$

Por fim, a porta de limiar linear de saída computa

$$f(X) = \text{sgn}\left(\sum_{k=1}^{l} 2\left(Q_k + q_k\right) - 2l - 1 \right) \tag{9}$$

Supondo que $\sum_{j=1}^{n} x_j \in \left[s_{m_1}, s_{(m-1)_1} - 1 \right]$, então as somas telescópicas T_k e t_k (ver Lema 3.1 de [10, p. 118]), para $k = 1, \ldots, l$, valem $T_k = S_{m_k}$ e $t_k = s_{m_k}$.

Pela definição de função simétrica, f(X) = 1 se e, somente se, para algum k ocorra $s_{m_k} \leq \sum_{j=1}^{n} x_j \leq S_{m_k}$. Assumindo que $f(X) = 1$ para uma dada entrada X, então existe um i tal que $s_{m_i} \leq \sum_{j=1}^{n} x_j \leq S_{m_i}$. Na segunda camada, $\sum_{j=1}^{n} x_j$ é comparado com $T_k = S_{m_k}$ e $-t_k = s_{m_k}$ para cada um dos k e as saídas serão Q_k e q_k, respectivamente. Como $s_{m_i} \leq \sum_{j=1}^{n} x_j \leq S_{m_i}$, os valores de saída da segunda camada (Q_k, q_k) geram

$$Q_k + q_k = \begin{cases} 2 & \text{, se } k = i \\ 1 & \text{, se } k \neq i \end{cases} \tag{10}$$

Desta forma, a saída da porta de limiar da terceira camada é dada por $\text{sgn}\left(\sum_{k=1}^{l} 2\left(Q_k + q_k\right) - 2l - 1 \right) = \text{sgn}\left(2l + 2 - 2l - 1\right) = 1$. De forma semelhante, se $f(X) = 0$, então existe um k tal que $Q_k + q_k = 1$ para todos os k. Sendo assim, a saída da porta de limiar da terceira camada é dada por $\text{sgn}\left(\sum_{k=1}^{l} 2\left(Q_k + q_k\right) - 2l - 1 \right) = \text{sgn}\left(2l - 2l - 1\right) = 0$. Portanto, o circuito de três camadas fornece a resposta correta para todas as entradas $X = (x_1, \ldots, x_n)$.

A primeira camada consiste de d portas, a segunda camada consiste de $2l \leq \lceil n/d \rceil$ portas e a última camada possui uma porta de saída. Assim sendo, serão necessárias no máximo $d + \lceil n/d \rceil + 1$ portas de limiar linear. Escolhendo $d = \lceil \sqrt{n} \rceil$, obtém-se que o tamanho do circuito com três camadas é $\lceil 2\sqrt{n} \rceil + 1$, o que conclui a prova do Teorema 2. ■

II. Multiplicador de Mastrovito

Sejam $A(x) = \alpha_0+\alpha_1 x+\cdots+\alpha_{m-1}x^{m-1}+x^m$ e $B(x) = \beta_0+\beta_1 x+\cdots+\beta_{m-1}x^{m-1}+x^m$ dois elementos de $GF(2^m)$ e seja $GF(2^m)$ gerado por um polinômio primitivo $P(x) = p_0 + p_1 x + \cdots + p_{m-1}x^{m-1} + x^m \in GF(2)[x]$. O produto $A(x)B(x) \bmod P(x)$ é dado por

$$\begin{aligned} C(X) &= A(x)B(x) \bmod P(x) \\ &= \beta_0 \left(A(x) \bmod P(x)\right) + \beta_1 \left(xA(x) \bmod P(x)\right) \\ &\quad + \cdots + \beta_{m-1} \left(x^{m-1}A(x) \bmod P(x)\right) \end{aligned} \tag{11}$$

Define-se

$$Z_j(x) = x^j A(x) \bmod P(x) = \sum_{i=0}^{m-1} f_{i,j}x^i \tag{12}$$

em que $j = 0, 1, \ldots, m-1$ e $f_{i,j} \in GF(2)$. Desta forma, a Eq. 11 pode ser escrita como

$$C(x) = \beta_0 Z_0(x) + \beta_1 Z_1(x) + \cdots + \beta_{m-1}Z_{m-1}(x). \tag{13}$$

Em forma matricial, a Eq. 13 pode ser escrita como

$$\begin{aligned} \mathbf{C} &= \begin{pmatrix} \gamma_0 \\ \gamma_1 \\ \vdots \\ \gamma_{m-1} \end{pmatrix} \\ &= \begin{pmatrix} f_{0,0} & f_{0,1} & \cdots & f_{0,m-1} \\ f_{1,0} & f_{1,1} & \cdots & f_{1,m-1} \\ \vdots & \vdots & \ddots & \vdots \\ f_{m-1,0} & f_{m-1,1} & \cdots & f_{m-1,m-1} \end{pmatrix} \begin{pmatrix} \beta_0 \\ \beta_1 \\ \vdots \\ \beta_{m-1} \end{pmatrix} \\ &= \mathbf{ZB} \end{aligned} \tag{14}$$

em que $\mathbf{Z}$ é chamada de matriz produto e depende unicamente do polinômio $A(x)$ e do polinômio irredutível $P(x)$. Para se obter os valores de $f_{i,j}$, define-se $\mathbf{Q}$, a chamada de matriz de redução como

$$\begin{aligned} \begin{pmatrix} x^m \\ x^{m+1} \\ \vdots \\ x^{2m-2} \end{pmatrix} \bmod P(x) &= \mathbf{Q} \begin{pmatrix} 1 \\ x \\ \vdots \\ x^{m-1} \end{pmatrix} = \\ &= \begin{pmatrix} q_{0,0} & q_{0,1} & \cdots & q_{0,m-1} \\ q_{1,0} & q_{1,1} & \cdots & q_{1,m-1} \\ \vdots & \vdots & \ddots & \vdots \\ q_{m-2,0} & q_{m-2,1} & \cdots & q_{m-2,m-1} \end{pmatrix} \begin{pmatrix} 1 \\ x \\ \vdots \\ x^{m-1} \end{pmatrix} \end{aligned} \tag{15}$$

Desta forma, os elementos $f_{i,j}$ de $\mathbf{Z}$ são dados por

$$f_{i,0} = \alpha_i, \text{para } i = 0, 1, \ldots, m-1 \text{ e} \tag{16}$$

$$f_{i,j} = \operatorname{sgn}(i-j)\alpha_{i-j} + \sum_{t=0}^{j-1} q_{j-1-t,i}\alpha_{m-1-t} \tag{17}$$

$$\tag{18}$$

para $i = 0, 1, \ldots, m-1$ e $j = 1, \ldots, m-1$.

Pela Eq. 14, sabe-se que

$$\gamma_i = Bf_{i,-} = \beta_0 f_{i,0} + \beta_1 f_{i,1} + \cdots + \beta_{m-1}f_{i,m-1} \tag{19}$$

em que $i = 0, 1, \ldots, m-1$ e $f_{i,-}$ denota a i-ésima linha da matriz $\mathbf{Z}$, que também é dada por $x^j A(x) \bmod P(x)$.

Usando $P(x) = 1 + x + x^4$, um polinômio irredutível em $GF(4)$, pode-se obter por meio da Eq. 15 a matriz de redução $\mathbf{Q}$ como

$$\mathbf{Q} = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \end{pmatrix}$$

Usando as Eq. 16 e Eq. 17, pode-se obter a matriz de multiplicação

$$\mathbf{Z} = \begin{pmatrix} \alpha_0 & \alpha_3 & \alpha_2 & \alpha_1 \\ \alpha_1 & \alpha_0+\alpha_3 & \alpha_2+\alpha_3 & \alpha_1+\alpha_2 \\ \alpha_2 & \alpha_1 & \alpha_0+\alpha_3 & \alpha_3+\alpha_2 \\ \alpha_3 & \alpha_2 & \alpha_1 & \alpha_0+\alpha_3 \end{pmatrix} \tag{20}$$

Agora usando a Eq. 19, tem-se que

$$\gamma_0 = \beta_0\alpha_0 + \beta_1\alpha_3 + \beta_2\alpha_2 + \beta_3\alpha_1 \tag{21}$$

$$\gamma_1 = \beta_0\alpha_1 + \beta_1\alpha_0 + \beta_1\alpha_3 + \beta_2\alpha_2 + \beta_2\alpha_3 + \beta_3\alpha_1 + \beta_3\alpha_2 \tag{22}$$

$$\gamma_2 = \beta_0\alpha_2 + \beta_1\alpha_1 + \beta_2\alpha_0 + \beta_2\alpha_3 + \beta_3\alpha_2 + \beta_3\alpha_3 \tag{23}$$

$$\gamma_3 = \beta_0\alpha_3 + \beta_1\alpha_1 + \beta_2\alpha_1 + \beta_3\alpha_0 + \beta_3\alpha_3 \tag{24}$$

Desta forma, as Eq. 21, Eq. 22, Eq. 23, Eq. 24 definem as conexões de portas AND e XOR que devem ser feitas para a obtenção de γ_i, $i = 0, 1, 2, 3$.

III. Arquitetura Proposta

A arquitetura proposta utiliza TGs para calcular a soma de produtos definidos na Eq. 19. Para determinar os circuitos, será útil definir a chamada largura de uma equação.

Definição 3: [Largura de uma equação f] Define-se a largura de uma equação f, WD_f, como o número de coeficientes α_κ que compõem f.

Desta forma, as larguras dos γ_i são $WD_{\gamma_0} = 4$ (Eq. 21), $WD_{\gamma_1} = 7$ (Eq. 22), $WD_{\gamma_2} = 6$ (Eq. 23) e $WD_{\gamma_3} = 5$ (Eq. 24), respectivamente. As larguras WD_{γ_i} definirão o número de entradas da função de paridade, o intervalo $[0, WD_{\gamma_i}]$, o número d de subintervalos e o número l de inteiros contidos nesses subintervalos.

Para γ_0, $d = \sqrt{WD_{\gamma_0}} = 2$ e $l \leq \lceil WD_{\gamma_0}/(2 \cdot d)\rceil = 1$ e os subintervalos podem ser definidos como $[1, 2], [3, 4]$, de forma que, $s_{1_1} = 1 = S_{1_1}$, $s_{2_1} = 3 = S_{2_1}$. O circuito para computar γ_0 possui $d = 2$ portas na primeira camada, $2l = 2$ portas na segunda camada e 1 porta na camada de saída. Usando a Eq. 4, os limiares das portas da primeira camada são dados por $s_{i_1} - 1$, para $i = 1, 2$.

As entradas das portas da segunda camada são obtidas analisando a Eq. 5 e a Eq. 6. As portas da segunda camada recebem como entrada T_k ou $-t_k$ e valores de viés iguais ao oposto da soma das entradas da primeira camada (para T_k) ou a soma das entradas da primeira camada (para t_k) da função de paridade. Os limiares das portas da segunda camada valem zero.

Calculando T_k e t_k a partir da Eq. 5 e da Eq. 6, tem-se que $T_1 = 1z_1 + 2z_2$ e $t_1 = 1z_1 + 2z_2$. Desta forma, a entrada da primeira porta vale $T_1 = 1 + 2z_2$ e o viés

vale $v_0 = -(\beta_0\alpha_0 + \beta_1\alpha_3 + \beta_2\alpha_2 + \beta_3\alpha_1)$, o que define o vetor de pesos dessa porta como $\mathbf{w} = [1, 2, -1]$. A entrada da segunda porta vale $-t_1 = -1 - 2z_2$ e o viés vale $v_0 = (\beta_0\alpha_0 + \beta_1\alpha_3 + \beta_2\alpha_2 + \beta_3\alpha_1)$ e o vetor de pesos desta porta vale $\mathbf{w} = [-1, -2, 1]$.

Os valores dos pesos e limiares da porta da última camada são obtidos a partir da Eq. 9, que fornece o vetor de pesos como $\mathbf{w} = [2, 2, 0]$. O limiar vale $t = 2l+1 = 3$. Seguindo um procedimento semelhante é possível calcular γ_1, γ_2 e γ_3. Na Fig. 3 é exibido o circuito que computa a função de paridade, representado pelo bloco PAR, para γ_0.

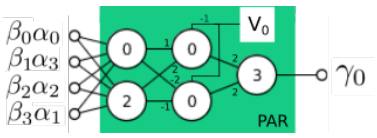

Fig. 3. Circuito de limiar linear para computar γ_0.

Cada um dos produtos $\beta_i\alpha_j$ pode ser determinado a partir de uma TG implementando uma porta AND. Um bloco denominado MULT pode ser definido como um circuito que recebe os elementos $A(x)$ e $B(x)$ e fornece como saída os produtos $\beta_i\alpha_j$, $i = 0, \ldots, m-1$, $j = 0, \ldots, m-1$. Na Fig. 4 são exibidos os blocos MULT e PAR para um multiplicador em $GF(4)$ usando $P(x) = 1 + x + x^4$.

A. Complexidade Espacial

Usando a Eq. 17 e a Definição 3, pode-se concluir que a largura de cada f_{ij} é de, no máximo, $WD_{f_{ij}} = j+1$. Usando a Eq. 19, tem-se que a largura de γ_i será no máximo

$$WD_{\gamma_i} = \sum_{j=0}^{m-1} WD_{f_{ij}} = \sum_{j=0}^{m-1} j + 1 = \frac{m^2}{2} + \frac{m}{2}.$$

O número de TGs é determinado por $\#TG = 2\sqrt{WD_{\gamma_i}}+1$ (ver Teorema 2). Sabendo disso, o número máximo de TGs para a construção da função da paridade é

$$\#TG_{XOR} = \sum_{i=0}^{m-1} 2\sqrt{WD_{\gamma_i}} + 1 = m + 2m\sqrt{\frac{m^2}{2} + \frac{m}{2}}. \quad (25)$$

Considerando as n^2 TGs necessárias para calcular os coeficientes $\beta_i\alpha_j$, o número total de portas de limiar linear para a construção do multiplicador de Mastrovito vale

$$\#TG = \#TG_{XOR} + m^2 \approx \left(1 + \sqrt{2}\right) m^2 + m. \quad (26)$$

Usando os mesmos argumentos, pode-se chegar ao número máximo de TGs para a construção do Multiplicador apresentada por [8], sendo esse número dado por

$$\#TG = m^2 + \sum_{i=0}^{m-1} \frac{WD_{\gamma_i}}{2} + 1 = \frac{m^3}{4} + \frac{5}{4}m^2 + m. \quad (27)$$

Na Fig. 5 são apresentadas as complexidades espaciais máximas para arquiteturas do multiplicador de Mastrovito utilizando as portas tradicionais (AON) [1], a construção com duas camadas e três camadas.

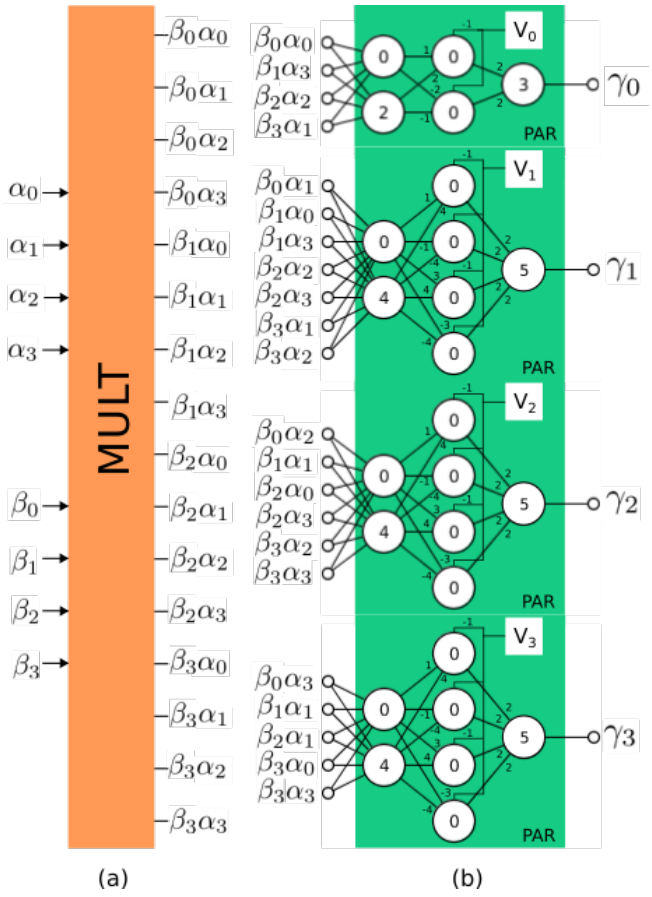

Fig. 4. Blocos para a construção do multiplicador de Mastrovito em $GF(4)$ usando $P(x) = 1 + x + x^4$.(a) Bloco MULT onde são calculados todos dos produtos $\beta_i\alpha_j$, para $i = 0, 1, 2, 3$ e $j = 0, 1, 2, 3$. (b) Conjunto de blocos PAR que realizam a soma dos produtos $\beta_\xi\alpha_k$ associados a cada um dos γ_i para $i = 0, 1, 2, 3$.

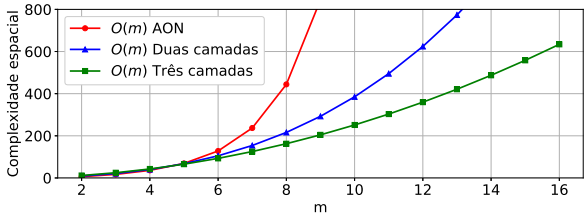

Fig. 5. Complexidades espaciais máximas para arquiteturas do multiplicador de Mastrovito.

IV. Resultados e Discussões

Foi feita uma busca exaustiva nos polinômios irredutíveis em $GF(2^m)$, para $2 \leq m \leq 16$, com o objetivo de determinar as complexidades espaciais do multiplicador de Mastrovito utilizando a arquitetura com duas e três camadas. O polinômio irredutível $P(x)$ que produziu a menor complexidade espacial foi chamado de $P(x)$ ótimo. Os resultados são exibidos na Tabela I.

Com o auxílio da Fig. 6, é possível notar que, apesar da arquitetura proposta que utiliza três camadas possuir menor

TABLE I

COMPLEXIDADE ESPACIAL DO MULTIPLICADOR DE MASTROVITO.

	AON	**Duas camadas**		**Três camadas**	
$GF(2^m)$	O(m)	O(m)	P(x) Ótimo	O(m)	P(x) Ótimo
m=4	36	40	31	43	39
m=8	444	216	139	163	138
m=12	6248	624	338	360	291
m=16	98556	1360	560	635	468

complexidade espacial teórica, quando se utiliza o $P(x)$ ótimo a diferença entre a complexidade entre as duas arquiteturas só se torna considerável para $m > 11$. Em aplicações nas quais $m \leq 11$ e a complexidade temporal é um fator crítico, a construção com duas camadas pode ser mais adequada. Os

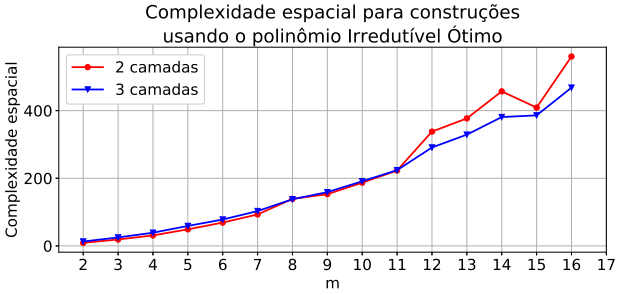

Fig. 6. Complexidades espaciais para construções com duas e três camadas usando polinômios ótimos.

polinômios ótimos para as arquiteturas com duas e três camadas são exibidos na Tabela II. Como esperado, os polinômios irredutíveis com menor peso de Hamming, w_p, produziram as menores complexidades espaciais.

TABLE II

POLINÔMIOS ÓTIMOS PARA A CONSTRUÇÃO USANDO DUAS E TRÊS CAMADAS.

	Duas Cam.		**Três Cam.**			**Duas Cam.**		**Três Cam.**	
m	P(x)	w_p	P(x)	w_p	**m**	P(x)	w_p	P(x)	w_p
2	7	3	7	3	**10**	1033	3	1033	3
3	13	3	13	3	**11**	2053	3	2053	3
4	25	3	25	3	**12**	4201	5	4201	5
5	37	3	41	3	**13**	8489	5	8489	5
6	97	3	97	3	**14**	16553	5	16553	5
7	131	3	131	3	**15**	32771	3	32771	3
8	391	5	391	5	**16**	67681	5	67681	5
9	529	3	529	3					

Na Fig. 7 são apresentadas as complexidades espaciais para o polinômio ótimo e o polinômio que gerou a maior complexidade espacial. É possível observar que para o caso da arquitetura de duas camadas ou de três camadas a utilização do polinômio ótimo fornece um valor de complexidade espacial inferior às cotas superiores estimadas nas Eq. 27 e Eq. 26.

V. CONCLUSÕES

A multiplicação em corpos finitos é fundamental em campos como criptografia, códigos corretores de erro e processamento digital de sinais. Como ela é a operação mais custosa espacial e temporalmente, multiplicadores eficientes são necessários.

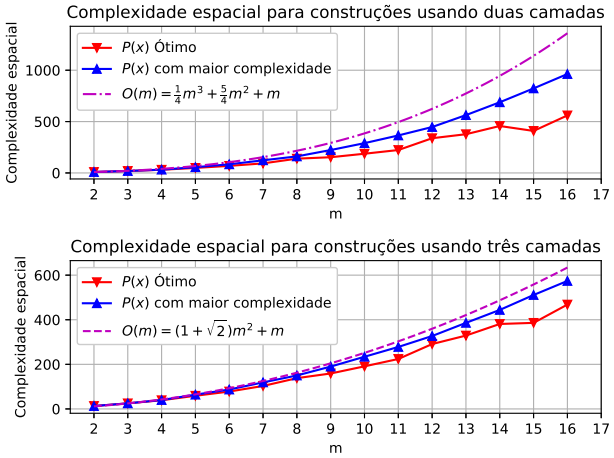

Fig. 7. Complexidades espaciais para os polinômios ótimos e para os polinômios que geraram maior complexidade espacial.

Neste artigo foi apresentada uma arquitetura para o multiplicador de Mastrovito implementado utilizando circuitos de limiar linear. Foram determinados os polinômios irredutíveis ótimos para a construção do multiplicador de Mastrovito em $GF(2^m)$, $2 \leq m \leq 16$, utilizando a arquitetura proposta e a arquitetura apresentada por Lidiano [7], [8].

A arquitetura proposta para o multiplicador de Mastrovito fornece menor complexidade espacial teórica. Quando se utiliza os polinômios irredutíveis ótimos, a arquitetura proposta passa a apresentar menor complexidade espacial para $m > 11$, quando comparada com a arquitetura proposta em [7].

REFERENCES

[1] Lidiano Augusto Nobrega de Oliveira. Multiplicador em corpo finito utilizando redes neurais discretas. Master's thesis, Universidade Federal de Campina Grande, 2000.

[2] Haining Fan and M. Anwar Hasan. A survey of some recent bit-parallel $gf(2^n)$ multipliers. *Finite Fields and Their Applications*, 32:5 – 43, 2015. Special Issue : Second Decade of FFA.

[3] S Gashkov and I Sergeev. Bit-Parallel Circuits for Arithmetic in Finite Fields. (05):104–125, 2008.

[4] J. L. Imaña. Efficient fpga implementation of binary field multipliers based on irreducible trinomials. In *2018 IEEE 26th Annual International Symposium on Field-Programmable Custom Computing Machines (FCCM)*, pages 222–222, April 2018.

[5] E.D. Mastrovito. Vlsi designs for multiplication over finite fields $gf(2^m)$. In Teo Mora, editor, *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes*, pages 297–309, Berlin, Heidelberg, 1989. Springer Berlin Heidelberg.

[6] E.D. Mastrovito. *VLSI Architectures for Computations in Galois Fields*. Linköping studies in science and technology: Dissertations. Department of Electrical Engineering, Linköping University, 1991.

[7] Lidiano Oliveira and Francisco M. de Assis. A New Architecture for Multipliers in $GF(2^n)$ Using Discrete Neural Networks. *Proceedings of the IV Brazilian Conference on Neural Networks*, 1:888–899, 1999.

[8] Lidiano Oliveira and Francisco M. de Assis. A Parallel Multiplier for $GF(2^n)$. *Anais do XVII Simpósio Brasileiro de Telecomunicações*, 1:677–681, 1999.

[9] Ajitha S S and Retheesh Dhason. Efficient implementation of bit parallel finite field multipliers. *International Journal of Research in Engineering and Technology*, 03:661–667, 03 2014.

[10] K.Y. Siu, V.P. Roychowdhury, and T. Kailath. *Discrete Neural Computation: A Theoretical Foundation*. Prentice-Hall information and system sciences series. Prentice Hall PTR, 1995.

[11] B. Sunar and C. K. Koc. Mastrovito multiplier for all trinomials. *IEEE Transactions on Computers*, 48(5):522–527, May 1999.