

Modelagem Quantum-Fuzzy para o E \ominus - Operador XOR

Bruna Novack¹, Juliano Buss² e Renata Reiser³

¹ Universidade Federal de Pelotas (UFPEL), Pelotas-RS, Brasil – bcdnovack@inf.ufpel.edu.br

² Universidade Federal de Pelotas (UFPEL), Pelotas-RS, Brasil – jsbuss@inf.ufpel.edu.br

³ Universidade Federal de Pelotas (UFPEL), Pelotas-RS, Brasil - reiser@inf.ufpel.edu.br

1. INTRODUÇÃO

A fusão de informação provida pela Computação Quântica (CQ) e Lógica Fuzzy (LF) permite modelar incertezas de formas distintas, com relevantes benefícios para ciência e tecnologias computacionais. A junção dessas duas áreas pode resultar em uma excelente abordagem para solucionar de forma mais eficiente problemas complexos da computação clássica. De um lado, a CQ utiliza fundamentos da Mecânica Quântica para modelar incertezas de sistemas físicos de dimensões nanométricas. Por outro lado, a LF modela a incerteza na expressão do raciocínio humano e a imprecisão na medida de características e atributos dos sistemas, via variáveis linguísticas associadas a relações de pertinência dos Conjuntos Fuzzy (CFs).

Este trabalho foca na interpretação de algoritmos flexíveis envolvendo o conectivo X(NOR) via operadores quânticos, considerando a integração de conceitos da CQ e FL.

As relevantes aplicações científicas e tecnológicas em diversas áreas do conhecimento e da computação, como na criptografia (ABOUGHALIA AND ALKISHIWO, 2018), motivam novos estudos de modelagem do operador XOR.

E, dentre as várias definições de operadores fuzzy X(N)OR (BEDREGAL et al., 2013a), consideramos a extensão fuzzy da abordagem clássica do XOR, interpretando a diferença entre a união e a intersecção de dois conjuntos X e Y, dada pela expressão: $x \ominus y = ((x \vee y) - (x \wedge y))$, para $x \in X, y \in Y$.

O presente artigo encontra-se estruturado da seguinte maneira: a Seção 2 aborda os conceitos fundamentais da LF necessários para compreensão do desenvolvimento desta pesquisa, além de realizar uma breve discussão sobre as transformações e circuitos quânticos. Na Seção 3, é exposta a aplicação da CQ com o propósito de modelar os conectivos da LF, os quais auxiliam a progressão deste estudo. O conectivo XOR, que constitui o foco deste artigo, é abordado na Seção 4. Finalmente, na última Seção são apresentadas as conclusões decorrentes do desenvolvimento deste trabalho.

2. PRELIMINARES

A lógica clássica define as relações de pertinência de modo rígido (crisp), onde um elemento pertence ou não a um dado conjunto. A Teoria dos Conjuntos Fuzzy é uma extensão da teoria clássica, pois via uma função de pertinência é possível que um elemento pertença parcialmente a um conjunto, com um grau de pertinência associado. Seja um CF A, em um universo U, não vazio, possuindo a função de pertinência representado por $f_A(x)$, onde $0 \leq f_A(x) \leq 1$, dado pela expressão $A = \{(x, f_A(x)) : x \in X\}$ (KLEMENT AND NAVARA, 1999).

Intersecções (uniões) de CFs são definidas por t-(co)normas, classe de funções $T(S) : [0, 1]^2 \rightarrow [0, 1]$ que são comutativas, associativas, monotônicas e

satisfazem, respectivamente, $T(x, 1) = x$ e $S(x, 0) = x$, $\forall x \in [0, 1]$. Veja exemplos ilustrando membros da classe de t-(co)normas.

1. Gödel: $T_G(x, y) = \min(x, y)$; e $S_G(x, y) = \max(x, y)$;
2. Lukasiewicz: $T_L(x, y) = \max(x + y - 1, 0)$; e $S_L(x, y) = \min(x + y, 1)$;
3. Produto: $T_P(x, y) = x \cdot y$; e $S_P(x, y) = x + y - x \cdot y$.

Uma negação fuzzy $N : [0, 1] \rightarrow [0, 1]$ é uma função que satisfaz: $N(0) = 1$ e $N(1) = 0$; e é monotônica decrescente: se $x \leq y$, $N(x) \geq N(y)$, $\forall x, y \in [0, 1]$.

Se a negação fuzzy satisfaz a propriedade de involutividade:

(N3) $N(N(x)) = x$, $\forall x \in [0, 1]$, então ela é dita uma negação forte.

A negação padrão (Zadeh) é forte e é expressa por: $N_S(x) = 1 - x$.

O conectivo fuzzy XOR $E : [0, 1]^2 \rightarrow [0, 1]$ e sua construção dual, o conectivo difuso XNOR $D : [0, 1]^2 \rightarrow [0, 1]$ são definidos pelas propriedades:

E1: $E(1, 1) = E(0, 0) = 0$ e $E(1, 0) = 1$; D1: $D(1, 1) = D(0, 0) = 1$ e $D(1, 0) = 0$;

E2: $E(x, y) = E(y, x)$; D2: $D(x, y) = D(y, x)$;

E3: Se $x \leq y$ então $E(0, x) \leq E(0, y)$; D3: Se $x \leq y$ então $D(0, x) \geq D(0, y)$;

Se $x \leq y$ então $E(1, x) \leq E(1, y)$. Se $x \leq y$ então $D(1, x) \geq D(1, y)$.

Em BEDREGAL et al. (2013b), as funções $E_{S,T}, D_{S,T} : [0, 1]^2 \rightarrow [0, 1]$ são:

$$E_{S,T}(x, y) = S(x, y) - T(x, y); \text{ e } D_{S,T}(x, y) = N(N(T(x, y))) - N(S(x, y)). \quad (1)$$

E, usando funções S_P e T_P , tem-se as funções $E_{S_P, T_P}, D_{S_P, T_P} : [0, 1]^2 \rightarrow [0, 1]$:

$$E_{S,T}(x, y) = x + y - 2xy \quad \text{e} \quad D_{S,T}(x, y) = 1 - x - y + 2xy. \quad (2)$$

No contexto da CQ, as transformações quânticas, ou portas quânticas, são responsáveis pela manipulação dos estados quânticos. Tais transformações podem ser unitárias, controladas e de medidas. O bit quântico (qubit) é a unidade básica de informação na CQ, composto por um vetor unitário e bidimensional com componentes complexos, equacionada como $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, com amplitudes α e β , que influenciam na probabilidade de encontrar o elemento na posição de medida. Uma medição é uma operação que realiza a leitura de um qubit, a partir da projeção sobre os estados da base computacional.

Este estudo considera o modelo de circuitos quânticos. A porta Toffoli tem sua expressão matricial representada na Figura 1, operando sobre três qubits, sendo os dois primeiros de controle ($|\psi\rangle$ e $|\varphi\rangle$) indicados na Figura 2, e o terceiro é o qubit alvo ($|\omega\rangle$) que sofre transformações (troca de amplitudes) conforme o valor dos qubits de controle (NIELSEN AND CHUANG, 2011).

$$T|\chi\rangle = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} \alpha \\ \beta \\ \gamma \\ \delta \\ \epsilon \\ \theta \\ v \\ \sigma \end{pmatrix} = \begin{pmatrix} \alpha \\ \beta \\ \gamma \\ \delta \\ \epsilon \\ \theta \\ v \\ \sigma \end{pmatrix}$$

Figura 1. Expressão Matricial da Porta T .

Figura 2. Circuito da Porta T .

3. MODELAGEM, INTERPRETAÇÃO E SIMULAÇÃO PARA XOR FUZZY E $^\ominus$

Os CFs podem ser obtidos a partir de superposições de CFs associados com registradores quânticos. Interpretações das operações fuzzy podem ser

obtidas através da composição de portas quânticas atuantes sobre a definição de registradores fuzzy quânticos. As modelagens apresentadas a seguir serão desenvolvidas considerando as funções de pertinência $f, g \rightarrow [0, 1]$ associadas com dois CFs A e B , e o par $|S_{f_i}\rangle$ e $|S_{g_i}\rangle$ de estados:

$$|S_{f_i}\rangle = \sqrt{fA(i)}|1\rangle + \sqrt{1 - fA(i)}|0\rangle \text{ e } |S_{g_i}\rangle = \sqrt{fB(i)}|1\rangle + \sqrt{1 - fB(i)}|0\rangle. \quad (3)$$

As seguintes instâncias para os estados $|S_{A_i}\rangle$ e $|S_{B_i}\rangle$ serão utilizados para realizar cálculos sobre a amplitude dos estados obtidos durante a sua evolução:

$$|S_{A_i}\rangle = \frac{\sqrt{2}}{2}|1\rangle + \frac{\sqrt{2}}{2}|0\rangle \text{ e } |S_{B_i}\rangle = \frac{\sqrt{3}}{3}|1\rangle + \frac{\sqrt{3}}{3}|0\rangle. \quad (4)$$

Em MANNUCCI (2006), a interpretação quantum-fuzzy para a operação de complemento a operação de complemento representando a negação fuzzy padrão é expressa por: $NOT(|S_{f_i}\rangle) = \sqrt{1 - fA}|1\rangle + \sqrt{fA}|0\rangle$.

Sejam $|S_{f_i}\rangle$ e $|S_{g_i}\rangle$ estados quânticos dadas pelas Eq. (3)a e Eq. (3)b. O conectivo XOR fuzzy E^\ominus , dado na Figura 3, e definido pela Eq. (1)a, é o operador XOR_\ominus :

$$\begin{aligned} XOR_\ominus(|S_{f_i}\rangle, |S_{g_i}\rangle) &= OR(|S_{f_i}\rangle, |S_{g_i}\rangle) - AND(|S_{f_i}\rangle, |S_{g_i}\rangle) \\ &= NOT_{3,4,5}(\mathcal{T}_5^{3,4}(NOT_{3,4}(NOT_1(\mathcal{T}_3^{1,2}(NOT|S_{f_i}\rangle, |S_{g_i}\rangle, |0\rangle)), \\ &\quad NOT_2(\mathcal{T}_4^{1,2}(|S_{f_i}\rangle, NOT|S_{g_i}\rangle, |0\rangle)), |0\rangle))). \end{aligned} \quad (5)$$

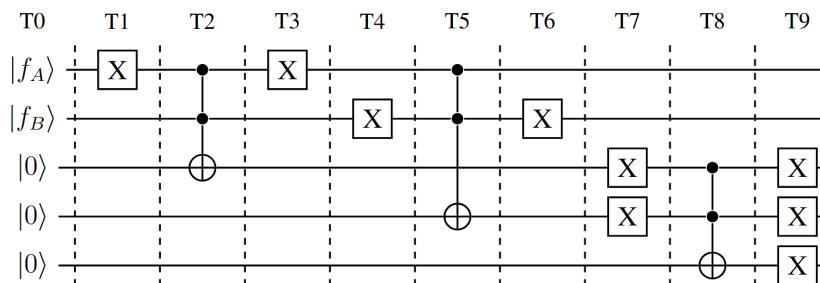


Figura 3. Circuito para E_\ominus , apresentando entradas e evolução no período T0-T9.

Na representação gráfica do conectivo E^\ominus ocorrem dez etapas de evolução temporal (de T0 a T9) estruturados em um sistema de dimensão espacial de cinco qubits. Assim, na coluna T9 da Tabela 2, apresentam-se os quadrados dos coeficientes não nulos dos estados clássicos (base computacional) em uma evolução temporal das computações relacionadas ao operador fuzzy XOR E^\ominus . E o estado quântico obtido e descrito pela Eq. (6) está expresso logo a seguir:

$$\begin{aligned} |\ominus 9\rangle &= \sqrt{(1 - fA)(1 - fB)}|0000\rangle + \sqrt{(1 - fA)fB}|01101\rangle + \\ &\quad \sqrt{fA(1 - fB)}|10011\rangle + \sqrt{fAfB}|11000\rangle. \end{aligned} \quad (6)$$

De um lado, uma medida realizada no 5º qubit (mas relacionada ao estado $|1\rangle$) do estado quântico descrito pela Eq. (6) resulta no estado final:

$$|\ominus '9\rangle = \frac{1}{\sqrt{1-fA-fB+2fAfB}}(\sqrt{(1 - fA)fB}|01101\rangle + \sqrt{fA(1 - fB)}|10011\rangle), \quad (7)$$

com a probabilidade correspondendo à expressão: $p(1) = fA + fB - 2fAfB$, indicando o grau de pertinência de um elemento $x \in X$ no CF $A \ominus B$ obtido pela aplicação de um conectivo fuzzy XOR E^\ominus e tomando fA, fB como argumentos.

Amplitudes não nulas	T0	T3	T6	T9
$(1 - f_A) * (1 - f_B)$	00000	00000	00000	00000
$(1 - f_A) * f_B$	01000	01100	01100	01101
$f_A * (1 - f_B)$	10000	10000	10010	10011
$f_A * f_B$	11000	11000	11000	11000

Tabela 2. Evolução Temporal dos Estados Quânticos na Modelagem do XOR E_{\ominus} .

E, uma medida realizada no 5º qubit (referente ao estado $|0\rangle$) retorna:

$$|\ominus^{\prime\prime}9\rangle = \frac{1}{\sqrt{f_A+f_B-2f_Af_B}} (\sqrt{(1-f_A)(1-f_B)}|0000\rangle + \sqrt{f_Af_B}|11000\rangle), \quad (8)$$

apresentando uma probabilidade dada por: $p(0) = 1 - (f_A + f_B - 2f_Af_B)$.

Uma simulação consistente com os registradores dados na Eq. (6) tomando os estados iniciais da Eq. (4)a e Eq. (4)b, resulta após medições, nos estados (i) $|\ominus\rangle$ e (ii) $|\ominus^{\prime\prime}\rangle$ e respectivas probabilidades: (i) $p(1) = 0.5$; (ii) $p(0) = 0.5$.

5. CONCLUSÃO

O artigo mostra a utilização da CQ para a modelagem do conectivo XOR da LF, desenvolvendo sua modelagem e analisando as suas amplitudes. Tal modelagem é atrativa pelo fator de obter vantagens tanto da CQ quanto da LF, podendo solucionar rapidamente problemas complexos da computação clássica de forma ágil. A contínua expansão e investimento direcionados ao progresso da CQ ressaltam uma área interessante para as tecnologias futuras, e novos estudos se mostram relevantes. Trabalhos futuros podem estender a interpretação dual de conectivos via CQ.

6. REFERÊNCIAS BIBLIOGRÁFICAS

- ABOUGHALIA,R.A.; ALKISHRIWO, O.A.S. Color Image Encryption Based on Chaotic Block Permutation and XOR Operation. **Libyan International Conference on Electrical Engineering and Technologies**, Trípoli, v. , n. p.492-497, 2018.
- BEDREGAL, B.R.C.; REISER, R.H.S.; DIMURO, G.P. Revisiting XOR-Implications: Classes of fuzzy (Co)Implications Based On f-Xor (f-XNor) Connectives. **International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems**, v.21, n.6, p.899-926, 2013.
- KLEMENT, E. P.; NAVARA, M. **Fuzzy Sets, Logics and Reasoning About Knowledge**. Dordrecht: Kluwer Academic Publishers, 1999.
- CRESSMAN, A. J.; WATTANAPANITCH, W.; CHUANG, I.; SARPESHKAR, R. Formulation and Emulation of Quantum-Inspired Dynamical Systems With Classical Analog Circuits. **Neural Computation**, v. 34, n. 4, p. 856-890, 2022.
- NIELSEN, M. A.; CHUANG, I. L. **Quantum Computation and Quantum Information**. In: NIELSEN, M. A.; CHUANG, I. L. (Ed.) **Quantum Computation and Quantum Information: 10th Anniversary Edition**. New York, NY, USA: Cambridge University Press, 2011. 10th ed.
- MANNUCCI, M. A. Quantum Fuzzy Sets: Blending Fuzzy Set Theory and Quantum Computation. **CoRR**, v. abs/cs/0604064, 2006.