COMPUTADORES CLÁSSICOS E QUÂNTICOS:

ESTUDOS, IMPLEMENTAÇÕES E IMPACTOS SOCIAIS

Gabriel R. Zsigmond

INICIAÇÃO CIENTIFICA

ESCOLA SUPERIOR DE PROPAGANDA E MARKETING

Sistemas de informaçâo em comunicação e gestão

Brasil

05 de maio de 2020

Gabriel R. Zsigmond

COMPUTADORES CLÁSSICOS E QUÂNTICOS:

ESTUDOS, IMPLEMENTAÇÕES E IMPACTOS SOCIAIS

Projeto de Iniciação Científica para a Escola Superior de Propaganda e Marketing, sob a orientação do Professor Doutor Humberto Sandmann.

Orientador: Prof. Dr. Humberto Sandmann

Brasil

05 de maio de 2020

ESTUDOS, IMPLEMENTAÇÕES E IMPACTOS SOCIAIS:

ESTUDOS, IMPLEMENTAÇÕES E IMPACTOS SOCIAIS

Gabriel R. Zsigmond

Resumo

O presente projeto, ”Computadores Clássicos e Quânticos: Estudos, Implementação, Simuladores e Impactos Sociais”, se propõe a estudar a história do computador e sua evolução. A mais recente inovação na área é a computação quântica, que certamente, inaugura a próxima geração de computadores. A computação quântica muda toda uma arquitetura na forma de computação, permitindo que os novos computadores sejam exponencialmente mais eficientes quando comparados aos mais modernos da atualidade. O projeto se propõe a entender e prototipar um computador tradicional de 8 bits em hardware, usando apenas portas lógicas simples, a fim de ilustrar, de forma clara, o funcionamento de um computador tradicional. Também, esse projeto busca entender e estimar as consequências sociais que os avanços da tecnologia e o desenvolvimento da computação quântica pode gerar. Entende-se que para essa análise, se faz necessário, inicialmente, uma ampla revisão bibliográfica, a fim de comparar esses dois tipos de computadores. Para ilustrar esta, será desenvolvida uma aplicação web que simula um computador tradicional e um computador quântico executando o mesmo algoritmo. É esperado que ao final do projeto, esse estudo traga um amplo e aprofundado conhecimento da área, além de, uma contribuição em relação ao impacto social do uso computação da quântica.

Sumário

1 Introdução

1.1 Definição justificada dos objetivos e da sua relevância

A palavra computador é usada desde o século XVII, tendo a sua primeira referência escrita datada de 1613. No entanto, por muito tempo a palavra computador não tinha o mesmo significado que leva hoje. Até a década de 1940 a palavra "computador" era tida como uma profissão de alguém que calcula, segundo o dicionário Michaelis: "Aquele ou aquilo que calcula baseado em valores digitais; calculador, calculista". [4]

Então o que é um computador no significado atual da palavra? Pode parecer uma pergunta simplista que não precisa ser respondida, porém, é uma pergunta para a qual muitas pessoas não sabem a verdadeira resposta. Computadores existem há muito mais tempo que o transistor [1] na forma mecânica e teórica. A definição real de um computador foi elaborada por Alan Turing (Reino Unido, 1912-1954), um matemático, lógico, criptógrafo e herói de guerra que se procupava exatamente com a quetsão relacionada ao que era computável e o que não era. Ele descreveu uma máquina denominada Máquina de Turing. Seu trabalho foi submetido em 1936 e publicado no ano seguinte. Atualmente, desde o computador ou telefone celular em que você está lendo essa pesquisa até os supercomputadores, podem ser classificados como uma Máquina de Turing no nível mais simplista.

A Máquina de Turing é o modelo mais poderoso de um computador. Esta é similar a um autômato finito [2], porém com uma mémoria ilimitada e irrestrita, constituindo um modelo mais exato de um computador de forma geral. Esta é composta por três principais, fita semi-infinita; processador; máquina de estado finito.

A fita semi-infinita é dividida em células, cada uma contendo um simbolo de um alfabeto finito. O processador é responsavêl por se deslocar para a direita ou esquerda

[1] Um transistor é um dispositivo semicondutor usado para amplificar ou alternar sinais eletrônicos e eletricidade.

[2] Um sub-tópico da Ciência da computação teórica, também chamado máquina de estados finita determinística — é uma Máquina de estados finita que aceita ou rejeita cadeias de símbolos gerando um único ramo de computação para cada cadeia de entrada.

e efetuar leitura ou escrita em uma célula. Assim, Fabio Gagliardi Cozman [2], explica seu funciona da seguinte forma:

1. Inicialmente a fita contém somente a cadeia de entrada, disposta a partir da primeira célula da fita (fita semi-infinita), com o processador posicionado no início da cadeia (o resto está em branco);

2. Para armazenar algo, a máquina escreve na fita;

3. Se tentar mover o processador para a esquerda, estando na primeira célula da fita, o processador não sai do lugar (fita semi-infinita);

4. As saídas aceita e rejeita são obtidas ao entrar nos estados de aceitação e rejeição;

5. Se não entrar em um estado de aceitação ou rejeição, continuará sua computação para sempre (loop infinito).

O primeiro computador digital eletrônico de grande escala, foi criado em fevereiro de 1946 por cientistas norte-americanos, John Presper Eckert e John W. Mauchly, da Electronic Control Company . No final de sua operação em 1956, o ENIAC (Electrical Numerical Integrator and Calculator), continha 20.000 tubos de vácuo 7.200 diodos de cristal 1.500 relés 70.000 resistores 10.000 capacitores e aproximadamente 5.000.000 de juntas soldadas à mão. Ele pesava mais de 27 toneladas, tinha aproximadamente 2,4m * 0,9m * 30m de tamanho, ocupava 167 m2 e consumia 150 kW de eletricidade. [7]

Apartir do ENIAC, as possibiliades tecnologicas tomaram uma nova proporção. Em 1969, apenas 13 anos após o desligamento do primeiro computador digital eletronico, o computador de bordo da Apollo 11, missão que levou o homem a lua, tinha 32.768 bits [para uma explicação elaborada sobre bits refira-se ao cápitilo 2 pagina 7] de RAM, o suficiente para armazenar um texto não formatado com cerca de 2.000 palavras. Em 2018, o iPhone XS, com 4GB de RAM (ou 34.359.738.368 bits), tem cerca de 1 milhão de vezes mais memória que o Apollo Guinche Computer. [6]

Durante o século XX, além do aumento de poder computacional dos dispositivos, outro fator impactante foi a refatoração de seus tamanhos. Assim, com tecnologias wearables [3], os computadores se tornam ativamente presentes no cotidiano.

Levando em consideração o rápido avanço e desenvolvimento computacional, mencionados anteriormente, entende-se que os computadores agregam à sociedade, seja facilitando a comunicação e o compartilhamento de conhecimentos, como em outros aspectos. No entanto, a agilidade pela qual se deu tais transformações da tecnologia da computação, também gera grandes expectativas e incertezas sobre o que ainda está por vir, tanto nas questões de mudanças tecnológicas quanto nos impactos relevantes na sociedade.

Tendo em vista a incerteza sobre o futuro da computação em relação aos proximos grandes avanços, nessa pesquisa serão estudados os conceitos da física clássica e da física quântica aplicados à computação, além disso, será estudado os princípios de criptografia [4]. Assim, a presente pesquisa irá prototipar um computador clássico de 8 bits em hardware usando apenas portas lógicas simples, dessa forma, ilustrando claramente o seu funcionamento. Junto a isso também será desenvolvida uma aplicação web que ilustre o funcionamento de um processador quântico. Ao final, conceitos de criptografia serão ultilizados para exemplificar possíveis mudanças sociais que os próximos avanços tecnologicos podem gerar.

1.2 Metodologia a ser empregada

Para a realização da pesquisa de iniciação cientifica, é indispensavel o uso de pesquisa bibliográfica, assim recuperando conhecimento científico acumulado sobre o assunto. Segundo Telma Cristiane Sasso de Lima, o conhecimento da realidade não é apenas a simples transposição dessa realidade para o pensamento, pelo contrário,

[3] A tecnologia em questão não somente pode ser usada como uma peça de roupa ou um acessório, como também tem que possuir características que a conectem a outros aparelhos ou à internet.

[4] Criptografia é um sistema de algoritmos matemáticos que codificam dados para que só o destinatário possa ler.

consiste na reflexão crítica que se dá a partir de um conhecimento acumulado e que irá gerar uma síntese, o concreto pensado [3]. E também a utilização do processo cientifico para a elaboração e efetivação do projeto em si. Ambas metodologias citadas acima, são cruciais para o desenvolvimento do relatório final na área de pesquisa em computação, já que na grande parte dos estudos científicos, a utilização do processo cientifico é frequentemente utilizada para um maior entendimento da obra e a construção do projeto se tornar mais facilmente executável.

Para o desenvolvimento da entrega do protótipo, computador de 8-bits, e para o simulador do computador quântico web, a principal metodologia utilizada será Project Based Learnig (PBL). De acordo com David Van Andel, o PBL envolve os alunos em um processo rigoroso de investigação, onde eles fazem perguntas, encontram recursos e aplicam informações para resolver problemas do mundo real [1]. Assim, assumisse que esta é a melhor metodologia para desenvolver um protótipo físico de um computador e programar um site.

2 Computação Clássica

Computadores clássicos são todos aqueles que a maior parte da população mundial conhece, por exemplo computadores da Apple, Samsung, Dell dentre outros. É possível questionar o que todos esse tem em comum, a final todos possuem características bastante distintas. A resposta é bem simples, esses usam fenômenos da física clássica para operar. Assim, são classificados como computadores clássicos (ou binários), esses processam dois tipos de sinais, 1 e 0, ligado e desligado respectivamente. É com base nos bits [5] ligados e desligados que o computador baseia sua linguagem.

Esses computadores podem ser referidos como computadores binários, assim, julga-se importante e de larga relevância ao tema compreender o que é um número binário.

Números binários usam base 2, por tanto, qualquer valor é composto por apenas dois digitos, 0 e 1. Em computação, esses digitos são chamados de bits. [5]

2.1 A computação clássica e sua evolução

[5] A menor unidade de informação que pode ser armazenada ou transmitida na comunicação de dados.

3 Computação Quântica

3.1 A computação quântica e sua evolução

4 Computador

Construir um computador parece uma tarefa complicada e assustadora. Porem, uma CPU [6] é bastante simples em operação depois que os fundamentos por trás de todos os seus processos são compreendidos. Este cápitulo destina-se a executar o passo a passo para que qualquer pessoa interessada seja capaz em construir seu próprio computador e obter o conhecimento que acompanha o processo.

4.1 Modulos

Para facilitar o compreendimento, e também o desenvolvimento do computador, este capitulo será dividido em alguns subcapitulos, assim cada um abordará uma parte do computador.

4.1.1 Clock

O clock do computador é uma parte essencial para o seu funcionamento. Este tem a função de sincronizar todas as operações. A ação mais rápida que o computador consegue executar é equivalente a uma vibração do seu clock.

4.1.2 Materiais Necessários

[6] CPU é a sigla para Central Process Unit, ou Unidade Central de Processamento. É o principal item de hardware do computador, que também é conhecido como processador, essa é a parte responsável por calcular e realizar tarefas determinadas pelo usuário.

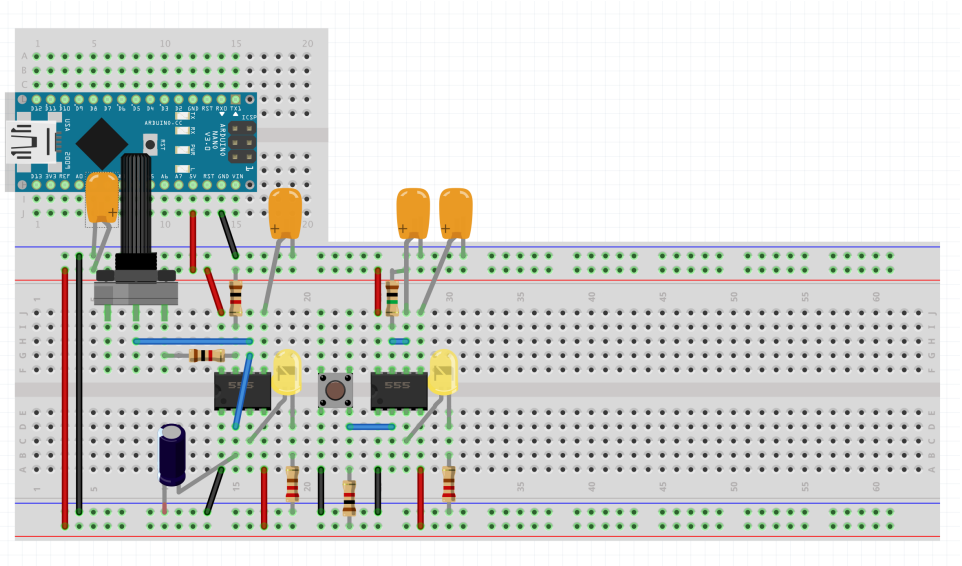

Figura 1: Esquema do Clock

5 Simulador

6 Criptografia

6.1 Conceitos básicos de criptografia

6.2 Criptografia aplicada computação clássica

6.3 Criptografia aplicada computação quântica

7 Próximos passos

7.1 Plano de Redação

7.2 Cronograma

7.3 Problemas

8 Reflexos sociais

9 Conclusões

9.1 Perspectivas

Referências

[1] Grand Rapids Business Journal – David Van Andel. Project-based learning is the future of education, out. 2019.

[2] Fabio Gagliardi Cozman. Turing e complexidade. University Lecture, 2000.

[3] Telma Cristiane Sasso de Lima e Regina Célia Tamaso Mioto. Procedimentos metodológicos na construção do conhecimento científico: a pesquisa bibliográfica. *Revista Katálysis*, 10(SPE):37–45, 2007.

[4] Melhoramentos ltda. – Michaels. Computador, out. 2019.

[5] B. Ram. *Computer Fundamentals: Architecture and Organization*. New Age International, 2000.

[6] UOL – Bruno Santana. Iphone 6 é 120 milhões de vezes mais poderoso que o computador de bordo da apollo 11, jul. 2019.

[7] Paul Wazlawick. *História da computação*. Elsevier, Rio de Janeiro, RJ, 2016.