TCC - Parte Subjetiva

Gervásio Protásio dos Santos Neto

November 2016

1 Desafios e Frustrações

O principal desafio para este TCC foi a familiarização com a área de Teoria dos Códigos, algo que não vemos normalmente na graduação. Além de dependerem fortemente de Álgebra (que eu eu não estudava há algum tempo), os textos introdutórios podem ser difíceis de acompanhar.

Outro grande desafio foi me adaptar a forma de escrever e pensar dos pesquisadores de Criptografia. Artigos da área, com óbvia exceções, não costumam ser muito claros e são difíceis de entender sem bastante estudo prévio.

Escrever a monografia se provou um desafio maior do que esperado. Muitas vezes conceitos eram claros para mim, mas a melhor forma de explicá-los no texto de forma didática não era óbvia.

2 Disciplinas relevantes para o TCC

Com a exceção de Engenharia de Software, todas as disciplinas que eu cursei no IME acabaram sendo úteis em algum momento ou outro da vida acadêmica e profissional. Contudo, as que tiveram mais relevância para meu TCC foram:

- **Introdução à Computação** e **Princípios de Desenvolvimento de Algoritmos**

  que foram indispensáveis para que eu aprendesse a pensar de forma algorítmica.

- **Criptografia e Segurança de Dados**

  que foi essencial para absorver os conceitos relacionados com criptografia e segurança que aparecem ao longo do trabalho.

- **Análise de Algoritmos**

  onde foram estudados conceitos de classes de complexidade computacional, análise de tempo de algoritmos e que me ensinou a sempre ter a eficiência computacional (seja ela de tempo ou espaço) em mente.

- **Álgebra II**

  onde aprendi sobre anéis, polinômios, corpos finitos e extensões, conceitos sem os quais não teria conseguido abordar a teoria de códigos algébricos de forma profunda.

- **Álgebra Linear**

  onde os conceitos de espaço vetorial, dependência linear me foram introduzidos e onde minha capacidade de entender e manipular matrizes se expandiu.

- **Introdução a Teoria dos Grafos**

  que me introduziu conceitos sobre grafos que foram úteis enquanto estudava códigos LDPC e MDPC.

3 Agradecimentos

Agradeço, em primeiro lugar, todos os amigos que conheci no IME. Eles passaram comigo madrugadas programando assembly, domingos estudando séries de Fourier, tardes fazendo listas de exercícios e cinco anos me ajudando a crescer como pessoa. Se cheguei aqui, foi por tê-los ao meu lado. Em especial, agradeço à Luciana de Melo, sem quem eu provavelmente teria reprovado inúmeras matérias.

Agradeço a Thales Paiva e Glaúcio Oliveira, que juntamente com o professor Routo compunham nosso pequeno grupo de estudos em criptografia baseada em códigos corretores de erros e que me ajudaram com feedbacks e referências bibliográficas.

Gostaria também de agradecer muito a todos os bons professores que tive no IME por terem compartilhado comigo um pouco do seu conhecimento. Em especial, sou muitíssimo grato ao professor Routo Terada, que vem me orientando desde meu primeiro ano no IME e que dividiu comigo muito do seu conhecimento e me auxiliou bastante em todo o desenvolvimento deste trabalho.

Por fim, preciso agradecer minha avó Sara, que foi minha primeira professora e que me ensinou o que tenho de mais valioso: o gosto por aprender.