

## 1. Introdução

Bem-vindo à esta jornada de programação em computadores quânticos! Baseado nos dias atuais, achei que a primeira frase deste livro deveria ser, e que é muito pertinente, **é que este livro não foi escrito por uma IA**. Triste que tenhamos chegado ao ponto de ter que tornar esta afirmação clara. **Nenhuma linha, nenhum parágrafo sequer foi escrito por IA**. Qualquer erro ou discordância verbal pode ser creditada ao autor, não foi uma alucinação de alguma IA. Adoro IAs, como complemento ao cérebro humano, mas não como substituição a ele, mas este poderia ser o tema de outro livro. A escrita deveria ser um prazer e não uma obrigação. Ela estabelece conexões cerebrais que de outras formas não seriam criadas. E como consequência disto, possivelmente um dia qualquer no futuro este livro poderá ser parte do treinamento de novas IAs, assim como novas obras sobre computação quântica, que deverão surgir em breve. Quem sabe um dia contribuirei para que IAs falem sobre quantum de forma didática também? Também vale salientar que a escrita deste livro foi um incrível esforço de criatividade, pois muitos dos conceitos de mecânica quântica podem ser provados pela matemática, mas não existem muitos comparativos simples com o mundo real. Por esta razão frequentemente se encontram livros que são oceanos de matemática muitas vezes complexos de se entender.

E como esta provavelmente será uma das primeiras páginas do livro que você lerá antes de adquiri-lo, acho que vale a pena dizer do que ele trata e outras frentes que não são o foco dele. **Em primeiro lugar, este NÃO é um compêndio de matemática**. Sou formado em matemática, e adoro esta ciência, mas uma fórmula matemática não parece explicar conceitos difíceis. A matemática prova veracidade dos conceitos, mas não me parece explicá-los. Algum grande matemático já disse que matemática não tem a ver com operações aritméticas, mas enfim é algo polêmico...

Quando comecei a estudar quantum, comprei diversos livros sobre o tema, e depois de páginas e mais páginas recheadas de equações que misturam coisas “mais recentes” como “bra”, “ket” e “braket” inseridos no contexto de senos, cossenos e multiplicações matriciais, se chega ao final da explanação com a retumbante frase vitoriosa “*como queríamos demonstrar – CQD*”. Mas eu tinha a percepção de que, embora estivesse convencido de que seria verdade mesmo (eu já havia acreditado antes mesmo da prova matemática se iniciar), ao final eu não havia entendido o fundamental, o conceito por trás da implementação.

Isto me lembra bastante quando tive aulas de Fourier e processamento de sinais no mestrado, e logo na primeira aula o professor preencheu toda a lousa com fórmulas matemáticas, e me lembro que ao final levantei a mão, e vale salientar que vários

alunos queriam fazer o mesmo mas se intimidaram, e perguntei: “*professor não entendi*”, ao que o professor respondeu prontamente: “*o que você não entendeu, caro aluno?*”. Eu também prontamente respondi “*não entendi nada depois daquela primeira integral logo no canto superior esquerdo...*”. De fato, não havia entendido o que significava Fourier. E mesmo depois de compreender que Fourier decompunha formas de onda em termos das frequências fundamentais componentes, ainda não entendia como este processo acontecia. Como seria possível somar um monte de números, e eles somarem zero ou apresentar algo escondido dentro de uma forma de onda? Só fui entender, muito tempo depois, lendo o livro de Anders Zonst chamado “*Understand the FFT*”, uma das recomendações que farei ao final deste livro. Após ler o livro de Zonst, algo desbloqueou em meu cérebro e passei a entender partes daquelas fórmulas que o professor de análise de sinais insistentemente nos “mandava sinais”. O livro do Zonst também não é um compêndio de matemática, e de fato a forma como explico FFT e QFT neste livro tenta se aproximar da forma maravilhosa como Zonst explorou em seu livro.

Provavelmente, se você pensar como eu, este livro será o ponto de partida para estudar mais profundamente a matemática, e aprofundar em provas e teoremas que aqui são explorados os conceitos fundamentais, e de forma muito visual e intuitiva. Como não é um compêndio de matemática, todos os assuntos que verá por aqui, desde a simples representação de um QUBIT até algoritmos completos como Shor, QFT, Grover e outros, serão explicados com termos simples, desenhos, infográficos e pequenos trechos de códigos, apresentando os conceitos fundamentais, e todas as vezes que for possível apresentando metáforas que tragam clareza ao que está sendo explorado. Por exemplo, ao invés de simplesmente colocarmos a explicação que, colocamos um QUBIT em superposição, para que exploremos rotações em fase como “claramente” está definido por:

$$|\psi\rangle = \cos(\theta/2) |0\rangle + e^{i\varphi} \sin(\theta/2) |1\rangle$$

Ou mesmo outras explicações como: “*colocamos o QUBIT em superposição porque a maioria das instruções de um computador quântico trabalham com rotações de fase, que é aquela parcela da equação em cor destacada*”. A explicação que pretendo passar aqui é mais ou menos assim: De fato quando programamos em um computador quântico, em quase todas as vezes atuamos como velejadores. Quando as velas de nosso veleiro estão enroladas em volta do mastro, mesmo os ventos que vêm de várias direções horizontalmente não fazem com que o veleiro se mova. Não existe a área da vela que ofereça resistência necessária ao vento, para que qualquer força atue sobre o veleiro. Se você observar o mastro enquanto o vento exerce sua força, verá que ele gira em falso ao redor do próprio eixo Z, sob a força do vento. NÃO estamos em superposição neste

momento. Por outro lado, quando o velejador baixa as velas, está posicionando boa parte da vela em torno dos eixos X e Y, deixando a vela ocupando espaço em um plano que permeia desde a ponta superior do mastro até um plano paralelo à superfície da água. Com isto aumentamos a área da vela susceptível à ação do vento, e dependendo do ângulo ou o giro que se faz na vela nos eixos X e Y, podemos aproveitar os ventos para acelerar, frear ou mesmo mudar a direção do veleiro, e é exatamente o que fazemos com as instruções de um computador quântico, quando o QUBIT está em superposição. Colocar um QUBIT em superposição é portanto colocá-lo em um estado em que ele estará mais receptivo a aceitar instruções que mudem sua fase, como a vela está mais susceptível à atuação do vento. Este será o tipo de explanação que você terá para muitos itens deste livro. Se você acha que é uma explicação tola e prefere um monte de fórmulas matemáticas, talvez esse livro não seja o ideal para suas expectativas.



Figura 1 – A superposição comparada com uma vela de um veleiro.

Mas isto não quer dizer que não apresentaremos algoritmos e códigos completos, e sempre utilizando portas comuns e não bibliotecas prontas de algoritmos que encapsulem a funcionalidade em um framework. Na realidade, todos os Jupyter Notebooks com os códigos dos capítulos e os principais infográficos estão disponíveis no site abaixo. Se desejar o fonte de alguma imagem, que não esteja disponível no github, talvez para uso como material de apoio para alguma aula, contate por favor o autor. Para todos os outros recursos disponíveis, você pode usar livremente, basta manter a referência do autor.

[https://github.com/gsreis/gsreis\\_quantum\\_book](https://github.com/gsreis/gsreis_quantum_book)

De forma similar, se você se sente confortável com a explicação do teste de primalidade de Fermat, que nos diz que: “dados dois números primos entre si, se elevarmos um dos primos ao outro com potência subtraída de 1, e calcularmos o módulo, teremos este módulo igual a 1”.

$$a^{m-1} \equiv 1 \pmod{m}$$

Figura 2 – Fórmula primalidade de Fermat.

Se você fica feliz com a declaração e aceita como verdadeira, tudo bem. Agora, se você é como eu, que embora reverencie Fermat, ainda não entende como pode funcionar, verá neste livro explicações como esta aqui:

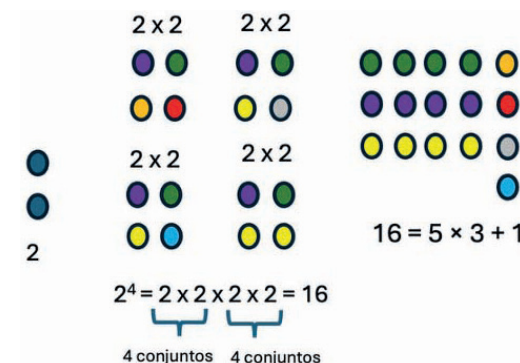


Figura 3 – Exemplo visual de teste de primalidade para  $2^{5-1} \equiv 1 \pmod{5}$ .

Vamos utilizar os números 2 e 5, que são primos entre si. Se dispormos  $2^{5-1}$  elementos em agrupamentos de 4 elementos, teremos  $2^4 = (2 \times 2) \times (2 \times 2)$  ou quatro agrupamentos de quatro elementos cada, como a imagem central nos mostra os 16 elementos. O que o teorema nos diz é que, se tentarmos criar um novo agrupamento de 5 elementos, como a imagem da direita, ou o número que desejamos calcular o módulo, podemos iniciar o processo removendo um círculo para cada um daqueles grupos menores de 4 elementos, mas não será possível completar os 5 elementos de uma linha no novo agrupamento. Teremos que “roubar” um elemento extra de uma das coleções menores de 4 elementos (que agora estão com 3 elementos cada uma), e uma delas ficará desfalcada de um elemento. Quando preencheremos a segunda linha, o mesmo acontece. Tomamos um elemento de cada coleção com 3 elementos (lembre-se de que um está desfalcado e tem dois elementos), mas ainda falta um elemento para completar os 5 de uma linha, e somos novamente obrigados a “roubar” um elemento extra. Este processo se segue, e ao final sempre teremos uma “sobra” que não permite completar uma linha de 5 elementos, ou resta 1 elemento de um dos conjuntos originais de 4 elementos, que fomos retirando elementos extras para completar a nova linha de 5 elementos. Isto não acontecerá se os dois valores que tomarmos forem divisíveis um pelo outro

Em resumo, utilizaremos aqui formas de explicar conceitos que sejam mais simples para uma pessoa não iniciada em física ou matemática. Afinal, se Eratóstenes utilizou um tipo de “cartela de bingo” para apresentar seu crivo, e se Schroedinger utilizou gatos e caixas hermeticamente fechadas com veneno para explicar a superposição, por que não utilizarmos metáforas que apresentem de forma mais simples estes conceitos? Entendemos que a computação quântica não deve ser algo complexo, cheio de fórmulas e explicações complicadas, mas algo que possa ser compreendido por segmentos além da matemática e da física, principalmente por programadores. Caso contrário corremos o risco de a computação quântica nunca escalar, ficando presa a nichos acadêmicos, o que não seria muito desejável.

The diagram illustrates the layers of abstraction in computer systems, showing a progression from Chemistry to Logic. A large blue arrow points from the Logic layer back to the Assembly layer.

**Química (Chemistry):** Shows the chemical structure of silicon,  $\text{H}_3\text{C}-\text{Si}-\text{CH}_3$ , with a central silicon atom bonded to four methyl groups.

**tecnologia (Technology):** Shows a 3D representation of a microchip or wafer with various components.

**Engenharia eletrônica (Electrical Engineering):** Shows a circuit board with components, including a logic gate (AND gate) with inputs A and B, and output C, labeled  $AB = C$ .

**lógica (Logic):** Shows a truth table for a 3-variable function, with columns for A, B, C, and the output. The table is divided into two sections: a top section with 8 rows (A, B, C combinations) and a bottom section with 4 rows (A, B, C combinations). The output is 1 for the first 8 rows and 0 for the last 4 rows.

**Assembly:** Shows assembly code for a 32-bit system, including instructions like `add %d1, -0x77(%ebp)`, `begin`, `push %ebp`, `mov %esp, %ebp`, `sub $0x8, %esp`, `mov %eax, -0x8(%ebp)`, and `mov %edx, -0x4(%ebp)`.

**Linguagem de mais alto nível (Higher-level Language):** Shows C code for a program that prints "Alo Mundo!". The code includes `#include <stdio.h>`, `#include <stdlib.h>`, `int main() { printf("Alo Mundo!"); return 0; }`, and `};`.

Eu já fui um razoável programador em linguagem C, no passado. Mas não me lembro de ter sido necessário conhecimentos de química, para entender a composição do

Iremos explorar uma parte importante da álgebra booleana, e entre outros tópicos iremos apresentar os segredos das portas lógicas, mapas de Veitch Karnaugh e como podem ser utilizados em certos tipos de algoritmos em computação quântica. As correlações entre a álgebra booleana e operações que podem ser feitas em computadores quânticos serão apresentadas. Os computadores quânticos recebem BITS como entrada, “transformam” em QUBITS fazendo operações e retornam BITS de volta aos computadores tradicionais. Sem conhecer como manipular os BITS, será impossível utilizar os QUBITS em sua plenitude. Mas também tentaremos trazer estes conceitos de forma leve. E veremos que não seria nem mesmo possível a criação de um operador fundamental em quantum, o Swap, sem conhecimentos de álgebra booleana. Em resumo, este livro explora aspectos da programação, mas não a criação de um hardware para computador quântico.

34

como este exemplo a seguir. Isto torna a leitura mais agradável, mesmo diante de conhecimentos mais difíceis de assimilar.



Figura 5 – Introduzindo leveza e diversão nas explicações.

Embora este não seja um compêndio de matemática, todos os conhecimentos necessários para o entendimento das principais portas quânticas estão presentes. Na minha jornada em entender estes conceitos, muitas vezes encontrei autores que exploravam até a exaustão coisas como o cálculo de determinantes e a resolução de sistemas de equações lineares utilizando matrizes. Não conseguia entender como estes conhecimentos seriam necessários para compreender quantum, mas entendia que o autor sentia prazer e necessidade em explorar todos os aspectos da matemática envolvida. Talvez para preservar uma referência futura. Totalmente louvável. De forma similar, somente os conceitos importantes e relevantes para o entendimento das instruções serão apresentados aqui. Iremos explorar álgebra linear, principalmente no tópico transformações lineares, trigonometria e números complexos, números primos e aritmética modular. Todos eles da forma mais lúdica possível. Sempre que necessário será feita a ligação e o conceito matemático relacionado à computação quântica, e em quase todas as explicações utilizando formas visuais de apresentação. Espero que este seja um livro agradável, e que ao final você entenda por que a computação quântica é tão importante.

Os principais algoritmos serão explorados, como Deutsch, Deutsch's Jozsa, Grover, QFT, QAOA. Em todos eles, SEM o romantismo de propor que a resolução de

um caso particular resolve todos os casos genéricos, e sem afirmar frases como “levam horas em um computador quântico mas que levariam centenas de bilhões de anos em computadores tradicionais”. De fato os computadores quânticos prometem fazer coisas que hoje não são possíveis para computadores tradicionais, mas serão apresentados neste livro de forma comedida, sem previsões apocalípticas que preveem o fim dos bancos e ruína de toda segurança estabelecida no mundo moderno, nem afirmando que poderão resolver todos os problemas do mundo em segundos. A apresentação destes algoritmos será feita de forma ponderada, com exemplos que fazem sentido além de uma equação matemática. Entretanto todos os segmentos preocupados com segurança corporativa deveriam ter a computação quântica como prioridade hoje, pois a curva de aprendizagem é longa, e saltos quânticos na evolução podem fazer com que alguns marcos cheguem mais rapidamente.

Em todo momento em que usei uma metáfora, busquei exemplos que tentam explorar o mais próximo da realidade. Por exemplo, aquele comparativo de que um computador quântico resolve problemas mais rapidamente do que um computador clássico porque “**uma partícula em superposição está em dois estados ao mesmo tempo**”. Certamente você já encontrou variantes deste problema aqui:

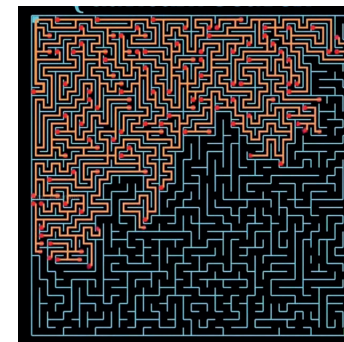


Figura 6 – De onde surge a velocidade dos computadores quânticos?

A explicação comum que se apresenta, para que a saída do labirinto seja mais rápida do que uma busca utilizando computação tradicional é a de que, o computador quântico consegue percorrer “**todos os caminhos ao mesmo tempo porque se utiliza da superposição da partícula, que coloca o QUBIT em dois estados ao mesmo tempo**”. Bem, se pudéssemos mesmo utilizar uma matemática que gerasse operações aritméticas para todo espaço de estados simultaneamente, poderíamos executar algoritmos que já existem hoje e foram consolidados ao longo dos anos, como propostos por Dijkstra e Knuth, em segundos ao invés de horas. A realidade



atual é que precisamos descobrir e apresentar novos algoritmos estatísticos que façam melhor uso das partículas em superposição, e talvez este seja o maior desafio da computação quântica.

O entendimento apresentado neste livro é o de que a partícula está em um estado onde têm iguais probabilidades de se tornar 0 ou 1 após lida, e tentamos efetuar operações com a partícula sem que um estado seja estabelecido pela sua leitura, ainda no espaço de Hilbert. Estaremos explorando este assunto mais adiante nas explicações, de forma a explorar como o computador quântico processa estes programas. Embora a natureza ondulatória das partículas permeiem o espaço ao redor dela, podendo até mesmo ter seus efeitos presentes em vários locais ao mesmo tempo, a utilização dentro de um computador quântico exige formas criativas para seu uso, e precisamos de novos algoritmos para que os QUBITS se alterem sem que sejam observados, aproximando cada vez mais de uma resposta adequada ao final do processamento. Tentaremos entender como isto pode ser possível nesse livro. No que acredito é que a partícula está em um estado onde existe igual probabilidade de ser lida em Zero ou Um. Portanto, embora a metáfora para explicação do labirinto seja lúdica e válida para o entendimento, não existem algoritmos em quantum hoje que encontrem uma saída de labirinto desta forma, buscando por todas saídas ao mesmo tempo. Ou melhor, não existem algoritmos genéricos que façam isto hoje. Existem casos particulares como Deutsch, Deutsch-Jozsa e Grover, que especializam para certos casos, mas ainda precisam se provar válidos para casos genéricos, e certamente não processando hoje tudo ao mesmo tempo. Mas, se formos conversar sobre casos genéricos e específicos, precisaremos tocar em um tema muito popular hoje em dia.

Existe um termo que se chama de “supremacia quântica”, uma busca similar àquela feita pelo Santo Graal ao longo da história.

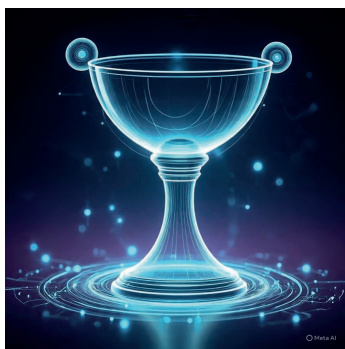


Figura 7 – Busca pelo Santo Graal quântico.

Aparecem com frequência relatos de cientistas que dizem ter atingido a supremacia quântica com seus times. Este termo, supremacia quântica, é um ponto de inflexão, quando um único computador quântico conseguiria resolver um problema que mesmo todos os computadores da terra ainda levariam um tempo existencial. Ou seja, quando ele puder fazer algo que não seja possível para a computação clássica, não importando a quantidade de recursos computacionais. O problema da supremacia quântica é que a frase é vaga. Ao contrário do teste de Turing, que estabelece ao menos certas regras claras, a supremacia quântica não estabelece critérios para este atingimento. Por exemplo, outro dia encontrei nas redes sociais a notícia de que um grupo de cientistas da China haviam atingido a supremacia quântica, e portanto reivindicavam o status de serem o segundo país do mundo ao atingir esta supremacia. Segundo eles, resolveram em segundos um problema que necessitaria de 2,5 bilhões de anos com supercomputadores tradicionais. Fiquei empolgadíssimo, e fui ler. Na verdade estou mentindo, se você entender como os QUBITS funcionam, e como se programa em um computador quântico de verdade, por exemplo lendo este livro, irá ficar mais cético quando se deparar com frases deste tipo na internet. Bem, estes cientistas Chineses criaram um computador baseado em fótons, e resolveram o problema:

*Para testar este computador, os pesquisadores realizaram uma tarefa chamada amostragem de bóson. Trata-se de um aparelho no qual pulsos laser são enviados a um labirinto de 300 divisores de feixes e 75 espelhos. A função do computador é calcular e simular o ponto de saída que os fótons (um dos componentes de qualquer luz, como os lasers do experimento) no labirinto, o que é algo bem difícil de prever até para os computadores mais poderosos não-quânticos....*

A frase é complexa, mas vejamos. Eles usaram um computador quântico baseado em fótons para resolver um experimento baseado em fótons. Este problema de fótons foi resolvido em 200 segundos, enquanto o mais rápido computador Chinês levaria 2,5 bilhões de anos para chegar ao mesmo resultado. Aqui vou utilizar uma comparação ao estilo Sabine Hossenfelder (uma física que vocês deveriam seguir nas redes sociais). Imagine uma colher de sopa que consegue armazenar exatamente 10 ml de sopa. Quando você coloca a colher e recolhe uma dose de sopa, existe uma quantidade aproximada de moléculas de sopa capturadas por ela (o valor pode variar em função da gravidade, inclinação da colher, densidade da sopa e muitas outras variáveis). Mas, vamos estimar levemente que em uma colher de sopa seja possível armazenar  $6,022 \times 10^{23}$  moléculas (a constante de Avogadro nos dá esta aproximação). Promoveremos momentaneamente a colher de sopa a um dispositivo computacional, como faremos mais adiante com ábacos, régua de cálculo, caixinhas de música e astrolábios

com mais propriedade. A colher de sopa tem a capacidade de nos fornecer a quantidade de moléculas de sopa contida em uma tigela. Basta que se remova repetidamente colheres de sopa, contando o número de vezes que a operação foi feita. Quando não for mais possível remover colheres de sopa da tigela, por um mecanismo complexo de extrapolação matemática também conhecido levemente como regra de três, chegaremos ao número aproximado de moléculas de sopa que estavam na tigela.

Agora, imagine que utilizemos o dispositivo tecnológico mais avançado que encontrarmos, talvez algum tipo de laser que vaporize e contabilize partícula a partícula da tigela. Com o mais avançado dispositivo tecnológico, é provável que demoremos algumas centenas de anos, contando molécula a molécula, o que com a colher de sopa fizemos em algumas horas, talvez minutos dependendo da fome. Portanto nossa conclusão “óbvia” é de que a colher de sopa atingiu a supremacia quântica. Você pode estar achando este exemplo “esdrúxulo”, mas veja, vamos a alguns pontos.

O primeiro ponto é que obviamente “*there is no spoon*”.



Figura 8 – “*There is no spoon*”.

Mas o ponto importante é que o experimento parte de um facilitador que é um dispositivo baseado em fótons para resolver um problema relacionado a fótons. Um computador clássico já se provou válido inclusive na resolução de problemas não relacionados à natureza de sua construção. Conceder esta honraria da supremacia quântica, a um experimento quântico da mesma natureza de sua construção, seria como conceder uma medalha de ouro na modalidade triatlão a Usain Bolt, somente porque ele é mais veloz no triatlão, naquela parte da corrida em terra. E a colher de sopa ainda estaria no páreo por outra modalidade!

O que deveria conceder o “selo imperial” de supremacia quântica a um computador quântico seria a capacidade de resolução de problemas genéricos, ou no mínimo **resolver um problema que não fosse da mesma natureza que a tecnologia utilizada**

**para construir o próprio computador quântico, e ainda executando centenas de milhares de vezes mais rapidamente do que um computador tradicional.** Utilizar um dispositivo ótico para resolver um problema ótico não prova que o dispositivo “poderia acelerar a resolução de outros problemas de caráter mais prático”, como por vezes acaba sendo sugerido.

Aprenderemos a usar portas lógicas, que são as unidades que um computador clássico reconhece, para efetuarmos operações aritméticas, inclusive em computadores quânticos. Isto já se provou verdadeiro e útil no mundo quântico.

O último ponto a se esclarecer é que neste livro não discutiremos assuntos místicos, como a existência de outros universos, nem mesmo a possível capacidade de um QUBIT entrelaçado se comunicar com outro além da velocidade da luz. Tudo que será explanado aqui é possível com a tecnologia atual, ainda que com erros. Muito ainda se faz necessário provar sobre as partículas e sua natureza, e deixaremos estes assuntos fascinantes para físicos de plantão!

Como um bônus, ao final do livro apresentaremos dicas para o exame de certificação do Qiskit 2.0, que é um divisor de águas para todos os que buscam respeito na programação em computação quântica. Além de ajudar para o exame, as dicas ajudam a compreender tópicos importantes sobre o tema.

Bem, se você chegou até este ponto, e gostou das premissas apresentadas, apreciou o linguajar não científico, chegou o momento de mergulhar neste fascinante mundo da computação quântica! Espero que esteja ainda mais empolgado que eu, e que tenha entendido a forma como iremos explorar estes assuntos aqui neste livro!