cadernos IHU idéias

Computação Quântica

Desafios para o Século XXI

Fernando Haas

ano 4 - nº 53 - 2006 - 1679-0316

UNISINOS

INSTITUTO HUMANITAS UNISINOS

UNIVERSIDADE DO VALE DO RIO DOS SINOS – UNISINOS

Reitor
Marcelo Fernandes de Aquino, SJ

Vice-reitor
Aloysio Bohnen, SJ

Instituto Humanitas Unisinos

Diretor
Inácio Neutzling, SJ

Diretora adjunta
Hiliana Reis

Gerente administrativo
Jacinto Aloisio Schneider

Cadernos IHU Idéias
Ano 4 – Nº 53 – 2006
ISSN: 1679-0316

Editor
Prof. Dr. Inácio Neutzling – Unisinos

Conselho editorial
Profa. Dra. Cleusa Maria Andreatta – Unisinos
Prof. MS Dárnis Corbellini – Unisinos
Prof. MS Gilberto Antônio Faggion – Unisinos
Prof. MS Laurício Neumann – Unisinos
MS Rosa Maria Serra Bavaresco – Unisinos
Esp. Susana Rocca – Unisinos
Profa. MS Vera Regina Schmitz – Unisinos

Conselho científico
Prof. Dr. Adriano Naves de Brito – Unisinos – Doutor em Filosofia
Profa. MS Angélica Massuquetti – Unisinos – Mestre em Economia Rural
Prof. Dr. Antônio Flávio Pierucci – USP – Livre-docente em Sociologia
Profa. Dra. Berenice Corsetti – Unisinos – Doutora em Educação
Prof. Dr. Fernando Jacques Althoff – Unisinos – Doutor em Física e Química da Terra
Prof. Dr. Gentil Corazza – UFRGS – Doutor em Economia
Profa. Dra. Hiliana Reis – Unisinos – Doutora em Comunicação
Profa. Dra. Stela Nazareth Meneghel – Unisinos – Doutora em Medicina
Profa. Dra. Suzana Kilpp – Unisinos – Doutora em Comunicação

Responsável técnico
Laurício Neumann

Revisão
Mardilê Friedrich Fabre

Secretaria
Caren Joana Sbabo

Editoração eletrônica
Rafael Tarcísio Forneck

Impressão
Impressos Portão

Universidade do Vale do Rio dos Sinos
Instituto Humanitas Unisinos
Av. Unisinos, 950, 93022-000 São Leopoldo RS Brasil
Tel.: 51.35908223 – Fax: 51.35908467
www.unisinos.br/ihu

COMPUTAÇÃO QUÂNTICA
DESAFIOS PARA O SÉCULO XXI

Fernando Haas

Introdução

Este trabalho dedica-se a uma introdução à computação quântica. Espera-se contemplar um público amplo e não apenas o grupo dos iniciados na ciência da computação e na física. Tendo em vista a natureza da empreitada, cabem algumas considerações iniciais sobre a arte de escrever artigos de divulgação científica.

Quando é iniciado algum texto sobre um tema da física, da matemática ou das tecnologias em geral, direcionado ao chamado público leigo, normalmente o autor começa por afirmar categoricamente que o assunto será desmistificado, que o tratamento será plenamente acessível a todos e assim por diante. Logo em seguida, o que costuma aparecer é uma seqüência de analogias um tanto quanto vagas, uma tentativa (desesperada?) do autor de conseguir se fazer entender sem utilizar o jargão próprio da sua especialidade. Em outras ocasiões, o autor simplesmente não consegue se libertar da linguagem técnica do seu dia-a-dia, tendo como resultado um texto suficientemente árido para confirmar, aos olhos daqueles que já têm preconceito, ou mesmo temor, a aridez das chamadas ciências "duras".

Tendo em vista estas observações, seria de bom agouro mencionar outras idéias que podem nos ser úteis.

Em primeiro lugar, tomando a liberdade de citar uma opinião de um amigo, não dominamos plenamente um assunto caso não nos sintamos capazes de explicá-lo a qualquer pessoa, não interessando o preparo técnico do ouvinte. Desta verdade incontestável, conclui-se que, de algum modo, deve ser possível explicar temas avançados da física e da matemática a todos. Poucos manifestam perplexidade diante da exposição dos últimos avanços da medicina. Por que a física e a matemática costumeiramente suscitam tamanho espanto? Possivelmente porque as questões da física e da matemática, às vezes, pareçam ser um tanto quanto afastadas do dia-a-dia de todos. Entretanto, um olhar um pouco mais atento é suficiente para conven-

cer-nos de que estamos cercados de física e de matemática. Para isso, nem é necessário apelarmos aos inúmeros artefatos tecnológicos que nos rodeiam. Basta olharmos a natureza, a luz, os movimentos em geral, as regularidades que percebemos no transcorrer de dias e noites.

Em segundo lugar, é incontestável que o correto entendimento de uma área de ponta em ciência e tecnologia exige, sim, anos de dedicação, de uma adequada preparação. Tal não se consegue sem um árduo esforço, a despeito de algumas afirmativas em contrário que nos são ofertadas de vez em quando. Veja-se, por exemplo, a famosa expressão "matemática sem dor", repetidas vezes utilizada na mídia. Como se a matemática de bom nível pudesse prescindir de abstração, de um esforço especial de quem a pratica. Acontece que as ciências "duras" são dureza! Não queremos aqui chegar a ponto de dizer que a matemática dói... Bem, só um pouquinho, mas é daquelas dores que agregam mais prazer do que propriamente dor, sabe como é? Além disso, quando nos referimos a "árduo esforço", não queremos dizer que seguir uma carreira numa área tecnológica chegue a arder, com o perdão do trocadilho. Seguramente, existem coisas na vida que ardem muito mais do que o esforço para compreender matemática. Na mesma linha de raciocínio, não é privilégio das ditas ciências exatas possuir um linguajar específico e inacessível sem um preparo prévio. Tente ler fluentemente uma partitura sem haver estudado teoria musical a fundo. Tente ler um livro de filosofia analítica sem se preparar adequadamente com estudos anteriores ou mesmo algumas cadeiras de um curso de filosofia. Tente atingir o estado místico de iluminação sem ser guiado por um monge. Dar palpites sobre algum assunto costuma ser fácil, difícil é ir além da conjectura.

O que podemos concluir, a partir do comentado nos dois últimos parágrafos? Que escrever textos de divulgação científica é um exercício salutar de comunicação ou, pelo contrário, é uma tarefa vã? Na nossa opinião, acreditamos sim que é possível comunicar, numa certa medida, algo sobre tópicos avançados de ciência e tecnologia a um público não-iniciado. Não chegamos, entretanto, de modo algum, a ter a pretensão de estarmos transmitindo um conhecimento preciso. Vez por outra, talvez nos vejamos até mesmo obrigados a lançar mão das famigeradas analogias usadas neste tipo de exposição. Estas considerações, o leitor verá, não serão nada rigorosas. Este é um texto informal que pretende, sobretudo, divertir o leitor. Talvez, justamente pelo tom despretensioso que assumiremos, nos seja possível avançar de modo mais eficiente no campo minado que é a explicação de um tema como o da computação quântica a um público não-iniciado em física e computação.

Enfim, tomemos coragem, iniciemos de uma vez por todas com o assunto da computação quântica! Como o próprio nome

diz, temos aí um tema que está na fronteira entre ciência da computação e física quântica. Para a maioria de nós, a computação é vista apenas como uma ferramenta. Neste exato momento, por exemplo, cá estou eu a batucar algumas teclas, usando um editor de texto, sem fazer a mínima idéia de como foi arquitetado o programa do tal editor de texto. Não faço idéia, igualmente, de uma série de detalhes do *hardware* envolvidos no funcionamento de meu computador. Não obstante, apesar de não ter uma formação centrada na ciência da computação, sou capaz de explicar alguns princípios básicos da ciência da computação. Estes princípios básicos são essenciais para um entendimento do que se trata, afinal de contas, a tal da computação quântica. Evidentemente, antes de passarmos à computação quântica, temos de nos dedicar a alguns rudimentos sobre a física quântica, tema da próxima seção. Uma vez atravessada esta etapa inicial, poderemos nos aventurar a tentar compreender o que significa este novo paradigma, o da computação *quântica.* Assim, na seção seguinte consideraremos simultaneamente algumas idéias sobre o que são as computações clássica e quântica. Esperamos comunicar algo sobre o significado da computação quântica, as suas promessas e as suas dificuldades. Finalmente, a quarta seção será dedicada a algumas conclusões que podemos tirar e algumas considerações adicionais, à guisa de uma reflexão crítica sobre o assunto.

Na medida do possível, e até mesmo do impossível, tentaremos reduzir ao máximo o uso de formulações matemáticas. Para o leitor interessado em um aprofundamento, mencionaremos agora algumas referências. Para uma introdução à física quântica, considere-se a referência [Dionísio, 2004], publicada nestes mesmos *Cadernos IHU Idéias*. Para textos introdutórios à computação quântica, considerem-se os trabalhos (Davidovich, 2004), (Oliveira, 2002) e (Oliveira, 2003). Finalmente, para uma discussão mais detalhada do ponto de vista técnico, existem alguns livros-textos sobre a computação quântica, entre os quais se destacam as referências (Nielsen, 2004), (Portugal, 2004) e (Preskill, 2005).

O autor desde já manifesta gratidão a qualquer um que queira enviar sugestões que possam tornar o trabalho mais palatável ou que deseje apontar eventuais imprecisões.

Bom proveito!

1 Física Quântica

É possível que alguns de nós tenhamos reagido com estupefação ao depararmo-nos, talvez em um jornal, numa revista ou em outro meio de comunicação, com a notícia da existência de projetos para uma tal de computação quântica. Se não me falha a memória, até mesmo o popular personagem de quadrinhos, o

Dilbert, já tocou no assunto, tratando a computação quântica como se fosse das idéias mais mirabolantes. Mirabolante, por um lado, por utilizar um paradigma nada popular, o da física quântica. De fato, embora a física quântica já seja centenária, o seu conteúdo está longe de fazer parte do nosso inconsciente. Boa parte das pessoas carrega consigo ainda o paradigma milenar da física aristotélica, ou seja, aquela física que dizia, entre outras coisas, que, para manter um corpo em movimento, necessariamente seria preciso aplicar uma força. A física aristotélica, de certa forma, é a física do senso comum, o que naturalmente acarreta imprecisões e preconceitos, a despeito do brilhantismo de Aristóteles. Outros, mais ilustrados, já incorporaram a mensagem da física newtoniana, também chamada de física clássica. A física clássica é notavelmente bem sucedida na explicação de uma grande variedade de processos, como o das órbitas planetárias ou o da propagação de ondas de rádio, conforme a teoria eletromagnética de Maxwell. Apesar disso, existem inúmeras facetas da natureza que necessitam da física quântica para seu entendimento. Por exemplo, podemos citar o comportamento da luz, a estabilidade dos átomos, a superfluidez, a existência de condensados de Bose-Einstein e o laser como alguns fenômenos que não são adequadamente explicados pela física clássica. Entretanto, mesmo físicos experimentados seguidamente encontram dificuldades para engolir certas peculiaridades da física quântica, conforme daremos uma noção mais adiante. Então, fica a nítida sensação de que a física quântica é efetivamente um ramo um tanto esotérico do conhecimento, apesar de seus múltiplos sucessos.

Por sua vez, são tão óbvios os inúmeros sucessos da computação clássica que se torna ainda mais difícil compreender, à primeira vista, o recente investimento acadêmico e financeiro na computação quântica. A computação clássica, isto é, a computação tal como a conhecemos no nosso dia-a-dia, está no centro das atenções da nossa sociedade. Internet, computação móvel, robótica, automação... Enfim, seria ingênuo tentar enumerar todas as facetas de nossa sociedade tecnológica que são influenciadas pela informática. Estamos mesmo longe de apreender todas as conseqüências deste rápido desenvolvimento técnico. Vez por outra, alguns inclusive manifestam descontentamento com um possível excesso de informática, tal como aqueles que organizavam campanhas contra as máquinas, no início da revolução industrial. Estaríamos nós sendo governados pelos computadores, sacrificando nosso tempo livre a eles em vez de usarmos a máquina para ampliar nossa liberdade? Esta é uma questão controversa. Todavia, sabemos que o mundo em que viveremos será decisivamente modificado pela informática, para o bem ou para o mal. Basta lembrar que até a década de 1970, antes do advento da calculadora de bolso, o grande artefato tecno-

lógico de que dispúnhamos era a régua de cálculo. Para explicar aos mais moços: a régua de cálculo era uma espécie de engenhoca mecânica de madeira (sim, de madeira...) que permitia fazer contas relativamente elaboradas, tais como tirar a raiz cúbica de uma expressão. Em minutos, o feliz proprietário chegava ao seu intento, se fosse um usuário experimentado no uso tanto da régua de cálculo quanto de tabelas de logaritmos. Hoje em dia, apenas trinta anos se passaram e qualquer calculadora de bolso efetua qualquer operação básica de cálculo numa fração de segundos.

A computação clássica já é suficientemente complexa para causar seguidos embaraços. Por que avançar ainda mais em complexidade, criando a computação quântica? Todos já se defrontaram com uma daquelas típicas mensagens desmoralizantes na tela do micro, do tipo "Erro fatal. Você perdeu todos os seus dados". É o popular "deu pau" que tantas vezes nos leva à loucura. Por que, então, complicar ainda mais? No futuro, todos terão que tomar cursos de física quântica para tirar o extrato do caixa eletrônico? No futuro, as crianças se entreterão com jogos quânticos? Seria curioso ver os jovens apostando para ver quem seria teletransportado a outra galáxia. Aí está um jogo que gostaríamos de jogar com nossos inimigos!

Bem, encontram-se algumas justificativas bastante concretas para a pesquisa sobre computação quântica, ou seja, existem alguns problemas relevantes que poderiam ser resolvidos por um computador quântico e que, ao que tudo indica, não poderiam ser solucionados eficientemente por nenhum computador clássico. A computação quântica poderá ser aplicada à criptografia (transmissão segura de dados), a buscas mais eficientes em bancos de dados (Internet), à aceleração do processamento dos computadores, à transmissão de informação a distância (teletransporte). Por essas razões, a um só tempo práticas e teóricas, a computação quântica e sua irmã, a teoria da informação quântica, têm atraído atenção e investimentos de grandes empresas como a IBM (*International Business Machines Corporation*) e das universidades. Sobre as promessas da computação quântica, falaremos mais na próxima seção. Por hora, limitar-nos-emos a enumerar alguns fatos sobre a física quântica, a qual é a base da computação quântica.

Atualmente, a teoria mais bem sucedida nas ciências naturais é a mecânica quântica. De fato, o comportamento das moléculas, dos átomos e das partículas elementares que compõem nosso universo, a ciência dos materiais, a supercondutividade, o funcionamento dos dispositivos eletrônicos, a predição do valor da carga do elétron com uma precisão extrema, são todos assuntos corretamente descritos pela mecânica quântica. Não se quer aqui dizer que a mecânica quântica seja a última palavra. Nas ciências naturais, não se pode demonstrar a veracidade de

alguma teoria. Temos acesso apenas a um número finito de experiências que podem desdizer as predições da teoria. Atualmente, o que se pode dizer é que, desde seu surgimento, há já várias décadas, a mecânica quântica tem sido testada diariamente em inúmeras situações, sempre obtendo sucesso, isto é, a mecânica quântica tem se saído extremamente bem diante do crivo da experimentação.

Ao longo do tempo, a mecânica quântica tem adquirido um grau de sofisticação cada vez maior, com seu domínio continuamente ampliado. Por exemplo, a aplicação da física (e, conseqüentemente, da mecânica quântica) a fenômenos biológicos tem sido uma das novas fronteiras que atrai mais e mais atenção. Para citar uma aplicação em biologia, considera-se a possibilidade de efeitos quânticos na emergência da consciência. Especificamente, um dos dilemas ao longo dos séculos é a explicação de como a matéria inanimada, uma coleção de átomos na linguagem moderna, pode eventualmente se organizar com tal grau de complexidade que possa se dar conta de sua existência como individuo singular. Conjectura-se sobre o papel da mecânica quântica em alguns processos cerebrais, envolvendo estruturas muito pequenas, os microtúbulos, que são estruturas protéicas cujo diâmetro é da ordem de 25 nanômetros. O prefixo grego “nano” se refere à pequenez de tais dispositivos, equivalendo um nanômetro a um bilionésimo de metro. Está em voga o uso desta terminologia, como na chamada nanotecnologia, com a qual se pretende construir máquinas de tamanho extremamente pequeno. Com estas máquinas, espera-se exercer um domínio maior sobre a natureza, manipulando átomos e moléculas quase que individualmente, a nosso bel-prazer.

Uma crítica endereçada às abordagens quânticas para a consciência está no fato de o cérebro operar a altas temperaturas em regimes em que eventualmente a física clássica deveria ser suficiente. De fato, uma das situações em que a mecânica quântica pode se revelar necessária é a baixíssimas temperaturas, como no caso dos supercondutores da antiga geração. Nesses materiais, a corrente elétrica, uma vez estabelecida, pode fluir sem nenhuma necessidade de fornecimento de energia. Esta ausência de resistência elétrica, ou supercondutividade, surge devido a efeitos quânticos que se manifestam a temperaturas próximas do zero absoluto, a menor temperatura admissível na natureza. Atualmente, muito dinheiro é investido na busca de materiais supercondutores a temperatura ambiente, e já se conseguiu supercondutividade a temperaturas apreciavelmente superiores ao zero absoluto, mas esta é outra história. Enfim, aparentemente, a aplicação da teoria quântica ao fenômeno da consciência poderia ser uma sofisticação desnecessária, já que o cérebro opera a altas temperaturas. Na nossa opinião, esta é uma crítica descabida. De fato, efeitos quânticos se

tornam necessários não apenas a baixas temperaturas, mas também em outras situações, como aquelas envolvendo dimensões diminutas ou altas densidades. Por exemplo, alguns dispositivos microeletrônicos da próxima geração deverão ter dimensões tão pequenas que a microeletrônica habitual, embasada na física clássica, já não será apropriada para a sua descrição. O investimento na miniaturização é justificado, tendo em vista o ganho em velocidade de processamento. Neste caminho de miniaturização cada vez maior, entretanto, não se pode prescindir da mecânica quântica. Pode-se demonstrar, por exemplo, que dispositivos microeletrônicos conhecidos por nanoMOSFETS têm sua performance degradada devido a efeitos quânticos, apresentando uma resposta que não está de acordo com a física clássica. Vale dizer que os nanoMOSFETS operam a temperaturas altas como a temperatura ambiente.

Outras situações em que a física quântica é necessária, mesmo a altas temperaturas, ocorrem, por exemplo, nos plasmas de fusão a laser, em que amostras de átomos leves como hidrogênio e trítio são bombardeadas por feixes de laser muito intensos. O objetivo deste gênero de experiência é promover a fusão dos núcleos destes átomos leves, com uma conseqüente liberação de energia. Este processo acontece de forma descontrolada nas terríveis bombas de hidrogênio. Supondo que se possa controlar a liberação de energia, daí surgiria uma fonte de energia de combustível barato e abundante, sem maiores danos ao meio ambiente. Nestes tempos de extinção dos combustíveis fósseis como o petróleo, justifica-se a pesquisa e o gasto de dinheiro na busca desta chamada técnica de fusão termonuclear controlada. Pois bem, no caso da fusão termonuclear controlada, produzida com feixes de laser, eventualmente são atingidas densidades de uma magnitude tal que não é mais possível prescindir da mecânica quântica. É desnecessário dizer que, nestes casos, as temperaturas atingidas não estão perto do zero absoluto. Muito pelo contrário, ao direcionarem-se feixes de laser extremamente intensos a um material é de imaginar que cheguemos a temperaturas de milhões e milhões de graus.

Para encerrar o argumento, na astrofísica também encontramos sistemas a altas temperaturas e que, mesmo assim, evidenciam claramente efeitos quânticos. Este é o caso, por exemplo, das estrelas anãs brancas, nas quais a matéria atinge uma densidade muitíssimo superior do que aquelas densidades às quais estamos acostumados no nosso dia-a-dia. De fato, se pudéssemos recolher uma porção de uma anã branca com uma colher de chá, teríamos conosco muitas e muitas toneladas de matéria. Isso imaginando que a colher de chá não se desintegre, porque as anãs brancas apresentam altíssimas temperaturas... Enfim, não é justo descartar a presença de fenômenos quânticos na emergência da consciência sob o argumento de que o

cérebro seria um sistema elétrico operando a altas temperaturas. A presença visível de efeitos quânticos não depende apenas da temperatura, mas de detalhes finos, tais como a densidade ou as dimensões envolvidas. Não seria de estranhar que detalhes sutis interviessem no processamento de informação pelo cérebro, de tal modo que fenômenos quânticos pudessem levar aquilo que chamamos de consciência. É, portanto, justo que prossiga a pesquisa visando a um entendimento detalhado da física nos microtúbulos. O leitor pode obter mais detalhes sobre a emergência da inteligência e da consciência com base em eventuais efeitos quânticos, por exemplo, em algumas obras de Penrose (PENROSE, 1989; PENROSE, 1996).

Repetidas vezes, temos nos referido aos tais efeitos quânticos. O que, afinal de contas, queremos sugerir com isso? O que distingue a realidade quântica? No nosso dia-a-dia, estamos acostumados a pensar o mundo mecanicamente, isto é, quando jogamos futebol, subimos uma escada ou observamos qualquer tipo de movimento, temos uma certa imagem causal da realidade. Mais exatamente, no caso do futebol, com base na posição e na velocidade da bola num certo instante de tempo, podemos predizer, com uma certa dose de certeza, qual será a posição e a velocidade da bola no tempo imediatamente posterior. Geometricamente, estamos associando ao movimento dos corpos uma certa trajetória, uma curva no espaço, a qual é percorrida com uma certa velocidade ao longo do tempo. Esta é a base conceitual da chamada física clássica, ou física newtoniana.

Podemos aplicar a física newtoniana, nos termos que explicamos, não apenas ao futebol, como também ao movimento dos astros e estrelas ou ao movimento das massas de ar produzindo um ou outro clima no nosso planeta. Se fôssemos capazes de determinar, com absoluta precisão, o estado de movimento de todos os corpos do universo e as forças agindo entre eles, num certo instante, então, segundo a física newtoniana, seríamos capazes de prever com absoluta precisão o estado de movimento de todas as partículas, num futuro arbitrário. Para isso, seria necessária a existência de uma inteligência suficientemente elevada para levar a cabo, com exatidão, todos os cálculos envolvidos no processo de obtenção do estado futuro do universo a partir do presente. Eventualmente, supondo que as leis da física sejam reversíveis no tempo, seria possível também descobrir qual o passado exato do universo, a partir do presente. Esta imagem foi sugerida por Laplace, notável físico-matemático do século XVIII, e resume de modo eficiente o esquema conceitual da física clássica.

Na verdade, pouco importa a existência concreta de uma inteligência (um supercomputador?) capaz de executar a tarefa operacional de resolver as equações de movimento para todos os corpos do universo. O que é relevante, aqui, é a visão com-

pletamente determinista da natureza que emerge do paradigma newtoniano. Os acontecimentos no mundo se desenrolariam como num filme, sem sobressaltos de espécie alguma. Num universo mecânico deste gênero, não parece haver lugar para o livre-arbítrio ou acaso. O fato de o futuro nos ser desconhecido seria reflexo apenas da limitação de nossos cérebros para processar a informação necessária para, a partir do presente, desvendar o futuro e, quem sabe, também o passado. O livre-arbítrio seria uma doce ilusão, fruto de nossa pequenez. Esta é a imagem do universo newtoniano, como se o universo fosse um supercomputador processando continuamente informação de modo totalmente determinista, levando-nos do passado para o futuro e vice-versa.

Cabe observar que a física clássica não se aplica apenas a fenômenos mecânicos, como nos casos do movimento de um pêndulo ou de um jogo de futebol. Os chamados fenômenos eletromagnéticos também recebem um tratamento bastante acurado por parte da física clássica. A teoria eletromagnética clássica é notavelmente bem sucedida numa série de problemas, como o da explicação da propagação das ondas de rádio, ou seja, é pouco provável que existissem rádio, televisão ou Internet sem a física clássica. Mesmo assim, certos fenômenos eletromagnéticos não são bem descritos pelo paradigma clássico, o que levou a concepção da teoria quântica de campos, descrevendo o comportamento quântico dos campos eletromagnéticos. Acredita-se hoje que a luz não seja simplesmente uma onda, de certa forma tal como as ondas no mar o são. Uma tal interpretação seria incapaz, por exemplo, de explicar o chamado efeito fotoelétrico, no qual se gera uma corrente elétrica da exposição de metais à luz. Na visão da teoria quântica de campos, a luz é uma coleção de partículas de energia, os fótons, que seriam mais eficientes para arrancar elétrons da eletrosfera dos átomos de um determinado metal do que uma onda eletromagnética clássica. Ao mesmo tempo, os fótons seriam capazes de desenvolver fenômenos típicos das ondas habituais, como difração e interferência. Esta dualidade onda-partícula é característica da física quântica. Não é mais considerado correto pensar as partículas simplesmente como concentrações pontuais de matéria, em tudo semelhantes a bolas de bilhar infinitamente pequenas, mas guardando ainda uma certa massa e, eventualmente, uma certa carga elétrica. No universo quântico, as partículas podem sofrer interferência tal como as ondas costumam interferir. Por exemplo, quando o sinal de uma onda de rádio ou televisão soma-se ao sinal de uma outra fonte, o resultado pode não ser dos melhores, o que se reflete no que qualquer técnico em eletrônica chama de “interferência”. Outra característica peculiar às ondas é o processo de difração, que se manifesta quando uma onda

contorna um objeto que está em seu caminho ou quando atravessa uma abertura estreita.

É estranho imaginar que elétrons ou quaisquer outros pontos materiais possam exibir comportamentos próprios das ondas, como no caso da interferência. Não costumamos ver bolas de bilhar se difratando ou interferindo, a menos que estejamos sob efeito de uma forte dose de cerveja. No entanto, a teoria quântica de campos se aplica a uma enorme variedade de fenômenos em que a teoria eletromagnética clássica falha, como no caso do efeito fotoelétrico. De resto, é consenso de que seja pouco provável que a física clássica possa ser adaptada de modo a dar conta da física das partículas elementares, as quais são o tijolo básico de que é composto o universo. Para observar com nitidez a estranha natureza do universo quântico, em geral é preciso ir ao mundo microscópico das moléculas, dos átomos e das partículas elementares. Entretanto, existem alguns modelos clássicos simulando alguns aspectos da realidade quântica (HAAS, 2005a; HAAS, 2005b).

Com o risco de sermos excessivamente sucintos, poderíamos enumerar as características básicas do universo quântico como sendo a superposição de estados, o indeterminismo fundamental e o entrelaçamento. Tentaremos explicar uma por uma destas características básicas da mecânica quântica, a começar pela superposição de estados. Na física clássica, o estado de movimento de uma partícula num certo instante é completamente especificado pela sua posição e pela sua velocidade. Na física quântica, existe uma limitação essencial a esta abordagem. De fato, na física quântica, não é possível medir a posição e a velocidade de uma partícula com absoluta precisão num certo instante. Não se trata aqui de uma incerteza operacional, como no caso da física clássica, na qual as incertezas vêm das limitações do processo experimental, ou seja, como não existe experiência perfeita, todas as medidas que vêm de um laboratório vêm acompanhadas de uma certa margem de erro. Esta é uma incerteza, ou ignorância, de origem clássica. Por exemplo, seria muito difícil conceber alguma experiência que nos permitisse descobrir a posição e a velocidade de todas as partículas compondo o ar de uma sala qualquer, com precisão absoluta. Entretanto, o que nos diz a mecânica quântica é que esta é uma ignorância essencial e não apenas operacional, isto é, não pode existir uma tal experiência. Dessa maneira, está posta em cheque a existência de trajetórias, uma vez que seria um conceito teórico não-passível de verificação. É bom lembrar que muitos dos próceres da mecânica quântica são herdeiros da tradição positivista, segundo a qual aquilo que não pode ser mensurado seria irrelevante para a ciência (BUNGE, 1973). Dessa forma, a interpretação tradicional da mecânica quântica abandona a própria idéia de trajetória, a qual está na essência da física newtoniana.

Se não é mais razoável descrever o movimento através de trajetórias, ou seja, de curvas percorridas pelos corpos ao longo do tempo, qual seria a sugestão proposta pela física quântica? A interpretação tradicional está longe de ser unanimidade, com inúmeras outras escolas propondo visões alternativas (AMMER, 1974). Entretanto, para simplificar vamos nos ater essencialmente à interpretação canônica, da escola de Copenhagen (BOHR, 1958; HEISENBERG, 1958). Segundo a interpretação de Copenhagen, o objetivo básico da mecânica quântica é a construção da chamada *função de onda.* Sem entrar em detalhes matemáticos, por meio do conhecimento da função de onda somos capazes de descobrir as *probabilidades* de um dado sistema estar numa certa posição, com uma certa velocidade, num certo instante de tempo. Apenas probabilidades, nada mais do que isso. E o pior de tudo é que não se pode chegar a predições com precisão absoluta simultaneamente para velocidade e posição, ou seja, na mecânica quântica é impossível afirmar que "num certo instante, a partícula estará na posição x com probabilidade de 100% e com a velocidade v com probabilidade de 100%". Se desejarmos fixar a posição, perderemos informação sobre a velocidade e vice-versa. É o famoso "princípio da incerteza de Heisenberg", evocado devida ou indevidamente nas mais variadas situações, inclusive em conversas de bar. O princípio da incerteza tem sido usado como uma panacéia para argumentação a respeito de inúmeros assuntos, aí se incluindo a questão do livre-arbítrio. Há que se ter cuidado para não extrapolar na aplicação do princípio da incerteza, o qual se manifesta em equações matemáticas bem precisas. Entretanto, não resta dúvida de que poucas relações resumem tão bem o conteúdo epistemológico da mecânica quântica como o princípio da incerteza de Heisenberg.

Eventualmente, a função de onda pode incorporar a descrição probabilística de outras variáveis sem contrapartida na física clássica. Entre estas variáveis, destaca-se o *spin*, uma espécie de quantidade de movimento "rotacional", semelhante à quantidade de movimento portada por um pião. Cabe observar que esta é apenas uma analogia pobre, porque o *spin* não é equivalente à quantidade de movimento rotacional eventualmente possuída por uma dada partícula, tendo propriedades matemáticas distintas. O *spin*, o *isospin*, a carga bariônica e outras tantas quantidades têm uma natureza quântica, sem contrapartida exata no mundo clássico.

A estrutura da mecânica quântica é tal que diferentes funções de onda podem ser somadas, daí resultando uma função de onda admissível. Isso quer dizer que os estados de um sistema mecânico, especificados pela função de onda, podem ser superpostos. De certo modo, isso é análogo à teoria eletromagnética clássica, em que várias ondas eletromagnéticas podem

ser superpostas, daí resultando uma onda eletromagnética igualmente aceitável. É o que acontece quando dois ou mais raios de luz ocupam a mesma região do espaço, ao mesmo tempo. É o fenômeno da *interferência.* Na mecânica quântica, este tipo de superposição acontece mesmo quando se trata de partículas. Nada disso seria imaginável na física newtoniana. Não parece fazer muito sentido combinar dois corpos sólidos, ou duas partículas elementares como elétrons, daí resultando uma superposição coerente. Entretanto, na mecânica quântica, as partículas não têm mais o caráter acadêmico das partículas do mundo clássico: elétrons interferem, funções de onda se superpõem. É possível ir mais longe, fazendo valer o argumento inverso, isto é, na mecânica quântica, as ondas possuem propriedades de partícula, como uma localização bem específica. É o que ocorre no caso da luz, que é vista como uma onda composta por partículas de energia concentrada, os fótons. Portanto, os conceitos de onda e partícula deixam de estar limitados por fronteiras rígidas. É a chamada dualidade onda-partícula, característica da mecânica quântica.

Para a computação, o princípio da superposição inerente à mecânica quântica abre portas de interesse prático. Na computação clássica, já temos o chamado processamento paralelo, que é a divisão de uma certa tarefa em várias tarefas menores, a serem executadas simultaneamente. Uma analogia para processamento paralelo ocorre na cozinha de um grande restaurante. Um cozinheiro descasca a batata, um outro tempera o peixe, um terceiro lê o jornal, palita os dentes e reclama da lentidão dos demais e assim por diante. Para terminar, o trabalho é integrado e o peixe vai para o forno. O mesmo acontece no computador, só que aí não se trata de palitar dentes ou assar um peixe, e sim de executar simultaneamente uma série de cálculos que são integrados no final. Este processamento paralelo permite reduzir o tempo de execução de um programa, ou melhor, permite aumentar a eficiência da computação. Se o objeto da computação é a função de onda, isto é, se o computador estiver manipulando a função de onda, teremos um esquema natural para processamento paralelo. De fato, a função de onda pode ser vista como uma superposição de um certo número de funções de onda, as quais podem ser simultaneamente transformadas pelo computador. Nesse caso, teria de ser necessariamente um computador quântico, isto é, um computador capacitado para executar transformações sobre a função de onda. Este é o princípio da computação quântica. Pode-se demonstrar que o processamento paralelo quântico assim pode ser muitíssimas vezes mais poderoso do que o processamento paralelo em computadores clássicos como aqueles de que dispomos atualmente. Por isso, há a promessa de que a computação quântica acelere grandemente a velocidade dos cálculos, ao menos em princípio.

É concebível um esquema mais complexo, com relação ao chamado *operador densidade*, o qual oferece a possibilidade de tratar sistemas quânticos numa classe mais ampla do que aqueles descritos pela função de onda. Entretanto, em linhas gerais, nossa argumentação não se modifica em sua essência caso utilizássemos o operador densidade e não a função de onda.

Anteriormente, nos referimos aos pilares da física quântica como sendo superposição de estados, o indeterminismo fundamental e o entrelaçamento. Já nos detemos um pouco sobre a superposição de estados, ou seja, aos efeitos ondulatórios no comportamento das partículas. Sobre o indeterminismo, já mencionamos algumas propostas da mecânica quântica, entre as quais a existência de um princípio da incerteza, impossibilitando a obtenção simultânea de posição e velocidade com precisão absoluta. Entretanto, o indeterminismo quântico consegue ser bem mais radical do que o indeterminismo expresso pelo princípio da incerteza de Heisenberg. De fato, na física quântica, ao ser realizada a medição de alguma variável, como, por exemplo, a energia de um sistema, normalmente é impossível prever, *a priori,* qual será o resultado. Mais uma vez, para um certo estado quântico, a teoria permite apenas obter as probabilidades de ocorrer uma medição x ou y. Uma analogia é fornecida pelo jogo de cara ou coroa. Na física quântica, é como se o estado da moeda fosse uma superposição de "cara" e "coroa". A mecânica quântica nos fornece regras para calcular as probabilidades de o sistema cair no estado "cara" ou no estado "coroa" após uma eventual medição, que pressupõe alguma interação entre a moeda e o resto do universo. Aqui, medição não supõe alguma consciência humana ou algum aparato de medida, tal como um voltímetro. Num sentido mais amplo, medição significa *interação* entre o sistema sob análise e o resto do universo. Medições, na mecânica quântica, geralmente implicam perturbações irremediáveis. No nosso exemplo da moeda, caso tenha sido medido o resultado "cara" não restaria mais vestígio algum da superposição dos estados cara e coroa.

Muito tem sido debatido a respeito do estranho papel das medições na física quântica ou, de modo mais geral, a respeito do indetermismo fundamental que somos obrigados a engolir. Alguns, como Einstein, afirmavam ser a mecânica quântica uma teoria incompleta que não estaria levando em conta certas variáveis relevantes. Estas tais *variáveis ocultas* seriam incorporadas por uma teoria mais geral. Seria como no caso da imagem defeituosa de uma televisão, que estaria sendo perturbada por um sinal aleatório não correspondente à emissora desejada. Esta aleatoriedade seria consertada caso o sinal adicional fosse descoberto e bloqueado. No dizer de Einstein, "Deus não joga dados". É possível, entretanto, imaginar critérios objetivos para a existência destas variáveis ocultas, conforme expresso pelas chama-

das desigualdades de Bell (BELL, 1964). As desigualdades de Bell têm sido confirmadas experimentalmente, até o momento. Portanto, aparentemente a descrição quântica seria completa, sem a possibilidade de existirem variáveis ocultas. A descrição clássica parece parte de um paraíso perdido. Nossa televisão está irremediavelmente estragada.

As desigualdades de Bell tratam também da terceira faceta fundamental da física quântica, a do *entrelaçamento,* também chamado de *emaranhamento*. O entrelaçamento inerente à mecânica quântica já havia sido percebido por Einstein, Podolsky e Rosen num artigo histórico (EINSTEIN, PODOLSKY e ROSEN, 1935). Não entraremos em maiores detalhes sobre os aspectos técnicos do entrelaçamento, limitando-nos a defini-lo como uma certa ligação entre dois sistemas quânticos após uma interação entre eles. Assim, o que ocorre com um dos sistemas afetaria o outro, não interessando a distância espacial separando-os. Por mais estranha que pareça, a propriedade do entrelaçamento já foi testada e comprovada em laboratório. Filosoficamente, o entrelaçamento vai contra a idéia cartesiana de dividir o mundo em subsistemas que poderiam ser estudados isoladamente. O universo e suas partes estariam intrinsecamente correlacionados. Isso corrobora a noção holística de que o todo é mais do que a soma das partes: a interação entre sistemas individuais leva à emergência de uma complexidade adicional. Na computação quântica, o entrelaçamento relaciona-se com transmissão de informação a distância e com compressão de dados. É o entrelaçamento que torna a computação quântica diferente da computação clássica com processamento paralelo massivo. Na computação quântica, os processadores paralelos eventualmente não atuam independentemente, mas sim de modo correlacionado. Voltaremos a estas questões relativas ao entrelaçamento e a computação quântica mais adiante.

Concluindo a seção, podemos afirmar que tudo se passa como se o universo fosse um computador processando informação quântica e levando-nos do presente para o futuro. Entretanto, este é um computador muito diferente daquele computador determinístico imaginado por Laplace. Vale também observar que, ao contrário do que se escuta de vez em quando, a teoria do caos não sabota o determinismo laplaciano. A teoria do caos lida com o comportamento da natureza diante da ignorância sobre sua configuração inicial exata. Ora, o supercomputador antevisto por Laplace pressupunha acesso ao estado físico exato de todos os sistemas do universo. A dificuldade para este conhecimento completo, na física clássica, é apenas operacional e não uma questão de princípio como na mecânica quântica.

2 Computação Quântica

Antes de tratarmos da computação quântica, havemos de definir o que é computação clássica. Muito se fala sobre informática, mas o que é fazer computação? Mais exatamente: o que é fazer computação clássica? Pois bem, as bases da computação clássica foram lançadas pelo matemático Alan Turing nos idos da década de 40 do século passado. Entretanto, a idéia de realizar tarefas de cálculo de forma automática remonta, quem sabe, ao ábaco ou até antes. O conceito formal de computação prescinde da realização física do computador, que pode ser um sistema de espelhos que manipula raios de luz ou uma engrenagem mecânica. A eficiência dos computadores modernos se apóia no uso de circuitos eletrônicos, cuja indústria é bem desenvolvida e que operam a uma alta velocidade. Sem fazer referência à realização concreta de um computador, Turing demonstrou que *computar* pode se resumir a manipular de modo automatizado zeros e uns, ou melhor, para uma dada seqüência de zeros e uns, tal como 0010011101, o programa retornaria uma outra seqüência de zeros e uns, como 0111001010. Quando digitamos uma palavra de busca na Internet, o computador, que não entende português, codifica cada letra numa certa seqüência de zeros e uns, que será utilizada para a busca.

Turing escolheu o zero e o um, como poderia ter escolhido "sim" e "não", ou "dois" e "três", ou "vermelho" e "azul", ou "cara" e "coroa". O importante aqui é que a computação (clássica) pode ser resumida a um conjunto de operações matemáticas sobre um conjunto composto por apenas dois elementos. Neste sistema binário, a unidade básica da informação é o *bit*, o qual, por definição, assume ou o estado zero, ou o estado um. Quando observamos que a taxa de transferência de um dado arquivo ao fazermos um *download* é de 450 bits/s, isto quer dizer que, a cada segundo, 450 zeros ou uns estão sendo assimilados pelo nosso microcomputador a partir da rede. Fisicamente, no interior do computador, um *bit* é simulado por um capacitor carregado ou não ou pela magnetização de um disco rígido. Cada um destes *bits* é devidamente processado, ou decodificado, até que, lá pelas tantas, o programa de busca nos retorna um certo número de endereços relacionados ao tema sobre o qual estamos pesquisando. Antes de passar-nos esta informação em português, o computador decodifica uma seqüência de zeros e uns em letras que podemos compreender com mais facilidade. Claramente este esquema, para funcionar, exige uma elevada velocidade de processamento. A Internet seria inimaginável apenas com o ábaco ou engenhocas do gênero. É preciso um sistema eficiente de codificação, decodificação, manipulação e armazenamento de *bits*. As portas para a tecnologia necessária à informática foram abertas com a invenção do transistor por volta dos

anos 50 do século passado. Curiosamente, o funcionamento do transistor só pode ser explicado pela mecânica quântica, sem a qual, portanto, não teríamos sequer a computação clássica no nível que temos hoje. Sem a mecânica quântica, a computação seria basicamente apenas um ramo da lógica.

Referimos-nos à manipulação de *bits*. Um exemplo disso estaria na operação que transforma zero em um e vice-versa. Assim, se a entrada fosse dada pela seqüência 001, a saída seria 110. Uma operação desse tipo é chamada de *porta lógica*. Pode-se demonstrar que qualquer operação sobre *bits* pode ser resumida a um conjunto reduzido de portas lógicas elementares. Quando se escreve um programa de computador, utilizando uma linguagem de programação, no fundo se está mascarando o fato de que estamos ordenando ao micro que uma certa seqüência de portas lógicas seja executada. As linguagens de programação com seus famigerados comandos são apenas uma forma mais amigável de interagirmos com o computador. É mais fácil aprender uma linguagem de programação do que se tornar um especialista em lógica, de modo a manipular diretamente qualquer seqüência de *bits*.

Muito bem, já que a computação clássica se resume à manipulação de zeros e uns, o que seria a computação quântica? Historicamente, a computação quântica surgiu de especulações de Feynman (Feynman, 1982) e Benioff (Benioff, 1980) acerca das potencialidades de uma máquina baseada nos mesmos princípios que regem a natureza, isto é, princípios quânticos. Matematicamente, a computação quântica nada mais é do que a manipulação de *superposições* de zeros e uns. Se, na computação clássica, a unidade de informação é o *bit*, na computação quântica a unidade de informação é o *bit quântico*, abreviado por *q-bit*. Um típico *q-bit*, por exemplo, poderia ser representado por algo como

$$|\text{q-bit}> = a\,|\text{zero}> + b\,|\text{um}>\,,$$

onde |zero> representa o bit (clássico) zero e |um> representa o bit um e onde *a* e *b* são números, possivelmente complexos. Se *a* e *b* forem números reais, então a probabilidade de uma medição do q-bit resultar no bit zero será a^2. Correspondentemente, a probabilidade de uma medição resultar no bit um será b^2.

Este processo é semelhante ao lançamento de uma moeda. Antes do final do lançamento, existe uma probabilidade de o resultado ser cara e uma probabilidade de ser coroa. Neste caso, o estado da moeda é um gênero de superposição entre os estados cara e coroa. Entretanto, esta imagem não é mais do que uma analogia. De fato, se fosse conhecido o estado mecânico exato da moeda no instante do lançamento, poderíamos prever com precisão absoluta o resultado final, cara ou coroa. Isso

implicaria conhecer sua massa, seu formato, sua posição inicial, sua velocidade inicial, bem como todas as forças a que está sujeita a moeda, tais como a força de gravidade e a força do vento. Do ponto de vista da física clássica, uma abordagem probabilística para o jogo de cara ou coroa estaria relacionada a um déficit de informações, as quais poderiam ser obtidas com um processo experimental mais preciso. No caso quântico, em geral, não há como evitar o uso da teoria das probabilidades. Os estados cara e coroa (ou zero e um) estão superpostos "de verdade" e não apenas "de mentirinha". Uma vez, porém, que já se concluiu o jogo, obtendo cara ou coroa, a superposição de estados é destruída. Realizar uma medição implica perturbar a superposição. O *q-bit* colapsa, dando lugar a um *bit* ordinário. Aí está uma das dificuldades fundamentais, senão a dificuldade principal da computação quântica, ou melhor, como operar com *q-bits* sem que estes degenerem nos *bits* ordinários. Esta situação em que um estado na forma de uma superposição recai em *bits* clássicos é dita *descoerência*, devido ao caráter "coerente" inerente às superposições correspondendo aos *q-bits*. O funcionamento correto de um computador quântico implica evitar a descoerência a qualquer custo. Para tanto, é necessário um elevado grau de controle sobre o aparelho. Não se sabe se é possível construir uma máquina que realize computação quântica além de algumas tarefas triviais, justamente pelo problema da descoerência. Descoerência não quer dizer necessariamente observar o sistema de *q-bits*, utilizando algum aparelho de medição. A perda de coerência advém da simples interação dos *q-bits* com o meio externo.

Uma parte dos esforços teóricos em computação e informação quântica está em obter uma prova de que seja *impossível* a fabricação de um computador quântico complexo o bastante para que seja útil. Não seria a primeira vez que uma demonstração negativa teria sido bastante útil para a ciência e a tecnologia. Por exemplo, a primeira lei da termodinâmica foi utilizada para descartar a criação do moto perpétuo, que seria uma máquina capaz de realizar trabalho eternamente, sem a necessidade de lhe ser fornecida energia. Seria uma lástima ter que abandonar assim tão abruptamente o projeto da computação quântica, mas paciência, se não dá, não dá e não se fala mais nisso.

Outra parte dos esforços na área está direcionada à concepção de esquemas de computação quântica estáveis o suficiente para contornar o problema da descoerência. Esta questão passa pela realização física, concreta, dos computadores quânticos. Por exemplo, existem propostas para computadores quânticos, utilizando luz em cavidades, ressonância magnética nuclear ou íons aprisionados em armadilhas. Cada uma destas sugestões padece de uma ou outra dificuldade, que se tem procurado contornar. Para maiores detalhes, consultar as refe-

rências (Davidovich, 2004, Nielsen, 2004, Portugal, 2004 ou Preskill, 2005). Atualmente, o computador quântico real capaz de executar as tarefas mais complexas é um computador quântico que vem de uma colaboração entre o MIT (*Massachussets Institute of Technology*) e a empresa IBM. Este computador quântico está baseado na manipulação de uma molécula de cinco átomos de flúor e dois de carbono, utilizando ondas de rádio-freqüência. O estado de cada um destes átomos simula um *q-bit*, de modo que são apenas sete *q-bits* presentes na máquina. Portanto, a sua aplicabilidade a problemas práticos é muito limitada.

Mais exatamente, este computador quântico foi utilizado para a fatoração do número 15 através do algoritmo de Shor. O resultado, como esperado, foi que 15 = 3 x 5. Voltaremos à questão da fatoração e do algoritmo de Shor com mais detalhes adiante. Por hora, vamos apenas observar que, por mais prosaica que seja a conclusão de que 15 = 3 x 5, não podemos menosprezar o feito do computador quântico do MIT e da IBM, mostrando que a descoerência pode ser evitada ao menos numa situação bem simplificada. Vale dizer que o computador quântico do MIT e da IBM envolve uma estrutura enorme, inclusive com um sofisticado sistema de refrigeração. Efetivamente, altas temperaturas implicariam um certo grau de aleatoriedade no movimento dos *q-bits*, que é justamente o que se pretende evitar. Além disso, a manipulação por ondas de rádio exige, por sua vez, uma complicada estrutura de engenharia. Há aqui um paralelo com os primórdios da computação clássica, quando os computadores necessitavam de salas inteiras e um complexo sistema de refrigeração para evitar a destruição dos seus circuitos eletrônicos. No momento, não se acredita seriamente que seja possível evoluir a ponto de chegar a computadores quânticos portáteis. O cenário mais razoável seria aquele em que apenas alguns computadores quânticos fossem direcionados à resolução de problemas específicos. Seriam uma espécie de "hiper-supercomputadores", gerenciados por algumas universidades, empresas ou governos arcando com o ônus da construção e da manutenção das máquinas, bem como usufruindo os seus benefícios.

No dia-a-dia do nosso mundo macroscópico, os objetos estão continuamente sofrendo descoerência devido à interação com o meio externo. Isso faz nossa realidade parecer clássica e não quântica. Entretanto, é fundamental entender melhor o processo de transição do microscópico para o macroscópico, tratando, então, de sistemas que não chegam a ponto de prescindir completamente de uma descrição quântica, mas que, em certa medida, possam ser considerados "clássicos". A nanotecnologia poderá oferecer algumas perspectivas nesta direção.

Vejamos algumas possíveis utilizações da computação quântica. Certamente, a idéia teórica da computação quântica e

da informação quântica é bastante atraente, filosofica e esteticamente, mas não é a busca da beleza que move as grandes corporações a investirem no setor. De fato, existem comprovadamente algumas aplicações concretas da computação quântica, que seriam capazes de resolver problemas inacessíveis à computação clássica. Sem estas aplicações a problemas reais, a computação quântica provavelmente se manteria como uma curiosidade intelectual, um tema meramente acadêmico. Foi Peter Shor (Shor, 1997) quem primeiro elaborou um algoritmo quântico capaz de resolver de modo eficiente o problema da fatoração. A *fatoração* é aquela operação matemática em que se decompõe um número inteiro em um produto de números primos. Assim, por exemplo, fatoramos o número 20 conforme $20 = 2 \times 2 \times 5$. No trabalho referido, Shor mudou radicalmente a visão externa sobre a computação quântica, que passou a receber atenção séria da sociedade. Para tratar do feito de Shor, tentaremos explicar alguns termos que podem não ser do conhecimento de todos.

Por *algoritmo*, entende-se uma seqüência de passos para a execução de uma tarefa. Assim, por exemplo, podemos desmembrar um bom número de tarefas em algoritmos. Isso não significa que *tudo* possa ser tratado por algoritmos. A este respeito, não existe um algoritmo universal para a demonstração de todos os teoremas da matemática. É bastante duvidoso, além disso, que exista algum algoritmo para a criação artística, embora existam pesquisas (abomináveis, na nossa opinião) sobre música escrita por computadores e assim por diante. Aparentemente, há algo na mente humana que transcende a computação, a qual é calcada sempre em algoritmos. No caso da computação clássica, as etapas dos algoritmos correspondem a determinadas operações matemáticas sobre *bits*. Na computação quântica, o que se manipula são os *q-bits*, isto é, superposições coerentes de zeros e uns. A forma física como isso é feito depende da engenharia do computador quântico. Eventualmente, as etapas do algoritmo quântico podem ser efetuadas graças à manipulação por laser de íons aprisionados, no caso de um computador quântico feito com armadilhas de íons. O algoritmo quântico em sí mesmo, contudo, não se refere a nenhuma realização física do computador. Um dos desafios atuais é como elaborar *algoritmos quânticos* eficientes, levando em conta os princípios básicos da física quântica, que são a superposição de estados, o entrelaçamento e a teoria da medida. Como não somos treinados a "pensar de modo quântico", este parece ser um grande desafio. O caso é ainda pior porque não basta escrever um bom algoritmo quântico: este tem de ser capaz de resolver algum problema de maneira mais eficiente que os algoritmos clássicos disponíveis. Pois bem, Shor conseguiu isso no caso do problema da fatoração.

Aparentemente, não é tão difícil assim fatorar. Entretanto, considere um número inteiro grande, tal como 3746587789347437876527625765237235785237897396. À medida que o número de dígitos cresce, os algoritmos clássicos disponíveis implicam a realização de um número exponencialmente maior de etapas intermediárias. Assim, mesmo com os melhores processadores de que dispomos, seria necessário esperar cerca de cem mil anos para fatorar números descritos por, digamos, mil *bits*. Entretanto, com o algoritmo de Shor, apenas alguns minutos seriam necessários para fatorar o mesmo número! É uma melhoria extraordinária na eficiência da resolução do problema. Entretanto, não está categoricamente demonstrado que não existe um algoritmo clássico eficiente para a fatoração. O que sabemos é que há décadas se direcionam esforços para a concepção de um tal algoritmo, sem sucesso até agora. A lição que extraímos é que não basta escrever um algoritmo para resolver algum problema; a solução há de ser *eficiente.* Um dos aspectos da eficiência se relaciona ao tempo necessário para executar o algoritmo. Outro aspecto se refere às exigências físicas do algoritmo, relativamente ao consumo de energia e de espaço. Não adianta nada propor um algoritmo que necessite de um computador do tamanho do sistema solar.

O que há de tão especial no problema da fatoração? Do ponto de vista prático, os esquemas mais utilizados para a transmissão segura de informação pala Internet envolvem a fatoração de grandes números. A codificação e a decodificação de informação é a milenar arte da *criptografia*, de notável importância comercial nesta era dos cartões de crédito. Um espião munido de um computador quântico e do algoritmo de Shor será capaz de quebrar os esquemas de criptografia usuais num tempo acessível, o que levaria virtualmente ao colapso da economia mundial. Apenas para dar uma idéia do que significa criptografar, vejamos o esquema utilizado por Júlio César para trocar mensagens com seus generais, na Roma antiga. Simplesmente, as letras eram todas deslocadas três vezes para a direita no alfabeto. Assim, A virava D, B virava E e assim por diante. Por exemplo, a expressão

GATO GORDO

seria codificada conforme

JDXR JRUGR .

Na codificação acima, estamos considerando um alfabeto que não contém as letras K, Y e W. Desse modo, a letra T é codificada em X e não em W.

É de impressionar que os bárbaros não fossem capazes de se dar conta de um esquema tão ingênuo.

Mais recentemente, a criptografia evoluiu muito. Na Segunda Guerra, a quebra dos esquemas de criptografia dos alemães foi muito importante para o desenlace do conflito, o que alavancou o desenvolvimento da teoria da informação. Atualmente, organizações para espionagem, privadas ou governamentais, investem pesadamente na quebra de esquemas de criptografia. Não precisamos entrar em detalhes técnicos, bastando observar que a dificuldade para a fatoração de grandes números é que confere segurança às trocas de informação pela rede mundial de computadores. A *chave* do esquema criptográfico é um número com muitos dígitos, utilizado para codificar as mensagens. A chave criptográfica é de domínio público. Entretanto, para decodificar as mensagens, isto é, decifrá-las, é preciso fatorar a chave criptográfica, o que é um problema de grande complexidade. Os agentes que trocam as mensagens devem estar a par dos fatores primos da chave criptográfica. É muitíssimo pouco provável que um espião possa descobrir os fatores primos da chave num tempo hábil. Isso, antes de aparecer o algoritmo de Shor...

Se, por um lado, a computação quântica parece estar querendo colaborar com espiões e terroristas, por outro lado, também é possível utilizá-la para tornar invioláveis as mensagens trocadas entre computadores. De fato, ao interceptar uma mensagem clássica, um espião precisa descobrir quais são os *bits* que estão sendo transmitidos de um computador para outro. Descobrir o valor dos *bits* significa medi-los de algum modo. Na computação quântica, entretanto, o que se troca são *q-bits*, e a medição do estado de um *q-bit* acarreta uma perturbação grande demais para permanecer oculta, ou melhor, o processo de espionagem leva à descoerência, o que pode ser quantificado de modo preciso. Alguém até poderia espionar, mas não passaria despercebido. Estas idéias podem ser levadas a cabo com todo detalhe, de modo a produzir um esquema de transmissão segura de informação quântica. Inclusive, já existem experiências reais onde se troca, com absoluta segurança, informação quântica, com algumas empresas oferecendo *kits* para o processo. O leitor pode confirmar isso numa procura na Internet, usando a expressão *quantum cryptography.* Do exposto, concluímos que a criptografia quântica é uma área florescente.

Um aspecto interessante da troca segura de informação quântica se refere à impossibilidade genérica de se copiar *q-bits* com absoluta fidelidade. Isso se expressa matematicamente pelo teorema da não-clonagem. Muitos até podem se lamentar pela não existência de um teorema da não-clonagem na biologia. No caso clássico, é fácil clonar informação, como no caso das máquinas de xerox ou do grupo de *rock* Aerosmith, que é

uma cópia bastante fiel dos Rolling Stones (opinião pessoal). No caso quântico, entretanto, o teorema da não-clonagem impede a cópia de *q-bits*. Caso contrário, seria possível elaborar um número suficientemente grande de cópias de um dado *q-bit*, usando isso para descobrir seu estado sem nenhuma perturbação, ou seja, poderíamos medir o estado do *q-bit* efetuando medidas de suas cópias e não dele próprio, evitando a descoerência. Na analogia do jogo de cara ou coroa, repetir-se-ia o jogo, copiando o estado da moeda em pleno vôo e avaliando o resultado. Caso fosse encontrado o valor "cara" em 40 % das vezes e o valor "coroa" em 60 %, a conclusão seria que a moeda original estaria descrita pelo *q-bit* composto por 40 % de cara e 60 % de coroa. Esta conclusão não implicaria nenhuma perturbação do estado da moeda, já que foram as suas cópias que foram medidas! Entretanto, o teorema da não-clonagem descarta esta experiência: não é possível copiar informação quântica com absoluta fidelidade.

Além da criptografia quântica, temos aplicações da computação quântica ao problema da busca em bancos de dados. Um exemplo a este respeito é fornecido pelos programas de busca na Internet. O algoritmo de Grover (Grover, 1996) proporciona-nos um método quântico de acelerar o processo de procura em bancos de dados. No caso do algoritmo de Grover, o ganho não é tão espetacular quanto no caso do algoritmo de Shor. A título de comparação, se o número de etapas envolvidas no algoritmo clássico de busca for 1000, então esta mesma busca poderá ser efetuada com o algoritmo de Grover com um número aproximado de 32 etapas. Mesmo assim, trata-se de um avanço respeitável, levando em conta que não consideramos buscas em bancos de dados unicamente no caso da Internet. Se fosse assim, não haveria tanta necessidade de um novo algoritmo, já que dá para considerar bastante bons os resultados que costumamos obter em pesquisas na Internet. Em outros problemas de busca, não podemos afirmar o mesmo. Por exemplo, um problema básico em dinâmica molecular consiste em determinar a conformação geométrica ideal de uma macromolécula, como uma proteína, com base em uma listagem dos seus componentes. O objetivo da busca, neste caso, é encontrar a conformação geométrica que minimiza a energia potencial do sistema. Conhecendo a forma da macromolécula, é possível obter conclusões sobre as suas funções fisiológicas, os tipos de reação química que a macromolécula facilitará e assim por diante. Ocorre que os algoritmos atualmente existentes, clássicos, não dão conta deste problema com eficiência. Em geral, é necessário impor algumas aproximações mais ou menos grosseiras até que se obtenha algum resultado. Portanto, a construção de um computador quântico seria útil para a biologia molecular e, por que não imaginar, para a indústria farmacêutica interessada na fabri-

cação de novos remédios cuja base seria uma ou outra macromolécula artificialmente construída. Engenharia genética, medicina, entendimento mais acurado da molécula de DNA... são inúmeras as possibilidades abertas.

Os algoritmos de Shor e de Grover, bem como praticamente todos os algoritmos quânticos, envolvem a medição do estado dos *q-bits* que são manipulados. Como o processo de medida é intrinsecamente probabilístico, os algoritmos quânticos dão sempre resultados probabilísticos. No caso do problema da busca em banco de dados, por exemplo, um algoritmo quântico forneceria a informação de que, com 99,9 % de probabilidade, a conformação mais estável de uma proteína seria esta ou aquela. Conviver com as incertezas faz parte do mundo quântico. Entretanto, sempre é possível obter condições para que o grau de acerto do algoritmo seja suficientemente alto. Além disso, pode-se demonstrar que o processo de medição pode ser deixado para a última etapa do algoritmo. Antes disso, os *q-bits* são manipulados de modo completamente determinístico.

Na computação clássica, também se lança mão de algoritmos probabilísticos, como no caso do método de Monte Carlo, por exemplo. Uma das aplicações mais prosaicas do método de Monte Carlo é o cálculo numérico da área determinada por uma certa região. Nesse caso, a resposta fornecida pelo método de Monte Carlo é mais veloz do que a de outros algoritmos não-probabilísticos. Não se trata, porém, de uma resposta absolutamente segura: vem acompanhada de um erro, diminuto que seja, mas ainda assim um erro. O que se ganha em eficiência, ou velocidade de processamento, se perde em confiabilidade. Na prática, o erro costuma ser tão pequeno que vale a pena perder em confiabilidade para ganhar em velocidade. Entretanto, o caráter aleatório dos algoritmos clássicos não é semelhante ao dos algoritmos quânticos. Vejamos o método de Monte Carlo ou qualquer outro instrumento que se baseia na geração de números aleatórios. Por sinal, qualquer calculadora que se preze tem uma tecla que fornece números aleatórios. Na realidade, estes números aleatórios são fruto de alguma operação matemática complicada, mas determinística. É difícil desvendar a natureza exata desta operação, de modo que, para todos os efeitos práticos, o número pode ser considerado aleatório. Pelo contrário, no caso quântico há uma etapa genuinamente probabilística, que é aquela em que se mede o estado dos *q-bits*, no sentido em que não há regra determinística que possa fornecer o resultado.

Mencionamos a questão da predição da forma exata de uma macromolécula, usando algoritmos quânticos. De modo mais geral, o processamento paralelo massivo permitido pela manipulação de superposições coerentes de estados permite acelerar em muito qualquer simulação computacional. Assim, a

computação quântica poderia resolver um sem número de problemas computacionais atualmente inacessíveis mesmo aos melhores computadores clássicos. Existe a tendência a imaginar que tudo, com relação às ciências exatas, pode ser eficientemente simulado em computadores, mas não é bem assim. Por exemplo, o comportamento detalhado de alguns dispositivos microeletrônicos exige a resolução numérica (computacional) de um certo sistema de equações, o que atualmente só pode ser feito eficientemente considerando apenas duas dimensões espaciais. Como o mundo é tridimensional, temos aqui uma perda de informação, ao menos no estágio tecnológico atual... Virtualmente, todas as áreas de pesquisa que utilizam modelagem matemática teriam a ganhar com computadores muito mais velozes do que os atuais. Este é também um incentivo à pesquisa sobre computação quântica.

Um outro algoritmo quântico de relevância é o algoritmo para o *teletransporte.* Aqui, teletransporte designa a transmissão de informação à distância, sem a necessidade, por exemplo, de envio de um sinal elétrico. Por exemplo, os *bits* que são transferidos de um microcomputador a outro, na Internet, envolvem algum tipo de sinal eletromagnético. Ao contrário, no caso do teletransporte não é necessária nenhuma troca de sinais. O princípio do teletransporte é o sutilíssimo entrelaçamento quântico. Utilizando a não-localidade, torna-se possível enviar o estado quântico de um conjunto de *q-bits* a outro conjunto de *q-bits* sem precisar enviar sinais eletromagnéticos ou transportar fisicamente os *q-bits* originais de um ponto a outro. Inicialmente realizado experimentalmente com fótons (partículas de luz), mais recentemente conseguiu-se rodar o algoritmo de teletransporte, utilizando-se átomos. A essência do teletransporte consiste em enviar as propriedades físicas de um sistema de um canto a outro. Por exemplo, um raio de luz pode surgir reproduzindo as mesmas propriedades de um raio original. Naturalmente, o teletransporte se refere a sistemas microscópicos, não sendo possível enviar, digamos, uma pessoa de um canto a outro... O problema, como sempre, é controlar a descoerência, que se manifesta sempre que tratamos de entidades macroscópicas. De modo poético, a primeira experiência sobre o teletransporte com matéria envolveu a transmissão do estado de átomos através do leito do rio Danúbio, em Viena (jornal *Zero Hora*, edição de 18 jun. 2004).

Esperamos que o teletransporte e a não-localidade quântica sirvam para a transmissão segura de informação e também para o envio de informação ultradensa. Nesta última aplicação, consideram-se algoritmos quânticos análogos aos algoritmos clássicos para compressão de dados, os quais levam em conta o fato de que sempre há um certo grau de redundância em qualquer linguagem. No caso da teoria da informação clássica, de-

monstramos que é possível comprimir uma mensagem até um certo limite, que depende do tipo de mensagem que tentamos transmitir e das características físicas do canal de comunicação. Apenas para fixar as idéias e sem nenhuma pretensão de rigor, temos um exemplo de compactação de mensagens na linguagem das salas de bate-papo na Internet. Considere-se, a respeito, as abreviações "tb" para "também", "bj" para "beijo" e assim por diante. Não fazemos aqui a apologia da grosseria e do desrespeito à língua, mas, do ponto de vista da transmissão rápida de informação, é claro que é conveniente poder compactar mensagens. Existem esquemas matemáticos bem precisos para fazer isso com a máxima eficiência. No caso da teoria da informação quântica, podemos demonstrar que é possível compactar com eficiência em um grau superior ao do caso clássico. É a isso que nos referimos quando falamos de envio de informação ultradensa. Fisicamente, o que permite esta compactação adicional é o entrelaçamento, a não-localidade inerente à física quântica, que comparece também no caso do teletransporte.

Entrando de cabeça no terreno da alta especulação, é de se imaginar se a computação quântica não teria alguma implicação na pesquisa sobre inteligência artificial. Os especialistas divergem sobre ser ou não possível o surgimento de máquinas pensantes. Afinal de contas, o que vem a ser a consciência, a alma ou os sentimentos? Uma máquina, por definição, procede segundo algum algoritmo. Faz sentido imaginar um algoritmo capaz de reproduzir algo como a experiência da beleza? Supondo que uma máquina venha a manifestar algo semelhante ao livre-arbítrio, quais seriam nossas responsabilidades éticas diante disso? Quem sabe, sejamos obrigados a eleger os computadores como nossos irmãos ou, pior, quem sabe *eles* é que passem a nos tratar com a condescendência dos senhores. Os adeptos da teoria da emergência, *grosso modo*, acham que basta esperar pelo aumento da complexidade dos circuitos eletrônicos dos computadores e pronto, lá pelas tantas, as máquinas manifestarão comportamentos tão inteligentes ou mais do que os nossos próprios comportamentos. Outros, ao contrário, argumentam pela insuficiência de processos algorítmicos, sistemáticos, para chegar a tanto. Pessoalmente, acho que há algo mais na consciência do que a simples manipulação sistemática de *bits*, mas esta é uma questão de fé pessoal. Não creio que exista um algoritmo extremamente complexo que dê conta da experiência humana do livre-arbítrio. Seria como um retorno ao universo de Laplace: todo livre-arbítrio seria mera ilusão, fruto de nossa ignorância. Seríamos como autômatos sem o saber. A questão toda assume outro tom quando consideramos a computação quântica. Há um grau de indeterminação no processamento de informação com *q-bits*, devido ao caráter probabilístico da interação dos *q-bits* com o meio externo. Conforme argu-

mentamos anteriormente, há uma espécie de jogo de azar sempre que a descoerência entra em campo. Conseqüentemente, quem sabe, os computadores quânticos sejam candidatos mais naturais para máquinas pensantes de fato, não oferecendo um mero simulacro do que chamamos inteligência. Seria interessante conhecer o ponto de vista de Roger Penrose a respeito, já que este físico-matemático publicou suas obras mais conhecidas sobre o problema da consciência (Penrose, 1989; Penrose, 1996) anteriormente ao *boom* da computação quântica.

Conclusão

Mostramos algumas das possibilidades que seriam abertas graças à construção de computadores quânticos com um número razoável de *q-bits*. Além disso, refletimos um pouco sobre a teoria da informação quântica, a qual não é mais apenas especulação. Já se tem a realização concreta de esquemas para teletransporte ou de transmissão de dados com alta compactação, graças a uma engenhosa utilização do entrelaçamento quântico. Nosso país, inclusive, tem investido na área de informação quântica (DAVIDOVICH, 2004). De tudo isso, concluímos que a informação quântica veio para ficar, tanto como área de pesquisa quanto como área de aplicações tecnológicas. Também não podemos afirmar com absoluta segurança sobre o futuro da computação quântica. Não dispomos atualmente de uma tecnologia que nos dê o grau de controle necessário para a manipulação de um número suficientemente grande de *q-bits*, contornando o problema da descoerência. Esta afirmação é verdadeira no que tange aos esquemas já propostos para computadores quânticos. Entretanto, nada impede que, num futuro talvez nem tão distante, surjam novas propostas para a computação quântica que dêem conta satisfatoriamente da questão da descoerência. É impossível prever. Basta recordar o álacre ceticismo com que foram recebidas as geringonças precursoras dos primeiros computadores. Quem sabe algo parecido não acontecerá com os computadores quânticos? Comparativamente, a computação quântica está sendo recepcionada com muito mais entusiasmo que a computação clássica. Lógico, trata-se de uma questão até mesmo de espírito dos tempos. Na nossa sociedade, parece ser de mau tom expressar ceticismo diante das promessas da ciência. O planeta pode ir às favas e nem por isso nossa fé na ciência será abalada. É educativo recordar a história da fusão termonuclear controlada. A pesquisa na fusão termonuclear controlada surgiu na década de 50 do século passado, na esteira da guerra fria e da corrida armamentista. Isso aconteceu porque os processos físicos da fusão controlada são os mesmos que intervêm na explosão das bombas de hidrogênio. Entretanto, como o nome diz, no caso da fusão *controlada*, espera-se liberar energia

de maneira suficientemente segura. Nosso Sol, por exemplo, é um reator nuclear à fusão ao natural, liberando energia para o espaço. Nesse caso, o mecanismo que impede que o Sol se comporte como uma bomba de hidrogênio é a força de gravidade, que mantém a coesão entre as suas partículas a despeito das reações nucleares que ocorrem continuamente. Se conseguíssemos arquitetar, em laboratório, reatores de fusão termonuclear controlada eficiente, teríamos uma fonte de energia barata, virtualmente inesgotável e pouco danosa ao meio ambiente. Acalentados por essa perspectiva, inúmeros cientistas se dedicaram à questão nos primórdios da pesquisa em fusão controlada, no afã de resolver o problema rapidamente. Foi feita propaganda do assunto entre os parlamentares (notadamente nos Estados Unidos), com a liberação generosa de recursos. Entretanto, havia otimismo exagerado. Décadas se passaram e, até agora, não temos um reator nuclear à fusão que seja eficiente, ou seja, que libere mais energia do que aquela que é necessária para sua ignição. Existe em andamento o projeto ITER (*International Thermonuclear Experimental Reator*), envolvendo a União Européia, o Japão, os Estados Unidos, a Rússia, a Coréia do Sul e a China, prometendo nos aproximar do desejado, mas os mais otimistas falam em décadas de trabalho até obter sucesso. Conseqüentemente, hoje em dia, os governos são muito mais reticentes à liberação de financiamento para projetos em pesquisa da fusão termonuclear controlada. Esta desconfiança vem em péssima hora diante do consumo cada vez maior de recursos energéticos finitos, tais como o petróleo. É de imaginar-se que os governos voltem a investir pesadamente na fusão, quando não houver outra saída, ou seja, quando chegar à hora do desespero, com o colapso da indústria diante da escassez de recursos energéticos. É esperar para ver. Enfim, não é impossível que a computação quântica não passe de um sonho de uma noite de verão, ainda mais radical do que foi a fusão termonuclear controlada. Entretanto, no cenário otimista, a simulação numérica pesada relativa ao ITER poderá ser realizada num computador quântico, contribuindo decisivamente para a resolução da questão energética. Não há dúvida de que as empresas pioneiras na computação quântica terão os maiores lucros e que os países envolvidos seriamente com pesquisa na área terão grande vantagem sobre os outros com relação ao poder geopolítico. As tecnologias para informação e para geração de energia estarão certamente entre as mais decisivas no futuro e no presente. É interessante observar que, enquanto este trabalho era escrito, foi decidido que o sítio para a construção do reator nuclear do ITER será em Cadarache, cidade do sul da França (*BBC News*, 28 jun. 2005). Ponto para a União Européia!

Quem sabe seja interessante realizarmos um exercício de futurologia, tentando prever alguns aspectos do desenvolvimen-

to da computação quântica. Não é de imaginar-se que venham a ser disponibilizados computadores quânticos portáteis, a menos que alguma tecnologia completamente revolucionária apareça. O cenário mais provável envolve alguns computadores quânticos sob a guarda de forças militares, grandes empresas ou universidades. Esses poucos computadores estariam reservados a tarefas muito específicas, tais como a simulação detalhada do dobramento de proteínas. Do ponto de vista empresarial, isso seria um empecilho ao rápido desenvolvimento da computação quântica, devido aos vultosos gastos que seriam necessários para a criação e a manutenção destes computadores de grande porte. Há que se comparar com o desenvolvimento da computação clássica, quando, historicamente, pequenas empresas foram capazes de novas propostas de *hardware* e *software*, contribuindo para a disseminação da informática em todas as áreas da sociedade. Naturalmente, isso só pôde acontecer graças ao baixo custo dos materiais envolvidos. "Empreendedorismo", na computação quântica, só se for na hora de inventar alguma teoria física revolucionária. Não é de se esperar que algum *nerd* viciado em baixar música pela Internet entre na garagem do pai e saia dali com um computador quântico portátil montado com ferro velho. Entretanto, há lendas (comprovadas ou não) de fatos semelhantes na história da computação clássica.

Outro cenário possível seria aquele em que computadores clássicos estariam conectados a computadores quânticos. Nesse caso, as tarefas mais pesadas na execução de alguns programas ficariam reservadas aos processadores quânticos. Os resultados do processamento quântico poderiam ser, então, comunicados ao computador clássico, inclusive pela Internet.

Uma terceira possibilidade seria a criação de máquinas híbridas, entre o clássico e o quântico. Esta avenida nem sempre é recebida com entusiasmo, porque parece pouco razoável esperar que fenômenos como o entrelaçamento possam ser reproduzidos por um computador semiclássico. Entrando, no terreno da pura especulação, talvez seja necessário esperar pelo surgimento de uma teoria física que descreva eficientemente tanto o mundo macroscópico quanto o mundo microscópico. Sabemos que a física clássica, adequada para o mundo macroscópico, surge como uma aproximação da física quântica, adequada para o mundo microscópico. Aqui, a questão central é a *eficiência* das descrições. Em princípio, nada nos impede de descrever a evolução temporal dos sistemas macroscópicos, utilizando a mecânica quântica, ou seja, analisando a função de onda de todas as partículas do sistema macroscópico. O problema é que esta abordagem não é eficiente matematicamente. Há informação em excesso na função de onda, no que tange ao movimento de corpos de tamanho razoável, como uma bola de futebol ou

um robô. Infelizmente, porém, ao fazermos a redução da física clássica à física quântica, descartamos fatores fundamentais como o entrelaçamento e a superposição de estados. É como jogar fora a água da bacia, jogando fora o bebê junto. Será que é possível encontrar uma teoria que estivesse no meio do caminho entre a física clássica e a física quântica, de modo a obter cada uma destas descrições como casos especiais? Esta é uma pergunta fundamental para a física teórica. Uma tal descrição híbrida, igualmente adaptada aos mundos do grande e do pequeno, poderia ser útil na invenção de computadores híbridos, entre o clássico e o quântico.

Referências bibliográficas

BELL, J. S. On the Einstein-Podolsky-Rosen Paradox. *Physics*, v. 1, p. 195,1964.

BENIOFF, P. The Computer as a Physical System: a Microscopic Quantum Hamiltonian Model of Computers as Represented by Turing Machines. J. Stat. *Phys*, v. 22, p. 563,1980.

BOHR, N. H. D. *Atomic Physics and Human Knowledge*. New York: John Wiley & Sons, 1958.

BUNGE, M. *Philosophy of Physics.* Dordrecht: Reidel, 1973.

DAVIDOVICH, L. Informação Quântica: do Teletransporte ao Computador. *Ciência Hoje*, v. 35, n. 206, p. 24, 2004.

DEUTSCH, D. Quantum Theory, the Church-Turing Principle and the Universal Quantum Computer. *Proc. R. Soc. London A,* v. 400, p. 97, 1985.

DIONÍSIO, P. H. *Física Quântica: da sua Pré-História à Discussão sobre seu Conteúdo Essencial*. n. 22, 2004. (Cadernos IHU Idéias).

PHYSICS TODAY EDITOR. Quantum Cryptography Defies Eavesdropping. *Phys*. Today, p. 21, nov. 1992.

EINSTEIN, A; PODOLSKY, B; ROSEN, N. Can the Quantum-Mechanical Description of Physical Reality be Considered Complete? *Phys. Rev*., v. 47, p. 777, 1935.

FEYNMAN, R. P. Simulating Physics with Computers. *Int. J. Theor. Phys*, v. 21, p. 467,1982.

GROVER, L. K. *A Fast Quantum Mechanical Algorithm for Database Search.* In 28th Association for Computing Machinery Symposium on Theory of Computation, p. 212, New York, 1996.

HAAS, F. Stochastic Quantization of Time-Dependent Systems by the Haba-Kleinert Method, *Int. J. Theor. Phys*, v. 44, p. 1, 2005.

_____. Low Momentum Classical Mechanics with Effective Quantum Potentials, *Phys. Rev. B,* v. 71, p. 23511, 2005.

HEISENBERG, W. *Physics and Philosophy: the Revolution in Modern Science*. New York: Harper and Brothers, 1958.

JAMMER, M. *The Philosophy of Quantum Mechanics: the Interpretations in Quantum Mechanics in Historical Perspective*. New York: John Wiley & Sons, 1974.

NIELSEN, M. A; CHUANG, I. L. *Computação Quântica e Informação Quântica*. Porto Alegre: Bookman, 2005.

OLIVEIRA, I. S. *Computação Quântica*. Disponível em: <http://www.comciencia.br/reportagens/nanotecnologia/nano01.htm> Acesso em: nov. 2002.

OLIVEIRA, I. S; SARTHOUR, R; BULNES, J;. BELMONTE, S. B; GUIMARÃES, A. P; AZEVEDO E. R. de; VIDOTO; E. L. G.; BONAGAMBA T. J; FREITAS, J. C. C. Computação Quântica: Manipulando a Informação Oculta do Mundo Quântico. *Ciência Hoje*, v. 33, n. 193, p. 22, 2003.

PENROSE, R. *The Emperor's New Mind*. Oxford, Oxford University Press, 1989.

_____. *The Large, the Small and the Human Mind*. Cambridge: Cambridge University Press, 1996.

PORTUGAL, R; C. LAVOR C; CARVALHO L. M; MACULAN, N. M. Uma Introdução à Computação Quântica. *Notas em Matemática Aplicada*, v. 8. São José dos Campos: Sociedade Brasileira de Matemática Aplicada e Computacional, 2004.

PRESKILL, J. Notas de aula do curso de computação quântica no Califórnia Institute of Technology (CALTECH). Disponível em: <http://www.theory.caltech.edu/preskill/ph219>.

SHOR, P. W. Polynomial-time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer. *SIAM J. Comp*., v. 26, p. 1484, 1997.

Artigo enviado ao IHU
em 16 de novembro de 2005.

TEMAS DOS CADERNOS IHU IDÉIAS

N. 01 *A teoria da justiça de John Rawls* – Dr. José Nedel.
N. 02 *O feminismo ou os feminismos: Uma leitura das produções teóricas* – Dra. Edla Eggert.
O Serviço Social junto ao Fórum de Mulheres em São Leopoldo – MS Clair Ribeiro Ziebell e Acadêmicas Anemarie Kirsch Deutrich e Magali Beatriz Strauss.
N. 03 *O programa Linha Direta: a sociedade segundo a TV Globo* – Jornalista Sonia Montaño.
N. 04 *Ernani M. Fiori – Uma Filosofia da Educação Popular* – Prof. Dr. Luiz Gilberto Kronbauer.
N. 05 *O ruído de guerra e o silêncio de Deus* – Dr. Manfred Zeuch.
N. 06 *BRASIL: Entre a Identidade Vazia e a Construção do Novo* – Prof. Dr. Renato Janine Ribeiro.
N. 07 *Mundos televisivos e sentidos identiários na TV* – Profa. Dra. Suzana Kilpp.
N. 08 *Simões Lopes Neto e a Invenção do Gaúcho* – Profa. Dra. Márcia Lopes Duarte.
N. 09 *Oligopólios midiáticos: a televisão contemporânea e as barreiras à entrada* – Prof. Dr. Valério Cruz Brittos.
N. 10 *Futebol, mídia e sociedade no Brasil: reflexões a partir de um jogo* – Prof. Dr. Édison Luis Gastaldo.
N. 11 *Os 100 anos de Theodor Adorno e a Filosofia depois de Auschwitz* – Profa. Dra. Márcia Tiburi.
N. 12 *A domesticação do exótico* – Profa. Dra. Paula Caleffi.
N. 13 *Pomeranas parceiras no caminho da roça: um jeito de fazer Igreja, Teologia e Educação Popular* – Profa. Dra. Edla Eggert.
N. 14 *Júlio de Castilhos e Borges de Medeiros: a prática política no RS* – Prof. Dr. Gunter Axt.
N. 15 *Medicina social: um instrumento para denúncia* – Profa. Dra. Stela Nazareth Meneghel.
N. 16 M*udanças de significado da tatuagem contemporânea* – Profa. Dra. Débora Krischke Leitão.
N. 17 *As sete mulheres e as negras sem rosto: ficção, história e trivialidade* – Prof. Dr. Mário Maestri.
N. 18 *Um initenário do pensamento de Edgar Morin* – Profa. Dra. Maria da Conceição de Almeida.
N. 19 *Os donos do Poder, de Raymundo Faoro* – Profa. Dra. Helga Iracema Ladgraf Piccolo.
N. 20 *Sobre técnica e humanismo* – Prof. Dr. Oswaldo Giacóia Junior.
N. 21 *Construindo novos caminhos para a intervenção societária* – Profa. Dra. Lucilda Selli.
N. 22 *Física Quântica: da sua pré-história à discussão sobre o seu conteúdo essencial* – Prof. Dr. Paulo Henrique Dionísio.
N. 23 *Atualidade da filosofia moral de Kant, desde a perspectiva de sua crítica a um solipsismo prático* – Prof. Dr. Valério Rodhen.
N. 24 *Imagens da exclusão no cinema nacional* – Profa. Dra. Miriam Rossini.
N. 25 *A estética discursiva da tevê e a (des)configuração da informação* – Profa. Dra. Nísia Martins do Rosário.
N. 26 *O discurso sobre o voluntariado na Universidade do Vale do Rio dos Sinos – UNISINOS* – MS. Rosa Maria Serra Bavaresco.
N. 27 *O modo de objetivação jornalística* – Profa. Dra. Beatriz Alcaraz Marocco.
N. 28 *A cidade afetada pela cultura digital* – Prof. Dr. Paulo Edison Belo Reyes.
N. 29 *Prevalência de violência de gênero perpetrada por companheiro: Estudo em um serviço de atenção primária à saúde – Porto Alegre, RS* – Profº MS. José Fernando Dresch Kronbauer.

N. 30 *Getúlio, romance ou biografia?* – Prof. Dr. Juremir Machado da Silva.
N. 31 *A crise e o êxodo da sociedade salarial* – Prof. Dr. André Gorz.
N. 32 *À meia luz: a emergência de uma Teologia Gay - Seus dilemas e possibilidades* – Prof. Dr. André Sidnei Musskopf.
N. 33 *O vampirismo no mundo contemporâneo: algumas considerações* – Prof. MS Marcelo Pizarro Noronha.
N. 34 *O mundo do trabalho em mutação: As reconfigurações e seus impactos* – Prof. Dr. Marco Aurélio Santana.
N. 35 *Adam Smith: filósofo e economista* – Profa. Dra. Ana Maria Bianchi e Antonio Tiago Loureiro Araújo dos Santos.
N. 36 *Igreja Universal do Reino de Deus no contexto do emergente mercado religioso brasileiro: uma análise antropológica* – Prof. Dr. Airton Luiz Jungblut.
N. 37 *As concepções teórico-analíticas e as proposições de política econômica de Keynes* – Prof. Dr. Fernando Ferrari Filho.
N. 38 *Rosa Egipcíaca: Uma Santa Africana no Brasil Colonial* – Prof. Dr. Luiz Mott.
N. 39 *Malthus e Ricardo: duas visões de economia política e de capitalismo* – Prof. Dr. Gentil Corazza
N. 40 *Corpo e Agenda na Revista Feminina* – MS Adriana Braga
N. 41 *A (anti)filosofia de Karl Marx* – Profa. Dra. Leda Maria Paulani
N. 42 *Veblen e o Comportamento Humano: uma avaliação após um século de "A Teoria da Classe Ociosa"* – Prof. Dr. Leonardo Monteiro Monasterio
N. 43 *Futebol, Mídia e Sociabilidade. Uma experiência etnográfica* – Édison Luis Gastaldo, Rodrigo Marques Leistner, Ronei Teodoro da Silva & Samuel McGinity
N. 44 *Genealogia da religião. Ensaio de leitura sistêmica de Marcel Gauchet. Aplicação à situação atual do mundo* – Prof. Dr. Gérard Donnadieu
N. 45 *A realidade quântica como base da visão de Teilhard de Chardin e uma nova concepção da evolução biológica* – Prof. Dr. Lothar Schäfer
N. 46 *"Esta terra tem dono". Disputas de representação sobre o passado missioneiro no Rio Grande do Sul: a figura de Sepé Tiaraju* – Profa. Dra. Ceres Karam Brum
N. 47 *O desenvolvimento econômico na visão de Joseph Schumpeter* – Prof. Dr. Achyles Barcelos da Costa
N. 48 *Religião e elo social. O caso do cristianismo* – Prof. Dr. Gérard Donnadieu.
N. 49 *Copérnico e Kepler: como a terra saiu do centro do universo* – Prof. Dr. Geraldo Monteiro Sigaud
N. 50 *Modernidade e pós-modernidade – luzes e sombras* – Prof. Dr. Evilázio Teixeira
N. 51 *Violências: O olhar da saúde coletiva* – Élida Azevedo Hennington & Stela Nazareth Meneghel
N. 52 *Ética e emoções morais* – Prof. Dr. Thomas Kesselring;
Juízos ou emoções: de quem é a primazia na moral? – Prof. Dr. Adriano Naves de Brito

Cadernos IHU Idéias: Apresenta artigos produzidos pelos convidados-palestrantes dos eventos promovidos pelo IHU. A diversidade dos temas, abrangendo as mais diferentes áreas do conhecimento, é um dado a ser destacado nesta publicação, além de seu caráter científico e de agradável leitura.

Fernando Haas (1970) é natural de Porto Alegre/RS. É professor adjunto na Unisinos desde 2003. É bacharel (1991) e mestre em Física (1994) pelo Instituto de Física da Universidade Federal do Rio Grande do Sul – UFRGS, instituição onde também concluiu o Doutorado em Ciências (1998), com a tese *Sistemas de Ermakov Generalizados, Simetrias e Invariantes Exatos.* Em 2000, obteve o Pós-Doutorado na área de física de plasma pelo Laboratoire de Physique des Millieux Ionisés et Applications, Université Henri Poincaré, Nancy, França.

Algumas publicações do autor

A magnetohydrodynamic model for quantum plasmas. *Physics of Plasmas*, Princeton, v. 12, n. 6, p. 062117-1 – 062117-9, jun. 2005.

Low momentum classical mechanics with effective quantum potentials. *Physical Review B: Condensed Matter*, New York, v. 71, n. 23, p. 235111-1 - 235111-6, jun. 2005.

Jacobi structures in R3. *Journal of Mathematical Physics*, Melville, v. 46, n. 10, p. 102703-1 - 102703-11, out. 2005.

Stochastic quantization of time-dependent systems by the Haba and Kleinert method. *International Journal of Theoretical Physics*, Atlanta, v. 44, n. 1, p. 1-9, jan. 2005

GARCIA, Leonardo Geissler; HAAS, Fernando; GOEDERT, João; DE OLIVEIRA, Luís Paulo Luna. Modified Zakharov equations for plasmas with a quantum correction. *Physics of Plasmas*, Princeton, v. 12, n. 1, p. 012302-1 - 012302-8, jan. 2005.