UNIVERSIDADE FEDERAL DE UBERLÂNDIA
INSTITUTO DE FÍSICA
PROGRAMA DE PÓS-GRADUAÇÃO EM FÍSICA

MÁRCIO MACEDO SANTOS

Correlações quânticas e o modelo DQC1

Uberlândia
2015

MÁRCIO MACEDO SANTOS

Correlações quânticas e o modelo DQC1

Tese apresentada ao Programa de Pós-Graduação do Instituto de Física da Universidade Federal de Uberlândia, como requisito parcial para a obtenção de Título de Doutor em Física.

Orientador: Prof. Dr. Eduardo Inacio Duzzioni

Uberlândia
2015

Dados Internacionais de Catalogação na Publicação (CIP)
Sistema de Bibliotecas da UFU, MG, Brasil.

S237c 2015

Santos, Márcio Macedo, 1987-
Correlações quânticas e o modelo DQC1 / Márcio Macedo Santos. - 2015.
107 f. : il.

Orientador: Eduardo Inácio Duzzioni.
Tese (doutorado) - Universidade Federal de Uberlândia, Programa de Pós-Graduação em Física.
Inclui bibliografia.

1. Física - Teses. 2. Computaçao quântica - Teses. I. Duzzioni, Eduardo Inácio. II. Universidade Federal de Uberlândia, Programa de Pós-Graduação em Física. III. Título.

CDU: 53

SERVIÇO PÚBLICO FEDERAL
MINISTÉRIO DA EDUCAÇÃO
UNIVERSIDADE FEDERAL DE UBERLÂNDIA
INSTITUTO DE FÍSICA
PROGRAMA DE PÓS-GRADUAÇÃO EM FÍSICA

MÁRCIO MACEDO SANTOS

Tese apresentada a coordenação do Programa de Pós-graduação em física, do Instituto de Física da Universidade Federal de Uberlândia, para obtenção do título de Doutor em Física.

Uberlândia, 31 de julho de 2015.

BANCA EXAMINADORA

Prof. Dr. Eduardo Inácio Duzzioni
Universidade Federal de Uberlândia – UFU

Profª. Dra. Liliana Sanz de la Torre
Universidade Federal de Uberlândia - UFU

Prof. Dr. José Maria Villas-Bôas
Universidade Federal de Uberlândia – UFU

Prof. Dr. Marcos Cesar de Oliveira
Universidade Federal de Campinas/UNICAMP

Prof. Dr. Roberto Menezes Serra
Universidade Estadual do ABC/UFABC

A minha amada esposa, Sharita, que pelo apoio e companheirismo imensuráveis merece crédito nesse trabalho.

A meus pais e irmãos que tanto me ensinaram na vida e de várias formas contribuíram para que eu trilhasse o caminho que culmina nesta tese.

Agradecimentos

Agradeço ao professor Eduardo Duzzioni pela orientação, pelas discussões e pelo exemplo de profissionalismo.

Agradeço ao Programa de Pós-Graduação em Física da Universidade Federal de Uberlândia, pelo curso e pelos profissionais envolvidos, técnicos e docentes altamente qualificados.

À compreensão do Instituto de Ciência, Engenharia e Tecnologia da Universidade Federal dos Vales do Jequitinhonha e Mucuri, em especial ao diretor Carlos Henrique Alexandrino, nos momentos em que precisei desempenhar minhas atividades referentes ao doutorado, meus agradecimentos.

Agradeço ao Grupo de Óptica e Informação Quântica pelo ambiente e pelas discussões com os pesquisadores docentes e os discentes. Agradeço aqui a meus colegas discentes do grupo, entre eles, Halyne, Antônio e Patrícia, pelas discussões de pesquisa e também pelas banalidades.

Para passar por um período árduo como o de um curso de doutorado, ter colegas com quem dividir o peso, as frustrações e o trabalho é de grande importância. Tive a oportunidade de conviver desde a graduação, passando pelo mestrado e até o doutorado, com dois colegas com quem pude cooperar. Foi uma honra passar esses dez anos ao lado de William e Renato.

O afeto e apoio que recebi de meus pais e de minha família foram imprescindíveis para que eu pudesse ter equilíbrio para passar por todo o processo estressante de um doutorado. Cabe aqui, além do agradecimento à minha família, o reconhecimento aos meus sogros por terem me acolhido como um membro da família, o que foi muito importante na distância da minha própria família.

Durante os anos de doutorado houve ocasiões em que parecia que tudo daria errado. Houve vários momentos em que a dúvida na capacidade de resolver os problemas tornou-se enorme. Nesses momentos eu pude contar com minha esposa, Sharita, para perceber que tudo poderia ser resolvido e que eu era capaz de enfrentar todos os problemas. Sem a parceria, e as praticamente sessões de análise, dessa pessoa especial este trabalho não teria sido concluído. Meu muito obrigado por ações de uma magnitude que são impossíveis de retribuir, mas que sempre tentarei.

Resumo

A computação quântica pode representar um avanço inestimável na solução de alguns problemas para os quais não se conhece solução eficiente ou não há tal solução afinal. Para que essa forma de computação se consolide como uma realidade vários problemas têm sido tratados pela comunidade científica como, por exemplo, a identificação de uma propriedade que seja responsável pela vantagem computacional ou, ainda, o desenvolvimento de novos algoritmos, protocolos e modelos computacionais, além do desenvolvimento técnico para produção de sistemas capazes de realizar tal computação. Considerando este cenário, os estudos apresentados nesta tese têm como temas principais as correlações quânticas — uma propriedade que conjectura-se ser uma fonte de ganho computacional para a computação quântica — e o modelo computacional denominado Deterministic Quantum Computation with One Quantum Bit (DQC1). Estuda-se, através de métodos numéricos, as correlações quânticas geradas entre dois pontos quânticos não interagentes, inseridos em uma nanocavidade óptica, na presença de canais de decoerência e observa-se que estes canais, apesar de reduzirem o potencial de geração de correlações quânticas em uma maneira geral, têm um pequeno papel construtivo. Além disso, a realização experimental de uma testemunha de classicalidade neste sistema é proposta. Avalia-se a presença destas correlações no passo-a-passo do algoritmo de Deutsch-Jozsa pelo modelo DQC1, notando-se que elas podem ser geradas e consumidas neste processo. Apresenta-se uma forma de se realizar computação pelo modelo DQC1 em um sistema óptico, onde o estado de um conjunto de qbits é codificado nos graus de liberdade transversais e a polarização é tomada como o qbit controle. Seguindo este esquema são desenvolvidas formas de realizar os algoritmos de Deutsch-Jozsa, de fatoração e de estimação de decaimento da fidelidade média, tendo sido o primeiro efetivamente realizado experimentalmente, assim como o cálculo do traço de uma matriz unitária.

Palavras-chave: Computação quântica. Informação quântica. Correlações quânticas.

Abstract

Quantum computation may represent a progress of great value for the solution of some problems whose efficient solution is not known or that cannot be efficiently solved at all. In order to continuously develop this unconventional form of computing a number of problems are being assessed by the science community such as the identification of a property that may be the source of a computational gain, or the development of new quantum algorithms, protocols and computational models, besides the technical development towards the production of systems capable of implement such computations. Considering that, the studies presented in this thesis have as main subjects quantum correlations — a property that is pointed out as a likely source of computational gain for quantum computation — and the Deterministic Quantum Computation with One Quantum Bit (DQC1) model. The quantum correlations generated between two non-interacting quantum dots inside an optical nanocavity in the presence of decoherence channels are studied by means of numerical calculations, and the results show that these channels, although in general reduce the potential for quantum correlations generation, have a minor constructive role. Furthermore, the experimental implementation of a classicality witness in this system is proposed. The presence of these correlations in the realization of the Deutsch-Jozsa algorithm by the DQC1 model is assessed, noting that it may be generated and consumed in the process. A way to implement quantum computation by the DQC1 model on a optical system, where the state of a set of qbits is encoded on the transverse degrees of freedom of light and the polarization is taken as the control qbit is also proposed. Following this scheme some ways to implement the Deutsch-Jozsa, factoring and average fidelity decay estimation algorithms are presented, with the former being effectively experimentally tested along with the evaluation of the normalized trace of a unitary matrix.

Keywords: Quantum computing. Quantum Information. Quantum correlations.

Lista de Figuras

Sumário

Capítulo 1

Introdução e fundamentos teóricos

A acessibilidade a computadores em vários meios da sociedade (indústrias, lares, universidades, etc...) representou avanços em vários aspectos. De fato, os editores disponíveis em um computador pessoal permitem que a escrita desta tese seja feita de forma muito mais conveniente do que seria há poucos anos. A aplicação da computação moderna possibilita a automatização de processos industriais, elevando a eficiência e produtividade de tais entidades. O tratamento de dados e a solução de problemas científicos também se beneficiam intensamente do uso de computadores. Porém, mesmo que em evolução constante, a computação convencional tem seus limites. É possível estender o conjunto de soluções eficientes possíveis se o processamento de informação envolver fenômenos de caráter exclusivamente quântico. Essa ideia tem sido trabalhada por algumas décadas e vários problemas que não têm solução eficiente pela computação convencional, ou não se conhece uma, mas que podem ser solucionados de maneira eficiente em computadores quânticos, já são conhecidos [1–6]. Apesar desta evolução, a razão para que a computação quântica seja mais eficiente do que a computação convencional em alguns problemas ainda é tópico de discussão. Para alguns casos, em que os estados utilizados são puros, uma propriedade denominada emaranhamento parece ser essencial para se observar uma vantagem computacional [7]. Em outras situações, onde a computação é realizada com estados mistos, o emaranhamento não parece ser essencial para se observar qualquer ganho computacional, mas sim correlações quânticas de uma forma geral, que podem ser quantificadas, entre outras medidas, pela discórdia quântica [8–10].

Investigações sobre o papel das correlações quânticas para a vantagem computacional de sistemas quânticos são valiosas para o desenvolvimento do campo de computação quântica e seus desdobramentos científicos e tecnológicos. Incluem-se nestas investigações a avaliação do potencial de sistemas físicos em gerar correlações quânticas, a fim de que possam realizar computação quântica, e também a análise da presença de correlações quânticas nas realizações de protocolos de computação e informação para que se permita buscar um padrão de geração e consumo de correlações ideal que auxilie na obtenção de um

ganho computacional. Nesta tese iremos estudar a geração dessas correlações quânticas em alguns cenários, a saber, na evolução de um sistema composto por dois pontos quânticos inseridos em uma nanocavidade óptica e na realização do algoritmo de Deutsch-Jozsa em um modelo computacional de estados mistos denominado DQC1. Proporemos, ainda, a implementação de alguns algoritmos utilizando este modelo computacional em sistemas ópticos. Tais sistemas permitem a utilização de procedimentos sobre os quais se tem muito conhecimento e controle além de serem sistemas que se comportam de maneira previsível, com um baixo nível de interação com elementos que não pertencem ao processo da computação. Na sequência deste capítulo apresentaremos algumas definições que serão úteis ao desenvolvimento deste trabalho.

1.1 Computação clássica e quântica

Operações, sejam elas do cotidiano (como trocar uma lâmpada), de marketing (por exemplo, fazer o maior número possível de consumidores conhecer um determinado produto), matemáticas (como a adição ou a multiplicação), operações das mais variadas naturezas podem ser descritas, ou melhor, planejadas, como uma sequência de ações. Recorrendo a uma definição informal, estas sequências de ações constituem um algoritmo que partindo de um estado inicial resulta em uma solução esperada. Retomando os exemplos iniciais, partindo de um cenário em que uma lâmpada não ilumina suficientemente um ambiente pode-se realizar uma sequência de ações para que se tenha um ambiente devidamente iluminado (adquirir uma nova lâmpada, remover a lâmpada defeituosa, inserir a nova, etc...). Ou ainda, dados dois números, um conjunto específico de ações é capaz de determinar a soma destes valores e um outro conjunto distinto de ações irá gerar um novo número que descreve o resultado da multiplicação dos números iniciais.

A capacidade de expressar um problema de uma forma lógica, pelo emprego de alguma linguagem (conjunto de símbolos), e de se buscar soluções pela utilização de um algoritmo constituído por um conjunto de operações lógicas que altere elementos dessa linguagem está no cerne da computação moderna. Essas ideias foram capturadas por Alan Turing em sua máquina de Turing, descrevendo matematicamente o conceito de algoritmo [11]. Esta máquina é constituída por elementos básicos de um computador e é capaz de reproduzir qualquer algoritmo computacional. Apesar de seu poderio e relevância, teórica e histórica, a máquina de Turing não é comumente utilizada para se descrever a computação convencional. Isto ocorre pelo fato de que outro modelo, denominado modelo circuital, se aproxima mais do processo computacional real. Neste modelo a informação é conduzida por trilhos e é manipulada por portas, que realizam operações lógicas sobre os valores. A unidade básica de informação para a computação clássica é o bit, usualmente definido como uma variável binária, que pode assumir os valores 0 e 1, de forma não

concomitante. Esta informação é codificada no estado de algum sistema físico como, por exemplo, a voltagem em um circuito elétrico: dois valores distintos de voltagem são permitidos, atribuindo-se a um desses estados o valor 0 e a outro o valor 1. Deste modo, a solução de um problema pode ser encontrada iniciando-se um conjunto de portadores de informação em um dado estado, aplicando-se uma sequência de operações lógicas sobre estes elementos, definidas pelo algoritmo de solução do problema, e avaliando-se o estado final do sistema. No modelo circuital de computação clássica, cada trilho simboliza a evolução temporal da informação em cada portador e as portas reproduzem as operações lógicas a serem aplicadas.

A consolidação da teoria computacional e o avanço científico-tecnológico relacionado à produção de elementos semicondutores miniaturizados possibilitou a utilização de computadores em vários ambientes (industriais, domésticos, acadêmicos, etc...). Este fato, por sua vez, resultou em uma revolução, considerando-se acesso a informação, comunicação e desenvolvimento científico e tecnológico, entre outros. O poder de cálculo dos computadores foi gradualmente elevado à medida que quantidades maiores de portadores de informação puderam ser integrados através de arquiteturas cada vez mais avançadas. Este alta capacidade de processar dados permitiu que problemas cada vez mais complexos fossem tratados pelo uso de computadores. Porém, os avanços na capacidade de processamento exigem uma quantidade cada vez maior de recursos físicos, e a integração destes elementos em um único dispositivo requer miniaturização. Em algum ponto do desenvolvimento dos computadores é possível que essa miniaturização atinja um limite em que fenômenos quânticos possam se tornar extremamente relevantes. É possível, ainda, que o modelo computacional convencional tenha um limite, além do qual não é eficiente em solucionar alguns problemas específicos (por exemplo, a simulação da dinâmica de sistemas quânticos).

O poder de processamento de informação do modelo convencional de computação pode ser elevado modificando-se a natureza dos portadores de informação. Consideremos que o portador de informação apresente efeitos quânticos evidentes (e denominemos este elemento qbit). Este qbit então apresentará uma característica exclusivamente quântica: a possibilidade de ser descrito por um estado de superposição. De forma sucinta isto indica que o qbit pode ser descrito pelo estado 0, pelo estado 1 ou por uma superposição destes estados, ou seja, pode estar simultaneamente nos dois estados. O estado de superposição representa uma grande vantagem, visto que possibilita um certo paralelismo computacional. Pode-se observar isso tomando por exemplo o problema de calcular o valor $f(0) + f(1)$. No modelo computacional convencional seria necessário preparar um bit no estado 0 e aplicar um algoritmo para calcular $f(0)$, então preparar o bit no estado 1 e aplicar o algoritmo novamente para calcular $f(1)$ e, por fim, calcular-se a soma $f(0) + f(1)$. Utilizando um qbit, pode-se preparar o estado inicial em uma superposição dos estados 0 e 1, em seguida aplicar o algoritmo, calculando simultaneamente os valores

$f(0)$ e $f(1)$, e preparar o estado para que a leitura do estado final do sistema forneça o valor de $f(0) + f(1)$. A superposição em um conjunto de dois ou mais qbits possibilita a geração de correlações entre estes elementos com natureza exclusivamente quântica, como definiremos em alguns momentos, ao que se atribui uma importante contribuição à vantagem observada na solução de alguns problemas pelo uso de sistemas quânticos.

Dentre os algoritmos desenvolvidos com o intuito de aproveitar as especificidades de sistemas quânticos citamos três de maior conhecimento geral: os algoritmos de Deutsch-Jozsa, de Grover e de Shor [2–4]. O primeiro identifica a classe de uma função entre duas possibilidades: constante ou balanceada. Como discutiremos no capítulo 4, considerando-se o pior caso possível na realização clássica, a versão determinística com estados puros deste algoritmo apresenta um ganho computacional significativo sobre a solução clássica. Neste cenário, se o sistema inicial é composto por n bits (ou qbits), a solução clássica pode levar até $2^{n-1}+1$ repetições para se ter completa certeza da resposta, enquanto o algoritmo quântico fornece a resposta em apenas uma realização. O algoritmo de Grover permite encontrar um dado elemento em um conjunto de dados distribuídos aleatoriamente de forma mais eficiente do que a solução clássica, apresentando um ganho quadrático sobre o modelo convencional. O algoritmo de Shor será discutido no capítulo 3 e trata de encontrar fatores primos de um dado número, apresentando também um ganho suprapolinomial sobre a solução clássica. Como veremos, este algoritmo está diretamente relacionado à segurança de informação, visto que a dificuldade em se fatorar números grandes está na base da proteção oferecida pelo principal sistema criptográfico utilizado de maneira dominante atualmente.

Para que esses algoritmos sejam realizados experimentalmente é necessário encontrar sistemas apropriados em que qbits possam ser adequadamente definidos. Na prática, estas unidades de informação quântica podem ser definidas nos mais variados sistemas físicos, os quais têm maior ou menor potencial para realização de computação quântica. Em cada sistema codifica-se a informação envolvida na computação em propriedades apropriadas que podem ser manipuladas de maneira bem definida. Alguns dos sistemas em maior evidência são:

- íons, altamente resfriados, confinados em armadilhas eletromagnéticas: o qbit é definido nos estados internos e no grau de liberdade de movimento dos íons e as operações lógicas podem ser realizadas por aplicação de lasers e pela interação coulombiana direta entre os íons. O conjunto de operações necessárias para realização de computação já foi desenvolvido e alguns algoritmos já foram realizados [12–15];

- ressonância magnética nuclear (RMN): os estados do qbit são codificados nos spins nucleares dos átomos em uma molécula. A interação entre qbits possibilitada pela proximidade na geometria molecular é utilizada para realizar operações lógicas entre

dois qbits conjuntamente com a aplicação de pulsos eletromagnéticos que também são utilizados para realização de operações de um qbit. A computação é realizada em um ensemble de moléculas (contendo um número de moléculas da ordem de 10^8), mais comumente no estado líquido. A medida se dá pela leitura do momento de dipolo magnético do ensemble, ou seja, é uma média da computação realizada simultaneamente em um grande quantidade de computadores. Por ser um esquema amplamente utilizado, por exemplo, em aplicações médicas, o domínio técnico é bastante desenvolvido. Com isto, há profusão de realização de operações lógicas e algoritmos [16–20].

- sistemas ópticos: fótons apresentam alguns graus de liberdade em que se pode codificar um qbit, sendo polarização e modo espacial mais frequentemente adotados. A codificação de qbits em fótons é vantajosa pelo fato de que a interação deste ente com elementos indesejáveis que podem afetar negativamente a computação é fraquíssima, o que resulta em uma alta fidelidade do estado do sistema. Além disso, devido à sua natureza, fótons permitem a transferência de qbits por longas distâncias. Por outro lado, encontra-se dificuldades para realizar operações entre dois qbits pela interação fraca entre dois fótons, apesar de que pesquisadores encontrem formas de realizar tais operações mediante utilização de fótons adicionais ou elementos ópticos não-lineares. Elementos não-lineares são também utilizados para geração de pares de fótons emaranhados que têm grande valor para realização de protocolos de computação e comunicação quântica [21–28].

- supercondutores: dispositivos produzidos por técnicas extremamente desenvolvidas, formados por elementos supercondutores, tendo como elemento principal as junções Josephson. A depender do dispositivo os qbits podem ser codificados no número de cargas armazenadas, no sentido do fluxo magnético ou ainda em uma fase relativa específica [29–31].

- semicondutores: Elementos nanométricos, denominados pontos quânticos, apresentam estados quantizados, seja relacionados a portadores de cargas elétricas ou ao spin desses portadores, nos quais se pode definir qbits. Esse sistema possui a vantagem de que grande parte da indústria de computadores se baseia em materiais semicondutores. Outro fator importante é a capacidade de construir dispositivos em que pontos quânticos interagem fortemente com um modo eletromagnético quantizado, o que permite a interação entre um qbit definido no ponto quântico e um qbit definido em um fóton. Esta interação é valiosa para realização de protocolos de comunicação quântica e tem potencial para gerar interações entre dois pontos quânticos mediadas pelo campo eletromagnético [32–35].

Uma característica valiosa para um sistema no qual se deseja implementar computação quântica é a capacidade de que diferentes elementos básicos de computação quântica definidos nesse sistema possam se comunicar, apresentando alguma forma de ligação. A comunicação entre diferentes dispositivos levaria a formação de uma rede, permitindo que a informação seja tratada em algum local e então dispensada a alguma outra unidade para ser manipulada de acordo com a necessidade específica, permitindo a solução de problemas mais elaborados por protocolos de computação mais sofisticados. Este requerimento está diretamente relacionado aos critérios de DiVincenzo, particularmente à necessidade de transmitir "qbits móveis"entre posições específicas [36]. A forma mais natural de se enviar informação entre dois pontos diferentes por meio de qbits se dá através do uso de fótons. Para que a informação contida nestes entes seja entregue a um dispositivo quântico de processamento, constituído de qbits fixos como átomos ou pontos quânticos, por exemplo, é necessário que ocorra uma interação radiação-matéria de alta qualidade. A interação entre qbits móveis e diferentes qbits fixos, ao permitir a comunicação entre diferentes dispositivos em uma rede, possibilita a geração de correlações quânticas entre estes últimos elementos, um recurso que pode ser importante para a realização de computação quântica.

Dentre os sistemas com potencial para formar um futuro computador quântico, os que mais se destacam na capacidade de realizar interação entre qbits fixos e móveis são átomos e íons aprisionados e pontos quânticos inseridos em nanocavidades definidas em nanocristais fotônicos [37–42]. Em parte deste trabalho estamos interessados no último caso, tratando os pontos quânticos como sistemas de dois níveis efetivos. Neste sistema os pontos quânticos estão acoplados a modos eletromagnéticos da cavidade e esta interação permite a troca de excitações entre estes elementos. Já se tem domínio de métodos de fabricação deste sistema que permitem que o acoplamento entre os pontos quânticos e o modo da cavidade seja intenso em relação aos parâmetros de decoerência [43, 44]. Além disso, a informação contida nos qbits definidos nos pontos quânticos pode ser manipulada através de pulsos laser, o que permite a realização de operações rápidas [45]. Outra demonstração do refinado controle experimental sobre este sistema se dá pela possibilidade de manipular a dessintonia entre os níveis energéticos dos pontos quânticos e o modo da cavidade através do ajuste de parâmetros externos, como a aplicação de um campo elétrico sobre o dispositivo [34]. O referido domínio sobre a fabricação deste sistema tem culminado na produção de sistemas mais complexos apresentando integração entre diferentes dispositivos [35, 46]. Com o potencial de desenvolvimento de redes de dispositivos integrados cada vez mais complexas, contendo um maior número de dispositivos, possibilitadas pelo contínuo desenvolvimento técnico-científico, o sistema em questão é de inegável interesse para o problema de realização de computação e informação quântica.

Com a possibilidade de integrar diferentes elementos, a geração de correlações quânticas entre qbits no sistema é altamente provável. Com indicativos de que a discórdia

quântica pode ser diretamente relacionada à performance da realização computacional [47, 48], é importante estudar como essas correlações são geradas no sistema de interesse. Esta análise é apresentada no próximo capítulo.

Os variados elementos físicos propícios para a codificação de qbits apresentam, naturalmente, características físicas diversas entre si que podem favorecer diferentes formas de se realizar computação. De fato, é possível adotar diferentes modelos computacionais para realizar computação quântica [49]:

- circuital: é o modelo mais adotado. Nele um conjunto de qbits é inicializado em um estado puro específico. O estado do sistema é alterado de maneira determinística pela realização de uma sequência bem definida de operações lógicas. Desta forma cada operação tem como dados de entrada a informação contida nos estados dos qbits e modifica essa informação que virá a ser novamente modificada pela operação seguinte e assim por diante. Assim como a preparação do estado inicial e as operações lógicas, medidas na base computacional são realizadas de maneira controlada sobre os qbits.

- computação baseada em medidas: é uma família de modelos que têm como operações principais as medidas. Enquadram-se a computação via teleportes, computação de sentido único e computação cega. Estes modelos exigem a inicialização do sistema em um estado altamente emaranhado ou um conjunto de cópias de um estado emaranhado. Os algoritmos são efetivamente traduzidos na sequência e na base das medidas. Uma grande vantagem nestes casos é o fato de não ser necessária a realização de operações entre dois ou mais qbits [22, 27, 50–52].

- computação adiabática: neste modelo a computação não é realizada através de aplicação de operações lógicas mas pela evolução contínua do estado do sistema. O estado inicial dos qbits é descrito pelo estado fundamental de um hamiltoniano inicial enquanto a solução da computação é codificada no estado fundamental de um hamiltoniano final. Através da variação temporal do hamiltoniano , sendo essa variação suficientemente lenta, a resposta da computação é obtida através da caracterização do estado dos qbits [53, 54].

- computação quântica determinística com um qbit (DQC1, do original em inglês): um conjunto de n qbits é inicializado no estado maximamente misto junto a um qbit iniciado em um estado semi-puro. A computação é realizada pela aplicação de uma operação unitária controlada pelo estado do qbit semi-puro sobre o conjunto de qbits mistos. O resultado é obtido através do valor esperado de uma observável do qbit semi-puro [55]. Este modelo será apresentado em mais detalhe a seguir e será abordado novamente nos capítulos 3 e 4.

O modelo computacional DQC1

Os algoritmos citados anteriormente neste capítulo foram inicialmente desenvolvidos com o intuito de se utilizar o modelo circuital de computação quântica. Porém, é possível realizar computação com estados mistos e se obter alguma vantagem computacional sobre o modelo clássico, por exemplo, através do modelo DQC1. Como descrito logo antes, este modelo computacional exige a inicialização de um conjunto de qbits no estado maximamente misto e apenas um qbit com algum nível de pureza. Diferentemente da computação quântica circuital, em que a resposta do problema é obtida através de uma medida sobre um subconjunto de qbits, neste modelo a resposta é representada pelo valor esperado de um dado operador, por exemplo $\langle\sigma_z\rangle$. Alguns algoritmos já foram desenvolvidos para solucionar problemas através deste modelo [5, 6, 56–59]. No campo experimental as realizações ainda são escassas, tendo mais sucesso em sistemas de ressonância magnética nuclear (RMN) e algum êxito em óptica linear [60–65].

Dentre os algoritmos desenvolvidos, destaca-se o algoritmo de fatoração, baseado no algoritmo de fatoração de Shor e que, como descrito anteriormente, tem importantes e diretas implicações para a segurança de informação [56]. O algoritmo para a estimação de decaimento de fidelidade média também é relevante. Também desenvolvido para o modelo DQC1, este algoritmo é capaz de estimar o decaimento da fidelidade entre dois estados finais resultantes de um estado inicial idêntico mas cuja evolução é regida por operadores diferentes, porém extremamente similares [5]. Através da solução deste algoritmo é possível caracterizar a dinâmica de um sistema como caótica ou regular. Voltaremos a discutir estes dois algoritmos no capítulo 3. A Fig. 1.1 apresenta o circuito para o cálculo do traço normalizado de uma matriz unitária U_n de dimensão 2^n pelo modelo DQC1, outro problema em que se obtém uma solução mais eficiente do que no caso clássico [66]. O qbit controle é inicializado no estado $(I_0 + \alpha Z_0)/2$, onde $0 < \alpha < 1$ é a sua polarização, enquanto um conjunto de n qbits é inicializado no estado maximamente misto $I^{\otimes n}/2^n$. O estado inicial do sistema, portanto, é $\rho_I = 2^{-(n+1)}(I_0 + \alpha Z_0) \otimes I^{\otimes n}$, onde o índice 0 se refere ao qbit semi-puro (qbit controle), I é a matriz identidade, Z é a matriz de Pauli σ_Z, e $I^{\otimes n}$ é a matriz identidade do conjunto de n qbits. Após a aplicação da operação U sobre o conjunto de qbits mistos, condicionada ao estado do qbit controle, o estado do sistema é

$$\rho = \frac{1}{2^{n+1}} \left(I_0 \otimes I_n + |1\rangle\langle 0| \otimes U_n + |0\rangle\langle 1| \otimes U_n^\dagger \right), \tag{1.1}$$

Desta forma, nota-se que um conjunto de medidas sobre o qbit controle deve estar de acordo com $\langle\sigma_x\rangle = \mathrm{Re}[\mathrm{tr}(U_n)]/2^n$ e $\langle\sigma_y\rangle = \mathrm{Im}[\mathrm{tr}(U_n)]/2^n$. Este cálculo representa uma grande vantagem computacional sobre a solução clássica. É possível compreender a origem desta vantagem considerando-se a decomposição da matriz unitária U_n em um conjunto de operações universais. Para calcular o traço por métodos clássicos é necessário somar

a amplitude de um grande número de "caminhos"disponibilizados pela decomposição da matriz unitária que levem cada estado inicial em si mesmo multiplicado por uma fase. O número total de amplitudes a serem somadas tem uma relação exponencial com a dimensão de U_n, o que torna esse cálculo ineficiente [66].

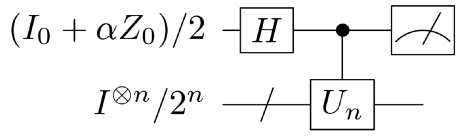

Figura 1.1: Circuito DQC1 utilizado para avaliar o traço normalizado de uma matriz unitária U_n. A operação de Hadamard H gera uma superposição no qbit controle e em seguida a operação U_n é aplicada sobre o registro de qbits mistos condicionada ao estado do qbit controle. Por fim, a medida no qbit controle permite o conhecimento do traço normalizado de U_n.

É razoável especular que a superposição seja o fator que fornece vantagem computacional ao se utilizar qbits no lugar dos bits clássicos, visto que um grande número de qbits preparados cada um em um estado de superposição permite o cálculo por um número consideravelmente maior de vias simultâneas. De fato, um conjunto de n qbits pode ser preparado em uma superposição de 2^n estados, o que permite a realização de cálculos em paralelo de forma intensa para um grande número de qbits. Deixe-se claro que este fator só representa uma vantagem se a informação resultante dessa computação paralela, que corresponde à solução correta de um problema específico, puder ser obtida de uma maneira eficiente. Contudo, um fenômeno específico, possibilitado pela superposição, tem um papel mais ligado a esse possível ganho computacional. Recentemente, pesquisadores têm concentrado esforços para tratar da questão de identificar o recurso físico responsável pela vantagem da computação quântica sobre a convencional. Para computação com estados puros, emaranhamento é tido como um recurso necessário para se obter uma vantagem sobre a computação clássica [7, 67]. Todavia, este recurso não se mostra essencial para computação quântica com estados mistos. Já se mostrou que a quantidade de emaranhamento presente em um sistema ao final da avaliação do traço de uma matriz unitária pelo modelo DQC1 não pode explicar o ganho computacional resultante [8, 68]. Porém, existem algumas correlações de natureza quântica presentes no sistema ao final da computação, que englobam também o emaranhamento mas são mais gerais do que este, e que podem ser quantificadas, entre outras formas, pela discórdia quântica [9, 10]. Deste modo, é possível que estas correlações quânticas sejam a fonte da vantagem da computação quântica sobre a computação convencional.

1.2 Correlações quânticas

Apresentamos agora algumas definições de classes de estados e de medidas que serão úteis nos próximos capítulos desta tese. Comecemos com a definição de algumas classes

de estados de sistemas formados por dois subsistemas, ou seja, estados estados bipartidos. Estes subsistemas podem conter quaisquer quantidades de qbits e, inclusive, podem ter tamanhos diferentes. Um sistema está em um estado emaranhado se não pode ser descrito como um produto de estados de duas partições (ou uma soma desses produtos). Isto é, uma sistema bipartido, com subsistemas A e B, está emaranhado se seu estado não pode ser escrito na forma $\rho = \sum_i p_i \rho_i^A \otimes \rho_i^B$. Estados com este formato são denominados estados separáveis, sendo p_i a probabilidade de se observar o sistema no estado conjunto rotulado por i. Estes estados podem ser dispostos em três categorias: *a)* estados clássico-clássico (CC) com a forma $\rho = \sum_i p_i \left|i_A\right\rangle \left\langle i_A\right| \otimes \left|i_B\right\rangle \left\langle i_B\right|$ onde $\left\{\left|i_{A(B)}\right\rangle\right\}$ é um conjunto ortonormal, *b)* estados clássico-quântico (CQ) sob a forma $\rho = \sum_i p_i \left|i_A\right\rangle \left\langle i_A\right| \otimes \sigma_i^B$ onde $\left\{\sigma_i^B\right\}$ é um conjunto de operadores densidade em que não se pode atribuir uma única base $\{|i_B\rangle\}$ para descrever todos estes elementos, e *c)* estados quântico-quântico (QQ) com a forma $\rho = \sum_i p_i \sigma_i^A \otimes \sigma_i^B$ em que $\left\{\sigma_i^{A(B)}\right\}$, de maneira idêntica ao caso anterior, é um conjunto de operadores densidade em que não se pode atribuir uma única base $\left\{\left|i_{A(B)}\right\rangle\right\}$ para descrever todos estes elementos [69].

Emaranhamento bipartido em estados não-separáveis pode ser quantificado por uma vasta quantidade de medidas, entre as quais apresentamos aqui a negatividade [70]. Esta medida apresenta a vantagem de ser útil não apenas para estados puros, mas também para estados mistos. Além disso, a negatividade pode ser calculada para um estado misto bipartido geral, uma característica que não é encontrada em outras medidas de emaranhamento. A negatividade é definida pela seguinte expressão

$$\mathcal{N}(\rho) = \frac{\left\|\rho^{TA}\right\|_1 - 1}{2} \tag{1.2}$$

onde $\|O\|_1 = \mathrm{tr}\sqrt{O^\dagger O}$ é o traço da norma do operador O e a transposição parcial no subsistema A é denotada por ρ^{TA} (esta definição também pode ser realizada utilizando-se a transposição parcial sobre o subsistema B). A negatividade pode assumir valores entre 0 e $(d-1)/2$, onde d é o mínimo entre as dimensões das partições A e B.

Sistemas emaranhados possuem correlações que não podem ser criadas em sistemas clássicos. As partições de tais sistemas podem se correlacionar em maneiras que não podem ser reproduzidas por meios clássicos, isto é, as partições destes sistemas estão quanticamente correlacionadas. Além disso, mesmo estados separáveis podem apresentar correlações quânticas. De fato, apenas estados CC não podem apresentar correlações quânticas, visto que estes estados representam apenas distribuições clássicas de probabilidades. Por outro lado, estados sob a forma QQ e CQ, apesar de separáveis, podem apresentar correlações de natureza quântica, o que pode ser utilizado em favor da realização de tarefas de computação e informação quântica. Portanto, se é necessário verificar se um estado está correlacionado quanticamente, basta verificar se o estado pode ser escrito na forma CC, se a resposta é negativa então é detectada a presença

de correlações quânticas.

Correlações quânticas podem ser quantificadas, entre outras medidas, pela discórdia quântica [9, 10]. Esta quantidade é fruto de uma diferença entre duas definições de informação mútua $I(A:B) = S(A) + S(B) - S(A,B)$ e $J(A:B) = S(A) - S(A|B)$, onde $S(X) = -\mathrm{tr}X\log_2 X$ é a entropia de von Neumann de um operador densidade X. Na teoria de informação clássica estas duas quantidades são idênticas, porém, ao se considerar sistemas quânticos, $S(A|B)$, a entropia condicional do subsistema A dado um conhecimento prévio de B, envolve um processo de medidas que afeta o estado do sistema como um todo. Dado um conjunto completo de medidas POVM $\left\{\pi_j^B\right\}$ sobre o sistema B, o total de correlações clássicas de um dado sistema bipartido é dado por $C(A:B) = \max_{\left\{\pi_j^B\right\}} J(A:B)$. Uma vez que $I(A:B)$ quantifica o total de correlações no sistema, tanto clássicas como quânticas, a diferença entre estas duas quantidades revela o total de correlações de natureza quântica presentes no sistema, o que se define por discórdia quântica, dada por

$$D(A,B) = I(A:B) - \max_{\left\{\pi_j^B\right\}} J(A:B). \tag{1.3}$$

Este é um quantificador assimétrico, de maneira que fornece valores diferentes se a medida é realizada em uma partição ou em outra. Especialmente, se o estado é CQ, sendo A a partição clássica, a discórdia quântica será zero se a medida é realizada sobre esta partição. Por outro lado, se a medida é realizada sobre a partição B, a discórdia quântica terá um valor não-nulo.

1.3 Estrutura da tese

Como mencionado anteriormente, correlações quânticas podem ser responsáveis pela vantagem da computação quântica sobre a computação convencional. Considerando isso, é interessante investigar o potencial dos sistemas em gerar correlações quânticas entre dois qbits. Além disso, para que o problema seja abordado de uma forma mais completa é necessário que se considere os efeitos negativos causados pela interação dos qbits com o meio ambiente, isto é, é preciso observar o efeito dos canais de decoerência [71–76]. No próximo capítulo, ambientando a discussão no cenário de pontos quânticos inseridos em nanocavidades, estudaremos os efeitos dos canais de decoerência em um sistema composto por dois qbits, sem interação direta, acoplados a um modo eletromagnético, verificando os valores da discórdia quântica para diferentes parâmetros desses canais. Além disso, proporemos a realização de uma testemunha de classicalidade neste sistema, o que constitui um teste menos trabalhoso do que o cálculo da discórdia quântica. No capítulo 3 iremos estudar a geração de correlações quânticas na realização do algoritmo de Deutsch-Jozsa no modelo DQC1. Observaremos como essas correlações aparecem ao

longo da computação, após determinar uma decomposição da operação unitária U em um conjunto de operações lógicas envolvendo um e dois qbits. Em seguida, no capítulo 4, apresentamos uma forma de se realizar computações no modelo DQC1 usando um sistema óptico. Especificamente, mostraremos como os algoritmos de Deutsch-Jozsa, de fatoração e de estimação do decaimento de fidelidade média podem ser implementados nesse sistema. Além disso, apresenta-se o resultado da realização experimental do algoritmo de Deutsch-Jozsa que segue a proposta de implementação apresentada. Para finalizar, descrevemos as conclusões obtidas do trabalho aqui apresentado e o que esperamos ainda realizar.

Capítulo 2

Correlações quânticas entre dois pontos quânticos inseridos em uma nanocavidade óptica

Considerando-se que correlações quânticas podem ser um fator importante no ganho computacional que se pode observar em computação quântica é relevante que se estude o potencial de geração de correlações quânticas nos sistemas físicos em que esse tipo de computação pode ser implementado. Em particular, avaliaremos aqui, através de simulações numéricas, a presença de correlações quânticas em um sistema composto por dois pontos quânticos inseridos em uma nanocavidade óptica, com uma abordagem teórica que leva em conta variados canais de decoerência, buscando compreender para quais regiões de valores dos parâmetros físicos estas correlações quânticas são maximizadas. A busca pela maximização das correlações quânticas entre os qbits é motivada pelo fato de que, em alguns protocolos de computação e informação quântica, a discórdia quântica pode ser diretamente relacionada à performance da realização computacional [47, 48].

Apresentaremos adiante uma definição do sistema físico de interesse, ou seja, pontos quânticos semicondutores presentes no interior de cavidades em cristais fotônicos, indicando os termos que regem a evolução temporal do sistema, especificando como se dá a interação entre os subsistemas e os termos relacionados aos canais de decoerência. Em seguida realizaremos uma análise das correlações quânticas entre os pontos quânticos no estado assintótico do sistema, ou seja, para tempos muito maiores que o tempo característico relacionado ao maior parâmetro da equação mestra. Avaliaremos, também,

o efeito da aplicação de bombeios clássicos sobre a dinâmica das correlações quânticas partindo de um estado inicial específico. Por fim, proporemos a realização de uma testemunha de correlações quânticas neste sistema, no intuito de verificar a presença de correlações quânticas no estado assintótico do sistema, ou seja, verificamos se, em seu estado assintótico, o sistema possui recursos computacionais imediatamente disponíveis para realização de protocolos de computação e informação quântica.

2.1 Sistema físico

Os pontos quânticos de que trataremos neste texto são formados em um processo de deposição de camadas atômicas, ao se formar uma camada de uma substância sobre a camada de uma outra substância distinta [77,78]. A diferença entre os padrões de rede dos dois planos atômicos adjacentes gera uma tensão no material. Para reduzir esta tensão o material sendo depositado na camada mais recente tende a se agrupar em pequenas ilhas de átomos em que, devido às dimensões reduzidas, a energia é quantizada, o que faz com que estas estruturas tenham propriedades semelhantes às de átomos. Estes pontos quânticos, devido ao seu processo de criação, são denominados auto-organizados. Entre outros materiais, é comum estas estruturas serem compostas por InGaAs e formadas sobre um substrato de GaAs. O posicionamento dos pontos quânticos formados desta maneira é aleatório e sua densidade superficial é de aproximadamente 10^9 elementos por cm^2. Quanto à sua forma, os pontos quânticos apresentam diâmetro de aproximadamente 20 nm e altura de aproximadamente 5 nm. As dimensões reduzidas destes elementos resulta na quantização da energia em níveis discretos bem definidos em torno de 1.2 eV. O ponto quântico pode ser excitado através de um processo de relaxação proveniente do material de sua vizinhança. Ao fornecer energia ao material através de um bombeio óptico ou elétrico, elétrons são excitados para a banda de condução deixando buracos na banda de valência, sendo este par elétron-buraco em um estado ligado denominado éxciton. Esta excitação pode então relaxar para o ponto quântico, sendo confinado em três dimensões pelo tamanho reduzido do elemento e assumindo níveis de energia bem definidos [79].

Neste estudo, consideramos o caso em que os pontos quânticos estão no interior de nanocavidades ópticas, como no exemplo da Fig. 2.1. Microcavidades semicondutoras foram desenvolvidas em variadas formas, com diferentes volumes modais e fatores de

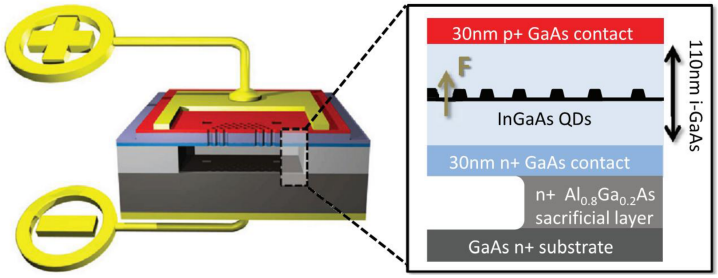

Figura 2.1: Esquema do sistema experimental (retirado da Ref. [34]). Pontos quânticos são criados no interior do dispositivo e uma cavidade eletromagnética é produzida por um padrão específico de uma rede de furos. No dispositivo apresentado é possível alterar a energia dos éxcitons através da aplicação de um campo elétrico.

qualidade, entre os quais destacamos os cristais fotônicos [80]. Essas estruturas são formadas através crescimento epitaxial com deposição de substâncias como GaAs e AlGaAs, resultando em uma forma planar [81]. Em seguida são realizados furos no material que formam uma rede periódica [82, 83]. Para finalmente produzir uma região em que o campo eletromagnético esteja confinado, a cavidade eletromagnética em si, alguns furos são removidos do padrão periódico, deslocados e ainda podem ter suas dimensões alteradas. Este defeito na rede de furos resulta no confinamento da radiação eletromagnética, sendo a geometria da rede de furos (e do defeito) ligada diretamente à definição dos modos eletromagnéticos quantizados no interior da cavidade. Estas cavidades apresentam fatores de qualidade muito elevados, tendo recentemente atingido valores da ordem de 10^6 e também pequenos volumes modais, o que permite um grande número de ciclos antes que os fótons sejam perdidos e modos eletromagnéticos bem definidos, que por sua vez possibilitam uma interação forte entre pontos quânticos inseridos na cavidade e o modo eletromagnético confinado [84, 85]. Para que, ao final da fabricação, haja pontos quânticos no interior da cavidade é necessário que, durante o crescimento do cristal, haja a deposição do material que dá origem aos pontos como InGaAs no caso apresentado na Fig. 2.1. Um fator importante na fabricação desta estrutura é que, ainda que não haja controle sobre o posicionamento dos pontos quânticos na amostra, é possível construir a cavidade de maneira a selecionar que pontos quânticos estarão na região do defeito do cristal fotônico, buscando, inclusive, maximizar o acoplamento entre o ponto e o modo da cavidade [43].

O modelo matemático para a dinâmica do sistema aqui adotado segue aquele apresentado nas referências [86, 87] em que se mostrou bem sucedido em tratar os

resultados experimentais discutidos. Consideramos o caso em que dois pontos quânticos são tratados como dois qbits cujos estados são definidos como a ausência e presença de um éxciton em uma definida energia. Este modelo é apropriado para o caso em que a intensidade de excitação sobre os pontos quânticos é baixa e a dimensão lateral dos pontos quânticos é suficientemente pequena, de modo que a interação coulombiana entre duas partículas eletricamente carregadas próximas torna a geração de dois éxcitons improvável [78]. Os pontos quânticos interagem com a cavidade através de um modo eletromagnético, desta maneira ocorre a troca de excitações entre cada ponto quântico e a cavidade. Define-se, ainda, que os dois pontos quânticos estão separados o bastante de maneira que a interação direta entre os dois éxcitons seja desprezível, podendo haver uma interação indireta entre eles através do modo da cavidade. Além disso,consideramos o caso em que a dessintonia entre o modo da cavidade e os éxcitons é pequena (na posterior análise definiremos a dessintonia com um valor nulo) e ainda que as frequências relacionadas às energias envolvidas são muito maiores dos que as outras taxas presentes no modelo. Deste modo, a interação entre os éxcitons e o modo da cavidade pode ser descrita de uma maneira simples, através da aplicação da aproximação de ondas girantes [88, 89].

A evolução temporal da matriz densidade que representa o estado do sistema, ρ, é regida por uma equação mestra escrita da seguinte forma

$$\dot{\rho} = -i[H, \rho] + \mathcal{L}(\rho), \tag{2.1}$$

onde H é o hamiltoniano do sistema e $\mathcal{L}$ é o operador relacionado aos canais de decoerência considerados (ou liouvilliano).

O hamiltoniano do sistema é composto por três elementos

$$H = H_0 + H_c + H_d. \tag{2.2}$$

Os termos em $H_0 = \omega_c a^\dagger a + \sum_{i=1,2}[(\omega_i/2)\sigma_i^z]$ representam, na sequência, a evolução livre do modo da cavidade e dos pontos quânticos, sendo ω_c e ω_i as frequências relacionadas às energias do modo da cavidade e dos éxcitons. O segundo elemento, $H_c = \sum_{i=1,2}[g(a\sigma_i^+ + a^\dagger\sigma_i^-)]$, representa a interação entre os pontos quânticos e a cavidade através de uma troca de excitações com um acoplamento g. Por fim,

$H_d = g_c(a^\dagger e^{-i\omega_c' t} + a e^{i\omega_c' t}) + \sum_{i=1,2}[g_0(\sigma_i^+ e^{-i\omega' t} + \sigma_i^- e^{i\omega' t})]$ modela a aplicação de bombeios clássicos sobre a cavidade e sobre os pontos com respectivas frequências ω_c' e ω' e acoplamentos g_c e g_0.

O liouvilliano que descreve a atuação dos canais de decoerência é

$$\mathcal{L}(\rho) = \sum_{i=1,2}\Bigg[\frac{\Gamma_0}{2}(2\sigma_i^-\rho\sigma_i^+ - \sigma_i^+\sigma_i^-\rho - \rho\sigma_i^+\sigma_i^-) + \frac{P_0}{2}(2\sigma_i^+\rho\sigma_i^- - \sigma_i^-\sigma_i^+\rho - \rho\sigma_i^-\sigma_i^+) + \gamma_2(\sigma_i^z\rho\sigma_i^z - \rho)\Bigg] + \frac{\Gamma_c}{2}(2a\rho a^\dagger - a^\dagger a\rho - \rho a^\dagger a) + \frac{P_c}{2}(2a^\dagger\rho a - aa^\dagger\rho - \rho aa^\dagger). \quad (2.3)$$

O primeiro termo do lado direito da equação representa a perda de uma excitação no ponto quântico a uma taxa Γ_0, através da recombinação do par elétron-buraco que pode se dar, entre outros motivos, por processos não-radiativos. O termo seguinte modela a excitação incoerente do ponto quântico a uma taxa P_0. Estas excitações podem ser geradas pela aplicação de um laser com energia que faça com que o elétron seja levado ao contínuo de estados na banda de condução. Pode ocorrer, então, relaxação até que se tenha a configuração do éxciton de interesse. O dephasing no ponto quântico, a uma taxa γ_2, é determinado pelo terceiro termo e está relacionado ao acoplamento com fônons da rede atômica do material. A saída de fótons da cavidade é definida pelo terceiro termo, relacionada a uma taxa Γ_c. E, finalmente, o último termo modela a injeção incoerente de fótons no modo da cavidade, com uma respectiva taxa P_c. É possível que este fenômeno esteja relacionado à interação de outros pontos quânticos presentes na amostra com o modo da cavidade [90].

2.2 Discórdia quântica e decoerência

Observaremos, agora, de que maneira os canais de decoerência afetam a geração de correlações quânticas entre os dois pontos quânticos através do cálculo da discórdia quântica no estado assintótico do sistema. Não nos ateremos ao estudo do emaranhamento assintótico aqui por termos observado, em simulações preliminares, que nesta região temporal o emaranhamento é nulo para os valores dos parâmetros considerados. Vários estudos descrevem a alteração dos valores da discórdia quântica entre dois qbits, que interagem com modos eletromagnéticos, com relação à taxa de decoerência atuante sobre sobre os modos eletromagnéticos e sobre tais qbits [71, 73–75]. Grande parte

destas avaliações é realizada levando em conta como decoerência dos qbits apenas a dissipação e somente alguns consideram a presença de bombeio incoerente e/ou dephasing. Considerando dois átomos de dois níveis inseridos em uma cavidade, Jia-sen Jin e colaboradores avaliaram o efeito de dissipação e bombeios incoerentes sobre átomos e sobre o modo da cavidade na geração de discórdia quântica entre os átomos [71]. Fixando um estado inicial sem excitações eles observaram que a discórdia quântica no estado assintótico é bastante reduzida se as taxas de decoerência sobre cavidade e pontos têm valores similares. De seus resultados pode-se inferir, ainda, que em um cenário em que a decoerência sobre a cavidade é mais intensa do que sobre os pontos, é possível obter valores de discórdia quântica mais elevados do que em outras situações. Em outro trabalho, Ying-Jie Zhang e colaboradores analisaram a dinâmica da discórdia quântica entre dois sistemas de dois níveis, que não interagem diretamente entre si, acoplados a um modo eletromagnético de uma cavidade [74]. Partindo de um estado em que os sistemas de dois níveis estavam correlacionados, e admitindo como canal de decoerência apenas a dissipação no modo da cavidade, os autores observaram que, se o estado inicial apresentar correlações entre estes sistemas e a cavidade, a discórdia quântica entre os qbits, após um intervalo de evolução grande, tende a ter valores mais elevados do que no caso em que a cavidade não está correlacionada com os outros elementos do sistema. Tomando uma descrição diferente, Ji-Bing Yuan e colaboradores, apresentaram a amplificação da discórdia quântica entre dois qbits, resultante da interação destes com um banho térmico capaz de induzir dephasing mas não dissipação [72]. A atuação de um campo clássico sobre dois qbits, interagindo com uma coleção de modos bosônicos, foi estudado por Jun-Qi Li, Jian Liu e J-Q Liang, observando-se seu efeito sobre a dinâmica das correlações quânticas entre os qbits [76]. Considerando apenas o acoplamento dos qbits com os modos bosônicos como fator decoerente eles observaram que, apesar de não modificar o valor assintótico das correlações, o acoplamento com o campo clássico gera uma dinâmica oscilatória que faz com que as correlações quânticas entre os qbits assumam valores superiores comparando-se ao caso sem aplicação do campo clássico. Note-se que os trabalhos mencionados não apresentam todos os canais de decoerência comuns em um sistema semicondutor de maneira simultânea. Como na descrição de nosso sistema físico de interesse o dephasing é um elemento importante, avaliaremos as correlações quânticas na presença de todos os canais de decoerência descritos pelo liouvilliano apresentado anteriormente. Além disso,

iremos observar o comportamento dos valores da discórdia quântica quando se aplica bombeios coerentes sobre os pontos quânticos e sobre a cavidade.

Definimos que inicialmente não há excitações nos pontos quânticos ou na cavidade e truncaremos o espaço do modo da cavidade de maneira que possam existir, no máximo, dois fótons. Para este estudo de correlações quânticas, consideramos o sistema em completa ressonância, ou seja, os pontos quânticos estão em ressonância entre si como também estão em ressonância com o modo da cavidade. Nesta análise os valores de quaisquer parâmetros serão apresentados em razão da taxa de dissipação do modo da cavidade, ou seja, um parâmetro genérico $\mathcal{P}$ será avaliado com valores $\frac{\mathcal{P}}{\Gamma_c}$, de maneira que a taxa de dissipação no modo da cavidade é $\Gamma_c = 1$. Como discutido na referência [91], num cenário em que não há decoerência sobre os qbits - ou essa decoerência é desprezível - a discórdia quântica entre estes elementos é máxima para $P_c = \Gamma_c$. Isto se relaciona ao fato de que no regime estacionário a dissipação efetiva sobre o modo da cavidade pode ser determinado por $\Gamma_c^{eff} = \Gamma_c - P_c$, o que levaria a um tempo de vida consideravelmente grande de um fóton na cavidade [92]. Desta forma, fixamos inicialmente $P_c = 1$. Apesar de esta não ser uma condição muito realista para os padrões atuais, pode-se avançar nesta direção pela produção de cavidades com refletividades mais elevadas, o que reduziria Γ_c e pelo bombeio de outros pontos quânticos, diferentes dos qbits de interesse, que emitiriam fótons no modo da cavidade elevando a taxa de bombeio incoerente P_c.

Para observar a dependência das correlações quânticas presentes no estado assintótico em relação aos parâmetros de decoerência, já tendo fixado $P_c = \Gamma_c = 1$, mantemos $P_0 = \gamma_2 = 0$ e, através de cálculos numéricos, variamos os valores de Γ_0 e g a fim de encontrar o conjunto de valores destas taxas que maximiza a discórdia quântica. Em seguida efetivamos o bombeio incoerente sobre os pontos quânticos, novamente analisando o valor das correlações para um intervalo de valores de P_0 e, por fim, adicionamos o dephasing procedendo de maneira análoga aos passos anteriores.

A figura 2.2 apresenta o comportamento das correlações quânticas entre os dois pontos quânticos (quantificadas pela discórdia quântica) em função da taxa de dissipação nos pontos quânticos e o acoplamento entre eles e o modo da cavidade, para um tempo $t \gg 1/\Gamma c$. A curva descrita por $\Gamma_0 = 0$ reproduz o resultado apresentado na referência [91], isto é, na ausência de decoerência sobre os pontos quânticos e com $P_c = \Gamma_c$ a discórdia quântica no estado assintótico assume um valor de $1/3$ para g diferente de zero. Um padrão

inesperado que se pode observar neste gráfico é o decréscimo da discórdia quântica assim que o acoplamento entre pontos quânticos e cavidade ultrapassa um valor ideal e Γ_0 é diferente de zero. Este comportamento pode ser observado de maneira mais clara na Fig. 2.3 em que são apresentados cortes da Fig. 2.2 paralelos ao eixo correspondente ao parâmetro g. Intuitivamente, valores elevados de g auxiliariam de maneira mais eficiente a troca indireta de excitações entre os dois pontos quânticos promovendo o estabelecimento de correlações quânticas entre estes qbits. Contudo, se $\Gamma_0 = 0$ não se observa um pico no valor da discórdia quântica com relação aos valores de g, portanto, este padrão inesperado se deve ao efeito da dissipação nos pontos quânticos. Uma possível explicação é que se g é muito elevado, há uma grande probabilidade de que, ao regressar ao estado fundamental, excitando o modo da cavidade, o ponto quântico recupere imediatamente esta excitação. Ao fazer isso algumas vezes, a excitação pode se perder pela dissipação no ponto quântico, reprimindo a troca de informação entre os dois qbits, impossibilitando o estabelecimento de correlações quânticas. Deve haver, então, alguma combinação ideal dos valores de g e Γ_0 para que a discórdia quântica tenha um valor máximo. Especificamente, encontramos um valor máximo de discórdia quântica de aproximadamente 0.092 para $g = 0.47$ e $\Gamma_0 = 1.3$. O valor específico de Γ_0 é um pouco elevado para padrões realistas, visto que em valores absolutos Γ_c é maior que Γ_0 [44, 87, 93]. Portanto, para se realizar um sistema com os parâmetros definidos até agora, seria satisfatório a construção de uma cavidade em que o escape de fótons seja bastante reduzido com relação aos padrões atuais. É possível, ainda, produzir pontos quânticos com diâmetros maiores, o que resulta em uma taxa de dissipação maior, elevando o valor da razão Γ_0/Γ_c. A construção de pontos quânticos com bases maiores, porém, levaria a um confinamento de partículas menos eficiente, alterando a estrutura energética destes elementos, o que possivelmente os descaracterizaria como qbits.

Utilizando os valores de Γ_0 e g definidos no parágrafo anterior, passamos à observação do comportamento da discórdia quântica com relação às taxas de bombeio incoerente e dephasing nos pontos quânticos. Para realizar esta avaliação produzimos o gráfico apresentado na figura 2.4. O caráter destrutivo do bombeio incoerente e dephasing sobre os pontos quânticos se torna evidente, visto que o comportamento da correlação quântica é monotonicamente decrescente com relação a ambos parâmetros de decoerência. Especificamente, a redução nos valores da discórdia quântica é mais acentuada com o

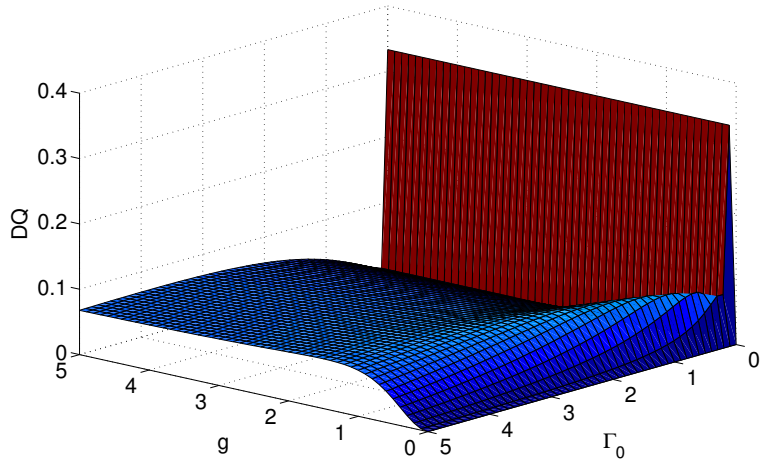

Figura 2.2: Valor da discórdia quântica entre dois pontos quânticos em função do acoplamento g e da taxa de dissipação nos pontos quânticos Γ_0 no regime assintótico ($t \gg 1/\Gamma_0$). Os parâmetros utilizados são $\Gamma_c = P_c = 1$ e $P_0 = \gamma_2 = 0$.

aumento de P_0 do que o observado com relação a γ_2. É possível que este fato seja originado pela competição entre a dissipação e o bombeio incoerente, regidos respectivamente pelas taxas Γ_0 e P_0. Se estas taxas têm valores com mesma ordem de grandeza, os canais de decoerência tendem a levar o sistema a estados ortogonais, sem construir alguma informação de fase no processo, o que resulta em um estado de mistura desprovido de correlações quânticas.

Observando a matriz densidade reduzida dos dois pontos quânticos notamos que, na presença de dissipação sobre estes elementos, o dephasing causa um decréscimo nos termos não diagonais, levando o estado para uma simples mistura estatística, fato que caracteriza a evolução para um estado puramente clássico. Além disso, o dephasing associado à dissipação nos pontos quânticos potencializa a perda de éxcitons[1]. Por seu efeito unicamente destrutivo em relação à discórdia quântica, é necessário que a taxa de dephasing seja a menor possível a fim de que as correlações entre os pontos quânticos não sejam desprezíveis (o valor utilizado nas próximas simulações será $\gamma_2 = 10^{-3}$). Este pode ser uma das maiores dificuldades na utilização de pontos quânticos auto-organizados em nanocavidades ópticas para a realização de protocolos de computação e informação quântica, visto que o dephasing, em geral, possui valores de mesma ordem de grandeza de que a dissipação na cavidade [94].

[1]Em uma análise paralela observamos que se não há dissipação nos pontos quânticos, mas apenas o bombeio incoerente, o dephasing potencializa a criação de éxcitons, elevando a população dos estados excitados

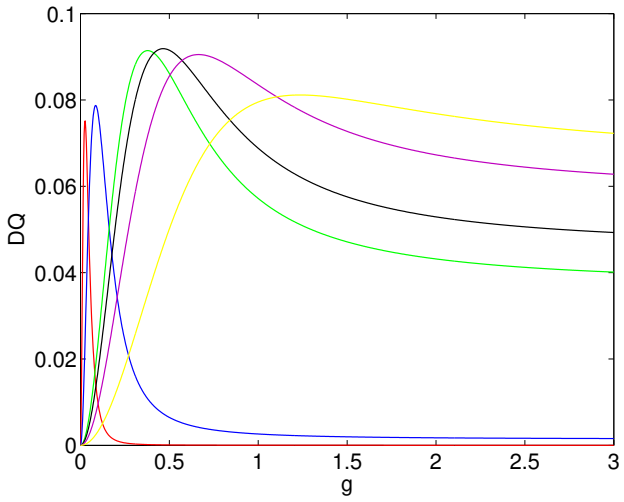

Figura 2.3: Curvas extraídas do gráfico da Fig. 2.2. Os valores de Γ_0 para cada curva são: 0,01 (vermelho), 0,1 (azul), 1 (verde), 1,3 (preto), 2 (rosa) e 4 (amarelo). Os parâmetros utilizados são $\Gamma_c = P_c = 1$ e $P_0 = \gamma_2 = 0$.

Por sua vez, a ação do bombeio incoerente sobre os pontos quânticos, concomitantemente com a dissipação, tende a levar o sistema ao estado maximamente misto, reduzindo drasticamente os termos não-diagonais da matriz densidade e distribuindo, de forma homogênea, a população dos estados da base. Para melhor observar a relação entre estes dois canais de decoerência, quanto ao efeito sobre o valor da discórdia quântica no regime assintótico, geramos o gráfico apresentado na figura 2.5. Um aspecto importante deste gráfico é a similaridade entre os planos $\Gamma_0 = 0$ e $P_0 = 0$. Na origem do gráfico a discórdia quântica é nula, isto ocorre porque definimos $\gamma_2 = 10^{-3}$, de modo que neste ponto o estado assintótico é maximamente misto. Porém, à medida que o valor de Γ_0 é elevado ocorre uma transferência de população para o estado fundamental e, ao mesmo tempo, alguns termos não diagonais assumem valores não-nulos, permitindo que o valor da discórdia quântica seja não-nulo. Um comportamento análogo é observado para a atuação do bombeio incoerente, com a diferença de que a população é transferida para os estados excitados dos pontos quânticos. Valores nulos de Γ_0 e P_0 não são realistas, portanto, é importante observar a área central do gráfico. Nesta região, os valores da discórdia quântica são muito pequenos com relação aos máximos observados no gráfico. Isto se deve ao fato de que cada um dos canais de decoerência tende a levar o sistema a um estado diferente, sendo eles ortogonais entre si (enquanto a dissipação tende a levar os pontos quânticos ao estado fundamental o bombeio incoerente força o sistema para o estado excitado). Logo, há uma competição entre as dinâmicas regidas por estes

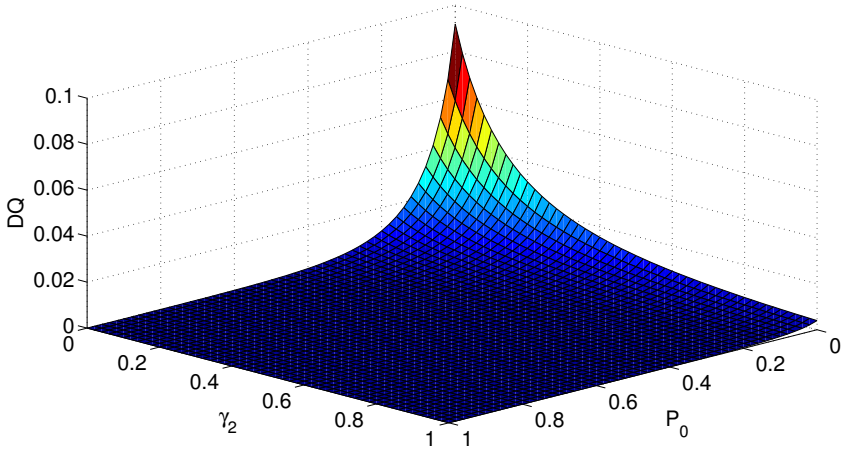

Figura 2.4: Comportamento do valor da discórdia quântica entre dois pontos quânticos em função das taxas de bombeio incoerente P_0 e dephasing γ_2. Os parâmetros utilizados para a geração do gráfico são $\Gamma_c = P_c = 1$, $g = 0.47$ e $\Gamma_0 = 1.3$.

dois termos que tende a levar o sistema a um estado maximamente misto, significando um valor nulo de discórdia quântica. Portanto, para que se tenha correlações quânticas em quantidade não desprezível neste sistema, é necessário que as taxas de dissipação e bombeio incoerente não apresentem a mesma ordem de grandeza. Por este motivo o valor definido para as próximas simulações será $P_0 = 10^{-3}$. Para atingir este valor, pode-se trabalhar com temperaturas reduzidas, a fim de inibir a troca de excitações com fônons, e também remover qualquer bombeio clássico que alimente a população excitônica (pela relaxação de estados mais energéticos produzidos por tal bombeio).

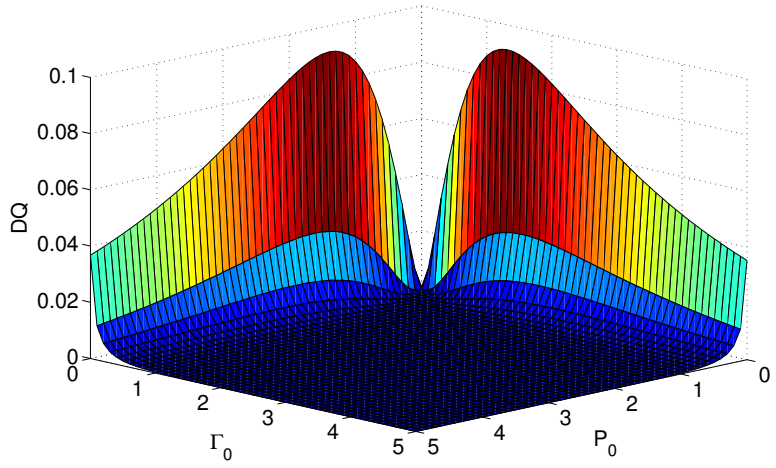

Figura 2.5: Curva de discórdia quântica em função das taxas de dissipação Γ_0 e bombeio incoerente P_0. Os parâmetros utilizados são $\Gamma_c = P_c = 1$, $g = 0.47$ e $\gamma_2 = 0.001$.

Tendo analisado o efeito dos canais de decoerência sobre a discórdia quântica gerada

entre os pontos quânticos, partimos para uma avaliação do comportamento desta medida de correlações quânticas considerando a aplicação de campos externos sobre os pontos quânticos e sobre a cavidade. Nesta análise fixamos os valores obtidos para os parâmetros de decoerência no processo de maximização da discórdia quântica na análise anterior, definindo diferentes valores dos acoplamentos dos campos clássicos com a cavidade ou com os pontos quânticos e observando a dinâmica temporal da discórdia quântica.

A fim de observar os efeitos da aplicação de um campo clássico sobre os pontos quânticos produzimos um gráfico que apresenta a evolução temporal da discórdia quântica para diferentes valores do acoplamento do campo clássico com os pontos quânticos g_0 (figura 2.6). Manteremos, em um primeiro momento, o sistema em completa ressonância, de maneira que os pontos quânticos têm propriedades idênticas e o bombeio clássico pode ser representado pela aplicação de um laser que atinge ambos os qbits devido às dimensões reduzidas do sistema. É possível identificar uma relação bem definida entre a discórdia quântica assintótica e o acoplamento g_0. Explicitamente, a discórdia quântica no estado assintótico decresce com a elevação de g_0. A aplicação do campo clássico força contínuas transições entre os estados fundamental e excitado de cada qbit. Este comportamento, em cooperação com os canais de dissipação e bombeio incoerente nos pontos quânticos, tende a levar o sistema a um estado muito próximo ao maximamente misto, com elementos não diagonais bem menores que a unidade. À medida que g_0 aumenta, o estado do sistema se aproxima mais do estado maximamente misto, o que leva a uma redução da discórdia quântica. Outra característica relevante observada no gráfico é o fato de que g_0 acelera a dinâmica da discórdia quântica, ou seja, quanto maior g_0, mais precocemente será atingido o valor estacionário da discórdia quântica. Um motivo possível para este comportamento é que ao estimular a emissão de fótons pelo ponto quântico (que é injetado no modo da cavidade e que pode vir a ser absorvido pelo outro ponto) o acoplamento efetivo entre ponto quântico e cavidade seja mais intenso, resultando em uma dinâmica mais veloz do sistema.

Consideramos agora a possibilidade de aplicar um campo clássico sobre o modo da cavidade. A figura 2.7 apresenta a dinâmica da discórdia quântica para diferentes valores do acoplamento do campo clássico com o modo da cavidade g_c. As mesmas propriedades encontradas na análise da discórdia quântica em função de g_0 também são reveladas nesta análise. O aumento de g_c resulta num decréscimo da discórdia quântica e na aceleração

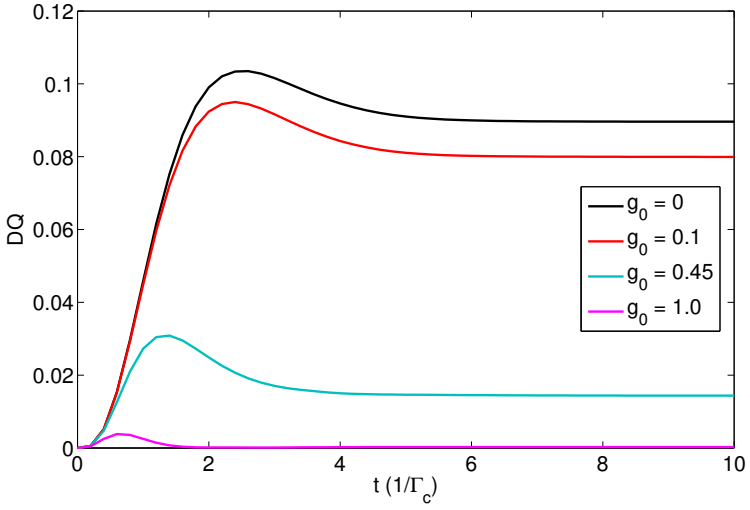

Figura 2.6: Evolução temporal da discórdia quântica para diferentes acoplamentos g_0, com o campo clássico atuando sobre os pontos quânticos. Os parâmetros utilizados nesta figura são $\Gamma_c = P_c = 1$, $g = 0.47$, $\Gamma_0 = 1.3$ e $P_0 = \gamma_2 = 0.001$.

da dinâmica das correlações quânticas. Uma diferença evidente entre os dois casos é o fato de que o decréscimo em discórdia quântica pela elevação do valor de g_c é muito menos acentuado do que no caso da aplicação de um campo clássico sobre os pontos quânticos. É possível que a aplicação do campo clássico iniba a interação indireta dos pontos quânticos ao dificultar a troca de excitações entre eles. Isto ocorreria pelo fato de que a probabilidade de um ponto quântico absorver um fóton emitido pelo outro ponto seria reduzida por ter uma alta probabilidade de absorver um outro fóton injetado na modo da cavidade pelo bombeio clássico. Isso representa um empecilho para a troca de informação entre os qbits, coibindo o estabelecimento de correlações quânticas entre estes elementos, levando diretamente a uma redução do valor da discórdia quântica.

Como apresentado até este ponto, a combinação de diferentes canais de decoerência faz com que canais específicos causem efeitos sobre os valores da discórdia quântica diferentes do que se observa quando atuam de maneira individual. Na análise anterior fixamos os valores de Γ_c e P_c e então os canais de decoerência dos pontos quânticos foram sendo adicionados, inicialmente a dissipação (com $P_0 = \gamma_2 = 0$) e, após obter parâmetros que maximizam a discórdia quântica no passo anterior, foram considerados valores não-nulos de P_0 e γ_2. Adiante, analisaremos o efeito dos diferentes canais de decoerência observando o valor da discórdia quântica em função da ordem de grandeza da razão entre as taxas de decoerência e Γ_c.

Nesta nova análise variamos as taxas dos canais de decoerência (parametrizando em

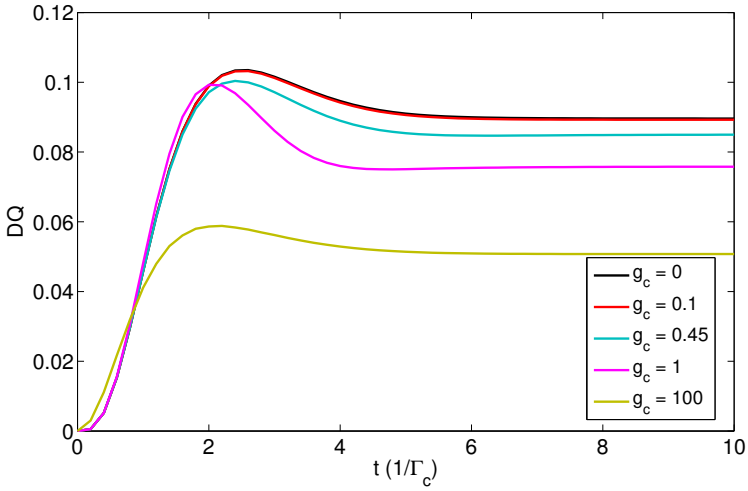

Figura 2.7: Evolução temporal da discórdia quântica para diferentes acoplamentos g_c do campo clássico atuando sobre a cavidade. Os parâmetros utilizados nesta figura são $\Gamma_c = P_c = 1$, $g = 0.47$, $\Gamma_0 = 1.3$ e $P_0 = \gamma_2 = 0.001$. 2.6

relação a Γ_c e, portanto, fixando $\Gamma_c = 1$), assim como o acoplamento g, entre os valores do conjunto $\{10^{-4}, 5\times10^{-4}, 10^{-3}, 5\times10^{-3}, 10^{-2}, 5\times10^{-2}, 10^{-1}, 5\times10^{-1}, 1, 5\}$ e calculamos a discórdia quântica para cada combinação de valores $\{g, P_c, \Gamma_0, P_0, \gamma_2\}$. O estudo dos dados obtidos neste procedimento pode levar à percepção de características que, porventura, não tenham sido explicitadas na análise anterior.

A fim de observar o comportamento da discórdia quântica em relação às taxas de decoerência e ao acoplamento entre os pontos quânticos e a cavidade, produzimos os gráficos apresentados na figura 2.8. No gráfico do painel esquerdo, cada ponto em uma dada curva representa o maior valor de discórdia quântica (entre o conjunto de valores computados) quando o respectivo parâmetro físico assume o valor relacionado a tal ponto. No painel direito, cada ponto corresponde à média dos valores computados de discórdia quântica para um valor específico do respectivo parâmetro físico. As curvas obtidas para o acoplamento g evidenciam o caráter construtivo deste parâmetro em relação à geração de correlações quânticas. Este comportamento se deve ao fato de que, com maiores valores de g, a troca de excitações entre os pontos quânticos, mediada pelo modo da cavidade, se torna mais efetiva possibilitando o compartilhamento de informação entre os dois qbits. Ao observar as curvas de discórdia quântica em função do dephasing, o que se observa é um padrão oposto ao obtido para as curvas relacionadas ao acoplamento g. De fato, quanto maior γ_2 menor será o valor da discórdia quântica, o que salienta o efeito unicamente destrutivo deste canal de decoerência sobre a geração de correlações

quânticas. As curvas de discórdia quântica em função de Γ_0 se assemelham ás relacionadas ao dephasing, revelando decréscimo de correlações quânticas com a elevação do valor de tal parâmetro. A curva relacionada ao bombeio incoerente sobre os pontos quânticos apresenta características diferentes às demais. Neste caso, observa-se um limite máximo quando o valor de P_0 é da ordem de 10^{-3} enquanto que para os outros parâmetros de decoerência, as curvas sugerem limites máximos de discórdia para os menores valores possíveis destes parâmetros. Analisando os dados obtidos pela simulação observamos que os maiores valores de discórdia quântica são obtidos obedecendo-se levemente um padrão definido por $P_0 > \Gamma_0$ com o valor do bombeio incoerente não sendo maior que 0,01. Como vimos anteriormente, é necessário que os valores do bombeio incoerente e da dissipação sobre os pontos quânticos sejam suficientemente diferentes para que a discórdia quântica assuma valores não-nulos. O padrão $P_0 > \Gamma_0$ se dá pelo fato de que, enquanto a dissipação sobre os pontos quânticos remove a excitação do sistema, o bombeio incoerente as insere. Esta é uma forma de excitar o sistema e, consequentemente, permitir que estas excitações sejam trocadas entre os pontos quânticos (através da interação com o modo da cavidade) levando-os a um estado correlacionado. Por outro lado, se o bombeio incoerente é muito intenso, o efeito oposto é obtido. Isto ocorre pois a alta taxa de geração de excitações nos pontos quânticos pelo bombeio incoerente inibe a troca de excitações entre estes elementos de forma coerente, uma vez que ao perder a excitação através da emissão de um fóton no modo da cavidade há alta probabilidade de o ponto ser excitado novamente de forma incoerente de maneira que não há contribuição para o estabelecimento de correlações entres os dois pontos quânticos. O comportamento da discórdia quântica em função do bombeio incoerente na cavidade P_c é surpreendente considerando-se o resultado obtido na referência [91]. O limite máximo do valor da discórdia quântica é reduzido á medida que P_c se aproxima de Γ_c. Este comportamento ressalta a importância da relação de forças entre os vários canais de decoerência na geração da discórdia quântica.

No painel esquerdo da figura 2.8 nota-se que para os parâmetros de decoerência (com exceção de γ_2) os limites máximos de discórdia quântica são menores quando os valores destes parâmetros se aproximam do valor de Γ_c. Este comportamento pode ser explicado, em parte, pelo fato de que cada canal de decoerência tende a levar o sistema para um estado assintótico diferente. Isto ocorre de maneira não cooperativa de forma que, ao atuar com intensidades semelhantes, o estado do sistema apresente altos níveis de mistura, o que

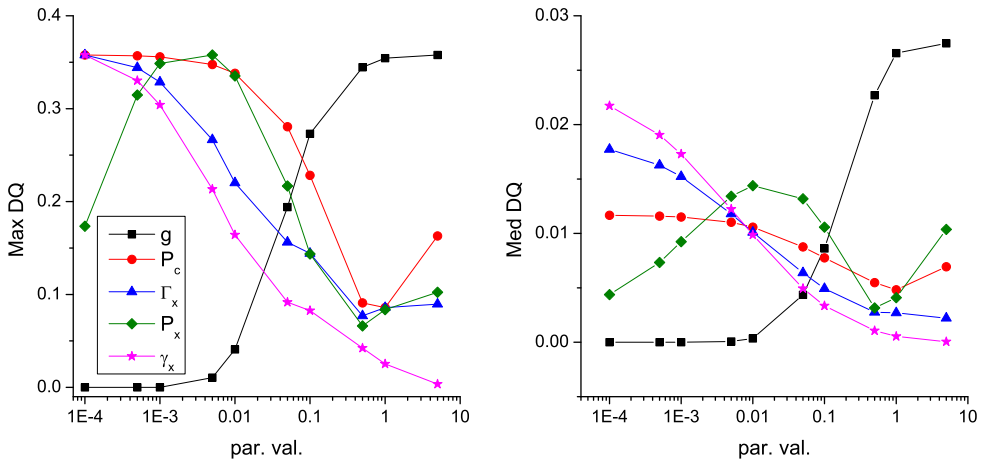

Figura 2.8: Painel esquerdo: Valores máximos da discórdia quântica (dentre os calculados) em função dos valores dos parâmetros físicos. Painel direito: Valores médios da discórdia quântica (dentre os calculados) em função dos valores dos parâmetros físicos. No eixo horizontal são apresentados os valores dos parâmetros (taxas de decoerência) com o rótulo par. val. e no eixo vertical apresentam-se os valores de discórdia quântica (máxima no painel esquerdo e média no painel direito).

pode levar a baixos valores de discórdia quântica. Deste modo, ao passo que os valores das taxas de decoerência ultrapassam o valor de Γ_c, o estado assintótico recupera parte das correlações quânticas pelo fato de que a competição entre os canais de decoerência não é mais tão intensa.

Uma característica importante revelada por estes cálculos é que a discórdia quântica máxima obtida, com valor aproximado de 0.36, é maior do que a apresentada na referência [91] com valor de aproximadamente 0.33. Ainda que este valor seja alcançado com parâmetros não muito realistas para o estágio atual de desenvolvimento do sistema físico - com taxas de decoerência da ordem de $10^{-4} - 10^{-3}$, este fato evidencia o poder dos canais de decoerência sobre os pontos quânticos de contribuir para a geração de discórdia quântica. É possível que valores maiores sejam encontrados ao se realizar os mesmos cálculos com uma resolução maior para os valores dos parâmetros físicos envolvidos.

É importante ressaltar que esta última análise é diferente da realizada anteriormente. Na primeira o processo de maximização foi realizado partindo-se de um conjunto inicial de valores para as taxas de decoerência e então observando-se o impacto da variação dessas taxas (aos pares) nos valores da discórdia quântica. O par de valores que resulta no maior valor possível de discórdia quântica é armazenado (e atualizado) e então repete-se a análise para outro par de taxas de decoerência. Nesta última análise definimos conjuntos de valores para os parâmetros físicos e calculamos todas as combinações possíveis dos valores

predeterminados. Com estes cálculos foi possível observar como os canais de decoerência limitam os valores de discórdia quântica, o que é uma avaliação mais geral do que a primeira.

2.3 Testemunha de correlações

Há indícios de que correlações quânticas possibilitam um ganho computacional na realização de protocolos de computação e informação quântica. Em geral, estes protocolos envolvem sistemas cujos estados não são puramente clássicos, mas possuem correlações quânticas. Portanto, a identificação de um caráter quântico nas correlações no estado de um sistema pode ser de grande utilidade para a realização de computação e informação quântica. Uma forma de se identificar a natureza quântica do estado de um sistema se dá pelo cálculo da discórdia quântica, pois, se a discórdia é não-nula o estado do sistema possui correlações quânticas que podem ser quantificadas por esta medida. O cálculo da discórdia quântica demanda trabalhos experimentais e teóricos complexos. Isto ocorre porque é necessário o conhecimento exato do estado do sistema, o que requer um complexo conjunto de medidas, além disso, o cálculo da discórdia envolve um processo de extremização computacionalmente exigente. Para contornar esta dificuldade, é possível utilizar observáveis, conhecidos como testemunhas, que indicam a presença ou ausência de correlações quânticas utilizando conjuntos reduzidos de medidas [95, 96]. Propomos, agora, a aplicação de uma testemunha de "classicalidade"para o sistema composto de dois pontos quânticos em uma cavidade em um nanocristal semicondutor.

Para dar prosseguimento à proposta é importante salientar que na ausência de bombeios clássicos a matriz densidade que representa o estado conjunto dos pontos quânticos durante toda a evolução temporal, o que engloba o estado assintótico, assume a forma de um estado do tipo X. Isto é, a forma matricial do estado conjunto dos qbits $\rho^{a,b} = \sum_{i=0}^{3}\sum_{j=0}^{3}\rho_{ij}|i\rangle\langle j|$ é

$$\rho^{a,b} = \begin{pmatrix} \rho_{00} & 0 & 0 & \rho_{03} \\ 0 & \rho_{11} & \rho_{12} & 0 \\ 0 & \rho_{21} & \rho_{22} & 0 \\ \rho_{30} & 0 & 0 & \rho_{33} \end{pmatrix} \tag{2.4}$$

onde foi adotada a base decimal para os estados, ou seja, $|0\rangle_a \otimes |0\rangle_b = |0\rangle_{a,b}$, $|0\rangle_a \otimes |1\rangle_b = |1\rangle_{a,b}$, $|1\rangle_a \otimes |0\rangle_b = |2\rangle_{a,b}$ e $|1\rangle_a \otimes |1\rangle_b = |3\rangle_{a,b}$. Este fato pode ser visualizado pelo gráfico apresentado na Fig. 2.9 que mostra a evolução temporal dos elementos da matriz densidade. Para esta simulação o sistema parte do estado $|0\rangle_{a,b}$, a atuação dos canais de decoerência e a interação com o modo da cavidade, causa uma redução do elemento ρ_{00} e elevação dos valores dos elementos ρ_{11}, ρ_{11}, ρ_{22}, ρ_{33} e ρ_{12} (e por consequência ρ_{21}), enquanto os outros elementos permanecem nulos a todo instante.

Jonas Maziero e Roberto Serra apresentaram uma testemunha a partir da qual pode-se determinar a natureza das correlações presentes no estado de um sistema, ou seja, é capaz de indicar se existem ou não correlações quânticas no sistema [97]. Esta testemunha é válida para uma classe diversificada de estados que inclui os estados tipo X. Deste modo, essa testemunha é válida para os estados assintóticos encontrados até aqui, visto que, na ausência de campos clássicos o estado conjunto dos pontos quânticos é do tipo X. A testemunha tem a seguinte forma

$$W_\rho = \sum_{i=1}^{3} \sum_{j=i+1}^{4} |\langle O_i \rangle_\rho \langle O_j \rangle_\rho|, \tag{2.5}$$

onde os observáveis são definidos por

$$O_i = \sigma_i^a \otimes \sigma_i^b \tag{2.6}$$

$$O_4 = \mathbf{z} \cdot \sigma^a \otimes \mathbf{I}^b + \mathbf{I}^a \otimes \mathbf{w} \cdot \sigma^b, \tag{2.7}$$

com $i = 1, 2, 3$. As matrizes de Pauli são representadas por σ_i, e para estes elementos podemos fazer a identificação $1 \to x$, $2 \to y$ e $3 \to z$. Os índices a e b identificam os dois pontos quânticos. Os vetores $\mathbf{z}$ e $\mathbf{w}$ são unitários e devem ser escolhidos de forma aleatória. A importância da equação (2.5) se baseia no fato de que se $W_\rho = 0$, então o sistema não possui correlações quânticas.

Ainda que a utilização de testemunhas seja mais simples do que o cálculo da discórdia quântica, visto que são projetadas para apenas indicar a natureza quântica das correlações e não para quantificá-las, a sua realização envolve alguns desafios experimentais. Para se obter o valor esperado de σ_3 é necessário ter informação da população do estado fundamental ou excitado dos pontos quânticos. Pesquisadores já conseguiram desenvolver

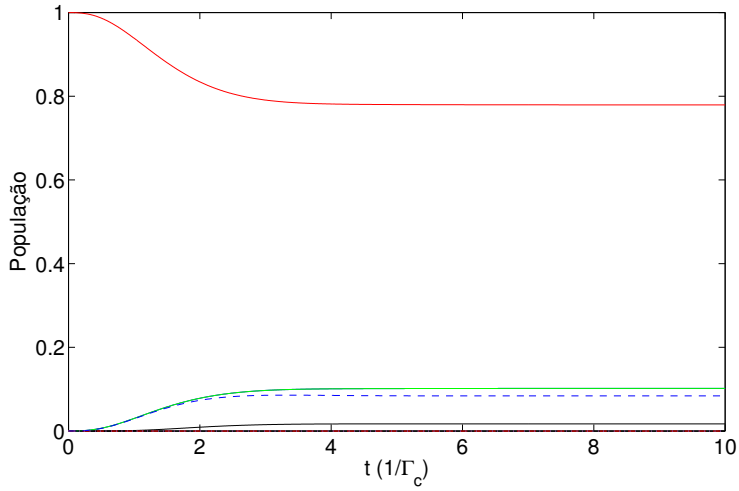

Figura 2.9: Evolução temporal dos elementos da matriz densidade conjunta dos dois pontos quânticos. As curvas correspondem aos elementos ρ_{00} (vermelho), ρ_{11} (encoberta pela curva de ρ_{00}), ρ_{22} (verde), ρ_{33} (preto), ρ_{12} (azul tracejado) e os elementos $\rho_{01}, \rho_{02}, \rho_{03}, \rho_{13}$ e ρ_{23} estão sempre com valores nulos. Os parâmetros utilizados são $\Gamma_c = P_c = 1, g = 0,47, \Gamma_0 = 1.3$ e $P_0 = \gamma_2 = 0,001$.

técnicas para medir transmissão óptica em um único ponto quântico [98–100]. Apoiando-se nestas técnicas, esperamos ser possível obter o valor esperado do observável O_3 realizando-se uma medida conjunta de transmissão nos dois qbits. A distância entre os pontos quânticos pode ser muito pequena, de maneira que pode ser difícil aplicar um laser apenas sobre um, mantendo o outro não iluminado. Portanto, pode-se considerar que os pontos quânticos não estão em ressonância entre si, de modo que sejam usados dois lasers com frequências diferentes (cada um ressonante com um ponto quântico específico). Essa diferenciação se faz necessária para a avaliação correta do observável O_4.

A aplicação de um pulso laser de área $\pi/2$ permite a avaliação de σ_2. Isto ocorre porque a aplicação do pulso tem como efeito rotacionar o estado do sistema na esfera de Bloch em torno do eixo x em um ângulo de $\pi/2$. Com isto, a medida que forneceria o valor esperado de σ_3, fornece agora o valor esperado de σ_2. Na figura 2.10, apresenta-se alguns exemplos da realização deste procedimento nos painéis a-c, assim como a simulação da aplicação de tal pulso laser sobre o estado assintótico do sistema no painel d.

Como pode ser visto na figura 2.10d, a medida deve ser realizada imediatamente após a aplicação do pulso pelo fato de que a atuação dos canais de decoerência atuam rapidamente, alterando os valores dos termos da matriz densidade e, por consequência, inserindo erros significativos na medida. A atuação dos canais de decoerência exigem, ainda, que a largura do pulso seja pequena em relação à taxa de dissipação na cavidade. A figura 2.11 evidencia o efeito nocivo da decoerência sobre a atuação do pulso laser. Um

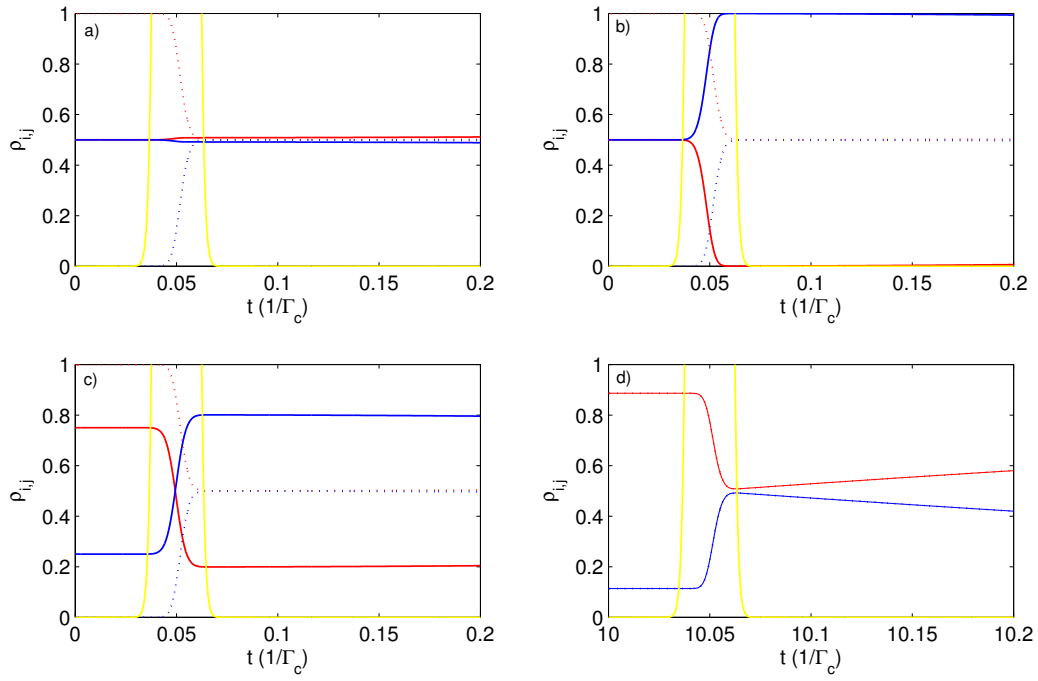

Figura 2.10: Aplicação de um pulso de área $\pi/2$ como preparação para medida de σ_y. Linhas contínuas (com exceção à linha amarela) se referem a um qubit rotulado por A e linhas pontilhadas referentes ao outro qbit rotulado por B. Linhas vermelhas se referem às populações dos estados fundamentais e linhas azuis aos estados excitados. A linha amarela se refere ao pulso aplicado cuja duração característica é de $0.01\Gamma_c$ (este valor é mantido por toda a análise). Gráficos de a - c são testes com respectivos estados $(|0\rangle + |1\rangle)/\sqrt{2}$, $(|0\rangle + i\,|1\rangle)/\sqrt{2}$ e $(3\,|0\rangle + \frac{1+i}{\sqrt{2}}\,|1\rangle)/2$ a fim de se demonstrar o efeito do pulso. Nestes casos decoerência não foi considerada. Para o gráfico em d, o pulso é aplicado sobre o estado estacionário, considerando-se decoerência e utilizando-se os parâmetros $\Gamma_c = P_c = 1$, $g = 0.47$, $\Gamma_0 = 1.3$ e $P_0 = \gamma_2 = 0.001$. Em todos os casos, a realização de uma medida de σ_z após a aplicação do pulso equivale a uma medida de σ_y no estado original. Os termos de coerência das matrizes densidades não são mostrados para melhor visualização. Para o estado estacionário no gráfico d, as matrizes densidade dos qbits apresentam termos de coerência nulos, portanto, o valor de σ_y é nulo.

pulso com largura relativamente grande não rotaciona o estado da maneira desejada, visto que a decoerência força o sistema a uma dinâmica indesejada. À medida que a largura do pulso se torna menor, a rotação é realizada em tempos menores do que os tempos característicos dos canais de decoerência, tornando a rotação mais eficaz e correta. Como o estado dos qbits no regime estacionário contém termos de coerência pequenos, a aplicação do pulso deve levar a população dos estados fundamental e excitado para valores próximos de 0.5, de maneira que uma medida de σ_z (equivalente a uma medida de σ_y sobre o estado estacionário) seja nula. Pulsos cuja duração são comparáveis ao tempo característico de atuação dos canais de decoerência não atingem o objetivo. O pulso apresentado no gráfico com duração de $0.01/\Gamma_c$ fornece os resultados mais satisfatórios.

Por fim, uma maneira de se preparar o estado do sistema para a medida de σ_1 se dá

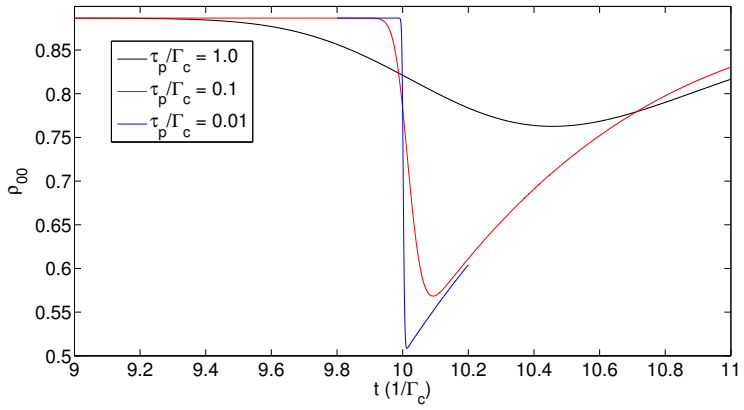

Figura 2.11: Comparação dos resultados obtidos pela aplicação de pulsos de larguras τ_p diferentes sobre o estado estacionário como preparação para medida de σ_y.

pela aplicação de um segundo pulso laser, de mesma área, defasado em $\pi/2$ em relação ao primeiro pulso. Isto causa uma rotação do estado na esfera de Bloch em torno do eixo y por um ângulo de $\pi/2$, logo, a medida original que forneceria o valor esperado de σ_3, revela agora o valor esperado de σ_1. O resultado da aplicação desta sequência de pulsos pode ser observada na figura 2.12. Nesta figura são apresentadas simulações deste procedimento para estados de teste e também para o estado assintótico do sistema, incluindo casos com dessintonia. O resultado da aplicação dos pulsos é satisfatória desde que o intervalo entre os pulsos seja pequeno, para evitar que a atuação dos canais de decoerência influencie negativamente o resultado da medida.

É importante notar que os canais de decoerência atuando durante a preparação das medidas, como apresentadas nesta seção, irão gerar algum erro. Isto ocorre pelo fato de que a interação com estes canais irá levar o sistema a um estado levemente diferente do que o esperado após a aplicação da rotação pelo pulso laser (ou pelo conjunto de pulsos). Podemos quantificar o erro gerado por este fator no caso específico da matriz densidade apresentada na Fig. 2.9, resultado da maximização de discórdia quântica do início do presente capítulo. Para este caso, os valores esperados dos operadores que compõem a testemunha são $\langle O_1\rangle = 0,1634$, $\langle O_2\rangle = 0,1634$, $\langle O_3\rangle = 0,6081$ e $\langle O_4\rangle = -1.0119$, onde foram selecionados os vetores unitários $\overrightarrow{z} = (0,2074, 0,5185, 0,8296)$ e $\overrightarrow{w} = (0,6852, 0,5481, 0,4793)$. Com estes valores o resultado ideal da testemunha é $W^i_\rho deal = 1.1722$, o que indica a presença de correlações quânticas. Por outro lado, realizando-se os procedimentos de preparação para medidas apresentados neste capítulo são obtidos os valores $\langle O_1\rangle = 0,1521$, $\langle O_2\rangle = 0,1608$, $\langle O_3\rangle = 0,6081$ e $\langle O_4\rangle = -1.0427$.

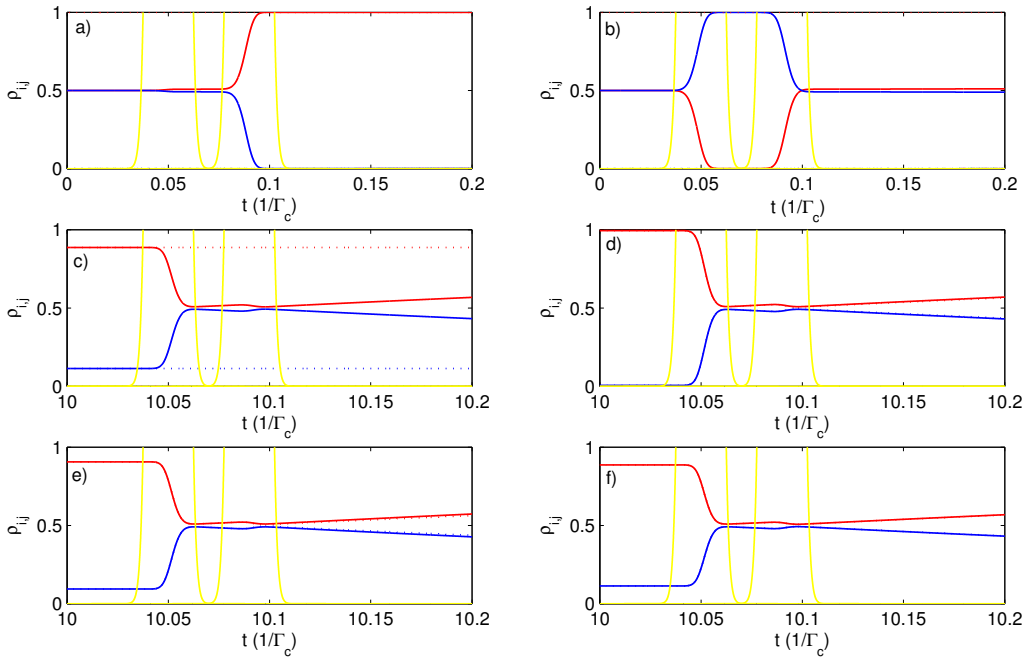

Figura 2.12: Aplicação de dois pulsos ressonantes com os pontos quânticos, tendo o segundo pulso uma fase de $\pi/2$ em relação ao primeiro. Para os gráficos a e b não se considera decoerência e os estados iniciais são $(|0\rangle + |1\rangle)/\sqrt{2}$ e $(|0\rangle + i\,|1\rangle)/\sqrt{2}$. Nos gráficos de c a f leva-se em consideração a atuação dos canais de decoerência, além disso, os pulsos são aplicados sobre o estado estacionário obtido sob a influência destes canais. No gráfico c os pulsos são aplicados apenas sobre o qbit A. Neste gráfico os pontos quânticos estão em ressonância com o modo da cavidade. Nos gráficos de d a f são aplicados dois pulsos sobre cada ponto quântico. Na figura d o qbit A(B) tem dessintonia em relação ao modo da cavidade de $10(-10)\Gamma_c$, na figura e esta dessintonia é $1(-1)\Gamma_c$ e na figura f a dessintonia é de $0.1(-0.1)\Gamma_c$. O esquema de pulsos funciona de maneira eficiente como preparação para as medidas de σ_z equivalentes às medidas σ_y e σ_x dos estados anteriores à sequencia de pulsos.

Estes valores levam a um resultado real da testemunha de $W_\rho^r eal = 1.1752$, representando um erro de apenas 0,26 % e indicando, corretamente, a presença de correlações quânticas.

2.4 Conclusão

Analisamos, neste capítulo, a influência dos canais de decoerência sobre a discórdia quântica gerada entre dois pontos quânticos inseridos em uma nanocavidade óptica. Os cálculos numéricos revelaram que o dephasing é extremamente nocivo para a geração de correlações quânticas, sendo necessário a fabricação de estruturas que permitam que este canal de decoerência seja desprezível para que os pontos quânticos estejam quanticamente correlacionados. Observamos que para gerar o máximo de correlações quânticas há um nível de acoplamento ideal, acima do qual os valores de discórdia quântica são menores, o que é surpreendente, visto que esperávamos valores de discórdia superiores

para acoplamentos mais intensos. Outro ponto indicado pelos cálculos é o fato de que as taxas de dissipação e o bombeio incoerente não podem pertencer à mesma ordem de grandeza para que a discórdia seja não nula. Isto ocorre, provavelmente, pela competição entre os canais de decoerência que tende a levar o sistema para o estado maximamente misto.

Avaliamos, ainda, como os canais de decoerência limitam os valores máximos de discórdia quântica. Enquanto o acoplamento g tem um caráter geral benéfico aos valores máximos de discórdia quântica, este limite máximo decresce à medida que as taxas Γ_0, γ_2 e P_c se aproximam do valor de Γ_c. O fato de o limite máximo do valor da discórdia quântica decrescer com a elevação de P_c evidencia a importância de se considerar os canais de decoerência atuantes nos pontos quânticos. Ao se considerar o bombeio incoerente sobre os pontos quânticos, observa-se um padrão diferente ao dos outros canais de decoerência, visto que o limite máximo do valor da discórdia quântica não é monotonicamente decrescente, apresentando um máximo em valores pequenos de P_0 e decrescendo em regiões mais afastadas de um valor ideal. Além disso, observamos que a atuação dos canais de decoerência sobre os pontos quânticos, em conjuntos de valores específicos das taxas de decoerência, é capaz de elevar o valor da discórdia quântica em relação ao valor que se obtém quando apenas são considerados a dissipação e o bombeio incoerente sobre a cavidade.

Por fim, propomos a aplicação de uma testemunha de classicalidade, a fim de que se possa verificar se o estado assintótico do sistema é útil para a realização de protocolos de informação e computação quântica. Com técnicas específicas de medidas de transmissão em pontos quânticos individuais esperamos que este procedimento possa ser realizado em pontos quânticos no interior de nanocavidades.

Para finalizar salientamos que, apesar de termos ambientado a análise em pontos quânticos inseridos em uma nanocavidade óptica em um cristal fotônico, tal análise pode ser estendida para qualquer sistema de um par de qbits que interagem com um modo eletromagnético e sofre a atuação de canais de decoerência como os considerados neste trabalho.

Capítulo 3

O algoritmo de Deutsch-Jozsa pelo modelo DQC1

Como discutido no capítulo introdutório, conjectura-se que correlações quânticas podem ser uma propriedade que permite um ganho para a computação quântica e, portanto, é interessante observar como estas correlações se desenvolvem ao longo da solução de um problema. Apresentamos aqui, a avaliação da presença de correlações quânticas na realização do algoritmo de Deutsch-Jozsa no modelo DQC1. Iniciaremos o capítulo apresentando o problema e o algoritmo de Deutsch, assim como sua evolução para o algoritmo de Deutsch-Jozsa e uma posterior simplificação. Veremos, também, como este algoritmo pode ser adaptado ao modelo computacional DQC1 de forma bastante direta. Posteriormente apresentaremos como as operações lógicas utilizadas nessa computação, que inclui uma operação controlada sobre um conjunto de múltiplos qbits, podem ser decompostas em um conjunto de operações sobre um ou dois qbits. Realizada a decomposição, avaliamos a presença de correlações quânticas após cada operação e observamos que, apesar de não haver correlações quânticas ao final da computação, elas são geradas e consumidas em passos intermediários da computação. Para avaliar o papel dos estados mistos no modelo DQC1 modificamos o estado inicial do sistema para um estado totalmente puro. Observando a geração de emaranhamento ao final da computação, quantificado pela negatividade, verificamos que a quantidade dessas correlações escala com a dimensão do sistema enquanto a eficiência do algoritmo não é alterada.

3.1 O algoritmo de Deutsch-Jozsa e sua adaptação ao modelo DQC1

O problema de Deutsch consiste em, dada uma função desconhecida $f : \{0,1\} \rightarrow \{0,1\}$, determinar a sua classe que pode ser constante ou balanceada [101]. A função é definida como constante se $f(0) = f(1) = 0$ ou $f(0) = f(1) = 1$ e é balanceada se $f(0) \neq f(1)$. Para solucionar este problema classicamente é necessário conhecer os valores $f(0)$ e $f(1)$ e então verificar se $f(0) = f(1)$ ou $f(0) \neq f(1)$, exigindo, portanto, duas avaliações de f. Por outro lado, o algoritmo quântico de Deutsch permite solucionar este problema em apenas uma execução, mostrando uma vantagem computacional sobre o método convencional. Apesar de a primeira versão apresentada deste algoritmo ser probabilística, houve desenvolvimento de forma que é possível determinar com total certeza a classe da função com apenas uma medida [102]. Este algoritmo exige a inicialização de dois qbits, um no estado $|0\rangle$ e outro no estado $|1\rangle$. O primeiro passo do algoritmo é a aplicação de uma porta Hadamard sobre cada um dos qbits, gerando o estado

$$|\Psi\rangle = [\frac{|0\rangle + |1\rangle}{\sqrt{2}}][\frac{|0\rangle - |1\rangle}{\sqrt{2}}].$$

O passo seguinte é uma operação controlada que não altera o estado do primeiro qbit mas altera o estado do segundo qbit, condicionado ao estado do primeiro, na forma $|x_1\rangle |x_2\rangle \rightarrow |x_1\rangle |x_2 \oplus f(x_1)\rangle$. Apesar da ação voltada ao segundo qbit, o algoritmo está baseado nas informações fornecidas pelo primeiro qbit. Após a aplicação da operação descrita o estado do primeiro qbit será, a menos de uma fase global, $1/\sqrt{2}(|0\rangle+|1\rangle)$ se f é constante e $1/\sqrt{2}(|0\rangle-|1\rangle)$ se f é balanceada. O algoritmo é finalizado aplicando uma porta de Hadamard sobre o primeiro algoritmo e medindo-se o seu estado. Da informação anterior, se a medida indicar o qbit no estado $|0\rangle$ pode-se afirmar que f é uma função constante e se obtemos $|1\rangle$ f é balanceada.

O problema de Deutsch possui uma modificação para trabalhar com um conjunto maior de elementos de entrada, solucionado pelo algoritmo de Deutsch-Jozsa [2]. Neste caso considera-se uma função desconhecida $f : \{0,1\}^n \rightarrow \{0,1\}$, definida como constante se $f(j) = 0$ ou $f(j) = 1$ para todo j ($j = 0, ..., 2^n - 1$) e é balanceada se $f(j) = 0$ para metade dos valores de j e $f(j) = 1$ para os valores de j restantes. Na solução clássica, são necessárias de 2 até $2^{n-1} + 1$ avaliações de f para se determinar a classe da função com

total certeza. Na computação quântica o algoritmo de Deutsch-Jozsa resolve o problema com apenas uma medida coletiva, ou seja, com n medidas individuais nos qbits. No caso ideal esta é a melhor solução para o problema e será usada como uma solução de referência. De maneira geral, este algoritmo é muito similar ao algoritmo de Deutsch. Inicializa-se um registro de n qbits todos no estado $|0\rangle$ e um único qbit no estado $|1\rangle$ e então aplica-se uma operação de Hadamard a cada um dos qbits. Em seguida aplica-se uma operação que, assim como no algoritmo de Deutsch, não altera o estado do registro com n qbits e modifica o estado do último qbit na forma $|x_c\rangle |x_2\rangle \rightarrow |x_c\rangle |x_2 \oplus f(x_1)\rangle$, onde $|x_c\rangle$ é o estado do registro controle com n qbits. Ao aplicar a operação de Hadamard sobre o registro de controle, o que se obtém é um resultado análogo ao algoritmo de Deutsch: se f é uma função constante o estado desse conjunto de qbits será $|0\rangle^n$ e se f for balanceada o estado será qualquer outro. Portanto, uma única medida sobre os n qbits determina a natureza dessa função, o que é um ganho exponencial em relação ao pior cenário da solução clássica.

A versão de Collins para esse algoritmo utiliza um registro com n qbits, eliminando o qbit inicializado no estado $|1\rangle$, e é representado pelo circuito na Fig. 3.1, onde a operação unitária U codifica a função f [103]. Após a aplicação das n portas de Hadamard o registro está em uma superposição igual de 2^n estados $|j\rangle$. A ação de U sobre $|j\rangle$ é $U|j\rangle = (-1)^{f(j)}|j\rangle$, ou seja, U é uma matriz na forma

$$U = \sum_j (-1)^{f(j)} |j\rangle \langle j| . \tag{3.1}$$

O resultado do algoritmo pode ser obtido pela projeção do estado final no estado $|j = 0\rangle$, fornecendo o resultado

$$\frac{1}{2^n} \sum_{j=0}^{2^n-1} (-1)^{f(j)} = \begin{cases} 1 & \text{if } f \text{ é constante,} \\ 0 & \text{if } f \text{ é balanceada.} \end{cases} \tag{3.2}$$

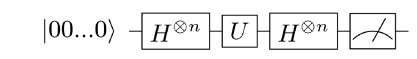

Figura 3.1: O circuito para realização do algoritmo de Deutsch-Jozsa na versão de Collins. Cada qbit, em um conjunto de n qbits é inicializado no estado $|0\rangle$. Uma operação de Hadamard é aplicada sobre cada qbit antes e depois da aplicação da operação U que define a função a ser avaliada. Para extrair o resultado é realizada uma medida ao final da computação.

A estrutura da operação U permite a determinação da classe da função f pelo cálculo

do seu traço, ou mesmo seu traço normalizado. Como apresentado anteriormente, uma maneira eficiente de se calcular o traço de uma matriz unitária se dá pelo modelo computacional DQC1 [55]. Para que o algoritmo de Deutsch-Jozsa seja implementado por este modelo basta que a operação U_n presente na figura 1.1 e na equação 1.1 represente a operação que codifica a função do problema de Deutsch-Jozsa. Neste caso, o estado final do qbit controle é $\rho_{bal} = I_0/2$ para uma função balanceada e $\rho_{const} = (I_0 \pm \alpha X_0)/2$ para uma função constante. Portanto, se uma medida σ_x é realizada sobre este qbit, o resultado para o valor esperado é $\langle\sigma_x\rangle = 0$ com variância $\triangle\sigma_x = 1$ para uma função balanceada e $\langle\sigma_x\rangle = \pm\alpha$ com variância $\triangle\sigma_x = \sqrt{1-\alpha^2}$ para uma função constante.

O algoritmo de Deutsch-Jozsa foi abordado em diferentes modelos de computação: computação clássica probabilística, computação quântica circuital com estados puros, computação quântica com ensembles, computação quântica adiabática, computação quântica unidirecional (one-way quantum computing), computação quântica dissipativa e computação quântica "às cegas"(blind quantum computation) [27, 102–109].

Eficiência do algoritmo - De acordo com a Ref. [110], a melhor situação para se distinguir entre os estados ρ_{bal} e ρ_{const} ocorre quando $\alpha = 1$, de forma que esse será o valor atribuído a α de agora em diante. Idealmente, se uma sequência de medidas é realizada, uma função balanceada será identificada imediatamente quando ambos os valores 1 e -1 estiverem entre o conjunto de valores obtidos. Se, em um dado número de medidas, todos os resultados das medidas apresentarem o mesmo valor, então a função será classificada como constante, assumindo-se uma certa probabilidade de erro. O algoritmo é eficiente visto que necessita de apenas um número polinomial de repetições para identificar a classe da função com alta probabilidade de sucesso. Isso ocorre devido ao fato de que este algoritmo é equivalente ao algoritmo clássico probabilístico apresentado por J. Preskill na Ref. [105], fato também discutido por Arvind e David Collins [104]. Em ambos os casos, clássico e quântico, uma função balanceada será identificada com total certeza se os dois diferentes valores estiverem presentes no conjunto do resultado das medidas. Por outro lado, se em k medidas obtém-se o mesmo resultado define-se a função como sendo constante, assumindo-se uma probabilidade de erro P_{err}. No algoritmo clássico a probabilidade de duas medidas sequenciais apresentarem o mesmo resultado, dado que a função é balanceada, é $1 \times \frac{(2^{n-1}-1)}{(2^n-1)}$, para três resultados iguais a probabilidade é $1 \times \frac{(2^{n-1}-1)}{(2^n-1)} \times \frac{(2^{n-1}-2)}{(2^n-2)}$, portanto, para k medidas, a probabilidade de todas as medidas

fornecerem o mesmo resultado é $g(k,n) = 1 \times \frac{(2^{n-1}-1)}{(2^n-1)} \times \frac{(2^{n-1}-2)}{(2^n-2)} \times ... \times \frac{(2^{n-1}-k+1)}{(2^n-k+1)}$. Seja p a probabilidade de a função ser balanceada, deste modo, a probabilidade de erro é $P^c_{err} = g(k,n)p$. No algoritmo quântico, a cada repetição da computação, o sistema é reinicializado para se realizar uma nova medida, de maneira que em cada nova medida a probabilidade de o resultado ser 1 ou -1 é $1/2$, sendo independente do número de qbits n. Assim, a probabilidade de erro é $P^q_{err} = p/2^{k-1}$. Este resultado ocorre no algoritmo clássico sob a condição $2^{n-1} \gg k$ e mostra que a performance do algoritmo clássico é um limitante superior para o algoritmo quântico implementado no modelo DQC1, como pode ser visto para $p = 1/2$ na Fig. 3.2. Comparando a solução probabilística clássica com a quântica determinística [103], pode-se notar que o primeiro também é eficiente, haja vista que são necessárias apenas k medidas para obter uma solução com uma probabilidade definida, enquanto o último exige n medidas para se obter a solução exata. Na Fig. 3.2 nós observamos que a probabilidade de uma solução incorreta P_{err} com relação à classe da função é consideravelmente pequena, com apenas $k = 6$ medidas a chance de um erro é de apenas 2%, resultado que independe do número de qbits n. Nosso resultado está de acordo com a Ref. [104], que mostra que a performance do algoritmo de Deutsch-Jozsa em computação quântica com ensembles é pior do que o algoritmo probabilístico clássico previamente apresentado.

Pode ser desejável que, em vez de usar o mesmo sistema a cada nova repetição da computação, usar um conjunto de k computadores quânticos de maneira que a computação é realizada sobre todos os computadores ao mesmo tempo e uma medida σ_x sobre o qbit puro de todos os sistemas irá resultar em $\Sigma_x = \sum_{j=1}^{k} \langle \sigma_x \rangle_k$. Se o conjunto de medidas fornecer $|\Sigma_x| < k$ a função é classificada como balanceada, visto que, logicamente, os dois valores possíveis para as medidas foram obtidos. Por outro lado, se todas as medidas fornecerem o mesmo valor, $\Sigma_x = \pm k$, define-se a função como sendo constante e, como discutido anteriormente, a probabilidade de erro associada a esta solução será $P^q_{err} = p/2^{k-1}$. Na realização experimental apresentada na referência [59], um sistema RMN contendo uma quantidade de moléculas da ordem de 10^{18} é utilizado. Portanto, o algoritmo de Deutsch-Jozsa é realizado no modelo DQC1 de maneira simultânea em todas as moléculas, logo, a computação é realizada um número de vezes igual à quantidade de moléculas presentes no sistema. Como discutido há pouco, este procedimento é probabilístico, sendo, no máximo, tão eficiente quanto a solução clássica. Além disso, não

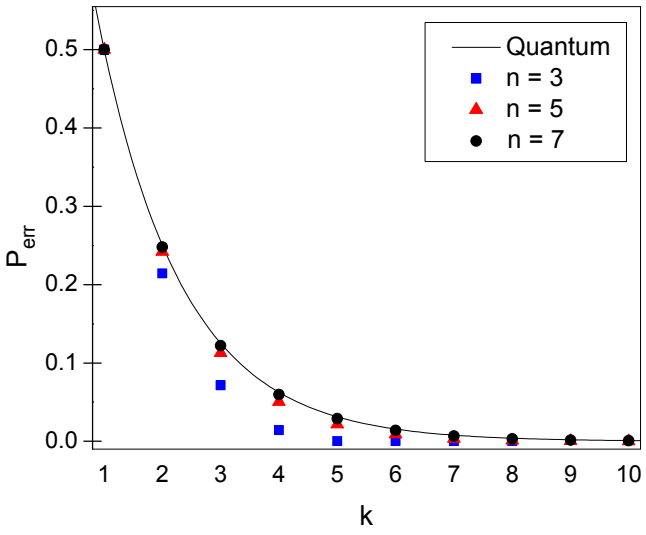

Figura 3.2: Probabilidade de erro na solução do algoritmo de Deutsch-Jozsa, P_{err}, após um número k de medidas com resultados idênticos, dado que a função é balanceada, tanto para a realização pelo modelo DQC1 (linha contínua) quanto para a solução clássica com 3 (quadrados), 5 (triângulos) e 7 bits (círculos)

há vantagem computacional sobre a solução clássica, a vantagem observada na realização experimental tem uma natureza técnica relacionada à enorme quantidade de recursos físicos, isto é, o número de moléculas no ensemble.

Correlações quânticas - Investigamos agora o papel das correlações quânticas na execução do algoritmo de Deutsch-Jozsa pelo modelo DQC1. De início, note-se que o estado final do computador quântico definido pela Eq. (1.1) pode ser escrito como

$$\begin{aligned}\rho &= \sum_{j=0}^{2^n-1}(1/2^{n+1})\left[|0\rangle\langle 0| + \alpha(-1)^{f(j)}|0\rangle\langle 1|\right. \\ &\quad \left. +\alpha(-1)^{f(j)}|1\rangle\langle 0| + |1\rangle\langle 1|\right]\otimes|j\rangle\langle j| \\ &= \sum_{j=0}^{2^n-1}(1/2^{n+1})(|a_j\rangle\langle a_j| + |b_j\rangle\langle b_j|)\otimes|j\rangle\langle j|\,, \end{aligned} \tag{3.3}$$

onde $|a_j\rangle = cos\phi\,|0\rangle + (-1)^{f(j)}sin\phi\,|1\rangle$, $|b_j\rangle = sin\phi\,|0\rangle + (-1)^{f(j)}cos\phi\,|1\rangle$, e $sin(2\phi) = \alpha$ [66]. Particularmente, para $\alpha = 1$ o estado final é

$$\rho = \sum_{j=0}^{2^n-1}(1/2^n)\,|f(j)\rangle\langle f(j)|\otimes|j\rangle\langle j|\,, \tag{3.4}$$

com $|f(j)\rangle = (|0\rangle + (-1)^{f(j)}|1\rangle)/\sqrt{2}$.

Pode-se notar das Eqs. (3.3) e (3.4) que o estado ρ é separável para qualquer partição, visto que os estados $|j\rangle$ descrevem a base computacional. Isto fica evidente quando se reescreve o estado da Eq. (3.3) na forma

$$\sum_{\substack{i=+,-\\0<j<2^n-1}} p_{i,j} \left|i\right\rangle \left\langle i\right| \otimes \left|j\right\rangle \left\langle j\right|, \tag{3.5}$$

onde $|\pm\rangle = (|0\rangle \pm |1\rangle)/\sqrt{2}$ e $p_{\pm,j} = (1 \pm \alpha(-1)^{f(j)})/2$. Nesta forma pode-se observar que o sistema é descrito por um estado do tipo CC. Portanto, ρ não possui correlações quânticas. Esta afirmação deve ser corroborada por qualquer medida do tipo discórdia sobre qualquer bipartição do sistema [9, 10, 111, 112].

Após realizar uma medida σ_x no qbit controle a melhor condição para discriminar entre funções balanceadas e constantes se dá quando $\alpha = 1$. O algoritmo de Deutsch-Jozsa é eficientemente implementado pelo modelo DQC1, visto que o valor de σ_x é conhecido com uma dada precisão, que é independente do número n de qbits mistos. Na Ref. [104] os autores mostram que este algoritmo quântico (para $\alpha = 1$) tem, no máximo, uma performance equivalente à do algoritmo clássico probabilístico. Portanto, as versões clássica e quântica do algoritmo de Deutsch-Jozsa discutido aqui têm performances equivalentes. Este não é um resultado óbvio, porque é possível que correlações quânticas estejam presentes em estados intermediários da computação, mesmo que os estados inicial e final não possuam estas correlações. Por outro lado, o sistema físico de um computador clássico sempre estará em um estado que não possui correlações quânticas. Isto é, enquanto a trajetória do sistema em uma computação clássica no espaço de estados seja constituída apenas por estados clássicos, a trajetória de um computador quântico no espaço de estados pode compreender estados quanticamente correlacionados, ainda que os pontos inicial e final sejam estados sem correlações quânticas, fato que pode prover uma vantagem computacional à solução quântica, por exemplo, pela utilização de um número inferior de operações lógicas [113].

Para investigar a geração e o consumo de correlações quânticas na realização do algoritmo utilizamos o procedimento apresentado por S. Bullock e L. Markov para decompor um operador unitário diagonal em uma sequência de um rotações de qbits a portas CNOT [114]. Esta síntese é geral, de forma que pode descrever qualquer operação unitária relacionada à função f utilizada no algoritmo de Deutsch-Jozsa, balanceada ou

constante. A decomposição foi realizada para os casos de dois e três qbits mistos e apresentamos este último caso na Fig. 3.3.

O ato de determinar a presença ou ausência das correlações quânticas após cada operação lógica no algoritmo sintetizado é equivalente a observar se é possível escrever o estado do sistema como uma distribuição de probabilidades clássica ou não. Os detalhes são apresentados no apêndice deste capítulo. Para o caso de dois qbits mistos, correspondendo a quatro valores para o índice j ($j = 00, 01, 10, 11$), não é possível encontrar correlações quânticas em qualquer ponto do algoritmo. Na decomposição para três qbits mistos, identificamos correlações quânticas entre a segunda e a penúltima operação CNOT para algumas funções balanceadas. Neste último caso nós encontramos um valor nulo de negatividade avaliada para todos os passos no algoritmo sintetizado considerando diferentes particionamentos para todos os tipos de funções: i) uma divisão que separa o qbit controle do outro registro e ii) uma divisão que coloca os dois qbits superiores em uma partição e os dois inferiores em outra partição [70]. Nós observamos que os ângulos de rotação θ_j presentes na síntese do algoritmo podem assumir, entre outros valores, o valor $\pm\pi/4$ para algumas funções balanceadas. Nestas situações a operação R_j é igual a porta T (ou $\pi/8$), uma operação que não pertence ao grupo de Clifford. Apesar do teorema de Gottesman-Knill e o resultado de Eastin (de que uma computação concordante pode ser simulada em um computador clássico) não se aplicarem a estes casos, o algoritmo aqui apresentado pode ser eficientemente simulado em um computador clássico [115, 116].

Para estados puros a discórdia quântica é igual à entropia de emaranhamento, i.e., quantifica o emaranhamento entre duas partições [10]. Analogamente, Collins, Kim a Holton chegaram a uma conclusão semelhante para o algoritmo de Deutsch-Jozsa implementado pelo modelo computacional quântico convencional com estados puros [103]. Os pesquisadores concluíram que não é gerado emaranhamento para o problema com dois qbits, enquanto para três qbits ou mais algumas funções balanceadas geram emaranhamento entre os qbits. Chaves e Melo mostraram que existem funções para as quais é possível implementar o algoritmo de Deutsch-Jozsa no modelo computacional unidirecional com decoerência partindo de um estado que possui apenas correlações clássicas [108]. Arvind, Dorai e Kulmar implementaram o algoritmo de Deutsch-Jozsa em um experimento em RMN e observaram a ausência de emaranhamento para o caso com um ou dois qbits e geração de emaranhamento para algumas funções balanceadas no

caso de três qbits [117].

3.2 O algoritmo de Deutsch-Jozsa pelo modelo DQCp

A ideia básica da computação quântica determinística com estados puros (DQCp) é reproduzir no qbit controle os valores esperados do modelo DQC1 [55]. Os mesmos resultados para o algoritmo de Deutsch-Jozsa no modelo DQC1 apresentados anteriormente, isto é, os valores esperados e variâncias de σ_x para o qbit controle, podem ser obtidos se $\alpha = 1$ e o registro com n qbits no circuito DQC1 forem inicializados no estado $|+\rangle^{\otimes n} = \left[(|0\rangle + |1\rangle)/\sqrt{2}\right]^{\otimes n}$. Este resultado, por sua vez, demonstra que resolver alguns problemas de oráculo em um computador quântico trabalhando pelo modelo DQC1 pode ser tão eficiente quanto em um computador trabalhando com o modelo DQCp [55]. Aqui, uma diferença importante entre os modelos DQC1 e DQCp é o fato de que com o estado inicial puro o circuito pode gerar quantidades significantes de emaranhamento entre os qbits ao final da computação, enquanto com estados mistos nenhuma correlação quântica é gerada.

Para verificar esta hipótese, fizemos simulações numéricas para realizar o algoritmo 50 vezes com funções balanceadas aleatórias com um número de qbits mistos de 1 a 10, avaliando também a negatividade para duas divisões distintas: *i*) uma divisão que separa os $(n+1)/2$ qbits superiores e os $(n+1)/2$ qbits inferiores para n ímpar, e *ii*) os $n/2$ qbits superiores e os $n/2+1$ qbits inferiores para n par. O valor máximo observado para a negatividade para cada número de qbits mistos está exposta na Fig. 3.4. A curva obtida apresenta um padrão geral crescente, com a característica de valores sequenciais aproximadamente constante aos pares visto que a negatividade é limitada pela dimensão da menor partição [66]. Apesar de o emaranhamento crescer com a dimensão do sistema a presença destas correlações não resulta em melhoria para o algoritmo quântico se comparado ao clássico.

Os estados finais do algoritmo de Deutsch-Jozsa no modelo DQC1 e DQCp para as classes de funções possíveis não têm suporte ortogonal, isto é, não se pode distinguir entre estes estados com apenas uma medida como na computação quântica convencional com estados puros [102, 103]. Isto caracteriza uma natureza probabilística deste algoritmo.

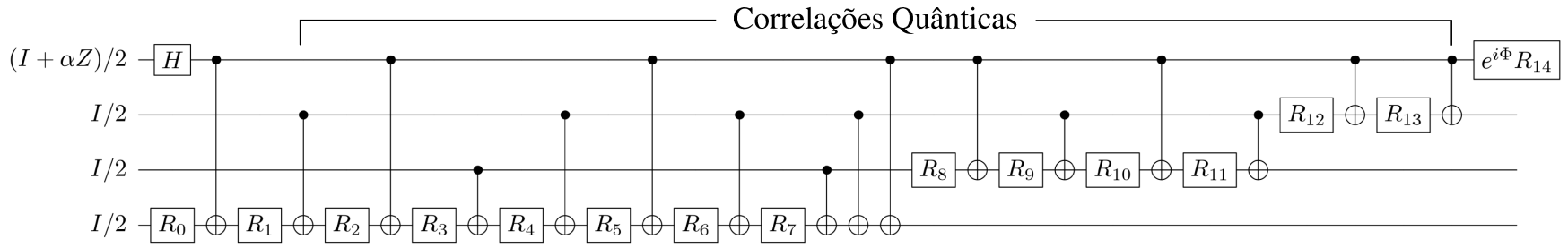

Figura 3.3: Algoritmo sintetizado de Deutsch-Jozsa implementado no modelo DQC1 para três qbits mistos. Dependendo da função balanceada os qbits podem se tornar correlacionados quanticamente nos trechos da circuito destacados na parte superior da figura. Aqui a operação $R_j \equiv R_z^l(\theta_j) = e^{-i\theta_j/2}\left|0\right\rangle_l\left\langle 0\right| + e^{i\theta_j/2}\left|1\right\rangle_l\left\langle 1\right|$ rotaciona o estado do l-ésimo qbit por um ângulo θ_j em volta do eixo z. Os ângulos de rotação são definidos por $\theta_0 = -\theta_1 \equiv -\pi(f_0 - f_1 + f_2 - f_3 + f_4 - f_5 + f_6 - f_7)/8$, $\theta_2 = -\theta_3 \equiv \pi(f_0 - f_1 + f_2 - f_3 - f_4 + f_5 - f_6 + f_7)/8$, $\theta_4 = -\theta_7 \equiv -\pi(f_0 - f_1 - f_2 + f_3 - f_4 + f_5 + f_6 - f_7)/8$, $\theta_5 = -\theta_6 \equiv -\pi(f_0 - f_1 - f_2 + f_3 + f_4 - f_5 - f_6 + f_7)/8$, $\theta_8 = -\theta_9 \equiv -\pi(f_0 + f_1 - f_2 - f_3 + f_4 + f_5 - f_6 - f_7)/8$, $\theta_{10} = -\theta_{11} \equiv \pi(f_0 + f_1 - f_2 - f_3 - f_4 - f_5 + f_6 + f_7)/8$, $\theta_{12} = -\theta_{13} \equiv -\pi(f_0 + f_1 + f_2 + f_3 - f_4 - f_5 - f_6 - f_7)/8$, e $\theta_{14} = 2\Phi \equiv \pi(f_0 + f_1 + f_2 + f_3 + f_4 + f_5 + f_6 + f_7)/8$.

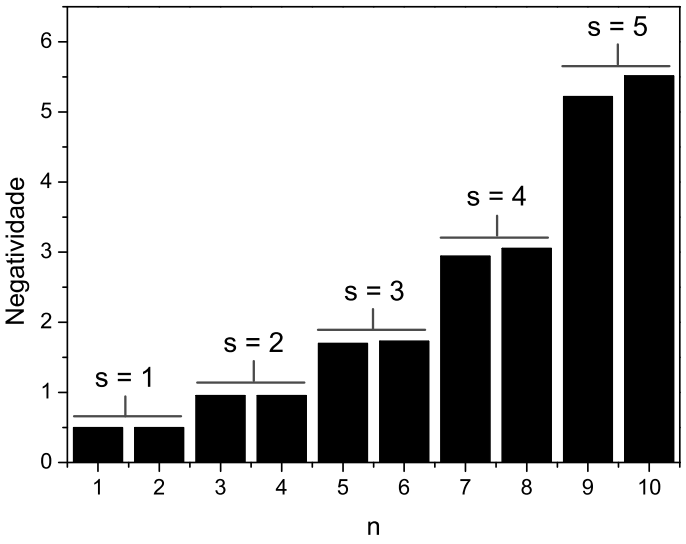

Figura 3.4: Negatividade para o estado final da realização do algoritmo de Deutsch-Jozsa pelo modelo DQCp em função do número de qbits n. Os valores são calculados em relação à divisão que separa os $(n+1)/2$ qbits superiores e os $(n+1)/2$ qbits inferiores, para n ímpar, e os $n/2$ qbits superiores e os $n/2+1$ qbits inferiores para n par. A sequência de valores aproximadamente constantes se deve à limitação dos valores da negatividade pela dimensão da menor partição. Aqui, s é o número de qbits na menor partição.

Com objetivo de eliminar este caráter probabilístico da solução do problema em ambos modelos tentamos obter uma melhoria através do modelo de computação $\mathrm{DQC1}_k$ (e DQCP_k) [118]. Este modelo é similar ao modelo DQC1 (DQCp), porém permite-se a realização de medidas sobre k qbits. Porém, não foi possível determinar uma forma de se obter ganho através deste modelo. Uma possível razão para estes resultados está relacionada ao fato de que, para funções balanceadas, o estado do qbit controle é proporcional ao operador identidade, o que torna impossível a tarefa de distingui-lo perfeitamente de qualquer outro estado.

3.3 Conclusão

Apresentamos neste capítulo o algoritmo de Deutsch-Jozsa e sua implementação no modelo DQC1, além de expandir esta ideia para o modelo DQCp. Em ambos modelos o estado inicial dos qbits não apresenta correlações, sejam elas clássicas ou quânticas. No modelo DQC1 o estado final do algoritmo não possui correlações quânticas. Por outro lado, no modelo DQCp os qbits ao final do algoritmo estão altamente correlacionados para algumas funções balanceadas e o emaranhamento entre blocos de qbits aumenta

com o tamanho do sistema. O algoritmo é eficientemente implementado nestes modelos de computação. Independentemente da presença ou ausência de correlações quânticas entre os qbits em cada passo do algoritmo, a solução quântica não apresenta vantagem sobre a apresentada pelo algoritmo clássico probabilístico. A solução pelo modelo $\mathrm{DQC1}_k$ (e DQCp_k) não apresentou vantagens sobre as soluções previamente analisadas.

No artigo original do modelo DQC1 os autores afirmam que tal modelo é ineficiente para solucionar problemas de oráculo uma vez que seria necessário realizar um número exponencial de medidas para distinguir entre duas operações unitárias, visto que os resultados diferem por um valor muito menor que a unidade. Nosso exemplo, entretanto, contradiz esta afirmação e mostra que para o algoritmo de Deutsch-Jozsa os modelos DQC1 e DQCp são equivalentes.

Apêndice: Detecção de correlações quânticas no algoritmo sintetizado

Aqui nós mostramos como detectamos correlações quânticas no estado do sistema após a aplicação de cada operação do algoritmo sintetizado para o caso de três qbits mistos. O procedimento é o mesmo para o caso de dois qbits mistos, no qual não encontramos correlações quânticas. Isto é realizado através da verificação da forma do estado, de maneira que se ele pode ser escrito na forma CC então não possui correlação quântica alguma, caso contrário há alguma natureza quântica nas correlações presentes [69]. Como apresentado no texto principal, o algoritmo sintetizado é composto por operações de Hadamard, rotações de um qbit, aqui indicadas por R_k^i (onde k é o mesmo índice de rotação utilizado na Fig. 3.3 e i é o índice do qbit, iniciando de 0 para o qbit semipuro e variando de 1 a 3 para os qbits mistos), e operações controladas, aqui indicadas por $CNOT_m^n$, onde m e n são os índices dos qbits controle e alvo, respectivamente.

O estado inicial $\rho_{ini} = 2^{-(n+1)}(I_0 + \alpha Z_0) \otimes I^{\otimes n}$ não possui correlações quânticas. Visto que I_0 pode ser escrito em qualquer base, incluindo os autoestados de Z_0, este estado pode ser apresentado na forma $\rho_{ini} = \sum_i p_i \left|i\right\rangle \left\langle i\right|$, com $p_i = \{2^{-(n+1)}(1+\alpha), 2^{-(n+1)}(1-\alpha)\}$ representando uma distribuição de probabilidades clássicas.

Apresentamos, agora, os estados ρ_s obtidos após cada passo s do algoritmo sintetizado (partindo do passo 0) e fazemos uma análise da natureza quântica das correlações presentes

nestes estados.

0) Operação Hadamard sobre o qbit 0 e R_0^3:

$$\rho_0 = 2^{-4}(I_0 + \alpha X_0) \otimes I^{\otimes 3},$$

onde usamos $n = 3$ para indicar que estudamos especificamente o caso com três qbits mistos. Este estado pode ser colocado na mesma forma do anterior, e também representa uma distribuição clássica de probabilidades, portanto, não possui correlações quânticas.

1) $CNOT_0^3$:

$$\rho_1 = 2^{-4}(I^{\otimes 4} + \alpha X_0 I_1 I_2 X_3),$$

onde nós eliminamos alguns $\otimes$ para deixar a equação mais simples. Novamente, as identidades dos qbits 0 e 3 no primeiro termo podem ser escritas na mesma base de X_0 e X_3 no segundo termo, logo, o estado pode ser escrito em uma forma totalmente clássica.

2) R_1^3:

$$\rho_2 = 2^{-4}(I^{\otimes 4} + \alpha X_0 I_1 I_2 Q_3(\theta_1)),$$

onde cada matriz $Q_k(x)$ assume a forma $|0\rangle\langle 1|_k e^{-ix} + |1\rangle\langle 0|_k e^{ix}$. Neste caso, como a identidade assume a mesma forma em qualquer base, I_0 e X_0 são diagonais na base de X_0 assim como I_3 e $Q_3(\theta_1)$ possuem uma base em comum, de forma que ρ_2 assume uma forma clássica.

3) $CNOT_1^3$:

$$\rho_3 = 2^{-4}\left\{I^{\otimes 4} + \alpha X_0 |0\rangle\langle 0|_1 I_2 Q_3(\theta_1) + \alpha X_0 |1\rangle\langle 1|_1 I_2 Q_3^*(\theta_1)\right\},$$

onde $Q_3^*(\theta_1)$ é o complexo conjugado de $Q_3(\theta_1)$. A comutatividade entre $Q_3(\theta_1)$ e $Q_3^*(\theta_1)$ depende do valor de θ_1. Do texto principal temos que, para funções balanceadas, θ_1 pode assumir um valor do conjunto $\{0, \pm\pi/4, \pm\pi/2\}$. Nota-se que $Q_3(\theta_1)$ e $Q_3^*(\theta_1)$ possuem uma base em comum apenas se $\theta_1 = \pm\pi/4$, portanto, o estado ρ_3 possuirá correlações quânticas se $\theta_1 = \pm\pi/4$, e será um estado clássico se $\theta_1 = 0$ or $\theta_1 = \pm\pi/2$. Assim, o sistema possuirá correlações quânticas neste ponto do algoritmo sintetizado apenas para funções balanceadas que satisfaçam $\theta_1 = \pm\pi/4$.

4) R_2^3:

$$\rho_4 = 2^{-4}\left\{I^{\otimes 4} + \alpha X_0 \left|0\right\rangle\left\langle 0\right|_1 I_2 Q_3(\theta_2+\theta_1) + \alpha X_0 \left|1\right\rangle\left\langle 1\right|_1 I_2 Q_3(\theta_2-\theta_1)\right\}.$$

Como no passo anterior, para alguns valores de θ_1 e θ_2 (e.g. $\theta_1 = \pm\pi/4$ e $\theta_2 = 0$) o estado não pode ser escrito em uma forma diagonal, de modo que, para algumas funções balanceadas ρ_4 estará correlacionado quanticamente.

5) $CNOT_0^3$:

$$\rho_5 = 2^{-4}\left\{I^{\otimes 4} + [\alpha \left|0\right\rangle\left\langle 1\right|_0 [\left|0\right\rangle\left\langle 0\right|_1 I_2 P_3(\theta_2+\theta_1) + \left|1\right\rangle\left\langle 1\right|_1 I_2 P_3(\theta_2-\theta_1)] + H.c.]\right\},$$

onde $H.c.$ indica o conjugado de $P_k(x) = \left|0\right\rangle\left\langle 0\right|_k e^{-ix} + \left|1\right\rangle\left\langle 1\right|_k e^{ix}$. Rearranjando esta expressão obtemos $\rho_5 = \left|0\right\rangle\left\langle 0\right|_1 I_2 [I_0 I_3 + \alpha \left|0\right\rangle\left\langle 1\right|_0 P_3(\theta_2+\theta_1) + \alpha \left|1\right\rangle\left\langle 0\right|_0 P_3^*(\theta_2+\theta_1)] + \left|1\right\rangle\left\langle 1\right|_1 I_2 [I_0 I_3 + \alpha \left|0\right\rangle\left\langle 1\right|_0 P_3(\theta_2-\theta_1) + \alpha \left|1\right\rangle\left\langle 0\right|_0 P_3^*(\theta_2-\theta_1)]$. Em todos os termos de ρ_5 os estados dos qbits 1 e 2 são diagonais na mesma base (para o espaço de estados de cada qbit), mas os termos para os qbits 0 e 3 não o são. A comutação entre os dois termos do lado direito da expressão anterior é proporcional a $(\left|0\right\rangle\left\langle 0\right|_0 - \left|1\right\rangle\left\langle 1\right|_0)[P_3(\theta_2+\theta_1)P_3^*(\theta_2-\theta_1) - P_3(\theta_2-\theta_1)P_3^*(\theta_2+\theta_1)]$, o que, por sua vez, é proporcional a $sen(2\theta_1)$. Deste modo, se $\theta_1 = \pm\pi/4$ ρ_5 possuirá correlações quânticas neste ponto do algoritmo sintetizado, caso contrário ele representará apenas uma distribuição clássica de probabilidades.

Como o procedimento para detectar correlações quânticas é o mesmo para os estados restantes, nós apenas iremos escrever estes estados e informamos, de antemão, que todos os estados até o estado ρ_{28} podem possuir correlações quânticas para algumas funções balanceadas. Retornaremos à análise para os estados finais da computação.

6) R_3^3:

$$\rho_6 = \rho_5.$$

7) $CNOT_0^3$:

$$\begin{aligned}\rho_7 \;=\; & 2^{-4}\left\{I^{\otimes 4} + [\alpha \left|0\right\rangle\left\langle 1\right|_0 [\left|0\right\rangle\left\langle 0\right|_1 [\left|0\right\rangle\left\langle 0\right|_2 P_3(\theta_2+\theta_1) + \left|1\right\rangle\left\langle 1\right|_2 P_3^*(\theta_2+\theta_1)]\right. \\ & \left. + \left|1\right\rangle\left\langle 1\right|_1 [\left|0\right\rangle\left\langle 0\right|_2 P_3(\theta_2-\theta_1) + \left|1\right\rangle\left\langle 1\right|_2 P_3^*(\theta_2-\theta_1)]] + H.c.]\right\}.\end{aligned}$$

8) R_4^3:

$$\rho_8 = \rho_7.$$

9) $CNOT_1^3$:

$$\begin{aligned}\rho_9 &= 2^{-4}\left\{I^{\otimes 4} + [\alpha\,|0\rangle\langle 1|_0\,[|0\rangle\langle 0|_1\,[|0\rangle\langle 0|_2\,P_3(\theta_2+\theta_1) + |1\rangle\langle 1|_2\,P_3^*(\theta_2+\theta_1)]\right.\\ &\quad \left. + |1\rangle\langle 1|_1\,[|0\rangle\langle 0|_2\,P_3^*(\theta_2-\theta_1) + |1\rangle\langle 1|_2\,P_3(\theta_2-\theta_1)]] + H.c.]\right\}.\end{aligned}$$

10) R_5^3:

$$\rho_{10} = \rho_9.$$

11) $CNOT_0^3$:

$$\begin{aligned}\rho_{11} &= 2^{-4}\left\{I^{\otimes 4} + [\alpha\,|0\rangle\langle 1|_0\,[|0\rangle\langle 0|_1\,[|0\rangle\langle 0|_2\,Q_3(\theta_2+\theta_1) + |1\rangle\langle 1|_2\,Q_3^*(\theta_2+\theta_1)]\right.\\ &\quad \left. + |1\rangle\langle 1|_1\,[|0\rangle\langle 0|_2\,Q_3^*(\theta_2-\theta_1) + |1\rangle\langle 1|_2\,Q_3(\theta_2-\theta_1)]] + H.c.]\right\}.\end{aligned}$$

12) R_6^3:

$$\begin{aligned}\rho_{12} &= 2^{-4}\left\{I^{\otimes 4} + [\alpha\,|0\rangle\langle 1|_0\,[|0\rangle\langle 0|_1\,[|0\rangle\langle 0|_2\,Q_3(\theta_6+\theta_2+\theta_1) + |1\rangle\langle 1|_2\,Q_3(\theta_6-\theta_2-\theta_1)]\right.\\ &\quad \left. + |1\rangle\langle 1|_1\,[|0\rangle\langle 0|_2\,Q_3(\theta_6-\theta_2+\theta_1) + |1\rangle\langle 1|_2\,Q_3(\theta_6+\theta_2-\theta_1)]] + H.c.]\right\}.\end{aligned}$$

13) $CNOT_1^3$:

$$\begin{aligned}\rho_{13} &= 2^{-4}\left\{I^{\otimes 4} + [\alpha\,|0\rangle\langle 1|_0\,[|0\rangle\langle 0|_1\,[|0\rangle\langle 0|_2\,Q_3(\theta_6+\theta_2+\theta_1) + |1\rangle\langle 1|_2\,Q_3(\theta_6-\theta_2-\theta_1)]\right.\\ &\quad \left. + |1\rangle\langle 1|_1\,[|0\rangle\langle 0|_2\,Q_3^*(\theta_6-\theta_2+\theta_1) + |1\rangle\langle 1|_2\,Q_3^*(\theta_6+\theta_2-\theta_1)]] + H.c.]\right\}.\end{aligned}$$

14) R_7^3:

$$\begin{aligned}\rho_{14} &= 2^{-4}\left\{I^{\otimes 4}\right.\\ &\quad + [\alpha\,|0\rangle\langle 1|_0\,[|0\rangle\langle 0|_1\,[|0\rangle\langle 0|_2\,Q_3(\theta_7+\theta_6+\theta_2+\theta_1) + |1\rangle\langle 1|_2\,Q_3(\theta_7+\theta_6-\theta_2-\theta_1)]\\ &\quad \left. + |1\rangle\langle 1|_1\,[|0\rangle\langle 0|_2\,Q_3(\theta_7-\theta_6+\theta_2-\theta_1) + |1\rangle\langle 1|_2\,Q_3(\theta_7-\theta_6-\theta_2+\theta_1)]] + H.c.]\right\}.\end{aligned}$$

15) $CNOT_2^3$:

$$\begin{aligned}\rho_{15} &= 2^{-4}\left\{I^{\otimes 4}\right. \\ &+\Big[\alpha\left|0\right\rangle\left\langle 1\right|_0\Big[\left|0\right\rangle\left\langle 0\right|_1\Big[\left|0\right\rangle\left\langle 0\right|_2 Q_3(\theta_7+\theta_6+\theta_2+\theta_1)+\left|1\right\rangle\left\langle 1\right|_2 Q_3^\dagger(\theta_7+\theta_6-\theta_2-\theta_1)\Big] \\ &+\left|1\right\rangle\left\langle 1\right|_1\Big[\left|0\right\rangle\left\langle 0\right|_2 Q_3(\theta_7-\theta_6+\theta_2-\theta_1)+\left|1\right\rangle\left\langle 1\right|_2 Q_3^\dagger(\theta_7-\theta_6-\theta_2+\theta_1)\Big]\Big]+H.c.\Big]\Big\}.\end{aligned}$$

16) $CNOT_1^3$:

$$\begin{aligned}\rho_{16} &= 2^{-4}\left\{I^{\otimes 4}\right. \\ &+\Big[\alpha\left|0\right\rangle\left\langle 1\right|_0\Big[\left|0\right\rangle\left\langle 0\right|_1\Big[\left|0\right\rangle\left\langle 0\right|_2 Q_3(\theta_7+\theta_6+\theta_2+\theta_1)+\left|1\right\rangle\left\langle 1\right|_2 Q_3^\dagger(\theta_7+\theta_6-\theta_2-\theta_1)\Big] \\ &+\left|1\right\rangle\left\langle 1\right|_1\Big[\left|0\right\rangle\left\langle 0\right|_2 Q_3^\dagger(\theta_7-\theta_6+\theta_2-\theta_1)+\left|1\right\rangle\left\langle 1\right|_2 Q_3(\theta_7-\theta_6-\theta_2+\theta_1)\Big]\Big]+H.c.\Big]\Big\}.\end{aligned}$$

17) $CNOT_2^3$:

$$\begin{aligned}\rho_{17} &= 2^{-4}\left\{I^{\otimes 4}\right. \\ &+\Big[\alpha\left|0\right\rangle\left\langle 1\right|_0\Big[\left|0\right\rangle\left\langle 0\right|_1\Big[\left|0\right\rangle\left\langle 0\right|_2 P_3(\theta_7+\theta_6+\theta_2+\theta_1)+\left|1\right\rangle\left\langle 1\right|_2 P_3^\dagger(\theta_7+\theta_6-\theta_2-\theta_1)\Big] \\ &+\left|1\right\rangle\left\langle 1\right|_1\Big[\left|0\right\rangle\left\langle 0\right|_2 P_3^\dagger(\theta_7-\theta_6+\theta_2-\theta_1)+\left|1\right\rangle\left\langle 1\right|_2 P_3(\theta_7-\theta_6-\theta_2+\theta_1)\Big]\Big]+H.c.\Big]\Big\}.\end{aligned}$$

Define-se agora $A_3 = P_3(\theta_7+\theta_6+\theta_2+\theta_1)$, $B_3 = P_3^*(\theta_7+\theta_6-\theta_2-\theta_1)$, $C_3 = P_3^*(\theta_7-\theta_6+\theta_2-\theta_1)$ and $D_3 = P_3(\theta_7-\theta_6-\theta_2+\theta_1)$.

18) R_8^2:

$$\rho_{18} = \rho_{17}.$$

19) $CNOT_0^2$:

$$\begin{aligned}\rho_{19} &= 2^{-4}\left\{I^{\otimes 4}+\left[\alpha\left|0\right\rangle\left\langle 1\right|_0\left[\left|0\right\rangle\left\langle 0\right|_1\left[\left|0\right\rangle\left\langle 1\right|_2 A_3+\left|1\right\rangle\left\langle 0\right|_2 B_3\right]\right.\right.\right. \\ &\left.\left.\left.+\left|1\right\rangle\left\langle 1\right|_1\left[\left|0\right\rangle\left\langle 1\right|_2 C_3+\left|1\right\rangle\left\langle 0\right|_2 D_3\right]\right]+H.c.\right]\right\}.\end{aligned}$$

20) R_9^2:

$$\begin{aligned}\rho_{20} &= 2^{-4}\left\{I^{\otimes 4}+\left[\alpha\left|0\right\rangle\left\langle 1\right|_0\left[\left|0\right\rangle\left\langle 0\right|_1\left[e^{-i\theta_9}\left|0\right\rangle\left\langle 1\right|_2 A_3+e^{i\theta_9}\left|1\right\rangle\left\langle 0\right|_2 B_3\right]\right.\right.\right. \\ &\left.\left.\left.+\left|1\right\rangle\left\langle 1\right|_1\left[e^{-i\theta_9}\left|0\right\rangle\left\langle 1\right|_2 C_3+e^{i\theta_9}\left|1\right\rangle\left\langle 0\right|_2 D_3\right]\right]+H.c.\right]\right\}.\end{aligned}$$

21) $CNOT_1^2$:

$$\begin{aligned}\rho_{21} &= 2^{-4}\left\{I^{\otimes 4}+\left[\alpha\left|0\right\rangle\left\langle 1\right|_0\left[\left|0\right\rangle\left\langle 0\right|_1\left[e^{-i\theta_9}\left|0\right\rangle\left\langle 1\right|_2 A_3+e^{i\theta_9}\left|1\right\rangle\left\langle 0\right|_2 B_3\right]\right.\right.\right.\\ &\left.\left.\left.+\left|1\right\rangle\left\langle 1\right|_1\left[e^{-i\theta_9}\left|1\right\rangle\left\langle 0\right|_2 C_3+e^{i\theta_9}\left|0\right\rangle\left\langle 1\right|_2 D_3\right]\right]+H.c.\right]\right\}.\end{aligned}$$

22) R_{10}^2:

$$\begin{aligned}\rho_{22} &= 2^{-4}\left\{I^{\otimes 4}+\left[\alpha\left|0\right\rangle\left\langle 1\right|_0\left[\left|0\right\rangle\left\langle 0\right|_1\left[e^{-i(\theta_{10}+\theta_9)}\left|0\right\rangle\left\langle 1\right|_2 A_3+e^{i(\theta_{10}+\theta_9)}\left|1\right\rangle\left\langle 0\right|_2 B_3\right]\right.\right.\right.\\ &\left.\left.\left.+\left|1\right\rangle\left\langle 1\right|_1\left[e^{i(\theta_{10}-\theta_9)}\left|1\right\rangle\left\langle 0\right|_2 C_3+e^{-i(\theta_{10}-\theta_9)}\left|0\right\rangle\left\langle 1\right|_2 D_3\right]\right]+H.c.\right]\right\}.\end{aligned}$$

23) $CNOT_0^2$:

$$\begin{aligned}\rho_{23} &= 2^{-4}\left\{I^{\otimes 4}+\left[\alpha\left|0\right\rangle\left\langle 1\right|_0\left[\left|0\right\rangle\left\langle 0\right|_1\left[e^{-i(\theta_{10}+\theta_9)}\left|0\right\rangle\left\langle 0\right|_2 A_3+e^{i(\theta_{10}+\theta_9)}\left|1\right\rangle\left\langle 1\right|_2 B_3\right]\right.\right.\right.\\ &\left.\left.\left.+\left|1\right\rangle\left\langle 1\right|_1\left[e^{i(\theta_{10}-\theta_9)}\left|1\right\rangle\left\langle 1\right|_2 C_3+e^{-i(\theta_{10}-\theta_9)}\left|0\right\rangle\left\langle 0\right|_2 D_3\right]\right]+H.c.\right]\right\}.\end{aligned}$$

24) R_{11}^2:

$$\rho_{24}=\rho_{23}.$$

25) $CNOT_1^2$:

$$\begin{aligned}\rho_{25} &= 2^{-4}\left\{I^{\otimes 4}+\left[\alpha\left|0\right\rangle\left\langle 1\right|_0\left[\left|0\right\rangle\left\langle 0\right|_1\left[e^{-i(\theta_{10}+\theta_9)}\left|0\right\rangle\left\langle 0\right|_2 A_3+e^{i(\theta_{10}+\theta_9)}\left|1\right\rangle\left\langle 1\right|_2 B_3\right]\right.\right.\right.\\ &\left.\left.\left.+\left|1\right\rangle\left\langle 1\right|_1\left[e^{i(\theta_{10}-\theta_9)}\left|0\right\rangle\left\langle 0\right|_2 C_3+e^{-i(\theta_{10}-\theta_9)}\left|1\right\rangle\left\langle 1\right|_2 D_3\right]\right]+H.c.\right]\right\}.\end{aligned}$$

26) R_{12}^1:

$$\rho_{26}=\rho_{25}.$$

27) $CNOT_0^1$:

$$\begin{aligned}\rho_{27} &= 2^{-4}\left\{I^{\otimes 4}+\left[\alpha\left|0\right\rangle\left\langle 1\right|_0\left[\left|0\right\rangle\left\langle 1\right|_1\left[e^{-i(\theta_{10}+\theta_9)}\left|0\right\rangle\left\langle 0\right|_2 A_3+e^{i(\theta_{10}+\theta_9)}\left|1\right\rangle\left\langle 1\right|_2 B_3\right]\right.\right.\right.\\ &\left.\left.\left.+\left|1\right\rangle\left\langle 0\right|_1\left[e^{i(\theta_{10}-\theta_9)}\left|0\right\rangle\left\langle 0\right|_2 C_3+e^{-i(\theta_{10}-\theta_9)}\left|1\right\rangle\left\langle 1\right|_2 D_3\right]\right]+H.c.\right]\right\}.\end{aligned}$$

28) R_{13}^{1}:

$$\begin{aligned}\rho_{28} &= 2^{-4}\left\{I^{\otimes 4}+\left[\alpha\left|0\right\rangle\left\langle 1\right|_0\left[e^{-i\theta_{13}}\left|0\right\rangle\left\langle 1\right|_1\left[e^{-i(\theta_{10}+\theta_9)}\left|0\right\rangle\left\langle 0\right|_2 A_3+e^{i(\theta_{10}+\theta_9)}\left|1\right\rangle\left\langle 1\right|_2 B_3\right]\right.\right.\right.\\ &\left.\left.\left.+e^{i\theta_{13}}\left|1\right\rangle\left\langle 0\right|_1\left[e^{i(\theta_{10}-\theta_9)}\left|0\right\rangle\left\langle 0\right|_2 C_3+e^{-i(\theta_{10}-\theta_9)}\left|1\right\rangle\left\langle 1\right|_2 D_3\right]\right]+H.c.\right]\right\}.\end{aligned}$$

Este estado é claramente diagonal nos qbits 2 e 3, mas não é completamente diagonal nos qbits 0 e 1 para funções balanceadas. Portanto, as correlações no estado ρ_{28} podem apresentar alguma natureza quântica.

29) $CNOT_0^1$:

$$\begin{aligned}\rho_{29} &= 2^{-4}\left\{I^{\otimes 4}+\left[\alpha\left|0\right\rangle\left\langle 1\right|_0\left[e^{-i\theta_{13}}\left|0\right\rangle\left\langle 0\right|_1\left[e^{-i(\theta_{10}+\theta_9)}\left|0\right\rangle\left\langle 0\right|_2 A_3+e^{i(\theta_{10}+\theta_9)}\left|1\right\rangle\left\langle 1\right|_2 B_3\right]\right.\right.\right.\\ &\left.\left.\left.+e^{i\theta_{13}}\left|1\right\rangle\left\langle 1\right|_1\left[e^{i(\theta_{10}-\theta_9)}\left|0\right\rangle\left\langle 0\right|_2 C_3+e^{-i(\theta_{10}-\theta_9)}\left|1\right\rangle\left\langle 1\right|_2 D_3\right]\right]+H.c.\right]\right\}.\end{aligned}$$

A operação $CNOT_0^1$ faz com que o estado torne-se diagonal no qbit 1, além de já ser diagonal nos qbits 2 e 3. Agora, todos os estados do qbit 0 em cada termo da expressão do estado ρ_{29} admite a mesma base de maneira que as correlações neste estado são puramente clássicas para qualquer função constante ou balanceada.

30) $e^{i\Phi}R_{14}^{0}$:

$$\begin{aligned}\rho_{30} &= 2^{-4}\left\{I^{\otimes 4}\right.\\ &+\left[\alpha e^{-i\theta_{14}}\left|0\right\rangle\left\langle 1\right|_0\left[e^{-i\theta_{13}}\left|0\right\rangle\left\langle 0\right|_1\left[e^{-i(\theta_{10}+\theta_9)}\left|0\right\rangle\left\langle 0\right|_2 A_3+e^{i(\theta_{10}+\theta_9)}\left|1\right\rangle\left\langle 1\right|_2 B_3\right]\right.\right.\\ &\left.\left.\left.+e^{i\theta_{13}}\left|1\right\rangle\left\langle 1\right|_1\left[e^{i(\theta_{10}-\theta_9)}\left|0\right\rangle\left\langle 0\right|_2 C_3+e^{-i(\theta_{10}-\theta_9)}\left|1\right\rangle\left\langle 1\right|_2 D_3\right]\right]+H.c.\right]\right\}.\end{aligned}$$

A aplicação desta última operação não gera qualquer correlação no estado final do sistema, como é descrito no texto principal.

Capítulo 4

Proposta de implementação de algoritmos quânticos através do modelo DQC1 em sistemas ópticos

Em geral, realizar computação quântica com estados puros envolve a capacidade de proteger o estado do sistema de forma que a interação com o meio externo não leve a computação a resultados infestados por erros. Uma maneira de se atingir essa aspiração é utilizar protocolos de correção de erros, com a aplicação de operações que resultem em uma compensação do erro produzido pela interação com o meio ambiente na evolução do estado do sistema [119–122]. Uma outra maneira de se contornar o problema é formular maneiras de realizar computação que utilizem a dinâmica decoerente como uma parte ativa no processo, por exemplo, utilizando proteção de estados em subespaços livres de decoerência [109, 123–126]. De certa forma o modelo DQC1 contorna estes problemas em alguma extensão ao utilizar um conjunto de qbits que, em quase sua totalidade, são inicializados no estado maximamente misto. Do ponto de vista experimental, um dos sistemas mais indicados para realizar computação com baixos níveis de interação com o meio é encontrado no campo da óptica, visto que as propriedades dos fótons dificilmente são alteradas a não ser pela interação com os próprios instrumentos do laboratório. Reunindo estes elementos, propomos neste capítulo uma maneira de realizar computação com um sistema óptico com base na utilização de fótons gêmeos para preparação do sistema e codificação do estado de um conjunto de qbits no grau de liberdade transversal dos fótons. Especificaremos, ainda, os circuitos que realizam o algoritmo de Deutsch-Jozsa,

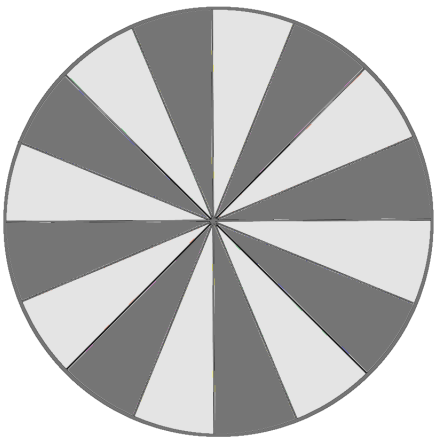

Figura 4.1: O perfil transversal de um feixe laser tem simetria rotacional em relação ao eixo de propagação, portanto, um particionamento do perfil transversal como apresentado gera um conjunto de regiões com intensidades idênticas.

de fatoração e o algoritmo de estimação do decaimento de fidelidade média. Além disso, apresentamos os resultados de um experimento realizado segundo a proposta de realização do algoritmo de Deutsch-Jozsa.

4.1 Sistema básico para computação

Para codificar os estados de um conjunto de n qbits no grau de liberdade transversal de um fóton, propomos a utilização de fótons oriundos de um laser. O perfil transversal de um feixe laser é gaussiano com relação à distância ao centro do feixe e tem simetria rotacional em relação ao eixo de propagação. Estes dois fatores resultam em um padrão de intensidade que é máximo no centro do feixe e decai exclusivamente com a distanciamento radial, independentemente, portanto, da "posição angular". Desta forma, se a seção transversal do laser for dividida conforme a Fig. 4.1 cada uma das partições terá a mesma área, ou seja, a intensidade em cada uma será idêntica, ou, de outra maneira, a taxa de incidência de fótons em cada uma dessas regiões será igual. Rotulando cada partição, poderíamos mapear cada uma como um estado transversal possível do sistema. A quantidade de partições, assim como sua forma e a identificação de cada uma pode ser definida de acordo com a computação específica.

Convencionalmente, uma fonte laser emite um número extremamente grande de fótons de forma simultânea. Como veremos na proposta a ser apresentada, a computação

será realizada com a utilização de apenas um fóton, enquanto o uso de um laser, na forma usual, corresponde à realização da computação DQC1 inúmeras vezes. A fim de possibilitar o acompanhamento da computação de forma mais individual, por exemplo com a capacidade de se rotular cada realização individualmente e atribuir um resultado específico a ela, é possível recorrer a formas de reduzir a quantidade de fótons. Isto pode ser obtido através da utilização de cristais não-lineares capazes de realizar conversão paramétrica descendente. Ao se propagar pelo cristal um fóton tem uma pequena chance de ser convertido em um par de fótons gêmeos, devido à resposta não-linear do meio [127]. O processo ocorre com conservação de energia e não há transferência de momento do fóton para o cristal. Dessa forma, as energias dos fótons gêmeos somadas correspondem à energia do fóton original e, mais importante para este trabalho, o momento transversal dos fótons gêmeos está anticorrelacionado. Isto indica que, uma vez que o fóton original tem momento transversal (aproximadamente) nulo, os fótons gêmeos terão momentos transversais opostos. Desta forma, o par de fótons gerado pelo processo é altamente correlacionado no momento linear. O processo de conversão paramétrica é bastante ineficiente, de forma que uma parcela ínfima dos fótons incidentes sobre o cristal darão origem a um par de fótons gêmeos. Isso permite a obtenção de fótons em pequenas quantidades, possibilitando a manipulação do estado desses entes físicos de forma "individualizada", o que, como veremos mais adiante neste capítulo, corresponde a uma única realização da computação DQC1 que discutiremos.

Como o momento é conservado no processo de conversão paramétrica descendente, incluso o momento transversal, os fótons gêmeos se propagam em direções transversais opostas (a Fig. 4.2 apresenta um esquema simplificado deste efeito). Outro fator importante é que o perfil transversal do laser é transferido para os fótons gêmeos, ou seja, o perfil do laser determina o espectro angular dos fótons gerados (o que descreve a distribuição dos vetores de onda transversal). Além disso, a conservação do momento transversal faz com que os fótons estejam anti-correlacionados no grau de liberdade transverso. Deste modo, se um dos fótons for detectado sem distinção quanto ao seu estado transverso, o outro fóton deve ser descrito por um estado misto.

Explicitamente, o estado dos fótons gêmeos assume a forma

$$|\Psi\rangle = \int d\overrightarrow{q}_s \int d\overrightarrow{q}_i \Phi(\overrightarrow{q}_s, \overrightarrow{q}_i) \, |1\overrightarrow{q}_s\rangle \, |1\overrightarrow{q}_i\rangle \,, \tag{4.1}$$

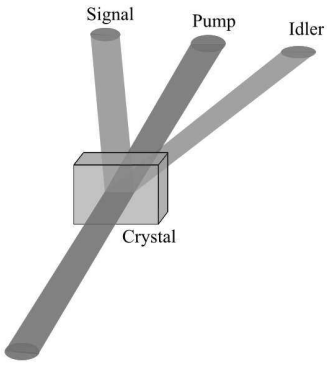

Figura 4.2: Na conversão paramétrica descendente, um feixe (pump) incide sobre um cristal não-linear, resultando em dois feixes, signal e idler. Como o momento linear total é conservado, tais feixes se propagam em direções opostas no plano perpendicular a direção de propagação do feixe laser (figura retirada da Ref. [127]).

onde i e s rotulam os fótons, convencionalmente denominados idler (i) e signal (s), $\overrightarrow{q}_k$ é o vetor de onda transversal do fóton k, $|1\overrightarrow{q}_k\rangle$ é o estado de um fóton k com momento transversal $\overrightarrow{q}_k$ e $\Phi(\overrightarrow{q}_s, \overrightarrow{q}_i)$ é a amplitude conjunta dos fótons gêmeos. Para um cristal fino, na aproximação paraxial (condição em que os fótons se propagam aproximadamente na direção normal aos elementos ópticos como o próprio cristal e lentes), esta amplitude pode ser aproximada por $\Phi(\overrightarrow{q}_s, \overrightarrow{q}_i) \approx v(\overrightarrow{q}_s + \overrightarrow{q}_i)$, sendo $v(\overrightarrow{q}) \propto e^{-W_0^2|\overrightarrow{q}|^2/4}$ o espectro angular do laser. Mantendo-se as aproximações anteriores e considerando-se que W_0, a cintura do feixe laser no cristal, é suficientemente grande, $\Phi(\overrightarrow{q}_s, \overrightarrow{q}_i)$ terá valores relevantes apenas para $\overrightarrow{q}_s + \overrightarrow{q}_i \approx 0$, ou seja $\overrightarrow{q}_i \approx -\overrightarrow{q}_s$. Desta forma, no caso extremo em que $W_0 \to \infty$ o estado dos fótons gerados por conversão paramétrica pode ser escrito como $|\Psi\rangle = \int d\overrightarrow{q}\, |1\overrightarrow{q}\rangle_s\, |-1\overrightarrow{q}\rangle_i$. A forma do estado indica claramente um alto nível de emaranhamento entre os dois fótons, além disso o espectro angular do estado marginal é uniforme, ou seja, todos os estados possíveis têm a mesma probabilidade de detecção. Como consequência, o estado marginal dos fótons é maximamente misto, o que é útil para a realização do algoritmo DQC1. Logo, é possível preparar o registro no estado misto necessário para o modelo DQC1 gerando-se um par de fótons por conversão paramétrica descendente e então detectar a presença do fóton idler de uma maneira em que não seja possível identificar seu estado na variável transversa. Ao realizar a detecção desta maneira, devido à distribuição uniforme no caso ideal discutido, a informação que se obtém é apenas uma confirmação da presença do fóton signal, mas nenhuma informação é obtida quanto ao estado transversal deste fóton. Isso corresponde a realizar o traço sobre o espaço de estados do fóton idler no operador densidade do sistema, o que leva a um estado marginal

misto do fóton signal, considerando-se as condições discutidas neste parágrafo.

O qbit de controle, por sua vez, pode ser mapeado na polarização do fóton. Isto é útil pelo fato de que existem formas de alterar o estado transverso do fóton condicionalmente ao estado de polarização. Um elemento que possibilita este feito é o divisor de feixe polarizado, pelo qual o fóton toma um caminho em função de seu estado de polarização, transmitindo fótons que possuem polarização paralela ao plano de incidência e refletindo fótons com polarização perpendicular a este plano. A operação controlada pode ser realizada, preparando-se o fóton num estado de superposição em sua polarização, através de um polarizador. Logo, ao passar pelo divisor de feixe polarizado, estando num estado de superposição na polarização, esta superposição se estende ao caminho tomado após o divisor de feixe. Colocando elementos ópticos para alterar o estado transverso do fóton em um dos caminhos, como lentes e prismas, e deixando o outro caminho livre, o que resulta na livre propagação do fóton neste caminho, realiza-se uma operação no estado transverso controlada pelo estado de polarização.

A utilização de um modulador espacial de luz também pode ser uma maneira simples e útil de aplicar operações controladas. Este elemento se trata de um painel, constituído por cristal líquido, o qual possui uma quantidade específica de pixels. O modulador tem a função de adicionar fases à frente de onda da luz incidente e o faz de maneira independente para cada pixel, ou seja, este elemento é capaz de inserir diferentes fases para diferentes regiões da frente de onda do laser. Isto se faz possível pelo envio de sinais elétricos a cada pixel originados por um software, o que altera as propriedades ópticas de cada pixel. Uma característica de grande valia deste dispositivo é que seu material ativo é birrefringente e, portante, não interage de forma idêntica com luz de polarizações distintas. Especificamente, os moduladores são projetados de forma que seja capaz de adicionar fases apenas à luz incidente polarizada horizontalmente não afetando luz incidente com polarização vertical. Por atuar de maneira condicionada ao estado de polarização da luz, este dispositivo é útil para realização de operações controladas.

Com embasamento nestas ideias iremos propor na sequência do capítulo formas de realizar três algoritmos formulados no modelo DQC1, os quais, em nosso entendimento, possuem poucas, ou nenhuma, realização experimental publicada. Primeiramente trataremos do algoritmo de Deutsch-Jozsa, o qual foi abordado no capítulo anterior, apresentando os resultados de uma realização experimental de acordo com o esquema

Figura 4.3: Circuito óptico para realização do algoritmo de Deutsch-Jozsa no modelo DQC1. O estado inicial é preparado pelo descarte de um dos fótons gêmeos gerados por conversão paramétrica descendente no cristal PDC pela incidência de um fóton gerado em S. A placa de meia onda HWP aplica a operação Hadamard sobre a polarização do fóton e o modulador espacial de luz SLM aplica a operação U que contém as informações da função sob estudo. A detecção em uma base específica em D finaliza o circuito.

proposto, em seguida abordaremos o algoritmo de fatoração, que tem origem no algoritmo de Shor, e por fim trataremos do algoritmo de estimação do decaimento de fidelidade média causado por pequenas alterações na evolução ideal de um sistema.

4.2 Algoritmo de Deutsch-Jozsa

O algoritmo de Deutsch-Jozsa pelo modelo DQC1 pode ser implementado em um sistema óptico de uma maneira suficientemente simples. O circuito óptico proposto para a implementação deste algoritmo é apresentado na Fig. 4.3. Uma pequena fração dos fótons gerados pela fonte laser S sofrem conversão paramétrica descendente no cristal PDC e o estado inicial é preparado descartando-se um dos fótons resultantes deste processo, como discutido no capítulo anterior. Em seguida o qbit controle codificado na polarização do fóton sofre a operação de Hadamard na placa de meia onda HWP. A operação unitária que contém a informação da função sob estudo é aplicada pelo modulador espacial de luz SLM. Como o SLM é ativo apenas para uma componente da polarização do fóton a operação é aplicada de forma controlada, ou seja, a aplicação da operação é condicionada ao estado da polarização do fóton. Finalizando o circuito, o resultado da computação é obtido pela detecção em uma base específica da polarização em D. Note-se que o algoritmo é realizado a cada par de fótons gerados por conversão paramétrica descendente, portanto, o algoritmo pode ser repetido em abundância considerando-se uma fonte laser, ainda que a taxa de conversão no cristal seja pequena.

Há que se notar que o problema de Deutsch-Jozsa pode ser reduzido ao problema de cálculo do traço de uma matriz. O modulador SLM, por sua vez, é capaz de implementar qualquer operação unitária representada por uma matriz diagonal com entradas de módulo

igual a um (a operação U do problema de Deutsch-Jozsa é um caso específico dessa classe de operações). Este é um fator favorável ao circuito proposto, haja vista que uma matriz unitária tem autovalores complexos de módulo unitário, isto é, sempre é possível escrever uma matriz unitária numa forma diagonal com entradas complexas de módulo igual a um para uma base específica. Esta propriedade, considerando-se que o estado dos qbits de trabalho utilizados no algoritmo é maximamente misto, e que este estado possui a mesma descrição em qualquer base, permite que o circuito apresentado na Fig. 4.3 calcule o traço de qualquer operação unitária. O traço de uma matriz, em geral, é um problema que não tem solução eficiente em computação clássica, mas que é solucionada de forma eficiente no circuito DQC1. Portanto, ainda que o algoritmo de Deutsch-Jozsa não tenha apresentado vantagens sobre a solução clássica, o circuito apresentado pode ser utilizado para obter vantagem computacional através do modelo DQC1.

A implementação experimental deste problema foi discutida com os pesquisadores do Laboratório de óptica Quântica do Instituto de Física da Universidade Federal do Rio de Janeiro. Os experimentos foram então conduzidos e os resultados, obtidos corroboraram a expectativa teórica [128]. No experimento foi usado um modulador espacial de luz com 256 valores possíveis de fase e 2073600 pixels, que equivale a um mapeamento dos graus de liberdade transversais dos fótons de aproximadamente 21 qbits. O esquema experimental utilizado é apresentado na Fig. 4.4. Pares de fótons gêmeos com comprimento de onda de 650 nm são gerados por conversão paramétrica descendente pela interação de fótons de comprimento de onda de 325 nm emitidos pelo laser de hélio-cádmio (He-Cd) com o cristal não-linear (BBO). O espelho dicroico (DM) separa os fótons gêmeos criados do feixe original emitido pelo laser. Após serem separados em um divisor de feixe (BS), um fóton do par de fótons gêmeos segue direto para um contador de fótons individuais (DET1) e o outro fóton sofre a ação do modulador espacial de luz (SLM), então passa por uma placa de quarto de onda ($\lambda/4$), uma placa de meia onda ($\lambda/2$) e um divisor de feixe polarizado (PBS) para fins de manipulação da polarização e em seguida é detectado em um contador de fótons individuais (DET2). Detecção de coincidência é realizada para certificar a presença do fóton no detector DET2 pela presença do outro fóton no detector DET1. Utilizando uma área de detecção grande no detector DET1 leva-se o outro fóton, a ser detectado em DET2, ao estado altamente misto necessário para o modelo DQC1. O conjunto de lentes (L1, L2 e L3) projeta os fótons de maneira adequada sobre o SLM e

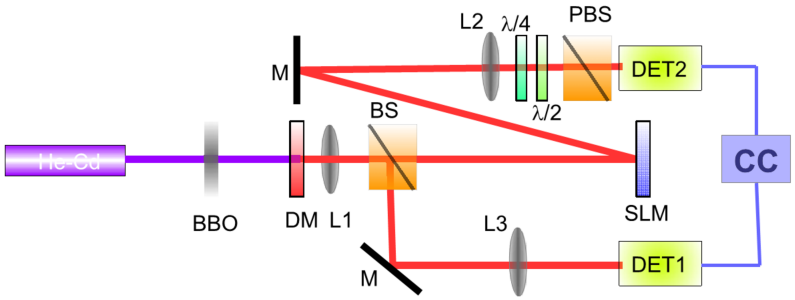

Figura 4.4: Esquema experimental para realização do algoritmo de Deutsch-Jozsa e para o cálculo normalizado do traço de matrizes pelo modelo computacional DQC1 (figura retirada da Ref. [128]). O aparato é composto por uma laser de hélio-cádmio (He-Cd), um cristal não-linear (BBO), um espelho dicroico (DM), um conjunto de lentes (L1, L2 e L3), um divisor de feixe de proporção 50:50 (BS), um modulador espacial de luz (SLM), espelhos (M), uma placa de quarto de onda ($\lambda/4$), uma placa de meia onda ($\lambda/2$), um divisor de feixe polarizado (PBS), módulos de contagem de fótons individuais (DET1 e DET2) e um circuito para medidas de coincidência (CC).

nos detectores.

A implementação do algoritmo de Deutsch-Jozsa apresentou erros pequenos. Os valores obtidos para o traço normalizado de funções balanceadas foram de 0.92 e -0.94, que são muito próximos dos valores ideais 1 e -1. Para funções balanceadas (que foram aplicadas através de um mapeamento randomizado no modulador) notou-se que a qualidade do resultado depende da dimensão das divisões da frente de onda. Para divisões correspondentes a uma quantidade de pixel maior o resultado se mostra mais apurado. Para a menor divisão testada (1 pixel) o resultado obtido foi 0.19, enquanto que para 5 pixels o valor foi -0.04 e para 10 pixels o resultado de -0.01 foi ainda mais próximo ideal, ou seja, do valor nulo. A dependência com a definição pode estar relacionada com efeito de difração, além disso, independentemente do mapeamento aplicado, a interação com o modulador leva a um efeito de defasagem na polarização do fóton, sobre a qual se define o qbit controle [129].

Além disso, também foram realizados experimentos para determinação do traço normalizado de matrizes com termos menos restritos, permitindo-se a aplicação de fases pelo modulador espacial entre os valores 0 e 2π. Neste caso, as entradas da matriz serão números complexos e, portanto, há o interesse do cálculo da parte real e imaginária do traço normalizado. Para este fim, o SLM foi programado para apresentar um padrão de fase que varia linearmente em uma direção. Definindo aqui essa direção como y esta função pode ser escrita como $\phi(x_i, y_i) = \phi_0 + (y_i/N)\phi_f$, onde (x_i, y_i) define a posição de um pixel no SLM, N = 1080 é a quantidade de pixeis na direção y e também na direção

x, i é um inteiro que varia de 1 até 1080 e ϕ_0 e ϕ_f são constantes a serem definidas arbitrariamente. O cálculo foi realizado para quatro casos diferentes, com valores obtidos experimentalmente concordando fortemente com os valores esperados teoricamente. Para $\phi_0 = 3\pi/4$ e $\phi_f = 3\pi/4$ os valores obtidos foram $\langle\sigma_x\rangle_{exp} = -0.811 \pm 0.005$ e $\langle\sigma_y\rangle_{exp} = 0.007 \pm 0.008$, enquanto os valores esperados teoricamente são $\langle\sigma_x\rangle_{teo} = -0.773$ e $\langle\sigma_y\rangle_{teo} = 0.008$. Para $\phi_0 = \pi$ e $\phi_f = 2\pi$ os valores são $\langle\sigma_x\rangle_{exp} = -0.039 \pm 0.008$ e $\langle\sigma_y\rangle_{exp} = -0.628 \pm 0.007$, com $\langle\sigma_x\rangle_{teo} = 0.002$ e $\langle\sigma_y\rangle_{teo} = 0.587$. No caso em que $\phi_0 = \pi/2$ e $\phi_f = 3\pi/2$ foram calculados $\langle\sigma_x\rangle_{exp} = -0.646 \pm 0.006$ e $\langle\sigma_y\rangle_{exp} = -0.034 \pm 0.008$, com $\langle\sigma_x\rangle_{teo} = -0.593$ e $\langle\sigma_y\rangle_{teo} = -0.009$. E para $\phi_0 = \pi/2$ e $\phi_f = \pi$ os valores experimentais são $\langle\sigma_x\rangle_{exp} = -0.579 \pm 0.007$ e $\langle\sigma_y\rangle_{exp} = 0.521 \pm 0.007$, com $\langle\sigma_x\rangle_{teo} = -0.548$ e $\langle\sigma_y\rangle_{teo} = 0.545$.

A pequena margem de erros apresentada nestes cálculos e também no problema de Deutsch-Jozsa indica que o esquema aqui proposto em um sistema ótico é apropriado para a realização de algoritmos no modelo DQC1 e encoraja uma futura implementação dos demais algoritmos abordados neste capítulo.

4.3 Algoritmo de fatoração

Com a popularização do uso da internet a troca de informação (e.g. mensagens) por vias não-materiais se tornou mais intensa. Empresas passaram a utilizar esse meio para realizar comércio, assim como bancos passaram a disponibilizar serviços online. Essas operações envolvem o envio de informações do usuário das quais este pode necessitar manter em segredo de outros indivíduos que não sejam os destinatários desejados. O uso de protocolos de criptografia é uma forma de proteger a informação de eventuais ataques realizados por terceiros a fim de interceptar a comunicação. O sistema de criptografia RSA é muito eficiente e, por isso, utilizado de forma abrangente. Neste protocolo a codificação e decodificação da informação está baseada na geração de um número grande por um produto de números primos e é a esse fator que se atribui a segurança da informação, pois a fatoração de um número é um problema que não tem solução eficiente por métodos clássicos. Todavia, Peter Shor desenvolveu um algoritmo para computação quântica que determina os fatores não triviais de um número de forma eficiente [3]. Este algoritmo já foi testado experimentalmente com sucesso para alguns números pequenos, abrindo o

caminho para que a criptografia RSA seja colocada em prova assim que os computadores quânticos possuam uma quantidade maior de qbits [19, 24, 25, 130, 131]. Este fato instiga o desenvolvimento de novos esquemas criptográficos que utilizem sistemas quânticos para combater ataques com poderios também quânticos. A seguir introduziremos o algoritmo de fatoração de Shor, reproduziremos então a modificação apresentada na ref. [56] para realizar a fatoração no modelo DQC1 e enfim propomos a realização deste algoritmo em um sistema óptico.

O algoritmo de fatoração de Shor

O algoritmo de Shor tem como finalidade encontrar os fatores primos p e q de um número inteiro $N = pq$ que pode ser descrito por $z = \lceil log_2 N \rceil$ bits. Este algoritmo realiza a tarefa de fatoração com $O(z^3)$ operações, enquanto não se conhece algoritmo clássico que realize a mesma tarefa com recursos polinomiais em z. Para introduzir a ideia do algoritmo tomemos o exemplo de fatoração do número $N = 15$. Seja um número inteiro positivo a qualquer, tal que $a < N$, por exemplo $a = 2$. Façamos agora a sucessiva potenciação de a por números inteiros. Temos um conjunto de valores $2^0 = 1$, $2^1 = 2$, $2^2 = 4$, $2^3 = 8$, $2^4 = 16$, $2^5 = 32$, $2^6 = 64$, $2^7 = 128$, $2^8 = 256$, $2^9 = 512$, $2^{10} = 1024$ e assim sucessivamente. Tomemos agora o resultado desta operação módulo $N = 15$. Isto é, o resultado que nos interessa é o resto da divisão do valor da potenciação por N (por exemplo, 11 (mod 9) = 2 visto que o resto da divisão 11/9 é igual a 2). Desta forma, a sequência calculada se torna 1, 2, 4, 8, 1, 2, 4, 8, 1, 2, 4 e continua neste padrão. Como se pode notar há a repetição de uma sequência base dos números 1, 2, 4 e 8. Esta sequência é composta por 4 números distintos e, deste modo, dizemos que a ordem de 2 módulo 15 é igual a 4. De maneira mais técnica, dados dois inteiros positivos sem fatores em comum, a e N tal que $a < N$, a ordem de a módulo N é definida como o menor número positivo, r, tal que $a^r = 1(\mathrm{mod} N)$.

A determinação da ordem r é de fundamental importância para o problema da fatoração. Se a é escolhido de maneira aleatória, há grande probabilidade de que a ordem r determinada seja par, de modo que os fatores de N podem ser obtidos calculando-se o máximo divisor comum $\mathrm{mdc}\left(a^{r/2} \pm 1, N\right)$. Por exemplo, se $N = 15$ e $a = 2$ a ordem será $r = 4$ como discutido anteriormente. Neste caso, os fatores de $N = 15$ serão exatamente $p = \mathrm{mdc}\left(a^{r/2} + 1, N\right) = \mathrm{mdc}\left(2^{4/2} + 1, 15\right) = \mathrm{mdc}\left(4 + 1, 15\right) = \mathrm{mdc}\left(5, 15\right) = 5$ e

$q = \text{mdc}\left(2^{4/2} - 1, 15\right) = \text{mdc}\left(4 - 1, 15\right) = \text{mdc}\left(3, 15\right) = 3$.

Como discutido, a tarefa de fatoração é baseada na rotina de determinação da ordem r de a módulo N. Isto é realizado aplicando-se uma operação do tipo $U\left|x\right\rangle = \left|ax(\text{mod}N)\right\rangle$. Os autoestados de U com autovalor $\exp\left[\frac{2\pi is}{r}\right]$têm a forma

$$\left|u_s\right\rangle = \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} \exp\left[\frac{-2\pi isk}{r}\right] \left|a^k \text{mod}N\right\rangle,$$

com $0 \leq s \leq r-1$. Desta forma a ordem r pode ser estimada diretamente da fase adquirida. A preparação do estado $\left|u_s\right\rangle$ exigiria o conhecimento prévio de r, que é a quantidade que deseja-se determinar. Uma forma de se evitar isso é preparar uma sobreposição de estados $\left|u_s\right\rangle$ com s variando de 0 a $r-1$, ou seja

$$\frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} \left|u_s\right\rangle.$$

Ao realizar esta soma cada termo $\left|a^k \text{mod}N\right\rangle$ estará acompanhado por um somatório em s de fases complexas que estão uniformemente distribuídas sobre o círculo trigonométrico. Este fato levará à anulação de todos os termos com $k \neq 0$, resultando em um estado $\left|a^0 \text{mod}N\right\rangle = \left|1\right\rangle = \left|00...001\right\rangle$. Logo, para executar o algoritmo deve-se preparar o estado

$$\frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} \left|u_s\right\rangle = \left|1\right\rangle.$$

Como descrito no início desta discussão, este estado exige um registro de $z = \lceil log_2 N \rceil$. Além disso, este procedimento exige um segundo registro com $l = 2z + 1 + \left\lceil \log\left(2 + \frac{1}{2\epsilon}\right) \right\rceil$ qbits inicializados no estado $\left|0\right\rangle$ para se obter a resposta correta com probabilidade $1 - \epsilon$. Sobre este segundo registro são realizadas uma medida sobre cada qbit, totalizando l medidas. Os resultados das medidas fornecem um estado $\left|c\right\rangle$, codificado na forma decimal. A partir desta informação é possível estimar a ordem r, dado que o valor $c/2^l$ é uma aproximação do valor s/r. Nos casos específicos analisados posteriormente, pode-se notar que a probabilidade de determinar o valor de r correto é grande e cresce à medida que o número l de qbits se eleva. O circuito responsável por esse procedimento, em condições levemente distintas das apresentadas aqui, será apresentado mais adiante no texto.

Este último passo de aproximação de frações é um procedimento clássico e é realizado

escrevendo-se a fração $c/2^l$ em sua forma continuada e então desprezando-se um ou mais termos dessa fração. Após este procedimento a rotina do algoritmo de Shor é concluída com um processo clássico adicional. Este último passo consiste no cálculo dos fatores através do máximo divisor comum mdc $\left(a^{r/2} \pm 1, N\right)$ e a seguinte verificação $N = pq$.

O algoritmo de fatoração para estados mistos

A quantidade de recursos necessários para a realização deste algoritmo pode ser reduzida, como demonstrado por Robert Griffiths e Chi-Sheng Niu, limitando-se o registro de leitura a apenas um qbit, através de reciclagem de qbit, pela utilização de informação clássica [132]. Para isso, as medidas que seriam realizadas sobre cada qbit do primeiro registro, são realizadas de maneira sucessiva sobre o qbit único, reinicializando-se o qbit após cada medida e aplicando-lhe uma rotação controlada cujo ângulo é dependente das medidas anteriores, o que exige feed-forwarding. Neste formato o algoritmo exige um registro de um qbit inicializado no estado $|0\rangle$ e um segundo registro de z qbits inicializado no estado $|1\rangle = |00...001\rangle$.

Baseados no novo formato do algoritmo de Shor, possibilitado pelo estudo de Griffiths e Niu, Stephen Parker e Martin Plenio mostraram que não é necessário iniciar o segundo registro de qbits em um estado puro para que o algoritmo seja eficiente [56]. Mantendo um qbit controle, a inicialização do segundo registro no estado maximamente misto $I/2^z$, em oposição ao estado puro $|1\rangle$, resulta em um circuito similar ao modelo computacional DQC1 capaz de solucionar o problema da fatoração. Isto é possível devido ao fato de que a aplicação repetida da operação U sobre cada estado $|x\rangle$ $(x = 0, 1, ..., N-1)$ gera uma sequência periódica, de forma análoga ao que ocorre no algoritmo original, de maneira que existe um $R(x)$ tal que $U^{R(x)}|x\rangle = |x\rangle$. Por exemplo, se $a = 2$ e $N = 15$, a aplicação repetida de U gera as seguintes sequências

$$|1\rangle \to |2\rangle \to |4\rangle \to |8\rangle \to |1\rangle$$
$$|3\rangle \to |6\rangle \to |12\rangle \to |9\rangle \to |3\rangle$$
$$|5\rangle \to |10\rangle \to |5\rangle$$
$$|7\rangle \to |14\rangle \to |13\rangle \to |11\rangle \to |7\rangle$$

A primeira sequência é a sequência utilizada no algoritmo de Shor original, que dá a ordem $r = 4$ de onde se obtém os valores $p = \text{mdc}\left(2^{4/2} + 1, 15\right) = \text{mdc}\,(5, 15) = 5$ e

$q = \text{mdc}\left(2^{4/2} - 1, 15\right) = \text{mdc}\left(3, 15\right) = 3$. A segunda e a quarta sequência apresentam a mesma ordem $r = 4$. Particularmente, dados os números N e a tal que a ordem é r, a maioria dos valores $0, 1, ..., N-1$ estarão contidas em sequências com a mesma ordem r obtida pela repetida aplicação de U sobre o estado inicial $|1\rangle$. Deste modo, cada sequência será similar à sequência observada no algoritmo original e, da mesma maneira que foram definidos os autoestados $|u_s\rangle$ de U no início do texto (autoestados referentes à sequência que possui o estado $|1\rangle$), é possível definir os autoestados para cada sequência i de ordem r_i. Como a preparação destes estados exige o conhecimento prévio de r_i, busca-se preparar uma combinação de autoestados para cada sequência. Porém, ainda assim, é necessário conhecer os estados que a operação unitária irá induzir para cada sequência. Para prevenir este problema, recorre-se ao fato de que os autoestados definidos em cada sequência são ortogonais entre si e, obviamente, estados pertencentes a diferentes sequências também são ortogonais. Portanto, o conjunto de autoestados de todas as sequências forma um conjunto ortogonal. Em vista disso, uma forma de se preparar um estado sem o conhecimento prévio das quantidades que se quer determinar é inicializar o segundo registro em um estado obtido pela mistura de todos os autoestados definidos para cada uma das sequências possíveis, com pesos idênticos, obtendo-se o estado maximamente misto $I/2^z$. O algoritmo, com o segundo registro preparado no estado maximamente misto, determina algum valor s_i/r_i de onde pode-se calcular o valor da ordem r_i, que tem grande probabilidade de ser igual à ordem correta r. A utilização do estado misto em substituição ao estado puro $|1\rangle$ causa um leve aumento no número de repetições necessárias para que o algoritmo determine a ordem com alta probabilidade, enquanto o algoritmo original de Shor exige $O\left(\text{loglog}r\right)$ repetições, o algoritmo com estado misto (e apenas um qbit no primeiro registro) exige $O\left(\frac{pq}{(p-1)(q-1)}\text{loglog}r\right)$ repetições. Note-se que à medida que o número $N = pq$ cresce, a quantidade de repetições do algoritmo misto se aproxima daquela do algoritmo original. Mesmo para pequenos números esta carga extra não é significativa como, por exemplo, no caso em que $N = 15$ são necessárias aproximadamente o dobro de repetições do que no algoritmo original, uma vez que $\frac{pq}{(p-1)(q-1)} = 1,875$.

O circuito do algoritmo de fatoração com estados mistos é mostrado na figura 4.5. O qbit controle é inicializado no estado $\frac{|0\rangle+|1\rangle}{\sqrt{2}}$ enquanto o segundo registro, contendo z qbits, é inicializado no estado maximamente misto $I/2^z$. Após cada aplicação da operação controlada U^{2^j}, com j inteiro seguindo de $l-1$ a 0, o qbit controle sofre uma rotação R'_{l-j}

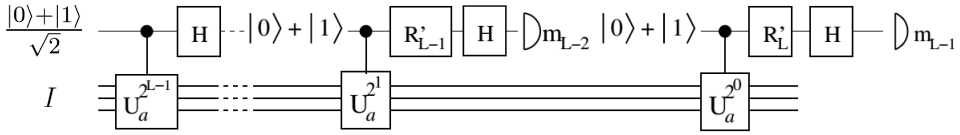

Figura 4.5: Circuito para o algoritmo de fatoração com estados mistos. As operações $R_p^{'} = \begin{pmatrix} 1 & 0 \\ 0 & \varphi_p^{'} \end{pmatrix}$ são rotações com ângulo $\varphi_p^{'} = \exp\left(-2\pi i \sum_{k=2}^{p} m_{p-k}/2^k\right)$. As operações H são portas de Hadamard e $U_a^{2^k}$ representa a k-ésima potência da operação U do algoritmo de fatoração, discutida no texto, para um valor específico de a. Figura retirada da Ref. [56]

e então é medido para fornecer um valor m_{l-1-j}. As rotações são definida por

$$R_h^{'} = \begin{pmatrix} 1 & 0 \\ 0 & \varphi_h^{'} \end{pmatrix} \tag{4.2}$$

onde o ângulo $\varphi_h^{'}$ depende dos resultados das medidas anteriores e é dado por $\varphi_h^{'} = \exp\left(-2\pi i \sum_{k=2}^{h} m_{h-k}/2^k\right)$. A quantidade de iterações l determina a precisão dos resultados, ou seja, a distribuição de valores obtida do conjunto de medidas, para um dado número de repetições do algoritmo, terá picos mais estreitos à medida que l se torna maior. A cada realização do algoritmo o conjunto de medidas fornecerá um valor $\frac{s_i}{r_i} = \sum_{j=0}^{l-1} m_j 2^{j-l}$, de onde pode-se apurar o valor r_i que é igual à ordem r com alta probabilidade.

O caso mais simples é o da fatoração do número $N = 15$ com uma ordem $r = 2$, que é encontrada selecionando-se, por exemplo, o número $a = 4$. Neste caso, procedendo pelo algoritmo de Shor original, a aplicação da operação $U|x\rangle = |4x(\text{mod}15)\rangle$ sobre o estado $|1\rangle$ leva ao estado $U|1\rangle = |4(\text{mod}15)\rangle = |4\rangle$ e a aplicação dupla da operação U leva ao estado $U^2|1\rangle = U(U|1\rangle) = U|4\rangle = |16(\text{mod}15)\rangle = |1\rangle$. Portanto, como esperado, a ordem para $a = 4$ é $r = 2$, o que permite o cálculo dos fatores $p = 3$ e $q = 5$. As

sequências possíveis para estes N e a são

$$|1\rangle \to |4\rangle \to |1\rangle$$
$$|2\rangle \to |8\rangle \to |2\rangle$$
$$|3\rangle \to |12\rangle \to |3\rangle$$
$$|5\rangle \to |5\rangle$$
$$|6\rangle \to |9\rangle \to |6\rangle$$
$$|7\rangle \to |13\rangle \to |7\rangle$$
$$|10\rangle \to |10\rangle$$
$$|11\rangle \to |14\rangle \to |11\rangle$$

além disso, ocorrem as sequências triviais $|10\rangle \to |10\rangle$ e $|15\rangle \to |15\rangle$. Como esperado, a maioria das sequências tem ordem $r_i = r = 2$.

Proposta experimental em um sistema óptico

Propomos aqui a realização experimental da fatoração do número $N = 15$ tomando $a = 4$ em um sistema óptico, tendo um conjunto de lentes como elemento principal. Como discutido anteriormente, isto pode ser feito mapeando-se os estados quânticos em regiões da frente de onda de um laser, como explicitado na figura 4.6.

Com os estados definidos dessa forma, as sequências de estados observadas no algoritmo de fatoração podem ser geradas pela atuação sucessiva de um conjunto de duas lentes biconvexas separadas pelo dobro da distância focal sobre o laser. Portanto, o conjunto de lentes realiza exatamente a operação U sobre o estado do segundo registro. A fatoração do número $N = 15$ é simplificada pelo fato de que sendo $U^{2^j} = I$ para todo $j > 0$, a única iteração de U necessária para a fatoração é $U^{2^0} = U$.

O estado do sistema necessário para a realização do algoritmo pode ser inicializado pela produção de fótons gêmeos, conforme discutido na seção 2.1. O estado de posição na frente de onda (ou momento transversal) de um dos fótons se aproxima da identidade, uma vez que se realiza o traço sobre os estados do outro fóton pela detecção sem sensibilidade ao momento transversal, de maneira que o segundo registro é inicializado corretamente. O estado de polarização do fóton utilizado efetivamente para a realização do algoritmo, que atuará como qbit controle, pode ser inicializado por meio de um placa de meia onda que realiza a porta de Hadamard. Divisores de feixe polarizadores aliados a placas de

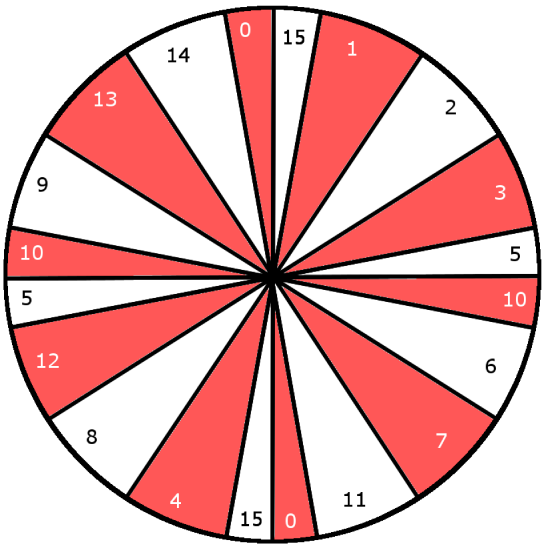

Figura 4.6: O mapeamento dos estados na frente de onda do laser apresentado, é apropriado para que a operação U do algoritmo de fatoração seja realizada por um conjunto de lentes. Idealmente, todos os estados ocupariam regiões da frente de onda com áreas iguais.

meia onda seriam responsáveis pela preparação do estado para as medidas.

O algoritmo de fatoração já foi realizado experimentalmente, pela versão de estados puros, para alguns valores de N, inclusive $N = 15$ [19, 24, 25, 130, 131]. Nestes trabalhos os circuitos são construídos especificamente para calcular os fatores de um dado N. Os trabalhos que fatoram $N = 15$ através de uma ordem $r = 2$, simplificam o circuito aproveitando-se do fato, apresentado anteriormente, de que $U^{2^j} = I$ para todo $j > 0$. Desta forma todas as operações U^{2^j} são removidas do circuito, exceto para o caso em que $j = 0$.

De acordo com o exposto até aqui, um circuito capaz de realizar a fatoração é apresentado na figura 4.7. Como a computação envolve apenas uma medida, o estado obtido da medida do qbit controle ao final da computação será $|0\rangle$ ou $|1\rangle$. Se o estado medido é o estado $|0\rangle$, calcula-se o valor $s_i/r_i \approx 0/2^1 = 0$ de onde não se pode extrair informação alguma sobre a ordem r. Esta situação é um erro inerente deste algoritmo de fatoração. Por outro lado, se o estado obtido é $|1\rangle$, calcula-se $s_i/r_i \approx 1/2^1 = 1/2$ e identifica-se $s_i = 1$ e $r_i = 2$, onde r_i tem alta probabilidade de ser igual a r. Para verificar o resultado calcula-se, tendo $a = 4$, $p = \text{mdc}\left(a^{r_i/2} + 1, N\right) = 5$ e $q = \text{mdc}\left(a^{r_i/2} - 1, N\right) = 3$. Como r_i fornece os fatores corretos, a ordem é dada por $r = r_i = 2$.

É possível mostrar que se o sistema é inicializado como exige o algoritmo, ou seja,

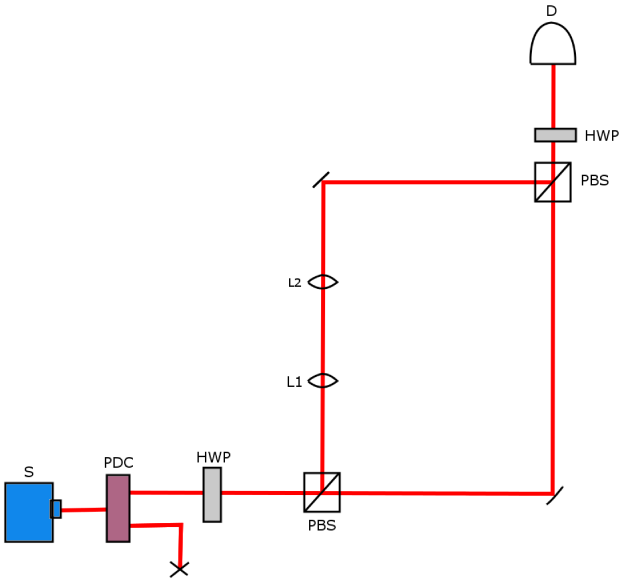

Figura 4.7: Circuito ótico para a implementação do algoritmo de fatoração por estados mistos. Os fótons gerados pela fonte S passam por um conversor paramétrico PDC de forma que é gerado um par de fótons em que um fóton é descartado e o outro efetivamente utilizado para a computação. O fóton, então no estado $|H\rangle$, passa por uma placa de meia onda HWP para criar o estado $|+\rangle$. O divisor de feixe polarizado PBS permite que a operação controlada U, aplicada pelas lentes $L1$ e $L2$, seja devidamente realizada. Por fim, os elementos PBS e HWP preparam o sistema para a realização da medida em D.

partindo do estado

$$\rho = |+\rangle\langle+| \otimes \frac{I}{2^4},$$

onde a primeira parte corresponde ao qbit controle e a segunda parte ao segundo registro, sendo $I = \sum_{k=0}^{15} |k\rangle\langle k|$, então, após a aplicação da operação controlada U e da porta de Hadamard o estado do qbit controle, se encontra no estado

$$\rho_c = \frac{3}{4}|0\rangle\langle 0| + \frac{1}{4}|1\rangle\langle 1|.$$

Isto indica que a cada repetição do algoritmo há uma chance de sucesso de 25%. Logo, com poucas repetições é possível obter a ordem $r = 2$, com a qual é possível calcular os fatores de $N = 15$. Na solução deste problema de fatoração a probabilidade de sucesso do algoritmo original em uma repetição é de 50%. A redução na probabilidade de sucesso é devida à utilização de estados mistos no segundo registro e exige um maior número de repetições.

Uma forma de elevar a precisão da resposta, obtida através da distribuição de probabilidades para o estado final do qbit controle, baseia-se em utilizar mais iterações da

operação U, ou seja, considerar os valores $j > 1$. Neste caso, como descrito anteriormente, as operações serão $U^{2^j} = I$, de maneira que todas as medidas, exceto a última, sempre resultarão no estado $|0\rangle$. Particularmente, é possível mostrar que os ângulos de rotação, dependentes dos valores de medidas anteriores, sempre serão nulos, o que leva as operações de rotação $R'_{l-j} = I$. Portanto, para o caso em estudo, não é necessário aplicar estas rotações, e, como consequência, feed-forwarding é desnecessário. Além disso, se são realizadas l iterações, como consequência do exposto agora, o estado do qbit controle antes de se realizar a última medida será, novamente, $\rho_c = \frac{3}{4}|0\rangle\langle 0| + \frac{1}{4}|1\rangle\langle 1|$ e o conjunto de medidas fornecerá o estado $|0\rangle$ com probabilidade $3/4$ e o estado $\left|2^{l-1}\right\rangle$ com probabilidade $1/4$. Como já discutido, a primeira situação está relacionada a um erro inerente ao algoritmo e a segunda fornecerá o valor $s_i/r_i \approx 2^{l-1}/2^l = 1/2$ de onde se pode obter a ordem $r = 2$. Portanto, neste caso, a expansão da dimensão do conjunto de valores obtidos do qbit controle pelas medidas não causam nenhum efeito na probabilidade de sucesso do algoritmo.

Por fim, enquanto a proposta experimental aqui apresentada tem por objetivo fatorar o número $N = 15$, é importante notar que para qualquer número N que se queira fatorar, para o qual existe um outro número a tal que a ordem seja $r = 2$, o circuito será o mesmo, sendo necessário, apenas, encontrar um mapeamento dos estados na frente de onda do laser que seja compatível com a solução do problema. Portanto, este esquema pode, por exemplo, fatorar o número $N = 35$ escolhendo-se apropriadamente $a = 6$.

Tomemos como um segundo exemplo, a fatoração do número $N = 21$, selecionando $a = 2$. Podemos observar melhor a precisão do resultado do algoritmo realizando mais iterações da operação U. A fim de obter um resultado preciso aplicaremos aqui cinco iterações e ao fim do processo será possível observar uma distribuição de resultados dos quais temos uma chance considerável de obter a ordem correta $r = 6$, ou algum de seus fatores ($r = 2$ ou $r = 3$).

O procedimento necessário para a realização deste caso pode ser obtido através de repetições de parte do esquema apresentado na Fig. 4.7. Após a última placa de meia onda (HWP) deve ser posicionado outro divisor de feixe polarizado (PBS), enviando as componentes $|H\rangle$ e $|V\rangle$ do qbit controle em direções diferentes. Então em cada braço o qbit deve ser reinicializado na superposição exigida $|+\rangle$, através de uma HWP com adição de alguns elementos ópticos se necessário. Então todo o circuito do primeiro PBS

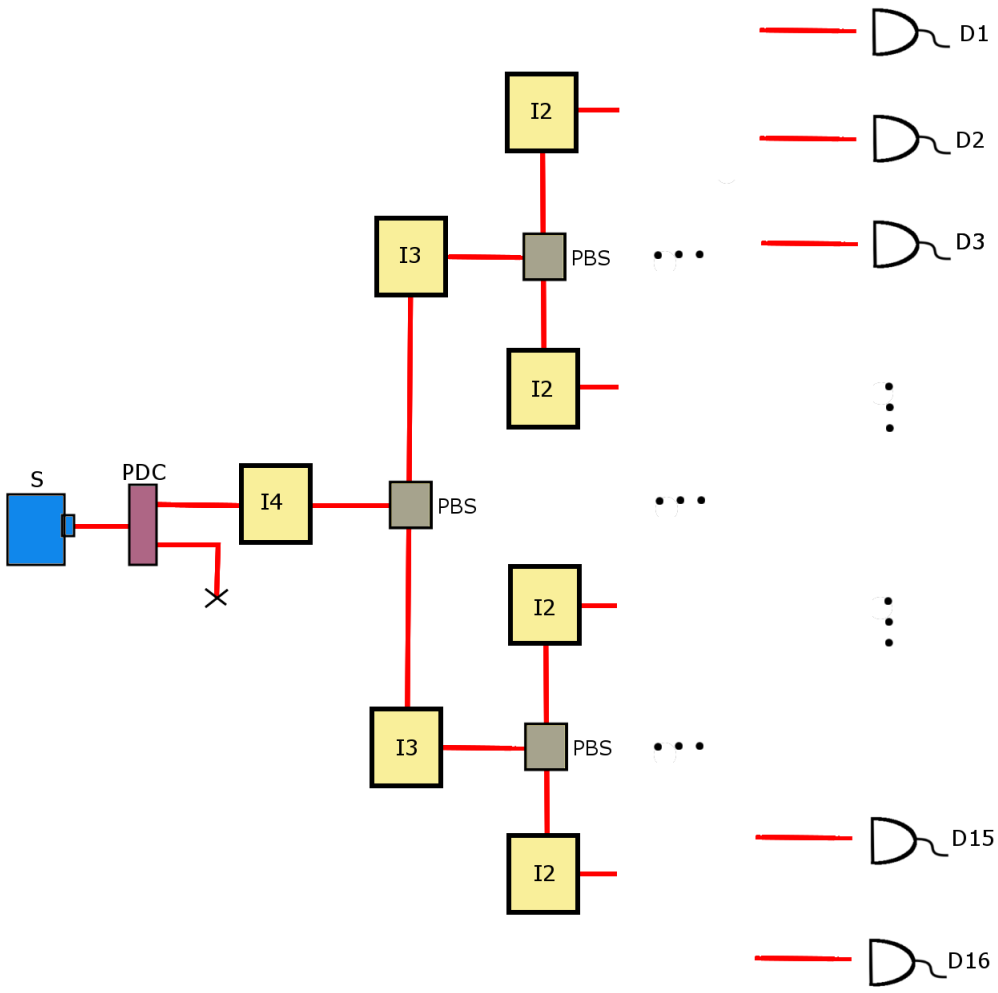

Figura 4.8: Circuito para implementação da fatoração do número $N = 21$, no caso em que $a = 2$. As caixas I_j reinicializam o qbit controle e aplicam a operação controlada U^{2^j}. Pelo conhecimento da chegada do fóton em um dos detectores e seu estado de polarização possibilita a rotulação em um estado da base computacional de um conjunto de 5 qbits.

ao segundo HWP na Fig. 4.7 deve ser construída em cada braço. Neste ponto, duas iterações terão sido realizadas. O processo é repetido em cada braço do circuito de acordo com o número de iterações desejadas. Com um mapeamento de estados nos moldes do que discutimos anteriormente a operação unitária necessária pode ser aplicada pela utilização de duas lentes cilíndricas posicionadas com os eixos direcionados de forma específica para rotacionar o estado transversal por um ângulo $2\pi/6 = \pi/3$. O esquema para realização desse processo é apresentado na Fig. 4.8. Nessa representação cada aplicação I_j trata-se do bloco de operações reproduzidas do circuito anterior discutidas acima, com o conjunto de lentes configurado para exercer a operação U^{2^j}, onde j é um inteiro entre 0 e 5.

Seguindo os procedimentos descritos, a distribuição de probabilidades para o estado

medido ao final da computação tem a forma apresentada na Fig. 4.9. À medida que o número de iterações aumenta a resolução da distribuição é aprimorada, de maneira que os picos ficam cada vez mais definidos e os outros elementos tendem a zero. Considerando a representação decimal do estado $|c\rangle$ medido resultante de l iterações (sendo $l = 5$ neste caso) a fração $c/2^l$ é uma aproximação de uma fração s_i/r_i, onde r_i é tem grandes chances de ser igual à ordem $r = 6$ ou às ordens $r = 2$ e $r = 3$ de outras sequências envolvidas neste problema que estão relacionadas com a ordem principal. Esses valores podem ser obtidos analisando-se a forma continuada da fração $c/2^l$. Especificamente, se o estado final medido é $|5\rangle$ ou $|27\rangle$, identifica-se corretamente a ordem $r = 6$, através das aproximações $5/32 \approx 1/6$ e $27/32 \approx 5/6$. Deste modo há uma probabilidade de aproximadamente $22,95$ % de que a ordem correta seja obtida em uma única realização do algoritmo. Há uma probabilidade de erro inerente a esse algoritmo que se dá pela obtenção $|0\rangle$ do qual não se pode inferir a ordem. No caso estudado esta probabilidade é de aproximadamente $16,80$ %. A probabilidade de se obter as ordens $r = 2$ e $r = 3$ das sequências secundárias é de $45,66$ %, através da medida dos estados $|10\rangle$, $|11\rangle$, $|16\rangle$, $|21\rangle$ e $|22\rangle$. Apesar de não representarem a ordem correta, se em duas repetições diferentes do algoritmo são obtidas as duas ordens o produto entre elas fornece o resultado correto. Isto é vantajoso pelo fato de que a verificação desse resultado não exige grandes esforços computacionais. Há ainda uma probabilidade menor, de $5,89$ %, de se obter os estados $|6\rangle$ e $|26\rangle$ que estão relacionados a uma ordem $r = 5$, que representa um erro evidente. Porém, como citado previamente nesta análise, estes últimos estados, assim como todos os outros não citados, tendem a ter uma probabilidade nula de serem medidos à medida que o numero de iterações aumenta.

Portanto, como visto neste último caso, um número maior de iterações permite uma probabilidade maior de acerto e uma distribuição de probabilidades com melhor resolução. Além disso, ainda que não seja possível garantir um resultado correto em apenas uma realização do algoritmo, pelas probabilidades envolvidas é possível notar que a ordem pode ser obtida em poucas repetições.

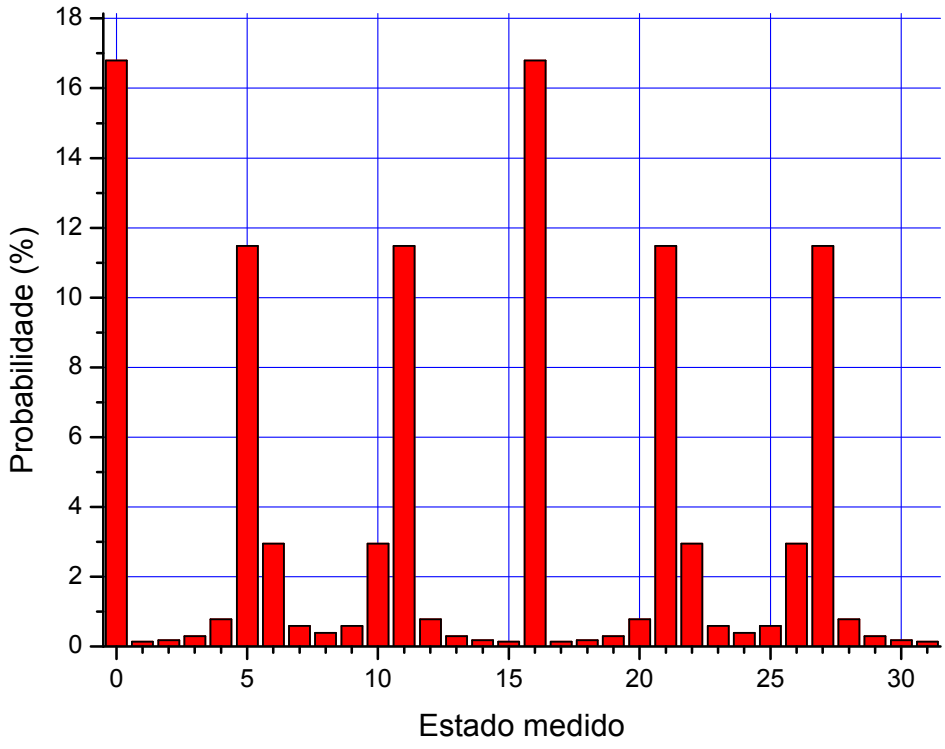

Figura 4.9: Distribuição de probabilidades para o resultado composto das medidas realizadas para fatoração do número $N = 21$, no caso em que $a = 2$.

4.4 Algoritmo de estimação de decaimento de fidelidade

A evolução de um sistema fechado por um período de tempo τ pode ser regida por um operador unitário U. Porém, isolar completamente um sistema da interação com outros sistemas é improvável de modo que, efetivamente, a evolução do sistema será definida por um operador U_p levemente diferente de U. Por consequência disso, o estado do sistema é diferente se a evolução se dá por U ou U_p. Uma forma de se quantificar a diferença do estado do sistema após evoluir por uma dinâmica regida por U ou U_p é calcular a fidelidade entre os estados finais. David Poulin e colaboradores desenvolveram uma maneira de calcular a fidelidade média após um período de evolução através do modelo computacional DQC1 [5]. Isto é, calcula-se a fidelidade do estado final do sistema para um conjunto de estados iniciais diferentes com o que se determina a fidelidade média. Em seu trabalho os autores consideram um operador perturbado específico do tipo $U_p = UP$, com $P = e^{-i\delta V}$ sendo δ pequeno e V uma matriz hermitiana A evolução do sistema durante algum tempo

equivale a uma sequência de aplicações do operador U, ou U_p, n vezes, para algum inteiro n. Logo, sendo $|\psi\rangle$ o estado inicial a fidelidade após um período de evolução é definida por

$$F_n(\psi) = \left| \langle\psi| (U^n)^\dagger U_p^n |\psi\rangle \right|^2 .$$

O decaimento da fidelidade pode indicar algumas características da dinâmica do sistema (como a sensibilidade a pequenas variações de parâmetros), portanto, determinar o padrão de decaimento pode revelar informações valiosas. Como a fidelidade pode apresentar flutuações significativas com a evolução temporal deve-se realizar uma média sobre diferentes estados iniciais. O cálculo da fidelidade por meios clássicos é difícil, visto que está ligado diretamente ao cálculo do traço de uma matriz, situação que é agravada pela necessidade de uma média sobre diferentes estados. No artigo citado anteriormente os autores afirmam que o algoritmo desenvolvido é eficiente ao calcular a fidelidade média de qualquer par de operadores U e U_p que possam ser implementados eficientemente. Ainda mais, mostram que o algoritmo fornece um ganho exponencial sobre os métodos clássicos.

A implementação no modelo DQC1 é possível pelo fato de que a fidelidade média entre as evoluções por U e U_p pode ser calculada pela expressão

$$\overline{F_n(\psi)} = \frac{\left| \mathrm{Tr}\left\{ (U^n)^\dagger U_p^n \right\} \right|^2 + N}{N^2 + N} \tag{4.3}$$

que envolve o traço de $(U^n)^\dagger U_p^n$. O traço normalizado de um operador pode ser eficientemente calculado pelo circuito DQC1, logo, a fidelidade média pode ser diretamente calculada por este modelo. A eficiência do algoritmo pode ser inferida pelo fato de que a equação anterior tem como termo central o cálculo do traço de uma matriz geral $(U^n)^\dagger U_p^n$ através do módulo quadrado do traço. A realização deste cálculo é uma tarefa computacionalmente difícil classicamente, enquanto é realizada de maneira eficiente pelo modelo DQC1. Deste modo é razoável afirmar que este algoritmo apresenta um ganho computacional como demonstrado no artigo da proposta original do algoritmo em DQC1.

Poulin e colaboradores mostram que o circuito necessário para a realização envolve uma sequência de aplicações controladas de P e não controladas de U, como exibe a figura 4.10. Em um sistema óptico um modulador espacial realiza exatamente uma operação P, ainda que simples. Pode-se notar isso atentando-se para o fato de que o modulador aplica

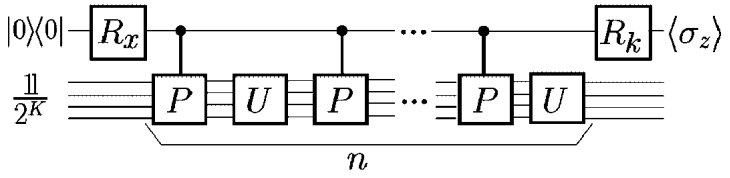

Figura 4.10: Circuito para calcular a fidelidade média entre estados que sofrem evolução por um operador U e $U_p = UP$. O cálculo exige um qbit controle inicializado em um estado puro e k qbits no registro de trabalho iniciados no estado maximamente misto. A rotação R_x gera um estado de superposição no qbit controle e a rotação final prepara o estado do sistema para a medida final. O circuito calcula a fidelidade média para um período de evolução correspondente a uma sequência de n aplicações das operações U e U_p. Figura retirada da Ref. [5].

fases $e^{i\varphi}$ a elementos diagonais da matriz densidade de um sistema, de modo que a matriz unitária correspondente é diagonal com estas fases nos termos correspondentes. Logo, pode-se identificar V como uma matriz hermitiana (especificamente real e diagonal) com fases reais φ nas entradas, de modo que $e^{-i\delta V}$ indica a aplicação do modulador espacial e δ atua como um limitador para os valores das fases. De forma oportuna, o modulador realiza essa operação de uma maneira controlada em relação ao estado de polarização do fóton, o que é necessário para a realização do algoritmo em DQC1.

Tendo a capacidade de realizar a perturbação P, deve-se escolher uma operação U para a qual se observará o decaimento médio de fidelidade. Revisitando um outro trabalho em que se propõe a realização do algoritmo de Shor via DQC1 em um sistema óptico, propõe-se uma operação U. Tomaremos uma operação do tipo $U = \sum_{i=0}^{N-1} |(i + N/2) \mathrm{mod} N\rangle \langle i|$(com $N = 2^k$, sendo k o número de qbits) que causa a transição entre dois estados diferentes do sistema. Esta operação pode ser realizada por um conjunto composto por duas lentes esféricas, idênticas, separadas pelo dobro da distância focal, levando um fóton em uma região da frente de onda para a região radialmente oposta e vice-versa. Um possível mapeamento dos estados na frente de onda do laser é apresentado na figura 4.11. Logo, tomando-se como qbit controle a polarização de um fóton e como qbits de trabalho a "posição" de um fóton na frente de onda podemos transcrever o algoritmo de cálculo da fidelidade média por DQC1 em um sistema óptico, como descrito na 4.12. O circuito proposto é capaz de calcular a fidelidade média para vários períodos de evolução diferentes, ou seja, para várias sequências de aplicações de U e U_p, cada uma com um número n de aplicações diferentes.

Para prever os resultados experimentais em casos simples, uma rotina computacional numérica foi desenvolvida simulando as operações envolvidas na proposta aqui realizada.

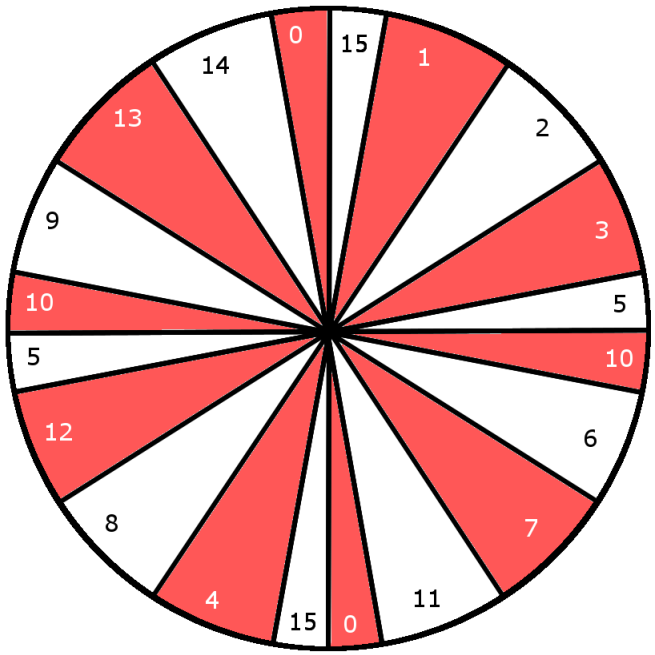

Figura 4.11: Um possível mapeamento de estados do sistema na frente de onda de um feixe laser. Um conjunto de lentes pode realizar uma operação que cause transições entre pares de estados como, por exemplo, $|0\rangle$ e $|8\rangle$ ou $|5\rangle$ e $|13\rangle$.

Esta rotina permite a seleção do número de qbits, gera fases aleatórias que compõem a perturbação e resulta em um gráfico em que cada ponto indica a fidelidade média após um dado número de aplicações de U e U_p. Alguns gráficos são apresentados na figura 4.13 e indicam, como esperado, um decaimento na fidelidade média à medida em que a sequência de aplicações de U e U_p progride. Um comportamento geral observado é um decréscimo da fidelidade média no início da curva seguido de uma estabilização com flutuações significativas. O número de qbits no registro de trabalho influencia no comportamento da curva, sendo que para um número maior de qbits o decréscimo inicial na fidelidade é mais acentuado além do fato de que o valor estável se torna menor assim como as flutuações são consideravelmente reduzidas. Uma possível causa para este padrão é o fato de que o aumento no número de qbits aumenta exponencialmente a dimensão do espaço de estados permitindo que a perturbação conduza o sistema a estados com características substancialmente diferentes do que ocorre no caso sem perturbação. Expressando de outra maneira, a possibilidade de que a dinâmica perturbada e a não perturbada gerem estados semelhantes se torna menor à medida que o espaço de estados

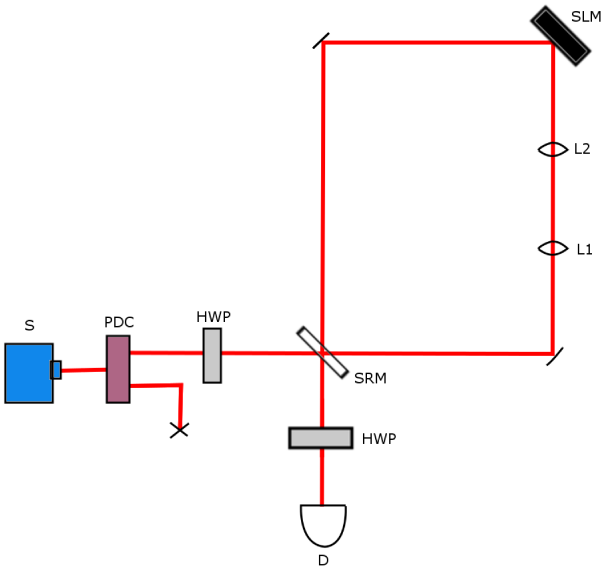

Figura 4.12: Circuito ótico para o cálculo da fidelidade média. Fótons gerados pela fonte S passam por um cristal (PDC) onde há a geração de fótons gêmeos. O descarte de um dos fótons permite que o fóton utilizado tenha um estado do grau de liberdade transversal próximo ao maximamente misto, como exigido pelo modelo DQC1. O qbit controle é codificado no estado de polarização do fóton. Após passar pela placa de meia onda (HWP), o que leva o estado de polarização a uma superposição, o fóton encontra um espelho semirrefletor (SRM). Se não for refletido ele irá passar pelo par de lentes $L1$ e $L2$ que realizam a operação U e então irá interagir com o modulador espacial (SLM) que aplicará a perturbação P. O fóton irá novamente passar pelo espelho semirrefletor e, em caso de transmissão, passará pela placa de meia onda que irá preparar o sistema para a medida. Se o fóton for refletido no espelho semirrefletor ele sofrerá mais uma evolução e assim por diante.

se expande.

O padrão do decaimento da fidelidade média é capaz de indicar se a evolução de um dado sistema se dá em um regime regular ou caótico. Alguns sistemas podem exibir regime regular e caótico dependendo de parâmetros específicos. A alteração do valor de tal parâmetro pode definir o tipo de regime a ser observado. Deste modo, o estudo do decaimento da fidelidade média é uma ferramenta valiosa para a caracterização das configurações de um sistema para que a evolução exiba um ou outro regime.

Um exemplo experimental pertinente ao trabalho aqui apresentado pode ser encontrado na Ref. [133]. Os autores investigam a evolução de um oscilador harmônico que é perturbado periodicamente por um impulso que pode ser modelado por uma função delta. As variáveis do oscilador são mapeadas nos graus de liberdade transversais de um laser (posição e momento) e a oscilação é produzida pela propagação do feixe por um conjunto de lentes. A perturbação por sua vez é produzida através de sucessivas reflexões da luz em um modulador espacial de luz. Considerando isto, o esquema apresentado no

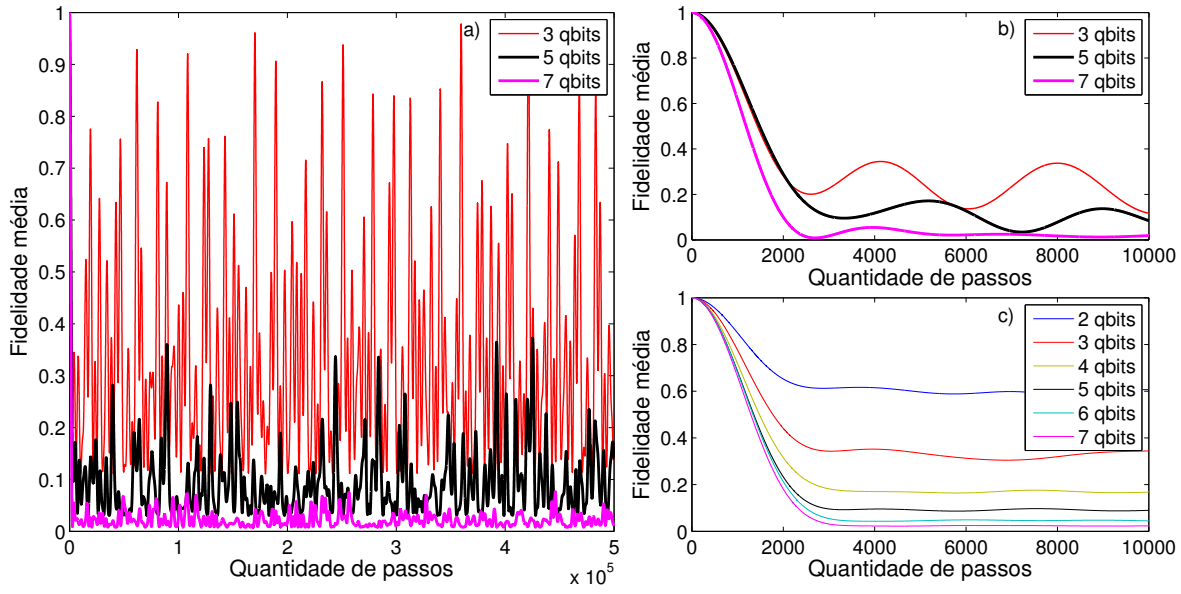

Figura 4.13: Simulações do decaimento da fidelidade média para diferentes números de qbits. Em a) são apresentadas as curvas de fidelidade média em função do número de aplicações das operações U e U_p para uma perturbação aleatória. Em b) apresenta-se a porção inicial da evolução das curvas em a). Em c) são apresentadas curvas de fidelidade média para vários números de qbits resultantes de uma média sobre 100 perturbações aleatórias.

referido artigo pode ser levemente alterado para se adaptar ao modelo DQC1, calculando o decaimento de fidelidade média através de medidas sobre o qbit controle codificado na polarização do fóton.

Como apresentado na equação 4.3 a fidelidade média calculada pelo algoritmo DQC1 depende explicitamente do traço do produto entre os operadores $(U^n)^\dagger$ e U_P^n e da dimensão N do espaço de Hilbert do registro misto. Lembrando que o circuito DQC1 apresentado na Fig. 4.10 calcula o traço normalizado $\Lambda = Tr[(U^n)^\dagger U_P^n]/N$ podemos manipular essa equação para obter

$$\overline{F_n}\left(1+\frac{1}{N}\right)-\frac{1}{N}=|\Lambda|^2 \tag{4.4}$$

É oportuno observar que o referido trabalho é desenvolvido sobre variáveis contínuas. Desta forma, é apropriado trabalhar no limite $N \to \infty$, o que leva à identidade $\overline{F_n} = |\Lambda|^2$ [134–136]. Este resultado indica que o resultado da computação permite o cálculo direto da fidelidade média após n iterações do mapa de evolução. Realizamos uma simulação da evolução do sistema, apresentada na Fig. 4.14, em que se pode notar o forte padrão decrescente de um caso em que o sistema se comporta de maneira caótica.

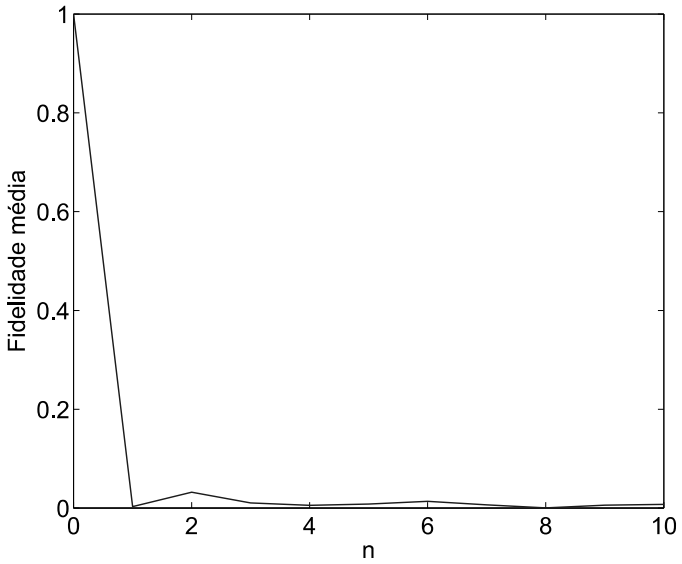

Figura 4.14: Simulação do decaimento da fidelidade média para o oscilador harmônico perturbado periodicamente por uma função tipo delta.

4.5 Conclusão

Propomos um circuito óptico para a realização deste algoritmo que pode ser também utilizado para realizar o cálculo do traço de uma matriz unitária qualquer. Destaca-se que este último problema representa um ganho computacional em relação à solução clássica. Estes experimentos foram realizados no Laboratório de óptica Quântica da UFRJ e os resultados obtidos estão em conformidade com a teoria.

O modelo computacional DQC1 foi elaborado tendo como uma das motivações os estados naturais com os quais se trabalha em experimentos de RMN. Neste capítulo apresentamos um procedimento que permite trabalhar com este modelo computacional em um sistema óptico, codificando o qbit controle na polarização de um fóton e codificando os qbits mistos na variável de momento transversal. Com a preparação do estado inicial padronizado, propomos maneiras de se realizar os algoritmos de Deutsch-Jozsa, fatoração e de estimação do decaimento da fidelidade média com circuitos ópticos simples. A realização experimental destas propostas poderá fornecer mais confirmações do poder da computação quântica, de maneira mais específica, computação quântica com estados mistos.

Destacamos que o circuito óptico para a realização do algoritmo de Deutsch-Jozsa também pode ser utilizado para realizar o cálculo do traço de uma matriz unitária qualquer. Este fato é importante visto que este último problema representa um ganho

computacional em relação à solução clássica. De fato, estes experimentos foram realizados no Laboratório de Óptica Quântica da UFRJ e os resultados obtidos apresentaram grande similaridade aos valores fornecidos pela teoria.

Capítulo 5

Conclusões e perspectivas

A computação quântica pode representar um avanço inestimável na solução de alguns problemas insolúveis. Alguns destes problemas podem ser tratados pelo modelo computacional DQC1 que trabalho com sistemas quânticos com estados mistos. Considerando a relevância desse modelo tratamos, nesta tese, alguns aspectos relacionados a ele. Argumenta-se que o ganho computacional observado nesse modelo possa ser devido às correlações quânticas presentes no estado do sistema, o que nos levou também a estudar esta propriedade em algumas situações.

Observamos, aqui, que dois pontos quânticos, que não interagem diretamente entre si, inseridos em uma nanocavidade óptica em comum, trocando excitações com um mesmo modo dessa cavidade, apresentam correlações quânticas, calculadas pela discórdia quântica. Isto ocorre mesmo que haja canais de decoerência sobre os elementos. Estudando o efeito desses canais sobre a geração da discórdia quântica observamos que, considerando-se este efeito inevitável, tais canais não têm um papel unicamente destrutivo, mas que podem, de certa forma, auxiliar na formação de correlações quânticas. Ainda, para maximizar o valor dessa propriedade é necessário que este sistema seja desenvolvido a fim de que os valores dos parâmetros desejáveis para este fim sejam atingidos. Além disso, a atuação de bombeios clássicos, como a aplicação de campos laser, podem ser nocivos à geração de correlações quânticas no sistema, fazendo com que o estado do sistema evolua para uma forma bem próxima à do estado maximamente misto. Propomos, também, a realização de uma testemunha de classicalidade neste sistema, apoiando-nos na evolução das técnicas de observação óptica, o que possibilita a verificação da natureza quântica do estado do sistema, evitando processos bem mais trabalhosos para calcular quantificadores

como a discórdia quântica.

Estudamos como as correlações quânticas estão presentes na realização do algoritmo de Deutsch-Jozsa pelo modelo DQC1. Notamos, por uma análise que é geral em relação à função a qual se quer definir a classe, que essas correlações podem ser geradas ao longo do algoritmo e que estas correlações são consumidas posteriormente. Apesar deste comportamento, efetivamente, esta solução quântica não é mais eficiente do que a clássica, o que indica que geração e consumo de correlações quânticas por si só não é um fator capaz de gerar um ganho computacional. Portanto, é provável que existam condições específicas, ou fatores adicionais, para que tal geração e consumo resultem em uma vantagem observável.

Apresentamos a ideia de utilizar as variáveis transversais dos fótons gerados por um laser, e também sua polarização, para realizar computação pelo modelo DQC1, tirando proveito da forma do estado dos fótons gêmeos gerados por conversão paramétrica descendente. Propomos a realização dos algoritmos de Deutsch-Jozsa, de fatoração e da estimação de decaimento de fidelidade média neste cenário. A utilização de sistemas ópticos é vantajosa pelo grande conhecimento técnico e pelo controle experimental que se tem com os elementos envolvidos, além do fato de estar relacionado a codificações de qbits resistentes a decoerência.

Particularmente, como o problema de Deutsch-Jozsa pode ser reduzido ao problema de cálculo do traço, acabamos por mostrar, também, como o cálculo do traço de uma matriz pode ser realizado no modelo DQC1 no sistema adotado. O cálculo do traço de uma matriz pelo modelo DQC1 é mais eficiente do que no modelo convencional, portanto, a realização experimental deste algoritmo pode contribuir a ressaltar o ganho computacional envolvido ao se utilizar sistemas quânticos. Os experimentos foram realizados pelos pesquisadores do Laboratório de Óptica Quântica da UFRJ e os resultados indicam que a vantagem computacional é real.

A quantidade de propostas experimentais para a realização de outros algoritmos no modelo DQC1 em sistemas ópticos deve ser expandida futuramente. Esperamos que estes algoritmos, juntamente aos de fatoração e estimação de decaimento da fidelidade média, sejam colocados a prova para que seja confirmada o ganho computacional da computação quântica e, especificamente, do modelo DQC1.

Referências Bibliográficas

1 FEYNMAN, R. Simulating physics with computers. *International Journal of Theoretical Physics*, Kluwer Academic Publishers-Plenum Publishers, v. 21, n. 6-7, p. 467–488, 1982. ISSN 0020-7748. Disponível em: ⟨http://dx.doi.org/10.1007/BF02650179⟩.

2 DEUTSCH, D.; JOZSA, R. Rapid solution of problems by quantum computation. *Proceedings of the Royal Society of London. Series A: Mathematical and Physical Sciences*, v. 439, n. 1907, p. 553–558, 1992. Disponível em: ⟨http://rspa.royalsocietypublishing.org/content/439/1907/553.abstract⟩.

3 SHOR, P. Algorithms for quantum computation: discrete logarithms and factoring. In: *Foundations of Computer Science, 1994 Proceedings., 35th Annual Symposium on*. [S.l.: s.n.], 1994. p. 124–134.

4 GROVER, L. K. Quantum mechanics helps in searching for a needle in a haystack. *Phys. Rev. Lett.*, American Physical Society, v. 79, p. 325–328, Jul 1997. Disponível em: ⟨http://link.aps.org/doi/10.1103/PhysRevLett.79.325⟩.

5 POULIN, D. et al. Exponential speedup with a single bit of quantum information: Measuring the average fidelity decay. *Phys. Rev. Lett.*, American Physical Society, v. 92, p. 177906, Apr 2004. Disponível em: ⟨http://link.aps.org/doi/10.1103/PhysRevLett.92.177906⟩.

6 JORDAN, S.; SHOR, P. W. Estimating jones polynomials is a complete problem for one clean qubit. *Quantum Inf, Comput.*, v. 8, p. 681, 2008.

7 JOZSA, R.; LINDEN, N. On the role of entanglement in quantum-computational speed-up. *Proceedings of the Royal Society of London. Series A: Mathematical, Physical and Engineering Sciences*, v. 459, n. 2036, p. 2011–2032, 2003. Disponível em: ⟨http://rspa.royalsocietypublishing.org/content/459/2036/2011.abstract⟩.

8 DATTA, A.; SHAJI, A.; CAVES, C. M. Quantum discord and the power of one qubit. *Phys. Rev. Lett.*, American Physical Society, v. 100, p. 050502, Feb 2008. Disponível em: ⟨http://link.aps.org/doi/10.1103/PhysRevLett.100.050502⟩.

9 OLLIVIER, H.; ZUREK, W. H. Quantum discord: A measure of the quantumness of correlations. *Phys. Rev. Lett.*, American Physical Society, v. 88, p. 017901, Dec 2001. Disponível em: ⟨http://link.aps.org/doi/10.1103/PhysRevLett.88.017901⟩.

10 HENDERSON, L.; VEDRAL, V. Classical, quantum and total correlations. *Journal of Physics A: Mathematical and General*, v. 34, n. 35, p. 6899, 2001. Disponível em: ⟨http://stacks.iop.org/0305-4470/34/i=35/a=315⟩.

11 NIELSEN, M. A.; CHUANG, I. L. *Quantum computation and quantum information*. [S.l.]: Cambridge University Press, 2000.

12 CIRAC, J. I.; ZOLLER, P. Quantum computations with cold trapped ions. *Phys. Rev. Lett.*, American Physical Society, v. 74, p. 4091–4094, May 1995. Disponível em: ⟨http://link.aps.org/doi/10.1103/PhysRevLett.74.4091⟩.

13 GULDE, S. et al. Implementation of the Deutsch-Jozsa algorithm on an ion-trap quantum computer. *Nature*, Nature Publishing Group, v. 421, n. 6918, p. 48–50, jan. 2003. ISSN 0028-0836. Disponível em: ⟨http://dx.doi.org/10.1038/nature01336⟩.

14 ZÄHRINGER, F. et al. Realization of a quantum walk with one and two trapped ions. *Phys. Rev. Lett.*, American Physical Society, v. 104, p. 100503, Mar 2010. Disponível em: ⟨http://link.aps.org/doi/10.1103/PhysRevLett.104.100503⟩.

15 MONROE, C.; KIM, J. Scaling the ion trap quantum processor. *Science*, v. 339, n. 6124, p. 1164–1169, 2013. Disponível em: ⟨http://www.sciencemag.org/content/339/6124/1164.abstract⟩.

16 CHUANG, I. L. et al. Experimental realization of a quantum algorithm. *Nature*, v. 393, n. 6681, p. 143–146, maio 1998. ISSN 0028-0836. Disponível em: ⟨http://dx.doi.org/10.1038/30181⟩.

17 CHUANG, I. L.; GERSHENFELD, N.; KUBINEC, M. Experimental implementation of fast quantum searching. *Phys. Rev. Lett.*, American Physical Society, v. 80, p. 3408–3411, Apr 1998. Disponível em: ⟨http://link.aps.org/doi/10.1103/PhysRevLett.80.3408⟩.

18 JONES, J. A.; MOSCA, M. Implementation of a quantum algorithm on a nuclear magnetic resonance quantum computer. *The Journal of Chemical Physics*, v. 109, n. 5, p. 1648–1653, 1998. Disponível em: ⟨http://scitation.aip.org/content/aip/journal/jcp/109/5/10.1063/1.476739⟩.

19 VANDERSYPEN, L. M. K. et al. Experimental realization of Shor's quantum factoring algorithm using nuclear magnetic resonance. *Nature*, Nature Publishing Group, v. 414, n. 6866, p. 883–887, dez. 2001. ISSN 0028-0836. Disponível em: ⟨http://dx.doi.org/10.1038/414883a⟩.

20 JONES, J. A. Quantum computing with {NMR}. *Progress in Nuclear Magnetic Resonance Spectroscopy*, v. 59, n. 2, p. 91 – 120, 2011. ISSN 0079-6565. Disponível em: ⟨http://www.sciencedirect.com/science/article/pii/S0079656510001111⟩.

21 KNILL, E.; LAFLAMME, R.; MILBURN, G. J. A scheme for efficient quantum computation with linear optics. *Nature*, v. 409, n. 6816, p. 46–52, jan. 2001. ISSN 0028-0836. Disponível em: ⟨http://dx.doi.org/10.1038/35051009⟩.

22 WALTHER, P. et al. Experimental one-way quantum computing. *Nature*, v. 434, n. 7030, p. 169–176, mar. 2005. ISSN 0028-0836. Disponível em: ⟨http://dx.doi.org/10.1038/nature03347⟩.

23 KOK, P. et al. Linear optical quantum computing with photonic qubits. *Rev. Mod. Phys.*, American Physical Society, v. 79, p. 135–174, Jan 2007. Disponível em: ⟨http://link.aps.org/doi/10.1103/RevModPhys.79.135⟩.

24 LANYON, B. P. et al. Experimental demonstration of a compiled version of shor's algorithm with quantum entanglement. *Phys. Rev. Lett.*, American Physical Society, v. 99, p. 250505, Dec 2007. Disponível em: ⟨http://link.aps.org/doi/10.1103/PhysRevLett.99.250505⟩.

25 LU, C.-Y. et al. Demonstration of a compiled version of shor's quantum factoring algorithm using photonic qubits. *Phys. Rev. Lett.*, American Physical Society, v. 99, p. 250504, Dec 2007. Disponível em: ⟨http://link.aps.org/doi/10.1103/PhysRevLett.99.250504⟩.

26 PREVEDEL, R. et al. High-speed linear optics quantum computing using active feed-forward. *Nature*, Nature Publishing Group, v. 445, n. 7123, p. 65–69, jan. 2007. ISSN 0028-0836. Disponível em: ⟨http://dx.doi.org/10.1038/nature05346⟩.

27 BARZ, S. et al. Demonstration of blind quantum computing. *Science*, v. 335, n. 6066, p. 303–308, 2012. Disponível em: ⟨http://www.sciencemag.org/content/335/6066/303.abstract⟩.

28 BARZ, S. Quantum computing with photons: introduction to the circuit model, the one-way quantum computer, and the fundamental principles of photonic experiments. *Journal of Physics B: Atomic, Molecular and Optical Physics*, v. 48, n. 8, p. 083001, 2015. Disponível em: ⟨http://stacks.iop.org/0953-4075/48/i=8/a=083001⟩.

29 CLARKE, J.; WILHELM, F. K. Superconducting quantum bits. *Nature*, Nature Publishing Group, v. 453, n. 7198, p. 1031–1042, jun. 2008. ISSN 0028-0836. Disponível em: ⟨http://dx.doi.org/10.1038/nature07128⟩.

30 DICARLO, L. et al. Demonstration of two-qubit algorithms with a superconducting quantum processor. *Nature*, Macmillan Publishers Limited. All rights reserved, v. 460, n. 7252, p. 240–244, jul. 2009. ISSN 0028-0836. Disponível em: ⟨http://dx.doi.org/10.1038/nature08121⟩.

31 SIDDIQI, I. Superconducting qubits: poised for computing? *Superconductor Science and Technology*, v. 24, n. 9, p. 091002, 2011. Disponível em: ⟨http://stacks.iop.org/0953-2048/24/i=9/a=091002⟩.

32 CHEN, G. et al. Quantum dot computing gates. *International Journal of Quantum Information*, v. 04, n. 02, p. 233–296, 2006. Disponível em: ⟨http://www.worldscientific.com/doi/abs/10.1142/S0219749906001761⟩.

33 FUSHMAN, I. et al. Controlled phase shifts with a single quantum dot. *Science*, v. 320, n. 5877, p. 769–772, 2008. Disponível em: ⟨http://www.sciencemag.org/content/320/5877/769.abstract⟩.

34 LAUCHT, A. et al. Electrical control of spontaneous emission and strong coupling for a single quantum dot. *New Journal of Physics*, v. 11, n. 2, p. 023034, 2009. Disponível em: ⟨http://stacks.iop.org/1367-2630/11/i=2/a=023034⟩.

35 FARAON, A. et al. Integrated quantum optical networks based on quantum dots and photonic crystals. *New Journal of Physics*, v. 13, n. 5, p. 055025, 2011. Disponível em: ⟨http://stacks.iop.org/1367-2630/13/i=5/a=055025⟩.

36 DIVINCENZO, D. P. The physical implementation of quantum computation. *Fortschritte der Physik*, WILEY-VCH Verlag Berlin GmbH, v. 48, n. 9-11, p. 771–783, 2000. ISSN 1521-3978. Disponível em: ⟨http://dx.doi.org/10.1002/1521-3978(200009)48:9/11⟨771::AID-PROP771⟩3.0.CO;2-E⟩.

37 MOREAU, E. et al. Single-mode solid-state single photon source based on isolated quantum dots in pillar microcavities. *Applied Physics Letters*, v. 79, n. 18, p. 2865–2867, 2001. Disponível em: ⟨http://scitation.aip.org/content/aip/journal/apl/79/18/10.1063/1.1415346⟩.

38 KUHN, A.; HENNRICH, M.; REMPE, G. Deterministic single-photon source for distributed quantum networking. *Phys. Rev. Lett.*, American Physical Society, v. 89, p. 067901, Jul 2002. Disponível em: ⟨http://link.aps.org/doi/10.1103/PhysRevLett.89.067901⟩.

39 MCKEEVER, J. et al. Deterministic generation of single photons from one atom trapped in a cavity. *Science*, v. 303, n. 5666, p. 1992–1994, 2004. Disponível em: ⟨http://www.sciencemag.org/content/303/5666/1992.abstract⟩.

40 KELLER, M. et al. Continuous generation of single photons with controlled waveform in an ion-trap cavity system. *Nature*, v. 431, n. 7012, p. 1075–1078, out. 2004. Disponível em: ⟨http://dx.doi.org/10.1038/nature02961⟩.

41 REITHMAIER, J. P. et al. Strong coupling in a single quantum dot-semiconductor microcavity system. *Nature*, Nature Publishing Group, v. 432, n. 7014, p. 197–200, nov. 2004. ISSN 0028-0836. Disponível em: ⟨http://dx.doi.org/10.1038/nature02969⟩.

42 YOSHIE, T. et al. Vacuum rabi splitting with a single quantum dot in a photonic crystal nanocavity. *Nature*, Nature Publishing Group, v. 432, n. 7014, p. 200–203, nov. 2004. ISSN 0028-0836. Disponível em: ⟨http://dx.doi.org/10.1038/nature03119⟩.

43 BADOLATO, A. et al. Deterministic coupling of single quantum dots to single nanocavity modes. *Science*, v. 308, n. 5725, p. 1158–1161, 2005. Disponível em: ⟨http://www.sciencemag.org/content/308/5725/1158.abstract⟩.

44 HENNESSY, K. et al. Quantum nature of a strongly coupled single quantum dot-cavity system. *Nature*, Nature Publishing Group, v. 445, n. 7130, p. 896–899, fev. 2007. ISSN 0028-0836. Disponível em: ⟨http://dx.doi.org/10.1038/nature05586⟩.

45 MELET, R. et al. Resonant excitonic emission of a single quantum dot in the rabi regime. *Phys. Rev. B*, American Physical Society, v. 78, p. 073301, Aug 2008. Disponível em: ⟨http://link.aps.org/doi/10.1103/PhysRevB.78.073301⟩.

46 FARAON, A. et al. Dipole induced transparency inwaveguide coupled photonic crystalcavities. *Opt. Express*, OSA, v. 16, n. 16, p. 12154–12162, Aug 2008. Disponível em: ⟨http://www.opticsexpress.org/abstract.cfm?URI=oe-16-16-12154⟩.

47 DAKIC, B. et al. Quantum discord as resource for remote state preparation. *Nat Phys*, Nature Publishing Group, v. 8, n. 9, p. 666–670, set. 2012. Disponível em: ⟨http://dx.doi.org/10.1038/nphys2377⟩.

48 GU, M. et al. Observing the operational significance of discord consumption. *Nat Phys*, Nature Publishing Group, v. 8, n. 9, p. 671–675, set. 2012. Disponível em: ⟨http://dx.doi.org/10.1038/nphys2376⟩.

49 WILLIAMS, C. O. *Explorations in Quantum Computing*. [S.l.]: Springer-Verlag London Limited, 2011.

50 GOTTESMAN, D.; CHUANG, I. L. Demonstrating the viability of universal quantum computation using teleportation and single-qubit operations. *Nature*, Macmillian Magazines Ltd., v. 402, n. 6760, p. 390–393, nov. 1999. ISSN 0028-0836. Disponível em: ⟨http://dx.doi.org/10.1038/46503⟩.

51 RAUSSENDORF, R.; BRIEGEL, H. J. A one-way quantum computer. *Phys. Rev. Lett.*, American Physical Society, v. 86, p. 5188–5191, May 2001. Disponível em: ⟨http://link.aps.org/doi/10.1103/PhysRevLett.86.5188⟩.

52 BROADBENT, A.; FITZSIMONS, J.; KASHEFI, E. Universal blind quantum computation. In: *Foundations of Computer Science, 2009. FOCS '09. 50th Annual IEEE Symposium on*. [S.l.: s.n.], 2009. p. 517–526. ISSN 0272-5428.

53 FARHI, E. et al. A quantum adiabatic evolution algorithm applied to random instances of an np-complete problem. *Science*, v. 292, n. 5516, p. 472–475, 2001. Disponível em: ⟨http://www.sciencemag.org/content/292/5516/472.abstract⟩.

54 ROLAND, J.; CERF, N. J. Quantum search by local adiabatic evolution. *Phys. Rev. A*, American Physical Society, v. 65, p. 042308, Mar 2002. Disponível em: ⟨http://link.aps.org/doi/10.1103/PhysRevA.65.042308⟩.

55 KNILL, E.; LAFLAMME, R. Power of one bit of quantum information. *Phys. Rev. Lett.*, American Physical Society, v. 81, p. 5672–5675, Dec 1998. Disponível em: ⟨http://link.aps.org/doi/10.1103/PhysRevLett.81.5672⟩.

56 PARKER, S.; PLENIO, M. B. Efficient factorization with a single pure qubit and log$N$ mixed qubits. *Phys. Rev. Lett.*, American Physical Society, v. 85, p. 3049–3052, Oct 2000. Disponível em: ⟨http://link.aps.org/doi/10.1103/PhysRevLett.85.3049⟩.

57 SHOR, P. W.; JORDAN, S. P. Estimating Jones polynomials is a complete problem for one clean qubit. *Quantum Information and Computation*, v. 8, p. 681+, fev. 2008. Disponível em: ⟨http://arxiv.org/abs/0707.2831v3⟩.

58 BOIXO, S.; SOMMA, R. D. Parameter estimation with mixed-state quantum computation. *Phys. Rev. A*, American Physical Society, v. 77, p. 052320, May 2008. Disponível em: ⟨http://link.aps.org/doi/10.1103/PhysRevA.77.052320⟩.

59 FAHMY, A. F. et al. Thermal equilibrium as an initial state for quantum computation by nmr. *Phys. Rev. A*, American Physical Society, v. 78, p. 022317, Aug 2008. Disponível em: ⟨http://link.aps.org/doi/10.1103/PhysRevA.78.022317⟩.

60 RYAN, C. A. et al. Characterization of complex quantum dynamics with a scalable nmr information processor. *Phys. Rev. Lett.*, American Physical Society, v. 95, p. 250502, Dec 2005. Disponível em: ⟨http://link.aps.org/doi/10.1103/PhysRevLett.95.250502⟩.

61 LANYON, B. P. et al. Experimental quantum computing without entanglement. *Phys. Rev. Lett.*, American Physical Society, v. 101, p. 200501, Nov 2008. Disponível em: ⟨http://link.aps.org/doi/10.1103/PhysRevLett.101.200501⟩.

62 PASSANTE, G. et al. Experimental approximation of the jones polynomial with one quantum bit. *Phys. Rev. Lett.*, American Physical Society, v. 103, p. 250501, Dec 2009. Disponível em: ⟨http://link.aps.org/doi/10.1103/PhysRevLett.103.250501⟩.

63 MOUSSA, O. et al. Testing contextuality on quantum ensembles with one clean qubit. *Phys. Rev. Lett.*, American Physical Society, v. 104, p. 160501, Apr 2010. Disponível em: ⟨http://link.aps.org/doi/10.1103/PhysRevLett.104.160501⟩.

64 MARX, R. et al. Nuclear-magnetic-resonance quantum calculations of the jones polynomial. *Phys. Rev. A*, American Physical Society, v. 81, p. 032319, Mar 2010. Disponível em: ⟨http://link.aps.org/doi/10.1103/PhysRevA.81.032319⟩.

65 PASSANTE, G.; MOUSSA, O.; LAFLAMME, R. Measuring geometric quantum discord using one bit of quantum information. *Phys. Rev. A*, American Physical Society, v. 85, p. 032325, Mar 2012. Disponível em: ⟨http://link.aps.org/doi/10.1103/PhysRevA.85.032325⟩.

66 DATTA, A. *Studies on the role of entanglement in mixed-state quantum computation.* Tese (Doutorado) — University of New Mexico, 2008.

67 NEST, M. Van den. Universal quantum computation with little entanglement. *Phys. Rev. Lett.*, American Physical Society, v. 110, p. 060504, Feb 2013. Disponível em: ⟨http://link.aps.org/doi/10.1103/PhysRevLett.110.060504⟩.

68 DATTA, A.; FLAMMIA, S. T.; CAVES, C. M. Entanglement and the power of one qubit. *Phys. Rev. A*, American Physical Society, v. 72, p. 042316, Oct 2005. Disponível em: ⟨http://link.aps.org/doi/10.1103/PhysRevA.72.042316⟩.

69 PIANI, M.; HORODECKI, P.; HORODECKI, R. No-local-broadcasting theorem for multipartite quantum correlations. *Phys. Rev. Lett.*, American Physical Society, v. 100, p. 090502, Mar 2008. Disponível em: ⟨http://link.aps.org/doi/10.1103/PhysRevLett.100.090502⟩.

70 VIDAL, G.; WERNER, R. F. Computable measure of entanglement. *Phys. Rev. A*, American Physical Society, v. 65, p. 032314, Feb 2002. Disponível em: ⟨http://link.aps.org/doi/10.1103/PhysRevA.65.032314⟩.

71 JIN, J. sen et al. Quantum discord induced by white noises. *J. Opt. Soc. Am. B*, OSA, v. 27, n. 9, p. 1799–1803, Sep 2010. Disponível em: ⟨http://josab.osa.org/abstract.cfm?URI=josab-27-9-1799⟩.

72 YUAN, J.-B.; KUANG, L.-M.; LIAO, J.-Q. Amplification of quantum discord between two uncoupled qubits in a common environment by phase decoherence. *Journal of Physics B: Atomic, Molecular and Optical Physics*, v. 43, n. 16, p. 165503, 2010. Disponível em: ⟨http://stacks.iop.org/0953-4075/43/i=16/a=165503⟩.

73 WANG, C. et al. Classical correlation, quantum discord and entanglement for two-qubit system subject to heat bath. *Optics Communications*, v. 284, n. 9, p. 2393

– 2401, 2011. ISSN 0030-4018. Disponível em: ⟨http://www.sciencedirect.com/science/article/pii/S0030401810013039⟩.

74 ZHANG, Y.-J. et al. Quantum discord dynamics in the presence of initial system-cavity correlations. *Journal of Physics B: Atomic, Molecular and Optical Physics*, v. 44, n. 3, p. 035503, 2011. Disponível em: ⟨http://stacks.iop.org/0953-4075/44/i=3/a=035503⟩.

75 EREMEEV, V.; MONTENEGRO, V.; ORSZAG, M. Thermally generated long-lived quantum correlations for two atoms trapped in fiber-coupled cavities. *Phys. Rev. A*, American Physical Society, v. 85, p. 032315, Mar 2012. Disponível em: ⟨http://link.aps.org/doi/10.1103/PhysRevA.85.032315⟩.

76 LI, J.-Q.; LIU, J.; LIANG, J.-Q. Environment-induced quantum correlations in a driven two-qubit system. *Physica Scripta*, v. 85, n. 6, p. 065008, 2012. Disponível em: ⟨http://stacks.iop.org/1402-4896/85/i=6/a=065008⟩.

77 LEONARD, D. et al. Direct formation of quantum-sized dots from uniform coherent islands of ingaas on gaas surfaces. *Applied Physics Letters*, v. 63, n. 23, p. 3203–3205, 1993. Disponível em: ⟨http://scitation.aip.org/content/aip/journal/apl/63/23/10.1063/1.110199⟩.

78 SKOLNICK, M.; MOWBRAY, D. Self-assembled semiconductor quantum dots: Fundamental physics and device applications. *Annual Review of Materials Research*, v. 34, n. 1, p. 181–218, 2004. Disponível em: ⟨http://dx.doi.org/10.1146/annurev.matsci.34.082103.133534⟩.

79 MICHLER, P. (Ed.). *Single Semiconductor Quantum Dots*. [S.l.]: Springer-Verlag Berlin Heidelberg, 2009.

80 VAHALA, K. J. Optical microcavities. *Nature*, Nature Publishing Group, v. 424, n. 6950, p. 839–846, ago. 2003. ISSN 0028-0836. Disponível em: ⟨http://dx.doi.org/10.1038/nature01939⟩.

81 REITZENSTEIN, S. Semiconductor quantum dot-microcavities for quantum optics in solid state. *Selected Topics in Quantum Electronics, IEEE Journal of*, v. 18, n. 6, p. 1733–1746, Nov 2012. ISSN 1077-260X.

82 PAINTER, O.; VUCKOVIC, J.; SCHERER, A. Defect modes of a two-dimensional photonic crystal in an optically thin dielectric slab. *J. Opt. Soc. Am. B*, OSA, v. 16, n. 2, p. 275–285, Feb 1999. Disponível em: ⟨http://josab.osa.org/abstract.cfm?URI=josab-16-2-275⟩.

83 AKAHANE, Y. et al. High-q photonic nanocavity in a two-dimensional photonic crystal. *Nature*, Nature Publishing Group, v. 425, n. 6961, p. 944–947, out. 2003. ISSN 0028-0836. Disponível em: ⟨http://dx.doi.org/10.1038/nature02063⟩.

84 LAI, Y. et al. Genetically designed l3 photonic crystal nanocavities with measured quality factor exceeding one million. *Applied Physics Letters*, v. 104, n. 24, p. 241101, 2014. Disponível em: ⟨http://scitation.aip.org/content/aip/journal/apl/104/24/10.1063/1.4882860⟩.

85 KURAMOCHI, E. et al. Large-scale integration of wavelength-addressable all-optical memories on a photonic crystal chip. *Nat Photon*, Nature Publishing Group, v. 8, n. 6, p. 474–481, jun. 2014. Disponível em: ⟨http://dx.doi.org/10.1038/nphoton.2014.93⟩.

86 LAUCHT, A. et al. Dephasing of exciton polaritons in photoexcited ingaas quantum dots in gaas nanocavities. *Phys. Rev. Lett.*, American Physical Society, v. 103, p. 087405, Aug 2009. Disponível em: ⟨http://link.aps.org/doi/10.1103/PhysRevLett.103.087405⟩.

87 LAUCHT, A. et al. Mutual coupling of two semiconductor quantum dots via an optical nanocavity. *Phys. Rev. B*, American Physical Society, v. 82, p. 075305, Aug 2010. Disponível em: ⟨http://link.aps.org/doi/10.1103/PhysRevB.82.075305⟩.

88 JAYNES, E.; CUMMINGS, F. Comparison of quantum and semiclassical radiation theories with application to the beam maser. *Proceedings of the IEEE*, v. 51, n. 1, p. 89–109, Jan 1963. ISSN 0018-9219.

89 SCULLY, M. O.; ZUBAIRY, M. S. *Quantum optics*. [S.l.]: Cambridge University Press, 1997.

90 VALLE, E. del; LAUSSY, F. Effective cavity pumping from weakly coupled quantum dots. *Superlattices and Microstructures*, v. 49, n. 3, p. 241 – 245, 2011. ISSN 0749-6036. Special issue: Proceedings of the 10th International Conference on the Physics of Light-Matter Coupling in Nanostructures, {PLMCN} 2010 (Cuernavaca, Mexico), 12-16 April, 2010. Disponível em: ⟨http://www.sciencedirect.com/science/article/pii/S0749603610000911⟩.

91 ROSSATTO, D. Z. et al. Nonclassical behavior of an intense cavity field revealed by quantum discord. *Phys. Rev. Lett.*, American Physical Society, v. 107, p. 153601, Oct 2011. Disponível em: ⟨http://link.aps.org/doi/10.1103/PhysRevLett.107.153601⟩.

92 LAUSSY, F. P.; VALLE, E. del; TEJEDOR, C. Luminescence spectra of quantum dots in microcavities. i. bosons. *Phys. Rev. B*, American Physical Society, v. 79, p. 235325, Jun 2009. Disponível em: ⟨http://link.aps.org/doi/10.1103/PhysRevB.79.235325⟩.

93 ENGLUND, D. et al. Controlling cavity reflectivity with a single quantum dot. *Nature*, Nature Publishing Group, v. 450, n. 7171, p. 857–861, dez. 2007. ISSN 0028-0836. Disponível em: ⟨http://dx.doi.org/10.1038/nature06234⟩.

94 KHITROVA, G. et al. Vacuum rabi splitting in semiconductors. *Nat Phys*, Nature Publishing Group, v. 2, n. 2, p. 81–90, fev. 2006. ISSN 1745-2473. Disponível em: ⟨http://dx.doi.org/10.1038/nphys227⟩.

95 RAHIMI, R.; SAITOH, A. Single-experiment-detectable nonclassical correlation witness. *Phys. Rev. A*, American Physical Society, v. 82, p. 022314, Aug 2010. Disponível em: ⟨http://link.aps.org/doi/10.1103/PhysRevA.82.022314⟩.

96 SAGUIA, A. et al. Witnessing nonclassical multipartite states. *Phys. Rev. A*, American Physical Society, v. 84, p. 042123, Oct 2011. Disponível em: ⟨http://link.aps.org/doi/10.1103/PhysRevA.84.042123⟩.

97 MAZIERO, J.; SERRA, R. M. Classicality witness for two-qubit states. *International Journal of Quantum Information*, v. 10, n. 03, p. 1250028, 2012. Disponível em: ⟨http://www.worldscientific.com/doi/abs/10.1142/S0219749912500281⟩.

98 HÖGELE, A. et al. Voltage-controlled optics of a quantum dot. *Phys. Rev. Lett.*, American Physical Society, v. 93, p. 217401, Nov 2004. Disponível em: ⟨http://link.aps.org/doi/10.1103/PhysRevLett.93.217401⟩.

99 SEIDL, S. et al. Absorption and photoluminescence spectroscopy on a single self-assembled charge-tunable quantum dot. *Phys. Rev. B*, American Physical Society, v. 72, p. 195339, Nov 2005. Disponível em: ⟨http://link.aps.org/doi/10.1103/PhysRevB.72.195339⟩.

100 ALÉN, B. et al. Absorptive and dispersive optical responses of excitons in a single quantum dot. *Applied Physics Letters*, v. 89, n. 12, p. 123124, 2006. Disponível em: ⟨http://scitation.aip.org/content/aip/journal/apl/89/12/10.1063/1.2354431⟩.

101 DEUTSCH, D. Quantum theory, the church-turing principle and the universal quantum computer. *Proceedings of the Royal Society of London. A. Mathematical and Physical Sciences*, v. 400, n. 1818, p. 97–117, 1985. Disponível em: ⟨http://rspa.royalsocietypublishing.org/content/400/1818/97.abstract⟩.

102 CLEVE, R. et al. Quantum algorithms revisited. *Proceedings of the Royal Society of London A: Mathematical, Physical and Engineering Sciences*, The Royal Society, v. 454, n. 1969, p. 339–354, 1998. ISSN 1364-5021.

103 COLLINS, D.; KIM, K. W.; HOLTON, W. C. Deutsch-jozsa algorithm as a test of quantum computation. *Phys. Rev. A*, American Physical Society, v. 58, p. R1633–R1636, Sep 1998. Disponível em: ⟨http://link.aps.org/doi/10.1103/PhysRevA.58.R1633⟩.

104 ARVIND; COLLINS, D. Scaling issues in ensemble implementations of the deutsch-jozsa algorithm. *Phys. Rev. A*, American Physical Society, v. 68, p. 052301, Nov 2003. Disponível em: ⟨http://link.aps.org/doi/10.1103/PhysRevA.68.052301⟩.

105 PRESKILL, J. *Lecture Notes on Quantum Computation, Physics 219*. Disponível em: ⟨http://www.theory.caltech.edu/people/preskill/ph229/notes/chap6.pdf⟩.

106 DAS, S.; KOBES, R.; KUNSTATTER, G. Adiabatic quantum computation and deutsch's algorithm. *Phys. Rev. A*, American Physical Society, v. 65, p. 062310, Jun 2002. Disponível em: ⟨http://link.aps.org/doi/10.1103/PhysRevA.65.062310⟩.

107 WEI, Z.; YING, M. A modified quantum adiabatic evolution for the deutsch-jozsa problem. *Physics Letters A*, v. 354, n. 4, p. 271 – 273, 2006. ISSN 0375-9601. Disponível em: ⟨http://www.sciencedirect.com/science/article/pii/S0375960106001290⟩.

108 CHAVES, R.; MELO, F. de. Noisy one-way quantum computations: The role of correlations. *Phys. Rev. A*, American Physical Society, v. 84, p. 022324, Aug 2011. Disponível em: ⟨http://link.aps.org/doi/10.1103/PhysRevA.84.022324⟩.

109 SANTOS, M. M. et al. Using quantum state protection via dissipation in a quantum-dot molecule to solve the deutsch problem. *Phys. Rev. A*, American Physical Society, v. 85, p. 032323, Mar 2012. Disponível em: ⟨http://link.aps.org/doi/10.1103/PhysRevA.85.032323⟩.

110 MYERS, J. M. et al. Rapid solution of problems by nuclear-magnetic-resonance quantum computation. *Phys. Rev. A*, American Physical Society, v. 63, p. 032302, Feb 2001. Disponível em: ⟨http://link.aps.org/doi/10.1103/PhysRevA.63.032302⟩.

111 MODI, K. et al. The classical-quantum boundary for correlations: Discord and related measures. *Rev. Mod. Phys.*, American Physical Society, v. 84, p. 1655–1707, Nov 2012. Disponível em: ⟨http://link.aps.org/doi/10.1103/RevModPhys.84.1655⟩.

112 RULLI, C. C.; SARANDY, M. S. Global quantum discord in multipartite systems. *Phys. Rev. A*, American Physical Society, v. 84, p. 042109, Oct 2011. Disponível em: ⟨http://link.aps.org/doi/10.1103/PhysRevA.84.042109⟩.

113 DATTA, A.; SHAJI, A. Quantum discord and quantum computing - an appraisal. *International Journal of Quantum Information*, v. 09, n. 07n08, p. 1787–1805, 2011. Disponível em: ⟨http://www.worldscientific.com/doi/abs/10.1142/S0219749911008416⟩.

114 BULLOCK, S. S.; MARKOV, I. L. Asymptotically optimal circuits for arbitrary n-qubit diagonal comutations. *Quantum Info. Comput.*, Rinton Press, Incorporated, Paramus, NJ, v. 4, n. 1, p. 27–47, jan. 2004. ISSN 1533-7146. Disponível em: ⟨http://dl.acm.org/citation.cfm?id=2011572.2011575⟩.

115 GOTTESMAN, D. The Heisenberg Representation of Quantum Computers. *arXiv:quant-ph/9807006*, jul. 1998. Disponível em: ⟨http://arxiv.org/abs/quant-ph/9807006⟩.

116 EASTIN, B. Simulating Concordant Computations. *arXiv:1006.4402*, jun. 2010. Disponível em: ⟨http://arxiv.org/abs/1006.4402⟩.

117 ARVIND, D. D.; KUMAR, A. Quantum entanglement in the nmr implementation of the deutsch-jozsa algorithm. *Pramana Jr. of Physics*, v. 56, n. L705, p. L705, 2001.

118 MORIMAE, T.; FUJII, K.; FITZSIMONS, J. F. Hardness of classically simulating the one-clean-qubit model. *Phys. Rev. Lett.*, American Physical Society, v. 112, p. 130502, Apr 2014. Disponível em: ⟨http://link.aps.org/doi/10.1103/PhysRevLett.112.130502⟩.

119 SHOR, P. W. Scheme for reducing decoherence in quantum computer memory. *Phys. Rev. A*, American Physical Society, v. 52, p. R2493–R2496, Oct 1995. Disponível em: ⟨http://link.aps.org/doi/10.1103/PhysRevA.52.R2493⟩.

120 STEANE, A. M. Error correcting codes in quantum theory. *Phys. Rev. Lett.*, American Physical Society, v. 77, p. 793–797, Jul 1996. Disponível em: ⟨http://link.aps.org/doi/10.1103/PhysRevLett.77.793⟩.

121 VIOLA, L.; KNILL, E.; LLOYD, S. Dynamical decoupling of open quantum systems. *Phys. Rev. Lett.*, American Physical Society, v. 82, p. 2417–2421, Mar 1999. Disponível em: ⟨http://link.aps.org/doi/10.1103/PhysRevLett.82.2417⟩.

122 VITALI, D.; TOMBESI, P. Using parity kicks for decoherence control. *Phys. Rev. A*, American Physical Society, v. 59, p. 4178–4186, Jun 1999. Disponível em: ⟨http://link.aps.org/doi/10.1103/PhysRevA.59.4178⟩.

123 ZANARDI, P.; RASETTI, M. Noiseless quantum codes. *Phys. Rev. Lett.*, American Physical Society, v. 79, p. 3306–3309, Oct 1997. Disponível em: ⟨http://link.aps.org/doi/10.1103/PhysRevLett.79.3306⟩.

124 LIDAR, D. A.; CHUANG, I. L.; WHALEY, K. B. Decoherence-free subspaces for quantum computation. *Phys. Rev. Lett.*, American Physical Society, v. 81, p. 2594–2597, Sep 1998. Disponível em: ⟨http://link.aps.org/doi/10.1103/PhysRevLett.81.2594⟩.

125 VERSTRAETE, F.; WOLF, M. M.; CIRAC, J. I. Quantum computation and quantum-state engineering driven by dissipation. *Nature Physics*, Nature Publishing Group, v. 5, n. 9, p. 633–636, jul. 2009. ISSN 1745-2473. Disponível em: ⟨http://dx.doi.org/10.1038/nphys1342⟩.

126 PASTAWSKI, F.; CLEMENTE, L.; CIRAC, J. I. Quantum memories based on engineered dissipation. *Phys. Rev. A*, American Physical Society, v. 83, p. 012304, Jan 2011. Disponível em: ⟨http://link.aps.org/doi/10.1103/PhysRevA.83.012304⟩.

127 WALBORN, S. et al. Spatial correlations in parametric down-conversion. *Physics Reports*, v. 495, n. 45, p. 87 – 139, 2010. ISSN 0370-1573. Disponível em: ⟨http://www.sciencedirect.com/science/article/pii/S0370157310001602⟩.

128 HOR-MEYLL, M. et al. Deterministic quantum computation with one photonic qubit. *Phys. Rev. A*, American Physical Society, v. 92, p. 012337, Jul 2015. Disponível em: ⟨http://link.aps.org/doi/10.1103/PhysRevA.92.012337⟩.

129 LEMOS, G. B. et al. Characterization of a spatial light modulator as a polarization quantum channel. *Phys. Rev. A*, American Physical Society, v. 89, p. 042119, Apr 2014. Disponível em: ⟨http://link.aps.org/doi/10.1103/PhysRevA.89.042119⟩.

130 POLITI, A.; MATTHEWS, J. C. F.; O'BRIEN, J. L. Shor's quantum factoring algorithm on a photonic chip. *Science*, v. 325, n. 5945, p. 1221, 2009. Disponível em: ⟨http://www.sciencemag.org/content/325/5945/1221.abstract⟩.

131 MARTÍN-LóPEZ, E. et al. Experimental realization of Shor's quantum factoring algorithm using qubit recycling. *Nature Photonics*, Nature Publishing Group, v. 6, n. 11, p. 773–776, out. 2012. ISSN 1749-4885. Disponível em: ⟨http://dx.doi.org/10.1038/nphoton.2012.259⟩.

132 GRIFFITHS, R. B.; NIU, C.-S. Semiclassical fourier transform for quantum computation. *Phys. Rev. Lett.*, American Physical Society, v. 76, p. 3228–3231, Apr 1996. Disponível em: ⟨http://link.aps.org/doi/10.1103/PhysRevLett.76.3228⟩.

133 LEMOS, G. B. et al. Experimental observation of quantum chaos in a beam of light. *Nat Commun*, v. 3, p. 1211, 2012.

134 SANDERS, B. C.; BARTLETT, S. D.; GUISE, H. de. From qubits to continuous-variable quantum computation. *arXiv quant-ph/0208008*, 2002.

135 BRAUNSTEIN, S. L.; LOOCK, P. van. Quantum information with continuous variables. *Rev. Mod. Phys.*, American Physical Society, v. 77, p. 513–577, Jun 2005. Disponível em: ⟨http://link.aps.org/doi/10.1103/RevModPhys.77.513⟩.

136 WEEDBROOK, C. et al. Gaussian quantum information. *Rev. Mod. Phys.*, American Physical Society, v. 84, p. 621–669, May 2012. Disponível em: ⟨http://link.aps.org/doi/10.1103/RevModPhys.84.621⟩.