

UNIVERSIDADE FEDERAL DO CEARÁ
CENTRO DE TECNOLOGIA
DEPARTAMENTO DE ENGENHARIA DE TELEINFORMÁTICA
CURSO DE PÓS-GRADUAÇÃO EM ENGENHARIA DE TELEINFORMÁTICA

DANIEL BARBOSA DE BRITO

SISTEMAS DE COMUNICAÇÃO QUÂNTICA
COM ÓPTICA LINEAR

FORTALEZA – CEARÁ
FEVEREIRO / 2007

UNIVERSIDADE FEDERAL DO CEARÁ
CENTRO DE TECNOLOGIA
DEPARTAMENTO DE ENGENHARIA DE TELEINFORMÁTICA
CURSO DE PÓS-GRADUAÇÃO EM ENGENHARIA DE TELEINFORMÁTICA

SISTEMAS DE COMUNICAÇÃO QUÂNTICA COM ÓPTICA LINEAR

Autor

Daniel Barbosa de Brito

Orientador

Prof. Dr. Rubens Viana Ramos

Dissertação submetida à Coordenação do Curso de Pós-Graduação em Engenharia de Teleinformática da Universidade Federal do Ceará, como parte dos requisitos exigidos para obtenção do grau de **Mestre em Engenharia de Teleinformática**.

FORTALEZA – CE

FEVEREIRO / 2007

Dedico este trabalho aos meus pais e irmãos.

Agradecimentos

À minha família por me apoiar e incentivar em todos os momentos da minha vida.

Ao professor Rubens Viana Ramos do departamento de Engenharia de Teleinformática da Universidade Federal do Ceará pela amizade e pela seriedade na orientação.

Aos colegas do laboratório de tecnologia da informação quântica (LATIQ): Caroline Timbó, Cláudio do Nascimento, David Sena, Fábio Alencar, George Thé, João Batista, Paulo Benício e Wellington Brito, pela amizade e valiosa troca de conhecimentos que ajudaram na minha formação.

Ao CNPq pela bolsa de mestrado que me foi concedida.

Sumário

Lista de Figuras.....	vii
Lista de Tabelas	viii
Resumo	ix
Abstract.....	x
Introdução.....	11
Capítulo 1 Correção de Erro Quântico com Inserção de Redundância	13
1.1 Introdução	13
1.2 Erro quântico	13
1.3 Sistemas de correção de erros com inserção de redundância	15
1.4 Códigos de correção quântica de erros em um qubit.....	16
Capítulo 2 Correção de Erro Quântico sem Inserção de Redundância.....	20
2.1 Introdução	20
2.2 Sistema de correção de erros de estados de fótons isolados usando óptica linear..	20
2.3 Sistema de correção de erros de estados coerentes usando óptica linear.....	23
2.4 Sistema de correção de erros de pares de fótons entrelaçados usando óptica linear	26
Capítulo 3 Correção de Erro Quântico em Estados Bipartes.....	28
3.1 Introdução	28
3.2 Correção de erros em estados bipartes de qubits	28
Capítulo 4 Sistemas Ópticos para Teleportação de Qubits	31
4.1 Introdução	31
4.2 Geração probabilística de um estado de Bell com qubit codificado na polarização	33
4.3 Circuito óptico para teleportação probabilística de estados quânticos	34
Capítulo 5 Conclusões e Perspectivas	37
5.1 Conclusões.....	37
5.2 Perspectivas	38
Referências	39
Apêndice A Análise dos Códigos de 5 e 9 qubits	40

A.1 Código de Shor.....	40
A.2 Código de 5 qubits.....	43
Anexo 1 Artigo Científico - I	49
Anexo 2 Artigo Científico - II.....	59
Anexo 3 Artigo Científico - III.....	75

Lista de Figuras

Figura 1.1. Modelo de circuitos quânticos do canal inversor de bit.....	14
Figura 1.2. Modelo de circuitos quânticos do canal inversor de fase.....	15
Figura 1.3. Correção de erro quântico com estados entrelaçados.	16
Figura 1.4. Código de repetição de três qubits.	16
Figura 1.5. Circuito quântico para o código de Shor.....	17
Figura 1.6. Circuito de codificação do código de 5 qubits.....	18
Figura 2.1. Esquema óptico para correção de erro de um qubit.	20
Figura 2.2. Esquema óptico para correção de erro de um qubit com duas saídas.	22
Figura 2.3. Esquema óptico passivo para estados coerentes.	24
Figura 2.4. Sistema óptico para distribuição livre de erro de um estado de Bell.	26
Figura 3.1. Sistema óptico para correção de erro de um estado biparte de qubits.	28
Figura 4.1. Circuito quântico para teleportar um qubit.....	31
Figura 4.2. Circuito óptico para geração probabilística de um estado de Bell.....	33
Figura 4.3. Circuito óptico para teleportação probabilística de qubits codificados na polarização.....	34
Figura 4.4. Circuito óptico completo para teleportação probabilística de qubits de polarização.....	35
Figura 4.5. Circuito óptico para teleportação probabilística de estados quânticos com correção de erros.....	36
Figura A 1. Circuito quântico para o código de Shor.	40
Figura A 2. Circuito de codificação para estados de 5 qubits.	43

Lista de Tabelas

Tabela 1.1. Evolução do estado quântico no esquema da Fig. 1.4 quando da ocorrência de zero (I) ou um erro (II-IV) no canal inversor de qubit.	17
---	----

Resumo

Nesta dissertação é proposto um sistema de correção de erro quântico para estados coerentes de luz e um sistema óptico completo para a teleportação probabilística de qubits codificados na polarização de um fóton. O trabalho se inicia com a análise de correção de erro quântico com a utilização de redundâncias. Depois, é apresentada uma forma de correção de erros utilizando qubits do tipo time-bin e sem acréscimo de redundâncias. Com base nesta abordagem, foi proposto um sistema de correção de erro quântico passivo, isto é, que não precisa de controle externo de sincronização, para sistemas de comunicações quânticas que utilizam estados coerentes de luz, utilizando apenas dispositivos ópticos lineares. É mostrado, também, que o sistema de correção de qubits individuais pode ser usado para corrigir estados bipartes de qubits. Em seguida, é analisada a teleportação de estados quânticos e é proposto um sistema probabilístico de teleportação de estados quânticos de polarização de fótons isolados utilizando dispositivos ópticos lineares. Por fim, os tópicos de correção de erro e teleportação são unidos na proposição de um sistema probabilístico de teleportação empregando um sistema de correção de erros na distribuição do par de fótons entrelaçados.

Abstract

In this dissertation it is considered a quantum error correction system for coherent states of light and a complete optical system for probabilistic teleportation of single-photon polarization encoded qubit. Initially, the quantum error correction with the use of redundancy is analyzed. After that, it is presented a form of error correction using time-bin qubit without redundancies. Based on this last approach, a passive quantum error correction system, that is, without external control and synchronization, for quantum communication system employing coherent states, using only linear optical devices, is proposed. It is shown that the quantum error correction system also works for bipartite states of qubits. Following, the teleportation of quantum states is analyzed and an optical system for probabilistic teleportation of single-photon polarization encoded qubit, using only linear optical devices, is proposed. Finally, the error correction and teleportation topics are put together in the proposal of a probabilistic teleportation system using an error correction system for distribution of the entangled pair of photons.

Introdução

A comunicação quântica, assim como a clássica, tem o desempenho afetado pela presença de ruídos. Portanto, os sistemas de correção quântica de erros exercem um papel importante na implementação prática de sistemas de comunicação quântica.

Uma forma de realizar correção de erro quântico é acrescentar redundâncias à informação e estimar o erro introduzido pelo canal através de medidas realizadas nos qubits de redundância. Assim, é possível determinar a operação que deve ser realizada no qubit que porta a informação para realizar a correção do mesmo. Apesar de efetivamente corrigir o erro, esta técnica exige a geração de estados entrelaçados de pelo menos 5 qubits para a correção de um erro geral em um qubit. Tal tarefa não é factível com o estágio tecnológico atual.

Visando contornar este problema, foi proposto um sistema de correção de erros quânticos sem acréscimo de redundâncias. Neste, os qubits são do tipo time-bin. Isto torna a implementação do sistema mais simples se comparada com a técnica citada anteriormente. Nesta abordagem, é possível detectar e corrigir qualquer erro, em um qubit, que possa ser modelado por uma transformação unitária.

Por outro lado, a teleportação de estados quânticos atrai atenção por sua potencialidade sem contrapartida nas comunicações clássicas. A teleportação possibilita a transmissão de informação entre duas partes distantes: um transmissor (T_x) pode enviar um qubit a um receptor (R_x) sem conhecer o estado do qubit e sem que o portador da informação seja enviado. As condições necessárias para que isso ocorra é que cada um, T_x e R_x , possua um qubit de um par de Bell, e que exista um canal clássico conectando-os.

Nesta direção, a presente dissertação propõe um sistema de correção de erro quântico passivo para correção de erros em sistemas de comunicação quântica que utilizam estados coerentes de luz, e um sistema probabilístico de teleportação de estados quânticos utilizando fótons isolados. No primeiro capítulo, é feita uma breve revisão da teoria de correção de erros quânticos com inserção de redundância. É mostrado como se realiza a correção de erros quânticos através da análise de três códigos corretores de erros em um qubit. No Capítulo 2, é mostrado como realizar a correção de erro quântico sem inserção de redundâncias e como aplicar esse tipo de correção de erro em sistemas de comunicação que utilizam estados coerentes. No Capítulo 3, é mostrado que o

sistema de correção de erro quântico apresentado no Capítulo 2 pode corrigir também erros em estados bipartes. No Capítulo 4, é revista a teoria de teleportação de qubits e é proposto um sistema probabilístico de teleportação de qubits codificados na polarização de fótons isolados, usando apenas dispositivos ópticos lineares. Por fim, no Capítulo 5, são apresentadas as conclusões e as perspectivas de trabalhos futuros.

Capítulo 1

Correção de Erro Quântico com Inserção de Redundância

1.1 Introdução

O emprego de sistemas de informação (comunicação e computação) quântica na realização de tarefas no mundo real está diretamente ligado ao desempenho de tais sistemas. Assim, a construção de sistemas de informação quântica confiáveis, isto é, que apresentem baixas taxas de erro, é crucial para a popularização da tecnologia da informação quântica. Os erros presentes em sistemas de informação quântica são inevitáveis e, na tentativa de combatê-los, normalmente códigos quânticos são utilizados. Assim como em sistemas de informação clássica, o objetivo do uso de um código quântico é introduzir redundância. Desta forma, qubits auxiliares (ancillas) são entrelaçados com os qubits que portam a informação pelo codificador quântico e todos os qubits são enviados pelo canal. Na saída do canal, a medição dos qubits auxiliares torna possível estimar a transformação sofrida pelos qubits de informação [1]. Uma vez conhecida a transformação aplicada pelo canal nos qubits de informação, para que o erro seja corrigido, a transformação inversa da do canal é aplicada a eles.

1.2 Erro quântico

Sistemas reais sofrem interações indesejadas com o ambiente. Estas representam ruído em sistemas de informação quântica e podem causar erros. É preciso entender e controlar tais ruídos a fim de construir sistemas que funcionem adequadamente. Os

tipos de ruído mais comuns são a inversão de bit, a inversão de fase, a despolarização do qubit, o desvanecimento de amplitude e o desvanecimento da fase.

O canal que insere inversão de qubit aplica a matriz X (porta NOT quântica) à entrada transformando o estado $|0\rangle(|1\rangle)$ em $|1\rangle(|0\rangle)$ com probabilidade p , e aplica a matriz I (identidade) com probabilidade $1-p$. Este tipo de canal quântico ruidoso pode ser representado por uma rotação de um qubit, $R(\theta)$, e uma porta CNOT, como mostra a Fig.1.1.

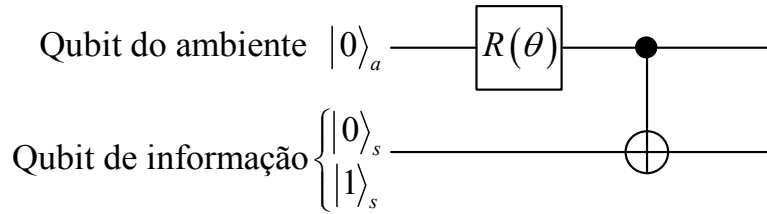


Figura 1.1. Modelo de circuitos quânticos do canal inversor de bit

Na Fig. 1.1 quando o qubit de informação $|0\rangle_s$ é enviado, o estado quântico conjunto ambiente-sinal é $\cos(\theta)|00\rangle_{as} + \sin(\theta)|11\rangle_{as}$. Portanto, o qubit de sinal é encontrado invertido na saída com probabilidade $p = \sin^2(\theta)$. Por outro lado, quando o qubit de sinal $|1\rangle_s$ é enviado, o estado conjunto ambiente-sinal é $\cos(\theta)|01\rangle_{as} + \sin(\theta)|10\rangle_{as}$ e o qubit de sinal será encontrado invertido na saída com probabilidade $p = \sin^2(\theta)$. Assim, o canal quântico ruidoso inversor de bit pode ser modelado pela equação:

$$\rho_o = (1-p)\rho_i + pX\rho_iX^\dagger. \quad (1.1)$$

Por sua vez, o canal que insere inversão de fase aplica a matriz Z ao estado de entrada, transformando o estado $|0\rangle(|1\rangle)$ em $|0\rangle(-|1\rangle)$, com probabilidade p e aplica a matriz I (identidade) com probabilidade $1-p$. Este tipo de canal quântico ruidoso pode ser representado por uma rotação de um qubit e uma porta Z-controlada, como mostra a Fig. 1.2.

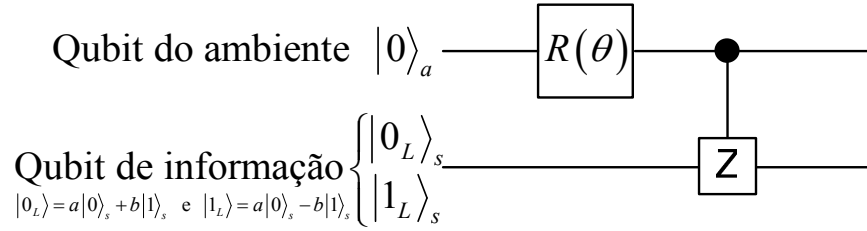


Figura 1.2. Modelo de circuitos quânticos do canal inversor de fase.

Na Fig 1.2. quando o qubit de informação $|0_L\rangle_s$ é enviado, o estado quântico conjunto ambiente-sinal é $\cos(\theta)|0\rangle_a(a|0\rangle_s+b|1\rangle_s)+\sin(\theta)|1\rangle_a(a|0\rangle_s-b|1\rangle_s)$. Portanto, o qubit de sinal é encontrado com a fase invertida na saída com probabilidade $p=\sin^2(\theta)$. Por outro lado, quando o qubit de sinal $|1_L\rangle_s$ é enviado, o estado conjunto ambiente-sinal é $\cos(\theta)|0\rangle_a(a|0\rangle_s-b|1\rangle_s)+\sin(\theta)|1\rangle_a(a|0\rangle_s+b|1\rangle_s)$ e o qubit de sinal será encontrado com a fase invertida na saída novamente com probabilidade $p=\sin^2(\theta)$. Assim, o canal quântico ruidoso inversor de fase pode ser modelado pela equação:

$$\rho_o = (1-p)\rho_i + pZ\rho_iZ^\dagger. \quad (1.2)$$

1.3 Sistemas de correção de erros com inserção de redundância

Um sistema de correção de erro quântico que utiliza redundância é mostrado na Fig.1.3, sendo $|\theta\rangle$ o qubit de informação e $|a_i\rangle$ ($i=1,\dots,n$) são os qubits auxiliares. O codificador entrelaça os qubits auxiliares com o qubit de informação e o decodificador faz o oposto. O número de erros que podem ser corrigidos e o número de qubits auxiliares utilizados dependem do tipo de código utilizado [1]. O código de Shor, por exemplo, pode corrigir qualquer tipo de erro em um qubit usando oito qubits auxiliares [2]. O código de correção de erros quânticos em um qubit mais eficiente utiliza quatro qubits auxiliares [1].

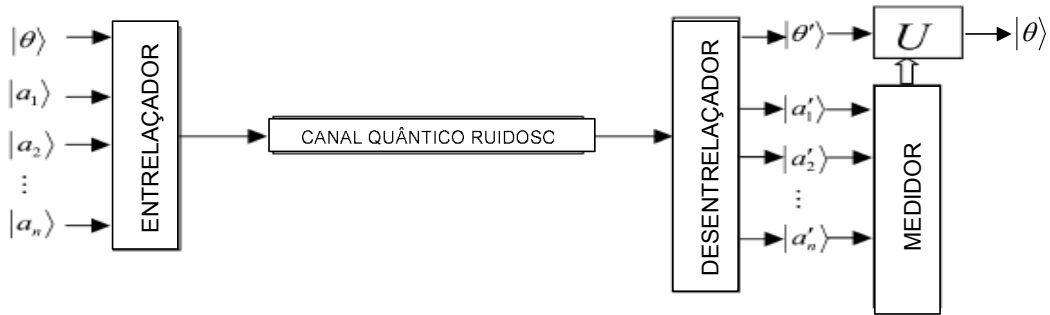


Figura 1.3. Correção de erro quântico com estados entrelaçados.

1.4 Códigos de correção quântica de erros em um qubit

O código de correção quântica de erro mais simples é o código de repetição. Por exemplo, um código de repetição de três qubit é: $|0_L\rangle=|000\rangle$ e $|1_L\rangle=|111\rangle$. Este código é capaz de corrigir um erro de inversão de bit em um qubit. O digrama com codificador e decodificador para o código de repetição de 3 qubits é mostrado na Fig. 1.4.

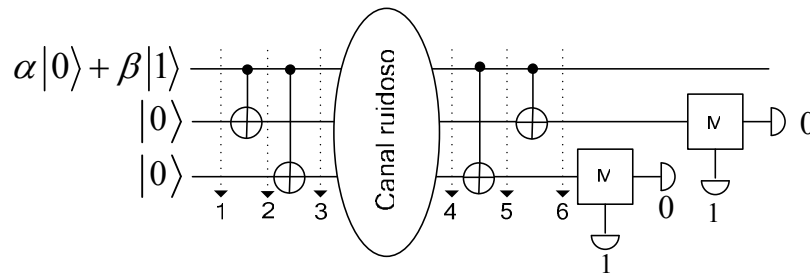


Figura 1.4. Código de repetição de três qubits.

O funcionamento do código quando da ocorrência de zero ou um erro é como mostrado na Tabela 1.1.

1	2	3	4	5	6	
$\alpha 000\rangle+\beta 100\rangle$	$\alpha 000\rangle+\beta 110\rangle$	$\alpha 000\rangle+\beta 111\rangle$	$\alpha 000\rangle+\beta 111\rangle$	$\alpha 000\rangle+\beta 110\rangle$	$\alpha 000\rangle+\beta 100\rangle$	I
			$\alpha 100\rangle+\beta 011\rangle$	$\alpha 101\rangle+\beta 011\rangle$	$\alpha 111\rangle+\beta 011\rangle$	II
			$\alpha 010\rangle+\beta 101\rangle$	$\alpha 010\rangle+\beta 100\rangle$	$\alpha 010\rangle+\beta 110\rangle$	III
			$\alpha 001\rangle+\beta 110\rangle$	$\alpha 001\rangle+\beta 111\rangle$	$\alpha 001\rangle+\beta 101\rangle$	IV

Tabela 1.1. Evolução do estado quântico no esquema da Fig. 1.4 quando da ocorrência de zero (I) ou um erro (II-IV) no canal inversor de qubit.

Como pode ser observado na Tabela 1.1, quando o resultado da medição dos dois últimos qubits for ‘11’, uma porta NOT deve ser aplicada no primeiro qubit de forma a recuperar o estado que foi inserido no canal. De forma semelhante, o código de repetição de 3 qubits $|0_L\rangle=|+++ \rangle$ e $|1_L\rangle=|--- \rangle$ corrige um erro de inversão de fase. O código proposto por Shor, por sua vez, é uma concatenação dos códigos para corrigir inversão de fase e inversão de bit [2]. A Fig. 1.5 mostra o circuito quântico que implementa esse código.

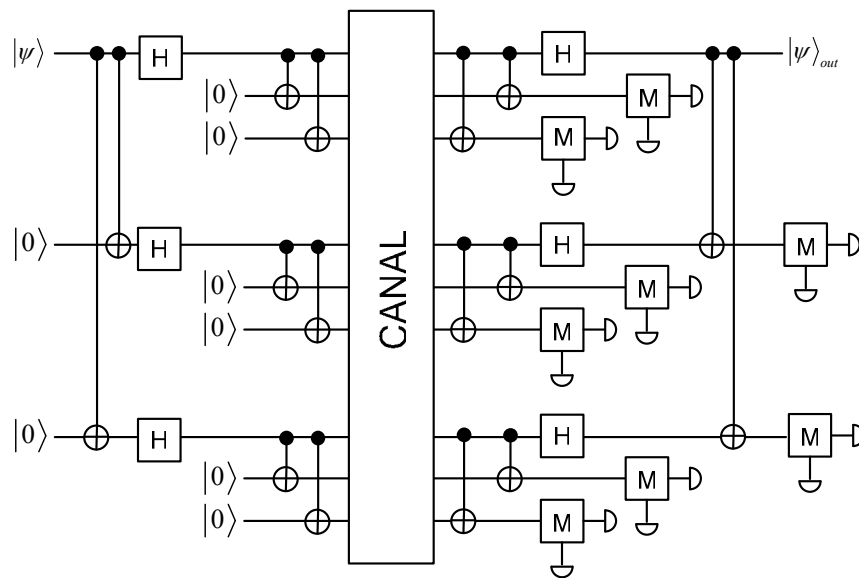


Figura 1.5. Circuito quântico para o código de Shor.

Se o estado de entrada do circuito quântico da Fig. 1.5 é $|\psi\rangle_i = (\alpha|0\rangle+\beta|1\rangle)|00000000\rangle$ e um erro do tipo $|0\rangle \rightarrow a|0\rangle+b|1\rangle$, $|1\rangle \rightarrow c|0\rangle+d|1\rangle$ acontece no primeiro qubit, então o estado de saída será (ver Apêndice A):

$$|\psi_o\rangle = (\alpha|0\rangle + \beta|1\rangle)[(a+d)/2|00000000\rangle] + (\alpha|1\rangle + \beta|0\rangle)[(a-d)/2|00100100\rangle] + (\alpha|0\rangle - \beta|1\rangle)[(c+b)/2|11000000\rangle] + (\alpha|1\rangle - \beta|0\rangle)[(c-b)/2|11100100\rangle] \quad (1.3)$$

Observando a equação (1.3) nota-se que, com base no resultado da medição dos oito últimos qubits, é possível determinar a operação (I, X, Z, XZ) necessária para recuperar o qubit transmitido.

O código quântico de menor tamanho capaz de corrigir um erro arbitrário em um qubit possui cinco qubits. O código é

$$|0_L\rangle = |00000\rangle + |10010\rangle + |01001\rangle + |10100\rangle + |01010\rangle - |11011\rangle - |00110\rangle - |11000\rangle - |11101\rangle - |00011\rangle - |11110\rangle - |01111\rangle - |10001\rangle - |01100\rangle - |10111\rangle + |00101\rangle \quad (1.4)$$

$$|1_L\rangle = |11111\rangle + |01101\rangle + |10110\rangle + |01011\rangle + |10101\rangle - |00100\rangle - |11001\rangle - |00111\rangle - |00010\rangle - |11100\rangle - |00001\rangle - |10000\rangle - |01110\rangle - |10011\rangle - |01000\rangle + |11010\rangle \quad (1.5)$$

e o mesmo pode ser implementado usando o circuito quântico mostrado na Fig. 1.6.

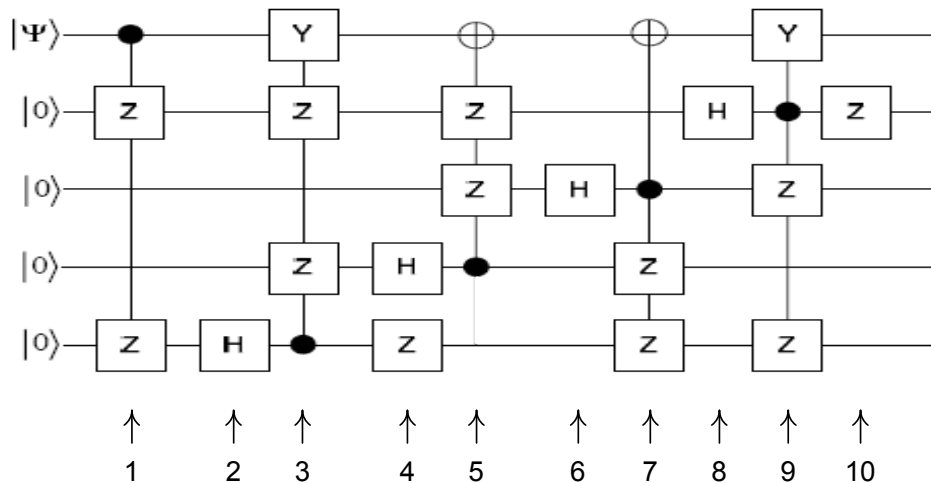


Figura 1.6. Circuito de codificação do código de 5 qubits.

No circuito da Fig. 1.6, a porta Y é a aplicação da porta X seguida da Z . Se o estado de entrada do circuito quântico da Fig. 1.6 é $|\psi\rangle_{in} = (\alpha|0\rangle + \beta|1\rangle)|0000\rangle$ e um erro do tipo

$|0\rangle \rightarrow a|0\rangle + b|1\rangle$, $|1\rangle \rightarrow c|0\rangle + d|1\rangle$ acontece no primeiro qubit, então o estado de saída será (ver Apêndice A):

$$|\psi_s\rangle = \frac{a+d}{2}(\alpha|0\rangle + \beta|1\rangle)|1011\rangle + \frac{a-d}{2}(\alpha|0\rangle - \beta|1\rangle)|0100\rangle + \frac{b+c}{2}(\alpha|1\rangle + \beta|0\rangle)|0000\rangle + \frac{b-c}{2}(\alpha|1\rangle - \beta|0\rangle)|1111\rangle \quad (1.6)$$

Com base no resultado da medição dos quatro últimos qubits é possível determinar a operação (I, X, Z, XZ) necessária para recuperar o qubit transmitido.

Do ponto de vista prático, é difícil de implementar tais protocolos de correção de erro no estágio atual da tecnologia, considerando-se a necessidade de uma fonte de pelo menos 5 fótons entrelaçados. Assim, é preciso buscar soluções mais simples. Nesse sentido, foi proposto um sistema óptico capaz de corrigir um erro arbitrário de um qubit que não usa estados entrelaçados [3]. No próximo capítulo é analisado o funcionamento desse sistema.

Capítulo 2

Correção de Erro Quântico sem Inserção de Redundância

2.1 Introdução

Diferente do que é normalmente usado para corrigir erros em comunicação quântica, foi proposto um sistema de correção de erros que não insere redundâncias à informação útil [3]. A análise de tal abordagem é feita neste capítulo considerando-se estados de fótons isolados, estados coerentes e pares de fótons entrelaçados.

2.2 Sistema de correção de erros de estados de fótons isolados usando óptica linear

O sistema óptico de correção/rejeição de erros quânticos utilizando apenas dispositivos ópticos lineares proposto na Referência [3] é mostrado na Fig. 2.1. Nesta, PBS são divisores de feixes por polarização, PC são células de Pockels e HWP é uma placa de meia onda.

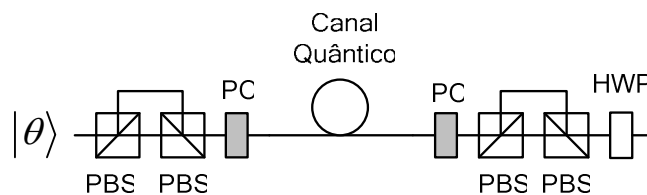


Figura 2.1. Esquema óptico para correção de erro de um qubit.

No esquema da Fig. 2.1, o pulso óptico incidente com um único fóton polarizado no estado $|\theta\rangle = \alpha|H\rangle + \beta|V\rangle$ é transformado num qubit *time-bin* pelo interferômetro desbalanceado formado pelos dois primeiros PBS's, a componente horizontal passa pelo caminho curto e a componente vertical passa pelo caminho longo, resultando no estado $\alpha|H\rangle_S + \beta|V\rangle_L$, sendo S e L, respectivamente, as designações dos caminhos curto e longo no interferômetro desbalanceado. Depois, a célula de Pockels do transmissor é ligada de forma a atuar apenas na segunda parte do qubit *time-bin*, provocando uma rotação da polarização de $\pi/2$. Assim, o estado quântico na entrada do canal é o estado $\alpha|H\rangle_S + \beta|H\rangle_L$. Esse estado é enviado pelo canal quântico (fibra óptica). Como se considera o tempo de separação do *time-bin* muito menor que o tempo de flutuação dos parâmetros do canal (birrefringência da fibra óptica), ambas as componentes sofrerão as mesmas influências do canal quântico representado pela evolução unitária U . Uma transformação unitária geral atua num estado com polarização horizontal da seguinte forma: $U|H\rangle = \cos(\varphi)e^{i\lambda}|H\rangle + \sin(\varphi)e^{i\xi}|V\rangle$. As letras gregas φ , λ e ξ representam parâmetros de uma transformação unitária geral 2x2. Assim, o estado que chega ao receptor é

$$\alpha \left[\cos(\varphi)e^{i\lambda}|H\rangle_S + \sin(\varphi)e^{i\xi}|V\rangle_S \right] + \beta \left[\cos(\varphi)e^{i\lambda}|H\rangle_L + \sin(\varphi)e^{i\xi}|V\rangle_L \right] \quad (2.1)$$

O receptor aciona sua célula de Pockels na primeira parte do *time-bin* provocando uma rotação da polarização de $\pi/2$, o que resulta no estado

$$\alpha \left[\cos(\varphi)e^{i\lambda}|V\rangle_S + \sin(\varphi)e^{i\xi}|H\rangle_S \right] + \beta \left[\cos(\varphi)e^{i\lambda}|H\rangle_L + \sin(\varphi)e^{i\xi}|V\rangle_L \right] \quad (2.2)$$

O estado (2.2) entra no interferômetro desbalanceado de polarização do receptor. A componente com polarização horizontal mais uma vez passa pelo caminho curto e a componente com polarização vertical passa pelo caminho longo. O estado depois dos PBS's do receptor é

$$\begin{aligned} & \alpha \left[\cos(\varphi)e^{i\lambda}|V\rangle_{SL} + \sin(\varphi)e^{i\xi}|H\rangle_{SS} \right] + \beta \left[\cos(\varphi)e^{i\lambda}|H\rangle_{LS} + \sin(\varphi)e^{i\xi}|V\rangle_{LL} \right] = \\ & = \cos(\varphi)e^{i\lambda} \left[\alpha|V\rangle_{SL} + \beta|H\rangle_{LS} \right] + \sin(\varphi)e^{i\xi} \left[\alpha|H\rangle_{SS} + \beta|V\rangle_{LL} \right]. \end{aligned} \quad (2.3)$$

Por fim, depois de passar pela HWP que rotaciona a polarização de $\pi/2$, o estado é

$$\cos(\varphi)e^{i\lambda} [\alpha|H\rangle_{SL} + \beta|V\rangle_{LS}] + \text{sen}(\varphi)e^{i\xi} [\alpha|V\rangle_{SS} + \beta|H\rangle_{LL}]. \quad (2.4)$$

O fóton que emerge do aparato óptico pode estar em três intervalos de tempo distintos (SS, SL ou LS e LL). Se o fóton estiver no intervalo de tempo central, então com certeza ele portará o qubit correto. Isto ocorre com probabilidade $\cos^2(\varphi)$. Fótons nos demais instantes de tempo (SS e LL) devem ser descartados.

O esquema da Fig. 2.1 nem sempre tem sucesso na correção do qubit. O esquema da Fig. 2.2 [4], por sua vez, sempre fornece na saída o qubit correto. O preço a ser pago, como será visto, é que não há certeza sobre em qual das duas saídas o fóton emergirá.

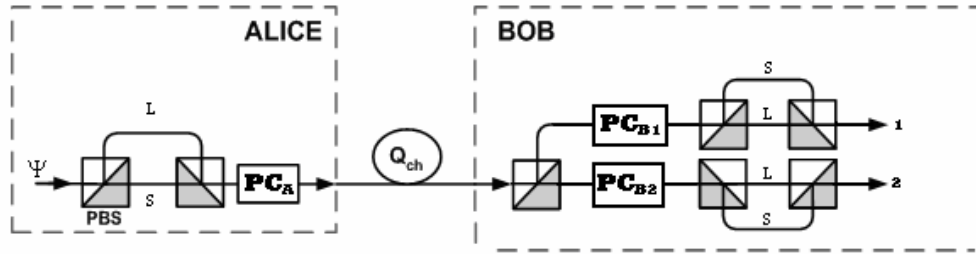


Figura 2.2. Esquema óptico para correção de erro de um qubit com duas saídas.

Alice entra com o estado $\alpha|H\rangle + \beta|V\rangle$ e o estado que chega ao receptor é aquele dado na equação (2.1) reescrito como

$$|\Phi'\rangle = \alpha [\cos(\varphi)|H\rangle_S + \text{sen}(\varphi)e^{i\phi}|V\rangle_S] + \beta [\cos(\varphi)|H\rangle_L + \text{sen}(\varphi)e^{i\phi}|V\rangle_L] \quad (2.5)$$

$$\phi = \xi - \lambda \quad (2.6)$$

Logo após o primeiro PBS de Bob, o estado é;

$$|\Phi''\rangle = \alpha [\cos(\varphi)|H\rangle_S^2 + \text{sen}(\varphi)e^{i\phi}|V\rangle_S^1] + \beta [\cos(\varphi)|H\rangle_L^2 + \text{sen}(\varphi)e^{i\phi}|V\rangle_L^1] \quad (2.7)$$

$$|\Phi''\rangle = \cos(\varphi)(\alpha|H\rangle_S^2 + \beta|H\rangle_L^2) + \text{sen}(\varphi)e^{i\phi}(\alpha|V\rangle_S^1 + \beta|V\rangle_L^1) \quad (2.8)$$

A célula de Pockels PC_{B1} é acionada de forma a rotacionar de $\pi/2$ apenas a parte inicial do time-bin (S) e a célula PC_{B2} , por sua vez, é acionada de forma a rotacionar de $\pi/2$ apenas a parte final do time-bin (L). Depois da ação das células de Pockels, o estado total é:

$$|\Phi^m\rangle = \cos\varphi\left(\alpha|H\rangle_S^2 + \beta|V\rangle_L^2\right) + \text{sen}\varphi e^{i\phi}\left(\alpha|H\rangle_S^1 + \beta|V\rangle_L^1\right). \quad (2.9)$$

Cada estado de (2.9) passa agora por um interferômetro de polarização com o mesmo desbalanceamento no comprimento dos braços que o interferômetro de polarização de Alice. Entretanto, diferentemente do que ocorre na codificação, a componente vertical viaja pelo braço curto enquanto que a componente horizontal viaja pelo braço longo. Assim, o estado total final na saída de Bob é

$$|\Psi_f\rangle = \cos(\varphi)\left(\alpha|H\rangle_{SL}^2 + \beta|V\rangle_{LS}^2\right) + \text{sen}(\varphi)e^{i\phi}\left(\alpha|H\rangle_{SL}^1 + \beta|V\rangle_{LS}^1\right). \quad (2.10)$$

Como pode ser observado em (2.10), o fóton tem probabilidade $\cos^2(\varphi)$ de emergir na saída 2 e $\text{sen}^2(\varphi)$ de emergir na saída 1. Em ambos os casos, o qubit será o mesmo enviado por Alice.

Qualquer erro que possa ser modelado pela seqüência compensador-rotacionador-compensador pode ser corrigido pelos esquemas ópticos das Figs. 2.1 e 2.2, contanto que a variação temporal dos parâmetros da fibra ocorra em uma escala de tempo maior que a separação entre os pulsos S e L.

2.3 Sistema de correção de erros de estados coerentes usando óptica linear

É importante analisar o esquema da Fig. 2.1 no caso em que os pulsos com um único fóton são substituídos por estados coerentes de luz, dada a aplicação de pulsos coerentes mesoscópicos em sistemas de comunicações quânticas [5-7]. No estado inicial $|\alpha, \beta\rangle$ a primeira posição representa a componente horizontal e a segunda representa a

componente vertical. O estado que sai do aparato do transmissor é $|\alpha, 0\rangle_S \otimes |\beta, 0\rangle_L$. O estado após propagação da luz no canal quântico ruidoso é $|\alpha \cos(\varphi)e^{i\lambda}, \alpha \text{sen}(\varphi)e^{i\xi}\rangle_S \otimes |\beta \cos(\varphi)e^{i\lambda}, \beta \text{sen}(\varphi)e^{i\xi}\rangle_L$. Depois da célula de Pockels do receptor o estado é

$$|\alpha \text{sen}(\varphi)e^{i\xi}, \alpha \cos(\varphi)e^{i\lambda}\rangle_S \otimes |\beta \cos(\varphi)e^{i\lambda}, \beta \text{sen}(\varphi)e^{i\xi}\rangle_L \quad (2.11)$$

e depois do HWP tem-se

$$|\alpha \text{sen}(\varphi)e^{i\xi}, 0\rangle_{SS} \otimes |\alpha \cos(\varphi)e^{i\lambda}, \beta \cos(\varphi)e^{i\lambda}\rangle_{SL} \otimes |0, \beta \text{sen}(\varphi)e^{i\xi}\rangle_{LL}. \quad (2.12)$$

Logo, o esquema óptico funciona para estados coerentes também.

As células de Pockels tornam a implementação prática do esquema da Fig. 2.1 um pouco complicada devido à necessidade de sincronização. Um sistema que utiliza a mesma idéia, mas que não precisa de nenhuma ação externa é apresentada na Fig. 2.3 [8].

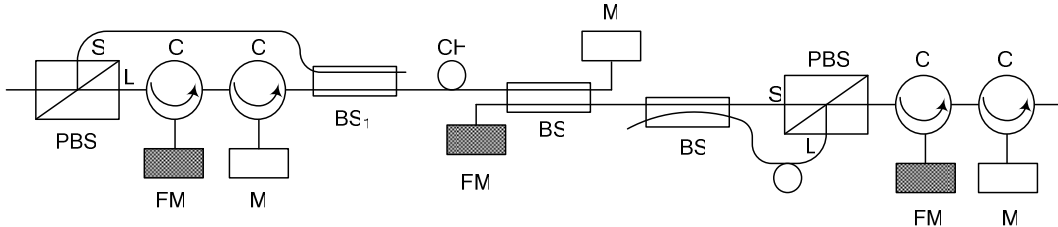


Figura 2.3. Esquema óptico passivo para estados coerentes.

Na Fig. 2.3, BS são divisores de feixe balanceados, BS₁ é um divisor de feixe com transmitância $T = 1/\sqrt{5}$ e refletância $R = 2/\sqrt{5}$. FM é um espelho de Faraday, M é um espelho comum, C é um circulator e CH é o canal quântico. Novamente S e L representam os caminhos curtos e longos, respectivamente. O circuito funciona da seguinte forma. O estado inicial é separado pelo primeiro PBS. A componente horizontal passa pelo caminho curto e a vertical pelo longo. No caminho longo a componente vertical passa por dois circuladores, um espelho de Faraday e um espelho

comum. A sua evolução é $|0, \beta\rangle \xrightarrow{FM} |\beta^*, 0\rangle \xrightarrow{M} |\beta, 0\rangle$. As componentes passam pelo canal separadas por um intervalo de tempo. Novamente, este deve ser pequeno o suficiente para que o canal possa ser considerado o mesmo para ambos os pulsos. O estado na entrada do canal é $|i2\alpha/\sqrt{5}, 0\rangle_S \otimes |\beta/\sqrt{5}\rangle_L$. Após propagação no canal ruidoso, o estado é

$$|i2\alpha \cos(\varphi)e^{i\lambda}/\sqrt{5}, i2\alpha \sin(\varphi)e^{i\xi}/\sqrt{5}\rangle_S \otimes |\beta \cos(\varphi)e^{i\lambda}/\sqrt{5}, \beta \sin(\varphi)e^{i\xi}/\sqrt{5}\rangle_L. \quad (2.13)$$

Quando o pulso do tempo curto chega ao primeiro PBS do aparato do receptor, metade é refletida e metade é transmitida. A parte refletida é desconsiderada. Da parte que vai para M, metade vai para FM. Da parte que vai para FM, metade vai para o segundo PBS. Este pulso é o primeiro que será considerado e o seu estado é

$$|\alpha \sin(\varphi)e^{i\xi}/\sqrt{10}, -\alpha \cos(\varphi)e^{i\lambda}/\sqrt{10}\rangle_S. \quad (2.14)$$

Do pulso no tempo longo será considerada apenas a parcela que é refletida pelo primeiro BS do receptor em direção ao segundo BS. O seu estado é

$$|i\beta \cos(\varphi)e^{i\lambda}/\sqrt{10}, i\beta \sin(\varphi)e^{i\xi}/\sqrt{10}\rangle_L. \quad (2.15)$$

Pelo tempo de chegada é possível identificar os pulsos de interesse. O comprimento do braço longo do transmissor deve ser pelo menos maior que duas vezes a distância entre M e FM para garantir que o pulso no tempo curto será o primeiro a chegar ao segundo BS do receptor. A nova distância entre os pulsos de interesse é igual à diferença entre o caminho longo e o caminho curto do interferômetro do receptor. Logo, o estado na saída do PBS é

$$\left| \frac{\alpha \sin(\varphi)e^{i\xi}}{2\sqrt{5}}, 0 \right\rangle_{SS} \otimes \left| \frac{i\beta \cos(\varphi)e^{i\lambda}}{2\sqrt{5}}, \frac{-i\alpha \cos(\varphi)e^{i\lambda}}{2\sqrt{5}} \right\rangle_{SL} \otimes \left| 0, \frac{-\beta \sin(\varphi)e^{i\xi}}{2\sqrt{5}} \right\rangle_{LL}. \quad (2.16)$$

Depois do espelho de Faraday e do espelho comum o pulso central tem o seguinte estado

$$\left| \frac{-i \cos(\varphi) e^{i\lambda}}{2\sqrt{5}} \alpha, \frac{-i \cos(\varphi) e^{i\lambda}}{2\sqrt{5}} \beta \right\rangle_{SL} \quad (2.17)$$

que possui a mesma polarização do estado enviado pelo transmissor, mostrando que o esquema da Fig. 2.3 funciona bem. A vantagem desse sistema é que não é necessária nenhuma ação externa. Uma desvantagem é que parte da energia é perdida em pulsos inúteis. Devido a essa perda, o circuito proposto não se aplica aos sistemas de comunicações que utilizam fótons isolados. Outro ponto positivo do sistema proposto é o fato de que os aparatos do transmissor e do receptor não precisam ser e não são iguais. No sistema proposto em [3] existe a necessidade de casamento entre os comprimentos das fibras. Isso não é um requisito fácil de atingir devido às flutuações ambientais nas localidades do transmissor e do receptor que estão separados fisicamente. Por fim, em sistemas com altas taxas de transmissão e com grandes distâncias, a dispersão por modo de polarização (PMD) é crítica. Se a fibra for suficientemente longa a PMD pode dividir um pulso em dois, tornando a evolução não unitária e o sistema ineficaz.

2.4 Sistema de correção de erros de pares de fótons entrelaçados usando óptica linear

Com o uso de dois sistemas ópticos do tipo mostrado na Fig. 2.2 é possível construir um sistema óptico para distribuição de um estado de Bell livre de erros. Este sistema é mostrado na Fig.2.4.

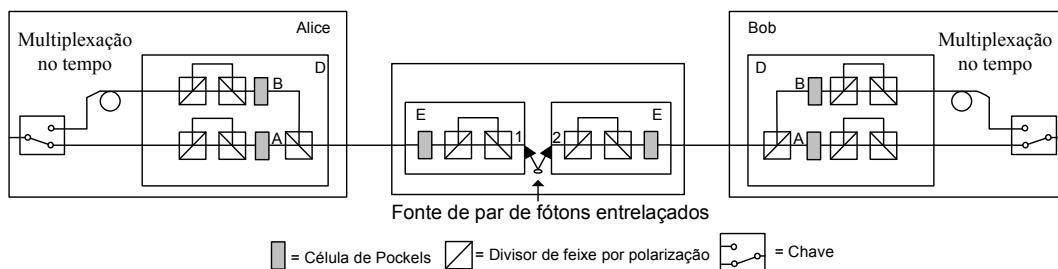


Figura 2.4. Sistema óptico para distribuição livre de erro de um estado de Bell.

Seguindo o procedimento apresentado na Seção 2.2, é possível mostrar que, dado o estado inicial

$$|\Phi\rangle_{12} = \frac{1}{\sqrt{2}} \left[|H\rangle_1 |H\rangle_2 + |V\rangle_1 |V\rangle_2 \right]. \quad (2.18)$$

a evolução ao longo do circuito é

$$|\Phi\rangle_{12} \xrightarrow{E} |\Phi\rangle_{12}^E = \frac{1}{\sqrt{2}} \left[|H\rangle_1^S |H\rangle_2^S + |H\rangle_1^L |H\rangle_2^L \right] \quad (2.19)$$

$$\begin{aligned} |\Phi\rangle_{12}^E \xrightarrow{\frac{U_1}{U_2}} |\Phi\rangle_{12}^{U_1 U_2} = \\ \frac{1}{\sqrt{2}} \left[\left(e^{i\phi_1} \cos(\theta_1) |H\rangle_1^S + e^{i\lambda_1} \sin(\theta_1) |V\rangle_1^S \right) \left(e^{i\phi_2} \cos(\theta_2) |H\rangle_2^S + e^{i\lambda_2} \sin(\theta_2) |V\rangle_2^S \right) + \right. \\ \left. \left(e^{i\phi_1} \cos(\theta_1) |H\rangle_1^L + e^{i\lambda_1} \sin(\theta_1) |V\rangle_1^L \right) \left(e^{i\phi_2} \cos(\theta_2) |H\rangle_2^L + e^{i\lambda_2} \sin(\theta_2) |V\rangle_2^L \right) \right] \end{aligned} \quad (2.20)$$

$$\begin{aligned} |\Phi\rangle_{12}^{U_1 U_2} \xrightarrow{D} |\Phi\rangle_{12}^D = \\ \frac{1}{\sqrt{2}} \left[\left(e^{i\phi_1} \cos(\theta_1) |H\rangle_{1A}^{SL} + e^{i\lambda_1} \sin(\theta_1) |H\rangle_{1B}^{SL} \right) \left(e^{i\phi_2} \cos(\theta_2) |H\rangle_{2A}^{SL} + e^{i\lambda_2} \sin(\theta_2) |H\rangle_{2B}^{SL} \right) + \right. \\ \left. \left(e^{i\phi_1} \cos(\theta_1) |V\rangle_{1A}^{LS} + e^{i\lambda_1} \sin(\theta_1) |V\rangle_{1B}^{LS} \right) \left(e^{i\phi_2} \cos(\theta_2) |V\rangle_{2A}^{LS} + e^{i\lambda_2} \sin(\theta_2) |V\rangle_{2B}^{LS} \right) \right] \end{aligned} \quad (2.21)$$

$$\begin{aligned} |\Phi\rangle_{12}^D = \frac{1}{\sqrt{2}} \left[e^{i\phi_1} \cos(\theta_1) e^{i\phi_2} \cos(\theta_2) \left(|H\rangle_{1A}^{SL} |H\rangle_{2A}^{SL} + |V\rangle_{1A}^{LS} |V\rangle_{2A}^{LS} \right) + \right. \\ e^{i\phi_1} \cos(\theta_1) e^{i\lambda_2} \sin(\theta_2) \left(|H\rangle_{1A}^{SL} |H\rangle_{2B}^{SL} + |V\rangle_{1A}^{LS} |V\rangle_{2B}^{LS} \right) + \\ e^{i\lambda_1} \sin(\theta_1) e^{i\phi_2} \cos(\theta_2) \left(|H\rangle_{1B}^{SL} |H\rangle_{2A}^{SL} + |V\rangle_{1B}^{LS} |V\rangle_{2A}^{LS} \right) + \\ \left. e^{i\lambda_1} \sin(\theta_1) e^{i\lambda_2} \sin(\theta_2) \left(|H\rangle_{1B}^{SL} |H\rangle_{2B}^{SL} + |V\rangle_{1B}^{LS} |V\rangle_{2B}^{LS} \right) \right]. \end{aligned} \quad (2.22)$$

Os canais ruidosos são modelados por evoluções unitárias que realizam a seguinte transformação $U_{1(2)} |H\rangle = \cos(\varphi_{1(2)}) e^{i\phi_{1(2)}} |H\rangle + \sin(\varphi_{1(2)}) e^{i\lambda_{1(2)}} |V\rangle$. O primeiro termo de (2.22), por exemplo, indica que, com probabilidade $\cos^2(\theta_1)\cos^2(\theta_2)$ os fótons emergirão na saída *A* em ambos os lados [9]. Utilizando-se um esquema de multiplexagem no tempo composto de um laço de atraso e uma chave eletro-óptica é possível garantir que ambos os fótons sempre estarão em uma mesma saída em cada lado. Neste caso, a incerteza espacial se transforma numa incerteza temporal.

Capítulo 3

Correção de Erro Quântico em Estados Bipartes

3.1 Introdução

No Capítulo 2, foi mostrado como usar um sistema óptico e linear de correção de erro quântico para proteger individualmente qubits. Neste capítulo, é mostrado que o mesmo sistema da Fig. 2.1 também pode ser utilizado para a correção de erros em estados bipartes de qubits.

3.2 Correção de erros em estados bipartes de qubits

Seja o sistema da Fig. 2.1 redesenhado na Fig. 3.1. O transmissor, chamado Alice, possui um estado biparte de qubits que deseja enviar para o receptor, chamado Bob.

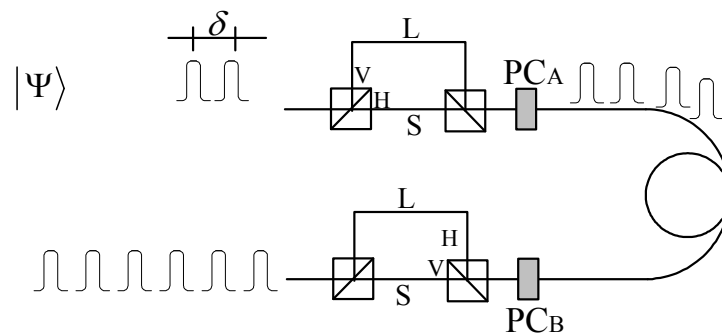


Figura 3.1. Sistema óptico para correção de erro de um estado biparte de qubits.

Assim, Alice possui o estado $|\Psi\rangle = \alpha|HH\rangle_{0\delta} + \beta|HV\rangle_{0\delta} + \gamma|VH\rangle_{0\delta} + \xi|VV\rangle_{0\delta}$, que corresponde a

dois fótons separados por δ no tempo, e ela quer enviar este estado para Bob. O estado quântico após o interferômetro de polarização de Alice é

$$|\psi_1\rangle = \alpha|HH\rangle_{S,\delta S} + \beta|HV\rangle_{S,\delta L} + \gamma|VH\rangle_{L,\delta S} + \xi|VV\rangle_{L,\delta L}. \quad (3.1)$$

O estado depois da célula de Pockels de Alice (PC_A) é

$$|\psi_2\rangle = \alpha|HH\rangle_{S,\delta S} + \beta|HH\rangle_{S,\delta S} + \gamma|HH\rangle_{L,\delta S} + \xi|HH\rangle_{L,\delta L}. \quad (3.2)$$

Em (3.1) pode-se observar que há quatro intervalos de tempo: S , $\delta+S$, L and $\delta+L$ e em (3.2) vê-se que PC_A é ativada com objetivo de rotacionar de $\pi/2$ a polarização apenas dos pulsos nos intervalos de tempo L e $\delta+L$. A propagação pelo canal é modelada por uma transformação unitária que age sobre ambos os qubits. De modo geral, pode-se dizer que $U|HH\rangle = a|HH\rangle + b|HV\rangle + c|VH\rangle + d|VV\rangle$ onde os coeficientes a , b , c e d dependem dos parâmetros de U e variam no tempo. Assim, o estado quântico na saída do canal é

$$\begin{aligned} |\psi_3\rangle = & a\left(\alpha|HH\rangle_{S,\delta S} + \beta|HH\rangle_{S,\delta L} + \gamma|HH\rangle_{L,\delta S} + \xi|HH\rangle_{L,\delta L}\right) + \\ & b\left(\alpha|HV\rangle_{S,\delta S} + \beta|HV\rangle_{S,\delta L} + \gamma|HV\rangle_{L,\delta S} + \xi|HV\rangle_{L,\delta L}\right) + \\ & c\left(\alpha|VH\rangle_{S,\delta S} + \beta|VH\rangle_{S,\delta L} + \gamma|VH\rangle_{L,\delta S} + \xi|VH\rangle_{L,\delta L}\right) + \\ & d\left(\alpha|VV\rangle_{S,\delta S} + \beta|VV\rangle_{S,\delta L} + \gamma|VV\rangle_{L,\delta S} + \xi|VV\rangle_{L,\delta L}\right). \end{aligned} \quad (3.3)$$

Bob, por sua vez, ativa a célula de Pockels PC_B com o objetivo de rotacionar de $\pi/2$ a polarização dos pulsos nos intervalos de tempo L e $\delta+L$. Além disso, no interferômetro de Bob, a componente horizontal passa pelo caminho longo e a vertical pelo curto. Assim o estado na saída de Bob é dado por

$$\begin{aligned} |\psi_4\rangle = & a\left(\alpha|HH\rangle_{SL,\delta SL} + \beta|HV\rangle_{SL,\delta LS} + \gamma|VH\rangle_{LS,\delta SL} + \xi|VV\rangle_{LS,\delta LS}\right) + \\ & b\left(\alpha|HV\rangle_{SL,\delta SS} + \beta|HH\rangle_{SL,\delta LL} + \gamma|VV\rangle_{LS,\delta SS} + \xi|VH\rangle_{LS,\delta LL}\right) + \\ & c\left(\alpha|VH\rangle_{SS,\delta SL} + \beta|VV\rangle_{SS,\delta LS} + \gamma|HH\rangle_{LL,\delta SL} + \xi|HV\rangle_{LL,\delta LS}\right) + \\ & d\left(\alpha|VV\rangle_{SS,\delta SS} + \beta|VH\rangle_{SS,\delta LL} + \gamma|HV\rangle_{LL,\delta SS} + \xi|HH\rangle_{LL,\delta LL}\right) \end{aligned} \quad (3.4)$$

Como pode ser visto em (3.4), há seis intervalos de tempo na saída: $S+S$, $S+S+\delta$, $S+L$, $S+L+\delta$, $L+L$, $L+L+\delta$. O estado correto é encontrado nos intervalos $S+L$, $S+L+\delta$ com probabilidade $|a|^2$. Dessa forma, selecionando apenas estes intervalos de tempo, sempre que houver fótons pode-se garantir que eles representam o estado biparte que foi inicialmente enviado por Alice.

Capítulo 4

Sistemas Ópticos para Teleportação de Qubits

4.1 Introdução

A teleportação quântica é uma técnica para enviar um estado quântico entre dois pontos distantes (Alice e Bob) sem que o portador da informação seja enviado [1]. Para que isso seja possível é necessário que haja entre eles um canal clássico e que cada um possua um qubit de um estado biparte entrelaçado. Em especial, se o par de qubits entrelaçados for um par EPR, como o estado $(|00\rangle+|11\rangle)/2^{1/2}$, então a taxa de erro é nula e a de transmissão de informação é máxima. Com esses pré-requisitos é possível enviar de Alice para Bob um estado quântico qualquer desconhecido por ambos. O circuito quântico da Fig. 4.1 mostra o processo de teleportação.

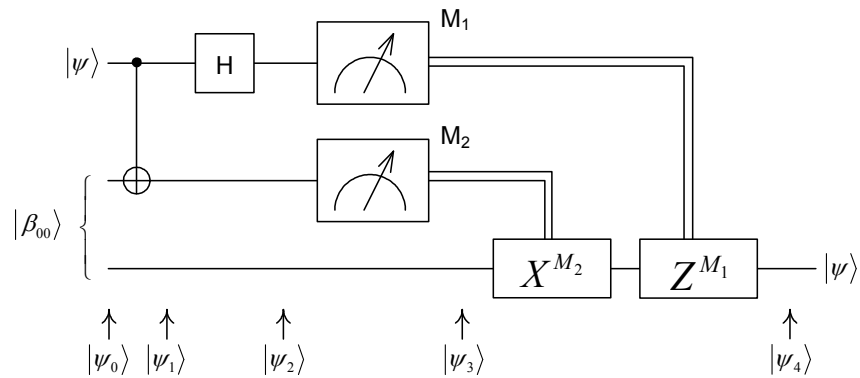


Figura 4.1. Circuito quântico para teleportar um qubit.

Inicialmente, Alice possui um qubit qualquer $|\psi\rangle=\alpha|0\rangle+\beta|1\rangle$ e deseja enviá-lo para Bob. Alice e Bob possuem, antecipadamente, cada um, um qubit de um par de EPR $|\beta_{00}\rangle=(|00\rangle+|11\rangle)/2^{1/2}$. Analisando o circuito da Fig. 4.1 percebe-se que Alice realiza uma operação nos dois qubits que estão com ela e em seguida os mede. O resultado dessa

medição é a informação necessária para que Bob converta, através da aplicação de transformações unitárias, o qubit que está em seu poder no estado que inicialmente estava com Alice. Isso fica mais claro quando se acompanha a evolução ao longo do circuito. Primeiramente, tem-se o estado

$$|\psi_0\rangle = |\psi\rangle|\beta_{00}\rangle = \frac{1}{\sqrt{2}}[\alpha|0\rangle(|00\rangle+|11\rangle) + \beta|1\rangle(|00\rangle+|11\rangle)], \quad (4.1)$$

sendo que os dois qubits à esquerda pertencem à Alice e o terceiro à Bob. Alice passa os seus dois qubits pela porta CNOT, obtendo o estado

$$|\psi_1\rangle = \frac{1}{\sqrt{2}}[\alpha|0\rangle(|00\rangle+|11\rangle) + \beta|1\rangle(|10\rangle+|01\rangle)] \quad (4.2)$$

Em seguida, ela passa o primeiro qubit por uma porta Hadamard. Obtendo o estado

$$|\psi_2\rangle = \frac{1}{2}[\alpha(|0\rangle+|1\rangle)(|00\rangle+|11\rangle) + \beta(|0\rangle-|1\rangle)(|10\rangle+|01\rangle)] = \quad (4.3)$$

$$= \frac{1}{2}[\alpha(|00\rangle+|10\rangle+|01\rangle+|11\rangle) + \beta(|10\rangle-|01\rangle-|11\rangle+|00\rangle)]. \quad (4.4)$$

Logo, de acordo com o resultado da medição dos qubits que estão consigo, Alice pode informar a Bob, via canal clássico, a operação que aplicada ao qubit dele levará a obtenção de $|\psi\rangle$. Como há quatro diferentes possibilidades, Alice tem que enviar dois bits clássicos para Bob: $00 \rightarrow I$, $01 \rightarrow X$, $10 \rightarrow Z$ e $11 \rightarrow ZX$.

Não há qualquer contradição entre teleportação quântica e transmissão de dados mais rápido que a velocidade da luz, uma vez que para realizar a teleportação é necessária a comunicação entre Alice e Bob via canal clássico. Também não há violação do princípio da não clonagem, visto que Alice consome o estado $|\psi\rangle$.

A realização de alguns protocolos de comunicação quântica requer operações não lineares. A teleportação quântica é um exemplo, pois, como pode ser visto na Fig. 4.1, uma porta CNOT é necessária. Entretanto, a realização prática de uma porta CNOT requer dispositivos ópticos que apresentem alta não linearidade, o que não é ainda

disponível na atualidade. Assim, tem sido proposta a utilização de dispositivos ópticos lineares para implementar sistemas de comunicações quânticos. O preço dessa escolha é o comportamento probabilístico de tais sistemas [10-12]. Dessa forma, o sistema tem uma probabilidade de sucesso na realização da tarefa a que é destinado e, em caso de falha, há uma sinalização indicativa da mesma.

Nesta direção, o presente capítulo apresenta um circuito óptico, baseado em dispositivos ópticos lineares, que implementa a teleportação probabilística de um qubit codificado na polarização de um fóton [13]. Adicionalmente, é utilizado um circuito óptico para correção de erro quântico semelhante ao apresentado na Seção 2.4 para distribuição de um par de qubits entrelaçados.

4.2 Geração probabilística de um estado de Bell com qubit codificado na polarização

Um gerador probabilístico de estados de Bell com qubit codificado na polarização de fótons pode ser produzido usando-se apenas um PBS. Um par de fótons entrelaçados é produzido com probabilidade 50% se o estado $[(|H\rangle+|V\rangle)/2^{1/2}] \otimes [(|H\rangle+|V\rangle)/2^{1/2}]$ for colocado na entrada de um divisor de feixes por polarização que resolve na base horizontal-vertical. Nesse caso, o estado final na saída do PBS é $[(|HH\rangle+|VV\rangle)/2^{1/2}]/2^{1/2} + [(|0,HV\rangle+|HV,0\rangle)/2^{1/2}]/2^{1/2}$. O PBS pode ser localizado no transmissor, por exemplo. Então, ele mantém um fóton consigo e manda o outro para o receptor através de um canal óptico. Uma outra forma possível de gerar um par entrelaçado é mostrado na Fig. 4.2.

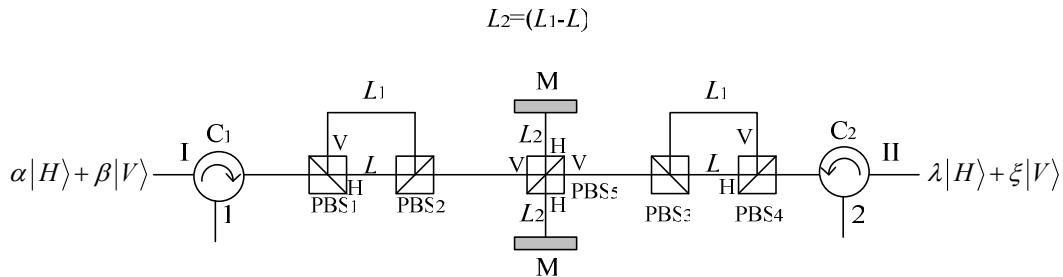


Figura 4.2. Circuito óptico para geração probabilística de um estado de Bell.

Na Fig. 4.2, C_1 e C_2 são circuladores ópticos, M são espelhos comuns, L , L_1 e L_2 são

comprimentos de fibra óptica que obedecem às relações $L_1 > L$ e $L_2 = L_1 - L$. Considerando como estado inicial o estado $[\alpha|H\rangle + \beta|V\rangle] \otimes [\lambda|H\rangle + \xi|V\rangle]$, o sistema evolui como mostrado nas equações (4.5)-(4.8)

$$|\psi\rangle_{I,II} = (\alpha|H\rangle + \beta|V\rangle)(\lambda|H\rangle + \xi|V\rangle) = \quad (4.5)$$

$$= \alpha\lambda|HH\rangle + \alpha\xi|HV\rangle + \beta\lambda|VH\rangle + \beta\xi|VV\rangle \xrightarrow[\text{PBS}_{3,4}]{\text{PBS}_{1,2}}$$

$$= \alpha^*\lambda^*|H_{L_2L_2}H_{L_2L_2}\rangle + \alpha^*\xi^*|H_{L_2L_2}V_{L_2}, 0\rangle + \beta\lambda^*|0, V_{L_2}H_{L_2L_2}\rangle + \beta\xi^*|V_{L_2}V_{L_2}\rangle \xrightarrow[\text{PBS}_{3,4}]{\text{PBS}_{1,2}} \quad (4.6)$$

$$\alpha^*\lambda^*|H_{L_2L_2}H_{L_2L_2}\rangle + \alpha^*\xi^*|H_{L_2L_2}V_{L_2}, 0\rangle + \beta\lambda^*|0, V_{L_2}H_{L_2L_2}\rangle + \beta\xi^*|V_{L_2}V_{L_2}\rangle = |\psi\rangle_{12} \quad (4.7)$$

Em particular, se $\alpha = \beta = \lambda = \xi = 2^{-1/2}$, então o estado de saída é

$$\frac{(|HH\rangle + |VV\rangle)/\sqrt{2} + (|0, HV\rangle + |HV, 0\rangle)/\sqrt{2}}{\sqrt{2}} \quad (4.8)$$

Assim, o estado de Bell é produzido com probabilidade de 50%. No entanto, o circuito óptico da Fig. 4.2 não apenas gera como também distribui os pares de fótons entrelaçados.

4.3 Circuito óptico para teleportação probabilística de estados quânticos

O circuito óptico da Figura 4.3 realiza a teleportação de um qubit codificado na polarização de um fóton de forma probabilística.

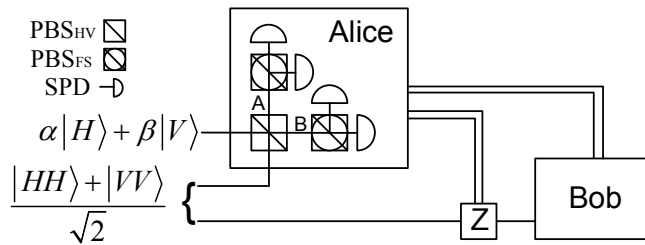


Figura 4.3. Circuito óptico para teleportação probabilística de qubits codificados na polarização.

Na Fig. 4.3 SPD representa um detector de fótons isolados, PBS_{HV} é um divisor de feixes por polarização na base retangular e PBS_{FS} é um PBS na base diagonal. Por fim, as linhas duplas indicam canais clássicos de comunicação. A evolução do estado quântico é

$$|\psi\rangle_{in} = \alpha|H\rangle + \beta|V\rangle \left(\frac{|HH\rangle + |VV\rangle}{\sqrt{2}} \right) = \frac{\alpha|HHH\rangle + \alpha|HVV\rangle + \beta|VHH\rangle + \beta|VVV\rangle}{\sqrt{2}} \quad (4.9)$$

$$|\psi\rangle_{PBS_W} = \frac{\alpha|HHH\rangle + \beta|VVV\rangle}{\sqrt{2}} + \frac{\alpha|HV,0,V\rangle + \beta|0,VH,H\rangle}{\sqrt{2}} = \frac{1}{\sqrt{2}} [\alpha|HHH\rangle + \beta|VVV\rangle] + \frac{1}{\sqrt{2}} |\Omega\rangle \quad (4.10)$$

$$|\psi\rangle_{PBS_{FS}} = \frac{\alpha(|F\rangle + |S\rangle)(|F\rangle + |S\rangle)|H\rangle + \beta(|F\rangle - |S\rangle)(|F\rangle - |S\rangle)|V\rangle}{2\sqrt{2}} + \frac{1}{\sqrt{2}} |\Omega\rangle =$$

$$\frac{1}{\sqrt{2}} \frac{|FF\rangle(\alpha|H\rangle + \beta|V\rangle) + |SS\rangle(\alpha|H\rangle + \beta|V\rangle) + |FS\rangle(\alpha|H\rangle - \beta|V\rangle) + |SF\rangle(\alpha|H\rangle - \beta|V\rangle)}{2} + \frac{1}{\sqrt{2}} |\Omega\rangle \quad (4.11)$$

Por simplificação, o estado $|\Omega\rangle$ representa os casos em que não ocorre teleportação por que ambos os fótons tomaram o mesmo caminho (A ou B) no PBS de Alice. Alice envia dois bits clássicos à Bob. O primeiro informa se houve teleportação, o que acontece em 50% dos casos, e o segundo, que só será lido caso haja teleportação, informa se Bob deve ou não aplicar ao seu qubit a operação de inversão de fase, Z .

O sistema da Fig. 4.3 pode ser feito mais completo inserindo-se também o circuito óptico gerador do estado de Bell. Assim, unindo os sistemas das Figs. 4.2 e 4.3 tem-se, na Fig. 4.4, o circuito completo para teleportação probabilística.

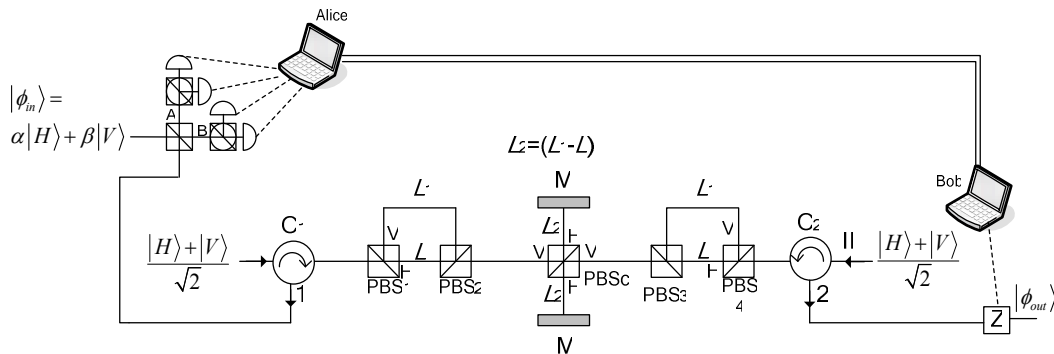


Figura 4.4. Circuito óptico completo para teleportação probabilística de qubits de polarização.

Por fim, é apresentado na Fig. 4.5 um circuito óptico completo para teleportação probabilística de qubits de polarização, com o sistema de correção de erros da Seção 2.4. Neste caso, o estado de Bell é gerado usando-se apenas um PBS, possivelmente em um nó central, e os fótons são enviados aos usuários do sistema de comunicação através de canais ruidosos.

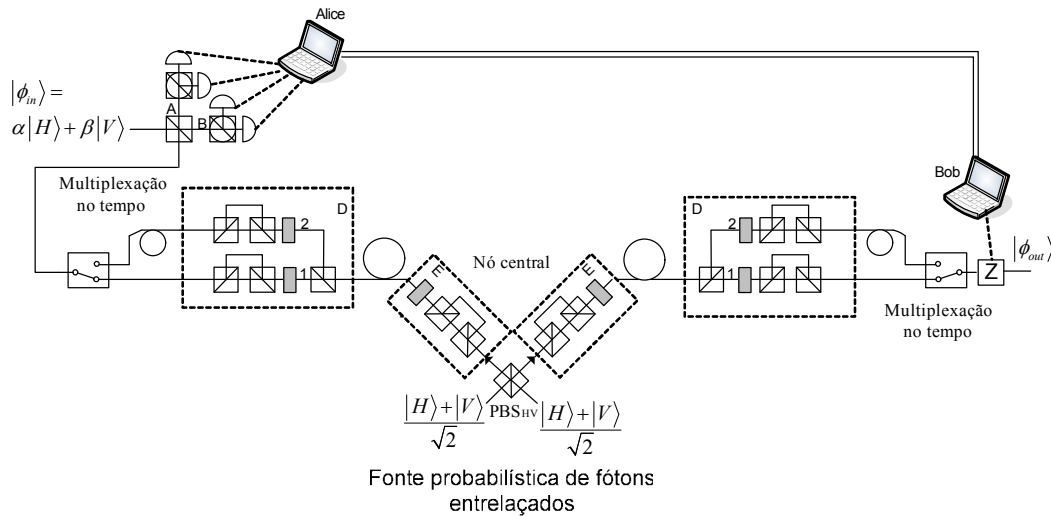


Figura 4.5. Circuito óptico para teleportação probabilística de estados quânticos com correção de erros.

Usando o circuito óptico da Fig. 4.5 a teleportação quântica será realizada com probabilidade $0,25\cos^2(\varphi_a)$ se Bob apenas medir os qubits recebidos. O termo $\cos^2(\varphi_a)$ aparece devido ao fato de Alice enviar o qubit $|\phi_{in}\rangle$ no tempo certo para que haja coincidência com a chegada do fóton que toma o caminho 1. Nos casos em que o fóton toma o caminho 2 não há teleportação. Caso Bob pretenda usar o qubit teletransportado para realizar outra operação quântica, ele terá que saber o tempo exato de chegada do fóton. Assim, a probabilidade de sucesso, assumindo que Bob também realiza uma sincronização com a saída 1, é $0,25\cos^2(\varphi_a)\cos^2(\varphi_b)$.

Capítulo 5

Conclusões e Perspectivas

5.1 Conclusões

Tendo sido realizada uma análise de sistemas de correção de erro que utilizam redundância e qubit time-bin, podem ser citadas as seguintes conclusões:

1. Ambas as abordagens realizam a correção desejada.
2. A realização experimental do sistema de correção de erro que utiliza qubit time-bin é mais simples que a realização do sistema que utiliza redundância, pois embora o primeiro possa exigir uma delicada sincronização, esta tarefa ainda é mais simples que a realização de operações não lineares exigida pelo segundo, que requerem materiais que ainda não existem e lasers de alta potência.
3. É possível fazer a correção de erros com o sistema que utiliza qubit time-bin sem utilizar sincronização, como proposto e mostrado na dissertação. Este sistema funciona bem em comunicações quânticas com estados coerentes e apresenta baixo desempenho em comunicações com fótons isolados, devido à grande taxa de perda destes.
4. É possível utilizar o sistema de correção de erros com qubit time-bin para a correção de um par de fótons entrelaçados. Isto é importante, pois a realização de vários protocolos de comunicação quântica requer a distribuição de fótons entrelaçados.
5. É possível utilizar o sistema de correção de erros com qubit time-bin para a correção de erros em estados biparte de qubits, como proposto e mostrado na dissertação.

Em relação aos sistemas de teletransportação as seguintes conclusões podem ser citadas:

1. A realização de teletransportação com dispositivos ópticos lineares permite a implementação experimental de protocolos de comunicação que utilizem teletransportação, com baixo custo. O preço a ser pago é o comportamento probabilístico. Assim, os sistemas ópticos propostos nesta dissertação para a realização de teletransportação em rede ópticas são relativamente simples e podem ser implementados em redes ópticas implantadas.
2. O sistema óptico de distribuição de um par de fótons entrelaçados pode ser utilizado na implementação de diversos protocolos que necessitem de um par de fótons entrelaçados como teletransportação, distribuição quântica de chaves e jogos quânticos.
3. Uma dificuldade prática na construção dos sistemas de teletransportação mostrados nas Figuras 4.4 e 4.5 é que os interferômetros de polarização devem ser idênticos, o que exige que haja controle das condições ambientais onde os mesmos se encontram de forma que os comprimentos das fibras do interferômetro não variem.

5.2 Perspectivas

Como perspectiva de trabalhos futuros pode-se apontar:

1. A realização experimental dos sistemas de correção de erros que utilizam qubit time-bin.
2. A proposição de sistemas ópticos para a teletransportação de estados biparte de qubit.
3. A análise de erro dos sistemas propostos quando da consideração de perdas, dispersão de polarização e ruído e ineficiência de detectores de fótons isolados reais.

Referências

- [1] M.A. Nielsen, I.L. Chuang, Quantum Computation and Quantum Information, Cambridge Univ. Press, Cambridge, 2000.
- [2] P.W. Schor, “Scheme for reducing decoherence in quantum computer memory”, Phys. Rev. A 52 R2493, 1995.
- [3] D. Kalamidas, “Single-photon quantum error rejection and correction with linear optics”, Phys. Lett. A, 343, 331, 2005.
- [4] J. C. do Nascimento, F. A. Mendonça and R. V. Ramos, “Linear optical setups for active and passive quantum error correction in polarization encoded qubits”, quant-ph/0608162, 2006.
- [5] H. Yuen, “KCQ: A New Approach to Quantum Cryptography I. General Principles and Key Generation”, quant-ph/0311061, 2004.
- [6] G. Barbosa, E. Corndorf, P. Kumar, H. Yuen, “Secure Communication Using Mesoscopic Coherent States”, Phys. Rev. Lett. 90 227901, 2003.
- [7] E. Corndorf, G. Barbosa, C. Liang, H. Yuen, P. Kumar, “High-speed data encryption over 25 Km of fiber by two-mode coherent-state quantum cryptography”, Opt. Lett. 28 2040, 2003.
- [8] D. B. de Brito, R. V. Ramos, “Passive quantum error correction with linear optics”, Phys. Lett. A, 352, 206, 2006.
- [9] D. Kalamidas, “Linear optical scheme for error-free entanglement distribution and a quantum repeater”, Phys. Rev. A, 73, 054304, 2006.
- [10] E. Knill, R. Laflamme and G. J. Milburn, “A scheme for efficient quantum computation with linear optics”, Nature, 409, 46, 2001.
- [11] T. B. Pitman, B. C. Jacobs and J. D. Franson, “Experimental Demonstration of a Quantum Circuit using Linear Optics Gates”, quant-ph/0404059, 2004.
- [12] T. C. Ralph, A. G. White, W. J. Munro, and G. J. Milburn, “Simple scheme for efficient linear optics quantum gates”, Phys. Rev. A, 65, 012314, 2001.
- [13] D. B. de Brito, J. B. R. Silva, R. V. Ramos, “Optical Setups for Probabilistic Bipartite and Tripartite Entanglement Generation and Quantum Teleportation in Optical Networks”, submetido para Journal of Modern Optics, 2007.

Apêndice A

Análise dos Códigos de 5 e 9 qubits

A.1 Código de Shor

Este código pode proteger a informação de um qubit contra o efeito de um erro arbitrário. O código proposto por Shor é uma combinação dos códigos para corrigir inversão de fase e inversão de bit [2]. A Fig. A1 mostra o circuito quântico que implementa esse código.

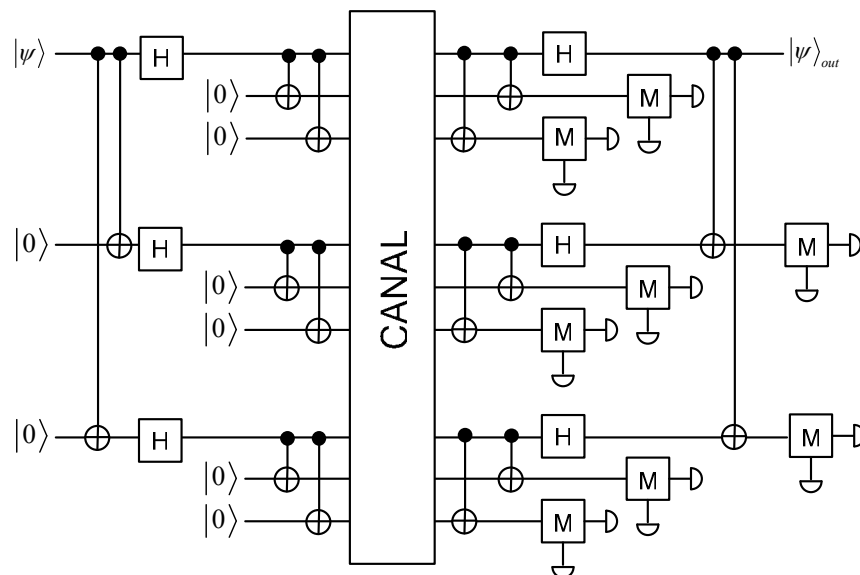


Figura A 1. Circuito quântico para o código de Shor.

A seguir é apresentada a evolução do estado através do circuito. Será mostrado que este código pode corrigir um erro arbitrário em um qubit. Primeiramente, acontece a fase de codificação do estado.

$$|\psi\rangle_{in} = [(\alpha|0\rangle + \beta|1\rangle)|00000000\rangle] = (\alpha|00000000\rangle + \beta|10000000\rangle) \xrightarrow{C_1} \quad (A.1)$$

$$\begin{aligned} & (\alpha|00000000\rangle + \beta|100100100\rangle) \xrightarrow{H_1} (\alpha|+00+00+00\rangle + \beta|-00-00-00\rangle) = \\ & = \alpha [(|000\rangle + |100\rangle)(|000\rangle + |100\rangle)(|000\rangle + |100\rangle)] / 2\sqrt{2} + \\ & + \beta [(|000\rangle - |100\rangle)(|000\rangle - |100\rangle)(|000\rangle - |100\rangle)] / 2\sqrt{2} \\ & \xrightarrow{C_2} \alpha [(|000\rangle + |111\rangle)(|000\rangle + |111\rangle)(|000\rangle + |111\rangle)] / 2\sqrt{2} + \\ & + \beta [(|000\rangle - |111\rangle)(|000\rangle - |111\rangle)(|000\rangle - |111\rangle)] / 2\sqrt{2} = \\ & = \alpha(|00000000\rangle + |000000111\rangle + |000111000\rangle + |000111111\rangle \\ & + |111000000\rangle + |111000111\rangle + |111111000\rangle + |111111111\rangle) / 2\sqrt{2} + \\ & + \beta(|00000000\rangle - |000000111\rangle - |000111000\rangle + |000111111\rangle - \\ & - |111000000\rangle + |111000111\rangle + |111111000\rangle - |111111111\rangle) / 2\sqrt{2} = |\psi\rangle_{cod} \quad (A.2) \end{aligned}$$

Em que C representa as portas CNOT e H a porta Hadamard. Em seguida é introduzido um erro arbitrário. Considerando um erro no primeiro qubit do tipo

$$|0\rangle = a|0\rangle + b|1\rangle, |1\rangle = c|0\rangle + d|1\rangle, \text{ tem-se}$$

$$\begin{aligned} |\psi\rangle_{err} & = \alpha(a|00000000\rangle + b|10000000\rangle + a|000000111\rangle + b|100000111\rangle + \\ & + a|000111000\rangle + b|100111000\rangle + a|000111111\rangle + b|100111111\rangle + \\ & + c|011000000\rangle + d|111000000\rangle + c|011000111\rangle + d|111000111\rangle + \\ & + c|011111000\rangle + d|111111000\rangle + c|011111111\rangle + d|111111111\rangle) / 2\sqrt{2} + \\ & + \beta(a|00000000\rangle + b|10000000\rangle - a|000000111\rangle - b|100000111\rangle - \\ & - a|000111000\rangle - b|100111000\rangle + a|000111111\rangle + b|100111111\rangle - \\ & - c|011000000\rangle - d|111000000\rangle + c|011000111\rangle + d|111000111\rangle + \\ & + c|011111000\rangle + d|111111000\rangle - c|011111111\rangle - d|111111111\rangle) / 2\sqrt{2} \quad (A.3) \end{aligned}$$

Finalmente, o estado chega à fase de decodificação.

$$\begin{aligned}
& |\psi\rangle_{err} \xrightarrow{C_3} \\
& \alpha(a|00000000\rangle + b|11100000\rangle + a|000000100\rangle + b|111000100\rangle + \\
& + a|000100000\rangle + b|111100000\rangle + a|000100100\rangle + b|111100100\rangle + \\
& + c|011000000\rangle + d|100000000\rangle + c|011000100\rangle + d|100000100\rangle + \\
& + c|011100000\rangle + d|100100000\rangle + c|011100100\rangle + d|100100100\rangle) / 2\sqrt{2} + \\
& + \beta(a|00000000\rangle + b|11100000\rangle - a|000000100\rangle - b|111000100\rangle - \\
& - a|000100000\rangle - b|111100000\rangle + a|000100100\rangle + b|111100100\rangle - \\
& - c|011000000\rangle - d|100000000\rangle + c|011000100\rangle + d|100000100\rangle + \\
& + c|011100000\rangle + d|100100000\rangle - c|011100100\rangle - d|100100100\rangle) / 2\sqrt{2} = \\
& = \alpha(a|000+00+00\rangle + b|111+00+00\rangle + c|011+00+00\rangle + d|100+00+00\rangle) / \sqrt{2} + \\
& + \beta(a|000-00-00\rangle + b|111-00-00\rangle - c|011-00-00\rangle - d|100-00-00\rangle) / \sqrt{2} \\
& \xrightarrow{H_z} \\
& \alpha(a|+00000000\rangle + b|-11000000\rangle + c|+11000000\rangle + d|-00000000\rangle) / \sqrt{2} + \\
& + \beta(a|+00100100\rangle + b|-11100100\rangle - c|+11100100\rangle - d|-00100100\rangle) / \sqrt{2} = \\
& = \alpha(a|000000000\rangle + a|100000000\rangle + b|011000000\rangle - b|111000000\rangle + \\
& + c|011000000\rangle + c|111000000\rangle + d|000000000\rangle - d|100000000\rangle) / 2 + \\
& + \beta(a|000100100\rangle + a|100100100\rangle + b|011100100\rangle - b|111100100\rangle - \\
& - c|011100100\rangle - c|111100100\rangle - d|000100100\rangle + d|100100100\rangle) / 2 \\
& \xrightarrow{C_4} \\
& \alpha(a|000000000\rangle + a|100100100\rangle + b|011000000\rangle - b|111100100\rangle + \\
& + c|011000000\rangle + c|111100100\rangle + d|000000000\rangle - d|100100100\rangle) / 2 + \\
& + \beta(a|000100100\rangle + a|100000000\rangle + b|011100100\rangle - b|111000000\rangle - \\
& - c|011100100\rangle - c|111000000\rangle - d|000100100\rangle + d|100000000\rangle) / 2 = \\
& = (\alpha|0\rangle + \beta|1\rangle)[(a+d)/2|00000000\rangle] + (\alpha|1\rangle + \beta|0\rangle)[(a-d)/2|00100100\rangle] + \\
& (\alpha|0\rangle - \beta|1\rangle)[(c+b)/2|11000000\rangle] + (\alpha|1\rangle - \beta|0\rangle)[(c-b)/2|11100100\rangle] \tag{A.4}
\end{aligned}$$

Foi mostrado que qualquer erro sobre o primeiro qubit pode ser corrigido. Com base no resultado da medição dos oito últimos qubits é possível determinar a operação (I , X , Z , XZ) necessária para recuperar o qubit transmitido. O código pode corrigir qualquer erro em 1 qubit.

A.2 Código de 5 qubits

O menor tamanho para um código quântico que corrija um erro arbitrário em um qubit é cinco qubits. A seguir é apresentado o código e o circuito que o implementa (figura A2).

$$|0_L\rangle = |00000\rangle + |10010\rangle + |01001\rangle + |10100\rangle + |01010\rangle - |11011\rangle - |00110\rangle - |11000\rangle - |11101\rangle - |00011\rangle - |11110\rangle - |01111\rangle - |10001\rangle - |01100\rangle - |10111\rangle + |00101\rangle$$

$$1_L = X 0_L$$

$$|1_L\rangle = |11111\rangle + |01101\rangle + |10110\rangle + |01011\rangle + |10101\rangle - |00100\rangle - |11001\rangle - |00111\rangle - |00010\rangle - |11100\rangle - |00001\rangle - |10000\rangle - |01110\rangle - |10011\rangle - |01000\rangle + |11010\rangle$$

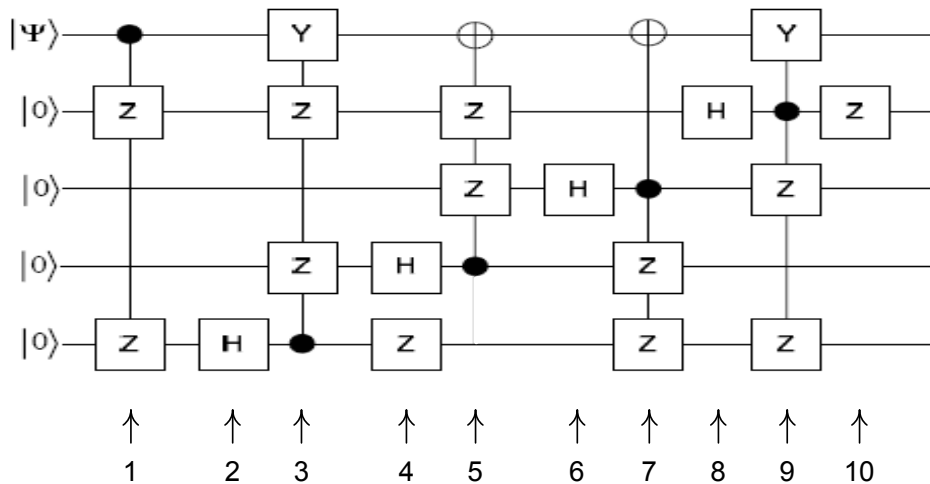


Figura A 2. Circuito de codificação para estados de 5 qubits.

No circuito da Figura A2, $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$. X é uma porta NOT. Z é a porta phase flip. Y é a porta XZ. H é porta Hadamard. O circuito mostrado realiza a codificação desse estado. É mostrada a seguir a evolução do estado $|\psi\rangle_{in} = \alpha|0\rangle + \beta|1\rangle|0000\rangle$ ao longo do circuito.

$$|\psi\rangle_{in} = [(\alpha|0\rangle + \beta|1\rangle)|0000\rangle] = \alpha|00000\rangle + \beta|10000\rangle \xrightarrow{1} \quad (A.5)$$

$$\begin{aligned} & \alpha|00000\rangle + \beta|10000\rangle \xrightarrow{2} (\alpha|0000\rangle + \beta|1000\rangle) / \sqrt{2} = \\ & = (\alpha|00000\rangle + \alpha|00001\rangle + \beta|10000\rangle + \beta|10001\rangle) / \sqrt{2} \xrightarrow{3} \\ & (\alpha|00000\rangle + \alpha|10001\rangle + \beta|10000\rangle - \beta|00001\rangle) / \sqrt{2} \xrightarrow{4} (\alpha|000+0\rangle - \alpha|100+1\rangle + \beta|100+0\rangle + \beta|000+1\rangle) / 2 = \\ & = (\alpha|00000\rangle + \alpha|00010\rangle - \alpha|10001\rangle - \alpha|10011\rangle + \beta|10000\rangle + \beta|10010\rangle + \beta|00001\rangle + \beta|00011\rangle) / 2 \xrightarrow{5} \\ & (\alpha|00000\rangle + \alpha|10010\rangle - \alpha|10001\rangle - \alpha|00011\rangle + \beta|10000\rangle + \beta|00010\rangle + \beta|00001\rangle + \beta|10011\rangle) / 2 \xrightarrow{6} \\ & (\alpha|00+00\rangle + \alpha|10+10\rangle - \alpha|10+01\rangle - \alpha|00+11\rangle + \beta|10+00\rangle + \beta|00+10\rangle + \beta|00+01\rangle + \beta|10+11\rangle) / 2\sqrt{2} = \\ & = (\alpha|00000\rangle + \alpha|00100\rangle + \alpha|10010\rangle + \alpha|10110\rangle - \alpha|10001\rangle - \alpha|10101\rangle - \alpha|00011\rangle - \alpha|00111\rangle + \\ & + \beta|10000\rangle + \beta|10100\rangle + \beta|00010\rangle + \beta|00110\rangle + \beta|00001\rangle + \beta|00101\rangle + \beta|10011\rangle + \beta|10111\rangle) / 2\sqrt{2} \xrightarrow{7} \\ & (\alpha|00000\rangle + \alpha|10100\rangle + \alpha|10010\rangle - \alpha|00110\rangle - \alpha|10001\rangle + \alpha|00101\rangle - \alpha|00011\rangle - \alpha|10111\rangle + \\ & + \beta|10000\rangle + \beta|00100\rangle + \beta|00010\rangle - \beta|10110\rangle + \beta|00001\rangle - \beta|10101\rangle + \beta|10011\rangle + \beta|00111\rangle) / 2\sqrt{2} \xrightarrow{8} \\ & (\alpha|0+000\rangle + \alpha|1+100\rangle + \alpha|1+010\rangle - \alpha|0+110\rangle - \alpha|1+001\rangle + \alpha|0+101\rangle - \alpha|0+011\rangle - \alpha|1+111\rangle + \\ & + \beta|1+000\rangle + \beta|0+100\rangle + \beta|0+010\rangle - \beta|1+110\rangle + \beta|0+001\rangle - \beta|1+101\rangle + \beta|1+011\rangle + \beta|0+111\rangle) / 4 = \\ & (\alpha|00000\rangle + \alpha|01000\rangle + \alpha|10100\rangle + \alpha|11100\rangle + \alpha|10010\rangle + \alpha|11010\rangle - \alpha|00110\rangle - \alpha|01110\rangle - \\ & - \alpha|10001\rangle - \alpha|11001\rangle + \alpha|00101\rangle + \alpha|01101\rangle - \alpha|00011\rangle - \alpha|01011\rangle - \alpha|10111\rangle - \alpha|11111\rangle + \\ & + \beta|10000\rangle + \beta|11000\rangle + \beta|00100\rangle + \beta|01100\rangle + \beta|00010\rangle + \beta|01010\rangle - \beta|10110\rangle - \beta|11110\rangle + \\ & + \beta|00001\rangle + \beta|01001\rangle - \beta|10101\rangle - \beta|11101\rangle + \beta|10011\rangle + \beta|11011\rangle + \beta|00111\rangle + \beta|01111\rangle) / 4 \xrightarrow{9} \\ & (\alpha|00000\rangle + \alpha|11000\rangle + \alpha|10100\rangle + \alpha|01100\rangle + \alpha|10010\rangle - \alpha|01010\rangle - \alpha|00110\rangle + \alpha|11110\rangle - \\ & - \alpha|10001\rangle - \alpha|01001\rangle + \alpha|00101\rangle + \alpha|11101\rangle - \alpha|00011\rangle + \alpha|11011\rangle - \alpha|10111\rangle + \alpha|01111\rangle + \\ & + \beta|10000\rangle - \beta|01000\rangle + \beta|00100\rangle - \beta|11100\rangle + \beta|00010\rangle + \beta|11010\rangle - \beta|10110\rangle - \beta|01110\rangle + \\ & + \beta|00001\rangle - \beta|11001\rangle - \beta|10101\rangle + \beta|01101\rangle + \beta|10011\rangle + \beta|01011\rangle + \beta|00111\rangle + \beta|11111\rangle) / 4 \xrightarrow{10} \\ & (\alpha|00000\rangle - \alpha|11000\rangle + \alpha|10100\rangle - \alpha|01100\rangle + \alpha|10010\rangle + \alpha|01010\rangle - \alpha|00110\rangle - \alpha|11110\rangle - \\ & - \alpha|10001\rangle + \alpha|01001\rangle + \alpha|00101\rangle - \alpha|11101\rangle - \alpha|00011\rangle - \alpha|11011\rangle - \alpha|10111\rangle - \alpha|01111\rangle + \\ & + \beta|10000\rangle + \beta|01000\rangle + \beta|00100\rangle + \beta|11100\rangle + \beta|00010\rangle - \beta|11010\rangle - \beta|10110\rangle + \beta|01110\rangle + \\ & + \beta|00001\rangle + \beta|11001\rangle - \beta|10101\rangle - \beta|01101\rangle + \beta|10011\rangle - \beta|01011\rangle + \beta|00111\rangle - \beta|11111\rangle) / 4 = |\psi\rangle_{cod} \quad (A.6) \end{aligned}$$

Ao final do processo de codificação é obtido o estado $|\psi\rangle_{cod}$. Considerando um erro no

primeiro qubit do tipo $|0\rangle = a|0\rangle + b|1\rangle$, $|1\rangle = c|0\rangle + d|1\rangle$, tem-se

$$\begin{aligned} |\psi\rangle_{err} = & (\alpha(a|00000\rangle + b|10000\rangle - c|01000\rangle - d|11000\rangle + c|00100\rangle + d|10100\rangle - a|01100\rangle - b|11100\rangle + \\ & + c|00010\rangle + d|10010\rangle + a|01010\rangle + b|11010\rangle - a|00110\rangle - b|10110\rangle - c|01110\rangle - d|11110\rangle - \\ & - c|00001\rangle - d|10001\rangle + a|01001\rangle + b|11001\rangle + a|00101\rangle + b|10101\rangle - c|01101\rangle - d|11101\rangle - \\ & - a|00011\rangle - b|10011\rangle - c|01011\rangle - d|11011\rangle - c|00111\rangle - d|10111\rangle - a|01111\rangle - b|11111\rangle) + \\ & + \beta(c|00000\rangle + d|10000\rangle + a|01000\rangle + b|11000\rangle + a|00100\rangle + b|10100\rangle + c|01100\rangle + d|11100\rangle + \\ & + a|00010\rangle + b|10010\rangle - c|01010\rangle - d|11010\rangle - c|00110\rangle - d|10110\rangle + a|01110\rangle + b|11110\rangle + \\ & + a|00001\rangle + b|10001\rangle + c|01001\rangle + d|11001\rangle - c|00101\rangle - d|10101\rangle - a|01101\rangle - b|11101\rangle + \\ & + c|00011\rangle + d|10011\rangle - a|01011\rangle - b|11011\rangle + a|00111\rangle + b|10111\rangle - c|01111\rangle - d|11111\rangle) / 4 \quad (A.7) \end{aligned}$$

Considerando o estado $|\psi\rangle_{err}$ como um estado codificado que após passar por um canal sofreu um erro geral no primeiro qubit é analisada a sua evolução ao longo do circuito de decodificação que é igual ao circuito de codificação. No entanto, o estado $|\psi\rangle_{err}$ passa pelo circuito em sentido contrário (da direita para a esquerda) para ser decodificado.

$$\begin{aligned}
|\psi\rangle_{err} & \xrightarrow{10} (\alpha(a|00000\rangle + b|10000\rangle + c|01000\rangle + d|11000\rangle + c|00100\rangle + d|10100\rangle + a|01100\rangle + b|11100\rangle + \\
& + c|00010\rangle + d|10010\rangle - a|01010\rangle - b|11010\rangle - a|00110\rangle - b|10110\rangle + c|01110\rangle + d|11110\rangle - \\
& - c|00001\rangle - d|10001\rangle - a|01001\rangle - b|11001\rangle + a|00101\rangle + b|10101\rangle + c|01101\rangle + d|11101\rangle - \\
& - a|00011\rangle - b|10011\rangle + c|01011\rangle + d|11011\rangle - c|00111\rangle - d|10111\rangle + a|01111\rangle + b|11111\rangle) + \\
& + \beta(c|00000\rangle + d|10000\rangle - a|01000\rangle - b|11000\rangle + a|00100\rangle + b|10100\rangle - c|01100\rangle - d|11100\rangle + \\
& + a|00010\rangle + b|10010\rangle + c|01010\rangle + d|11010\rangle - c|00110\rangle - d|10110\rangle - a|01110\rangle - b|11110\rangle + \\
& + a|00001\rangle + b|10001\rangle - c|01001\rangle - d|11001\rangle - c|00101\rangle - d|10101\rangle + a|01101\rangle + b|11101\rangle + \\
& + c|00011\rangle + d|10011\rangle + a|01011\rangle + b|11011\rangle + a|00111\rangle + b|10111\rangle + c|01111\rangle + d|11111\rangle) / 4 \\
& \xrightarrow{9} (\alpha(a|00000\rangle + b|10000\rangle + c|11000\rangle - d|01000\rangle + c|00100\rangle + d|10100\rangle - a|11100\rangle + b|01100\rangle + \\
& + c|00010\rangle + d|10010\rangle - a|11010\rangle + b|01010\rangle - a|00110\rangle - b|10110\rangle - c|11110\rangle + d|01110\rangle - \\
& - c|00001\rangle - d|10001\rangle + a|11001\rangle - b|01001\rangle + a|00101\rangle + b|10101\rangle + c|11101\rangle - d|01101\rangle - \\
& - a|00011\rangle - b|10011\rangle - c|11011\rangle + d|01011\rangle - c|00111\rangle - d|10111\rangle + a|11111\rangle - b|01111\rangle) + \\
& + \beta(c|00000\rangle + d|10000\rangle - a|11000\rangle + b|01000\rangle + a|00100\rangle + b|10100\rangle + c|11100\rangle - d|01100\rangle + \\
& + a|00010\rangle + b|10010\rangle + c|11010\rangle - d|01010\rangle - c|00110\rangle - d|10110\rangle + a|11110\rangle - b|01110\rangle + \\
& + a|00001\rangle + b|10001\rangle + c|11001\rangle - d|01001\rangle - c|00101\rangle - d|10101\rangle + a|11101\rangle - b|01101\rangle + \\
& + c|00011\rangle + d|10011\rangle - a|11011\rangle + b|01011\rangle + a|00111\rangle + b|10111\rangle + c|11111\rangle - d|01111\rangle) / 4 = \\
& = (\alpha(a|00000\rangle - a|00011\rangle + a|00101\rangle - a|00110\rangle + a|11001\rangle - a|11010\rangle + a|11111\rangle - a|11100\rangle + \\
& + b|10000\rangle - b|10011\rangle + b|10101\rangle - b|10110\rangle + b|01100\rangle - b|01111\rangle + b|01010\rangle - b|01001\rangle + \\
& + c|11000\rangle - c|11011\rangle + c|11101\rangle - c|11110\rangle + c|00100\rangle - c|00111\rangle + c|00010\rangle - c|00001\rangle - \\
& + d|01110\rangle - d|01101\rangle + d|01011\rangle - d|01000\rangle + d|10010\rangle - d|10001\rangle + d|10100\rangle - d|10111\rangle) + \\
& + \beta(a|00111\rangle + a|00100\rangle + a|00010\rangle + a|11110\rangle + a|11101\rangle + a|00001\rangle - a|11000\rangle - a|11011\rangle + \\
& + b|01000\rangle + b|01011\rangle + b|10100\rangle + b|10010\rangle + b|10001\rangle + b|10111\rangle - b|01110\rangle - b|01101\rangle + \\
& + c|00000\rangle + c|00011\rangle + c|11001\rangle + c|11010\rangle + c|11111\rangle + c|11100\rangle - c|00101\rangle - c|00110\rangle - \\
& + d|10000\rangle + d|10011\rangle - d|01100\rangle - d|01111\rangle - d|10101\rangle - d|10110\rangle - d|01001\rangle - d|01010\rangle) / 4 \xrightarrow{8}
\end{aligned}$$

$$\begin{aligned}
& (\alpha(a|0+000\rangle - a|0+011\rangle + a|0+101\rangle - a|0+110\rangle + a|1-001\rangle - a|1-010\rangle + a|1-111\rangle - a|1-100\rangle \\
& \quad + b|1+000\rangle - b|1+011\rangle + b|1+101\rangle - b|1+110\rangle + b|0-100\rangle - b|0-111\rangle + b|0-010\rangle - b|0-001\rangle + \\
& \quad + c|1-000\rangle - c|1-011\rangle + c|1-101\rangle - c|1-110\rangle + c|0+100\rangle - c|0+111\rangle + c|0+010\rangle - c|0+001\rangle + \\
& \quad + d|0-110\rangle - d|0-101\rangle + d|0-011\rangle - d|0-000\rangle + d|1+010\rangle - d|1+001\rangle + d|1+100\rangle - d|1+111\rangle) + \\
& \quad + \beta(a|0+111\rangle + a|0+100\rangle + a|0+010\rangle + a|1-110\rangle + a|1-101\rangle + a|0+001\rangle - a|1-000\rangle - a|1-011\rangle + \\
& \quad + b|0-000\rangle + b|0-011\rangle + b|1+100\rangle + b|1+010\rangle + b|1+001\rangle + b|1+111\rangle - b|0-110\rangle - b|0-101\rangle + \\
& \quad + c|0+000\rangle + c|0+011\rangle + c|1-001\rangle + c|1-010\rangle + c|1-111\rangle + c|1-100\rangle - c|0+101\rangle - c|0+110\rangle - \\
& \quad + d|1+000\rangle + d|1+011\rangle - d|0-100\rangle - d|0-111\rangle - d|1+101\rangle - d|1+110\rangle - d|0-001\rangle - d|0-010\rangle) / 4\sqrt{2} = \\
& = (\alpha[a(|00000\rangle + |01000\rangle - |00011\rangle - |01011\rangle + |00101\rangle + |01101\rangle - |00110\rangle - |01110\rangle + \\
& \quad + |10001\rangle - |11001\rangle - |10010\rangle + |11010\rangle + |10111\rangle - |11111\rangle - |10100\rangle + |11100\rangle) + \\
& \quad + b(|10000\rangle + |11000\rangle - |10011\rangle - |11011\rangle + |10101\rangle + |11101\rangle - |10110\rangle - |11110\rangle + \\
& \quad + |00100\rangle - |01100\rangle - |00111\rangle + |01111\rangle + |00010\rangle - |01010\rangle - |00001\rangle + |01001\rangle + \\
& \quad + c(|10000\rangle - |11000\rangle - |10011\rangle + |11011\rangle + |10101\rangle - |11101\rangle - |10110\rangle + |11110\rangle + \\
& \quad + |00100\rangle + |01100\rangle - |00111\rangle - |01111\rangle + |00010\rangle + |01010\rangle - |00001\rangle - |01001\rangle + \\
& \quad + d(|00110\rangle - |01110\rangle - |00101\rangle + |01101\rangle + |00011\rangle - |01011\rangle - |00000\rangle + |01000\rangle + \\
& \quad + |10010\rangle + |11010\rangle - |10001\rangle - |11001\rangle + |10100\rangle + |11100\rangle - |10111\rangle - |11111\rangle) + \\
& \quad + \beta[a(|00111\rangle + |01111\rangle + |00100\rangle + |01100\rangle + |00010\rangle + |01010\rangle + |10110\rangle - |11110\rangle + \\
& \quad + |10101\rangle - |11101\rangle + |00001\rangle + |01001\rangle - |10000\rangle + |11000\rangle - |10011\rangle + |11011\rangle) + \\
& \quad + b(|00000\rangle - |01000\rangle + |00011\rangle - |01011\rangle + |10100\rangle + |11100\rangle + |10010\rangle + |11010\rangle + \\
& \quad + |10001\rangle + |11001\rangle + |10111\rangle + |11111\rangle - |00110\rangle + |01110\rangle - |00101\rangle + |01101\rangle) + \\
& \quad + c(|00000\rangle + |01000\rangle + |00011\rangle + |01011\rangle + |10001\rangle - |11001\rangle + |10010\rangle - |11010\rangle + \\
& \quad + |10111\rangle - |11111\rangle + |10100\rangle - |11100\rangle - |00101\rangle - |01101\rangle - |00110\rangle - |01110\rangle) + \\
& \quad + d(|10000\rangle + |11000\rangle + |10011\rangle + |11011\rangle - |00100\rangle + |01100\rangle - |00111\rangle + |01111\rangle - \\
& \quad - |10101\rangle - |11101\rangle - |10110\rangle - |11110\rangle - |00001\rangle + |01001\rangle - |00010\rangle + |01010\rangle) / 4\sqrt{2} \xrightarrow{7} \\
& (\alpha[a(|00000\rangle - |00100\rangle + |00111\rangle - |00011\rangle - |01011\rangle - |01111\rangle - |10101\rangle + |10001\rangle - \\
& \quad - |11001\rangle - |11101\rangle - |10010\rangle + |10110\rangle + |11010\rangle + |11110\rangle + |01000\rangle + |01100\rangle) + \\
& \quad + b(|10000\rangle + |10100\rangle + |11000\rangle - |11100\rangle - |10011\rangle - |10111\rangle - |11011\rangle + |11111\rangle - \\
& \quad - |00001\rangle - |00101\rangle + |01001\rangle - |01101\rangle + |00010\rangle + |00110\rangle - |01010\rangle + |01110\rangle + \\
& \quad + c(|10000\rangle + |10100\rangle - |11000\rangle + |11100\rangle - |10011\rangle - |10111\rangle + |11011\rangle - |11111\rangle - \\
& \quad - |00001\rangle - |00101\rangle - |01001\rangle + |01101\rangle + |00010\rangle + |00110\rangle + |01010\rangle - |01110\rangle + \\
& \quad + d(|10010\rangle - |10110\rangle + |11010\rangle + |11110\rangle + |10101\rangle - |10001\rangle - |11101\rangle - |11001\rangle + \\
& \quad + |00011\rangle - |00111\rangle - |01011\rangle - |01111\rangle - |00000\rangle + |00100\rangle + |01000\rangle + |01100\rangle) + \\
& \quad + \beta[a(-|10011\rangle + |10111\rangle + |11011\rangle + |11111\rangle - |10000\rangle + |10100\rangle + |11000\rangle + |11100\rangle + \\
& \quad + |00010\rangle - |00110\rangle + |01010\rangle + |01110\rangle + |00001\rangle - |00101\rangle + |01001\rangle + |01101\rangle) + \\
& \quad + b(|00000\rangle + |00100\rangle - |01000\rangle + |01100\rangle + |00011\rangle + |00111\rangle - |01011\rangle + |01111\rangle + \\
& \quad + |10010\rangle + |10110\rangle + |11010\rangle - |11110\rangle + |10001\rangle + |10101\rangle + |11001\rangle - |11101\rangle) + \\
& \quad + c(|00000\rangle + |00100\rangle + |01000\rangle - |01100\rangle + |00011\rangle + |00111\rangle + |01011\rangle - |01111\rangle + \\
& \quad + |10001\rangle + |10101\rangle - |11001\rangle + |11101\rangle + |10010\rangle + |10110\rangle - |11010\rangle + |11110\rangle) + \\
& \quad + d(|10000\rangle - |10100\rangle + |11000\rangle + |11100\rangle + |10011\rangle - |10111\rangle + |11011\rangle + |11111\rangle - \\
& \quad - |00001\rangle + |00101\rangle + |01001\rangle + |01101\rangle + |01010\rangle + |01110\rangle - |00010\rangle + |00110\rangle) / 4\sqrt{2} =
\end{aligned}$$

$$\begin{aligned}
&= (\alpha[a(|00-00\rangle - |00-11\rangle - |01+11\rangle + |10-01\rangle - |11+01\rangle - |10-10\rangle + |11+10\rangle + |01+00\rangle) + \\
&+ b(|10+00\rangle + |11-00\rangle - |10+11\rangle - |11-11\rangle - |00+01\rangle + |01-01\rangle + |00+10\rangle - |01-10\rangle) + \\
&+ c(|10+00\rangle - |11-00\rangle - |10+11\rangle + |11-11\rangle - |00+01\rangle - |01-01\rangle + |00+10\rangle + |01-10\rangle) + \\
&+ d(|10-10\rangle + |11+10\rangle - |10-01\rangle - |11+01\rangle + |00-11\rangle - |01+11\rangle - |00-00\rangle + |01+00\rangle)] + \\
&+ \beta[a(-|10-11\rangle + |11+11\rangle - |10-00\rangle + |11+00\rangle + |00-10\rangle + |01+10\rangle + |00-01\rangle + |01+01\rangle) + \\
&+ b(|00+00\rangle - |01-00\rangle + |00+11\rangle - |01-11\rangle + |10+10\rangle + |11-10\rangle + |10+01\rangle + |11-01\rangle) + \\
&+ c(|00+00\rangle + |01-00\rangle + |00+11\rangle + |01-11\rangle + |10+01\rangle - |11-01\rangle + |10+10\rangle - |11-10\rangle) + \\
&+ d(|10-00\rangle + |11+00\rangle + |10-11\rangle + |11+11\rangle - |00-01\rangle + |01+01\rangle + |01+10\rangle - |00-10\rangle)] / 4 \xrightarrow{6} \\
&(\alpha[a(|00100\rangle - |00111\rangle - |01011\rangle + |10101\rangle - |11001\rangle - |10110\rangle + |11010\rangle + |01000\rangle) + \\
&+ b(|10000\rangle + |11100\rangle - |10011\rangle - |11111\rangle - |00001\rangle + |01101\rangle + |00010\rangle - |01110\rangle) + \\
&+ c(|10000\rangle - |11100\rangle - |10011\rangle + |11111\rangle - |00001\rangle - |01101\rangle + |00010\rangle + |01110\rangle) + \\
&+ d(|10110\rangle + |11010\rangle - |10101\rangle - |11001\rangle + |00111\rangle - |01011\rangle - |00100\rangle + |01000\rangle)] + \\
&+ \beta[a(-|10111\rangle + |11011\rangle - |10100\rangle + |11000\rangle + |00110\rangle + |01010\rangle + |00101\rangle + |01001\rangle) + \\
&+ b(|00000\rangle - |01100\rangle + |00011\rangle - |01111\rangle + |10010\rangle + |11110\rangle + |10001\rangle + |11101\rangle) + \\
&+ c(|00000\rangle + |01100\rangle + |00011\rangle + |01111\rangle + |10001\rangle - |11101\rangle + |10010\rangle - |11110\rangle) + \\
&+ d(|10100\rangle + |11000\rangle + |10111\rangle + |11011\rangle - |00101\rangle + |01001\rangle + |01010\rangle - |00110\rangle)] / 4 \xrightarrow{5} \\
&(\alpha[a(|00100\rangle + |00110\rangle + |10111\rangle + |10101\rangle + |11011\rangle - |11001\rangle + |01000\rangle - |01010\rangle) + \\
&+ b(|10000\rangle + |10010\rangle + |11100\rangle - |11110\rangle - |00001\rangle - |00011\rangle + |01101\rangle - |01111\rangle) + \\
&+ c(|10000\rangle + |10010\rangle - |11100\rangle + |11110\rangle - |00001\rangle - |00011\rangle - |01101\rangle + |01111\rangle) + \\
&+ d(-|00100\rangle - |00110\rangle + |01000\rangle - |01010\rangle - |10101\rangle - |10111\rangle - |11001\rangle + |11011\rangle)] + \\
&+ \beta[a(|00101\rangle + |00111\rangle + |01001\rangle - |01011\rangle - |10100\rangle - |10110\rangle + |11000\rangle - |11010\rangle) + \\
&+ b(|00000\rangle + |00010\rangle - |01100\rangle + |01110\rangle + |10001\rangle + |10011\rangle + |11101\rangle - |11111\rangle) + \\
&+ c(|00000\rangle + |00010\rangle + |01100\rangle - |01110\rangle + |10001\rangle + |10011\rangle - |11101\rangle + |11111\rangle) + \\
&+ d(|10110\rangle + |10100\rangle + |11000\rangle - |11010\rangle - |00101\rangle - |00111\rangle + |01001\rangle - |01011\rangle)] / 4 = \\
&= (\alpha[a(|001+0\rangle + |101+1\rangle - |110-1\rangle + |010-0\rangle) + b(|100+0\rangle + |111-0\rangle - |000+1\rangle + |011-1\rangle) + \\
&+ c(|100+0\rangle - |111-0\rangle - |000+1\rangle - |011-1\rangle) + d(-|001+0\rangle + |010-0\rangle - |101+1\rangle - |110-1\rangle) + \\
&+ \beta[a(|001+1\rangle + |010-1\rangle - |101+0\rangle + |110-0\rangle) + b(|000+0\rangle - |011-0\rangle + |100+1\rangle + |111-1\rangle) + \\
&+ c(|000+0\rangle + |011-0\rangle + |100+1\rangle - |111-1\rangle) + d(|101+0\rangle + |110-0\rangle - |001+1\rangle + |010-1\rangle)] / 2\sqrt{2} \xrightarrow{4} \\
&(\alpha[a(|00100\rangle - |10101\rangle + |11011\rangle + |01010\rangle) + b(|10000\rangle + |11110\rangle + |00001\rangle - |01111\rangle) + \\
&+ c(|10000\rangle - |11110\rangle + |00001\rangle + |01111\rangle) + d(-|00100\rangle + |01010\rangle + |10101\rangle + |11011\rangle)] + \\
&+ \beta[a(-|00101\rangle - |01011\rangle - |10100\rangle + |11010\rangle) + b(|00000\rangle - |01110\rangle - |10001\rangle - |11111\rangle) + \\
&+ c(|00000\rangle + |01110\rangle - |10001\rangle + |11111\rangle) + d(|10100\rangle + |11010\rangle + |00101\rangle - |01011\rangle)] / 2\sqrt{2} \xrightarrow{3} \\
&(\alpha[a(|00100\rangle + |00101\rangle + |01010\rangle - |01011\rangle) + b(|10000\rangle + |10001\rangle + |11110\rangle - |11111\rangle) + \\
&+ c(|10000\rangle + |10001\rangle - |11110\rangle + |11111\rangle) + d(-|00100\rangle - |00101\rangle + |01010\rangle - |01011\rangle)] + \\
&+ \beta[a(-|10100\rangle - |10101\rangle + |11010\rangle - |11011\rangle) + b(|00000\rangle + |00001\rangle - |01110\rangle + |01111\rangle) + \\
&+ c(|00000\rangle + |00001\rangle + |01110\rangle - |01111\rangle) + d(|10100\rangle + |10101\rangle + |11010\rangle - |11011\rangle)] / 2\sqrt{2} =
\end{aligned}$$

$$\begin{aligned}
& (\alpha[a(|0010\rangle + |0101\rangle) + b(|1000\rangle + |1111\rangle) + c(|1000\rangle - |1111\rangle) + d(-|0010\rangle + |0101\rangle)] + \\
& + \beta[a(-|1010\rangle + |1101\rangle) + b(|0000\rangle - |0111\rangle) + c(|0000\rangle + |0111\rangle) + d(|1010\rangle + |1101\rangle)] / 2 = \xrightarrow{2} \\
& (\alpha[a(|0010\rangle + |0101\rangle) + b(|1000\rangle + |1111\rangle) + c(|1000\rangle - |1111\rangle) + d(-|0010\rangle + |0101\rangle)] + \\
& + \beta[a(-|1010\rangle + |1101\rangle) + b(|0000\rangle - |0111\rangle) + c(|0000\rangle + |0111\rangle) + d(|1010\rangle + |1101\rangle)] / 2 \xrightarrow{1} \\
& (\alpha[a(|0010\rangle + |0101\rangle) + b(|1000\rangle + |1111\rangle) + c(|1000\rangle - |1111\rangle) + d(-|0010\rangle + |0101\rangle)] + \\
& + \beta[a(-|1010\rangle + |1101\rangle) + b(|0000\rangle - |0111\rangle) + c(|0000\rangle + |0111\rangle) + d(|1010\rangle + |1101\rangle)] / 2 = \\
& = (a(\alpha|0\rangle - \beta|1\rangle)|0100\rangle + a(\alpha|0\rangle + \beta|1\rangle)|1011\rangle + b(\alpha|1\rangle + \beta|0\rangle)|0000\rangle + b(\alpha|1\rangle - \beta|0\rangle)|1111\rangle + \\
& c(\alpha|1\rangle + \beta|0\rangle)|0000\rangle + c(-\alpha|1\rangle + \beta|0\rangle)|1111\rangle + d(-\alpha|0\rangle + \beta|1\rangle)|0100\rangle + d(\alpha|0\rangle + \beta|1\rangle)|1011\rangle) / 2 = \\
& = \frac{a+d}{2}(\alpha|0\rangle + \beta|1\rangle)|1011\rangle + \frac{a-d}{2}(\alpha|0\rangle - \beta|1\rangle)|0100\rangle + \\
& + \frac{b+c}{2}(\alpha|1\rangle + \beta|0\rangle)|0000\rangle + \frac{b-c}{2}(\alpha|1\rangle - \beta|0\rangle)|1111\rangle
\end{aligned} \tag{A.8}$$

Foi mostrado que qualquer erro sobre o primeiro qubit pode ser corrigido. Com base no resultado da medição dos quatro últimos qubits é possível determinar a operação (I , X , Z , XZ) necessária para recuperar o qubit transmitido. O código pode corrigir qualquer erro em 1 qubit.

Anexo 1

Artigo Científico - I

Artigo publicado na revista científica arbitrada Physics Letters A.

D. B. de Brito, R. V. Ramos, “Passive quantum error correction with linear optics”,
Phys. Lett. A, vol. 352, No. 3, 206-209, 2006.

Passive quantum error correction with linear optics

Daniel Barbosa de Brito and *Rubens Viana Ramos

Department of Teleinformatic Engineering, Federal University of Ceara, Campus do Pici, 710, C.P. 6007, 60455-760, Fortaleza-Ceará, Brasil

Abstract

Recently it was proposed by Kalamidas in [D. Kalamidas, Phys. Lett. A 343 (2005) 331-335] an optical set-up able to correct single qubit errors using Pockels cells. In this work, we present a different set-up able to realize error correction passively, in the sense that none external action is needed.

PACS: 03.67.Dd

Keywords: Quantum communication, quantum error correction, linear optics,

Quantum communication and computation have attracted much attention due to its potentialities without counter-part in the classical systems. Quantum key distribution [1] and quantum teleportation [2] are the most famous examples. However, as happen in any classical communication or computation system, the presence of noise degrades the performance of quantum circuits and protocols. Hence, in order to have quantum communication systems and quantum computers working properly one must take care of quantum noise. Usually, in order to realize quantum error correction, quantum codes are employed. Basically, redundancy is introduced entangling the qubit-signal with ancillas before send them through the channel. At channel output, the measurements of the ancillas will give us an idea of what happened with the qubit-signal [3]. In order to correct the error, according to the results of the ancillas measurement, a unitary evolution is chosen and applied in the qubit-signal. This scheme is shown in Fig. 1.

*Corresponding author

E-mail addresses: danielbb@deti.ufc.br, rubens@deti.ufc.br

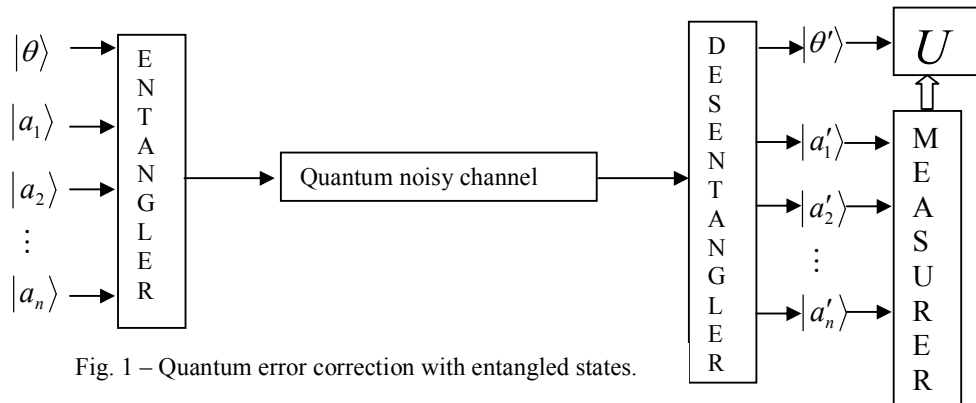


Fig. 1 – Quantum error correction with entangled states.

In Fig. 1 $|\theta\rangle$ is the qubit-signal, $|a_i\rangle$ ($i=1,2,\dots,n$) are the ancillas, entangler and desentangler are, respectively, the coder and decoder. The number of errors that can be corrected and the kind of errors depends on the number of ancillas and the kind of code used [3]. The Shor's code, for example, can correct any kind of error in a single qubit using eight ancillas [4]. The lowest order block code able to correct any single-qubit error uses four ancillas. From a practical point of view, with present technology it is quite hard to implement such error correction protocols. Therefore, simple and feasible error correction schemes are much desired. In this direction, Kalamidas [5] proposed an optical set-up able to correct an arbitrary single qubit error without using entangled states. The set-up proposed can be seen in Fig. 2 and it works as follows:

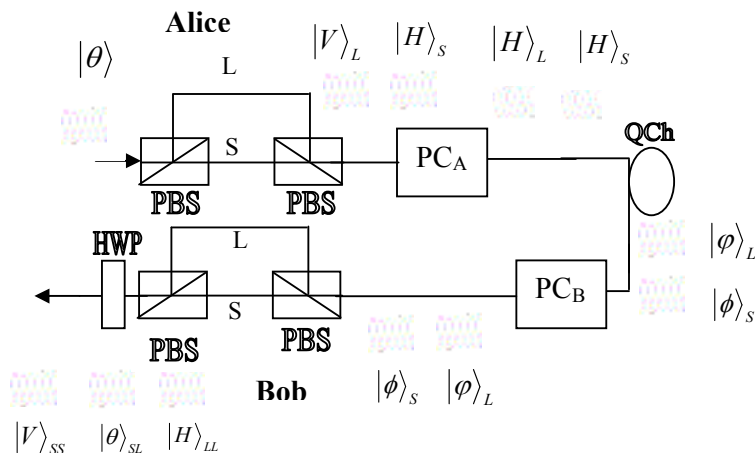


Fig. 2 – Optical set-up for arbitrary single qubit error correction. PBS: polarization beam splitter. PC: Pockles Cell. HWP: Half wave plate.

Initially, the single-photon pulse in the polarization state $|\theta\rangle = \alpha|H\rangle + \beta|V\rangle$ is transformed in a time-bin qubit [1] by two polarization beam splitters (PBS) in a unbalanced interferometer, resulting in the quantum state $\alpha|H\rangle_S + \beta|V\rangle_L$, meaning the horizontal component took the short path while the vertical component took the long path. After, Alice's Pockels cells (PC_A) acts in order to give a rotation of $\pi/2$ only in the second part of the time-bin qubit, resulting in the state $\alpha|H\rangle_S + \beta|H\rangle_L$. This state is launched in the quantum channel, an optical fiber. Since the time separation between the components of the time-bin qubit is taken to be much lesser than the time of fluctuation of the channels parameters (fluctuation in the fiber birefringence) both components, S and L, will see the same stationary quantum channel represented by the unitary evolution U . A general unitary transformation will act in the horizontal polarization state like $|H\rangle \rightarrow \cos(\varphi)e^{i\lambda}|H\rangle_k + \sin(\varphi)e^{i\xi}|V\rangle_k$, $k=S,L$. Hence, the quantum state leaving the quantum channel and arriving at Bob's place is:

$$|\psi\rangle = \alpha[\cos(\varphi)e^{i\lambda}|H\rangle_S + \sin(\varphi)e^{i\xi}|V\rangle_S] + \beta[\cos(\varphi)e^{i\lambda}|H\rangle_L + \sin(\varphi)e^{i\xi}|V\rangle_L] \quad (1)$$

Bob, by his turn, turns on his Pockels cell (PC_B) in order to give a rotation of $\pi/2$ only in the first part of the time-bin qubit resulting in the state:

$$\alpha[\cos(\varphi)e^{i\lambda}|V\rangle_S + \sin(\varphi)e^{i\xi}|H\rangle_S] + \beta[\cos(\varphi)e^{i\lambda}|H\rangle_L + \sin(\varphi)e^{i\xi}|V\rangle_L] \quad (2)$$

The state of (2) will enter in a two PBS set-up equal to the one used by Alice in the first step of the error correction. Once more, the horizontal polarization will take the short path while the vertical polarization will take the long path. The resulting state is:

$$\alpha[\cos(\varphi)e^{i\lambda}|V\rangle_{SL} + \sin(\varphi)e^{i\xi}|H\rangle_{SS}] + \beta[\cos(\varphi)e^{i\lambda}|H\rangle_{LS} + \sin(\varphi)e^{i\xi}|V\rangle_{LL}] = \cos(\varphi)e^{i\lambda}(\alpha|V\rangle_{SL} + \beta|H\rangle_{LS}) + \sin(\varphi)e^{i\xi}(\alpha|H\rangle_{SS} + \beta|V\rangle_{LL}) \quad (3)$$

At last, after the half-wave plate (HWP) the state is:

$$\cos(\varphi)e^{i\lambda}(\alpha|H\rangle_{SL} + \beta|V\rangle_{LS}) + \sin(\varphi)e^{i\xi}(\alpha|V\rangle_{SS} + \beta|H\rangle_{LL}) \quad (4)$$

Hence, there will be three possible time slots where the signal can be found, SS, SL (or LS) and LL. If the signal is found in time slot SS or LL one will be sure that an error occurred, otherwise, if the signal is found in the time slot SL it represents the correct qubit. This last case happens with probability $\cos^2(\varphi)$. Now, let us consider what happens when two-mode bright coherent states are used instead of single-photon pulses. This is important because some quantum communication schemes using polarization of mesoscopic coherent states have been proposed [6-8]. The initial state is $|\alpha, \beta\rangle$, where the first position represents the horizontal component while the second position represents the vertical component. The state leaving Alice (after PC_A) is $|\alpha, 0\rangle_S \otimes |\beta, 0\rangle_L$. At quantum channel output the state is $|\alpha \cos(\varphi)e^{i\lambda}, \alpha \sin(\varphi)e^{i\xi}\rangle_S \otimes |\beta \cos(\varphi)e^{i\lambda}, \beta \sin(\varphi)e^{i\xi}\rangle_L$. After Bob's Pockels cell the state is $|\alpha \sin(\varphi)e^{i\xi}, \alpha \cos(\varphi)e^{i\lambda}\rangle_S \otimes |\beta \cos(\varphi)e^{i\lambda}, \beta \sin(\varphi)e^{i\xi}\rangle_L$. Finally, before the half-wave plate, the three pulses are $|\alpha \sin(\varphi)e^{i\xi}, 0\rangle_{SS} \otimes |\alpha \cos(\varphi)e^{i\lambda}, \beta \cos(\varphi)e^{i\lambda}\rangle_{SL} \otimes |\beta \sin(\varphi)e^{i\xi}\rangle_{LL}$. Hence, the second pulse has already the correct polarization information and the half-wave plate must not be used anymore. The useful pulse power will be $\cos^2(\varphi)$ times the incident pulse power (if losses are not considered). As expected, the single qubit error-correction optical set-up proposed by Kalamidas works also for coherent states. However, the synchronization of the Pockels cells makes it a little bit hard to implement. A passive, in the sense that

none external action is needed, error correction set-up for coherent states, using the same idea proposed by Kalamidas, can be implemented as shown in Fig. 3.

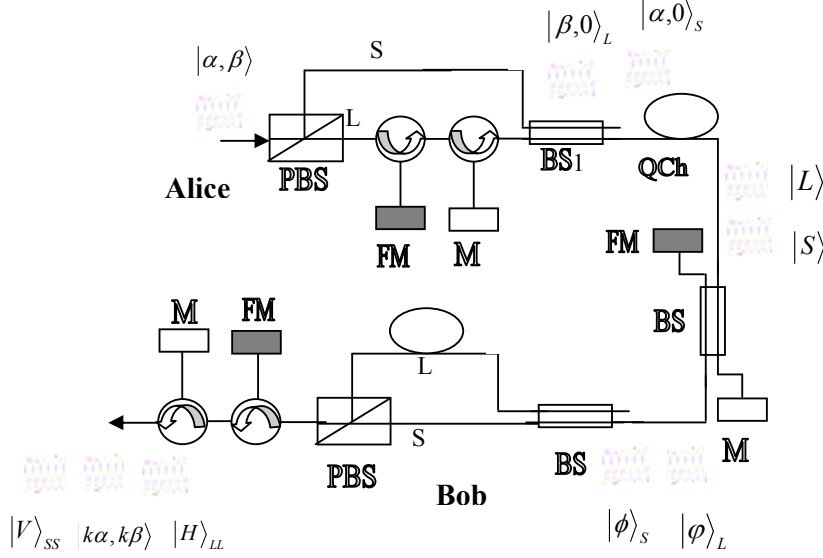


Fig. 3 – A passive error correction set-up for coherent states based quantum communication systems.

In Fig. 3, BS_1 is a beam splitter having transmittance $T=1/\sqrt{5}$ and reflectance $R=2/\sqrt{5}$, while the two other BS's are balanced. FM is a Faraday mirror and M is a common mirror. The set-up works as follow: The components of the initial state are separated by the first PBS. The horizontal component takes the short path while the vertical component takes the long path, passing trough two circulators, a Faraday mirror and a common mirror. Its evolution is $|0, \beta\rangle \xrightarrow{FM} |\beta^*, 0\rangle \xrightarrow{M} |\beta, 0\rangle$. Both pulses are now launched in the quantum channel, separated by a time interval short enough in order to make the channel the same for both of them. The state at the channel input is $|i2\alpha/\sqrt{5}, 0\rangle_S \otimes |\beta/\sqrt{5}, 0\rangle_L$. As before, after channel propagation the state is:

$$|S\rangle \otimes |L\rangle \quad (5)$$

$$|S\rangle = |i2\alpha \cos(\varphi)e^{i\lambda}/\sqrt{5}, i2\alpha \sin(\varphi)e^{i\xi}/\sqrt{5}\rangle_S \quad (6)$$

$$|L\rangle = |\beta \cos(\varphi)e^{i\lambda}/\sqrt{5}, \beta \sin(\varphi)e^{i\xi}/\sqrt{5}\rangle_L \quad (7)$$

where once more φ , λ , and ξ are the parameters of a general 2x2 unitary transformation. When the S pulse arrives at the receiver, half of it is reflected toward the interferometer composed by the third BS, a fiber delay and the second PBS. This first pulse is not considered. The other half goes to mirror M, half of this one goes to Faraday mirror FM and, at last, half of this one is sent toward the interferometer. This pulse is the first important one and its state is:

$$\left| \alpha \sin(\varphi) e^{i\xi} / \sqrt{10}, -\alpha \cos(\varphi) e^{i\lambda} / \sqrt{10} \right\rangle_S \quad (8)$$

When the L pulse arrives at the second BS, half of it is reflected toward the interferometer. This is the second important pulse and its state is:

$$\left| i\beta \cos(\varphi) e^{i\lambda} / \sqrt{10}, i\beta \sin(\varphi) e^{i\xi} / \sqrt{10} \right\rangle_L \quad (9)$$

The other pulses resulting from several reflections in the cavity composed by BS, M and FM are not considered, hence, Bob has to pay attention at the time of detections. The length of long arm in Alice is a little bit larger than twice the distance between M and FM. This mean the cavity must be very short and the pulses very narrow. Now, the new distance between both important pulses going to the Bob's interferometer is equal to the delay in the long arm of the same. Therefore, once more there are three pulses at the second PBS output:

$$\left| \frac{\alpha \sin(\varphi) e^{i\xi}}{2\sqrt{5}}, 0 \right\rangle_{SS} \otimes \left| \frac{i\beta \cos(\varphi) e^{i\lambda}}{2\sqrt{5}}, \frac{-i\alpha \cos(\varphi) e^{i\lambda}}{2\sqrt{5}} \right\rangle_{SL} \otimes \left| 0, \frac{-\beta \sin(\varphi) e^{i\xi}}{2\sqrt{5}} \right\rangle_{LL} \quad (10)$$

After the last Faraday mirror and common mirror, the middle pulse is in the state:

$$\left| \frac{-i \cos(\varphi) e^{i\lambda}}{2\sqrt{5}} \alpha, \frac{-i \cos(\varphi) e^{i\lambda}}{2\sqrt{5}} \beta \right\rangle_{SL} \quad (11)$$

As can be seen, the second pulse (*SL*) has the correct polarization. As stated before, the advantage of this scheme is its passive operation; on the other hand, its disadvantage is the loss of energy in not useful pulses. For a lossless channel, the power of the useful pulses is $\cos^2(\varphi)/20$ of the input pulse power at Alice's place. Due to this loss, the set-up proposed in this work would have a low performance if it would be employed in a single-photon quantum communication system. On the other hand, it can be used in quantum communication systems employing bright coherent states as that proposed in references [6-8].

Now it is worthy to clarify exactly what kind of errors can be corrected. Any error (polarization change) that can be modeled by the sequence compensator-rotator-compensator can be corrected. For this, as explained before, the time of change of the fiber parameters must be larger than time separation between S and L pulses. Hence, fast polarization fluctuation will not be corrected. Another critical point in Kalamidas scheme is that both interferometers PBS-fiber-PBS in Alice and Bob must be equal. Since Alice and Bob are supposed to be separated, the match of fibers length in Alice and Bob is not so easy due to environmental fluctuation. On the other hand, for the scheme proposed in this work, Alice's set-up is already different of Bob's set-up, hence, that mismatch is not a problem. A third important question is the polarization mode dispersion, PMD. Usually PMD is considered a problem in very fast (transmission rates larger than 10 Gbs) and long haul optical communication systems. If the fiber is long

enough, the PMD can split the input pulse in two pulses and this is not a unitary evolution anymore and, hence, the proposed error correction scheme will not be useful. Therefore, the proposed system is adequate for optical quantum communication system in which PMD is not a severe problem. At last, it is important to stress that only errors (polarization change) due to channel propagation can be corrected. Errors owing to, for example, non-ideal detectors and modulators are not corrected by the system proposed. Other errors caused by fiber propagation like depolarization and polarization dependent loss are not corrected because are owing to non-unitary evolution.

In summary, we began explaining the single-photon error correction set-up using linear optics proposed by Kalamidas [5]. Following, it was analyzed its functioning when coherent were used instead of single-photon pulses. In this case, the half wave plate is not necessary. After that, we proposed a passive error correction set-up using Faraday mirrors and common mirrors. The set-up proposed has the advantage of needing no control and, hence, it has an easy implementation, while Kalamidas' set-up requires a good synchronization of two Pockels cells. The disadvantage of the set-up proposed is the loss of power in not useful pulses generated at the beam splitters.

Acknowledgements

This work was supported by the Brazilian agency CNPq.

References

- [1] N. Gisin, G. Ribordy, W. Tittel, H. Zbinden, *Rev. Mod. Phys.* 74 (2002) 145.
- [2] C. H. Bennet, *Phys. Scrip.* T76 (1998) 210.
- [3] M. A. Nielsen, I. L. Chuang, *Quantum computation and Quantum Information*, Cambridge Univ. Press, Cambridge, England, 2000.

[4]P.W. Schor, Phys. Rev. A 52 (1995) R2493.

[5]D. Kalamidas, Phys. Lett. A 343 (2005) 331.

[6]H. Yuen, quant-ph/0311061.

[7]G. Barbosa, E. Corndorf, P. Kumar, H. Yuen, Phys. Rev. Lett. 90 (2003) 227901.

[8]E. Corndorf, G. Barbosa, C. Liang, H. Yuen, P. Kumar, Opt. Lett. 28 (2003) 2040.

Anexo 2

Artigo Científico - II

Artigo submetido para a revista científica arbitrada Journal of Modern Optics.

Optical setups for probabilistic bipartite and tripartite entanglement generation and quantum teleportation in optical networks

Daniel Barbosa de Brito, João Batista Rosa Silva and Rubens Viana Ramos

Department of Teleinformatic Engineering, Federal University of Ceará, 60455-760, C.P. 6007,

Fortaleza-Ce, Brazil

Abstract

In this work we present optical setups for polarization encoded qubit, based only on common optical devices, which implement probabilistic bipartite and tripartite entanglement generation, as well probabilistic quantum teleportation. The setups can be implemented with current technology and they permit the realization of several quantum communication protocols.

1. Introduction

The efficient experimental implementation of some quantum communication protocols requires a non-linear operation as, for example, in the realization of the quantum teleportation protocol. In this case, a Bell measurement, that needs a CNOT operation, is required. However, since nowadays large non-linearities, mainly based in Kerr effect, in optical materials are not yet easily available, it is highly desirable to

construct quantum optical devices and quantum communication systems using only linear devices. This can be achieved if one pays the price of a probabilistic behavior [1-3]. Thus, sometimes the quantum gate/protocol works and sometimes it fails, however, it is possible to know when a fail occurred. An example of such probabilistic quantum gates are the CNOT gates proposed in [1,3-5]. In particular, the solution presented in [4,5] can be shortly described as follows. The setup proposed in those references is shown in Fig. 1.

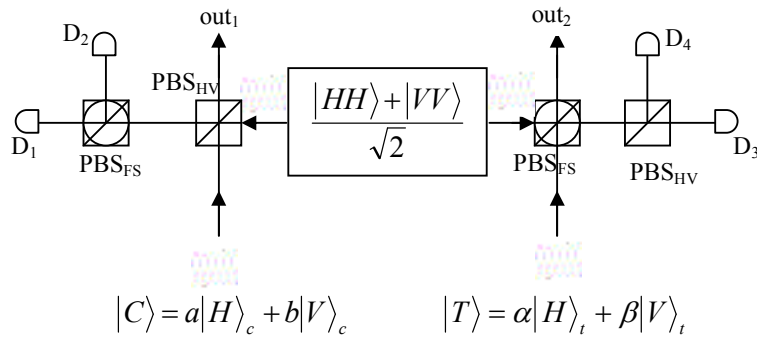


Figure 1. Probabilistic CNOT gate implemented with two-photon entangled state. PBS: polarization beam splitters. PBS_{HV}: PBS in horizontal-vertical basis. PBS_{FS}: PBS in diagonal basis ($\pi/4$, $3\pi/4$). D₁₋₄ are single-photon detectors.

In Fig. 1, D₁-D₄ are single-photon detectors, PBS_{HV} is a PBS (polarization beam splitter) in the rectangular basis $\{|H\rangle, |V\rangle\}$ while PBS_{FS} is a PBS in the diagonal basis $\{|F\rangle = [|H\rangle + |V\rangle] / 2^{1/2}, |S\rangle = [|H\rangle - |V\rangle] / 2^{1/2}\}$. The optical setup shown in Fig. 1 succeeds in implementing the CNOT gate only when a single-photon is detected in D₁ or D₂ and another single-photon is detected in D₃ or D₄. The output state of the setup in Fig. 1 is:

$$|\Psi_f\rangle = \frac{1}{4} [|F,H\rangle|\psi_1\rangle + |S,H\rangle|\psi_2\rangle + |F,V\rangle|\psi_3\rangle + |S,V\rangle|\psi_4\rangle] + \frac{\sqrt{3}}{2} |\Psi_u\rangle \quad (1)$$

$$|\psi_1\rangle = [a\alpha |HH\rangle_{ct} + a\beta |HV\rangle_{ct} + b\alpha |VV\rangle_{ct} + b\beta |VH\rangle_{ct}] \quad (2)$$

$$|\psi_2\rangle = [-a\alpha |HH\rangle_{ct} - a\beta |HV\rangle_{ct} + b\alpha |VV\rangle_{ct} + b\beta |VH\rangle_{ct}] = [(XZX) \otimes I] |\psi_1\rangle \quad (3)$$

$$|\psi_3\rangle = [a\alpha |HV\rangle_{ct} + a\beta |HH\rangle_{ct} + b\alpha |VH\rangle_{ct} + b\beta |VV\rangle_{ct}] = [I \otimes X] |\psi_1\rangle \quad (4)$$

$$|\psi_4\rangle = [-a\alpha |HV\rangle_{ct} - a\beta |HH\rangle_{ct} + b\alpha |VH\rangle_{ct} + b\beta |VV\rangle_{ct}] = [(XZX) \otimes I] [I \otimes X] |\psi_1\rangle \quad (5)$$

In (1) $|\Psi_u\rangle$ is the useless part that contains the situations where none or two photons were detected in D_{1-2} and/or D_{3-4} . Further, $|F,H(V)\rangle$ means a single-photon going to D_1 and another single-photon going to D_3 (D_4), while $|S,H(V)\rangle$ means a single-photon going to D_2 and another single-photon going to D_3 (D_4). Observing (1) and (2) one sees that the success probability of the CNOT operation is $1/16$. However, if one uses single-qubit operations to correct the output state according to where the detections were obtained (detections in D_2 and $D_3 \rightarrow XZX$ in the control qubit, detections in D_1 and $D_4 \rightarrow X$ in the target qubit and detections in D_2 and $D_4 \rightarrow XZX$ in the control qubit and X in the target qubit) the probability of success goes to $1/4$.

A crucial component in the CNOT implementation of Fig. 1 is the entangled pair of photons. Hence, in order to realize the CNOT one must firstly be able to produce the entangled state $(|HH\rangle + |VV\rangle)/2^{1/2}$. Such entangled state has been produced by using parametric down conversion [6-10] and non-linear optical crystal inside waveguides [11-14]. In both cases, a non-linear process is used. Once the entangled state has been created it can also be used for the realization of several quantum communication protocols as teleportation, quantum key distribution and quantum games [15-17].

In this direction, we present in this work, for polarization encoded qubit, optical setups for bipartite and tripartite entanglement generation in optical networks as

well an optical setup for probabilistic quantum teleportation using the entangled states probabilistically produced. All proposed setups employ only linear optical devices that are easily found, making their implementation quite simple. This work is outlined as follows: in Section 2 an optical setup for probabilistic quantum teleportation of polarization encoded qubit is presented; in Section 3 the optical setup for probabilistic bipartite Bell state generation in an optical network is shown and used together with setup given in Section 2; in Section 4, the optical setup for probabilistic tripartite Bell state generation in an optical network is presented and used together with the setup given in Section 2; at last, the conclusions are presented in Section 5.

2. Optical setup for probabilistic quantum teleportation

A probabilistic teleportation can be implemented using the setup shown in Fig. 2.

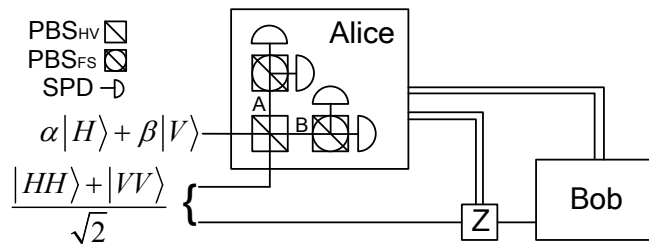


Figure 2. Optical setup for probabilistic teleportation of polarization encoded qubit.

As can be seen, the setup in Fig. 2 reminds half of the setup shown in Fig. 1. However, in the former the control qubit is also measured in the diagonal basis in Alice's place. The double lines mean classical communication. The quantum state evolution in the setup of Fig. 2 is as follow:

$$|\psi\rangle_{in} = \alpha|H\rangle + \beta|V\rangle \left(\frac{|HH\rangle + |VV\rangle}{\sqrt{2}} \right) = \frac{\alpha|HHH\rangle + \alpha|HVV\rangle + \beta|VHH\rangle + \beta|VVV\rangle}{\sqrt{2}} \quad (6)$$

$$|\psi\rangle_{PBS_{HV}} = \frac{\alpha|HHH\rangle + \beta|VVV\rangle}{\sqrt{2}} + \frac{\alpha|HV,0,V\rangle + \beta|0,VH,H\rangle}{\sqrt{2}} = \frac{1}{\sqrt{2}} [\alpha|HHH\rangle + \beta|VVV\rangle] + \frac{1}{\sqrt{2}} |\Omega\rangle \quad (7)$$

$$|\psi\rangle_{PBS_{FS}} = \frac{\alpha(|F\rangle + |S\rangle)(|F\rangle + |S\rangle)|H\rangle + \beta(|F\rangle - |S\rangle)(|F\rangle - |S\rangle)|V\rangle}{2\sqrt{2}} + \frac{1}{\sqrt{2}} |\Omega\rangle =$$

$$\frac{1}{\sqrt{2}} \frac{|FF\rangle(\alpha|H\rangle + \beta|V\rangle) + |SS\rangle(\alpha|H\rangle + \beta|V\rangle) + |FS\rangle(\alpha|H\rangle - \beta|V\rangle) + |SF\rangle(\alpha|H\rangle - \beta|V\rangle)}{2} + \frac{1}{\sqrt{2}} |\Omega\rangle \quad (8)$$

Hence, as can be seen in (8), Alice has to send two classical bits to Bob, the first one informing if the teleportation succeeded, what happens with probability 50%, and the second informing if Bob has or has not to apply a phase shift in his photon.

3. Probabilistic bipartite Bell state generation for polarization encoded qubit in an optical network

A probabilistic Bell state generator for polarization encoded qubit can be produced using only a polarizing beam splitter, PBS_{HV} . A maximally entangled pair of photons is probabilistically (50%) produced if the state $[(|H\rangle + |V\rangle)/2^{1/2}] \otimes [(|H\rangle + |V\rangle)/2^{1/2}]$ is placed at the PBS_{HV} inputs. In this case, the total output state is $[(|HH\rangle + |VV\rangle)/2^{1/2}]/2^{1/2} + [(|0,HV\rangle + |HV,0\rangle)/2^{1/2}]/2^{1/2}$. The PBS can be located in Alice, for example. Then, she keeps one photon to her and sends the other to Bob through an optical channel. Another possible way to produce probabilistically an entangled state is as shown in Fig. 3.

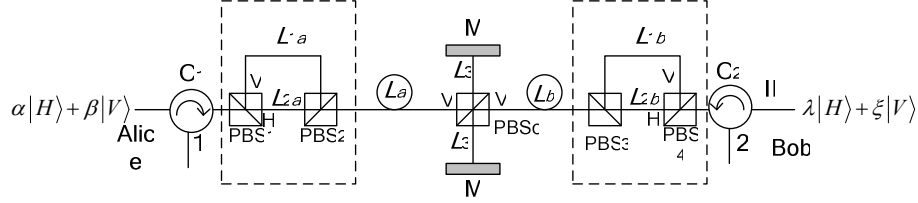


Figure 3. Optical setup for probabilistic bipartite Bell state generation and distribution.

In Fig. 3, C_1 and C_2 are optical circulators, M are common mirrors and $L_a, L_b, L_{1a,b}, L_{2a,b}$ and L_3 are fiber lengths. The $PBS_{1(2,3,4)}$ transmits the horizontal component while PBS_C transmits the vertical component. After some trivial calculations, one easily finds the output state

$$|\Psi\rangle_{12} = \alpha\lambda|HH\rangle + \beta\xi|VV\rangle + \alpha\xi|HV,0\rangle + \beta\lambda|0,HV\rangle \quad (9)$$

for the input state $[\alpha|H\rangle + \beta|V\rangle] \otimes [\lambda|H\rangle + \xi|V\rangle]$. If $\alpha = \beta = \lambda = \xi = 2^{-1/2}$, then the output state is $[(|HH\rangle + |VV\rangle)/2^{1/2}]/2^{1/2} + [(|0,HV\rangle + |HV,0\rangle)/2^{1/2}]/2^{1/2}$. Thus, once more the Bell state is produced with probability equal to 50%. However, the optical setup of Fig. 3 not only generates but it also distributes the entangled pair of photons. One can imagine Alice placed in one side and Bob at the other. Each one of them sends one photon and, if the entanglement generation succeeds, each one receives one photon, being the pair entangled. At this moment a question arises: why should someone to use the setup shown in Fig. 3 if the entangled state can be generated using only a PBS in Alice, for example? The answer is the reason for which the produced entangled state will be used. If the entangled state will be used in a quantum game or in the realization of classical games using quantum states, for example, depending on the game, each player can try to control the produced entangled state in order to obtain a larger chance to win the game.

In this case, the entanglement generation must be distributed and, in the state (9), the player Alice would control the parameter α while the player Bob would control the parameter λ . Since Alice and Bob have different distances from the central PBS, $L_a \neq L_b$, the unbalanced polarization interferometers (structures inside the dashed boxes in Fig. 3) allow Alice and Bob to control the total length propagated by the horizontal and vertical components such that, if both photons entered in the setup at the same time, they will also emerge from the setup at the same time. For this, Alice and Bob set their parameters such that

$$2L_{2a} - (L_{1b} + L_{1a}) = L_b - L_a - 2L_3 \quad (10)$$

$$2L_{2b} - (L_{1b} + L_{1a}) = L_a - L_b - 2L_3 \quad (11)$$

Now, one can put the setups shown in Figs. 2 and 3 together to obtain a complete optical setup for probabilistic quantum teleportation using only linear optical devices, as shown in Fig. 4.

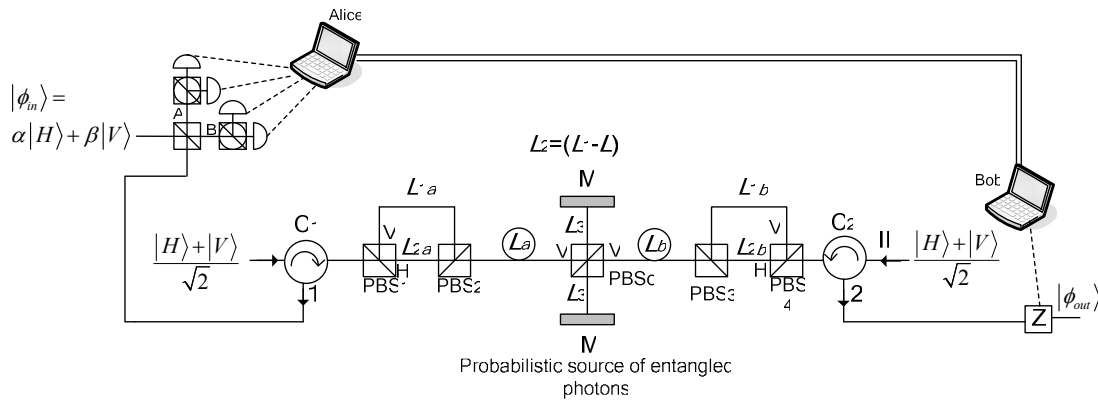


Figure 4. Complete optical setup for probabilistic teleportation.

As can be seen in Fig. 4, differently from most teleportation setups described in the literature, the proposed setup does not use parametric down conversion. The efficient

coupling of the entangled photons, produced by parametric down conversion, in single-mode optical fibers is a little bit hard procedure [18,19]. This problem does not exist in the setup in Fig. 4. On the other hand, the rate of entangled photons produced by the setup in Fig. 4 depends on the losses in the setup and, hence, it depends on the distance between Alice and Bob. Considering ideal detectors and lossless devices the optical setup in Fig. 4 succeeds with probability equal to 25%.

4. Probabilistic tripartite Bell state generation for polarization encoded qubit in an optical network

A generalization of the optical setup in Fig. 3 for three parts is shown in Fig. 5.

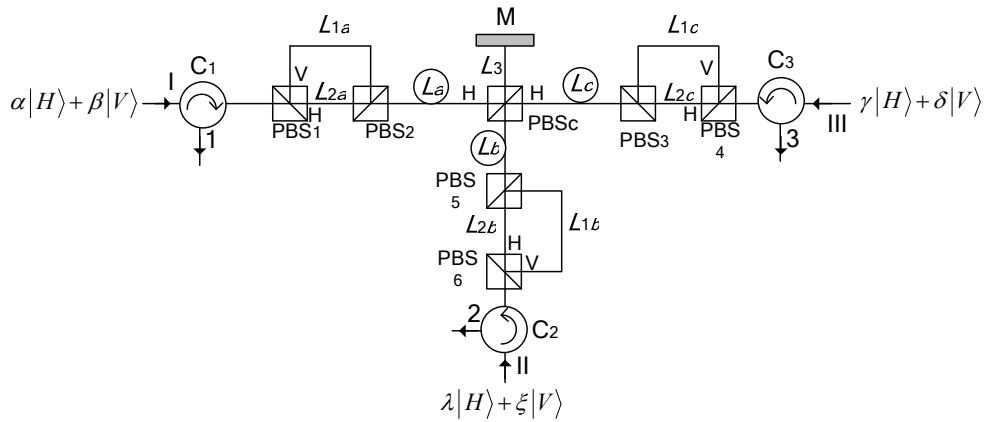


Figure 5. Optical setup for probabilistic tripartite Bell state generation and distribution.

In Fig. 5 all PBS's transmits the horizontal component component. The optical setup in Fig. 5 realizes the following transformation

$$(\alpha|H\rangle + \beta|V\rangle)_I \otimes (\lambda|H\rangle + \xi|V\rangle)_{II} \otimes (\gamma|H\rangle + \delta|V\rangle)_{III} \rightarrow \alpha\lambda\gamma|HHH\rangle + \beta\xi\delta|VVV\rangle + |\Omega\rangle \quad (12)$$

where, for simplification, hereafter the state $|\Omega\rangle$ represents the superposition of the quantum states having zero photon in one of the individual outputs. If the each input qubit is an equally weighted superposition of horizontal and vertical polarizations, then the total output state is

$$\frac{1}{2} \frac{(|HHH\rangle + |VVV\rangle)}{\sqrt{2}} + \frac{\sqrt{3}}{2} |\Omega\rangle \quad (13)$$

and, hence, the setup in Fig. 4 produces a maximally entangled tripartite (of qubits) GHZ state with probability 0.25, if losses are not considered. In order to have all polarization components emerging from the setup at the same time, the following conditions must be satisfied

$$L_{2a} - 2L_{2b} + L_{2c} = 2L_b - L_a - L_c + 2L_3 \quad (14)$$

$$L_{1a} + L_{1b} - 2L_{1c} = 2L_c - L_a - L_b + 2L_3 \quad (15)$$

Two teleportation schemes using the setups in Figs. 2 and 5 together are possible. The first one is shown in Fig. 6.

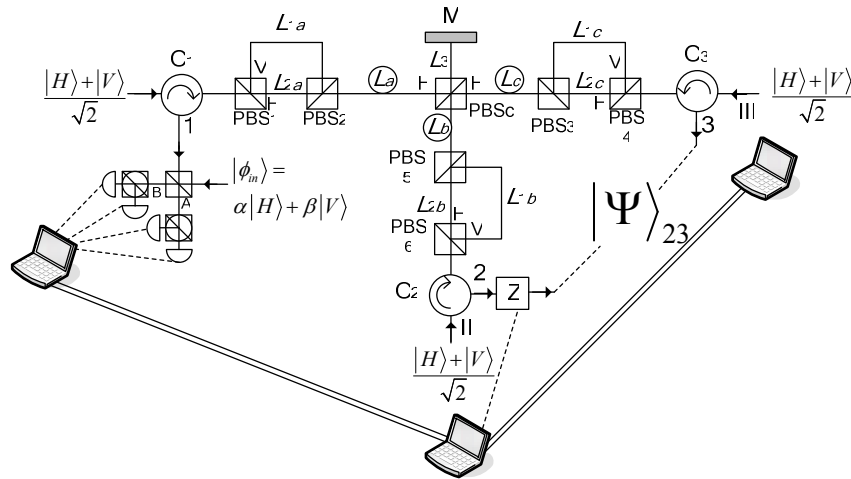


Figure 6. Optical setup for probabilistic teleportation of quantum information from a qubit to a bipartite state.

The optical system presented in Fig. 6 works as follows:

Input state:

$$(\alpha|H\rangle + \beta|V\rangle) \otimes \left(\frac{|HHH\rangle + |VVV\rangle}{\sqrt{2}} \right) \quad (16)$$

After PBS_{HV} :

$$\alpha|HHHH\rangle + \beta|VVVV\rangle + |\Omega\rangle \quad (17)$$

After Both PBS_{FS} :

$$\frac{1}{2}(\alpha|HH\rangle + \beta|VV\rangle) \otimes \left(\frac{|FF\rangle + |SS\rangle}{\sqrt{2}} \right) + \frac{1}{2}(\alpha|HH\rangle - \beta|VV\rangle) \otimes \left(\frac{|FS\rangle + |SF\rangle}{\sqrt{2}} \right) + \frac{1}{\sqrt{2}}|\Omega\rangle \quad (18)$$

From (18) one sees that the probabilistic quantum teleportation succeeds with probability 0.5 if the tripartite GHZ state is generated. Hence, the complete probability of success of the setup in Fig. 6 is 0.125 and, when it happens, the following operation is realized $(\alpha|H\rangle + \beta|V\rangle)_1 \otimes (|HHH\rangle + |VVV\rangle)_{123} / 2^{1/2} \rightarrow (\alpha|HH\rangle + \beta|VV\rangle)_{23}$, since the user at location 1 informs to user in location 2 if he/she has or not to apply a Z gate in his/her qubit. Obviously the other two qubits are consumed in the measurements.

The second setup for probabilistic quantum teleportation using tripartite GHZ state is shown in Fig. 7.

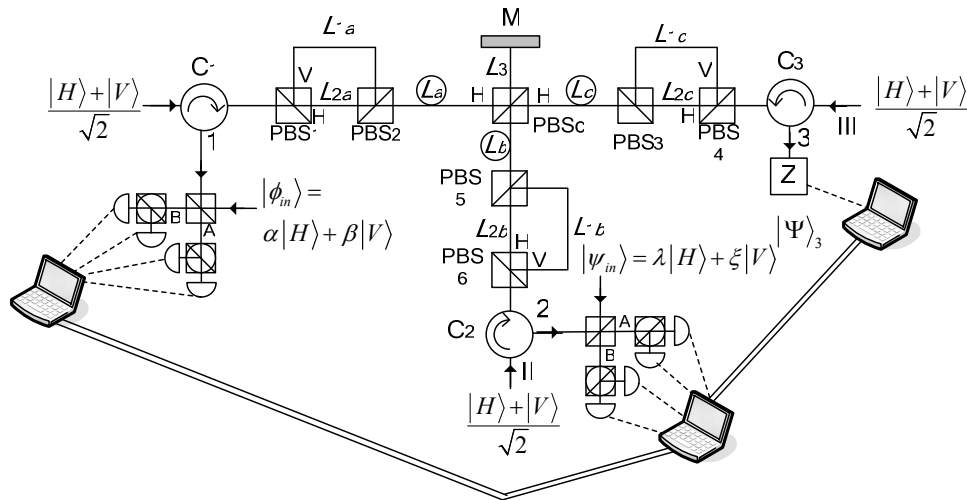


Figure 7. Optical setup for probabilistic teleportation of quantum information from two qubits to one qubit.

The optical system presented in Fig. 7 works as follows:

Input state:

$$(\alpha|H\rangle + \beta|V\rangle) \otimes (\lambda|H\rangle + \xi|V\rangle) \otimes \left(\frac{|HHH\rangle + |VVV\rangle}{\sqrt{2}} \right) \quad (19)$$

After both PBS_{HV}:

$$\alpha\lambda|HHHHH\rangle + \beta\xi|VVVVV\rangle + |\Omega\rangle \quad (20)$$

After both PBS_{FS}:

$$\frac{\sqrt{|\alpha\lambda|^2 + |\beta\xi|^2}}{2} \left(\frac{\alpha\lambda|H\rangle + \beta\xi|V\rangle}{\sqrt{|\alpha\lambda|^2 + |\beta\xi|^2}} \right) \otimes |\Phi\rangle_e + \frac{\sqrt{|\alpha\lambda|^2 + |\beta\xi|^2}}{2} \left(\frac{\alpha\lambda|H\rangle - \beta\xi|V\rangle}{\sqrt{|\alpha\lambda|^2 + |\beta\xi|^2}} \right) \otimes |\Phi\rangle_o + |\Omega\rangle \quad (21)$$

$$|\Phi\rangle_e = \frac{|SS\rangle + |FF\rangle}{\sqrt{2}}; \quad |\Phi\rangle_o = \frac{|SF\rangle + |FS\rangle}{\sqrt{2}} \quad (22)$$

From (21)-(22), one sees that the probabilistic quantum teleportation succeeds with probability $(|\alpha\lambda|^2 + |\beta\xi|^2)/2$ when the tripartite state is generated. When the teleportation succeeds the following operation is realized

$$(\alpha|H\rangle + \beta|V\rangle)_1 \otimes (\lambda|H\rangle + \xi|V\rangle)_2 \otimes (|HHH\rangle + |VVV\rangle)_{123} / 2^{1/2} \rightarrow (\alpha\lambda|H\rangle + \beta\xi|V\rangle)_3 / (|\alpha\lambda|^2 + |\beta\xi|^2)^{1/2}, \quad (23)$$

since the users at locations 1 and 2 inform to user in location 3 if he/she has or not to apply a Z gate in his/her qubit. A slightly different version of the setup in Fig. 7, shown in Fig. 8, can be used to teleport the xor function between two classical bits [20]. The teleportation of the xor function between two classical bits has practical importance since it can be used in a variety of quantum information protocols, as quantum key distribution, error correction, access control and secure contract signature.

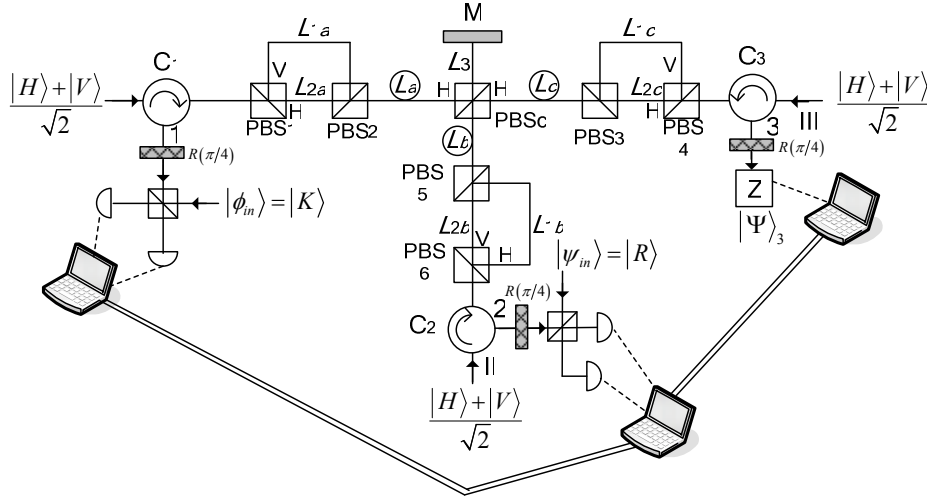


Figure 8. Optical setup for probabilistic teleportation of the xor function of two classical bits.

In Fig. 8 K and $R \in \{H, V\}$ and, due to the polarization rotators $R(\pi/4)$ (Hadamard gates) at each output, the tripartite entangled state generated when the setup succeeds is

$$|\psi\rangle_{123} = \frac{1}{2} [|HHH\rangle + |HVV\rangle + |VHV\rangle + |VVH\rangle] \quad (24)$$

The optical system presented in Fig. 8 works as follows:

Input state:

$$|K\rangle |R\rangle \otimes \left(\frac{|HHH\rangle + |HVV\rangle + |VHV\rangle + |VVH\rangle}{2} \right) \quad (25)$$

After both PBS_{HV} :

$$|HHHHH\rangle + |\Omega\rangle \quad \text{if } K = R = H \quad (26)$$

$$|HHVVV\rangle + |\Omega\rangle \quad \text{if } K = H \text{ and } R = V \quad (27)$$

$$|VVHHV\rangle + |\Omega\rangle \quad \text{if } K = V \text{ and } R = H \quad (28)$$

$$|VVVVH\rangle + |\Omega\rangle \quad \text{if } K = R = V \quad (29)$$

Hence, as can be seen in (26)-(29) every time the teleportation succeeds the qubit at output 3 (last qubit in (26)-(29)) is $|K \oplus R\rangle$.

5. Conclusions

Firstly, we have presented an optical setup able to implement a probabilistic teleportation of polarization encoded qubit using only common linear optical devices. Since the teleportation is probabilistic, Alice has to inform to Bob when the teleportation succeed and, in this case, if Bob has or has not to apply a phase-flip in his photon. Following, it was proposed two optical setups for entanglement generation and distribution, one for bipartite and the other for three partite states. Both of them were used together (as entanglement source) with the optical setup for probabilistic teleportation, providing complete optical setups for teleportation of quantum information from: 1) one qubit to another qubit ($\alpha|H\rangle+\beta|V\rangle \rightarrow \alpha|H\rangle+\beta|V\rangle$); 2) one qubit to a bipartite state ($\alpha|H\rangle+\beta|V\rangle \rightarrow \alpha|HH\rangle+\beta|VV\rangle$); 3) two qubits to one qubit ($[(\alpha|H\rangle+\beta|V\rangle)\otimes(\lambda|H\rangle+\xi|V\rangle)] \rightarrow [\alpha\lambda|H\rangle+\beta\xi|V\rangle]/(|\alpha\lambda|^2+|\beta\xi|^2)^{1/2}$). A particular case of this last one permits to implement the teleportation of the xor function between two classical bits. At last, the setups proposed are easy to implement since only common optical devices are used and they can be used to run different protocols of quantum communication.

Acknowledgment

This work was supported by the Brazilian agency CNPq.

References

- [1] E. Knill, R. Laflamme and G. J. Milburn, Nature, 409, (2001) 46.
- [2] T. B. Pitman, B. C. Jacobs and J. D. Franson, quant-ph/0404059 (2004).

- [3] T. C. Ralph, A. G. White, W. J. Munro, and G. J. Milburn, *Phys. Rev. A*, 65, (2001) 012314.
- [4] T. B. Pittman, B. C. Jacobs, and J. D. Franson, *Phys. Rev. A*, 64, (2001) 062311/1-9.
- [5] T. B. Pittman, M. J. Fitch, B. C. Jacobs, and J. D. Franson, *Phys. Rev. A*, 68, (2003) 032316/1-4.
- [6] Y. Li and T. Kobayashi, *Opt. Comm.*, 244, (2005), 285.
- [7] T. B. Pittman, B. C. Jacobs, and J. D. Franson, *Opt. Comm.*, 246, (2005) 545.
- [8] M. Oberparleiter and H. Weinfurter, *Opt. Comm.*, 183, (2000) 133.
- [9] P. G. Kwiat, K. Mattle, H. Weinfurter and A. Zeilinger, *Phys. Rev. Lett.*, 75, 24 (1995) 4337.
- [10] Y.-H. Kim, S. P. Kulik, Y. Shih, *Phys. Rev. A*, 63, (2001) 060301.
- [11] T. Suhara and H. Kintaka, *IEEE J. of. Quant. Elect.*, 41, (2005), 1203.
- [12] X. Li, J. Chen, P. Voss, J. Sharping and P. Kumar, *Opt. Express*, 12, 16, (2004) 3737.
- [13] M. J. A. de Dood, W. T. M. Irvine and D. Bouwmeester, *Phys. Rev. Lett.*, 93, 4, (2004) 040504-1.
- [14] K. Banaszek, A. B. U'Ren, I. A. Walmsley, *Opt. Lett.*, 26, 17, (2001) 1367.
- [15] A. Poppe, A. Fedrizzi, R. Ursin, H. R. Böhm, T. Lorünser, M. Peev, M. Suda, C. Kurtsiefer, H. Weinfurter, T. Jennewein, and A. Zeilinger, *Opt. Express*, 12, 16, (2004) 3865.
- [16] J.-W. Pan, M. Daniell, S. Gasparoni, G. Weihs and A. Zeilinger, *Phys. Rev. Lett.*, 86, 20, (2001) 4435.
- [17] D. Bouwmeester, J.-W. Pan, H. Weinfurter and A. Zeilinger, *J. of. Mod. Opt.*, 47, 2/3, (2000) 279.

- [18] F. A. Bovino, P. Varisco, A. M. Colla, G. Castagnoli, G. D. Giuseppe, and A. V. Segienko, *Opt. Comm.*, 227, (2003) 343.
- [19] A. Dragan, *Phys. Rev. A*, 70, (2004) 053814.
- [20] P. B. M. de Sousa, J. B. R. Silva, and R. V. Ramos, *J. of Mod. Opt.*, 53, (2006) 12.

Anexo 3

Artigo Científico - III

Artigo submetido para a revista científica arbitrada Journal of Lightwave Technology.

Quantum Communication with Polarization Encoded Qubit Using Quantum Error Correction

Daniel Barbosa de Brito, José Cláudio do Nascimento and Rubens Viana Ramos

Abstract — One of the most promising physical properties for practical implementation of quantum technology is light polarization. However, since light polarization is a fragile property, the use of quantum error correction is a crucial issue in order to make quantum information feasible. In this direction, this work discusses optical setups for quantum error correction. In particular, we show how to use the quantum error correction setup to provide error-free entanglement distribution and its use in an error-free probabilistic teleportation setup. After, we discuss the performance of the error correction setup in a very noisy channel. At last, we show that the same quantum error correction setup can also be used to correct bipartite of qubit states.

Keywords — Light polarization, quantum communication, quantum error correction.

I. INTRODUCTION

Quantum communication and computation are new areas of information processing that makes use of quantum properties in order to permit the realization of new ways communication and computation without counterpart in the classical world, as quantum key distribution [1-3], quantum teleportation [4-6] and quantum searching [7,8]. One of the most promising physical properties for experimental realization of quantum technologies is the light polarization. This happens because the polarization encoded qubit is easy to generate, detect and transform. On the other hand, it is well known that light polarization is also a fragile property that changes in a non-predicted way during light propagation in common single-mode fibers. Thus, in order to make quantum technology based on light polarization feasible, quantum error corrections schemes must be employed, that is, the unpredicted light polarization changes must be controlled. Quantum error correction can be achieved by using quantum codes [9-12]. Most quantum codes are based on the introduction of redundancy. Additional qubits are included and entangled with the qubit that carries the useful information. For a polarization encoded-qubit using single-photons, each qubit is represented by the polarization of an optical pulse containing only one photon. This mean that a quantum code of n -qubits will use n single-photon pulses, where $n-1$ are ancillas. The n photons must be entangled through an n -qubit quantum circuit. All of them are sent through the noisy channel and disentangled at the receiver by another quantum circuit. The ancillas are measured and, according to their values, a selected single-qubit operation (a polarization change) is applied in the signal qubit in order to recover the same polarization before noisy channel propagation. The block diagram is shown in Fig. 1. In this figure, $|\theta\rangle$ is the input signal and $|\theta'\rangle$ is the corrupted signal at channel output. The ancillas are considered initially in the horizontal linear polarization.

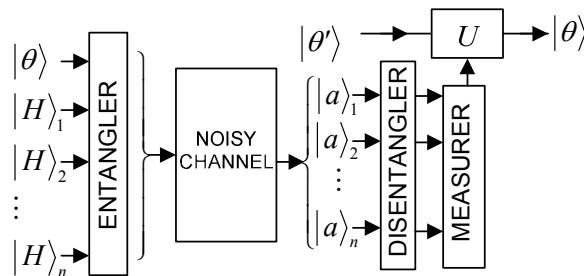


Figure 1 – Quantum error correction using entangled states.

The most famous quantum code able to correct a general single-qubit error is the Shor code [13]. It uses nine qubits. The smallest quantum code able to correct a general error in a qubit is a five qubits code [13]. The codification, using not normalized states, is as shown in (1) and (2).

$$\begin{aligned}
|0_i\rangle = & |HHHHH\rangle + |VHHVH\rangle + |HVHHV\rangle + |VHVHH\rangle - |HVHVH\rangle - \\
& |VVHVV\rangle - |HHVVH\rangle - |VVHHH\rangle - |VVVHV\rangle - |HHHVH\rangle - |VVVVH\rangle \\
& - |HVVVV\rangle - |VHHHV\rangle - |HVVHH\rangle - |VHVVV\rangle + |HHVHV\rangle
\end{aligned} \tag{1}$$

$$\begin{aligned}
|1_i\rangle = X |0_i\rangle = & |VVVVV\rangle + |HVVVV\rangle + |VHVVV\rangle + |HVHVH\rangle + |VHVHV\rangle \\
& - |HHVHH\rangle - |VVHHV\rangle - |HHVVH\rangle - |HHHVH\rangle - |VVVHH\rangle - |HHHHV\rangle \\
& - |VHHHH\rangle - |HVVVH\rangle - |VHHVV\rangle - |HVHHH\rangle + |VVHVH\rangle
\end{aligned} \tag{2}$$

In (2) X is a polarization rotator of $\pi/2$ (the NOT gate). The quantum coder and decoder is the quantum circuit shown in Fig. 2.

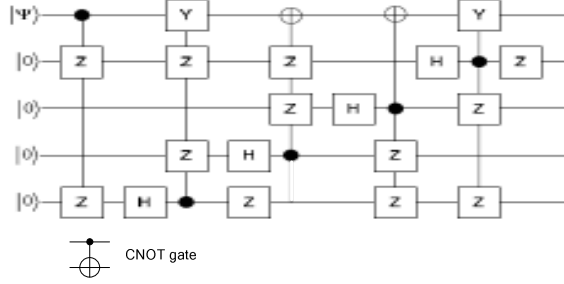


Figure 2 – Quantum circuit for five qubits quantum code.

In Fig. 2 Z , Y and H are the (single-qubit gates) polarization rotations

$$Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}, H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix} \tag{3}$$

Every single-qubit gate can be implemented using polarization rotators and compensators. On the other hand, the two-qubit gates Controlled-NOT (CNOT) and Controlled-Z require large non-linearities, not achievable with current technology. A CNOT gate using only linear optical device can be constructed, however, its behavior is probabilistic, sometimes the gate works and sometimes it fails [14-17]. Therefore, the physical implementation of quantum codes employing redundancy through entanglement is, with current technology, unfeasible. In order to overcome this problem, it has been proposed a single-qubit quantum error correction (QEC) system that does not use both ancillas and entanglement [18]. In this direction, this work extends the schemes proposed in [18,19] in three points: 1) Proposing a complete optical setup for probabilistic quantum teleportation using QEC. 2) Analyzing the performance of the QEC setup when the channel is very noisy due to fast variations of the fiber birefringence. 3) Showing that the QEC setup can also be used to protect bipartite of qubit quantum states.

This work is outlined as follow: In Section II, the QEC setup for single-photon quantum communication systems and its use in error-free entanglement distribution and probabilistic teleportation are considered. In Section III, it is analysed the performance of the QEC setup considering a very noisy channel. In Section IV we show that the QEC setup can also be used to correct bipartite of qubit quantum states. At last, the conclusions are presented in Section V.

II. QUANTUM ERROR CORRECTION SETUPS

In order to make the polarization encoded qubit transmission protected against the noise (unpredictable polarization rotations) during propagation, quantum codes can be used. However, a simpler QEC (without using ancillas and entanglement) based on time-bin qubit has been proposed [18] as well its use in error-free distribution of polarization entangled pair of photons [20]. A simplified version of the setup presented in [18] was proposed in [19]. Here we show this last is also suitable for error correction in polarization entangled pair of photons distribution. Firstly, we give a brief description of the optical setup used. It is shown in Fig. 3 [19].

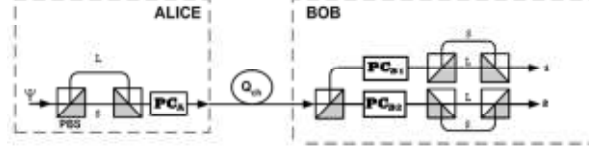


Figure 3. Optical setup for error correction.

In Fig. 3, PCs are Pockels cells and L and S mean, respectively, long and short path. Let us assume the input state at Alice's place is $|\psi\rangle = \alpha|H\rangle + \beta|V\rangle$ and the noisy channel is modeled by the unitary operation U that implements the transformation

$$U|H\rangle = \cos(\varphi)|H\rangle + \sin(\varphi)e^{i\lambda}|V\rangle, \quad (4)$$

where φ and λ are random variables. In Fig. 3, there are two paths after the first PBS, a short path (S) taken by the horizontal component and a long path (L) taken by the vertical component. When the input state passes through the unbalanced polarization interferometer, the components of the polarization are separated in the time, producing the state $\alpha|H\rangle_S + \beta|V\rangle_L$. Alice turns on her Pockels cell only when L component is present, effecting the transformation $|V\rangle_L \rightarrow |H\rangle_L$. Thus, the encoded state sent by Alice in the quantum channel is $|\Psi\rangle = \alpha|H\rangle_S + \beta|H\rangle_L$. Using (4), the quantum state at channel output is given by

$$U|\Psi\rangle = \alpha(\cos(\varphi)|H\rangle_S + e^{i\lambda}\sin(\varphi)|V\rangle_S) + \beta(\cos(\varphi)|H\rangle_L + \sin(\varphi)e^{i\lambda}|V\rangle_L) \quad (5)$$

At Bob's side, the Pockels cell PC_{B1} is activated to rotate the polarization only of the S component while PC_{B2} is activate to rotate only the L component. At each mode, 1 (upper arm) and 2 (lower arm) there exists an unbalanced polarization interferometer. In these interferometers, the horizontal component takes the long path while the vertical component takes the short path. When the corrupted state (5) arrives at Bob's place, after passing through the first PBS and Pockels cells, it is transformed to

$$\alpha[\cos(\varphi)|H\rangle_S^2 + \sin(\varphi)e^{i\lambda}|H\rangle_S^1] + \beta[\cos(\varphi)|V\rangle_L^2 + \sin(\varphi)e^{i\lambda}|V\rangle_L^1] \quad (6)$$

This state passes through the unbalanced polarization interferometers producing the total output state

$$\cos(\varphi)(\alpha|H\rangle_{SL}^2 + \beta|V\rangle_{LS}^2) + \sin(\varphi)e^{i\lambda}(\alpha|H\rangle_{SL}^1 + \beta|V\rangle_{LS}^1). \quad (7)$$

In (6) and (7) the superscripts 1 and 2 denote the paths towards the output modes 1 and 2. From (7) one sees that Bob obtains the corrected state in outputs 1 and 2 with probabilities, respectively, equal to $\sin^2(\varphi)$ and $\cos^2(\varphi)$. When the channel is approximately an ideal channel Bob obtains the uncorrupted state more likely in output 1, on the other hand, when φ is allowed to vary over its total range of values according to a uniform distribution, then the probability of obtaining the uncorrupted state in one of the outputs tends to $1/2$. One can not be sure in which output the photon will emerge, however, using an optical delay and an electro-optic switch to form a time multiplexing system, one can have the photon always at the same output (but in different times).

Any error (polarization change) that can be modeled by the sequence compensator-rotator-compensator can be corrected. For this, the characteristic time of change of the fiber parameters must be larger than the time separation between S and L pulses.

Using two equal setups of the type shown in Fig. 3, the setup for error correction in Bell state distribution is as shown in Fig. 4.

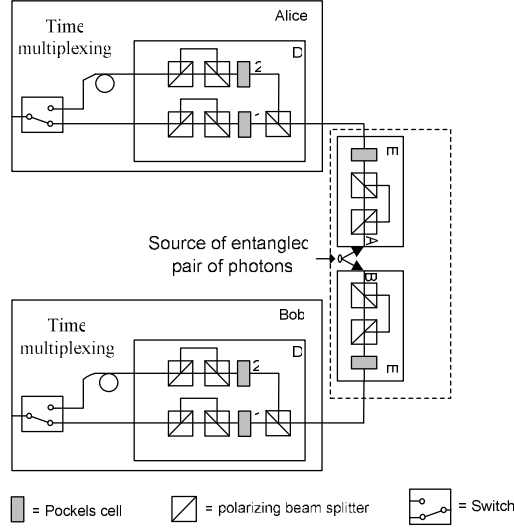


Figure 4. Error correction setup for polarization entangled pair of photons

In Fig. 4, the time multiplexing scheme composed by a time delay and an electro-optic switch it used to guarantee that both photons will always emerge from the same output at Alice and Bob sides. It is easy to show that, having the initial input state $|\Phi\rangle = [|HH\rangle + |VV\rangle] / 2^{1/2}$ the output state is

$$|\Phi\rangle = \sum_{j,k=1}^2 e^{i\xi_{jk}} \sin\left(\varphi_a - \frac{j\pi}{2}\right) \sin\left(\varphi_b - \frac{k\pi}{2}\right) |\phi\rangle_{jk} \quad (8)$$

$$|\phi\rangle_{jk} = \frac{|HH\rangle_{jk} + |VV\rangle_{jk}}{\sqrt{2}} \quad (9)$$

$$\xi_{11} = \phi_a + \phi_b; \xi_{12} = \phi_a + \lambda_b; \xi_{21} = \lambda_a + \phi_b; \xi_{22} = \lambda_a + \lambda_b; \quad (10)$$

where the noisy channels (channel a : from source of entangled photons to Alice; channel b : from source of entangled photons to Bob) are modeled by the unitary operations realizing the transformations $U_{a(b)}|H\rangle = \cos(\varphi_{a(b)})e^{i\phi_{a(b)}}|H\rangle + \sin(\varphi_{a(b)})e^{i\lambda_{a(b)}}|V\rangle$ (once more the angles are random variables). The state $|HH\rangle_{jk}$, for example, means a horizontal state emerging from output $j(k)$ at Alice (Bob). After the time multiplexing the spatial uncertainty becomes a time uncertainty, that is, the photon will appear earlier if it took the shortest path (output 1) or latter if it took the longest path (output 2). Once entangled photons can be distributed in an error-free way, it is possible to construct quantum communication with low error rate.

A probabilistic teleportation of polarization encoded qubit can be implemented using the setup shown in Fig. 5.

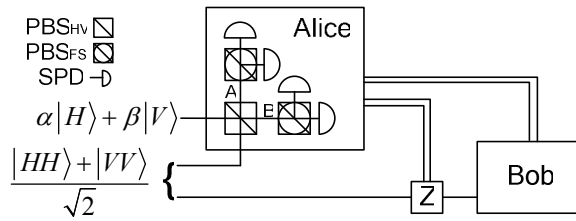


Figure 5. Optical setup for probabilistic teleportation of polarization encoded qubit.

In Fig. 5 SPD is a single-photon detector, PBS_{HV} is a PBS (polarization beam splitter) in the rectangular basis $\{|H\rangle, |V\rangle\}$ while PBS_{FS} is a PBS in the diagonal basis $\{|F\rangle = [|H\rangle + |V\rangle] / 2^{1/2}, |S\rangle = [|H\rangle - |V\rangle] / 2^{1/2}\}$. The double lines mean classical communication. The quantum state evolution in the setup of Fig. 5 is as follow:

$$|\psi\rangle_{in} = (\alpha|H\rangle + \beta|V\rangle) \left(\frac{|HH\rangle + |VV\rangle}{\sqrt{2}} \right) \quad (11)$$

$$|\psi\rangle_{PBS_{HV}} = \frac{1}{\sqrt{2}} [\alpha|HHH\rangle + \beta|VVV\rangle] + \frac{1}{\sqrt{2}} |\Omega\rangle \quad (12)$$

$$|\Omega\rangle = \alpha|HV, 0, V\rangle + \beta|0, VH, H\rangle \quad (13)$$

$$|\psi\rangle_{PBS_{VS}} = \frac{1}{\sqrt{2}} \frac{(|FF\rangle + |SS\rangle)|\Psi^+\rangle + (|FS\rangle + |SF\rangle)|\Psi^-\rangle}{2} + \frac{1}{\sqrt{2}} |\Omega\rangle \quad (14)$$

$$|\Psi^\pm\rangle = \alpha|H\rangle \pm \beta|V\rangle \quad (15)$$

The teleportation succeeds if Alice measures one photon in output A and one photon in output B. Hence, as can be seen in (14)-(15), Alice has to send two classical bits to Bob, the first one informing if the teleportation succeeded, what happens with probability 50%, and the second informing if Bob has or has not to apply a phase shift in his photon.

Now, it is possible to put the setups of Figs. 4 and 5 together in order to construct an optical setup for probabilistic quantum teleportation employing error correction and using only simple optical devices. The setup proposed is shown in Fig. 6. Using it, a quantum teleportation succeeds with probability $0.25\cos^2(\varphi_a)$ if Bob just measures the qubit received. The probability $\cos^2(\varphi_a)$ appears due to fact that Alice sends the qubit $|\phi_m\rangle$ in the right time to coincide with the arrival of the photon that took the path 1. If the photon coming from the central node took path 2, the teleportation does not happen. If Bob uses the qubit received to another quantum operation for which he has to know the exact time of arrival of the photon sent by the central node, then the probability of success is $0.25\cos^2(\varphi_a)\cos^2(\varphi_b)$, assuming that Bob also realizes his synchronization considering the output 1.

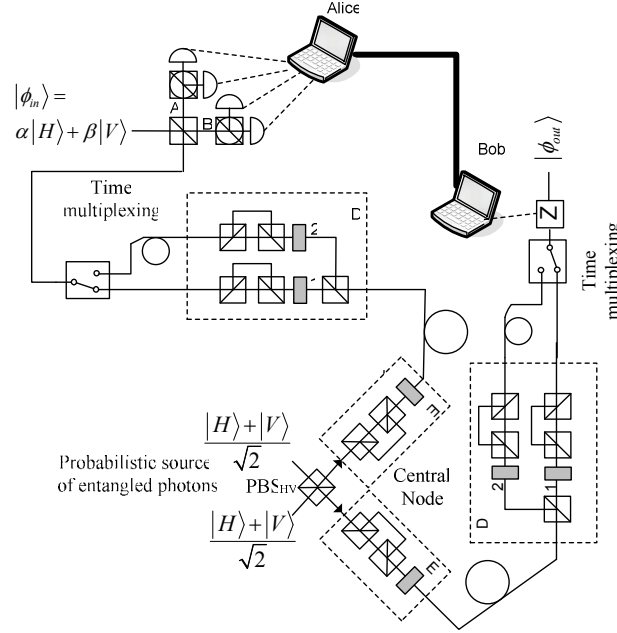


Figure 6. A simple optical setup for probabilistic teleportation employing error correction.

III. VERY NOISY CHANNEL

In this section we analyze the performance of the error correction setup when the channel is very noisy implying that the fiber birefringence has fast variations and it can change during the time interval between the short and long time slots. In this case, the pulses in each time slot will experiment different unitary evolutions. Since the channel varies between the S and L components of the state sent by Alice, what is the probability of the state received by Bob to be same sent by Alice? In order to answer this

question, consider that $U_S(\varphi_S, \xi_S, \lambda_S)$ and $U_L(\varphi_L, \xi_L, \lambda_L)$ are, respectively, the unitary transformations acting in the S and L pulses. The quantum state at Alice's encoder output can be represented by:

$$\alpha |H, S\rangle + \beta |H, L\rangle = |H\rangle (\alpha |S\rangle + \beta |L\rangle). \quad (16)$$

Hence, polarization and time-bin are not entangled. When the unitary transformation is the same for both pulses, the channel does not entangle polarization and time-bin and the qubit can be received corrected at the receiver. On the other hand, when the fiber birefringence varies in a time interval shorter than the time separation between S and L pulses, one has at channel output

$$\alpha U_S |H, S\rangle + \beta U_L |H, L\rangle = \quad (17)$$

$$\begin{aligned} & \alpha \cos(\varphi_S) |H, S\rangle + \alpha \sin(\varphi_S) e^{i\lambda_S} |V, S\rangle + \\ & \beta \cos(\varphi_L) |H, L\rangle + \beta \sin(\varphi_L) e^{i\lambda_L} |V, L\rangle \end{aligned} \quad (18)$$

and polarization and time-bin are entangled. The amount of entanglement of the state (18) is given by

$$E = 4|\alpha|^2 |\beta|^2 |\langle V | U_S^\dagger U_L | H \rangle|^2 = 4|\alpha|^2 |\beta|^2 \Delta_1 \quad (19)$$

$$\begin{aligned} \Delta_1 = & \cos^2(\varphi_S) \sin^2(\varphi_L) + \cos^2(\varphi_L) \sin^2(\varphi_S) - \\ & 2 \cos(\varphi_S) \sin(\varphi_L) \cos(\varphi_L) \sin(\varphi_S) \cos(\lambda_L - \lambda_S) \end{aligned} \quad (20)$$

As expected, when $U_S=U_L$ one has $U_S^\dagger U_L = I$, resulting in $E=0$, and the quantum error correction does not fail. The output state is

$$\begin{aligned} |\psi\rangle = & \sin(\varphi_S) e^{i\lambda_S} \alpha |H\rangle_{SL}^1 + \sin(\varphi_L) e^{i\lambda_L} \beta |V\rangle_{SL}^1 + \\ & \cos(\varphi_S) \alpha |H\rangle_{SL}^2 + \cos(\varphi_L) \beta |V\rangle_{SL}^2 \end{aligned}, \quad (21)$$

and its fidelity is given by

$$F = |\alpha|^4 + |\beta|^4 + 2|\alpha|^2 |\beta|^2 \Delta_2 \quad (22)$$

$$\Delta_2 = \cos(\varphi_S) \cos(\varphi_L) + \sin(\varphi_S) \sin(\varphi_L) \cos(\lambda_L - \lambda_S) \quad (23)$$

The larger the entanglement, the larger the error rate, $1-F$. This can be seen in the simple case that $\lambda_L=\lambda_S$. In this case Δ_1 and Δ_2 depend only on $\Delta\Phi=\varphi_L-\varphi_S$ and one can obtain the curve shown in Fig. 7 for $|\alpha|^2|\beta|^2=0.5$.

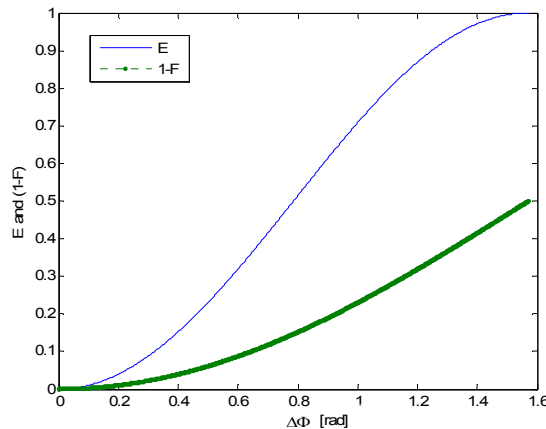


Figure 7. Error rate and entanglement versus $\Delta\Phi=\varphi_L-\varphi_S$ when $\lambda_L=\lambda_S$.

For other values of $|\alpha|^2$ and $|\beta|^2$ the same kind of behaviour is observed.

IV. BEYOND QUBIT ERROR CORRECTION

In Section II it has been shown how to use the QEC setup to protect the individual qubits of a bipartite state, that is, each individual qubit “sees” a different channel. In this section we consider the correction of the complete bipartite state. In other words, Alice has the bipartite state $|\Psi\rangle = \alpha|HH\rangle_{0,\delta} + \beta|HV\rangle_{0,\delta} + \gamma|VH\rangle_{0,\delta} + \xi|VV\rangle_{0,\delta}$, that are two photon separated by δ in time, and she wants to send this state to Bob. In order to do this, Alice uses the setup shown in Fig. 8.

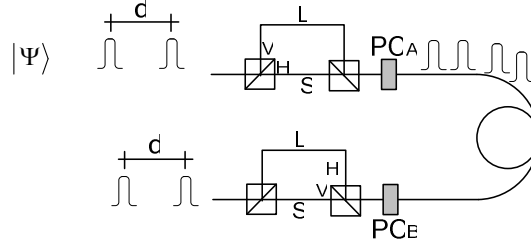


Figure 8. Quantum error correction of bipartite quantum state.

The quantum state leaving Alice’s polarization interferometer and after Alice’s Pockels cell are, respectively,

$$|\psi_1\rangle = \alpha|HH\rangle_{S,\delta S} + \beta|HV\rangle_{S,\delta L} + \gamma|VH\rangle_{L,\delta S} + \xi|VV\rangle_{L,\delta L} \quad (24)$$

$$|\psi_2\rangle = \alpha|HH\rangle_{S,\delta S} + \beta|HH\rangle_{S,\delta S} + \gamma|HH\rangle_{L,\delta S} + \xi|HH\rangle_{L,\delta L} \quad (25)$$

In (24) one can observe that there are four time slots: S , $\delta+S$, L and $\delta+L$. As can be noted in (25), the PC_A is activated in order to rotate the polarization ($\pi/2$) of the pulses only in the time slots L and $\delta+L$. Once more channel propagation is modelled by an unknown unitary transformation, but now this one acts in both qubits. In a general way, one can say that $U|HH\rangle = a|HH\rangle + b|HV\rangle + c|VH\rangle + d|VV\rangle$ where the coefficients a , b , c and d depend on the parameters of U . Thus, the quantum state at channel output is

$$\begin{aligned} |\psi_3\rangle = & a\left(\alpha|HH\rangle_{S,\delta S} + \beta|HH\rangle_{S,\delta L} + \gamma|HH\rangle_{L,\delta S} + \xi|HH\rangle_{L,\delta L}\right) + \\ & b\left(\alpha|HV\rangle_{S,\delta S} + \beta|HV\rangle_{S,\delta L} + \gamma|HV\rangle_{L,\delta S} + \xi|HV\rangle_{L,\delta L}\right) + \\ & c\left(\alpha|VH\rangle_{S,\delta S} + \beta|VH\rangle_{S,\delta L} + \gamma|VH\rangle_{L,\delta S} + \xi|VH\rangle_{L,\delta L}\right) + \\ & d\left(\alpha|VV\rangle_{S,\delta S} + \beta|VV\rangle_{S,\delta L} + \gamma|VV\rangle_{L,\delta S} + \xi|VV\rangle_{L,\delta L}\right) \end{aligned} \quad (26)$$

Now, Bob activates his Pockels cell in order to rotate the polarization only of the pulses in the time slots L and $\delta+L$. Further, in Bob’s polarization interferometer, the horizontal component takes the longest path while the vertical component takes the shortest path. Thus, the Bob’s output state is

$$\begin{aligned} |\psi_4\rangle = & a\left(\alpha|HH\rangle_{SL,\delta SL} + \beta|HV\rangle_{SL,\delta LS} + \gamma|VH\rangle_{LS,\delta SL} + \xi|VV\rangle_{LS,\delta LS}\right) + \\ & b\left(\alpha|HV\rangle_{SL,\delta SS} + \beta|HH\rangle_{SL,\delta LL} + \gamma|VV\rangle_{LS,\delta SS} + \xi|VH\rangle_{LS,\delta LL}\right) + \\ & c\left(\alpha|VH\rangle_{SS,\delta SL} + \beta|VV\rangle_{SS,\delta LS} + \gamma|HH\rangle_{LL,\delta SL} + \xi|HV\rangle_{LL,\delta LS}\right) + \\ & d\left(\alpha|VV\rangle_{SS,\delta SS} + \beta|VH\rangle_{SS,\delta LL} + \gamma|HV\rangle_{LL,\delta SS} + \xi|HH\rangle_{LL,\delta LL}\right) \end{aligned} \quad (27)$$

As can be seen in (27), there are six time slots at the output: $S+S$, $S+S+\delta$, $S+L$, $S+L+\delta$, $L+\delta$, $L+L+\delta$. With probability $|a|^2$ the correct state is found in the time slots $S+L$, $S+L+\delta$. Hence, selecting only these two time slots, one can be sure that, if there are photons, then they represent the correct bipartite state.

V. CONCLUSIONS

We have discussed an error correction setup based on time-bin qubit showing how using it to obtain error free entanglement distribution. Following, the complete setup for probabilistic teleportation of polarization encoded qubit with error correction for entanglement distribution was presented. The advantage of this setup is the fact that it uses only linear optical devices and, hence, it can be constructed with today technology. The difficulties in the setup proposed are the time synchronization due to the Pockels cell in the error correction setup, and the fact that the polarization interferometers at transmitter and receiver places must be equal. It also suffers of other problems common to every setup for quantum communication in optical networks like the low performance of present single-photon detectors and single-photon sources. Following it was shown that if the channel varies during the time interval between the first and the second time slot, then an entanglement between the photon polarization and time slot arises. In this case, the performance (ability to correct the polarization change during fiber propagation) of the error correction setup depends on the amount of entanglement between polarization and time-bin. The larger the entanglement, the larger the error rate, although this last also depends on the polarization qubit sent. At last, we showed that the optical setup used to correct single-qubit error can also be used to correct the error of a bipartite of qubit state.

REFERENCES

- [1] C. H. Bennett, "Quantum Cryptography Using Any Two Nonorthogonal States", *Phys. Rev. Lett.*, **68**, 21, 3121-3124, 1992.
- [2] N. Gisin, G. Ribordy, W. Tittel, H. Zbinden, "Quantum cryptography", *Rev. Mod. Phys.*, **74** 145, 2002.
- [3] C. H. Bennett, and G. Brassard, "1984 Quantum cryptography: public key distribution and coin tossing Proc. IEEE", *Conf. on Computers, Syst. and Signal Process.*, 175-9, 1992.
- [4] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters, "Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels", *Phys. Rev. Lett.* **70**, 1895-1898, 1993.
- [5] A. Zeilinger, "Quantum Entanglement: A Fundamental Concept Finding its Applications", *Phys. Scripta*, **T76**, 203-209, 1998.
- [6] C. H. Bennett, "Quantum Information", *Phys. Scripta*, **T76**, 210-217, 1998.
- [7] L. K. Grover, "A fast quantum mechanical algorithm for database search", in *Proceedings of the 28th Annual ACM Symposium on the Theory of Computing*, Philadelphia, Pennsylvania, 212-219, 1996.
- [8] A. Barenco, "Quantum physics and computers", *Contemp. Phys.*, **37**, 5, 375-389, 1996.
- [9] M. Grassl, T. Beth, and M. Roetteler, "On optimal quantum codes", *Inter. J. of Quant. Inf.*, **2**, 1, 55-64, 2004.
- [10] D. Kribs, R. Laflamme, and D. Poulin, "Unified and Generalized Approach to Quantum Error Correction", *Phys. Rev. Lett.* **94**, 180501, 2005.
- [11] B. Schumacher, "Quantum coding", *Phys Rev. A*, **51**, 4, 2738-2747, 1995.
- [12] A. Steane, "Quantum computing", *Rep. Prog. Phys.* **61**, 117-173, 1998.
- [13] M. A. Nielsen and I. L. Chuang, "*Quantum Computation and Quantum Information*", Cambridge Univ. Press, Cambridge, 2000.
- [14] T. B. Pitman, B. C. Jacobs and J. D. Franson, "Experimental Demonstration of a Quantum Circuit using Linear Optics Gates", *Phys. Rev. A*, **71**, 032307, 2005.
- [15] F. M. Spedalieri, H. Lee, and J. P. Dowling, "High-fidelity linear optical quantum computing with polarization encoding", *quant-ph/0508113*, 2005.
- [16] T. C. Ralph, A. G. White, W. J. Munro, and G. J. Milburn, "Simple scheme for efficient linear optics quantum gates", *Phys. Rev. A*, **65**, 012314, 2001.
- [17] P. Kok, W. J. Munro, K. Nemoto, T. C. Ralph, J. P. Dowling, and G. J. Milburn, "Review article: Linear optical quantum computing", *quant-ph/0512071*, 2005.
- [18] D. Kalamidas, "Single-photon quantum error rejection and correction with linear optics", *Phys. Lett. A*, **343**, 331-335, 2005.
- [19] J. C. do Nascimento, F. A. Mendonça, and R. V. Ramos, "Linear optical setups for active and passive quantum error correction in polarization encoded qubits" *J. of Mod. Opt.* 2007 (in press).
- [20] D. Kalamida, "Linear optical scheme for error-free entanglement distribution and a quantum repeater", *Phys. Rev. A*, **73**, 054304, 2006.