论文题目：量子计算机中的消相干研究和量子编码

作者简介：段路明，男，1972 年生，1996 年师从中国科学技术大学郭光灿教授，于 1998 年获博士学位。

摘 要

量子力学和计算机科学的交叉诞生了一门新的学科：量子计算机。最近，由于大数因子分解等一系列量子超快速算法的发现，量子计算机的研究已经取得了革命性的进展。量子计算机的优越性主要体现在量子并行算法上，正因为量子并行算法，一些经典计算机无法解决的问题，象大数的因子分解或复杂量子系统的模拟等，量子计算机可以轻而易举地解决。但量子并行算法本质性地利用了量子相干性，在实际中，由于系统和环境的不可避免的耦合，量子相干性将随时间衰减，此即消相干。消相干是实现量子计算的主要困难，为了使量子计算成为现实，一个首要的问题就是克服消相干。迄今为此，人们发现的克服消相干的最有效的方法为量子编码。本文的工作分为两个部分，第一部分对量子计算机中消相干的特性进行了系统的研究；第二部分根据量子系统消相干的具体特性，设计了一些新的高效率的量子编码方案，并改进和推广了原来已有的量子编码方案。具体如下：

量子系统中的消相干，按其理论描述方法，可分为两大类，即相位消相干和振幅消相干。相位消相干引起解相过程，而振幅消相干同时引起解相过程和能量耗散。我们首先给出单个量子比特相位消相干的计算结果，然后将结果推广到多比特的独立相位消相干。独立相位消相干是一种理想情形，作为另一种理想情形，我们考虑了多比特的集体相位消相干。研究发现，集体相位消相干和独立相位消相干具有本质的不同，最突出的一点是，对于集体相位消相干，存在相干保持态。相干保持态是指一类特殊的能在噪声环境下保持稳定的态，这类态在量子编码中有重要应用。独立和集体消相平均属于理想情形，接着我们考虑了一种实际的消相干模型：空间关税相位消相干。从此模型出发，在不同的极限情况下，我们分别导出了独立相位消相干和集体相位消相干，并给出了产生它们的具体条件。然后我们研究振幅消相干，也是按照从单比特到多比特，从独立消相干到集体消相干，再到一般的空间关联消相干的顺序。振幅消相干要比相位消相干复杂得多，为了完整地描述振幅消相干的特性，我们发展了一种新的处理量子开放系统的方法，即态的保真度的短时微扰展开法，该方法被证明是研究复杂量子开放系统的一个有力的工具。

在量子编码领域，本文主要完成了三方面的工作。量子编码按其原理，可分为量子纠错码、量子防错码、和量子避错码，其中量予纠错码是经典纠错码的量子推广，量子防错码基于量子 Zeno 效应，而量子避错码本质性地利用了消相干过程中的集体效应，后两种编码方法是量子信息论所特有的。我们在国际上率先提出了量子避错码方案，该方案利用两比特来编码一比特量子信息，通过将任意的输入态编码为一个较高维空间的相干保持态，该方案可以用来克服在物理上很重要的一类消相干。后来意大利的量子信息小组将该方案推广到更普遍的场合。我们改进了已有的量子防错码方案。原来的量子防错码方案至少需要用四比特来编码一比特量子信息，而且只克服独立消相干。我们提出一个量子防错码方案，只需用两比特来编码一比特信息，而且既可以克服独立消相干，也可以克服一般的空间关联消相干。我们还

推广了文献中量子纠错码的适用范围。量予纠错码是研究得最多的一种量子编码，原来的量子纠错方案均假定了量子比特独立地消相干。我们证明，所有的量子纠错方案都可以用来克服一般的空间关联消相干，而且量予纠错的操作步骤不需要改变。

关键词：量子计算机，量子并行算法，消相干，量子编码

Research on Decoherence in Quantum Computer and Quantum Codes

Duan Lu-Ming

Abstract

A combination of quantum mechanics and computer science yields an interesting new subject, quantum computers. The field of quantum computers has been revolutionized by the innovative work of Shor on factorization of large numbers. Quantum computers can so1ve efficiently some of the problems that cannot be attacked by any classical computers, since for these problems there are superfast quantum algorithms thanks to quantum paralle1ism. Quantum computers act as sophisticated interferometers. The coherent interference pattern between the multitude of superpositions is essential for taking advantage of quantum parallelism. However, decoherence of the qubits (quanum bits) due to the inevitable interaction with environment will collapse the state of quantum computers. Decoherence is now recognized as a main obstacle to realizing quantum computation. To overcome decoherence, many kinds of -- codes have been discovered. Quantum coding is the most efficient way to combat decoherence.

This work can be divided into two pans. In the first pan, we present a systematic study on decoherence properties in quantum computers. In the second part, we devise an efficient decoherence-reducing strategy in the presence of specific decoherence models, and improve and extend the previously-discovered quantum error correcting and preventing codes.

Decoherence in quantum systems can be divided into two main kinds, phase decoherence and amplitude decoherence. Phase decoherence induces dephasing, and amplitude decoherence induces dephasing and loss of energy at the same time. We first calculate phase decoherence of a single qubit, and then extend the result to the case of independent decoherence of multiple qubits. Independent decoherence is an ideal circumstance. As another ideal circumstance, we consider collective phase decoherence of multiple qubits. New phenomena take p1ace in collective decoherence. The most remarkable one is that for collective decoherence there are coherence-preserving states. The coherence-preserving states are a special type of states which are stable under noisy environment. These states play an important role in quantum coding. Independent decoherence and collective decoherence are ideal circumstances. We concern about the real situation, and then consider a practical decoherence model. It is found that in general circumstances qubits are decohered spatially-correlatedly. But under different extreme conditions, independent decoherence and collective decoherence can be obtained. We derive

the explicit conditions. Next, we study amplitude decoherence, in the same order as for studying phase decoherence, i.e., form the single qubit case to the multip1e qubits case, form the independent decoherence case to the collective decoherence case, and then to the general case of spatially-correlated decoherence. Amplitude decoherence is much more sophisticated than phase decoherence. To describe its properties, we develop a method called the short-time perturbative expansions for the state fidelities. This approach is proven to be a useful tool for studying open quantum systems.

There are three kinds of quantum codes, i.e., the quantum error correcting codes (QECCs), the quantum error preventing codes (QEPCs), and the quantum error avoiding codes (QEACs). The QECCs are quantum analogy of the classical error correcting codes. The QEPCs are based on the quantum Zeno effect, and the QEACs essentially exploit collective effects in the decoherence process. We have three aspects of contribution to the quantum coding theory. First, we propose the first extensive quantum error avoidance scheme. The scheme uses two qubits to protect one qubit information, and encodes arbitrary input states into corresponding coherence-preserving states in a larger Hilbert space. Second, we improve the previously-discovered quantum error prevention schemes. The previous schemes deal with independent decoherence, and use four qubits to encode one qubit information. We propose a two-bit QEPC which protects a bit of quantum information from general spatially correlated decoherence. Third, we extend the decoherence model in the quantum error correction schemes to more realistic circumstances. It is assumed that the qubits are decohered independently in the previous quantum error correction schemes. We show that the QECCs devised in the case of independent decoherence are also valid for reducing general spatia1ly-correlated decoherence, and the quantum error correction operations need not be altered.

Key words: quantum computers, quantum parallelism, decoherence, quantum coding