国防科技前沿论坛
FORUM ON FRONTIER DEFENSE TECHNOLOGY

国防科技前沿论坛'2008

论文集

二〇〇八年十月·长沙

国防科技前沿论坛'2008
论文集

二〇〇八年十月·长沙

序　言

金秋十月，我们喜迎四方嘉宾，相聚星城长沙，隆重召开第三届国防科技前沿论坛。国防科技前沿论坛由国防科学技术大学联合总装备部武器装备论证研究中心、海军装备研究院、空军装备研究院、二炮装备研究院于2006年发起并共同举办，今年是第三届。本届论坛又有军内外十二所高校参与协办，得到了军内外科研院所和高校的高度重视和大力支持，在此，我们对各兄弟单位的领导和专家表示衷心的感谢！

胡主席在党的十七大报告中指出，我军必须全面履行党和人民赋予的新世纪新阶段历史使命，提高应对多种安全威胁、完成多样化军事任务的能力，这对国防科技发展提出了更高的要求。胡主席在对学校的重要批示中，要求学校进一步增强攀登世界科技高峰的信心和勇气，不断提高自主创新能力，努力在若干重要领域掌握一批核心技术，为推进科技强军战略、建设创新型国家作出新的更大贡献。国防科技前沿论坛正是贯彻落实党中央、中央军委和胡主席重要指示的重要举措。

国防科技历来是极为活跃，极富竞争性和对抗性的领域，军事需求的牵引作用十分明显，科技创新和前沿探索的要求十分迫切。在关系国民经济命脉和国家安全的关键领域，真正的核心技术和关键技术只能依靠我们自己，只能依靠自主创新。因此，国防科技前沿论坛必须始终坚持围绕国家和军队关注的国防科技重点领域，加强国防科技创新和前沿探索，发挥科技进步和创新对战斗力提高的

推动作用，促进我军高新技术武器装备的自主发展，为广大国防科技战线的科研人员提供一个学术交流的平台。

这次会议选定新型信息技术基础研究、装备综合保障和无人作战系统技术这三个专题进行研讨。其中新型信息技术基础研究专题主要围绕对未来战争中的新型传感器、新型通信、新型高性能计算等具有重要意义的量子信息技术、太赫兹技术和光计算技术这些研究领域进行探讨；装备综合保障专题则从装备保障系统分析与设计、装备保障态势感知和装备保障综合决策三个方面对一体化联合作战中这一复杂的系统工程问题进行研讨；无人作战系统技术专题针对目前国际上普遍关注的无人作战系统，从复杂环境的感知与识别、无人作战系统的自主导航与控制和无人作战系统的规划、决策与协同等方面进行研讨。这三个专题均具有重要的学术价值和军事应用前景。让我们共同携手把论坛办得更具水平、更具特色，成为探讨国防科技发展前沿极具影响力的会议。

让我们在党中央、中央军委和胡主席的坚强领导下，深入学习实践科学发展观，进一步解放思想，集思广益，锐意进取，改革创新，瞄准军事斗争准备的紧迫需求，加快推进中国特色军事变革，把提高自主创新能力摆在更加突出的位置，为科技强军、开创国防和军队现代化建设的新局面做出更大贡献！

大会主席：张育林

二〇〇八年十月二十一日

目　录

一、新型信息技术基础

1.1　量子信息技术

1.2　太赫兹技术

1.3　光计算技术

二、装备综合保障

2.1　装备保障系统分析与设计

2.2 装备保障态势感知

2.3 装备保障综合决策

三、无人作战系统

3.1 复杂环境的感知与识别

3.2 无人作战系统的自主导航与控制

3.3 无人作战系统的规划、决策与协同

量子计算机的全电路超导簇态实现

李承祖
国防科技大学理学院，湖南　长沙　410073

摘　要：本文将文献中超导量子计算方案和簇态上的量子计算模型结合，提出了量子计算机超导全电路簇态实现方案。对这一方案实现的可行性以及超导簇态量子计算机可能带来的好处等进行了初步论证和分析。最后对量子计算机的可能发展方向提出了展望。

关键词：超导 Josephson 结量子位　簇态　簇态上的量子计算　超导簇态量子计算机

一、前言

量子计算机利用量子态编码信息，根据量子物理原理进行信息处理的机器。量子计算机不仅能克服量子物理原理对现有计算机进一步发展的制约，而且具有超出现在电子计算机的数据处理能力，成为下一代计算机发展重要方向。近十年来，人们已先后在离子阱系统、液体中分子系综核磁共振、腔 QED 以及线形光学系统实现了量子计算的基本门操作，实验演示了量子计算原理的可行性。但所有这些系统都存在一个共同的弱点，即难以规模化形成真正意义上的量子计算机。

近几年来采用固体物理系统实现量子计算引起了广泛的关注[1,2,3]。目前已提出的有量子点、超导 Josephson 电路等实现方案。一般说来，固体量子系统的环境情况更复杂，有更高的态密度，系统和环境有更强的耦合，造成计算机系统编码态的消相干，这是它的不利的一面。但它也具有其他系统不可能有的优势，例如系统参数可连续调节，易于优化设计。特别是超导电路实现，可以借助半个世纪以来发展起来的微电子学、成熟的光刻平版印刷技术制造其硬件，便于集成化、规模化，造出真正具有有一定实用价值的量子计算机。

簇态是量子系统的一种高度纠缠态，在具有 Ising 类相互作用的两能级系统中可以非常简单的制备。更重要的是小的簇态碎片可以方便的熔结成大的簇态。簇态上的量子计算模型根本不同于通常的量子门组网络模型——通过一系列的门操作么正演化输入态实现量子计算，簇态上的量子计算可仅仅通过单量子位测量执行。即任意量子计算任务，都可按算法规定测量模式，执行一系列的单量子位测量，前馈测量结果控制后续测量基实现[4,5]。信息伴随着物理量子位测量，在被处理的同时也向前传输。所以计算中所需的簇态可以边计算、边制备，这提供了战胜消相干的强有力的新方法。

采用固体超导 Josephson 电路量子位和簇态量子计算模型，通过二者的结合实现量子计算，是一有希望的量子计算机物理实现方案。

二、超导量子计算的物理原理

为了减小大规模集成芯片中电路电阻引起的热耗，超导计算机的概念已提出多年。但以前的超导计算机仍然属于经典计算的范畴，因为它仍然用器件导通和截止这样的经典物理态编码信息，并没有利用量子物理原理、量子相干叠加性质，计算操作原理仍然是经典物理的。

在物理上，人们早就认识到超导现象中的迈斯纳效应、磁通量子化、Josephson 效应等都是一种宏观量子现象，即这些用宏观参量描述的物理态，具有量子力学态的相干叠加等基本量子性质。固体超

导量子计算机就是用约瑟夫森结电路具有量子性质的宏观态编码信息。基本约瑟夫森结电路是由若干个低电容约瑟夫森结和超导电极（超导岛）组成的电路环。在低温和适当的电路参数设计条件下，电路的哈密顿量的本征空间可以简化为一个二维 Hilbert 空间，因此可以编码一个量子位。目前已经提出的量子位实现主要有两种：一种是用低电容 Josephson 结中的电荷自由度，量子位编码在超导岛上两个宏观 Cooper 对电荷数态上[6,7]；另一种基于 Josephson 结的相位或环几何磁通自由度，量子位用环中磁通态（相位）的宏观参量表征[8,9]。

还在上世纪 80 年代量子信息出现以前，人们就对 Josephson 结电路的宏观量子效应产生了兴趣，目的是研究量子力学规律是否适用于这些用宏观参数描述的态。实验上证明了宏观量子隧穿和共振隧穿[10-12]。90 年代以后，实验上还证明了 Cooper 对相干隧穿和电荷态的量子叠加[13-15]。1999 年 Nakamura etal 在时间域观测到制备在电荷本征态叠加态 Josephson 电荷量子位的量子相干振荡[6]，2000 年以后，还陆续观察到两个不同磁通态的相干叠加和 Rabi 震荡（表明可以制备出这两个宏观态的相干叠加)[16-19]。单量子位门操作，两量子位的耦合两量子位纠缠态以及两位门操作都已在实验室实现[20-24]；为了提取出量子位态信息的测量，可以用单 Cooper 对晶体管（SCT）电路和超导量子干涉仪（SQUID）实现[25-27]。这些理论和实验研究，为超导量子计算打下了坚实的基础。

2007 年 2 月 12 号，加拿大公司 D－Wave 展示了世界上第一台商用量子计算机[28]。这台计算机就是美国航空航天局（NASA）使用的芯片运用微电子元件和超低温技术制造的，芯片由铝和铌元素组成的的超导材料制成，被液氮冷冻在 5mK 的温度下。

三、簇态和簇态上的量子计算

在 2001 年德国 Raussendorf 等人提出了簇态和簇态上的量子计算方案。在这个方案中，利用事前制备的一类特殊纠缠态——簇态——为计算资源，计算由一系列的单个物理量子位测量完成。计算过程由测量的经典结果前馈控制后来测量的基组成。输入信息在测量过程中被处理，同时伴随着测量进行向前传输。整个计算过程，包括输入态制备、计算操作，计算结果的输出，完全由测量完成。测量的次序和测量基选择由特定问题的算法决定。由于簇态中的物理量子位态将在测量中被破坏，仅可使用一次，所以这个方案又称为单向量子计算方案。这一方案突出反映了测量以及纠缠对量子计算的重要性。

近几年理论、实验研究都证明了簇态上量子计算方案的可行性。首先簇态上的量子计算理论已相当完善[4,5]，产生超导电路簇态的理论方案最近已经提出[29,30]。2005 年，《Nature》上报道了 Walther 等人用参数下转换产生的 4 光子簇态，实现了单向量子计算中通用逻辑门组（一位逻辑门和两位逻辑门），并执行了 Grover 搜索算法，证明了簇态量子计算方案的可行性[31]。这一年，PRA 上还报道了澳大利亚 Nielson 等人证明的两个阈限定理[32]，表明只要在执行中的噪声低于某个常数阈值，以簇态为基础的单向量子计算可容错的进行，即足以执行任意复杂的量子计算。

以低温条件下约瑟夫森结电路宏观态的量子性质的研究，以及簇态量子计算研究为基础，有机地把它们结合起来，可能是解决当前量子计算机物理实现上的诸多难题一条出路，最终实现固态超导簇态量子计算机在原理上是可行的。

四、全电路超导簇态量子计算机

利用低温条件下约瑟夫森结电路宏观态的量子性质，采取簇态量子计算方案，实现固态、全电路量子计算机，具有下列重要的优点：

1．传统的量子计算采用网络线路模型，通过对输入态连续地、么正逻辑门操作执行量子计算。

采用簇态上以测量为基础的单向量子计算模型，利用事前制备（也可以边计算，边制备）的一类特殊纠缠态——簇态——为计算资源，计算过程由一系列的单个物理量子位测量，用测量的经典结果前馈控制后来测量的基构成。输入信息在测量过程中被处理，同时伴随着测量进行向前传输。整个计算过程，包括输入态制备、计算过程，计算结果的输出，完全由测量完成。测量的次序和测量基选择由特定问题的算法决定。这个方案具有两个明显的优点，一是单量子位测量一般比多量子位逻辑门操作要简单，更容易实现；二是鉴于簇态上的量子计算中，已经被测量过的物理量子位编码的信息已传输到后续的量子位上，被测量子位本身已从纠缠簇态中除去，根据簇态的性质，这些已经除去的量子位可以重新再纠缠起来，并方便地再熔结到后续的簇态上，这种量子处理器可以做成环形，计算循环地进行向前推进。这一方面可以节省量子处理器物理量子位数目，同时还可以做到计算所需资源“边消费，边制备”，由于消相干总是和量子态与环境相互作用时间有关，这种制备出来很快就消费掉的计算模型，提供了战胜消相干的一个有力方法。

2．和目前已经提出的量子计算物理实现方案：核磁共振、离子阱、线性光学等方案比较，核磁共振、离子阱、线性光学等方案是利用核自旋、离子或原子能级等自然界现成的系统充当量子位，参数不能自由选择，难于优化设计，特别到现在还没有找到可规模化成有实用价值的量子计算机的有效的方法。而量子计算机的超导实现则是利用人工制造宏观量子系统充当量子位。因而量子位设计参数可以人为控制，这样的系统设计灵活，易于优化。特别是采用超导 Josephson 电路实现，其硬件就可以借助于已发展半个多世纪的电子集成电路技术制造。可以方便地规模化，集成化。

3．众所周知，量子计算机相对经典计算机最主要的优点是量子计算机采用量子态编码信息，根据量子力学原理进行计算操作，可以实现大规模并行计算，大大降低问题的计算复杂度。采用簇态量子计算方案，具体问题的计算时间复杂度可以进一步降低。因为计算过程由对单个量子位测量完成，对那些测量基在算法中可以事前确定、或在计算进行到某一时间步，测量基可以确定的那些量子位，测量可以在同一时间步进行。这与量子计算的线路网络模型不同，在线路网络模型中，后一步逻辑操作必须在前一步完成后才能进行。所以簇态上的量子计算有进一步加速量子计算的作用。

4．超导簇态量子计算机，在一定程度上可以类比于经典电子计算机。代替经典电子计算机运算器的现在是“集成超导 Josephson 电路”，把这个电路制备在簇态上相当于“给经典运算器通以电流”。代替经典计算中的逻辑门操作，现在是对各个量子位按算法要求的测量。这种可类比性给超导簇态量子计算机结构设计带来清晰的、可循思路。

5．在簇态上量子计算模型中，编码态是量子的，但测量结果是经典的，计算过程需要处理前面测量得到的经典信息，然后用这些经典信息决定后续量子位的测量基，推动计算向前进行，经典信息流伴随着计算过程进行向前传输。因此，簇态上的量子计算需要经典信息处理，而这需要由经典计算机完成。

五、展望和总结

量子计算需要伴随着经典信息处理，可能不是簇态上量子计算独有的。我们可以大胆地预测，未来的计算机不可能是纯量子的。这是因为（1）我们总是和经典信息打交道，输入计算机的信息必定是经典的，我们需要的计算结果也必定是经典信息。而量子态制备、测量这样的经典信息和量子信息的变换，不可能由完全的量子系统实现。量子计算机很可能仅它的某些存储器、运算器是量子的，它的控制仍然是电路的；（2）迄今人们发现的量子算法仍然是为数不多，这很可能表明仅对少数特殊类型的问题（如分解大数至因子、随机数据库搜索等），量子计算才具有超出经典计算的能力，才需要用量子计算，而对于大量的实际问题量子计算并不具有加速计算的作用。（3）因此我们可以设想，新的计算机应当有智能的控制部分，把一个计算任务分解成适合量子计算的部分交量子处理器执行，而

把那些适合经典计算的交给电子计算机处理器执行，通过各部分协调工作执行计算任务。采用超导簇态量子计算，可能是实现这种复合型计算机的最值得研究的途径。

概括起来，超导簇态量子计算机，相对现在提出的其他量子计算实现方案就具有明显特色和一系列的优越性：(1) 超导量子计算机运算器操作、控制和测量，可以通过逻辑电子线路进行，计算过程可以实现高速度、自动进行；(2) 由于超导量子计算机量子态制备、操作和测量全都可以通过电路实现，这种计算机硬件可以借助于成熟的微电子学技术制造，非常方便优化、集成化、规模化。(3) 采用簇态量子计算模型，全部计算操作都可由单量子位测量实现，简化计算操作的实现，利用簇态性质，最大限度实现物理资源的节约，采取“边消费，变产生”策略，可以有效地战胜和环境相互作用引起的消相干；(4) 簇态量子计算方案可以进一步降低算法的时间复杂度，进一步加速量子计算。(5) 这种超导全电路簇态量子计算机非常适合于和现在的电子计算机结合，做成量子－经典复合计算机。这很可能是量子计算机发展的方向。

参考文献

[1] B.Ruggiero,etal.,Quantum Computing in Solid State Systems,Springer,(2006)

[2] Y.Makhlin ,etal.,Quantun－state engineering with Josephson－junction devices, R.M.P.,Vol.73,357,(2001);

[3] G.Wendin, etal.,Quntum bits with Josephson－junction (Review Article),Low.Temp.Phys.,33(9)724,(2007);

[4] R.Raussendorf,etal.,A one－way Quantum Computer, PRL.Vol.86(22),5188, (2001)

[5] R.Raussendorf, etal., Measurement－based quautum computation on cluster states, PRA.,68, 022312, (2003)

[6] Y.Nakamura, etal., Coherent control of macroscopic quantum states in a single－cooper－pair box, Nature,398,786,(1999)

[7] T.Duty.Etal.,Coherent dynamics of a charge qubit,PRB.,69,1405023(R), (2004)

[8] J.E.Mooij, etal.,Josephson persistent current qubit, Science,285,1036,(1999)

[9] T.P.Orlando,etal., Superconducting persisent－curent qubit,PRB.60(22),15398, (1999)

[10] Voss,R.F.,etal., Macroscopic quantum tunneling in 1μm Nb Josephson junction, PRL.47,265 ,(1981)

[11] Martinis,J.M.,etal.,Experimental tests for the quantum behavior of macroscopic degree of freedom:the phase difference across a Josephson junction, PRB,35,4682, (1987)

[12] J.Clarke, etal.,Quantum mechanics of a macroscopic variable:the phase difference of a Josephson junction, Science 239,992, (1988)

[13] Rouse,R.,S.etal.,Observation of resonant tunneling between macroscopic distinct quantum levels, PRL.75.1614,(1995)

[14] Nakamura,Y., etal.Spectroscopy of energy splitting between two macroscopic quantum states of charge coherently superposed by Josephson coupling, PRL., 79,2328, (1997)

[15] J.R.Fridman,etal.,Detection of a Schrodinger's cat in an rf－SQUID, Nature, 406,43,(2000)

[16] C.H.ver der Wal ,etal., Quantum superposition of macroscopic persistent stataes,Science 290,773,(2000)

[17] Yu.A.Pashkin, etal.,Quantum oscillations in two coupled charge qubits, Nature 421,823,(2003)

[18] J.Claudon, etal.,Coherent oscillations in a superconducting multilevel quantum system, PRL.,93,187003,(2004)

[19] E.Il'ichev,etal.,Continuous monitoring of Rabi oscillations in a Josephson flux qubitt,PRL.,91,097906,(2003)

[20] I.Chiorescu,Coherent quantum dynamics of a superconducting flux qubit,Science 299, 1869,(2003)

[21] T.Yamamoto, etal.,Demonstration of conditional gate operation using superconducting charge qubits, Nature 425,941,(2003)

[22] A.Izmalkov, etal.,Experimental evidence for entangled states in a system of two coupled flux qubits, PRL.,93,037003 ,(2004);PRL., 93,049902(E),(2004)

[23] J.B.Majet,etal.,Spectrospic on two coupled flux qubits, PRL.,94.090501, (2005)

[24] A.J.Bekley,etal.,Entangled macroscopic quantum states in two supercon－ ducting qubits,Science 368,284,(2003)

[25] A.Lupascu, etal.,Nondestructive readout for a superconducting flux qubite,PRL.,93,177006 (2004)

[26] O.Buisson,etal.,One－shot quantum measurement using a hystertic dc－SQUID,PRL.,90,238304,(2003)

[27] R.Mc.Dermott, etal.,Simultaneous state measurement of coupled Josephson phase qubits,Science ,307,1299,(2005)

[28] Â©2007 D－Wave Systems, Inc.

[29] T。 Tanamoto, Producting cluster in charge qubites and flux qubites, PRL., 97, 230501. (2006)
[30] J.Q. You, etal., Efficient one – step generation of large cluster states with solid – state circuits, PRA. 75, 052319, (2007)
[31] P. Walther, Experimental one – way quantum computing, Nature 434, 169, (2005)
[32] Nilson. M.A., et al., Phys. Rew. A., 71, 042323, (2005)

量子纠错码的构造

马　智　许亚杰　钟淑琴
信息工程大学信息工程学院，河南　郑州　450002

摘　要：本文介绍了量子纠错码的发展历史和研究现状，总结了量子 BCH 码的研究成果，给出了利用逻辑函数构造基态，从而得到量子纠错码的研究方法和成果。

关键词：量子计算　量子纠错码　量子 BCH 码　逻辑函数

一、引言

1994 年，Peter Shor[1] 等人提出了基于量子并行计算的量子计算机理论，给出了大整数因子分解的量子多项式时间算法。它给目前广泛使用的 RSA 公钥密码体制带来了巨大的威胁，显示出了量子计算这种新型计算模式强大的的优越性和重要的应用前景。自此，量子信息科学发展迅速，在量子计算、量子通信、量子密码、量子纠错等方面均取得重大突破。

研究已经发现，量子相干性在量子信息科学的各个领域都起着本质性的作用。量子计算机具有超出经典计算机的强大计算能力，就是利用了量子相干性。但是在实际应用中，量子计算机和环境之间存在着不可避免的相互作用，这种相互作用会造成量子计算机内量子态与环境态的纠缠，破坏计算机内量子态的相干叠加，这就是量子计算中要克服的一个重大障碍——量子消相干。而量子纠错码是克服量子消相干的重要手段。在量子通信中，在信息的传输和处理中不可避免的要出差错，而战胜出错的重要武器也是量子纠错码，它是保证量子传输中信息完整性、可靠性的重要方法。

在传统密码中，编码和密码总是密切相关的，对信息的编码本身就是一个加密的过程，在量子领域也是如此。事实上，量子纠错码可以应用于各种量子密码协议的设计和安全性证明，达到很好的效果，如用于设计量子消息认证方案、量子安全直接通信、量子秘密共享方案、量子公钥密码、量子数字签名和 BB84 量子密钥分配协议的安全性证明。由此可见量子纠错码与量子密码是密不可分的。

所以说，量子纠错在量子计算、量子通信和量子密码中均有着广泛而重要的作用。量子纠错码也成为量子信息科学中的热门研究领域。

量子纠错码是通过适当的方式引入冗余信息，防止和纠正量子错误，从而提高信息的抗干扰能力。不过，量子纠错码是在 Hilbert 空间实现的，而经典纠错码是在实空间实现的。量子情形下的纠错编码，并不是经典纠错码的简单推广，它有以下三个基本困难：量子态不可克隆原理限制态的复制、测量将扰动编码态、量子情形下错误类型更为复杂。由此可见，量子纠错码与经典纠错码有着本质机理的不同，对量子纠错码的研究必须要运用新的方法和手段。

1995，Peter Shor[2] 利用量子纠缠和部分编码等方法克服了上述困难，提出了最初的 9 量子比特编码 1 个量子比特，可以纠 1 个错的纠错码方案。自此，世界各国的学者纷纷投入到量子纠错码的研究中来，量子纠错码的研究发展迅速。

本文主要研究量子纠错码的构造，结构安排如下：第二部分介绍量子纠错码的发展历史和研究现状，第三部分总结我们关于量子 BCH 码的研究成果，第四部分给出我们由布尔函数构造基态，从而得到量子纠错码的研究成果。

二、量子纠错码的构造研究现状

一个参数为$((n,K,d))_q$的量子纠错码Q是Hilbert空间$\mathbf{C}^{q^n}$的一个K维子空间，并且可以纠正$t\leq\frac{d-1}{2}$个量子错误，且不扰动编码态。d称为Q的极小距离。若$K=q^k$，则量子纠错码Q将一个k—量子位的量子态编码为n—量子位，并记为$[[n,k,d]]_q$。在不加说明的情况下，$q=2$时下标省略。

由于篇幅有限，我们主要介绍量子稳定子码和由基态构造量子纠错码。有关量子非加性码、量子子系统码、纠缠辅助的量子纠错码读者可参考相关文献。

（一）量子稳定子码

量子稳定子码（又称加性码）是一类研究成果丰富的量子纠错码，每一个稳定子码对应于一个稳定子群，稳定子群中的任意一个元素保持任意一个编码态在忽略一个共同的全局相位下保持不动。到目前为止，量子稳定子码的研究已经形成了较为完备的体系，主要有以下突破和研究成果。

1996年，Calderbank等人[3]提出了量子CSS构造方法，使得由具有某种性质的经典纠错码来构造量子纠错码成为可能。从此，量子纠错码的发展进入了一个新阶段。1998年，Calderbank等人[4]系统地建立了量子纠错码的数学模型，并利用有限交换群的特征理论及有限域上的辛几何理论，给出了一种从$\mathbf{F}_2$或$\mathbf{F}_4$上的经典纠错码来构造量子纠错码的有效的数学方法，把量子纠错码的构造问题转化为寻找$\mathbf{F}_4$上在迹Hermitian内积意义下具有自正交性质的加法码的问题。

与此同时，非二元量子纠错码的研究也在进行。2000—2001年，Matsumoto等人[5]和Ashikhmin等人[6]较系统地建立了从$\mathbf{F}_{p^{2m}}$上的经典自正交码构造p^m-态量子码的方法。2006年，Bacon等人[7]给出了一类由两个经典码构造得来的量子子系统纠错码，这些码是Shor最初提出的量子纠错码的一种推广。同年，Hamada[8]给出了一种量子纠错码的多项式构造方法，此外还对扩大CSS码的极小距离的下界进行了改进。Ketkar等人[9]研究了有限域上稳定码的基理论，并以Galois理论为工具讨论了稳定码与一般的量子码之间的关系，给出了一些量子码的构造方法，并由此得到了一些量子码。

在上述研究基础上，各国学者利用经典纠错码的成就，主要是自正交码构造了参数好的量子纠错码，如量子RM码、BCH码、RS码、代数几何码和卷积码等。其中经由经典循环码，尤其是BCH码构造量子码是一类热点问题。Steane[10]给出了二元经典BCH包含其欧氏对偶的充分必要条件。马智等人[11]对非二元量子BCH码进行了研究，分别给出了狭义BCH码在欧氏内积和Hermitian内积意义下自正交的充分必要条件。Aly等人[12][13]进一步讨论了一些本原和狭义BCH码在这两种内积意义下具有自正交性质时，其设计距离需要满足的充分条件，并由此得到了一批量子BCH码。Guenda[14]给出了仿射不变的极大扩展循环码（affine-invariant maximal extended cyclic codes）的特征描述，在CSS构造下，根据这些码得到了一类纯量子码。特别的，对q模n的阶为偶数的情况，构造得到了退化的$[[n,1,\sqrt{n}]]_q$量子码。

（二）由基态构造量子纠错码

通过构造一组基态进而构造量子码是量子纠错码的另外一种思路。Danielsen[15]从布尔函数出发，构造得到与布尔函数相对应的量子态张成的一维量子码。Yu[16]等人在一个图论量子态的基础上，通过构造一组基态的方式构造维数大于1的量子纠错码，其中每一个基态都对应着图顶点集的一个子集。冯克勤等人[17]给出了量子纠错码的一种特征描述，从而得到一个根据具有某种性质的布尔函数构造p-态量子码的方法。接着，又把原有对p-态量子码的特征描述扩展到q-态，并由此把原来非线性代数几何码的渐进界转化为量子码的渐进界。基于布尔函数和投影算子的对应，Aggarwal等人[18]

给出了一个构造二元量子纠错码的一般的数学框架，以投影算子为出发点，在算子逻辑的帮助下构造了一批具有更优参数的二元量子纠错码。

此外，研究者们还探索量子纠错码的其它构造方法，从熟悉的对象出发，以不同的角度构造量子码。Schlingemann 等人[19]提出了通过构造某些具有特殊性质的图（或矩阵）来构造量子码的方法，给出了一个图论量子码$[[n,k,d]]_p$（p 为素数）存在的充分必要条件，得到了一些新的量子码（称为图论码）。马智等人[11]从图论量子码存在性的数学证明出发，得到了 p - 态图论量子码的一些推广结果。此外，还将 p - 态图论量子码的存在性和推广结果扩展到了二元和 q - 态（q 为素数的方幂）情形，从而也可得到一批二元和 q - 态量子纠错码。刘太琳等人[20]利用 Schlingemann 等人提出的构造量子纠错码的图论方法，给出了非二元量子循环码的方法，对于任意的奇素数 p，构造得到$[[8,2,4]]_p$ 和$[[n,n-2,2]]_p$。图论量子纠错码的构造方法本质上也可以视为由基态构造量子纠错码。

三、量子 BCH 码

定义 3.1 一个在有限域 $\mathbf{F}_q$ 上长为 n 的循环码$C(gcd(n,q)=1)$被称为一个设计距离为 δ 的 BCH 码，如果它的生成多项式是 α^l，α^{l+1}，…，$\alpha^{l+\delta-2}$的极小多项式。其中 α 是 $\mathbf{F}_{q^m}$ 中的一个 n 次本原单位根，m 是 q 模 n 的阶(通常记为 $m=ord_q(n)$)。若 $l=1$，则这个码被称为狭义的 BCH 码。若 $n=q^m-1$，则这个码被称为本原的 BCH 码。

在后面的叙述中，我们把有限域 $\mathbf{F}_q$ 上码长为 n，且$m=ord_n(q)$，设计距离为 δ，生成多项式是 α^l，α^{l+1}，…，$\alpha^{l+\delta-2}$的极小多项式的 BCH 码，称为参数为 l，n，q，δ 的 BCH 码。

量子 CSS（Calderbank - Shor - Steane）码是稳定子码的一种，它可以由经典纠错码构造得来，在经典纠错码和量子纠错码之间建立了一座桥梁，因而在量子纠错码中处于重要地位。

引理 3.2[3][10]（CSS 构造） 设存在经典二元线性码 $C_1=[n,k_1,d_1]$，$C_2=[n,k_2,d_2]$，且 $C_1^{\perp}\subseteq C_2$（于是 $n\le k_1+k_2$）。那么，存在量子码 $Q=[[n,k_1+k_2-n,d=min\{d_1,d_2\}]]$，且 Q 的一组基态为

$$\{|C_w\rangle=\frac{1}{2^{(n-k_1)/2}}\sum_{v\in C_1^{\perp}}|w+v\rangle\ \ w\in C_2/C_1^{\perp}\}$$

我们研究了非二元量子 BCH 码的构造，首先给出了狭义 BCH 码在欧氏内积和 Hermite 内积意义下具有自正交性质的充分必要条件，结果如下：

定理 3.3[11] 设 $m=ord_q(n)$，q 是一个奇素数的方幂，n 是一个正整数，C 是有限域 $\mathbf{F}_q$ 上码长为 n，设计距离为 δ 的狭义 BCH 码，则 $C^{\perp}\subseteq C$ 当且仅当 $\delta\le\Delta$，其中 $\Delta=\min\{1\le i\le n-1|[i]_n\ge[n-i]_n\}$（$[i]_n$ 表示 i 所在的模 n 的分圆陪集首项），$C^{\perp}$ 为 C 的对偶码。

定理 3.4[11] 设 $m=ord_q(n)$，q 是一个奇素数的方幂，n 是一个正整数，C 是一个有限域 $\mathbf{F}_{q^2}$ 上码长为 n，设计距离为 δ 的狭义 BCH 码，则 $C^{\perp_h}\subseteq C$ 当且仅当 $\delta\le\Delta'$，其中 $\Delta'=\min\{1\le i\le n-1|[i]_n\ge[n-qi]_n\}$，$C^{\perp_h}=\{y\in\mathbf{F}_q^n|y^q\cdot x=0$ 对任意的 $x\in C\}$（称为 C 的 Hermitian 对偶码）。

在此基础上，我们对 $n=q^m-1$ 和 $n=\frac{q^m-1}{q-1}$ 的情况确定了 Δ，由此得到一批经典的自正交狭义 BCH 码，从而由 CSS 构造方法获得一系列量子 BCH 码[11]。

进一步，我们利用算法的思想对狭义量子 BCH 码的构造进行了推广，讨论了一般意义下（非狭义、非本原）的经典 BCH 码在欧氏内积和 Hermitian 内积意义下具有自正交性质时其设计距离需要满足的充分必要条件，从而能够根据 CSS 方法来构造量子 BCH 码[21]。

我们给出了一个狭义 BCH 码不包含它的欧氏对偶时其设计距离的一个上界，这个上界是优于已

知上界$\lfloor qn^{1/2} \rfloor$的。并且给出了一个一般的 BCH 码不包含它的 Hermitian 对偶的充分必要条件。结果如下：

定理 3.5[21] 若一个狭义的 BCH 码不包含它的欧氏对偶，则其设计距离的一个上界为满足

$$a \geq b = \left[n_{i+j+1} + n_{i+j+2}q + \cdots + n_{i+k}q^{k-j-1} \right]_n$$

的最小的正整数 a。这里 $m = k+1$，n 的 $q-$adic 展开为 $n = n_0 + n_1 q + \cdots + n_k q^k$，$a = n_i + n_{i+1} q + \cdots + n_{i+j} q^j$，$j$ 是一个$[0, \left\lceil \frac{k}{2} \right\rceil]$中的正整数，脚标都在模 m 的意义下。

定理 3.6[21] 一个参数为 l，n，q^2，δ 的 BCH 码不包含它的 Hermitian 对偶的充分必要条件为在区间$[1, m]$中存在一个整数 k，使得在区间$[l + (l+\delta-2)q^{2k-1}, (l+\delta-2)(q^{2k+1}+1)]$中存在一个 n 的倍数。

我们共设计了 5 个算法，分别描述如下[21]：

算法 1：计算狭义 BCH 码在欧氏内积意义下自正交时，其设计距离的上界。

算法 2：计算一般的 BCH 码在欧氏内积意义下自正交时，其设计距离的上界。

算法 3：计算任意 BCH 码的维数。利用量子 CSS 构造和算法 3 的结果可以确定得到的量子 BCH 码的维数。

算法 4：计算狭义 BCH 码下在 Hermitian 内积意义下自正交时，其设计距离的上界。自正交当且仅当满足这个上界。

算法 5：计算一般的 BCH 码在 Hermitian 内积意义下自正交时，其设计距离的上界。自正交当且仅当满足这些上界。

四、由逻辑函数构造量子纠错码

我们首先由逻辑函数构造量子态。

一个 $\mathbf{F}_p$ 上含 n 个变元的逻辑函数对应一个向量$s = p^{-\frac{n}{2}} \zeta^{f(x)}$(其中 ζ 是 p 次本原单位根)，这个向量可以看作是一个量子态的概率分布向量，这个量子态表示为

$$|\psi_f\rangle = p^{-\frac{n}{2}} \sum_{x \in \mathbf{F}_p^n} \zeta^{f(x)} |x\rangle,$$

我们称$|\Psi_f\rangle$是与逻辑函数 $f(x)$相对应的逻辑态。特别的，$p=2$ 时，若一个量子态具有形式$|\Psi_f\rangle = 2^{-\frac{n}{2}} \sum_{x \in \mathbf{F}_2^n} (-1)^{f(x)} |x\rangle$，我们称它是一个与布尔函数 $f(x)$相对应的布尔态。

定义 K 个逻辑函数$g_i(x) = f(x) + \beta_i \cdot x$，并且对 $1 \leq i < j \leq K$，$\beta_i \neq \beta_j$。进一步定义 K 个量子态为

$$|\psi_i\rangle = p^{-\frac{n}{2}} \sum_{x \in \mathbf{F}_p^n} \zeta^{g_i(x)} |x\rangle$$

易知这个量子态是两两正交的。

在给出我们的结论之前，我们先把布尔函数 APC（aperiodic propagation criterion）距离的定义推广到任意素域上的逻辑函数。

定义 4.1 设$f(x)$是一个 n 元逻辑函数，则定义 $f(x)$的 APC 距离为最小的 $W_s(a,b)$，且 a, b 满