Subsystem Codes

Pradeep Sarvepalli, Andreas Klappenecker

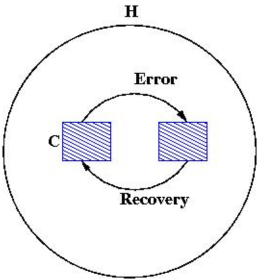
Department of Computer Science
Texas A&M University

Quantum Computing Seminar, 6th November 2006

Stabilizer Codes

Quantum code is a subspace in a finite dimensional Hilbert space

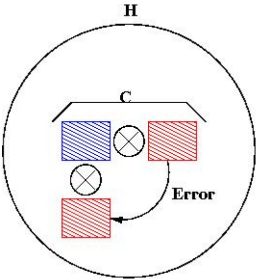
$$\mathcal{H} = C \oplus C^{\perp} \text{ where } \mathcal{H} = \underbrace{\mathbb{C}^q \otimes \mathbb{C}^q \otimes \cdots \otimes \mathbb{C}^q}_{n}$$



One main critique of quantum codes has been the need for active error-correction

Passive Error-Correction

In passive error-correction the recovery operation is trivial

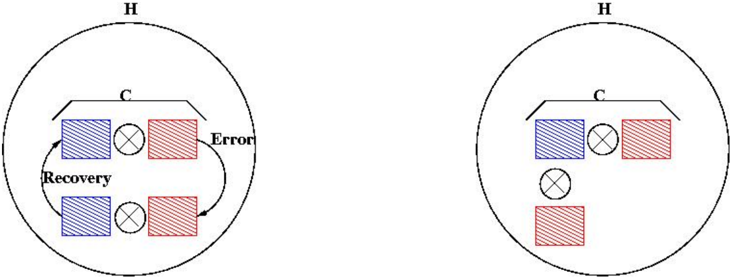


Unfortunately, noiseless subsystems (NS) have poor distance for the depolarizing channel

If the size of the redundant system is 1, then the code is called a decoherence free subspace (DFS)

Subsystem Codes

Operator codes or subsysytem codes are a generalization of the previous ideas



We do not care what is the state of subsystem B after recovery

The Big Picture

All these different methods can be unified using the idea of subsystem codes

- The code space can be resolved as a tensor product of two subsystems

$$\mathcal{H} = C \oplus C^{\perp} = (A \otimes B) \oplus C^{\perp}$$

- Information is stored in system A only, the subsystem B is often called the gauge subsystem
- There may not be a one to one correspondence between the physical qubits and the systems A and B, i.e., the virtual qubits

Operator Quantum Codes

Operator codes unify all the different types of quantum codes

We denote an operator code as $[[n, k, r, d]]_q$, where $\dim A = k$, $\dim B = r$ and distance of code is d

Code	Error-Correction	dim A	dim B
Operator	Active & Passive	k	r
Stabilizer	Active & Passive	k	0
NS	Passive	k	r
DFS	Passive	k	0

If we use the depolarizing channel model, then it means that NS and DFS cannot correct all errors.

Why Subsystem Codes?

Claims

- Lead to better error recovery schemes
- Possibility of codes that outperform the optimal stabilizer codes

Are these claims true?

For a large class of codes - No.

But the following claims could be

- Codes that beat the quantum Hamming bound may exist
- Conjectured that some codes maybe self-correcting
- Greater flexibility for fault-tolerant operations

Why Subsystem Codes?

Claims

- Lead to better error recovery schemes
- Possibility of codes that outperform the optimal stabilizer codes

Are these claims true?

For a large class of codes - No.

But the following claims could be

- Codes that beat the quantum Hamming bound may exist
- Conjectured that some codes maybe self-correcting
- Greater flexibility for fault-tolerant operations

Previous Work vs New Results

- No systematic methods to construct operator codes
- No bounds on the size of the gauge qubits
- Comparison of stabilizer and subsystem codes was not fair
- Many claims without any proofs

Operator Codes - A Closer Look

Error model: Assuming independent errors, the error group

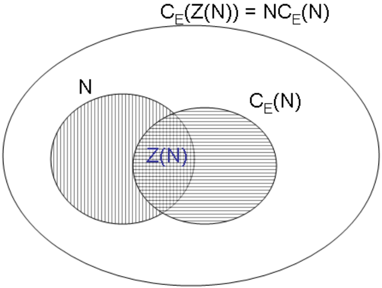
$$E = \{E_1 \otimes E_2 \otimes \cdots \otimes E_n \mid E_i \in \mathcal{P}\} \text{ where } \mathcal{P} = \langle i, I, X, Y, Z \rangle$$

Let N be normal subgroup of E and $Z(N)$, the center of N and $C_E(Z(N))$, the centralizer of $Z(N)$

Every nontrivial normal subgroup N defines a subsystem code C, which is precisely the stabilizer code defined by $Z(N)$.

The code $C = A \otimes B$, where B is the smallest subspace of $\mathcal{H}$ that is invariant under the action of N and A is the smallest subspace invariant under the action of $C_E(N)$

A Closer Look – cont'd

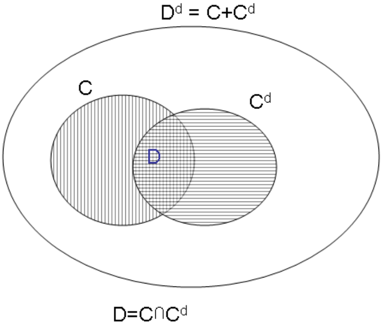


- Undetectable errors in $C_E(Z(N)) - N$
- Errors in N require no active error-correction
- Errors in $E - C_E(Z(N))$ require active error-correction

Let $q^r = \sqrt{\frac{|N|}{|Z(N)|}}$, $q^k = \sqrt{\frac{|C_E(Z(N))|}{|N|}}$ and $d = \text{wt}(C_E(Z(N)) - N)$, then N defines an $[[n, k, r, d]]_q$ code

Constructing Subsystem Codes

Like stabilizer codes we can construct subsystem codes from classical codes over $\mathbb{F}_q^{2n}$



- Undetectable errors in $D^{\perp_s} - C$
- Errors in C require no active error-correction
- Errors in $\mathbb{F}_q^{2n} - D^{\perp_s}$ require active error-correction

Let $q^r = \sqrt{\frac{|D^{\perp_s}|}{|C|}}$, $q^k = \sqrt{\frac{|C|}{|D|}}$ and $d = \mathrm{wt}(D^{\perp_s} - C)$, then C defines an $[[n, k, r, d]]_q$ code

Comparing Stabilizer Codes and Subsystem Codes

Criterion	Operator $[[n, k, r, d]]_q$	Stabilizer $[[n, k, d]]_q$
Error Recovery	n-k-r	n-k
Distance		Better?
Encoding	Same?	Same?
Fault Tolerance	Better?	

The main advantage is with respect to the number of syndrome measurements to be performed

- An $[[n, k, d]]_q$ stabilizer code requires $n - k$ syndrome measurements
- An $[[n, k, r, d]]_q$ subsystem code requires only $n - k - r$ syndrome qubits

An Obvious Question

Can we just throw away the gauge qubits?

No. There is no one to one correspodence between the physical qubits and the gauge qubits

Theorem (Gilbert-Varshamov Bound)

Let $\mathbb{F}_q$ be a finite field of characteristic p. If $0 < k + r \leq n$ and $d > 0$ such that

$$\sum_{j=1}^{d-1} \binom{n}{j} (q^2-1)^j (q^{n+k+r} - q^{n+r-k}) < (p-1)(q^{2n}-1)$$

holds, then an $[[n, k, r, \geq d]]_q$ operator quantum error-correcting code exists.

An Obvious Question - cont'd

Theorem

If $0 < k + r \leq q^n$ *and* $d > 0$ *such that*

$$\sum_{j=1}^{d-1} \binom{n}{j} (q^2 - 1)^j (q^{n+k+r} - q^{n-k+r}) < (p-1)(q^{2n} - 1)$$

holds, then an $[[n-r, k, \geq d]]_q$ *operator quantum error-correcting code exists.*

Our intuition does hold in most cases; we can just throw away the gauge qubits – But . . .

Upper Bounds on Subsystem Codes

Since the gains from subsystem codes are dependent on r, an upper bound on r will be useful

For linear $[[n, k, r, d]]_q$ subsystem codes, $k + r \leq n - 2d + 2$, for stabilizer codes $k \leq n - 2d + 2$

Indicates that there is a trade off between k and r

The bound suggests that reduction in syndrome measurements can be attained only by reducing the information stored

Better than MDS Stabilizer Codes

Quantum MDS codes

A stabilizer code with parameters $[[n, k, d]]$, where $2d = n - k + 2$, i.e., $[[k + 2d - 2, k, d]]_q$

Theorem

If a QMDS code $[[n, k, d]]_q$ exists, no linear operator code can have fewer syndrome measurements than $n - k$

Proof: Assume that that $[[n, k, r, d]]_q$ is better than an $[[k + 2d - 2, k, d]]_q$ code

$$\begin{aligned} k + 2d - 2 - k &> n - k - r \\ k + 2d - 2 &> n - r \\ k + r &> n - 2d + 2, \text{ contradiction for linear codes} \end{aligned}$$

Summary

- Systematic methods for construction of operator codes
- Upper bounds for pure or linear operator codes
- Lower bounds for additive operator codes
- Proved that linear operator codes cannot beat quantum MDS codes when they exist

Open Questions

- Does the Singleton bound hold for additive codes also?
- Are there subsystem codes that beat the quantum Hamming bound?
- Are there operator codes that beat the non MDS optimal stabilizer codes?
- Is a higher threshold possible for operator codes?

Questions? Thank You!

Questions? Thank You!