QUANTUM CODES OVER BINARY AND NONBINARY FIELDS

Zlatko Varbanov

University of Veliko Tarnovo

Mathematical Software and Combinatorial Algorithms
07 - 08.12.2020

Supported by Bulgarian Science Fund under Contract DN-02-2/13.12.2016

December 8, 2020

Overview

Introduction

- 1980s – the idea of using quantum mechanical effects to perform computations was first introduced by Feynman in the 1980s, when he discovered that classical computers could not simulate all aspects of quantum physics efficiently.
- 1985 – Deutsch showed that it is possible to implement any function which is computable by a classical computer using registers of entangled qubits and arrays of quantum gates, each performing a unitary quantum transformation.
- 1990 – P.Shor proved that there exists a randomized algorithm for integer factorization which runs in polynomial time on a quantum computer.

The relationship between quantum information and classical information is a subject currently receiving much study.

Quantum Computing

- In a classical computer, each bit of information is stored by a transistor containing trillions of electrons $\Leftrightarrow$ on a quantum computer, a single electron or nucleus in a magnetic field carries a bit of information (but interaction with the environment is much more serious).
- There could exist quantum-error-correcting codes (QECCs) which would protect quantum information as classical error-correcting codes protect classical information (Shor, 1995).
- The self-orthogonal codes over $\mathbb{F}_q$ are useful in order to construct QECCs (Calderbank et al., 1998; Ketkar et al., 2006).

MAIN PROBLEM:

To search for self-orthogonal codes over $\mathbb{F}_q$ with good parameters in order to improve some bounds for *QECC*.

Quantum Information

$V = \otimes^n(\mathbb{C}^q) = \mathbb{C}^q \otimes \mathbb{C}^q \otimes \cdots \otimes \mathbb{C}^q$, $dim V = q^n$.

The tensor factors $\mathbb{C}^q$ are often called *qubits* if $q = 2$ and *qudits* if $q > 2$.

A qubit has two possible states, labelled $|0\rangle$ and $|1\rangle$.

$|0\rangle = \binom{1}{0}$, $|1\rangle = \binom{0}{1}$, $\alpha|0\rangle + \beta|1\rangle = \binom{\alpha}{\beta}$

Unlike a classical bit, a qubit can be in a superposition of $|0\rangle$ and $|1\rangle$. The state of a general qubit can be denoted $\alpha|0\rangle + \beta|1\rangle$ $(\alpha, \beta \in \mathbb{C})$, with $|\alpha|^2 + |\beta|^2 = 1$.

Several qubits form *quantum register*. The state of a two-qubit register can be denoted $\alpha|00\rangle + \beta|01\rangle + \gamma|10\rangle + \delta|11\rangle$.

Quantum codes

The space of errors to a single qubit is spanned by the four unitary matrices (Pauli operators):

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, Y = iXZ$$

Any error on a single qubit, $|\phi\rangle \rightarrow E|\phi\rangle$, may be expressed as a linear combination of the Pauli matrices.

$$|\phi\rangle \rightarrow (aI + bX + cZ + dY)|\phi\rangle = a|\phi\rangle + bX|\phi\rangle + cZ|\phi\rangle + dY|\phi\rangle$$

Nonbinary case

A *qudit* is a generalization of the qubit to a q-dimensional Hilbert space $\mathbb{C}^q$. For example, a qutrit ($q = 3$) is a three-state quantum system. The computation basis is then a set of three (orthogonal) states $\{|0\rangle, |1\rangle, |2\rangle\}$ and an arbitrary qutrit is a linear combination of these three states $|\phi\rangle = \alpha|0\rangle + \beta|1\rangle + \gamma|2\rangle$.
The Pauli operators for a q-dimensional Hilbert space are defined by their action on the computational basis (Holsten et al., 2005): $X^{(q)}|j\rangle = |j+1\rangle$ and $Z^{(q)}|j\rangle = \omega^j|j\rangle$ where $j \in \mathbb{F}_q$ and ω is a primitive q-th root of unity. The matrix representations of X and Z for the qutrit are

$$X = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}, \quad Z = \begin{pmatrix} 1 & 0 & 0 \\ 0 & e^{2\pi i/3} & 0 \\ 0 & 0 & e^{4\pi i/3} \end{pmatrix}$$

Quantum codes

A quantum $[[n, k, d]]_q$ code is a q^k dimensional subspace of V with minimum distance d.
It is a unitary mapping (encoding) of k qudits into a subspace of the quantum state space of n qudits such that if any t (where $2t + 1 \leq d$) of the qudits undergo arbitrary decoherence, the resulting n qudits can be used to reconstruct the original quantum state of the k encoded qudits.

Linear codes

- $\mathbb{F}_q$ – a field with q elements.
- **Linear $[n,k]_q$ code C of length n** – k-dimensional linear subspace of $\mathbb{F}_q^n$.
- **Weight** of a codeword $c \in C$ $(wt(c))$ – the number of nonzero components of c.
- **Hamming distance** $H(x,y)$ between two codewords x and y – the number of coordinates in which x and y differ.
- **Minimum weight (distance)**:
- $d = d(C) = min\{wt(c)|c \in C, c \neq 0\} \rightarrow [n,k,d]_q$ code.
- **Generator matrix of** C – $k \times n$ matrix with entries in $\mathbb{F}_q$ whose rows are a basis of C.

Linear codes

Euclidean inner product

Euclidean inner product of two vectors
$x = (x_1, x_2, \ldots, x_n)$, $y = (y_1, y_2, \ldots, y_n)$ in $\mathbb{F}_q^n$ is

$$x.y = \sum_{i=1}^{n} x_i.y_i \tag{1}$$

Self-orthogonal and self-dual codes

- **Dual code** – $C^{\perp} = \{x \in \mathbb{F}_q^n \mid x.c = 0,\ \forall c \in C\}$
- C – **self-orthogonal** code if $C \subseteq C^{\perp}$
- C – **self-dual** code if $C = C^{\perp}$ $(k = n/2)$

Self-orthogonal codes over $\mathbb{F}_q$ and Quantum codes

CSS construction

It is known that if C is a classical linear $[n, k, d]$ code over $\mathbb{F}_q$ containing its dual ($C^{\perp} \subseteq C$) then there exists a quantum error-correcting $[[n, 2k - n, d]]_q$ code.

Calderbank–Shor–Sloane, 1996, for $q = 2$
Ketkar–Klappenecker–Kumar–Sarvepali, 2006, for $q > 2$

Cyclic codes

Cyclic code – $[n, k]$ linear code C, any cyclic shift of a codeword is another codeword. That is, if $c = (c_0, c_1, \ldots., c_{n-1})$ is a codeword then $c' = (c_1, \ldots, c_{n-1}, c_0)$ is also a codeword.
In polynomial form: $c(x) = c_0 + c_1 x + \cdots + c_{n-1} x^{n-1}$.
There is nonzero generating polynomial $g(x)$ for a cyclic code and $g(x)$ is a divisor of $x^n - 1$. Every codeword polynomial $c(x)$ is divisible by $g(x)$, i.e. a multiple of $g(x)$.
If $g(x) = g_0 + g_1 x + \cdots + g_{n-k} x^{n-k}$ then the generator matrix G of a cyclic code C is

$$G = \begin{pmatrix} g_0 & g_1 & \ldots & g_{n-k} & 0 & \ldots & 0 & 0 \\ 0 & g_0 & g_1 & \ldots & g_{n-k} & 0 & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & & \\ 0 & \ldots & 0 & g_0 & g_1 & \ldots & g_{n-k} & 0 \\ 0 & 0 & \ldots & 0 & g_0 & g_1 & \ldots & g_{n-k} \end{pmatrix}$$

Quasi-cyclic codes

Quasi-cyclic (QC) codes are a generalization of cyclic codes whereby a cyclic shift of a codeword by p positions results in another codeword. The QC codes can be described by circulants.
Circulant matrix:

$$A = \begin{pmatrix} a_0 & a_1 & a_2 & \dots & a_{n-2} & a_{n-1} \\ a_{n-1} & a_0 & a_1 & a_2 & \dots & a_{n-2} \\ \dots & \dots & \dots & \dots & \dots & \dots \\ a_2 & \dots & a_{n-2} & a_{n-1} & a_0 & a_1 \\ a_1 & a_2 & \dots & a_{n-2} & a_{n-1} & a_0 \end{pmatrix}$$

The generator matrix of a QC code can be represented as

$$G = [A_1 \ A_2 \ \dots \ A_p]$$

Our construction

We use a generating polynomial $g(x)$ of degree k where $g(x)$ is not a divisor of $x^n - 1$. Then we take following generator matrix:

$$G = \begin{pmatrix} g_0 & g_1 & \dots & g_k & 0 & \dots & 0 & 0 \\ 0 & g_0 & g_1 & \dots & g_k & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & & \\ 0 & \dots & 0 & g_0 & g_1 & \dots & g_k & 0 \\ 0 & 0 & \dots & 0 & g_0 & g_1 & \dots & g_k \end{pmatrix}$$

Construction of codes

We concatenate $(n-k) \times n/m$ (where $n-k \leq n/m$) generator matrices G_1 (it has generating polynomial $g_1(x)$), G_2 ($g_2(x)$), $\ldots$, G_m ($g_m(x)$), where $g_2(x), \ldots, g_m(x)$ are multiples of $g_1(x)$.

Then, the generator matrix of the constructed code is $(n-k) \times n$ matrix $G = [G_1 \ G_2 \ \ldots G_m]$.

Practically, this construction can be useful for small values of m. We use it for $m = 2$ or 3.

References

Calderbank A.R., Rains E.M., Shor P.W., Sloane N.J.A. (1998)

Quantum error correction via codes over $GF(4)$.

IEEE Trans. Inform.Theory 44, 1369 – 1387.

Ketkar A., Klappenecker A., Kumar S., Sarvepali P.K., Nonbinary Stabilizer Codes over Finite Fields, *IEEE Trans. of Inf.Theory, vol. 52 (11)*, 2006, pp.4892–4914.

P.W. Shor (1995)

Scheme for reducing decoherence in quantum memory

Phys. Rev. A., 52

M.Grassl (2017)

Table of bounds on minimum distance for $[[n, k, d]]$ *QECC* (www.codetables.de)

Y.Edel (2017), Parameters of some good Quantum Twisted Codes,

https://www.mathi.uni-heidelberg.de/ yves/Matritzen/QTBCH/QTBCHIndex.html