Quantum Error Correction
– Discrete Math. Meets Physics

Markus Grassl

http://iaks-www.ira.uka.de/home/grassl
Quantum Information Processing

Main Idea

Computation based on the laws of quantum mechanics

Main Algorithms (so far)

- integer factorisation, discrete log over $\mathbb{F}_p^*$ [Shor]
  generalisation to other groups (Abelian Hidden Subgroup Problems (HSP))
  $\implies$ exponential speed-up

- quantum “searching” [Grover]
  more precise: find the solutions of $f(x) = 1$ for a (efficiently computable)
  function $f : M \rightarrow \{0, 1\} \implies$ quadratic speed-up

Main Problem

Quantum mechanical systems are easy to disturb.
Quantum Systems

Model

- system is modelled by a complex Hilbert space $\mathcal{H}$
  in our context: finite dimensional $\mathcal{H} \cong \mathbb{C}^d$
- composed systems are modelled by the tensor product of the component
  spaces $\mathcal{H} = \mathcal{H}_1 \otimes \mathcal{H}_2 \implies$ exponential growth of dimension

Pure Quantum State

- normalised vector in $\mathcal{H}$
- basis states: $|0\rangle, |1\rangle, \ldots, |d-1\rangle$ (“classical information”)
- superposition:

$$|\psi\rangle = \sum_{i=0}^{d-1} \alpha_i |i\rangle$$

where

$$\sum_{i=0}^{d-1} |\alpha_i|^2 = 1$$
Quantum Operations

Unitary Operations

- all unitary operations on $\mathcal{H}$ are valid
- local operations: tensor product of $U \in \mathcal{U}(d)$ with identity matrices for the other tensor components

Measurements

- $\textit{observable } A$: Hermitian matrix
- spectral decomposition of $A$ yields (real) eigenvalues $\lambda_i$ and orthogonal projections $P_i$ onto the corresponding eigenspaces
- $\textit{measurement result } \lambda_i$:
  - random value with probability $p_i := \langle \psi | P_i | \psi \rangle$
  - projection (and re-normalisation): $| \psi' \rangle = \frac{1}{\sqrt{p_i}} P_i | \psi \rangle$
Entanglement

- superposition of basis states need not be tensor products, e.g.,

\[ |\Phi^+\rangle := \frac{1}{\sqrt{2}} (|0\rangle_L \otimes |0\rangle_R + |1\rangle_L \otimes |1\rangle_R) \]

- measuring \( \sigma_z := \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \) with eigenstates \( |0\rangle \) and \( |1\rangle \)
  - measuring \( \sigma_z \otimes I \) yields with prob. 1/2 either
    \[ |0\rangle_L \otimes |0\rangle_R \quad \text{or} \quad |1\rangle_L \otimes |1\rangle_R \]
  - then measuring \( I \otimes \sigma_z \)
    * gives a deterministic results, if the outcome of the first measurement is known
    * is completely random (prob. 1/2), if the first outcome is not known
System & Environment

**Without Error Correction**

- No access
- Environment
- System $|\phi\rangle$
- Interaction
- Entanglement $\Rightarrow$ decoherence

**With Error Correction**

- No access
- Environment
- System $|\phi\rangle$
- Encoding
- Ancillae $|0\rangle$
- Syndrome ancillae $|0\rangle$
- Interaction
- Error correction
- Decoding
- $|\phi\rangle$ $|0\rangle$
"Closed" System

\[
\begin{align*}
\text{environment } & |\varepsilon\rangle \\
\text{system } & |\phi\rangle
\end{align*}
\raisebox{0.5cm}{interaction} \quad \left\{ \right. = U_{\text{env/sys}} \left( |\varepsilon\rangle |\phi\rangle \right)
\]

"Channel"

\[
\begin{align*}
Q: \rho_{\text{in}} := |\phi\rangle \langle \phi| \quad \longrightarrow \quad \rho_{\text{out}} := Q(|\phi\rangle \langle \phi|) := \sum_i E_i \rho_{\text{in}} E_i^\dagger
\end{align*}
\]

with error operators (Kraus operators) \( E_i \)

**Local/low correlated errors**

- product channel \( Q^\otimes n \) where \( Q \) is "close" to identity
- \( Q \) can be expressed (approximated) with error operators \( \tilde{E}_i \) such that each \( E_i \) acts on few subsystems
 QECCs for Local Error Models

Quantum Error-Correcting Code (QECC)

\[ \mathcal{C} \subseteq (\mathbb{C}^q)^{\otimes n} \text{ where } \dim \mathcal{C} = q^k \]

Notation \( \mathcal{C} = [n, k, d]_q \)

- \( n \): number of subsystems used in total
- \( k \): number of (logical) subsystems encoded
- \( d \): “minimum distance”
  - correct all errors acting on at most \((d-1)/2\) subsystems
  - detect all errors acting on less than \(d\) subsystems
Basic Ideas

Partitioning all (binary) words
- combinatorics
- (linear) algebra

orthogonal decomposition

\[ (\mathbb{C}^d)^{\otimes n} = \mathcal{H}_C \oplus \mathcal{H}_{\mathcal{E}_1} \oplus \ldots \oplus \mathcal{H}_{\mathcal{E}_1} \oplus \ldots \]

- \text{codewords}
- \text{bounded weight errors}
- \text{other errors}
Characterisation of QECCs

[E. Knill & R. Laflamme, PRA 55, 900–911 (1997)]

A subspace $\mathcal{C}$ of $\mathcal{H}$ with orthonormal basis $\{|c_1\rangle, \ldots, |c_K\rangle\}$ is an error-correcting code for the error operators $\mathcal{E} = \{E_1, \ldots, E_\mu\}$, if there exists constants $\alpha_{k,l} \in \mathbb{C}$ such that for all $|c_i\rangle$, $|c_j\rangle$ and for all $E_k, E_l \in \mathcal{E}$:

$$\langle c_i | E_k^\dagger E_l | c_j \rangle = \delta_{i,j} \alpha_{k,l}.$$  \hfill (1)

It is sufficient that (1) holds for a vector space basis of $\mathcal{E}$.

$\implies$ only a finite set of errors
Error Basis

Unitary Error Basis
set of $d^2$ unitary matrices that forms a vector space basis of all $d \times d$ matrices

Nice Unitary Error Basis
basis elements $U_g$ are labelled by group elements $g \in G$ with the property:

$$U_g U_h = \omega(g, h) U_{g^* h}$$

$\Rightarrow$ irreducible projective representations

[E. Knill, Group Representations, Error Bases and Quantum Codes, quant-ph/9608049 (1996)]

Heisenberg-Weyl Group

Shift & Phase Operators

for arbitrary dimension $d$ with basis $B := \{ |0\rangle, |1\rangle, \ldots, |d - 1\rangle \}$

- shift operator $X : |x\rangle \mapsto |(x + 1) \mod d\rangle$

- phase operator $Z : |x\rangle \mapsto \omega_d^{|x|} |x\rangle$ where $\omega_d := \exp(2\pi i / d)$

Heisenberg-Weyl Group:

$$G := \langle X, Z \rangle$$

order $|G| = d^3$

centre $\zeta(G) = \langle \omega_d I \rangle$

quotient $G / \zeta(G) \cong \mathbb{Z} / d\mathbb{Z} \times \mathbb{Z} / d\mathbb{Z}$
Qudits and Finite Fields

Qudits

- tensor product of quantum systems of dimension $d$, in particular $d = p^m$, $p$ prime
- single qudit
  \[
  |\psi\rangle = \sum_{i=0}^{d-1} \alpha_i |i\rangle \quad \text{where } \alpha_i \in \mathbb{C} \text{ and } \sum_{i=0}^{d-1} |\alpha_i|^2 = 1
  \]

  labels $i$ of the basis states from an arbitrary set $\mathcal{A}$ with $d$ elements, e.g.
  \[
  \mathcal{A} = \{0, 1, \ldots, d-1\} \text{ or } \mathcal{A} = \mathbb{F}_{p^m} \text{ for } d = p^m, p \text{ prime}
  \]

Finite Fields

- trace: $\text{tr}: \mathbb{F}_q \rightarrow \mathbb{F}_p$ where $\text{tr}(\alpha) := \sum_{i=0}^{m-1} \alpha p^i \in \mathbb{F}_p$
- in $\mathbb{F}_q$ there exists a primitive $(q - 1)\text{th root of unity}
Single Qudit Gates

- \( X_\alpha := \sum_{x \in \mathbb{F}_q} |x + \alpha \rangle \langle x| \quad \text{for } \alpha \in \mathbb{F}_q \)
  \[= X_{\alpha_1} \otimes X_{\alpha_2} \otimes \ldots \otimes X_{\alpha_m} \]

- \( Z_\beta := \sum_{z \in \mathbb{F}_q} \omega^{tr(\beta z)} |z \rangle \langle z| \quad \text{for } \beta \in \mathbb{F}_q \) (\( \omega := \omega_p = \exp(2\pi i/p) \))
  \[= Z_{\beta_1} \otimes Z_{\beta_2} \otimes \ldots \otimes Z_{\beta_m} \]

- \( M_\gamma := \sum_{y \in \mathbb{F}_q} |\gamma y \rangle \langle y| \quad \text{for } \gamma \in \mathbb{F}_q \setminus \{0\} \)

- \( \text{DFT} := \frac{1}{\sqrt{q}} \sum_{x,z \in \mathbb{F}_q} \omega^{tr(xz)} |z \rangle \langle x| \)

University of Sydney, 05.03.2004
Universal Gates

- \( \text{ADD}^{(1,2)} := \sum_{x,y \in \mathbb{F}_q} |x\rangle_1 |x + y\rangle_2 \langle y|_2 \langle x|_1 \)

- \( \text{HORNER}^{(1,2,3)} := \sum_{a,x,b \in \mathbb{F}_q} |a\rangle_1 |x\rangle_2 |ax + b\rangle_3 \langle b|_3 \langle x|_2 \langle a|_1 \)

\( \implies \) any (classical) reversible function

\[ f : \mathbb{F}_q^n \longrightarrow \mathbb{F}_q^n \]

can be implemented with the HORNER-gate (using ancillae)
(Non-binary) Quantum Codes (QECCs)

Error Basis for Qudits
[A. Ashikhmin & E. Knill, IEEE-IT 47, 3065–3072 (2001)]

\[ \mathcal{E} = \{ X_\alpha Z_\beta : \alpha, \beta \in \mathbb{F}_q \} . \]

commutator relations:

\[ X_\alpha Z_\beta = \omega^{-\text{tr}(\alpha \beta)} Z_\beta X_\alpha \]

and

\[ (X_\alpha Z_\beta)(X_{\alpha'} Z_{\beta'}) = \omega^{\text{tr}(\alpha' \beta - \alpha \beta')}(X_{\alpha'} Z_{\beta'})(X_\alpha Z_\beta) \]

Stabiliser Code

\( \mathcal{C} \) is an eigenspace of \( \mathcal{S} \) w.r.t. some irred. (projective) character \( \chi \)

where the stabiliser \( \mathcal{S} \) is an Abelian subgroup of \( \mathcal{E} \otimes n \)
**Stabiliser Codes**

**Representation Theory**

$C$ is an eigenspace of $S$ w.r.t. some irred. character $\chi_1$

decomp. into
irred. components

the orthogonal spaces are labelled by the character (values)
$\implies$ operations that change the character (value) can be detected
Stabiliser Codes (contd.)

Error Group
\[ G_1 := \langle X_\alpha, Z_\beta : \alpha, \beta \in \mathbb{F}_q \rangle, \quad |G_1| = pq^2, \quad \text{centre } \zeta(G_1) = \langle \omega I \rangle \]
unique representation of the elements of \( G_1 \):
\[ \omega^\gamma X_\alpha Z_\beta \quad \text{where } \gamma \in \mathbb{F}_p = \{0, \ldots, p - 1\} \text{ and } \alpha, \beta \in \mathbb{F}_q \]

\( n \) qudits:
\[ G_n := G^\otimes n, \quad |G_n| = pq^{2n}, \quad \text{centre } \zeta(G_n) = \langle \omega I \rangle \]
unique representation of the elements of \( G_n \):
\[ \omega^\gamma (X_{\alpha_1} Z_{\beta_1}) \otimes (X_{\alpha_2} Z_{\beta_2}) \otimes \ldots \otimes (X_{\alpha_n} Z_{\beta_n}) =: \omega^\gamma X_\alpha Z_\beta \]
where \( \gamma \in \mathbb{F}_p \) and \( \alpha, \beta \in \mathbb{F}_q^m \)

quotient group:
\[ \overline{G}_n := G_n / \langle \omega I \rangle \cong (\mathbb{F}_q \times \mathbb{F}_q)^n \cong \mathbb{F}_q^m \times \mathbb{F}_q^m \]
Stabiliser Codes (contd.)

Abelian Subgroups $S$ of $G_n$

Symplectic inner product on $\mathbb{F}_q^n \times \mathbb{F}_q^n$:

$$(\alpha, \beta) \ast (\alpha', \beta') := \sum_{i=1}^{n} \text{tr}(\alpha'_i \beta_i - \alpha_i \beta'_i)$$

$C \subseteq \mathbb{F}_q^n \times \mathbb{F}_q^n$ self-orthogonal

$$\iff C \subseteq C^* := \{d : d \in \mathbb{F}_q^n \times \mathbb{F}_q^n | \forall c \in C : d \ast c = 0\}$$

Commutator relations in $G_n$:

$$(X_{\alpha} Z_{\beta})(X_{\alpha'} Z_{\beta'}) = \omega^{(\alpha, \beta) \ast (\alpha', \beta')}(X_{\alpha'} Z_{\beta'})(X_{\alpha} Z_{\beta})$$

$S$ Abelian subgroup

$$\iff (\alpha, \beta) \ast (\alpha', \beta') = 0 \text{ for all } \omega^\gamma(X_{\alpha} Z_{\beta}), \omega^\gamma'(X_{\alpha'} Z_{\beta'}) \in S$$
Stabiliser Codes (contd.)

Classical Error-Correcting Codes

Abelian subgroups $S$ of $G_n$ correspond to additively closed self-orthogonal subsets $C$ of $\mathbb{F}_q^n \times \mathbb{F}_q^n$.

$\implies \mathbb{F}_p$-linear codes over $\mathbb{F}_q = \mathbb{F}_{p^m}$

Variations (stronger conditions)

- $\mathbb{F}_q$-linear codes over $\mathbb{F}_q \times \mathbb{F}_q \cong \mathbb{F}_q^2$

  inner product: $(\alpha, \beta) * (\alpha', \beta') := \sum_{i=1}^{n} \alpha_i \beta_i - \alpha_i \beta'_i$

- $\mathbb{F}_q^2$-linear codes over $\mathbb{F}_q^2$

  Hermitian inner product: $\nu' * \nu = \sum_{i=1}^{n} \nu_i \nu_i^q$
### Effect of Errors

<table>
<thead>
<tr>
<th>operation $E \in G_n$</th>
<th>vector $v$</th>
<th>effect</th>
</tr>
</thead>
<tbody>
<tr>
<td>operations in the stabiliser $S$</td>
<td>elements of $C$</td>
<td>no effect</td>
</tr>
<tr>
<td>operations in the normaliser $N$ of $S$ in $G_n$</td>
<td>proper cosets of $C$ in $C^*$</td>
<td>preserve the code space</td>
</tr>
<tr>
<td>operations that change the character $\chi_0$</td>
<td>proper cosets of $C^*$</td>
<td>leave the code space</td>
</tr>
</tbody>
</table>

### Minimum Distance

$$d_{\text{min}} := \min \{ \text{wgt}(c) : c \in C^* \setminus C \}$$
Results

- quantum error-correction is possible
- QECCs allow “encoded” operations
  \[\Rightarrow \text{fault tolerant quantum computation:}\]
  arbitrary long quantum computations can be stabilised with only poly. overhead if all components are not too bad
  \[p_{\text{error}} < 10^{-6} - 10^{-4}\]
- codes for \(q > 2\) have better parameters

Challenge:

Is there a QECC \(C = [7, 1, 4]_4\)?

partial result: There is no such code which is \(\mathbb{F}_{16}\)-linear.