Entanglement-Assisted Quantum LDPC Codes from Combinatorial Designs

Yuichiro Fujiwara and Vladimir D. Tonchev
Department of Mathematical Sciences
Michigan Technological University

Entanglement-assisted stabiliser formalism
Bravyi, Devetak, and Preskill (2006)

Our goal:
Quantum error correcting codes with
Good error-correcting performance,
Flexibility,
Low decoding complexity,
Systematic constructions.

Combinatorial design theory
- Pairwise balanced designs
- Finite geometry

Classical coding theory
- Low-density parity-check codes

References
- F, Tonchev, arXiv:1108.0679v2
Entanglement-Assisted Quantum LDPC Codes from Combinatorial Designs

Yuichiro Fujiwara and Vladimir D. Tonchev

Department of Mathematical Sciences
Michigan Technological University

**Entanglement-assisted stabiliser formalism**
Brun, Devetak, and Hsieh (2006)

Our goal:
Quantum error correcting codes with
Good error-correcting performance,
Flexibility,
Low decoding complexity,
Systematic constructions.

**Combinatorial design theory**
- Pairwise balanced designs
- Finite geometry

**Classical coding theory**
- Low-density parity-check codes
  (used for digital television, Wi-Fi 802.11n, etc.)
  Gallager (1960)
Entanglement-assisted stabiliser formalism
Brun, Devetak, and Hsieh (2006)

Our goal:
Quantum error correcting codes with
Good error-correcting performance, Flexibility,
Codes with performance,

Classical coding theory

- Low-density parity-check codes
  (used for digital television, Wi-Fi 802.11n, etc.)

Gallager (1960)
Combinatorial design theory

• Pairwise balanced designs
• Finite geometry
A pairwise balanced design, PBD(v, K, 1), is an ordered pair (V, B), where
- V: finite set (points),
- B: family of subsets of V (blocks),
- each unordered pair of distinct points is contained in exactly one block,
- the sizes of blocks consist of the elements of K.

A PBD is said to be odd-replicate if each point appears in an odd number of blocks.

*This kind of mathematical object has been studied since the 19th century (i.e., we've got a bunch of mathematical tools).*
Entanglement-assisted stabiliser formalism
Brun, Devetak, and Hsieh (2006)

Our goal:
Quantum error correcting codes with Good error-correcting performance,
Flexibility,
Low decoding complexity,
Systematic constructions.

Classical coding
- Low-density (used for digital television, Wi-Fi)
Classical coding theory

- Low-density parity-check codes
  (used for digital television, Wi-Fi 802.11n, etc.)

Gallager (1960)
Low-density parity-check (LDPC) codes

LDPC codes are simply linear codes which are decodable by certain sub-optimal decoders.

The point is that LDPC codes can
  • almost achieve the Shannon limit
  • be decoded fast (in linear time)

To obtain better performance, it is desirable for the Tanner graphs of LDPC codes to be of "girth" 6 (or larger).
Entanglement-Assisted Quantum LDPC Codes from Combinatorial Designs

Yuichiro Fujiwara and Vladimir D. Tonchev
Department of Mathematical Sciences
Michigan Technological University

**Entanglement-assisted stabiliser formalism**
Brun, Devetak, and Hsieh (2006)

Our goal:
Quantum error correcting codes with
Good error-correcting performance,
Flexibility,
Low decoding complexity,
Systematic constructions.

**Combinatorial design theory**
- Pairwise balanced designs
- Finite geometry

**Classical coding theory**
- Low-density parity-check codes
  (used for digital television, Wi-Fi 802.11n, etc.)
  Gallager (1960)
Our goal:
Quantum error correcting codes with good error-correcting performance, flexibility,

Entanglement-assisted stabiliser formalism
Brun, Devetak, and Hsieh (2006)
Stabilizer formalism

- requires a severe condition (symplectic orthogonality),
- can only employ a limited range of classical codes (e.g., self-containing codes).

Entanglement-assisted stabilizer formalism

- removes the orthogonality condition with the help of preshared entanglement,
- allows the code designer to employ ANY binary or quaternary linear code.
EA-LDPC codes are quantum analogues of LDPC codes, so they are defined by quantum versions of parity-check matrices.

Calderbank-Shor-Steane (CSS) construction
A quantum check matrix of a homogenous quantum LDPC code looks like
\[
\begin{bmatrix}
H & 0 \\
0 & H
\end{bmatrix}
\]
where \(H\) is a parity-check matrix of a binary linear code (which forms a regular LDPC code).

\(M - \text{ln}_2 \text{d} \text{ec} \Rightarrow (\text{ln}_2 \text{d} \text{ec} \cdot n \cdot c, d)\) EA-LDPC code, where \(c = \text{rank}(H^2)\)

c is the amount of pre-shared entanglement, i.e., the required number of ebits.

Desirable EA-LDPC codes
- have large girth,
- consume a small number of ebits.

We consider EA-LDPC codes consuming only one ebit with the largest possible girth.
A-LDPC codes are quantum analogues of classical LDPC codes, so they are defined by quantum versions of the Calderbank-Shor-Steane (CSS) construction.

A quantum check matrix (of a homogenous quantum LDPC code) looks like:

$$
\begin{bmatrix}
H & 0 \\
0 & H
\end{bmatrix}
$$

where $H$ is a parity-check matrix of a binary linear code (which forms a regular LDPC code).

$H : [n, k, d] \text{code} \Rightarrow [[n, 2k - n + c, d; c]]$ EA-LDPC code, where $c = \text{rank}(HH^T)$

c is the amount of preshared entanglement, i.e., the required number of ebits.
Desirable EA-LDPC codes

- have large girth,
- consume a small number of ebits.

We consider EA-LDPC codes consuming only...
EA-LDPC codes are quantum analogues of LDPC codes, so they are defined by quantum versions of parity-check matrices.

**Calderbank-Shor-Steane (CSS) construction**

A quantum check matrix of a homogeneous quantum LDPC code looks like:

\[
\begin{bmatrix}
H & 0 \\
0 & H
\end{bmatrix}
\]

where $H$ is a parity-check matrix of a binary linear code (which forms a regular LDPC code).

If $[n, k, d_{\text{code}} = [n, 2k - n; c, d)]$ EA-LDPC code, where $c = \text{rank}(HH^T)$

$c$ is the amount of preshared entanglement, i.e., the required number of ebits.

Desirable EA-LDPC codes
- have large girth,
- consume a small number of ebits.

We consider EA-LDPC codes consuming only one ebit with the largest possible girth.
Homogeneous EA-LDPC codes consuming only one ebit with girth 6 (which is the largest possible) are equivalent to odd-replicate PBDs. If the LDPC code used as an ingredient is regular, it's a Steiner 2-design. (i.e., $S(2, k, v)$ with $\frac{v-1}{k-1}$ odd)

It is an incidence matrix of a PBD with index $t$ and odd replication number.

Combinatorial design theory characterizes EA-LDPC codes

We can

- derive bounds on the minimum distance, dimensions, girth, etc.
- give necessary and sufficient conditions for the existence,
- explicit constructions,
- and more (e.g., EA-LDPC codes for channels with biased noise).

Theorem 2.4 A necessary condition for the existence of a regular entanglement-assisted quantum LDPC code which requires only one ebit and is of length $n$, girth 6, and column weight $w$ is that the number $\frac{n-1}{w-1}$ is an odd integer. Conversely, there exists a constant $n_0$ such that for every pair of positive integers $n \geq n_0$ and $w$, the necessary condition is sufficient.

Theorem 3.4 Let $n$ be an integer greater than some. Thus, there exists a regular entanglement-assisted quantum LDPC code of length $n$, dimension $k$, girth 6, and column weight $w$ which requires only one ebit if and only if $\sqrt{26n+1} \equiv 3 \pmod{6}$ and $n = \sqrt{26n+1} + 1 \leq k \leq n - \sqrt{26n+1} + 2$, where $k$ is the integer satisfying $\sqrt{26n+1} = 2^{k-1}(4^k-3)$ with odd.

Theorem 3.7 The number of $k$-cycles in the classical equivalent of a regular entanglement-assisted quantum code which requires only one ebit and is of length $n$, girth 6, and column weight $w$ is $n(n-w+1)^k(2^{w-1}-1)^n$.
(i.e., $S(2, k, \nu)$ with $\frac{\nu - 1}{k - 1}$ odd)
Homogeneous EA-LDPC codes consuming only one ebit with girth 6 (with odd-replicate PBDs. If the LDPC code used as an ingredient is regular, then...)

Combinatorial design theory characterizes EA-LDPC codes

We can
- derive bounds on the minimum distance, dimensions, girth, etc.
- give necessary and sufficient conditions for the existence,
- explicit constructions,
- and more (e.g., EA-LDPC codes for channels with biased noise).
which is the largest possible) are equivalent as a Steiner 2-design. \( \text{(i.e., } S(2, k, v) \text{ with } \frac{v-1}{k-1} \text{ odd)} \)

\( H \) is an incidence matrix of a PBD with index 1 and odd replication number.

**Theorem 2.4** A necessary condition for the existence of a regular entanglement-assisted quantum LDPC code which requires only one ebit and is of length \( n \), girth six, and column weight \( \mu \) is that the number \( \frac{-1 + \sqrt{1 + 4n\mu(\mu-1)}}{2(\mu-1)} \) is an odd integer. Conversely, there exists a constant \( n_{\mu} \) such that for every pair of positive integers \( n > n_{\mu} \) and \( \mu \) the necessary condition is sufficient.

**Theorem 3.4** Let \( n \) be an integer greater than seven. Then, there exists a regular entanglement-assisted quantum LDPC code of length \( n \), dimension \( k \), girth six, and column weight three which require only one ebit if and only if \( \sqrt{24n + 1} \equiv 5 \text{ (mod 8)} \) and \( n - \sqrt{24n + 1} \leq k \leq n - \sqrt{24n + 1} + 2t - 2 \), where \( t \) is the integer satisfying \( \sqrt{24n + 1} = 2^{t+1}u - 3 \) with \( u \) odd.

**Theorem 3.7** The number of 6-cycles in the classical ingredient of a regular entanglement-assisted quantum code which requires only one ebit and is of length \( n \), girth six, and column weight \( \mu \) is \( \frac{n\mu(\mu-1)(1-2\mu+\sqrt{1+4n\mu(\mu-1)})}{12} \).
H is an incidence matrix of a PBD with index 1 and odd replication number.

**Theorem 2.4** A necessary condition for the existence of a regular entanglement-assisted quantum LDPC code which requires only one ebit and is of length \( n \), girth six, and column weight \( \mu \) is that the number \( \frac{\sqrt{n+1} + \sqrt{1+4n\mu(\mu-1)}}{2(\mu-1)} \) is an odd integer. Conversely, there exists a constant \( n_\mu \) such that for every pair of positive integers \( n > n_\mu \) and \( \mu \) the necessary condition is sufficient.

**Theorem 3.4** Let \( n \) be an integer greater than seven. Then, there exists a regular entanglement-assisted quantum LDPC code of length \( n \), dimension \( k \), girth six, and column weight three which require only one ebit if and only if \( \sqrt{24n+1} \equiv 5 \pmod{8} \) and \( n - \sqrt{24n+1} \leq k \leq n - \sqrt{24n+1} + 2t - 2 \), where \( t \) is the integer satisfying \( \sqrt{24n+1} = 2^{t+1}u - 3 \) with \( u \) odd.

**Theorem 3.7** The number of 6-cycles in the classical ingredient of a regular entanglement-assisted quantum code which requires only one ebit and is of length \( n \), girth six, and column weight \( \mu \) is \( \frac{n\mu(\mu-1)(1-2\mu+\sqrt{1+4n\mu(\mu-1)})}{12} \).
Theorem 2.4  A necessary condition for the existence of a regular entanglement-assisted quantum LDPC code which requires only one ebit and is of length \( n \), girth six, and column weight \( \mu \) is that the number \( \frac{-1+\sqrt{1+4\mu(\mu-1)}}{2(\mu-1)} \) is an odd integer. Conversely, there exists a constant \( n_\mu \) such that for every pair of positive integers \( n > n_\mu \) and \( \mu \) the necessary condition is sufficient.

Theorem 3.4  Let \( n \) be an integer greater than seven. Then, there exists a regular entanglement-assisted quantum LDPC code of length \( n \), dimension \( k \), girth six, and column weight three which require only one ebit if and only if \( \sqrt{24n+1} \equiv 5 \pmod{8} \) and \( n - \sqrt{24n+1} \leq k \leq n - \sqrt{24n+1} + 2t - 2 \), where \( t \) is the integer satisfying \( \sqrt{24n+1} = 2^{t+1}u - 3 \) with \( u \) odd.

Theorem 3.7  The number of 6-cycles in the classical ingredient of a regular entanglement-assisted quantum code which requires only one ebit and is of length \( n \), girth six, and column weight \( \mu \) is \( \frac{n\mu(\mu-1)(1-2\mu+\sqrt{1+4n\mu(\mu-1)})}{12} \).
Crossover probability $f$ on the depolarizing channel

- $\text{PG}_1(2,8)$
- $\text{PG}_1(2,16)$
- $\text{PG}_1(2,32)$
- $\text{AG}_1(2,8)$
- $\text{AG}_1(2,16)$
- $\text{AG}_1(2,32)$
Homogeneous EA-LDPC codes consuming only one ebit are equivalent to odd-replicate PBDs.

- Can we characterize heterogeneous EA-LDPC codes?
- What if we allow multiple ebits?
Thank you!

Entanglement-Assisted Quantum LDPC Codes from Combinatorial Designs

Yuichiro Fujiwara and Vladimir D. Tonchev
Department of Mathematical Sciences
Michigan Technological University

Our goal:
Quantum error correcting codes with
Good error-correcting performance,
Flexibility,
Low decoding complexity,
Systematic constructions.

References
• F, Tonchev, arXiv:1108.0679v2