

Generalized bicycle codes with small connectivity and their properties

Reza Dastbasteh

Department of Basic Sciences, Tecnun - University of Navarra,
San Sebastian, Spain

Joint Work: Olatz Sanz Larrarte, Josu Etxezarreta Martinez, Arun
John Moncy, Pedro M Crespo, and Ruben M Otxoa

8th Workshop on Design Theory, Hadamard Matrices and Applications
(Hadamard 2025)
28 May 2025

Outline

- 1 Introduction and Motivation
- 2 Background
- 3 Generalized Bicycle Codes
- 4 Syndrome Extraction and Hook errors
- 5 Code Capacity Threshold

Introduction and Motivation

A **quantum error-correcting code** is a scheme that protects quantum information from corruption by noise (decoherence) on the quantum channel.

Introduction and Motivation

A **quantum error-correcting code** is a scheme that protects quantum information from corruption by noise (decoherence) on the quantum channel.

Currently, quantum architectures can implement only a limited set of quantum error-correcting codes due to constraints such as **limited qubit connectivity** and **restricted qubit interaction range**. This is a case for example, in superconducting qubits (IBM and Google).

Introduction and Motivation

A **quantum error-correcting code** is a scheme that protects quantum information from corruption by noise (decoherence) on the quantum channel.

Currently, quantum architectures can implement only a limited set of quantum error-correcting codes due to constraints such as **limited qubit connectivity** and **restricted qubit interaction range**. This is a case for example, in superconducting qubits (IBM and Google).

Another limitation is the **need for fast (real-time) decoding algorithms**, as errors occur frequently and must be corrected quickly before they propagate and lead to system major errors.

Introduction and Motivation

Motivated by the previous restrictions, we investigate how to address such limitations through generalized bicycle codes.

The codes that we consider have the following properties¹:

- Scalability and systematic construction,
- Each code has low weight stabilizers (low qubit connectivity),
- Good decoding performance,
- Low thickness Tanner graph (Thickness ≤ 2),
- Short-depth syndrome measurement circuit.

¹Such conditions align with the codes designed by IBM:
Bravyi S, Cross AW, Gambetta JM, Maslov D, Rall P, Yoder TJ. “High-threshold and low-overhead fault-tolerant quantum memory. *Nature*”, 2024

Notation

\mathbb{F}_2 is the binary field.

For $x, y \in \mathbb{F}_2^n$, the Euclidean inner product is: $x \cdot y = \sum_{i=1}^n x_i y_i$

The Euclidean dual of a binary linear code $C \subseteq \mathbb{F}_2^n$ is

$$C^\perp = \{u \in \mathbb{F}_2^n : \forall x \in C, u \cdot x = 0\}.$$

The Hamming weight of $x \in \mathbb{F}_2^n$ is

$$\text{wt}(x) = |\{1 \leq i \leq n : x_i \neq 0\}|.$$

The minimum distance of a linear code C is

$$d(C) = \min\{\text{wt}(x) : x \in C, x \neq 0\}.$$

Quantum Stabilizer Codes

Consider 1-qubit Pauli matrices:

$$I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, Y = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}, \text{ and } Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}.$$

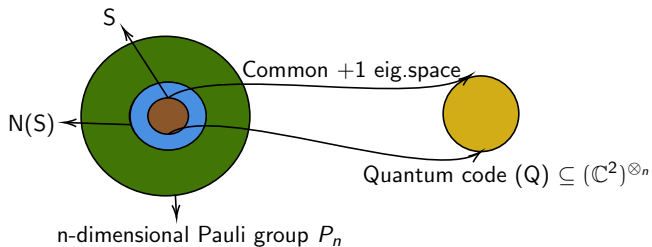
An n -qubit Pauli operator is an element of

$$\otimes_{i=1}^n \{I, X, Y, Z\}.$$

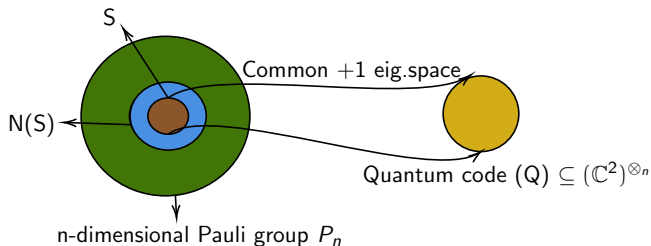
The n -dimensional Pauli group is

$$\{\pm 1, \pm i\} \times \otimes_{i=1}^n \{I, X, Y, Z\}.$$

Stabilizer Diagram

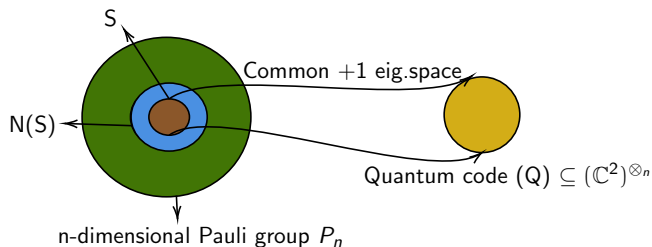


Stabilizer Diagram



S (Stabilizer): is a **commutative subgroup** of the Pauli group such that $-I \notin S$.

Stabilizer Diagram

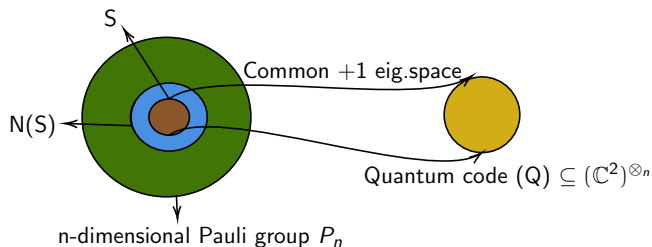


S (Stabilizer): is a **commutative subgroup** of the Pauli group such that $-I \notin S$.

If S has $n - k$ (linearly independent) generators, then Q is represented as an $[[n, k, d]]$, and it is called a **binary quantum stabilizer code**, where $d = \min\{\text{wt}(W) : W \in N(S) \setminus S\}$ and

$N(S)$ (Normalizer) is a subgroup of the Pauli group commuting with S .

Stabilizer Diagram



S (Stabilizer): is a **commutative subgroup** of the Pauli group such that $-I \notin S$.

If S has $n - k$ (linearly independent) generators, then Q is represented as an $[[n, k, d]]$, and it is called a **binary quantum stabilizer code**, where $d = \min\{\text{wt}(W) : W \in N(S) \setminus S\}$ and

$N(S)$ (Normalizer) is a subgroup of the Pauli group commuting with S .

The code Q can correct each error of weight up to $\lfloor \frac{d-1}{2} \rfloor$, given $n - k$ **correct syndromes**.

Quantum CSS Codes

Quantum Calderbank-Shor-Steane (CSS) construction ²:

Theorem

Let $C_2 \subseteq C_1$ be binary linear codes of length n with dimensions k_2 and k_1 , respectively. Then there exists an $[[n, k = k_1 - k_2, d]]$ binary quantum stabilizer code, where

$$d = \min\{d(C_1 \setminus C_2), d(C_2^\perp \setminus C_1^\perp)\}.$$

²A. R. Calderbank and P. W. Shor, "Good quantum error-correcting codes exist", Phys. Rev. A, 1996.

A. M. Steane, "Multiple particle interference and quantum error correction", Proc. Roy. Soc. A, 1996.

Quantum CSS Codes

Quantum Calderbank-Shor-Steane (CSS) construction ²:

Theorem

Let $C_2 \subseteq C_1$ be binary linear codes of length n with dimensions k_2 and k_1 , respectively. Then there exists an $[[n, k = k_1 - k_2, d]]$ binary quantum stabilizer code, where

$$d = \min\{d(C_1 \setminus C_2), d(C_2^\perp \setminus C_1^\perp)\}.$$

In this construction,

- 1 C_2 is in correspondence to (*X-type stabilizers*),
- 2 C_1^\perp is in correspondence to (*Z-type stabilizers*).
- 3 the rest of stabilizers can be obtained as a product of them.

²A. R. Calderbank and P. W. Shor, "Good quantum error-correcting codes exist", Phys. Rev. A, 1996.


A. M. Steane, "Multiple particle interference and quantum error correction", Proc. Roy. Soc. A, 1996.

Generalized Bicycle (GB)³ codes

Let $a(x) = \sum_{i=0}^{n-1} a_i x^i, b(x) \in \mathbb{F}_2[x]/\langle x^n - 1 \rangle$ for some positive integer n .

The $n \times n$ **circulant matrix** corresponding to $a(x)$ is:

$$G_{a(x)} = \begin{bmatrix} a_0 & a_{n-1} & a_{n-2} & \cdots & a_1 \\ a_1 & a_0 & a_{n-1} & \cdots & a_2 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ a_{n-1} & a_{n-2} & a_{n-3} & \cdots & a_0 \end{bmatrix}.$$

³A. A. Kovalev and L. P. Pryadko, "Quantum kronecker sum-product low-density parity-check codes with finite rate". Physical Review A, 2013. 

Generalized Bicycle (GB)³ codes

Let $a(x) = \sum_{i=0}^{n-1} a_i x^i$, $b(x) \in \mathbb{F}_2[x]/\langle x^n - 1 \rangle$ for some positive integer n .

The $n \times n$ **circulant matrix** corresponding to $a(x)$ is:

$$G_{a(x)} = \begin{bmatrix} a_0 & a_{n-1} & a_{n-2} & \cdots & a_1 \\ a_1 & a_0 & a_{n-1} & \cdots & a_2 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ a_{n-1} & a_{n-2} & a_{n-3} & \cdots & a_0 \end{bmatrix}.$$

Let C_1 be the dual of the linear code generated by $[G_{b(x^{-1})}|G_{a(x^{-1})}]$ and C_2 be the linear code generated by $[G_{a(x)}|G_{b(x)}]$.

³A. A. Kovalev and L. P. Pryadko, "Quantum kronecker sum-product low-density parity-check codes with finite rate". Physical Review A, 2013.

Generalized Bicycle (GB)³ codes

Let $a(x) = \sum_{i=0}^{n-1} a_i x^i$, $b(x) \in \mathbb{F}_2[x]/\langle x^n - 1 \rangle$ for some positive integer n .

The $n \times n$ **circulant matrix** corresponding to $a(x)$ is:

$$G_{a(x)} = \begin{bmatrix} a_0 & a_{n-1} & a_{n-2} & \cdots & a_1 \\ a_1 & a_0 & a_{n-1} & \cdots & a_2 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ a_{n-1} & a_{n-2} & a_{n-3} & \cdots & a_0 \end{bmatrix}.$$

Let C_1 be the dual of the linear code generated by $[G_{b(x^{-1})}|G_{a(x^{-1})}]$ and C_2 be the linear code generated by $[G_{a(x)}|G_{b(x)}]$.

Then the CSS code of $C_2 \subseteq C_1$ is called a **GB** code and has parameters $[[2n, 2k, d]]$, where $k = \deg(\gcd(a(x), b(x), x^n - 1))$ and $d = d(C_1 \setminus C_2)$.

³A. A. Kovalev and L. P. Pryadko, "Quantum kronecker sum-product low-density parity-check codes with finite rate". Physical Review A, 2013.

Generalized Bicycle Codes

Our next step is to investigate the structure of GB codes where all the generators of C_2 have small weights (**small quantum connectivity**).

Generalized Bicycle Codes

Our next step is to investigate the structure of GB codes where all the generators of C_2 have small weights (**small quantum connectivity**).

When at least one of $a(x)$ or $b(x)$ has weight less than 2, then the GB code produces a $[[2n, 0, d]]$ with a small d ($d \leq 3$), which are not very interesting.

Generalized Bicycle Codes

Our next step is to investigate the structure of GB codes where all the generators of C_2 have small weights (**small quantum connectivity**).

When at least one of $a(x)$ or $b(x)$ has weight less than 2, then the GB code produces a $[[2n, 0, d]]$ with a small d ($d \leq 3$), which are not very interesting.

The first interesting case: $a(x) = 1 + x$ and $\text{wt}(b(x)) = 2$. In this case, $k = \deg(\gcd(a(x), b(x), x^n - 1)) = 1$. So we get a $[[2n, 2 = 2k]]$ quantum code.

Such GB codes will be called connectivity four codes as $\text{wt}((a(x), b(x))) = 4$.

GB codes with connectivity 4

We performed numerical computations for odd values of n :

n	$a(x)$	$b(x)$	$d(C_1)$	$d(C_2)$	$d(C_1 \setminus C_2)$
5	$1 + x$	$1 + x^3$	3	4	
13	$1 + x$	$1 + x^5$	4	4	
25	$1 + x$	$1 + x^7$	4	4	
41	$1 + x$	$1 + x^9$	4	4	
61	$1 + x$	$1 + x^{11}$	4	4	
85	$1 + x$	$1 + x^{13}$	4	4	

GB codes with connectivity 4

We performed numerical computations for odd values of n :

n	$a(x)$	$b(x)$	$d(C_1)$	$d(C_2)$	$d(C_1 \setminus C_2)$
5	$1 + x$	$1 + x^3$	3	4	3
13	$1 + x$	$1 + x^5$	4	4	5
25	$1 + x$	$1 + x^7$	4	4	7
41	$1 + x$	$1 + x^9$	4	4	9
61	$1 + x$	$1 + x^{11}$	4	4	11
85	$1 + x$	$1 + x^{13}$	4	4	13

The table suggest the construction of a GB family with parameters $[[d^2 + 1, 2, d]]$ for each positive odd d , where $b(x) = 1 + x^d$.

GB codes with connectivity 4

We performed numerical computations for odd values of n :

n	$a(x)$	$b(x)$	$d(C_1)$	$d(C_2)$	$d(C_1 \setminus C_2)$
5	$1 + x$	$1 + x^3$	3	4	3
13	$1 + x$	$1 + x^5$	4	4	5
25	$1 + x$	$1 + x^7$	4	4	7
41	$1 + x$	$1 + x^9$	4	4	9
61	$1 + x$	$1 + x^{11}$	4	4	11
85	$1 + x$	$1 + x^{13}$	4	4	13

The table suggest the construction of a GB family with parameters $[[d^2 + 1, 2, d]]$ for each positive odd d , where $b(x) = 1 + x^d$.

The [rotated surface codes](#) (used in Google and IBM processors) have parameters $[[d^2, 1, d]]$.

GB codes with connectivity 4

We tried a similar computation for even values of n :

n	$a(x)$	$b(x)$	$d(C_1)$	$d(C_2)$	$d(C_1 \setminus C_2)$
8	$1 + x$	$1 + x^5$	4	4	
18	$1 + x$	$1 + x^7$	4	4	
32	$1 + x$	$1 + x^9$	4	4	
50	$1 + x$	$1 + x^{11}$	4	4	
72	$1 + x$	$1 + x^{13}$	4	4	
98	$1 + x$	$1 + x^{15}$	4	4	

GB codes with connectivity 4

We tried a similar computation for even values of n :

n	$a(x)$	$b(x)$	$d(C_1)$	$d(C_2)$	$d(C_1 \setminus C_2)$
8	$1+x$	$1+x^5$	4	4	4
18	$1+x$	$1+x^7$	4	4	6
32	$1+x$	$1+x^9$	4	4	8
50	$1+x$	$1+x^{11}$	4	4	10
72	$1+x$	$1+x^{13}$	4	4	12
98	$1+x$	$1+x^{15}$	4	4	13

The table suggest the construction of a GB family with parameters $[[d^2, 2, d]]$ for each positive odd d with $b(x) = 1 + x^{d+1}$.

GB Family with Connectivity 4

Theorem (D., Sanz, Etxezarreta, Moncy, Crespo, and Otxoa 2025)

Let d be a positive integer integer.

- (1) Then there exists a GB family of $[[d^2 + 1, 2, d]]$ for each odd d .*
- (2) Then there exists a GB family of $[[d^2, 2, d]]$ for each even d .*

GB Family with Connectivity 4

Theorem (D., Sanz, Etxezarreta, Moncy, Crespo, and Otxoa 2025)

Let d be a positive integer integer.

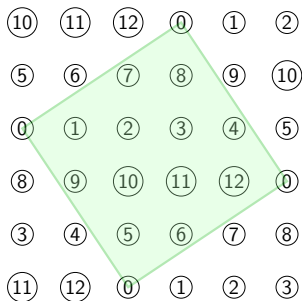
- (1) Then there exists a GB family of $[[d^2 + 1, 2, d]]$ for each odd d .*
- (2) Then there exists a GB family of $[[d^2, 2, d]]$ for each even d .*

Proof idea:

- Transform each GB into an additive cyclic code over \mathbb{F}_4 .
- Map the additive cyclic code to a 2D lattice using an established approach from the literature,
- Find the structure of minimum weight errors (in a similar fashion as surface codes).

GB Proof

2D Lattice for $d = 5$:



Syndrome Extraction and Hook Errors

In general, quantum error correction (or detection) is performed using syndrome information, which is obtained through measurements involving ancilla qubits.

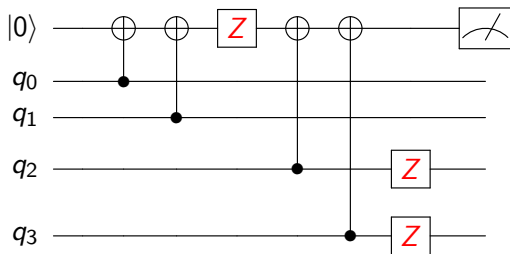
In particular, an $[[n, k, d]]$ code needs $n - k$ ancilla qubits to extract syndromes (total of $2n - k$ qubits to store and extract).

Syndrome Extraction and Hook Errors

In general, quantum error correction (or detection) is performed using syndrome information, which is obtained through measurements involving ancilla qubits.

In particular, an $[[n, k, d]]$ code needs $n - k$ ancilla qubits to extract syndromes (total of $2n - k$ qubits to store and extract).

For example, consider a Z-stabilizer of the form $(1 + x, 1 + x^d)$:

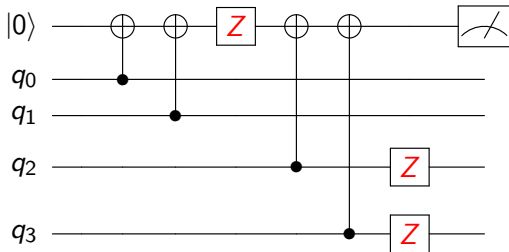


Syndrome Extraction and Hook Errors

In general, quantum error correction (or detection) is performed using syndrome information, which is obtained through measurements involving ancilla qubits.

In particular, an $[[n, k, d]]$ code needs $n - k$ ancilla qubits to extract syndromes (total of $2n - k$ qubits to store and extract).

For example, consider a Z-stabilizer of the form $(1 + x, 1 + x^d)$:

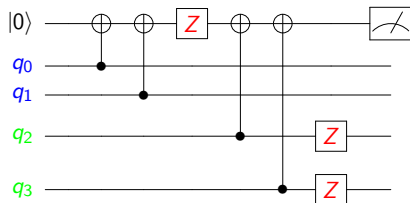


One ancilla qubit error can result in two data qubits error.

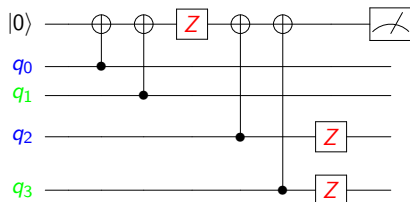
Order of qubits in the extraction circuit

Z-stabilizer: $(1 + x, 1 + x^d)$:

Type A:



Type B:

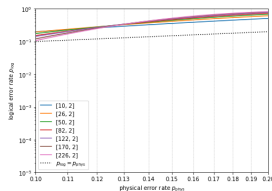
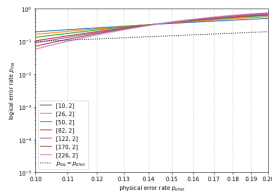
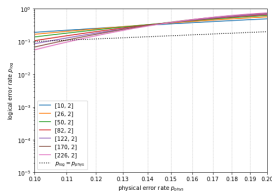
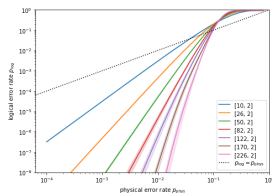
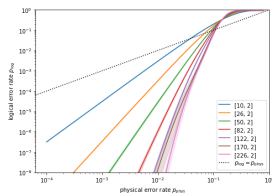
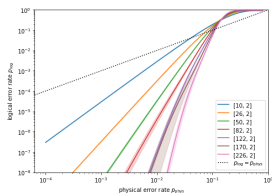


Theorem (D., Sanz, Etxezarreta, Moncy, Crespo, and Otxoa 2025)

Consider the GB families $[[d^2 + 1, 2, d]]$ and $[[d^2, 2, d]]$ for positive odd and even d , respectively. **If an error can happen to all qubits (data and ancilla), then Type A extraction circuit preserves the minimum distance.**

We showed through examples that Type B circuit can reduce the distance (up to $\lfloor \frac{d-1}{2} \rfloor$).

Code Capacity Threshold $[[d^2 + 1, 2, d]]$



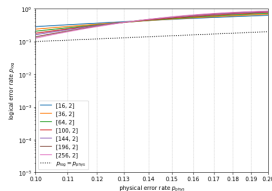
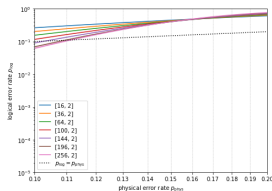
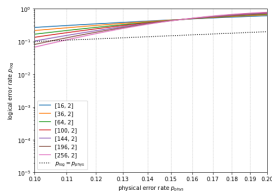
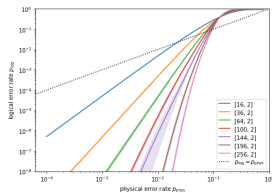
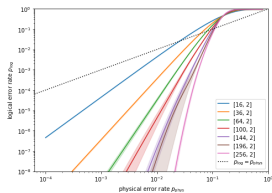
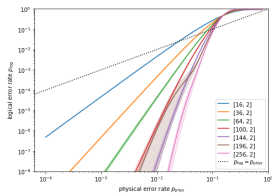
Left: Under minimum-weight perfect-matching decoder (MWPM)

Middle: Belief-propagation ordered statistics decoder (BP-OSD)

Right: Decoder based on belief finding (BF)

Family $[[d^2 + 1, 2, d]]$ under depolarizing noise

Code Capacity Threshold $[[d^2, 2, d]]$



Left: MWPM

Middle: BP-OSD

Right: BF

Family $[[d^2, 2, d]]$ under depolarizing noise

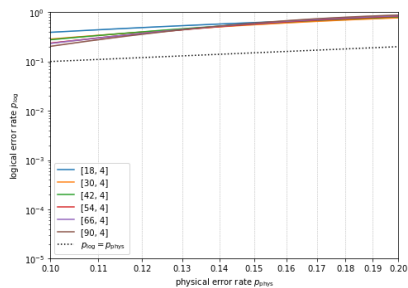
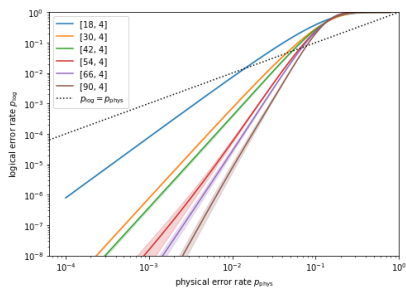
Other examples

We also conducted numerical search for optimal connectivity 5 and 6 GB codes.

Connectivity 5	Connectivity 6
[[18, 4, 3]]	[[18, 4, 4]]
[[30, 4, 5]]	[[30, 4, 6]]
[[42, 4, 6]]	
[[54, 4, 7]]	[[54, 4, 8]]
[[66, 4, 8]]	[[66, 4, 10]]
[[78, 4, 9]]	
[[90, 4, 9]]	[[90, 4, 12]]
[[102, 4, 10]]	
[[114, 4, 11]]	

Table: Connectivity 5 and 6 GB codes.

Code Capacity Threshold for Connectivity 5 GB Codes



BP-OSD

Under depolarizing noise.

Thank You!

Questions or Comments?