Coprime Bivariate Bicycle Codes and their Properties

Ming Wang and Frank Mueller (mwang42@ncsu.edu; fmuelle@ncsu.edu)
Department of Computer Science, North Carolina State University
NC STATE UNIVERSITY

Introduction

Motivation:

- Discover previously unknown, good bivariate bicycle (BB) codes.

Problem:

- Searching for and verifying good BB codes is very time-consuming.
  - Many combinations of polynomials are redundant, yielding codes with the same parameters.
  - Verifying the distances of codes are particularly resource-intensive.
- The search can be greatly accelerated if:
  1. We can eliminate some duplicated results.
  2. We can discard bad results during the verification process.
  3. We predict distance and dimension before the search to avoid generating undesirable codes.

Basic Definitions:

- BB codes: $H_X = [A \mid B], H_Z = [B^T \mid A^T]$, where $A = a(x,y), B = b(x,y)$, $x = S_l \otimes I_m, y = I_l \otimes S_m$ and $S_l = I_l \gg 1$
- Coprime BB codes: $A = a(\pi), B = b(\pi)$, where $\pi = xy$ and l, m are coprime integers. Require that $\mathrm{GCD}(a(\pi), b(\pi), \pi^{lm} + 1) \neq 1$, rest are the same as BB codes

Methodology

Fast search:

Equivalence:

Proved these four BB codes have the same $[[n,k,d]]$ parameters, allowing us to search within only one classof these codes.

$$C_1\!: H_X = [A|B], H_Z = [B^T|A^T]$$
$$C_2\!: H_X = [A^T|B^T], H_Z = [B|A]$$
$$C_3\!: H_X = [B|A], H_Z = [A^T|B^T]$$
$$C_4\!: H_X = [B^T|A^T], H_Z = [A|B]$$

Code selection:

Discard bad BB codes (low k and d) using BP-OSD decoding.

- k can be easily computed using $k = 2lm - \mathrm{rank}(H_X) - \mathrm{rank}(H_Z)$
- d can be bounded by performing multiple rounds of decoding. If d is low in one round, the rest rounds can be skipped.

Coprime BB codes:

The dimension of coprime BB codes is determined by $k = 2\deg g(\pi)$, where $g(\pi) = \mathrm{GCD}(a(\pi), b(\pi), \pi^{lm} + 1)$. Thus, the k is determined before the search.

Algorithms:

Algorithm 1: An algorithm to search for BB codes

Data: l, m, τ_k, τ_d
Result: codes of parameters $[[2lm, k, d]]$
Generate all polynomial pairs of the specified form
$L \leftarrow [(a_1(x,y), b_1(x,y)), \ldots]$;
Remove codes with the same parameters:
$L' \leftarrow$ remove_equivalent(L);
for $i \leftarrow 1$ **to** $|L'|$ **do**
  if is_connected$(a_i(x,y), b_i(x,y))$ **then**
    $H_X, H_Z =$ BB_matrices$(a_i(x,y), b_i(x,y))$;
    $k \leftarrow 2lm - 2$rank(H_X);
    if $k < \tau_k$ **then**
      continue ;
    else
      $d \leftarrow$ distance_upperbound(H_X, H_Z, τ_d);
    end
  else
    continue ;
  end
end

Algorithm 2: An algorithm to search for BB codes with the new form of polynomials.

Data: $l, m, \tau_d, p(\pi)$; /* $p(\pi)$ is a factor of $\pi^{lm}+1$ */
Result: codes of parameters $[[2lm, k, d]]$
$C \leftarrow$ all polynomials $f(\pi)$ in $\mathbb{F}_2[\pi]/(\pi^{lm}+1)$ s.t. wt$(f(\pi)) = 3$;
$C' \leftarrow$ all polynomials $c(\pi)$ in C s.t. $c(\pi) \bmod p(\pi) = 0$;
$L \leftarrow$ all polynomial pairs $(a(\pi), b(\pi))$ in C' s.t. $\mathrm{GCD}(a(\pi), b(\pi)) = p(\pi)$;
$L' \leftarrow$ remove_equivalent(L);
for $i \leftarrow 1$ **to** $|L'|$ **do**
  if is_connected$(a_i(x,y), b_i(x,y))$ **then**
    $H_X, H_Z =$ BB_matrices$(a_i(x,y), b_i(x,y))$;
    $k \leftarrow 2lm - 2$rank(H_X);
    $d \leftarrow$ distance_upperbound(H_X, H_Z, τ_d);
  else
    continue ;
  end
end

Results

BB codes found by Algorithm 1:

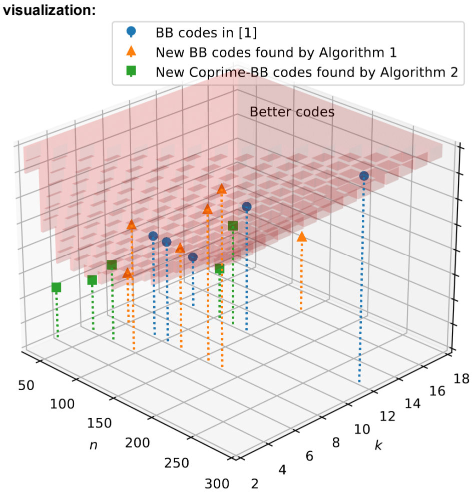
l	m	$a(x,y)$	$b(x,y)$	$[[n,k,d]]$
3	9	$1+y^2+y^4$	$y^3+x^1+x^2$	$[[54,8,6]]$
7	7	$x^3+y^5+y^6$	$y^2+x^3+x^5$	$[[98,6,12]]$
3	21	$1+y^2+y^{10}$	y^3+x+x^2	$[[126,8,10]]$
5	15	$1+y^6+y^8$	y^5+x+x^4	$[[150,16,8]]$
3	27	$1+y^{10}+y^{14}$	$y^{12}+x+x^2$	$[[162,8,14]]$
6	15	x^3+y+y^2	$y^6+x^4+x^5$	$[[180,8,16]]$

Coprime BB codes found by Algorithm 2:

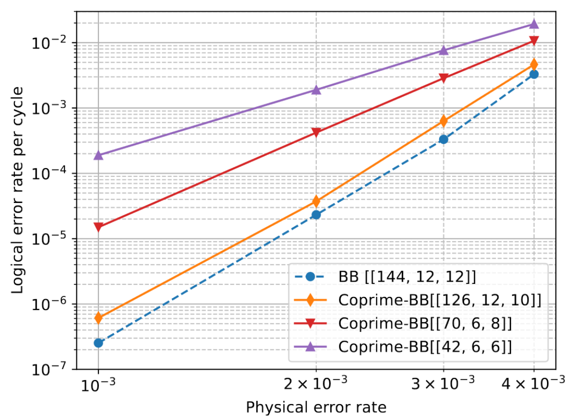
l	m	$a(\pi)$	$b(\pi)$	$[[n,k,d]]$
3	5	$1+\pi+\pi^2$	$\pi+\pi^3+\pi^8$	$[[30,4,6]]$
3	7	$1+\pi^2+\pi^3$	$\pi+\pi^3+\pi^{11}$	$[[42,6,6]]$
5	7	$1+\pi+\pi^5$	$1+\pi+\pi^{12}$	$[[70,6,8]]$
2	27	$\pi^2+\pi^5+\pi^{44}$	$\pi^8+\pi^{14}+\pi^{47}$	$[[108,12,6]]$
7	9	$1+\pi+\pi^{58}$	$\pi^3+\pi^{16}+\pi^{44}$	$[[126,12,10]]$

Some interesting short codes are found, e.g., [[30, 4, 6]] and [[42, 6, 6]]. A [[126, 12, 10]] code has also been found by Panteleev et al., 2021. However, the equivalence of the two codes is unknown.

Parameters visualization:



Performance comparison (under circuit noise model):



The [[126, 12, 10]] code exhibits a similar error rate to the [[144, 12, 12]] code, despite having a lower distance. This can likely be attributed to the circuit-level distance: the [[126, 12]] code has a circuit-level distance of 9, while the [[144, 12]] code has a circuit-level distance of 10.

Conclusion

- We developed algorithms for fast numerical searches for the discovery of BB codes.
- We proposed a novel construction of BB codes by choosing a factor polynomial from $\mathbb{F}_2[\pi]/(\pi^{lm}+1)$, where l and m are coprime integers. The new construction enables us to know the rate of BB codes before constructing them.
- The [[126, 12, 10]] code achieves a slightly higher error rate than the [[144, 12, 12]] code with fewer qubits. However, a challenge that remains is the practical implementation of these codes, specifically in mapping them onto quantum architectures that are constrained by the limitations of current quantum device technologies.

Acknowledgements

This research was supported by NSF awards DMR-1747426, PHY-1818914, MPS-2120757, and CCF-2217020.

Full text @ arxiv.org