Trade-Based LDPC Codes

Daniel Panario
School of Mathematics and Statistics
Carleton University
daniel@math.carleton.ca

Joint work with Farzane Amirzade and Mohammad-Reza Sadeghi

RICCOTA – July 3-7, 2023

Directed Group Divisible Designs

Let $k \leq v$. A (k, λ) directed group divisible design (DGDD) of type g^u with $gu = v$, is a triple $(V, \mathcal{G}, \mathcal{B})$, where V is a v-set, $\mathcal{G}$ is a collection of subsets (groups), each of cardinality g, which partition V into u groups of size g and $\mathcal{B}$ is a collection of ordered k-subsets of V and any pair of distinct elements of V appears in precisely λ blocks or one group but not in both. If $\lambda = 1$, then $(k, 1)$-DGDD is denoted by k-DGDD.

Example

A super-simple 4-DGDD of type 2^4 can be obtained by the groups $\{0, 1\}$, $\{2, 3\}$, $\{4, 5\}$, $\{6, 7\}$ and the blocks

$$\begin{aligned}\mathcal{B} = \quad & \{(3,0,5,6),(7,5,0,2),(5,7,1,3),(6,4,3,1),\\ & (4,6,2,0),(1,2,6,5),(0,3,4,7),(2,1,7,4)\}\end{aligned}$$

Trades

A $(v, k, 2)$ directed trade of volume s consists of two disjoint collections T_1 and T_2, each of s blocks, such that every pair of distinct elements of V is covered by precisely the same number of blocks of T_1 as of T_2.

Example

Super-simple 4-DGDD of type 2^4 with groups $\{0, 1\}$,$\{2, 3\}$,$\{4, 5\}$,$\{6, 7\}$ and the blocks $(3, 0, 5, 6), (7, 5, 0, 2), (5, 7, 1, 3), (6, 4, 3, 1), (4, 6, 2, 0)$, $(1, 2, 6, 5), (0, 3, 4, 7), (2, 1, 7, 4)$ contains four $(8, 4, 2)$ trades of volume 2.

T_1	T_2	T_1	T_2
$(3, 0, 5, 6)$	$(3, 5, 0, 6)$	$(5, 7, 1, 3)$	$(5, 7, 3, 1)$
$(7, 5, 0, 2)$	$(7, 0, 5, 2)$	$(6, 4, 3, 1)$	$(6, 4, 1, 3)$
T_1	T_2	T_1	T_2
$(4, 6, 2, 0)$	$(4, 2, 6, 0)$	$(0, 3, 4, 7)$	$(0, 3, 7, 4)$
$(1, 2, 6, 5)$	$(1, 6, 2, 5)$	$(2, 1, 7, 4)$	$(2, 1, 4, 7)$

Cyclical Trade

A set of s blocks $\{B_1, \ldots, B_s\}$ forms a cyclical trade of volume s if each pair of consecutive blocks B_i, B_{i+1} for $1 \leq i \leq s-1$, as well as B_1, B_s, form s trades of volume 2. We denote a cyclical trade of volume s by CT_s.

Example

A super-simple 4-DGDD of type 2^4 with groups $\{0,1\}, \{2,3\}, \{4,5\}, \{6,7\}$ and the blocks $(3,0,5,6), (7,5,0,2), (5,7,1,3), (6,4,3,1), (4,6,2,0),$ $(1,2,6,5), (0,3,4,7), (2,1,7,4)$ has a cyclical trade of volume 4

$CT_4 = \{(3,0,5,6), (7,5,0,2), (4,6,2,0), (1,2,6,5)\},$

and a cyclical trade of volume 5

$CT_5 = \{(3,0,5,6), (7,5,0,2), (5,7,1,3), (2,1,7,4), (1,2,5,6)\}.$

Protograph-Based QC-LDPC Codes

Quasi-cyclic low-density parity-check codes (QC-LDPC codes) is an important category of LDPC codes. These codes are practical and have simple implementation.

Two approaches to construct QC-LDPC codes are algebraic-based and protograph-based. Protograph-based QC-LDPC codes are allocated with two matrices, a base matrix W and an exponent matrix B.

Suppose W is an $m \times n$ base matrix. If all elements of W are 0 and 1, then we obtain a single-edge QC-LDPC code. If W contain elements bigger than 1, then we obtain a multi-edge QC-LDPC code.

Multi-Edge QC-LDPC Codes

Let N be an integer number; $B = [\vec{B}_{ij}]$ is an exponent matrix, where B_{ij} is (∞), or $|\vec{B}_{ij}| = W_{ij}$, $\vec{B}_{ij} = (b_{ij}^1, b_{ij}^2, \ldots, b_{ij}^l)$, $b_{ij}^r \in \{0, 1, \ldots, N-1\}$ and $b_{ij}^r \neq b_{ij}^{r'}$ for $1 \leq r < r' \leq l$, $l \in \mathbb{N}$,

$$B = \begin{bmatrix} \vec{B}_{00} & \vec{B}_{01} & \cdots & \vec{B}_{0(n-1)} \\ \vec{B}_{10} & \vec{B}_{11} & \cdots & \vec{B}_{1(n-1)} \\ \vdots & \vdots & \ddots & \vdots \\ \vec{B}_{(m-1)0} & \vec{B}_{(m-1)1} & \cdots & \vec{B}_{(m-1)(n-1)} \end{bmatrix}. \tag{1}$$

If B_{ij} is (∞), then it is replaced by an $N \times N$ zero matrix. If B_{ij} is a vector, then it is substituted by an $N \times N$ matrix H_{ij}:

$$H_{ij} = I^{b_{ij}^1} + I^{b_{ij}^2} + \cdots + I^{b_{ij}^l},$$

where $I^{b_{ij}^r}$ is a circulant permutation matrix (CPM) with 1 in the b_{ij}^r-th position of the top row and other rows are cyclic shifts of the first row. The null space of this parity-check matrix gives a QC-LDPC code.

Example

Given base and an exponent matrices of a QC-LDPC code with $N = 5$

$$W = \begin{bmatrix} 3 & 1 & 2 & 0 \\ 0 & 2 & 1 & 3 \end{bmatrix}, B = \begin{bmatrix} (0,1,3) & (0) & (0,4) & (\infty) \\ (\infty) & (2,4) & (3) & (1,2,3) \end{bmatrix},$$

the parity-check matrix of the QC-LDPC code is:

$$H = \left[\begin{array}{c|c|c|c}
11.1. & 1.... & 1...1 & ..... \\
.11.1 & .1... & 11... & ..... \\
1.11. & ..1.. & .11.. & ..... \\
.1.11 & ...1. & ..11. & ..... \\
1.1.1 & ....1 & ...11 & ..... \\
\hline
..... & ..1.1 & ...1. & .111. \\
..... & 1..1. & ....1 & ..111 \\
..... & .1..1 & 1.... & 1..11 \\
..... & 1.1.. & .1... & 11..1 \\
..... & .1.1. & ..1.. & 111..
\end{array}\right].$$

Our Results

First, we provide a new approach to construct parity-check matrices of LDPC codes of girth at least 6 based on trades of super-simple directed designs. We call these trade-based LDPC codes.

Then, we use those trade-based matrices to define base matrices of multi-edge protographs for which the construction of exponent matrices has less complexity compared to the existing base matrices in the literature.

We use a trade-based matrix to obtain parity-check matrices of time-varying spatially-coupled (SC-LDPC) codes in which each row shift of the trade-based matrix yields syndrome matrices of a certain time.

Finally, we give simulations, experimentally showing the advantage of trade-based LDPC codes.

Construction of Trade-Based LDPC Codes

Let $V = \{0, 1, \ldots, v-1\}$ be the v-set and $|\mathcal{B}| = n$.

Construct a $\binom{v}{2} \times n$ binary matrix A as follows:

- Row indices are pairs (x_i, x_j)s, where $x_i < x_j \in \{0, 1, \ldots, v-1\}$;
- Column indices are $B_1, \ldots, B_n$;
- $A_{(x_i,x_j)\ell} = \begin{cases} 1 & \text{if } (x_i, x_j) \text{ or } (x_j, x_i) \text{ belongs to } B_\ell \text{ and appears in a trade;} \\ 0 & \text{otherwise.} \end{cases}$

Then, remove all-zero columns and all-zero rows of A obtaining a binary matrix denoted by C.

The parity-check matrix of trade-based LDPC code is:

- C if the number of rows of C is less than the number of columns.
- C^T if the number of rows of C is more than the number of columns.

Example

Consider the super-simple design with blocks

$$\begin{aligned}\mathcal{B} = \ &\{(7,5,0,2),(5,7,1,3),(3,0,5,6),(1,2,6,5),\\ &(0,3,4,7),(2,1,7,4),(6,4,3,1),(4,6,2,0)\}.\end{aligned}$$

Taking all trades, we construct the trade-based matrix A which is a matrix of size 12×8 without any zero rows or zero columns.

Thus, the matrix C equals A and the following C^T yields the parity-check matrix of a $(2,3)$-regular LDPC code:

$$C^T = \begin{array}{c} \begin{matrix} 02 & 03 & 12 & 13 & 05 & 17 & 26 & 34 & 46 & 47 & 56 & 57 \end{matrix} \\ \begin{bmatrix} 1 & . & . & . & 1 & . & . & . & . & . & . & 1 \\ . & . & . & 1 & . & 1 & . & . & . & . & . & 1 \\ . & 1 & . & . & 1 & . & . & . & . & . & 1 & . \\ . & . & 1 & . & . & . & 1 & . & . & . & 1 & . \\ . & 1 & . & . & . & . & . & 1 & . & 1 & . & . \\ . & . & 1 & . & . & 1 & . & . & . & 1 & . & . \\ . & . & . & 1 & . & . & . & 1 & 1 & . & . & . \\ 1 & . & . & . & . & . & 1 & . & 1 & . & . & . \end{bmatrix} \end{array} \begin{matrix} (7,5,0,2) \\ (5,7,1,3) \\ (3,0,5,6) \\ (1,2,6,5) \\ (0,3,4,7) \\ (2,1,7,4) \\ (6,4,3,1) \\ (4,6,2,0) \end{matrix}$$

Trade-Based Multiple-Edge QC-LDPC Codes

A base matrix of a trade-based multi-edge protograph is defined as follows:

1. Call the matrix C or C^T as C_1.
2. Displace the rows of C_1 to obtain other matrix named as C_2 such that $[C_1|C_2]$ does not cause a 2×2 all-one submatrix.
3. Continue this process to find other C_is and the matrix $P = [C_1|C_2|\cdots|C_r]$ of the maximum size.
4. Convert all 1s of C_1 to integers $l \geq 1$ to obtain a base matrix W_1.
5. Define $W = [W_1|\cdots|W_r]$ such that each W_i is the row displacement of W_1 exactly as C_i is the row displacement of C_1.

An exponent matrix of a trade-based multi-edge protograph is $B = [B_1|\cdots|B_r]$ such that each B_i is the row displacement of B_1 exactly as W_i is the row displacement of W_1.

Example

Consider a super-simple design with $V = \{0, 1, \ldots, 7\}$, blocks

$$\mathcal{B} = \{(0,3,6,5),(7,5,0,2),(5,7,3,1),(6,1,4,3),\\ (4,6,2,0),(1,2,5,6),(3,0,7,4),(2,4,1,7)\}$$

and matrix C

(0, 3, 6, 5)	(7, 5, 0, 2)	(5, 7, 1, 3)	(2, 4, 1, 7)	(4, 6, 2, 0)	(1, 2, 5, 6)	(3, 0, 7, 4)	(6, 1, 4, 3)	
.	1	.	.	1	.	.	.	02
1	.	.	.	.	.	1	.	03
.	.	.	1	.	.	.	1	14
1	.	.	.	.	1	.	.	56
.	1	1	.	.	.	.	.	57

Taking C as C_1, we construct $W = [W_1 | \cdots | W_5]$ of the maximum size free of a 2×2 submatrix of nonzero entries. This is a base matrix of a $(3, 24)$-regular multi-edge QC-LDPC code:

$$W = \left[\begin{array}{c|c|c|c|c} 01003000 & 02300000 & 20000300 & 00030003 & 10000030 \\ 10000030 & 01003000 & 02300000 & 20000300 & 00030003 \\ 00030003 & 10000030 & 01003000 & 02300000 & 20000300 \\ 20000300 & 00030003 & 10000030 & 01003000 & 02300000 \\ 02300000 & 20000300 & 00030003 & 10000030 & 01003000 \end{array}\right]$$

Example (cont.)

To define $B = [B_1 | \cdots | B_5]$, first, we identify the entries of B_1 with $N = 41$:

$$B_1 = \begin{bmatrix} (\infty) & (0) & (\infty) & (\infty) & (0,1,3) & (\infty) & (\infty) & (\infty) \\ (0) & (\infty) & (\infty) & (\infty) & (\infty) & (\infty) & (0,4,9) & (\infty) \\ (\infty) & (\infty) & (\infty) & (0,6,13) & (\infty) & (\infty) & (\infty) & (0,8,22) \\ (7,27) & (\infty) & (\infty) & (\infty) & (\infty) & (0,10,25) & (\infty) & (\infty) \\ (\infty) & (19,36) & (6,24,36) & (\infty) & (\infty) & (\infty) & (\infty) & (\infty) \end{bmatrix}.$$

Next, we take $B = [B_1 | \cdots | B_5]$ such that each B_i is a row displacement of B_1 and is associated to W_i.

Computational complexity of our method

- The size of the search space to obtain the entries of B is reduced from N^{120} to N^{24}. The matrix B containes 120 entries. Using our method, defining only 24 entries we can construct the exponent matrix.

Merits of Our Method

- Low dense protographs.
  Both base and exponent matrices are low-dense. The cycle distributions in the Tanner graph has less density compared with other multi-edge protographs.

- Smaller computational complexity to define the exponent matrix.
  We only define the entries of B_1. If $B = [B_1| \cdots |B_r]$ and B_1 contains s entries, then the number of integers of B is rs. Thus, the computational complexity to construct B reduces from N^{rs} to N^s.

- Smaller lower bound on the lifting degree.
  The minimum lifting degree is smaller than other multi-edge protographs.

Properties of a Trade-Based LDPC Code

Theorem

Consider a trade-based LDPC code from a super-simple directed design $\mathcal{D}$. The Tanner graph of the trade-based LDPC code has $2s$-cycles if and only if $\mathcal{D}$ has a cyclical trade of volume s.

Corollary

- The Tanner graph of a trade-based LDPC code is free of 4-cycles.
- The existence of cyclical trades of volume 3 results in 6-cycles in the Tanner graph of a trade-based LDPC code.

Minimum Distance of Trade-Based LDPC Codes

A path in a Tanner graph is independent if the first and last vertices are only connected to vertices in the path.

Theorem

Consider a trade-based LDPC code from a super-simple directed design with $\lambda = 1$. The minimum distance of the code is equal to the smallest volume of a cyclical trade or the smallest length of an independent path.

Example

The minimum distance of the trade-based LDPC code with the following blocks is 4 since the smallest cyclical trade of this design is 4 and it has no independent paths:

$$\begin{aligned}\mathcal{B} = \quad & \{(7,5,0,2),(5,7,1,3),(3,0,5,6),(1,2,6,5),\\ & (0,3,4,7),(2,1,7,4),(6,4,3,1),(4,6,2,0)\}.\end{aligned}$$

- F. Amirzade, D. Panario and M.-R. Sadeghi, "Trade-based LDPC codes", *ISIT 2022 (International Symposium on Information Theory)*, IEEE Xplore, 542–547, 2022.
- M. P. C. Fossorier, "Quasi-Cyclic Low-Density Parity-Check codes from circulant permutation matrices," *IEEE Trans. Inf. Theory*, vol. 50, no. 8, pp. 1788–1793, (2004).
- H. Park, S. Hong, J. Seon and D. J. Shin, "Design of multiple-edge protographs for QC-LDPC codes avoiding short inevitable cycles," *IEEE Trans. Inf. Theory*, vol. 59, no. 7, pp. 4598–4614, (2013).
- M.-R Sadeghi and F. Amirzade, "Analytical Lower Bound on the Lifting Degree of Multiple-Edge QC-LDPC Codes with Girth 6," *IEEE Commun. Letters*, vol. 22, no. 8, pp. 1528–1531, (2018).

- F. Amirzade, D. Panario and M.-R. Sadeghi, "Trade-based LDPC codes", *ISIT 2022 (International Symposium on Information Theory)*, IEEE Xplore, 542–547, 2022.
- M. P. C. Fossorier, "Quasi-Cyclic Low-Density Parity-Check codes from circulant permutation matrices," *IEEE Trans. Inf. Theory*, vol. 50, no. 8, pp. 1788–1793, (2004).
- H. Park, S. Hong, J. Seon and D. J. Shin, "Design of multiple-edge protographs for QC-LDPC codes avoiding short inevitable cycles," *IEEE Trans. Inf. Theory*, vol. 59, no. 7, pp. 4598–4614, (2013).
- M.-R Sadeghi and F. Amirzade, "Analytical Lower Bound on the Lifting Degree of Multiple-Edge QC-LDPC Codes with Girth 6," *IEEE Commun. Letters*, vol. 22, no. 8, pp. 1528–1531, (2018).

Many Thanks For Your Attention!