MTNS 2022

A Number Theoretic Approach to Cycles in LDPC Codes

Simran Tinani[1]

Based on joint work with Julia Lieb

University of Zurich[UZH]

September 12, 2022

[1] Simran Tinani's research is supported by armasuisse Science and Technology.

Introduction

- LDPC (Low-density Parity-Check) codes, first introduced in 1962, are recently gaining traction for practical use due to the efficient bit-flipping and message-passing decoding algorithms.
- The parity-check matrix of an LDPC code can be associated to a sparse bipartite graph called the Tanner graph.
- The size of the smallest cycle in this graph is called the girth. For efficient decoding, it is desirable to come up with constructions of codes where the girth is not too small.

Introduction

- A popular subclass of LDPC codes has a block matrix as a parity-check matrix, with each block a permutation matrix.
- Using circulant permutation matrices as building blocks, one obtains quasi-cyclic LDPC (QC-LDPC) codes.

$$H_{i,j} = \begin{pmatrix} a_0 & a_{n-1} & \dots & a_1 \\ a_1 & a_0 & \dots & a_2 \\ \vdots & \vdots & \ddots & \vdots \\ a_{n-1} & \dots & a_1 & a_0 \end{pmatrix}; H = \begin{pmatrix} H_{0,0} & \dots & H_{0,n-1} \\ H_{1,0} & \dots & H_{1,n-1} \\ \vdots & \ddots & \vdots \\ H_{n-1,0} & \dots & H_{n-1,n-1} \end{pmatrix}$$

- We generalize the theory of QC-LDPC codes by studying parity-check matrices consisting of permutation matrices that are all powers of a fixed permutation f.

Introduction

- QC-LDPC codes are a special case: a permutation $i \mapsto i + k$ is a power of the cyclic permutation $\mathbb{Z}_n \to \mathbb{Z}_n,\ i \mapsto i + 1$.
- Associate to a permutation $R_{j,l} : \mathbb{Z}_n \to \mathbb{Z}_n$ an $n \times n$ permutation matrix P: $P_{j,l}(i, k) = 1$ if $i = R_{j,l}(k)$.
- Let $L, J \geq 1$ be positive integers and H be a block parity check matrix of the form
$$H = \begin{pmatrix} 1_{n\times n} & 1_{n\times n} & \cdots & 1_{n\times n} \\ 1_{n\times n} & P_{1,1} & \cdots & P_{1,L} \\ \vdots & \vdots & \ddots & \vdots \\ 1_{n\times n} & \cdots & P_{J,L-1} & P_{J,L} \end{pmatrix}.$$
- Write the entries of $P_{j,l}$ as $h_{jn+j',ln+l'}$, $0 \leq j \leq J$, $0 \leq l \leq L$, $0 \leq j', l' \leq n$.

Introduction

Definition (Cycle of length $2k$)

A sequence of positions (x_i, y_i) of the form $h_{x_0,y_0} = 1, h_{x_1,y_0} = 1, h_{x_1,y_1} = 1, \ldots, h_{x_{k-1},y_{k-1}} = 1, h_{x_0,y_{k-1}} = 1, h_{x_0,y_0} = 1$ in H obtained by changing alternately row or column only (starting with the row) with all positions are distinct, except the first and last.

Definition (Girth)

The girth $g(H)$ of H is the smallest positive even integer $2k$, $k > 1$, such that H contains a $2k$-cycle.

Each cycle can be associated to a unique path $(j_0, l_0), \ldots, (j_{k-1}, l_{k-1}), (j_k, j_{k-1}), (j_k, l_k) = (j_0, l_0)$ of indices labelling the permutation matrices.

Introduction: Cycles

$$H = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 \end{pmatrix}$$

Background

Theorem 1 (Fossorier, 2004)

There exists a cycle associated to the sequence

$$(j_0, l_0), \ldots, (j_{k-1}, l_{k-1}), (j_0, j_{k-1}), (j_k, l_k) = (j_0, l_0)$$

if and only if there exists a column index c_0, $0 \leq c_0 \leq n$, such that $R_{j_0,l_0}(c_0) = R_{j_0,l_{k-1}}(c_{k-1})$, or $c_k = c_0$, where $c_{i+1} = (R^{-1}_{j_{i+1},l_{i+1}}(R_{j_{i+1},l_i}(c_i))$ for $0 \leq i \leq k-1$.

Theorem 2

If H has a submatrix of the form $\begin{pmatrix} 1 & 1 & 1 \\ 1 & \sigma_1 & \sigma_2 \end{pmatrix}$ with $\sigma_1\sigma_2 = \sigma_2\sigma_1$ then H contains a 12-cycle, so that $g(H) \leq 12$.

Additive number theory concepts

Let $\mathcal{B} \subseteq \mathbb{Z}$ be a set.

Definition

Associate to $\mathcal{B}$ the following sets.

$$\mathcal{B}_\Delta = \{a - b \mid a, b \in \mathcal{B}, a \neq b\},\ \mathcal{B}_+ = \{a + b \mid a, b \in \mathcal{B}.\}$$

$$\mathcal{B}_S^t = \{(a_0, a_1 \ldots, a_t) \mid a_i \neq a_{i+1}, 0 \leq i < t,\ a_t \neq a_0\}$$

$$\mathcal{B}_D^t = \{(a_0 - a_t, a_1 - a_0, \ldots, a_t - a_{t-1}) \mid (a_0, \ldots, a_t) \in \mathcal{B}_S^t\}$$

Definition

A set $\mathcal{I} \subseteq \mathbb{Z}_m$ is called a Sidon m-B_t set (or, in short, an m-B_t set) if for $i_1, i_2, \ldots, i_t, j_1, \ldots j_t \in \mathcal{I}$, we have $i_1 + i_2 + \ldots + i_t = j_1 + j_2 + \ldots + j_t$ mod $m \iff \{i_1, i_2, \ldots, i_t\} = \{j_1, j_2, \ldots, j_t\}$.

Additive number theory Concepts

Let $f : \mathbb{Z}_n \to \mathbb{Z}_n$ be a permutation and let m be its order in the group $\mathcal{S}_n$. If n is prime and f is an n-cycle, then $m = n$ and we say that f is a prime m-cycle. A permutation f is said to be a **derangement** if it has no fixed points, i.e. if $f(c) \neq c \ \forall \ c \in \mathbb{Z}_n$.

Lemma 1

- *If c_0 is a fixed point of f then it is a fixed point of f^i $\forall i \geq 1$.*
- *If f is a derangement, f^i is a derangement for i coprime to m.*

We consider parity check matrices $H = \begin{pmatrix} 1 & 1 & \dots & 1 \\ 1 & f^{A_1 i_1} & \dots & f^{A_1 i_L} \\ 1 & f^{A_2 i_1} & \dots & f^{A_2 i_L} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & f^{A_J i_1} & \dots & f^{A_J i_L} \end{pmatrix}$.

Write $\mathcal{I} = \{0, i_1, i_2, \dots, i_L\} \subseteq \mathbb{Z}_m$, $\mathcal{A} = \{0, A_1, A_2, \dots A_J\} \subseteq \mathbb{Z}_m$.

Conditions for $2k$-cycles

Lemma 2

The following statements are equivalent.

- *H has a $2k$-cycle.*
- *There exists a sequence $A_D = (b_1, \ldots, b_k) \in \mathcal{A}_D^k$, a sequence $J_s = (j_1 \ldots, j_k) \in \mathcal{I}_S^k$, and a point $c_0 \in \mathbb{Z}_n$ such that for all $k' < k$, $f^{b_1 j_1 + \ldots + b_{k'} j_{k'}}(c_0) \neq c_0$, and $f^{b_1 j_1 + \ldots + b_k j_k}(c_0) = c_0$.*
- *There exists a sequence $A_S = (b_1, \ldots, b_k) \in \mathcal{A}_S^k$, a sequence $J_D = (j_1 \ldots, j_k) \in \mathcal{I}_D^k$, and a point $c_0 \in \mathbb{Z}_n$ such that for all $k' < k$, $f^{b_1 j_1 + \ldots + b_{k'} j_{k'}}(c_0) \neq c_0$, and $f^{b_1 j_1 + \ldots + b_k j_k}(c_0) = c_0$.*

Lemma 3

If f is a prime m-cycle, then H has no $2k$-cycle if and only if for any sequences $A_D = (b_1, \ldots, b_k) \in \mathcal{A}_D^k$, $J_S = (j_1 \ldots, j_k) \in \mathcal{I}_S^k$, we have $b_1 j_1 + \ldots + b_k j_k \neq 0$.

Conditions for $2k$-cycles: Case $J = 1$

$H = \begin{pmatrix} 1 & 1 & \dots & 1 \\ 1 & f^{i_1} & \dots & f^{i_L} \end{pmatrix}$. Here, all $(4k+2)$-cycles are absent.

Theorem 3

Consider the parity check matrix $H = \begin{pmatrix} 1 & 1 \\ 1 & f \end{pmatrix}$. *Then* H *has no* $4k$*-cycles if and only if* f^k *is a derangement. In particular, let* f *be a derangement and* $r > 2$ *be the smallest prime divisor of the order of* f. *Then,* $g(H) \geq 4r$. *So, if* f *has prime order* m, *then* $g(H) = 4m$.

Theorem 4

For $L > 1$ *the parity check matrix* $H = \begin{pmatrix} 1 & 1 & \dots & 1 \\ 1 & f^{i_1} & \dots & f^{i_L} \end{pmatrix}$ *has no* 4*-cycle if and only if* f^t *is a derangement for every* $t \in \mathcal{I}_\Delta$.

Conditions for $2k$-cycles: Case $J = 1$

Corollary 1

Suppose that f is a derangement of prime order $m = n$. Then H has no 4-cycle.

Example 1

We take $\mathcal{I} = \{0, 1, 4, 6, 12, 10, 15, 24\}$, so

$$\mathcal{I}_\Delta = \{\pm 1, \pm 2, \pm 3, \pm 4, \pm 5, \pm 6, \pm 8, \pm 9, \pm 10, \pm 11, \pm 12, \pm 14, \pm 15, \pm 18, \pm 20, \pm 23, \pm 24\}$$

Choosing f of order coprime to $2, 3, 5, 7, 11, 23$, H is free from 4-cycles. Choosing f to be a cycle of prime order, say $f = (1\ 2\ 3\ \ldots\ 17)$ gives a $(136, 103)$-code. We may also construct a $(208, 158)$-code with no 4-cycles using a non-cycle permutation, $f = (1\ 2\ \ldots\ 12\ 13) \cdot (14\ 15 \ldots\ 24\ 25\ 26)$.

Conditions for $2k$-cycles: Case $J = 1$

Theorem 5

For $L > 1$ $H = \begin{pmatrix} 1 & 1 & \dots & 1 \\ 1 & f^{i_1} & \dots & f^{i_L} \end{pmatrix}$ has no 8-cycle if and only if f^i is a derangement for every $i \in (\mathcal{I}_+)_\Delta$. In particular, if H has no 8-cycle then $\mathcal{I}$ is a B_2-set.

Corollary 2

If $J = 1$, $L > 1$, and f is a prime m-cycle, H has no 8-cycles if and only if $\mathcal{I}$ is a B_2-set.

Corollary 3

If $J = 1$, $L > 1$, and f is a prime m-cycle, $\mathcal{I}$ is an m-B_2 set $\implies$ $g(H) = 12$.

Conditions for $2k$-cycles: Case $J = 1$

Example 2

Consider $\mathcal{I} = \{0, 1, 4, 6, 13\}$. Then $\mathcal{I}_+ = \{0, 1, 2, 4, 5, 6, 7, 8, 10, 12, 13, 14, 17, 19, 26\}$ and $\mathcal{I}_\Delta = \{\pm 1, \pm 2, \pm 3, \pm 4, \pm 5, \pm 6, \pm 7, \pm 9, \pm 12, \pm 13\}$. Then $\mathcal{I}$ is a B_2-set (over $\mathbb{Z}$). Choosing any m coprime to $2, 3, 5, 7, 13, 17, 19$, we get that $0 \pmod m \notin \mathcal{I}_\Delta$ and $\mathcal{I}$ is an m-B_2 set. So H is free from 4-cycles. On the other hand, it is clear that $(\mathcal{I}_+)_\Delta$ is not a B_2-set. As a concrete example, f can be taken to be the 29-cycle, $f = (1\ 2\ 3\ 4\ \ldots\ 29)$. Then the parity check matrix $H = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & f^1 & f^4 & f^6 & f^{13} \end{pmatrix}$ has girth $g(H) = 8$. This gives a $(145, 88)$-code with girth 8.

Conditions for $2k$-cycles: Case $J > 1, L > 1$

Theorem 6

H contains no 4-cycle $\iff$ f^i is a derangement for all $i \in \mathcal{A}_\Delta \cdot \mathcal{I}_\Delta$.

Example 3

Take $\mathcal{A} = \{0, 1, -1\}$, so $\mathcal{A}_\Delta = \{-2, -1, 1, 2\}$. Here, $H = \begin{pmatrix} 1 & 1 & \dots & 1 \\ 1 & f^{i_1} & \dots & f^{i_L} \\ 1 & f^{-i_1} & \dots & f^{-i_L} \end{pmatrix}$. By Theorem 6, H has no 4-cycle if and only if f^i is a derangement for all $i \in \mathcal{I} \cup 2\mathcal{I} \cup \mathcal{I}_\Delta \cup 2\mathcal{I}_\Delta$. Take $\mathcal{I} = \{0, 2, 4, 6, 8\}$. Then $\mathcal{I}_\Delta = \{2, 4, 6, 8, -2, -4, -6, -8\}$, $2\mathcal{I} = \{4, 8, 12, 16\}$, $2\mathcal{I}_\Delta = \{4, 6, 8, 12, -4, -8, -12, -16\}$. Taking m to be a prime larger than 16 and f to be an m-cycle, we get $g(H) \geq 6$. E.g. with $f = (1\ 2\ 3\ \dots\ 17)$, H is a $(85, 52)$-code.

Conditions for $2k$-cycles: Case $J > 1$, $L > 1$

Theorem 7

If $J, L > 1$, then H contains no 6-cycles if and only if for distinct $j_1, j_2, j_3 \in \mathcal{I}$ and any $d_1, d_2 \in \mathcal{A}_\Delta$ such that $(d_1 + d_2) \in \mathcal{I}_\Delta$, $f^{d_1 j_1 + d_2 j_2 - (d_1+d_2) j_3}$ is a derangement. In particular, if f is a prime m-cycle and for any $d_1, d_2 \in \mathcal{A}_\Delta$ such that $(d_1 + d_2) \in \mathcal{A}_\Delta$, and distinct $j_1, j_2, j_3 \in \mathcal{I}$, we have $d_1 j_1 + d_2 j_2 \neq (d_1 + d_2) j_3 \mod m$, then H contains no 6-cycles.

Theorem 8

If $J,\ L > 1$ and $\mathcal{A}$ or $\mathcal{I}$ is not an m-$\mathcal{B}_2$ set then H contains an 8-cycle.

Conditions for $2k$-cycles: Case $J > 1, L > 1$

Example 4

Again, take $\mathcal{A} = \{0, 1, -1\}$, so $\mathcal{A}_\Delta = \{-2, -1, 1, 2\}$. Here, $H = \begin{pmatrix} 1 & 1 & \dots & 1 \\ 1 & f^{i_1} & \dots & f^{i_L} \\ 1 & f^{-i_1} & \dots & f^{-i_L} \end{pmatrix}$.

Let f be a prime m-cycle.

Then H has no 6-cycles if and only if $\mathcal{I} = \{0, i_1, \dots, i_L\}$ satisfies the following property: for distinct $j_1, j_2, j_3 \in \mathcal{I}$, we have $2j_1 = j_2 + j_3 \iff j_1 = j_2 = j_3$. For $\mathcal{I} = \{0, 1, 4, 6, 10\}$, $m = n = 17$, H has no 4-cycles. For all distinct $j_1, j_2, j_3 \in \mathcal{I}$, we have $j_1 + j_2 \neq 2j_3$. Thus, $H = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & f & f^4 & f^6 & f^{10} \\ 1 & f^{-1} & f^{-4} & f^{-6} & f^{-10} \end{pmatrix}$ has no 4- or 6-cycles.

However, by Theorem 8, it does have 8-cycles, since $\mathcal{A}$ is not an m-B_2 set, so it has girth $g(H) = 8$.

Thank you!