High-rate, short length, $(3, 3s)$-regular LDPC of girth 6 and 8

Michael E. O'Sullivan
Dept. of Mathematics and Statistics
San Diego State University
San Diego, CA 92182-7720
email: mosulliv@math.sdsu.edu

Roxana Smarandache
Dept. of Mathematics and Statistics
San Diego State University
San Diego, CA 92182-7720
email: rsmarand@math.sdsu.edu

Abstract — **This paper presents a simple construction of a class of LDPC codes generalizing [BHS01] and gives necessary and sufficient, easy to implement, conditions for avoiding $2m$ cycles, $m \geq 2$. The parity check matrix is formed by square blocks, with each block a sum of three permutation matrices, chosen such that the block is $(3,3)$ regular. The resulting codes have rate $(s-1)/s$.**

I. Construction of the check matrix

Let $n > 0$ be an integer. Let $F : r \mapsto a_F r + b_F \mod n$ be an affine map on $\mathbb{Z}_n$, with a_F coprime to n so that F is a permutation. We define the *affine permutation matrix*, $P^{(F)}$,

$$(P^{(F)})_{r,c} = \begin{cases} 1 & \text{if } a_F r + b_F \equiv c \pmod n \\ 0 & \text{else} \end{cases}$$

Let $s \geq 2$ be an integer and for $1 \leq i \leq s$ let F_i, G_i, H_i be affine permutations of $\mathbb{Z}_n$ such that $F_i(r)$, $G_i(r)$ and $H_i(r)$ are distinct for all $r \in \mathbb{Z}_n$. Let $X_i = P^{(F_i)} + P^{(G_i)} + P^{(H_i)}$. Then each X_i is $(3,3)$ regular. Let $Z = \begin{bmatrix} X_1 & X_2 & \ldots & X_s \end{bmatrix}^T$, and let C be the code with parity-check matrix Z. C is a regular $(3,3s)$ low-density parity-check code. When n is prime it may be assumed that a_{F_i}, a_{G_i}, a_{H_i}, are all 1 and that all F_i are the identity functions.

II. Conditions for cycles in an $n \times n$ matrix

A finite sequence $f_0, \ldots, f_{n-1}$ of elements of a set S is called a *swapping sequence from* S if $f_i \neq f_{i+1}$ for $i = 0, \ldots, n-1$. The sequence is *balanced* if for each $s \in S$ the sets $\{i \text{ odd} : f_i = s\}$ and $\{i \text{ even} : f_i = s\}$ have the same number of elements.

Proposition II.1 ([OS02]). *Let F, G, H and X be as above. Let R and C be copies of $\mathbb{Z}_n$ representing the set of rows and columns, respectively, of X. Then the sequence $r_0c_0r_1c_1r_2\ldots r_{m-1}c_{m-1}$, with $r_i \in R$ and $c_i \in C$, is a $2m$-cycle of the graph associated to X iff there exists a swapping sequence $f_0, f_1, f_2, \ldots, f_{2m-2}, f_{2m-1}$, from $\{F, G, H\}$, s.t. $f_{2k}(r_k) \equiv c_k \equiv f_{2k+1}(r_{k+1}) \pmod n$. If this is the case then $\sum_{k=0}^{m-1}(b_{2k+1} - b_{2k}) \prod_{i=0}^{k-1} a_{2i+1} \prod_{i=k+1}^{m-1} a_{2i} \equiv 0 \pmod n$.*

These congruences can be analyzed modulo each prime power dividing n. In particular, when n is prime, we get a simple condition ensuring no small cycles from unbalanced sequences.

Proposition II.2. *Let p be prime, F, G, H and X as above, and M a positive integer. Suppose that for all integers m, $1 < m \leq M$ and for all $0 < k < m$ with k coprime to m, $mx - ky - (m-k)z \not\equiv 0 \pmod p$, for x, y, z any permutation of b_F, b_G, b_H. Then the only cycles of length less than or equal to $2M$ in the graph of X are those arising from balanced sequences.*

The shortest balanced sequences are of the form $FGHFGH$, so for girth 6 the condition of the proposition is sufficient. For girth 8 we take $n = pq$ for p prime and $q = 3$. We choose $a_F \equiv a_G \equiv a_H \equiv 1 \mod p$ and enforce the conditions of the proposition. We take $a_F \equiv a_G \equiv 1 \mod 3$ and $a_H \equiv 2 \mod 3$. Then the girth of X is 8.

III. Construction of parity check matrices

For girth 6 we take $n = p$ a prime, F_i the identity function, $a_{G_i} = a_{H_i} = 1$, and we choose inductively b_{G_j} and b_{H_j} as follows (all computations in $\mathbb{Z}_p$):

$$b_{G_j} \notin D_j = \bigcup_{i<j} \{\pm(b_{F_i} - b_{G_i}), \pm(b_{G_i} - b_{H_i}), \pm(b_{H_i} - b_{F_i})\},$$

$$b_{H_j} \notin \{0, b_{G_j}, 2b_{G_j}, -b_{G_j}, b_{G_j}/2\},\ b_{H_j} \notin D_j,\ b_{H_j} - b_{G_j} \notin D_j.$$

s	rate	p	[*length*, *dimension*]
2	1/2	17	[34,17]
3	2/3	23	[69,46]
4	3/4	29	[116,87]
5	4/5	37	[185,148]
6	5/6	47	[282,235]
7	6/7	53	[371,318]
8	7/8	61	[488,427]

Table 1: Examples of $sp \times p$, $(3, 3s)$- regular graphs with girth 6.

The procedure for girth 8 is a bit more complicated. Some results are tabulated below.

s	rate	p	$n = 3p$	[*length*, *dimension*]
2	1/2	47	141	[282,141]
3	2/3	89	267	[801,534]
4	3/4	149	447	[1788,1341]

Table 2: Examples of $sp \times p$, $(3, 3s)$- regular graphs with girth 8.

References

[BHS01] J. Bond, S. Hui, and H. Schmidt. Linear-congruence construction of low-density check codes. In B. Marcus and J. Rosenthal, editors, *Codes, Systems and Graphical Models*, IMA Vol. 123, pages 83–100. Springer-Verlag, 2001.

[OS02] M. E. O'Sullivan, M. Greferath, R. Smarandache, Construction of LDPC codes from affine permutation matrices. In *Proceedings of the 40th Allerton Conference on Communication, Control and Computing*, 2002.