Construction of LDPC Codes from Affine Permutation Matrices

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

Marcus Greferath
Dept. of Mathematics and Statistics
San Diego State University
San Diego, CA 92182-7720
greferath@math.sdsu.edu

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

Abstract

One of the properties that undermines the performance of a low-density parity-check code is the existence of small cycles in the graph of the check matrix. We present an algebraic construction that, for relatively small n, creates $2n \times n$ low-density matrices with relatively large girth. The technique was introduced by Bond, Hui, and Schmidt and uses basic number theory. The parity check matrix is composed of blocks of square matrices. Each square matrix is a sum of permutation matrices which are defined by an affine equation over the integers mod n. We are able to determine algebraic inequalities in the parameters describing the affine equation that guarantee that the graph has no cycles of given size.

1 Introduction

Low-density parity-check (LDPC) codes have generated tremendous interest recently because of their performance near the Shannon limit under iterative decoding. One key parameter affecting the performance of an LDPC code is the girth of the incidence graph of the parity-check matrix. Graphs with large girth avoid the small cycles that undermine the effectiveness of the iterative decoding algorithm. Construction of good LDPC codes (with large girth, among other things) remains an interesting problem. One can discern two basic approaches to constructing codes, use random methods or systematic (e.g. algebraic or geometric) methods. This paper is a contribution to the systematic approach. We present a number theoretic technique for constructing matrices whose graph has large girth.

We briefly summarize some of the algebraic and geometric constructions of LDPC codes. The use of Cayley graphs of groups to construct LDPC codes was initiated by Margulis [Mar82, Mar88] and Lubotzky, Phillips, Sarnak [LPS88]. It was carried forward by Rosenthal and Vontobel [RV00] and Lafferty and Rockmore [LR00]. This construction provides matrices whose graphs have large girth, but the construction is somewhat limited since it is based on groups with optimal properties. The approach of Kou, Lin, Fossorier [KLF01] is to use incidence structure on affine and projective geometries. A problem with these codes is that the girth of the graph is only 6, unless some substantial changes are made to the basic construction. Vontobel and Tanner [VT01] use finite generalized polygons to construct LDPC codes. They derive lower bounds for the minimum distance of the resulting code. This method is limited by the existence of generalized polygons.

The method proposed here builds on the approach of Bond, Hui and Schmidt [BHS01]. The number theory involved is quite basic—the Chinese Remainder Theorem is the most advanced concept used—but the construction does involve a rather tedious derivation of parameters. The two key advantages are that relatively large girth (enough for a practical code) can be achieved for moderate n, and that the construction is more flexible than other methods.

2 The basic construction

Definition 2.1. Let $a, b \in \mathbb{Z}/n$ and consider the affine map on $\mathbb{Z}/n$, $F : r \mapsto ar + b \mod n$. We assume F defines a permutation of $\mathbb{Z}/n$, which is equivalent to assuming a is coprime to n. We define the *affine permutation matrix* $P^{(F)}$ by

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

We will also write the matrix as $P^{(a,b)}$.

The approach suggested by [BHS01] is to write a parity check matrix in blocks with each block being a sum of affine permutation matrices. For example, for a rate $(m-1)/m$ code, let $X_1, \dots, X_m$ be distinct $n \times n$ matrices each of which is the sum of permutation matrices. Use

$$Z = \begin{bmatrix} X_1 \\ X_2 \\ \cdots \\ \cdots \\ \cdots \\ X_m \end{bmatrix}$$

as the parity-check matrix.

We will consider the following two cases:

1. Let $F(r) = a_F r + b_F \mod n$; $G(r) = a_G r + b_G \mod n$; $H(r) = a_H r + b_H \mod n$; Consider a $(3, 3)$ regular $n \times n$ matrix X,

$$X = P^{(a_F,b_F)} + P^{(a_G,b_G)} + P^{(a_H,b_H)}$$

2. Let X and Y be constructed as in case 1.
   Consider a $(3, 6)$ regular $2n \times n$ matrix

$$Z = \begin{bmatrix} X \\ Y \end{bmatrix}$$

In the first case we have an $n \times n$ matrix, which will in general be nonsingular, so it is not of interest as a parity check matrix. But the conditions imposed to eliminate small cycles are best explained in that context.

Remark 2.2. Notice that the sum of three permutation matrices is not necessarily $(3,3)$-regular. To obtain regularity we must require that for any $r \in \mathbb{Z}/n$, $F(r)$, $G(r)$ and $H(r)$ are distinct.

Remark 2.3. Let R and C be copies of $\mathbb{Z}/n$ representing the set of rows and columns, respectively, of X. We may apply a change of variable on R to put the affine permutations defining the graph of X into a more convenient form. For example, let R' be another copy of $\mathbb{Z}/n$ and let $\phi : R' \to R$ be defined by $\phi(r') = \alpha r + \beta$. Let $F' = F \circ \phi$, so $F'(r') = a\alpha r' + a\beta + b$. Likewise define G' and H'. Let $X' = P^{(F')} + P^{(G')} + P^{(H')}$. The graph of X is isomorphic to the graph of X'. By choosing $\phi = F^{(-1)}$ we get F' is the identity function.

One can also apply a change of variable to C.

3 Conditions for the existence of cycles, $n \times n$ matrix

Let F, G, and H be affine permutations of $\mathbb{Z}/n$, and let $X = P^{(F)} + P^{(G)} + P^{(H)}$. Let R and C be copies of $\mathbb{Z}/n$ representing the set of rows and columns, respectively, of X. Suppose $r_0c_0r_1c_1r_2 \ldots r_{m-1}c_{m-1}$ is a $2m$-cycle of the graph associated to X, with $r_i \in R$ and $c_i \in C$. Then there exist $f_0, f_1, f_2, \ldots, f_{2m-2}, f_{2m-1}$, each in $\{F, G, H\}$, such that

$$f_{2k}(r_k) \equiv c_k \equiv f_{2k+1}(r_{k+1}) \mod n \tag{1}$$

Here $k = 0, \ldots, m-1$ and indices on r are computed modulo m, while indices on f are computed modulo $2m$. Furthermore, it must be the case that $f_{2k} \neq f_{2k+1}$. Otherwise we would have two distinct elements of $\mathbb{Z}/n$ both mapping to c_k under f_{2k}, violating the fact that f_{2k} is a permutation of $\mathbb{Z}/n$. Likewise, $f_{2k+1} \neq f_{2k+2}$, otherwise $c_k = f_{2k+1}(r_{k+1})$ would be congruent modulo n to $c_{k+1} = f_{2k+2}(r_{k+1})$, violating the assumption that $r_0c_0r_1c_1r_2 \ldots r_{m-1}c_{m-1}$ is a $2m$-cycle. This reasoning also shows that $f_{2m-1} \neq f_0$, which we consider a special case of the previous observation with $k = 2m-1$ and indices computed modulo $2m$. We will call a finite sequence $f_0, \ldots, f_{n-1}$ of elements of a set S such that $f_i \neq f_{i+1}$ for $i = 0, \ldots, n-1$, a *swapping sequence from S.*

Let $f_k(r) = a_k r + b_k$, so $(a_k, b_k) \in \{(a_F, b_F), (a_G, b_G), (a_H, b_H)\}$. We now rewrite equation (1), ignoring c_k, as

$$a_{2k}r_k + b_{2k} \equiv a_{2k+1}r_{k+1} + b_{2k+1} \mod n \tag{2}$$

This gives the following linear system modulo n.

$$\begin{bmatrix} a_0 & -a_1 & \ldots & 0 \\ 0 & a_2 & \ldots & 0 \\ 0 & 0 & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots \\ -a_{2m-1} & 0 & \ldots & a_{2m-2} \end{bmatrix} \begin{bmatrix} r_0 \\ r_1 \\ r_2 \\ \ldots \\ r_{m-1} \end{bmatrix} \equiv \begin{bmatrix} b_1 - b_0 \\ b_3 - b_2 \\ b_5 - b_4 \\ \ldots \\ b_{2m-1} - b_{2m-2} \end{bmatrix} \tag{3}$$

The left nullspace of the matrix is a free module of rank one and is spanned by the vector v with coordinates $v_k = \prod_{i=0}^{k-1} a_{2i+1} \prod_{i=k+1}^{m-1} a_{2i}$. The system has a solution only if the product of v and the right hand side of (3) is 0. That is

$$\sum_{k=0}^{m-1}(b_{2k+1}-b_{2k})\prod_{i=0}^{k-1}a_{2i+1}\prod_{i=k+1}^{m-1}a_{2i}\equiv 0 \mod n$$

Thus we have the following proposition:

Proposition 3.1. *Let F, G, and H be affine permutations of $\mathbb{Z}/n$, with $F(r)$, $G(r)$, $H(r)$ distinct for all $r \in \mathbb{Z}/n$. Let $X = P^{(a_F,b_F)} + P^{(a_G,b_G)} + P^{(a_H,b_H)}$. If there is a cycle of length $2m$ in the graph determined by X then there is a swapping sequence $(f_i) = f_0, f_1, f_2, \ldots, f_{2m-1}$ with each $f_i \in \{F, G, H\}$ such that*

$$\sum_{k=0}^{m-1}(b_{2k+1}-b_{2k})\prod_{i=0}^{k-1}a_{2i+1}\prod_{i=k+1}^{m-1}a_{2i}\equiv 0 \mod n \tag{4}$$

where $f_i(r) = a_i r + b_i$.

Therefore to ensure that there are no cycles of length $2m$ we choose (a_F, b_F), (a_G, b_G), and (a_H, b_H) so that (4) does not hold for any swapping sequence from $\{F, G, H\}$. By the Chinese remainder theorem, for a given sequence it is sufficient to show the congruence does not hold for some prime power dividing n.

4 The case where n is prime

We now consider the case where $n = p$ a prime. Recall from Remark 2.2 that to ensure regularity it must be the case that $F(r) \not\equiv G(r)$ for all $r \in \mathbb{Z}/p$. Since the congruence $a_F r + b_F \equiv a_G r + b_G \mod p$ always has a solution when $a_G \not\equiv a_F \mod p$—namely $r = (b_F - b_G)/(a_G - a_F)$—we are forced to assume that $a_G = a_F$. Similarly $a_H = a_F$. In fact, by Remark 2.3, we could assume without loss of generality that F is the identity and that $G(x) = x + 1$ (the latter involves applying a permutation to the columns).

Now equation (4) reduces to

$$\sum_{j\text{ odd}} b_j - \sum_{j\text{ even}} b_j \equiv 0 \mod p \tag{5}$$

Each b_i is one of b_F, b_G, or b_H, so we can rewrite the congruence as

$$s_F b_F + s_G b_G + s_H b_H \equiv 0 \mod p \tag{6}$$

where the integers s_F, s_G, and s_H satisfy

$$s_F + s_G + s_H = 0 \tag{7}$$

$$|s_F| + |s_G| + |s_H| \leq 2m \tag{8}$$

Example 4.1. Let $m = 2$. We seek to eliminate 4-cycles. The possible swapping sequences, up to renaming of variables are i) F, G, F, G; and ii) F, G, H, G. The first gives the congruence $2b_F - 2b_G \equiv 0 \mod p$. Presuming that $p > 2$ we get $b_F \neq b_G$. This imposes no new condition since we assume the permutations F, G and H are distinct. The second sequence gives the congruence $2b_F - b_G - b_H \equiv 0 \mod p$. Thus to eliminate 4-cycles we must choose b_F, b_G, and b_H such that $2x - y - z \not\equiv 0 \mod p$ for x, y, z any permutation of b_F, b_G, b_H. As noted earlier we may assume without loss of generality that $b_F = 0$ and $b_G = 1$. Thus we are led to $b_H \not\equiv 0, 1, 2, -1, 1/2 \mod p$.

Example 4.2. Let $m = 3$. We seek to eliminate 6-cycles. The possible swapping sequences, up to renaming of variables (and cyclic shift) can be classified by the number of occurrences of the variables.

i) F, G, F, G, F, G (no H);

ii) F, G, F, G, F, H (one H);

iii)F, G, F, H, G, H (two of each); and

iv) F, G, H, F, G, H (also two of each).

The resulting congruences are i) $3b_F \equiv 3b_G \mod p$; ii) $3b_F \equiv 2b_G + b_H \mod p$; iii) $2b_F + b_G \equiv b_G + 2b_H \mod p$; and iv)$b_F + b_G + b_H \equiv b_G + b_H + b_F \mod p$. The first (presuming $p > 3$) and third are the same restrictions as those imposed by eliminating 4-cycles. The third is new, imposing $3x - 2y - z \not\equiv 0 \mod p$ for x, y, z any permutation of b_F, b_G, b_H. The fourth sequence gives a condition that is an identity. In fact it is easy to show there is no way to avoid 6-cycles with this construction when n is prime.

Swapping sequences such as F, G, H, F, G, H which lead to an identity become fairly numerous as m increases. It should be clear that the following definition captures the property that leads to an identity in (5).

Definition 4.3. A swapping sequence of length $2m$ from a set S is called a *balanced sequence* 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.

The following proposition summarizes the observations of this section.

Proposition 4.4. *Let p be prime and let F, G, and H be distinct affine permutations of $\mathbb{Z}/p$ with the same linear term. Let $X = P^{(F)} + P^{(G)} + P^{(H)}$. Let M be a positive integer. Suppose that for all integers m satisfying $1 < m \leq M$ and for all positive $k < m$ with k coprime to m that*

$$mx - ky - (m - k)z \not\equiv 0 \mod p$$

for x, y, z a 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.

As a corollary we have the number of conditions imposed on b_H in terms of the other two.

Corollary 4.5. *Provided $p \geq -1 + 3\sum_{m=1}^{M} \phi(m)$, there exists a $p \times p$ matrix X in the form stated in the proposition such that the only cycles of length less than or equal to $2M$ in the graph of X are those arising from balanced sequences.*

PROOF: We have $b_H \not\equiv b_G$ and $b_H \not\equiv b_F$ modulo p. Then for each $m = 2, \ldots M$ and for each choice of x from $\{b_F, b_G, b_H\}$ there are $\phi(m)$ distinct congruences in the proposition, one for each choice of k coprime to p. Thus there are $2 + \sum_{m=2}^{M} \phi(m)$ conditions that p must satisfy. $\square$

5 The case where $n = pq$ for p, q primes

Let n be the product of two primes, p and q, and assume $X = P^{(F)} + P^{(G)} + P^{(H)}$ as previously. We will derive conditions on a_F, a_G, a_H, b_F, b_G and b_H to ensure that the graph of X has no cycles of length $2M$ or less. For any sequence $f_0, f_1, \ldots, f_{2m-1}$ we need to ensure that (4) does not hold. For unbalanced sequences we impose the condition of the last section. First,

$$a_F \equiv a_G \equiv a_H \mod p$$

Second, for x, y, z any permutation of b_F, b_G, b_H and for any m satisfying $1 < m \leq M$ and for all positive $k < m$ with k coprime to m,

$$mx - ky - (m-k)z \not\equiv 0 \mod p$$

Then the only possible cycles of length at most $2M$ in the graph of X occur from balanced sequences.

We are therefore led to the problem of classifying all balanced sequences and examining (4) for those sequences. We have not been able to find a general description of all such sequences, but we have classified them up to length 16. Up to cyclic shift and permutation of F, G, H those of length at most 14 are

$$\begin{array}{l}
F, G, H, F, G, H \\
F, G, F, G, H, F, G, F, G, H \\
F, G, H, F, G, H, F, G, H, F, G, H \\
F, G, H, F, G, H, G, F, H, G, F, H \\
F, G, F, G, H, F, H, F, G, H, G, H \\
F, G, F, G, F, G, H, F, G, F, G, F, G, H \\
F, G, F, G, F, H, G, F, H, F, H, F, G, H \\
F, G, F, H, F, G, H, F, G, F, H, F, G, H \\
F, G, F, H, F, G, H, F, H, F, G, F, G, H \\
F, H, F, G, F, G, H, F, H, F, G, F, G, H
\end{array}$$

The balanced sequences of length 16 are too numerous to list. The congruence (4) arising from F, G, H, F, G, H simplifies to

$$a_H(b_G - b_F) + a_G(b_F - b_H) + a_F(b_H - b_G) \equiv 0 \mod n$$

Reducing mod p this becomes an identity, so in order to ensure there are no 6 cycles we must impose

$$a_H \not\equiv \frac{a_G(b_F - b_H) + a_F(b_H - b_G)}{b_F - b_G} \mod q \tag{9}$$

If we assume (without loss of generality) that F is the identity function, this simplifies to

$$a_H \not\equiv b_G^{-1}(a_G b_H + b_G - b_H) \mod q \tag{10}$$

It turns out that all of the other balanced sequences that we have found lead to congruences with $a_H(b_G - b_F) + a_G(b_F - b_H) + a_F(b_H - b_G)$ as a factor. Therefore once the incongruence (9) is imposed the dependence on b_F, b_G and b_H factors out of the other congruences. This leaves a number of congruences involving a_F, a_G and a_H modulo q.

In the following examples we assume that F is the identity function and that $a_F \equiv a_G \equiv a_H \equiv 1 \mod p$. As noted in the previous section we can also assume that $b_F \equiv 1 \mod p$ without loss of generality.

Example 5.1. Let $M = 3$. We seek to eliminate all cycles of length 6 or less. We get $b_H \not\equiv -2, -1, -1/2, 0, 1, 2, 3, 1/2, 3/2, 1/3, 2/3 \mod p$ to eliminate cycles caused by unbalanced sequences. The condition imposed by (9), is $a_H \not\equiv 1 \mod q$. Since there are 11 conditions on b_H and just 2 on a_H (it can't be 0 modulo q) we can construct an $n \times n$ matrix X whose graph has girth at least 8 for any $n = pq$ with $p \geq 13$ and $q \geq 3$.

Example 5.2. Let $M = 5$. We seek to eliminate all cycles of length 10 or less. By Corollary 4.5 there are 29 conditions on b_H modulo p required to eliminate cycles of length at most 10 due to unbalanced sequences. Thus it is sufficient to choose $p \geq 31$. We also have the two conditions imposed on a_H discussed in the previous example. The balanced sequence $F, G, F, G, H, F, G, F, G, H$ imposes $x + y \not\equiv 0 \mod q$ for any choice of x and y from $\{F, G, H\}$. This gives altogether 4 conditions on a_H modulo q and it sufficient to choose $q \geq 5$. We can therefore achieve girth 12 by choosing $n = pq$ with $p \geq 31$ and $q \geq 5$.

Unfortunately the analysis of the larger girths gets tedious. We have not yet found a general formula describing the algebraic conditions imposed by the balanced sequences. For each choice of M, the balanced sequence must be classified and then the congruences (4) derived. We also have no proof that $a_H(b_G - b_F) + a_G(b_F - b_H) + a_F(b_H - b_G)$ is a factor of each of the congruences. Table 1 summarizes our findings.

girth	minimum p	minimum q	$n = pq$
6	7	1	7
8	13	3	39
10	19	3	57
12	31	5	155
14	37	7	259
16	59	17	1003

Table 1: Construction of an $n \times n$, $(3, 3)$- regular graph using a sum of 3 affine permutation matrices with given girth is guaranteed for $n = pq$ for primes p, q satisfying the bound shown.

6 Conditions for the existence of cycles, $2n \times n$ matrix

We now turn to the case of interest in coding: we consider a $2n \times n$ matrix $Z = [X, Y]^T$ with X and Y each the sum of three affine permutation matrices. Let F, G, H be the three permutations defining X and J, K, L the three permutations defining Y. Let R and R' be two copies of $\mathbb{Z}/n$ indexing the rows of X and the rows of Y, respectively, and let C index the columns.

Suppose $r_0c_0r_1c_1r_2\ldots r_{m-1}c_{m-1}$ is a $2m$-cycle of the graph associated to Z, with $r_i \in R\cup R'$ and $c_i \in C$. Then there exist $f_0, f_1, f_2, \ldots, f_{2m-2}, f_{2m-1}$ each in $\{F, G, H, J, K, L\}$ such that

$$f_{2k}(r_k) \equiv c_k \equiv f_{2k+1}(r_{k+1}) \mod n \tag{11}$$

As in the $n \times n$ case, $f_k \neq f_{k+1}$. We have one additional constraint. Since f_{2k-1} and f_{2k} both act on the same row, they must both be contained in $\{F, G, H\}$ or else they must both be contained in $\{J, K, L\}$.

We consider the case where n is the product of two distinct primes p and q (or $q = 1$ for girth 6). We work modulo p to eliminate cycles associated to unbalanced sequences and modulo q to eliminate cycles due to balanced sequences. We will assume $(3, 3)$ regularity for both X and Y. By applying permutations to R and R' as discussed in Remark 2.3 it may be assumed that a_F, a_G, a_H, a_J, a_K, and a_L are all congruent modulo p, in fact they can all be congruent to 1 mod p. In addition, we may assume both F and J are the identity functions.

The following procedures show how to choose b_F, b_G, b_H, b_J, b_K and b_L to ensure that there are no cycles of the stated size caused by unbalanced sequences.

- To eliminate 4-cycles it suffices to ensure that

  $$b - a \not\equiv x - y \mod p$$

  for a, b distinct elements of $\{F, G, H\}$ and x, y distinct elements of $\{J, K, L\}$.

- To eliminate 6-cycles it suffices to ensure, in addition, that

  $$\begin{aligned} b - a &\not\equiv 2x - 2y \mod p, \quad \text{and} \\ b - a &\not\equiv 2x - y - z \mod p \end{aligned}$$

  for a, b distinct elements of $\{F, G, H\}$ and x, y (and z in the second case) distinct elements of $\{J, K, L\}$ or vice-versa.

- To eliminate 8-cycles it suffices to ensure, in addition, that

  $$\begin{aligned} b - a &\not\equiv 3x - 3y \mod p, \\ b - a &\not\equiv 3x - 2y - z \mod p \quad \text{and} \\ 2b - 2a &\not\equiv 2x - y - z \mod p \end{aligned}$$

  for a, b distinct elements of $\{F, G, H\}$ and x, y (and z in the second and third case) distinct elements of $\{J, K, L\}$ or vice-versa.

Finally, we need to consider balanced sequences. The only balanced sequences of length 6 are chosen from one of the two sets $\{F, G, H\}$ or $\{J, K, L\}$. There are balanced sequences of length 8 with elements taken from both sets. They are all of the following form.

$$F, J, K, F, G, K, J, G$$

We avoid cycles associated to this sequence by imposing the following restriction:

$$(a_F - a_G)(a_J b_K - a_K b_J) \not\equiv (a_J - a_K)(a_F b_G - a_G b_F) \mod q$$

The code lengths for given girth that are achievable are summarized in the table.

girth	p	q	code length $2pq$
6	17	1	34
8	47	3	248
10	97	7	1358

Table 2: A rate 1/2, $(3,6)$-regular LDPC code with given girth can be constructed for length $n = 2pq$.

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.

[DPR02] C. Di, D. Proietti, T. Richardson, E. Telatar, and R. Urbanke. Finite length analysis of low density parity check codes. *IEEE Trans. Inform. Theory*, 48(6):1570–1579, 2002.

[KLF01] Y. Kou, S. Lin, and M. P. C. Fossorier. Low density parity check codes based on finite geometries: A rediscovery and new results. *IEEE Trans. Inform. Theory*, 47(7):2711-2736, 2001.

[LR00] J. Lafferty and D. Rockmore, *Codes and iterative decoding on algebraic expander graphs*, In the Proceedings of ISITA 2000, Honolulu, Hawaii, available at http://www.cs.cmu.edu/afs/cs.cmu.edu/user/lafferty/www/, November 2000.

[LPS88] A. Lubotzky, R. Phillips, and P. Sarnak. Ramanujan graphs. *Combinatorica*, 8(3):261–277, 1988.

[Mar82] G. A. Margulis. Explicit constructions of graphs without short cycles and low density codes. *Combinatorica*, 2(1):71–78, 1982.

[Mar88] G. A. Margulis. Explicit group-theoretic constructions of combinatorial schemes and their applications in the construction of expanders and concentrators. *Problems Inform. Transmission*, 24(1):39–46, 1988. Translation from Problemy Peredachi Informatsii.

[RV00] J. Rosenthal and P. O. Vontobel. Constructions of LDPC codes using Ramanujan graphs and ideas from Margulis. In *Proc. of the 38-th Allerton Conference on Communication, Control, and Computing*, pages 248–257, 2000.

[Wib96] N. Wiberg. *Codes and Decoding on General Graphs.* PhD thesis, Linköping University, Sweden, 1996.

[VT01] P. O. Vontobel and R. M. Tanner, Construction of Codes Based on Finite Generalized Quadrangles for Iterative Decoding. *Proc. IEEE Intern. Symp. on Inform. Theory*, Washington, D.C., USA, p. 223, 2001