On LDPC Codes from $(0,1)$-Geometries Induced by Finite Inversive Spaces of Even Order

Mark Flanagan, Marcus Greferath, and Cornelia Roessing

Claude-Shannon-Insitute for Discrete Mathematics,
Coding, and Cryptography

and the School of Mathematical Sciences
University College Dublin

Abstract. Low Density Parity Check (LDPC) codes have enjoyed increasing interest during recent years. In general these are described in the terminology of sparse bipartite graphs containing no 4-cycles, but an alternative way to deal with them are a particular class of incidence structures, namely partial linear spaces. This paper shows how to obtain a large class of partial linear spaces from inversive spaces and show via simulation that the induced LDPC codes have good error-correcting performance.

Keywords: Inversive space, pencil, (α,β)-geometry, LDPC code.

Introduction

Inversive spaces (also known as Möbius spaces), belong to the class of circle-geometries, or 3-designs in the language of design theory. These are structures consisting of points and circles (rather than lines) where any 3 distinct points are incident with a unique circle. In addition to this, the set of circles is equipped with with a relation *touching*, which is reflexive and symmetric. If two distinct circles c and d are touching, then they intersect in a unique point p, and we say that c and d touch in p. A set of circles touching each other in a given point is called a pencil.

A partial linear space is an incidence structure consisting of points and lines, such that every point is contained in the same number of lines, and

every pair of distinct points is contained in at most one line. A $(0,1)$-geometry is a partial linear space in which for every antiflag (p,g) the number of points on g that are collinear with p can take only two values, 0 or 1. Given an inversive space $\mathbb{M}$ of order q, we will form a new incidence structure, the points of which are the pencils of $\mathbb{M}$, and the lines of which are the circles of $\mathbb{M}$. If $\mathbb{M}$ is of even order, then it can be seen that this incidence structure is indeed an $(0,1)$-geometry. In geometric terms, the induced partial linear space contains no triangles, and in graph theoretic terms, the incidence graph does not contain n-cycles for $n \leq 6$.

Low Density Parity Check (LDPC) codes, although discovered early in the history of coding theory [7], have attracted the attention of many coding theorists during the recent years due to their rediscovery by MacKay [10]. They form a class of linear block codes that perform close to the Shannon limit and allows for efficient decoding using what is called belief propagation algorithms. It has been observed that random constructions of LDPC codes seem generally superior to systematic constructions, however in order to make storage and encoding for these codes practical there is a need for systematic constructions.

LDPC codes have been systematically constructed in various ways. Margulis [11] initiated the use of a Cayley graph of a group to construct a sparse bipartite graph which in turn induces an LDPC code once one writes down the incidence matrix of the graph. Further work has been done by Rosenthal and Vontobel [15,16] and Lafferty and Rockmore [9]. In both cases Ramanujan graphs, which are optimal relative to a certain expansion property, were constructed using the Cayley graph of a suitable group.

Another interesting approach is due to Bond, Hui and Schmidt [4] and later Greferath, O'Sullivan and Smarandache [13]. In all these constructions, linear congruences are used to relate the row and column numbers of the nonzeroentries of a sparse parity-check matrix. Simulation results have shown that the codes constructed using this method perform at least as well as the randomly generated low-density parity-check codes.

Geometric approaches can also be used in the construction of LDPC codes: for example, Vontobel and Tanner [17] discovered a way to use finite generalized polygons (FGPs) to construct Tanner graphs and LDPC

codes. This associated graph has the property that the girth is exactly twice the diameter which is the largest possible. Another construction was proposed by Kou, Lin and Fossorier [8] and makes use of the general concept of incidence structures. In [8] the underlying incidence structures were either affine or projective spaces over the finite field $\mathbb{F}_{2^s}$. The approach in [17] can be viewed on the same concept, namely that the occuring points are points of a projective space and the lines form a subset of the lines in that space determined by a bilinear form. By exploiting quadratic forms in such spaces, comparable work has been done recently in papers by Mellinger and Storme [12].

This paper's goal is to bring together circle geometries, $(0,1)$-geometries and LDPC codes. We start with inversive spaces of even order and derive the mentioned class of $(0,1)$-geometries. The incidence matrices of these then form check matrices of LDPC codes. We finally test the performance of a number of such codes in simulations, and present the results in waterfall diagrams.

1 LDPC codes and (α, β)-geometries

An *incidence structure* is a pair $\mathbb{I} = (P, B)$ where P is a set of *points* and $B \subseteq 2^P$ is a set of *blocks*. The incidence matrix of such an incidence structure is a binary $|P| \times |B|$-matrix the entries of which represent the incidence between points and blocks. If such an incidence matrix is sparse then it can be used as a check matrix for a low-density parity-check code.

We will now explain what partial linear spaces are, and how we can construct classes of these from inversive spaces. We will then analyze these partial linear spaces and find that they belong to the class of so-called $(0,1)$-geometries.

Definition 1. *An* partial linear space *or order* $(s,t) \in \mathbb{N}^2$ *is an incidence structure* $\mathbb{S} := (P, L)$ *where* P *is a set of* points *and* $L \subseteq 2^P$ *is a set of* lines *satisfying the following axioms:*

- **(i)** *Every line contains exactly* $s+1$ *points.*
- **(ii)** *Every point of* $\mathbb{S}$ *is contained in exactly* $t+1$ *lines.*
- **(iii)** *Two points of* $\mathbb{S}$ *are contained in at most one line.*

Partial linear spaces have enjoyed intensive investigation during the last decade (cf. [5]). A famous class of partial linear spaces form the so-called *generalised quadrangles*. Like the structures that we are going to discuss here, these quadrangles have played a role in the construction of Low-Density Parity-Check codes (cf. [17]).

Definition 2. *A partial linear space* $\mathbb{S} = (P, L)$ *is called an* (α, β)*-geometry if whenever* (p, ℓ) *is a non-incident point-line pair (*antiflag*) there are either* α *or* β *points on* ℓ *which are collinear with* p*.*

The generalised quadrangles we mentioned above form a class of $(1, 1)$-geometries. Obviously, in an (α, β)-geometry there do not exist any triangles if and only if α and β are at most 1. The bipartite graph whose adjacency matrix is build from the incidence matrix of these geometries then has a girth that is lower bounded by 8. This is known to be an important premise for the performance of the derived LDPC code.

2 Inversive spaces

We will first recall the notion of an inversive space and list all properties that we need for this article. These properties are known and can be found in most standard texts on finite geometry; as they are neither new nor our own results we will quote them as remarkss rather than lemmas, propositions, or theorems.

An *incidence structure* is a pair $\mathbb{I} = (P, B)$ where P is a set of *points* and $B \subseteq 2^P$ is a set of *blocks*. For any point $p \in P$ we define a new incidence structure $\mathbb{I}_p := (P_p, C_p)$ where

$$P_p := P \setminus \{p\}$$
$$C_p := \{c \setminus \{p\} \mid c \in C \text{ and } p \in c\}$$

Then $\mathbb{I}_p$ is called the *internal structure* of $\mathbb{I}$ with respect to p.

Definition 3. *An* inversive space *is an incidence structure* $\mathbb{M} := (P, C)$*, here the blocks are called* circles *such that the following are satisfied:*

(i) *Any three distinct points are contained in exactly one circle.*

(ii) *For every point* $p \in P$ *the internal structure* $\mathbb{M}_p$ *is an affine space.*

The following statements can be derived using elementary counting principles.

Remark 1. Let $\mathbb{M} = (P, C)$ be an inversive space. There exist non-negative integers q and n such that the following hold.

(a) All circles of $\mathbb{M}$ contain $q+1$ points.

(b) $\mathbb{M}$ contains exactly q^n+1 points. Each point is incident with exactly $q^{n-1}\frac{q^n-1}{q-1}$ circles, and for this reason $\mathbb{M}$ contains $q^{n-1}\frac{q^{2n}-1}{q^2-1}$ circles.

(c) $\mathbb{M}$ forms a 3-design with parameters $(q^n+1, q+1, 1)$.

Remark 2. **(a)** In the preceding remark we say q is the *order* of $\mathbb{M}$, and n is its *dimension*.

(b) For dimension 2 the above definition reduces to the definition of an *inversive plane*, an incidence structure where two circles are touching if and only if they are equal or share a unique common point.

We have a simple algebraic construction of a large class of inversive spaces in terms of suitable field extensions.

Example 1. Let $L : K$ be a field extension of degree $n \geq 2$, and let $\alpha \in L \setminus K$. The embedding of K into L induces a natural embedding of the projective line $\mathbb{P}(K^2)$ into $\mathbb{P}(L^2)$. We define an incidence structure $\mathbb{M}(L:K) := (P, C)$ by

$$P := \{L(x,y) \mid (x,y) \in L^2 \setminus \{(0,0)\}\}$$
$$C := \{c_0^\gamma \mid \gamma \in \mathrm{PGL}(L,2)\}$$

where $c_0 = \{L(x,y) \mid (x,y) \in K^2 \setminus \{(0,0)\}\}$ and $\mathrm{PGL}(L,2)$ is the projective general linear group of rank 2 over L. Then $\mathbb{M}(L:K)$ is an inversive space of dimension n.

Remark 3. Again, for dimension 2 this reduces to a known construction for Miquelian inversive planes.

3 Pencils and partial pencils in inversive spaces

Definition 4. *Let $\mathbb{M} = (P, C)$ be an inversive space of order q and dimension n, and let (p, c) be an incident point-circle pair. The set $\pi(p, c)$ of all circles touching c in p is called a* pencil *of $\mathbb{M}$. Point p is called the carrier of $\pi(p, c)$, and every pencil is uniquely defined by its carrier and any one of its circles.*

Remark 4. If (p, c) is an incident point-circle pair of $\mathbb{M}$ then $\pi(p, c)$ restricts to a parallel class of lines in $\mathbb{M}_p$. The number of circles in $\pi(p, c)$ is hence given by q^{n-1}.

Remark 5. Let $\mathbb{M}$ be an inversive space of order q and dimension n.

(a) Every point of $\mathbb{M}$ is a carrier of $\frac{q^n-1}{q-1}$ different pencils.

(b) There are $\frac{q^n-1}{q-1}(q^n+1)$ different pencils in $\mathbb{M}$.

(c) Every circle of $\mathbb{M}$ is a member of $q+1$ pencils.

(d) Two distinct pencils in $\mathbb{M}$ have at most one circle in common.

Let $\mathbb{M} = (P, C)$ be an inversive space, and let p be a point incident with a circle c. As mentioned above the set

$$\pi \;:=\; \{c \setminus \{p\} \mid c \in \pi(p, c)\}$$

forms a full class of parallel lines in $\mathbb{M}_p$. The following remark naturally yields the definition of what we will call a partial pencil.

Lemma 1. *Let $\mathbb{M} = (P, C)$ be an inversive space of order q, let p be one of its points, and let U be an affine subspace of dimension $m \geq 1$ of $\mathbb{M}_p$. For a circle c that contains p consider*

$$\pi_U(p, c) \;:=\; \{d \in \pi(p, c) \mid d \setminus \{p\} \subseteq U\}.$$

If $\pi_U(p, c) \neq \emptyset$ then it contains q^{m-1} elements.

Proof: In $\mathbb{M}_p$ the set $\{d \setminus \{p\} \mid d \in \pi(p, c)\}$ forms a full parallel class of lines. If U is an m-dimensional affine subspace of $\mathbb{M}_p$, then either no lines of this class are fully contained in U, or exactly q^{m-1} such lines.

□

Definition 5. *In an inversive space* $\mathbb{M}$ *let* p *be a point and* c *be a circle such that* $p \in c$. *A subset* $\sigma \subset \pi(p,c)$ *is called a* partial pencil of degree m, *if there is an* m*-dimensional affine subspace of* $\mathbb{M}_p$ *such that* $\sigma = \pi_U(p,c)$.

Remark 6. **(a)** In an n-dimensional inversive space every pencil is a partial pencil of degree n.

(b) For every circle c of an inversive space, the set $\{c\}$ is a partial pencil of degree 1.

Remark 7. Let $\mathbb{M}$ be an inversive space of order q and dimension n.

(a) Every point of $\mathbb{M}$ is a carrier of $\frac{q^n-1}{q-1}$ different pencils of degree m.

(b) There are $\frac{q^n-1}{q-1}\,q^{n-m}(q^n+1)$ distinct pencils of degree m in $\mathbb{M}$.

(c) Every circle of $\mathbb{M}$ is a member of $q+1$ pencils of degree m.

(d) Two distinct pencils of same degree in $\mathbb{M}$ have at most one circle in common.

Remark 8. Let $\mathbb{M}$ be an inversive space of even order. If π is a (partial) pencil in $\mathbb{M}$ and c a circle that does not belong to π, then there exists at most one circle $d \in \pi$ that touches c.

Proof: An equivalent statement is: there do not exist three circles in $\mathbb{M}$ which touch eachother pairwise in different points. For this statement we refer to Qvist [14] (cf. also [1,2,6]). □

4 The main construction and some performance examples

We now come to our main construction: we will use an inversive space of even order to construct a particular $(0,1)$-geometry.

Theorem 1. *Let* $\mathbb{M} = (P, C)$ *be an inversive space of even order. We define an incidence structure* $\mathbb{S} := (\Pi_m, C)$ *by*

$$\Pi_m := \{\pi \mid \pi \text{ is a partial pencil of degree } m \text{ in } \mathbb{M}\},$$

where $\pi \in \Pi_m$ *is incident with* $c \in C$ *if and only if* $c \in \pi$. *Then* $\mathbb{S}$ *is a* $(0,1)$*-geometry of order* $(q-1, q^{m-1}-1)$.

Proof : This follows directly from prop. 7 and prop. 8. □

We will base the LDPC codes discussed in the following on the inversive space constructed in example 1. In the case of even order we form $(0,1)$-geometries $\mathbb{S}$ as in the previous section and derive a parity-check matrix directly as the incidence matrix of $\mathbb{S}$. Note that the properties of these LDPC codes result from the structure of the given inversive space; non-isomorphic classes of inversive spaces might give rise to differently behaving LDPC codes.

Now, we first observe that the number of lines in the $(0,1)$-geometry $\mathbb{S}$ is equal to

$$b \;=\; \frac{q^{2n}-1}{q^2-1}\,q^{n-1}$$

and the number of partial pencils of degree m is given by

$$v \;=\; \frac{q^{n}-1}{q-1}\,q^{n-m}(q^n+1).$$

The ratio of these quantities is $b/v = \frac{q^{m-1}}{q+1}$, and, as can be seen, this ratio is greater than 1 if and only if $m \geq 3$. Therefore, if $m = 2$, we take the parity-check matrix to be the incidence matrix of $\mathbb{S}$; this LDPC code has length v and a target rate of $1 - b/v = 1/(q+1)$. If $m \geq 3$, we take the parity-check matrix to be the transpose of the incidence matrix of $\mathbb{S}$; this LDPC code has length b and a target rate of $1 - v/b = 1 - \frac{q+1}{q^{m-1}}$.

Next, error correcting performance is demonstrated for LDPC codes derived from the incidence matrices of $(0,1)$-geometries that we have introduced. BPSK transmission over the AWGN channel was assumed, and in each case decoding continued until either a valid codeword was detected (via syndrome check) or a maximum of 64 iterations were completed.

In each case at least 100 frame errors were simulated for each point to determine bit error rate. The binary-input AWGN channel Shannon limit for the each code rate is also shown in each figure; this was evaluated by numerical integration. For all constructions we take the order of $\mathbb{M}$ to be $q = 2$.

The first set of results is for LDPC codes constructed using inversive spaces of dimension $n = 4$. Setting $m = 3$ yields a 510×680 parity check matrix with rank 466. The Tanner graph has a girth of 10 and a diameter of 12. The bit error rate (BER) performance of this $(680, 214)$

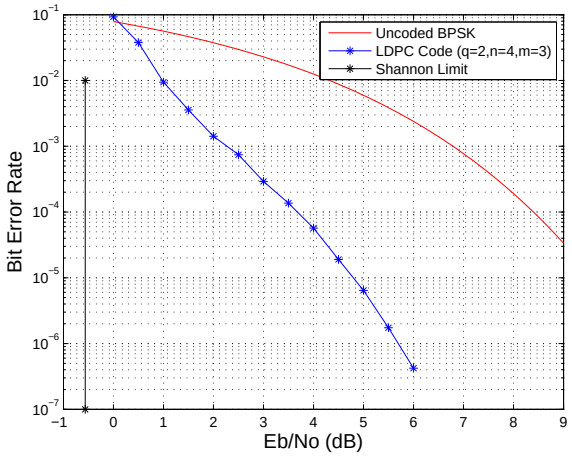

Fig. 1. Error performance of the $(680, 214)$ LDPC code constructed using the $(0, 1)$-geometry induced by the inversive space of order $q = 2$ with parameters $n = 4$, $m = 3$.

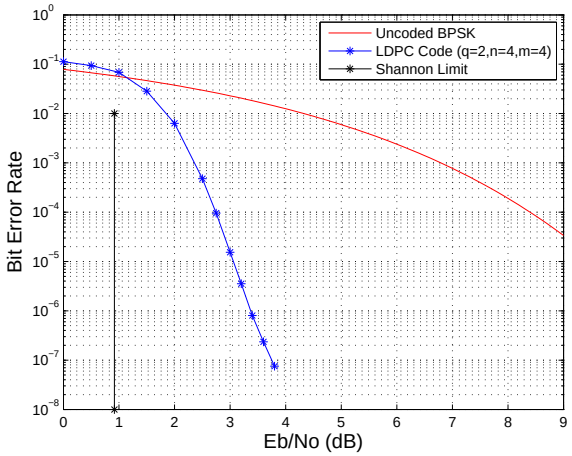

Fig. 2. Error performance of the $(680, 437)$ LDPC code constructed using the $(0, 1)$-geometry induced by the inversive space of order $q = 2$ with parameters $n = 4$, $m = 3$.

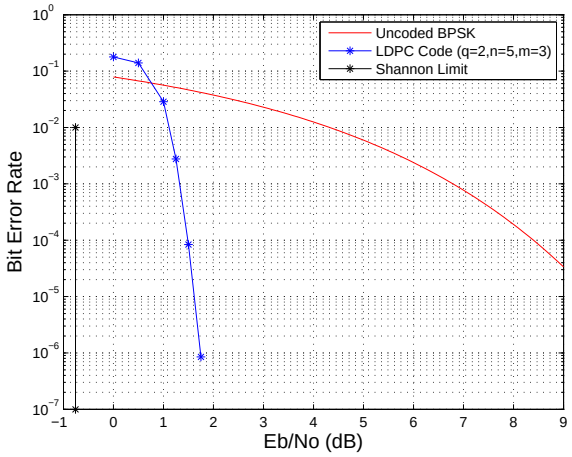

Fig. 3. Error performance of the $(5456, 1420)$ LDPC code constructed using the $(0, 1)$ -geometry induced by the inversive space of order $q = 2$ with parameters $n = 5$, $m = 3$.

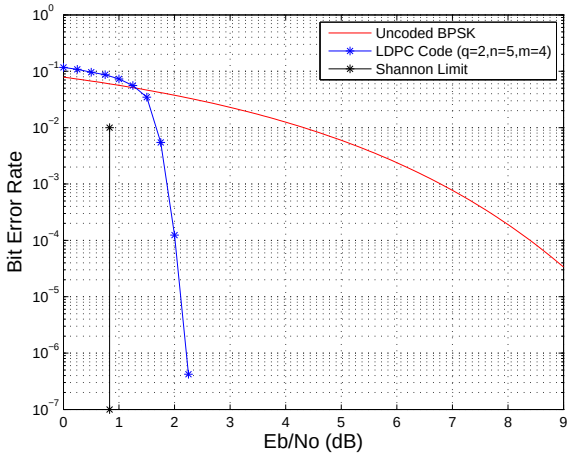

Fig. 4. Error performance of the $(5456, 3425)$ LDPC code constructed using the $(0, 1)$ -geometry induced by the inversive space of order $q = 2$ with parameters $n = 5$, $m = 4$.

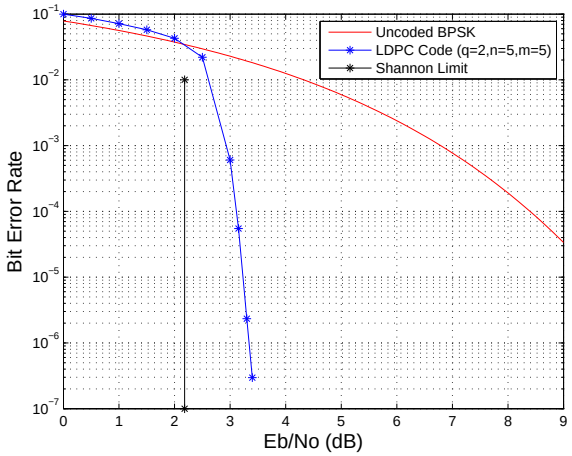

Fig. 5. Error performance of the $(5456, 4448)$ LDPC code constructed using the $(0, 1)$ -geometry induced by the inversive space of order $q = 2$ with parameters $n = 5$, $m = 5$.

LDPC code is shown in figure 1. Setting $m = 4$ yields a 255×680 parity check matrix with rank 243 . The Tanner graph has a girth of 10 and a diameter of 6 . The bit error rate (BER) performance of this $(680, 437)$ LDPC code is shown in figure 2.

The second set of results is for LDPC codes constructed using inversive spaces of dimension $n = 5$. Setting $m = 3$ yields a 4092×5456 parity check matrix with rank 4036 . The Tanner graph has a girth of 14 and a diameter of 14 . The BER performance of this $(5456, 1420)$ LDPC code is shown in figure 3. It may be seen that the performance of this code is 2.50 dB from the Shannon limit at a BER of 10^{-6} . Setting $m = 4$ yields a 2046×5456 parity check matrix with rank 2031 . The Tanner graph has a girth of 10 and a diameter of 10 . The bit error rate (BER) performance of this $(5456, 3425)$ LDPC code is shown in figure 4. The performance of this code is within 1.38 dB of the Shannon limit at a BER of 10^{-6} . Finally, setting $m = 5$ yields a 1023×5456 parity check matrix with a rank of 1008 . The Tanner graph has a girth of 10 and a diameter of 6 . The bit error rate (BER) performance of this $(5456, 4448)$ LDPC code is shown in figure 5. The performance of this code is 1.15 dB from the Shannon limit at a BER of 10^{-6} .

References

1. A. Beutelspacher: Einführung in die endliche Geometrie. B.I.- Wissenschaftsverlag, Mannheim, 1983.
2. A. Beutelspacher, U. Rosenbaum: Projective Geometry: From foundations to applications. Verlag Vieweg, Wiesbaden, 1992.
3. W. Benz: Geometrie der Algebren. Springer-Verlag, Berlin-Heidelberg-New-York, 1973.
4. J. Bond, S. Hui, and H. Schmidt, "Linear-congruence constructions of low-density parity-check codes," in *Codes, systems, and graphical models (Minneapolis, MN, 1999)*, vol. 123 of *IMA Vol. Math. Appl.*, pp. 83–100, New York: Springer, 2001.
5. F. de Clerck, H. van Maldeghem: Some classes of rank 2 geometries. In: F. Buekenhout, *Handbook of Incidence Geometry*. North-Holland, Amsterdam 1995, 433–475.
6. P. Dembowski: Finite Geometries. Ergebnisse der Mathematik und ihrer Grenzgebiete, Band 44, Springer-Verlag, Berlin, 1968.
7. R. G. Gallager, "Low density parity check codes," 1963. PhD Thesis, MIT press, Cambridge ,MA, 1963.
8. Y. Kou, S. Lin, and M. P. C. Fossorier, "Low density parity check codes based on finite geometries: A rediscovery and new results." Preprint, 2001.
9. J. D. Lafferty and D. N. Rockmore, "Codes and iterative decoding on algebraic expander graphs," in *Proceedings of the ISIT-A 2000*, 2000.
10. D. J. C.MacKay and R. M. Neal, "Good codes base on very sparse matrices," in *Cryptography and Coding, 5th IMA Conference*, pp. 100–111, Dec. 1995.
11. G. A. Margulis, "Explicit constructions of graphs without short cycles and low density codes," *Combinatorica*, vol. 2, no. 1, pp. 71–78, 1982.
12. K. E. Mellinger, "LDPC codes from triangle-free line sets," *Des. Codes Cryptogr.*, vol. 32, no. 1-3, pp. 341–350, 2004.
13. M. O'Sullivan, M. Greferath, and R. Smarandache, "Construction of ldpc codes from affine permutation matrices," in *Proceedings of the 40th Annual Allerton Fonference on Communication, Control and Computing*, 2002.
14. B. Qvist, "Some remarks concerning curves of the second degree in a finite plane," *Ann. Acad. Sci. Fenn*, **134** (1952).
15. 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*, pp. 248–257, 2000.
16. J. Rosenthal and P. O. Vontobel, "Constructions of regular and irregular LDPC codes using Ramanujan graphs and ideas from Margulis," in *Proceedings of the 2001 IEEE International Symposium on Information Theory*, p. 4, 2001.
17. P. O. Vontobel and R. M. Tanner, "Construction of codes based on finite generalized quadrangles for iterative decoding," in *Proc. IEEE Intern. Symp. on Inform. Theory, Washington, D.C., USA*, p. 223, 2001.