RZ 3299 (# 93345) 12/11/00
Electrical Engineering 11 pages

# Research Report

## Construction of Steiner Systems and High-Rate Low-Density Parity-Check Codes

T. Mittelholzer

IBM Research
Zurich Research Laboratory
Säumerstrasse 4
8803 Rüschlikon
Switzerland
Email: tmi@zurich.ibm.com

# Construction of Steiner Systems and High-Rate Low-Density Parity-Check Codes

T. Mittelholzer

*IBM Research, Zurich Research Laboratory, 8803 Rüschlikon, Switzerland*
*Email: tmi@zurich.ibm.com*

## Abstract

Starting from a finite projective plane, a simple construction of low-density parity check (LDPC) matrices is presented. The factor graphs associated with these LDPC matrices have no 4-cycles due to the incident structure of lines and points in the projective plane. Furthermore, two constructions are proposed to combine suitably sized smaller LDPC matrices into a larger LDPC matrix. These constructions can be used to obtain infinite sequences of Steiner systems of any block size, which are 2-designs.

**Index terms:** Finite geometries, Steiner systems, low-density parity-check (LDPC) codes

# 1 Introduction

Low-density parity-check (LDPC) codes, introduced by Gallager [1] some four decades ago, have recently attracted much interest due to their outstanding performance when decoded by the sum-product algorithm [2]. Numerous papers report on performance results of codes from sparse parity-check matrices and an on-line repository of such codes has been set up [3]. Typically, LDPC matrices are constructed by a random process and, therefore, the description length of these matrices is rather long.

In this paper, deterministic constructions of LDPC matrices are presented. The corresponding factor graphs of these LDPC matrices have no 4-cycles, which is desirable for an efficient decoding with the sum-product algorithm. High-rate 4-cycle free binary LDPC matrices with fixed column weight $j$ and row weight $k$ only exist if their rate satisfies a combinatorial bound [4], which is related to the number of blocks in a Steiner system. The proposed constructions can produce 4-cycle-free LDPC matrices of maximum lengths, which are Steiner systems.

The main construction relies on geometric properties of points and lines in the projective plane over a finite field or ring. Some basic results on the projective plane are summarized in Section 2. Section 3 presents a construction of LDPC matrices that are obtained as incidence matrices from points and lines from the projective plane. In Section 4, a method for constructing larger LDPC matrices from smaller LDPC matrices is presented, which can be used to obtain Steiner systems, as shown in Section 5. In the last section, simulation results are shown that compare the performance of some deterministically and randomly constructed LDPC codes.

# 2 The Projective Plane

Let $\mathbf{F}$ be a finite field of cardinality $q$. The "points" of the projective plane $\mathbf{P}^2(\mathbf{F})$ are the 1-dimensional subspaces in $\mathbf{F}^3$ (cf. Chap. 6.7 in [5]). A point $P$ is specified by a tripel of coordinates $\mathbf{x} = (x_1, x_2, x_3)$, which are not all zero. Since $\mathbf{x}$ is non-zero, it defines a 1-dimensional subspace. Every non-zero multiple of $\mathbf{x}$ defines the same point. Hence, two tripels $(x_1, x_2, x_3)$ and $(x'_1, x'_2, x'_3)$ determine the same point $P$ if and only if one is a non-zero multiple of the other. There are $(q^3 - 1)/(q - 1) = q^2 + q + 1$ points, i.e., 1-dimensional subspaces, in $\mathbf{P}^2(\mathbf{F})$.

The "lines" of the projective plane are all the 2-dimensional subspaces in $\mathbf{F}^3$. A line $l$ is characterized by a linear equation, i.e., the line is the 2-dimensional kernel of

$$\lambda(\mathbf{x}) \triangleq \lambda_1 x_1 + \lambda_2 x_2 + \lambda_3 x_3 = 0, \tag{1}$$

where the coefficients $\lambda_i$ are not all zero. In the same way as points, the line $l$ is determined by the tripel of coefficients $(\lambda_1, \lambda_2, \lambda_3)$ and a non-zero multiple of these coefficents determines the same line. There are $q^2 + q + 1$ lines in $\mathbf{P}^2(\mathbf{F})$.

The points and lines satisfy some incidence relations. We say that a point $P$ is incident with (or contained in) the line $l$ if the 1-dimensional subspace determined by $P$ is contained in the 2-dimensional subspace corresponding to $l$ or, equivalently, if $\lambda(\mathbf{x}) = 0$.

The projective plane has some desirable regularity properties (e.g., Chap. 10.3 in [6]):

- Every point lies on $q + 1$ lines.

- Every line containes $q+1$ points.
- Two lines meet in exactly 1 point.
- There is exactly one line that goes through two different points.

# 3 Construction of LDPC Matrices from the Projective Plane

Let $X$ be a subset of points and let $L$ be a subset of all lines from $\mathbf{P}^2(\mathbf{F})$. We will denote the cardinalities of these two sets by $m = |X|$ and $n = |L|$ and we will choose some ordering $P_1, P_2, \ldots, P_m$ of the points in $X$ and an ordering $l_1, l_2, \ldots, l_n$ for the lines in $L$. The *incidence matrix* of these sets of lines and points is a binary $m \times n$-matrix $H$, whose entries $h_{ij}$ are defined as follows:

$$h_{ij} = \begin{cases} 1 & \text{if } P_i \text{ is incident with } l_j \\ 0 & \text{otherwise .} \end{cases} \tag{2}$$

Due to the regularity properties of $\mathbf{P}^2(\mathbf{F})$, the matrix $H$ has no 4-cycles, i.e., any two points (two rows) are checked at most by one line (column). This is a desirable property for iterative decoding of LDPC codes. Note that the matrix $H$ will not have full rank, in general.

In the remaining part of this section, it will be shown how to construct parity-check matrices with a strong regularity property, namely, all rows will have the same number of ones, usually denoted by $k$ and all columns will also have a fixed number of ones, denoted by $j$ [1][1]. Such a regular matrix will be called a $(j,k)$ *matrix*. A $(j,k)$ matrix $H$ of size $m \times n$ is said to have a *band structure* with $j$ bands if it can be partitioned into equal-size blocks as

$$H = \begin{bmatrix} H^{(1)} \\ H^{(2)} \\ \vdots \\ H^{(j)} \end{bmatrix} \tag{3}$$

where each block $H^{(s)}$ is a $(1,k)$ matrix of size $\frac{m}{j} \times n$.

**Regular $(j,k)$ Construction:** The parameters of the resulting parity-check matrix depend on the cardinality of the projective plane and an additional design parameter $\rho$, which is in the range $1 \leq \rho \leq q$. Select a point, say $P_0$, in $\mathbf{P}^2(\mathbf{F})$ and define the line subset $L$ to consist of all lines except those passing through $P_0$. Choose $\rho$ "forbidden" lines $\mu_1, \mu_2, \ldots, \mu_\rho$, which pass through the point $P_0$. Choose the set of points $X$ to consist of all points except those lying on the forbidden lines $\mu_1, \mu_2, \ldots, \mu_\rho$. Let $H$ be the corresponding incidence matrix.

**Theorem 1** *A matrix $H$ that results from the regular $(j,k)$ construction is a $(j,k)$ matrix with a band structure and has no 4-cycles. Moreover, $H$ has the following parameters:*

*(i)* $j = q + 1 - \rho$ *and* $k = q$;

*(ii)* $m = q^2 - q(\rho - 1) = j \cdot k$ *and* $n = q^2 = k^2$.

[1]Note that the notation in [1] is not consistent with the terminology used for designs [7], where $k$ usually denotes the size of the blocks of a $t$-$(v,k,\lambda)$ design.

**Remark:** The projective plane over $\mathbf{F}$ =GF($q$) can be viewed as an $2-(q^2+q+1, q+1, 1)$ design with the dual incidence structure of points and lines, i.e., the $q^2+q+1$ lines in $\mathbf{P}^2(\mathbf{F})$ correspond to the $q^2+q+1$ points of the design and points of $\mathbf{P}^2(\mathbf{F})$ correspond to the blocks of the design. The dual affine plane can be obtained from the projective plane by deleting one point and all lines passing through this point (cf. Chap. 19 in [7]). This corresponds to the above construction with $\rho = 0$ and results in a $2-(q^2, q, 1)$ design, where the $q^2$ lines correspond to the $q^2$ points of the design. The above construction is a generalization of this transition from the projective to the dual affine plane. It does not result in a design but nevertheless it gives rise to a $(j, k)$ matrix.

**Proof:** The incidence properties of the projective plane imply that any two lines intersect in at most one point in $X$. Hence, there are no 4-cycles.
(i) There are $j = q+1-\rho$ points on any given line in $L$ and every such line has $\rho$ intersection points with the forbidden lines $\mu_1, \mu_2, \ldots, \mu_\rho$. These intersection points have been deleted from $\mathbf{P}^2(\mathbf{F})$, hence, there are $q+1-\rho$ remaining points on this line, which are contained in $X$. This shows that $j = q+1-\rho$.

In the projective plane, there are $q+1$ lines passing through each point $P \in X$. Out of these $q+1$ lines, there is exactly one line passing through $P$ and $P_0$. By construction, this line is not contained in the line set $L$ and, thus, there are $q$ lines in $L$ that pass through $P$, hence, $k = q$.
(ii): It is clear from the construction that there are $n = q^2$ lines. In the construction process, $q\rho + 1$ points are deleted and, therefore, a total of $m = q^2 + q + 1 - q\rho - 1 = q^2 - q(\rho - 1)$ points remain.

To obtain a band structure of $H$, one needs to choose a suitable ordering of the points in $X$, i.e., of the rows of $H$. Let $Q$, $Q \neq P_0$, be some point on a forbidden line, say on $\mu_1$. There are $q+1$ lines passing through $Q$ and, by construction, $q$ of these lines lie in $L$ because only one of the $q+1$ lines containes $P_0$. We label these lines as $\lambda_1, \ldots, \lambda_q$. Let $\mu_{\rho+1}, \ldots, \mu_{q+1}$ denote the $j$ lines through $P_0$ that are not forbidden. By construction, $X$ consists of the $j \cdot q$ intersection points of the lines $\lambda_1, \ldots, \lambda_q$ with the lines $\mu_{\rho+1}, \ldots, \mu_q$. We label the $j \cdot q$ intersection points $\lambda_\ell \cap \mu_{\rho+s}$ by $P_i$, where $i = \ell + (s-1)q$, $\ell = 1, \ldots, q$, $s = 1, \ldots, j$. This labelling provides the desired band structure: the submatrix $H^{(s)}$ is the incidence matrix of $L$ with the $q$ points on the line $\mu_{\rho+s}$. □

**Example 1** *To construct a $(j = 3, k = 3)$ LDPC matrix consider the projective plane $\mathbf{P}^2(\mathbf{Z}_3)$. Let $P_0$ be a point at infinity with coordinates, say $\mathbf{x}_0 = (0, 0, 1)$. The set of lines that does not pass through $P_0$ is given by*

$$L = \{(\lambda_1, \lambda_2, 1) : \lambda_1, \lambda_2 \in \mathbf{Z}_3\}.$$

*To construct a LDPC matrix with $j = 3$, we choose $\rho = 1$, by Theorem 1. As forbidden line $\mu_1$, we choose the line at infinity with coefficients $(1, 1, 0)$, for which $\mu_1(\mathbf{x}_0) = 0$ holds, i.e., $P_0$ lies on $\mu_1$. According to the construction, the point set $X$ consists of all the points $P$ (with coordinates $\mathbf{x} = (x_1, x_2, x_3)$) that do not lie on $\mu_1$, i.e., for which $0 \neq \mu_1(\mathbf{x}) = x_1 + x_2$. This point set is given by*

$$X = \{(1, 0, c) : c \in \mathbf{Z}_3\} \cup \{(0, 1, c) : c \in \mathbf{Z}_3\} \cup \{(1, 1, c) : c \in \mathbf{Z}_3\}$$

*and the corresponding incidence matrix*[2] *is*

$$H = \begin{bmatrix} 1 & 1 & 1 & & & & & & \\ & & & 1 & 1 & 1 & & & \\ & & & & & & 1 & 1 & 1 \\ 1 & & & 1 & & & 1 & & \\ & 1 & & & 1 & & & 1 & \\ & & 1 & & & 1 & & & 1 \\ 1 & & & & & 1 & & 1 & \\ & 1 & & 1 & & & & & 1 \\ & & 1 & & 1 & & 1 & & \end{bmatrix}.$$

The Regular $(j, k)$ Construction generates LDPC matrices with $j \leq k$, where $k = q$ is a prime power. The restriction to prime powers is due to the fact that the cardinality of a finite field is a prime power. If instead of a finite field $\mathbf{F}$, one uses a commutative ring $R$ for the components of the points and the coefficients of the lines, one obtains a projective plane $\mathbf{P}^2(R)$ defined over the ring $R$. Projective spaces over rings have been well studied in algebraic geometry (see e.g. [8]); here, we are interested in the rational points of the projective plane defined over $R$.

When using a ring instead of a field, the parameter $q$ need not be a prime power but can be any non-negative integer. As an example, we can consider the ring $R = \mathbf{Z}_q$ of integers modulo $q$ or rings of the form $R = \mathrm{GF}(q_1^{e_1}) \times \ldots \times \mathrm{GF}(q_s^{e_s})$, where $q = q_1^{e_1} \cdot \ldots \cdot q_s^{e_s}$ is the prime power decomposition of $q$. One can show that the statements of Theorem 1 remain true provided that one imposes the following conditions on the exceptional point $P_0$, the $j$ allowed lines $\mu_{\rho+1}, \mu_{\rho+2}, \ldots, \mu_{q+1}$ and the point set $X$:

**Full Rank Conditions:**

I The exceptional point $P_0$ must have at least one coordinate, which is a unit in the ring $R$.

II Each of the $j$ allowed lines $\mu_{\rho+1}, \ldots, \mu_{q+1}$ must have at least one component, which is a unit in the ring $R$.

III Each point in the point set $X$ must have at least one coordinate, which is a unit in the ring $R$.

IV The allowed lines $\mu_{\rho+1}, \ldots, \mu_{q+1}$ must satisfy the following *non-degenerate intersection condition*: Every distinct pair of lines $\mu_{\rho+i}$ and $\mu_{\rho+i'}$ must have *exactly one* intersection point (which is the point $P_0$).

The follwing example illustrates that in the ring case, two lines can have more than one intersection point and that if these lines are used in the regular $(j, k)$ construction, the resulting parity-check matrix will have 4-cycles. Thus, the non-degenerate intersection property, i.e., Full Rank Condition IV, is crucial to avoid 4-cycles.

**Example 2** *Consider the ring* $R = \mathbf{Z}_4$ *and let* $P_0$ *be the point at infinity* $\mathbf{x}_0 = (0, 0, 1)$. *The set of lines that do not pass through* $P_0$ *is given by*

$$L = \{(\lambda_1, \lambda_2, 1) : \lambda_1, \lambda_2 \in \mathbf{Z}_4\}.$$

[2]For better readability, the zero entries in the matrix are shown as blank entries.

*We choose $j = 2$, i.e., there are two allowed lines, which are chosen to be*

$$\mu = (1, 0, 0) \qquad\qquad \mu' = (1, 2, 0).$$

*Clearly, $\mu$ and $\mu'$ pass through $P_0$. But there is a second intersection point, namely, $P_1$ with coordintes $\mathbf{x}_1 = (0, 2, 1)$. The resulting regular $(j = 2, k = 4)$ parity check matrix is given by*

$$H = \begin{bmatrix} 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \end{bmatrix}.$$

**Remark.** For any ring, one can always find three lines, which satisfy the Full Rank Condition IV and pass through one common point $P_0$. E.g., the three lines with components

$$(1, 0, 0) \qquad (0, 1, 0) \qquad (1, 1, 0)$$

have the intersection point with coordinates $(0, 0, 1)$ and satisfy the mentioned condition. Thus, for $j = 3$ and any finite ring $R$, there is a Regular $(j = 3, k = |R|)$ Construction that results in an LDPC matrix with the properties stated in Theorem 1.

# 4 Construction of LDPC Matrices from LDPC Submatrices

When constructing high-rate LDPC matrices without 4-cycles, one wishes to maximize the code length $n$ for a given number $m$ of check equations and given $j$. The construction in the previous section does not give LDPC matrices of maximum length. In this section, we propose two constructions to extend the code length. In the next section, we will show that these extension constructions provide maximum length codes.

**Extension Construction 1**[3] Let $H_1$ be a (small) LDPC matrix with some parameters $j_1$, $k_1$, $m_1$ and $n_1$ without 4-cycles. Moreover, suppose we are given a second (large) LDPC matrix $H_2$ without 4-cycles, which has a band structure with $j_2$ bands. Thus, $H_2$ is an $m_2 \times n_2$ matrix with $j_2$ ones per column and $m_2 = j_2 \cdot m_1$. We define an LDPC matrix $H$ by

$$H = \left[ \; H_2 \;\middle|\; I_{j_2} \otimes H_1 \; \right] \tag{4}$$

where $I_{j_2} \otimes H_1$ denotes the tensor (or Kronecker) product of the $j_2 \times j_2$ identity matrix $I_{j_2}$ and $H_1$.

**Proposition 1** *The matrix $H$ of the Extension Construction 1 has no 4-cycles. It has a quasi-band structure (3) with $j$ bands and within each band there are $0, 1$ or $j_1$ ones per column. The parameters of $H$ are*

[3] A special case of this construction for $j = 3$ was first discovered in [9].

- $m = m_2$ *and* $n = j_2 \cdot n_1 + n_2$.
- $j = j_1$ *or* $j_2$, *i.e., there are* $n_1 \cdot j_2$ *columns with* $j_1$ *ones and* $n_2$ *columns with* $j_2$ *ones.*
- $k = k_1 + k_2$.

**Example 3** *The* $(3,3)$ *matrix of Example 1 has a band structure and can be used as matrix* $H_2$ *in the Extension Construction 1. For the small LDPC matrix we choose*

$$H_1 = \begin{bmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix}.$$

*The resulting* $9\times 18$ *irregular LDPC matrix has* $k = 5$ *and* $j = 2$ *or* $3$ *and is given by*

$$H = \begin{bmatrix}
1 & 1 & 1 & & & & & & & 1 & & 1 & & & & & \\
 & & & 1 & 1 & 1 & & & & 1 & 1 & & & & & & \\
 & & & & & & 1 & 1 & 1 & & 1 & 1 & & & & & \\
1 & & & 1 & & & 1 & & & & & & 1 & & 1 & & \\
 & 1 & & & 1 & & & 1 & & & & & 1 & 1 & & & \\
 & & 1 & & & 1 & & & 1 & & & & & 1 & 1 & & \\
1 & & & & & 1 & & 1 & & & & & & & & 1 & & 1 \\
 & 1 & & 1 & & & & & 1 & & & & & & & 1 & 1 & \\
 & & 1 & & 1 & & 1 & & & & & & & & & & 1 & 1
\end{bmatrix}$$

**Proof:** The statements about the parameters of $H$ are obvious from the construction and also the quasi-band structure of $H$ is a direct consequence of the construction.

It is clear that $H$ has no 4-cycles within the first $n_2$ columns or within the last $j_2 \cdot n_1$ columns because both $H_1$ and $H_2$ have no 4-cycles. Moreover, there are no 4-cycles between these first set and the second set of columns because $H_2$ has band structure (3), i.e., within the $j = j_2$ bands of $H$ there can be no 4-cycle because the first set of columns has exactly a single one per column in each band and neither can there be a 4-cycle accross two bands because of the tensor product structure of the second set of columns. Thus, there are no 4-cycles in $H$. $\square$

**Extension Construction 2** Suppose that $H_1$ and $H_2$ are given as in the Extension Construction 1 with the only difference that the band structure of $H_2$ consists of submatrices $H_2^\ell$ of size $(m_1 - 1)\times n_2$. Thus, $H_2$ is an $m_2 \times n_2$ matrix with $j_2$ ones per column and $m_2 = j_2 \cdot (m_1 - 1)$. We define an LDPC matrix $H$ by

$$H = \left[\begin{array}{ccc|c} & H_2 & & I_{j_2} \otimes H_1^u \\ 0 & \dots & 0 & H_1^l \quad \dots \quad H_1^l \end{array}\right], \tag{5}$$

where $H_1^u$ and $H_1^l$ denote the submatrices of $H_1$ consisting of the first $m_1 - 1$ rows and the last row, respectively. The following proposition can be proved in a similar way as Proposition 1.

**Proposition 2** *The matrix* $H$ *obtained by the Extension Construction 2 has no* 4*-cycles and its parameters are*

- $m = m_2 + 1$ *and* $n = j_2 \cdot n_1 + n_2$.

- *$j = j_1$ or $j_2$, i.e., there are $n_1 \cdot j_2$ columns with $j_1$ ones and $n_2$ columns with $j_2$ ones.*
- *$k = k_1 + k_2$ or $j_2 \cdot k_1$, i.e., the first $m-1$ rows have Hamming weight $k_1 + k_2$ and the last row has Hamming weight $j_2 \cdot k_1$.*

**Remark:** This construction can be modified and generalized by selecting $H_1^l$ to consist of $t$ rows of $H_1$ with pairwise non-overlapping support. $H_1^u$ will then consist of the $m_1 - t$ remaining rows. The resulting $H$ matrix has size $(m_2 + t) \times (n_1 + n_2)$, in particular, the block below $H_2$ consists of a $t \times n_2$ zero-matrix.

**Example 4** *Let $H_1$ be the $3 \times 1$ matrix given by the transpose of $[111]$ and let $H_2$ be the transpose of the incidence matrix of the affine plane over GF(2), i.e., the point set consists of the 4 points of the affine plane and the set of lines consists of all the possible 6 lines. Thus, $m_2 = 6$, $n_2 = 4$, $j_2 = 3$, and $k_2 = 2$. The LDPC matrix resulting from the Extension Construction 2 is given by*

$$H = \begin{bmatrix} 1 & 1 & & & 1 & & & \\ & & 1 & 1 & 1 & & & \\ 1 & & 1 & & & 1 & & \\ & 1 & & 1 & & 1 & & \\ 1 & & & 1 & & & 1 & \\ & 1 & 1 & & & & 1 & \\ & & & & 1 & 1 & 1 & \end{bmatrix}$$

*Note that $H$ is the incidence matrix of the projective plane over GF(2); in particular, it is a 2-$(7, 3, 1)$ design (or Steiner system).*

# 5 Construction of Steiner Systems

A Steiner system is a special type of $t$-design, usually denoted by $S(m, j, t)$ [7]. A Steiner system $S(m, j, t)$ is composed of a point set $X$ of $m$ points and a block set $L$, which consists of subsets $b \subset X$ that are called blocks and each block $b$ has cardinality $j$. The block set must satisfy the following constraint: Any choice of $t$ points in $X$ uniquely determines a block $b \in L$ that contains the $t$ chosen points. In [4], Steiner systems with $t = 2$ were related to LDPC matrices without 4-cycles and, in particular, it was shown that the maximum length $n$ of an LDPC matrix without 4-cycles and parameters $m$ and $j$ is bounded by the cardinality of the block set $L$, viz.,

$$n \leq \frac{m(m-1)}{j(j-1)}. \tag{6}$$

Moreover, every Steiner system gives rise to an LDPC matrix, which is the incidence matrix of the point set $X$ and the block set $L$ and the resulting LDPC matrix has maximum length. We will show that the three constructions presented above can be used to give some simple constructions of Steiner systems for all $j$.

The parameters $m$ and $j$ have to satisfy the following necessary conditions to obtain a Steiner system $S(m, j, 2)$ (see 2.4.30 in [10]):

$$m - 1 \equiv 0 \mod j - 1 \tag{7}$$

$$m(m-1) \equiv 0 \mod j(j-1). \tag{8}$$

For $j = 3, 4$ and 5, these necessary conditions are also sufficient for the existence of $S(m, j, 2)$ [10].

**Theorem 2** *Let $H_1$ be the incidence matrix of a Steiner system $S(m_1, j, 2)$ and let $H_2$ be a $(j_2 = j, k_2 = m_1)$ matrix obtained from the Regular $(j_2, k_2)$ Construction. The Extension Construction 1 produces an incidence matrix $H$ of a Steiner system $S(m = jm_1, j, 2)$.*

**Proof:** By Theorem 1 and Proposition 1, $H$ is a $(j, k_1 + m_1)$ matrix with $m = j \cdot m_1$ rows, where $k_1 = (m_1 - 1)/(j - 1)$ since $H_1$ comes from $S(m_1, j, 2)$. The number of columns of $H$ meet the upper bound (6):

$$\begin{aligned} n &= j \cdot n_1 + n_2 = j\frac{m_1(m_1-1)}{j(j-1)} + m_1^2 \\ &= \frac{m_1(jm_1-1)}{j-1} = \frac{m(m-1)}{j(j-1)} \end{aligned}$$

and, hence, $H$ is the incidence matrix of a Steiner system $S(m = jm_1, j, 2)$. □

**Theorem 3** *Let $H_1$ be the incidence matrix of a Steiner system $S(m_1, j, 2)$ and let $H_2$ be a $(j_2 = j, k_2 = m_1 - 1)$ matrix obtained from the Regular $(j_2, k_2)$ Construction. The Extension Construction 2 produces an incidence matrix $H$ of a Steiner system $S(m = j(m_1-1)+1, j, 2)$.*

**Proof:** By Theorem 1 and Proposition 2, $H$ is a $(j, k_1+k_2)$ matrix with $m = j \cdot (m_1-1)+1$ rows, where $k_1 = (m_1 - 1)/(j - 1)$ since $H_1$ comes from $S(m_1, j, 2)$. The number of columns of $H$ meet the upper bound (6):

$$\begin{aligned} n &= j \cdot n_1 + n_2 = j\frac{m_1(m_1-1)}{j(j-1)} + (m_1-1)^2 \\ &= \frac{m_1-1}{j-1}[j(m_1-1)+1] = \frac{(m-1)m}{(j-1)j} \end{aligned}$$

and, hence, $H$ is the incidence matrix of a Steiner system $S(m = j \cdot (m_1 - 1) + 1, j, 2)$. □

For any given $j$, the shortest Steiner system $S(j, j, 2)$ of length $n = 1$ has the all-one column of length $j$ as its incidence matrix. Thus, starting with this all-one incidence matrix as $H_1$ and using Theorems 2 and 3 iteratively, one can construct infinitely many Steiner systems provided that the full rank conditions are satisfied. For $j = 3, 4$, and 5 the parameters of the first few Steiner systems that are obtained in this way are given in Table 1. Note that the Steiner system $S(41, 5, 2)$ is obtained by a direct construction method (cf. Chap. 15.3 in [11]) and cannot be obtained from $S(5, 5, 2)$. The Steiner systems $S(201, 5, 2)$ and $S(205, 5, 2)$ can be constructed using Theorems 2 and 3, resp., based on the Steiner system $S(41, 5, 2)$.

# 6 Performance of Some High Rate LDPC Codes

In order to achieve a good performance on the AWGN channel, a code should not have too many codewords of small Hamming weight and, in particular, it should have a reasonable minimum Hamming distance $d_{min}$. For small lengths $n$ and high rate codes, the Hamming distances that are obtained from the Regular $(j, k)$ Construction were found to be above

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| $j=3$ | m | 3 | 7 | 9 | 19 | 21 | 25 | 27 | 55 |
| | n | 1 | 7 | 12 | 57 | 70 | 100 | 117 | 495 |
| | k | 1 | 3 | 4 | 9 | 10 | 12 | 13 | 27 |
| $j=4$ | m | 4 | 13 | 16 | 49 | 52 | 61 | 64 | 193 |
| | n | 1 | 13 | 20 | 196 | 221 | 305 | 336 | 3088 |
| | k | 1 | 4 | 5 | 16 | 17 | 20 | 21 | 64 |
| $j=5$ | m | 5 | 21 | 25 | 41 | 121 | 125 | 201 | 205 |
| | n | 1 | 21 | 30 | 82 | 726 | 775 | 2010 | 2091 |
| | k | 1 | 5 | 6 | 10 | 30 | 31 | 50 | 51 |

Table 1: Steiner systems obtained by the constructions given in Theorem 2 and 3.

the Gilbert-Varshamov bound. For large codes, the minimum Hamming distance could not be determined. However, for the extension constructions 1 and 2, one readily obtains the following upper bounds on the Hamming distance of the resulting LDPC matrix

$$d_{min} \leq min\{d_{min}^{(1)}, d_{min}^{(2)}\},$$

where $d_{min}^{(i)}$ denotes the minimum Hamming distance of the two codes with parity-check matrices $H_i$, $i = 1, 2$, which are used in the constructions. This upper bound implies that all the non-trivial codes that are obtained from Table 1 with the exception of those with $j = 5$, which are based on $S(41, 5, 2)$, have a poor minimum Hamming distance, viz., $d_{min} \leq 4, 6$ and 8, depending on $j = 3, 4$ and 5, respectively. This follows from the fact that the parity-check matrices of all these codes are built from the square parity-check matrices corresponding to the Steiner systems $S(7, 3, 2)$, $S(13, 4, 2)$ and $S(21, 5, 2)$, which satisfy the mentioned upper bounds. For the construction of good codes we have avoided to include the above mentioned Steiner systems into the constructions.

A small high rate code was constructed using the modified Extension Construction 2, where $H_1$ is an 21×49 matrix obtained from the Regular $(j = 3, k = 7)$ Construction and $H_2$ is an 57×361 matrix obtained from the Regular $(j = 3, k = 19)$ Construction. The resulting LDPC matrix $H$ has $j = 3$ and size 59×508, the dimension of the code is 449, which gives the rate 0.8838. A second code of length $n = 1849$ was obtained from the Regular $(j = 5, k = 43)$ Construction by choosing the set of lines $L$ and set of points $X$ as

$$\begin{aligned} L &= \{(\lambda_1, \lambda_2, 1) : \lambda_1, \lambda_2 \in \mathbf{Z}_{43}\} \\ X &= \{(1, 20, c) : c \in \mathbf{Z}_{43}\} \cup \{(0, 1, c) : c \in \mathbf{Z}_{43}\} \cup \{(1, 5, c) : c \in \mathbf{Z}_{43}\} \cup \\ &\quad \{(1, 13, c) : c \in \mathbf{Z}_{43}\} \cup \{(6, 23, c) : c \in \mathbf{Z}_{43}\} \end{aligned}$$

The 215×1849 parity-check matrix contains 4 redundant checks. Thus, the code has dimension 1638 and rate 0.8858. Both codes have no 4-cycles by construction.

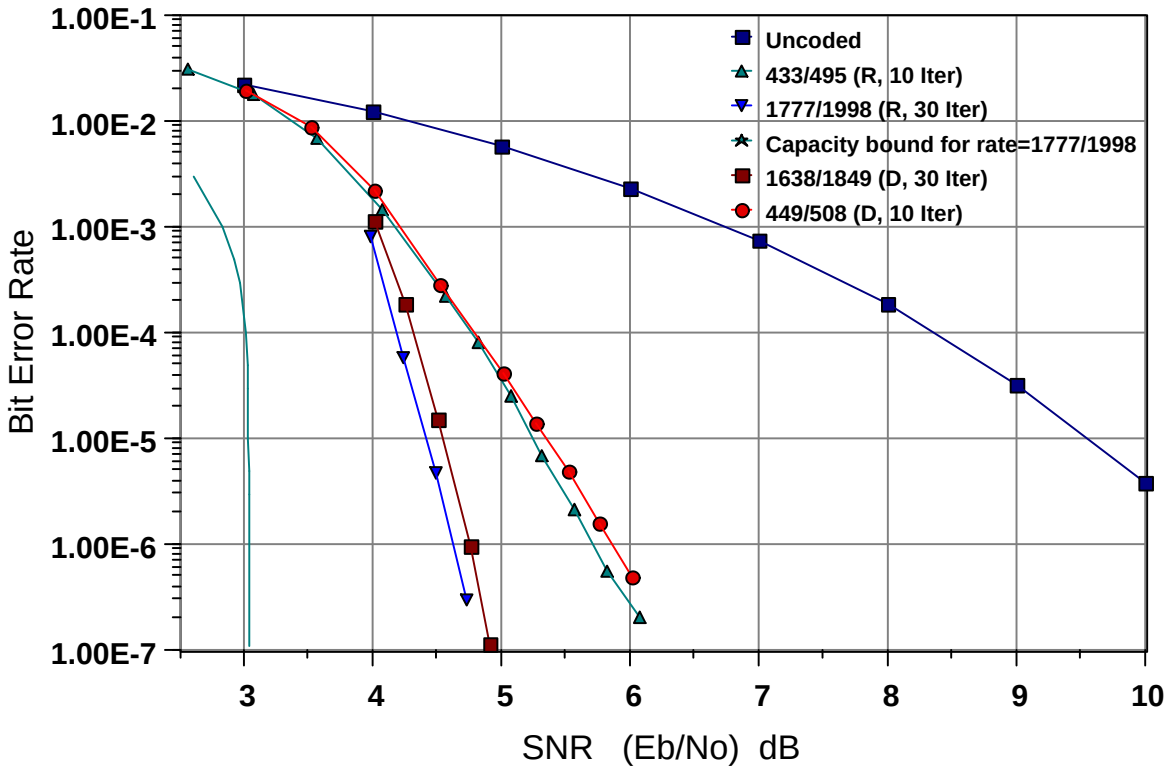


Figure 1: Performance of LDPC codes on the AWGN channel.

For the AWGN channel, the performance of the two codes using the sum-product decoding algorithm is shown in Fig. 1. For comparison, the performance of two randomly constructed codes of MacKay [3][4] with similar lengths and rates are also shown; the parameters of these two codes are $(n, m, j) = (495, 62, 3)$ and $(1998, 222, 4)$ with rates 0.8747 and 0.8893, respectively. The capacity achieving signal-to-noise ration (SNR) for the two short codes of lengths 495 and 508 is 2.841 dB and 2.963 dB, respectively. These two short codes have similar bit-error performance when decoded by the sum-product algorithm with at most 10 iterations. The capacity achieving SNR for the two longer codes is at 3.0402 dB for $n = 1849$ and at 2.991 dB for $n = 1998$. Limiting the sum-product algorithm to at most 30 iterations, MacKay's randomly constructed code of length $n = 1998$ is at 1.55 dB from capacity while the deterministically constructed code of length $n = 1849$ is at 1.7 dB from capacity at a bit-error rate of $10^{-6}$.

A comparision of the deterministically and randomly constructed codes shows that the deterministically constructed codes almost achieve the same performance as the randomly constructed codes but it is much simpler to construct 4-cycle-free high-rate LDPC matrices (which almost achieve the bound (6)) by the deterministic method. Moreover, the deterministically constructed codes are fully described by the specification of the point set and the line set; thus, they have a very short description length compared to the randomly constructed codes.

[4]We would like to acknowledge D.J.C. Mackey for providing these codes via his web site.

# References


[1] R.G. Gallager, "Low-Density Parity-Check Codes," *IRE Trans. on Information Th.*, pp. 21–28, 1962.

[2] Brendan J. Frey, *Graphical Models for Machine Learning and Digital Communications*, MIT Press, Cambridge Mass., 1998.

[3] D.C.J. MacKay, Encyclopedia of sparse graph codes (hypertext archive, 1999). `http://wol.ra.phy.cam.ac.uk/mackay/codes/data.html`.

[4] D.J.C. MacKay, M.C. Davey, "Evaluation of Gallager Codes for Short Block Length and High Rate Applications," to appear in the proceedings of the IMA workshop on Codes, Systems and Graphical Models 1999.

[5] N. Jacobson, *Basic Algebra I*, Freeman, San Francisco, 1980.

[6] W.W. Peterson, E.J. Weldon, Jr., *Error-Correcting Codes*, MIT Press, 1972.

[7] J.H. van Lint and R.M. Wilson, *A Course in Combinatorics*, Cambridge Univ. Press, 1992.

[8] Robin Hartshorne, *Algebraic Geometry*, GTM 52, Springer, 1977.

[9] Daniel Hösli, Erik Svensson, "Low-Density Parity-Check Codes for Magnetic Recording," ETH-Diploma Thesis, Signal and Information Processing Lab., Swiss Fed. Inst. of Techn., CH-8092 Zurich, March 2000.

[10] P. Dembowski, *Finite Geometries*, Springer, 1968.

[11] M. Hall, *Combinatorial Theory*, Wiley & Sons, 1967.