Explicit Construction of Families of LDPC Codes With No 4-Cycles

Jon-Lark Kim, *Member, IEEE*, Uri N. Peled, Irina Perepelitsa, Vera Pless, *Senior Member, IEEE*, and Shmuel Friedland

***Abstract*—Low-density parity-check (LDPC) codes are serious contenders to turbo codes in terms of decoding performance. One of the main problems is to give an explicit construction of such codes whose Tanner graphs have known girth. For a prime power q and $m \geq 2$, Lazebnik and Ustimenko construct a q-regular bipartite graph $D(m,q)$ on $2q^m$ vertices, which has girth at least $2\lceil m/2 \rceil + 4$. We regard these graphs as Tanner graphs of binary codes LU (m,q). We can determine the dimension and minimum weight of LU, $(2,q)$, and show that the weight of its minimum stopping set is at least $q+2$ for q odd and exactly $q+2$ for q even. We know that $D(2,q)$ has girth 6 and diameter 4, whereas $D(3,q)$ has girth 8 and diameter 6. We prove that for an odd prime p, LU, $(3,p)$ is a $[p^3,k]$ code with $k \geq (p^3 - 2p^2 + 3p - 2)/2$. We show that the minimum weight and the weight of the minimum stopping set of LU $(3,q)$ are at least $2q$ and they are exactly $2q$ for many LU $(3,q)$ codes. We find some interesting LDPC codes by our partial row construction. We also give simulation results for some of our codes.**

***Index Terms*—Large girth, low-density parity-check (LDPC) codes, Tanner graph.**

I. Introduction

LOW-density parity-check (LDPC) codes were originally introduced by Gallager [1]. They have again become interesting because of the success of iterative decoding for turbo codes. LDPC codes are competitors of these codes in performance of iterative decoding algorithms, as their performance approaches the Shannon limit [2]. Tanner's graphical representation of LDPC codes [3] influenced much of the current literature. Most of these codes are constructed randomly, but explicit constructions are needed for implementation purposes as well as for knowing the properties of these codes. We give such constructions based on constructions of graphs with good girth, since belief propagation decoding algorithms generally work better if the girth is at least 4 or more. A graph with a small diameter allows belief propagation to work faster.

Let $m \geq 2$ be an integer and q a power of a prime. In [4]. Lazebnik and Ustimenko construct a family $D(m,q)$ of q-regular bipartite graphs on $2q^m$ vertices, with q^m vertices called *points* and q^m vertices called *lines*. Points and lines are elements of GF $(q)^m$ and equations are given in [4], which determine incidence of points and lines. If a point is incident to a line, an edge joins them in $D(m,q)$. It is further shown [4] that when m is odd, $D(m,q)$ has girth at least $m+5$. It also follows from general graph homomorphism results of [5] that the girth of $D(m,q)$ is not less than the girth of $D(m-1,q)$, so for m even, the girth of $D(m,q)$ is at least $m+4$. Thus, for all m, the girth of $D(m,q)$ is at least $2\lceil m/2 \rceil + 4$. We let $H(m,q)$ be the incidence matrix of lines and points of $D(m,q)$, where rows are indexed by lines and columns are indexed by points, and consider $H(m,q)$ and its transpose $H(m,q)^T$ to be parity-check matrices of binary codes of length q^m called LU (m,q) codes. In other words, we take $D(m,q)$ to be the Tanner graph [3] of the LDPC code LU (m,q) and investigate the properties of these codes. As the rows as well as the columns of $H(m,q)$ are linearly dependent, the dimensions of these codes need to be determined.

It is shown in [4] that any two rows (columns) of $H(m,q)$ have a 1 in at most one common column (row). This implies that the girth of the graph is at least 6. We show that $D(2,q)$ has girth 6 and diameter 4. We derive the parameters of all LU $(2,q)$. When q is even we obtain Euclidean geometry codes.

We have computed the dimension of LU $(3,q)$ codes through $q = 25$. We prove that $D(3,q)$ has girth 8 (already shown in [6]). This implies that the minimum weight of LU $(3,q)$ is at least $2q$ [3]. We show that when LU $(3,q)$ is derived from $H(3,q)$, the minimum weight is exactly $2q$. For $q \geq 3$, the diameter of $D(3,q)$ is 6 [6]. We conjecture the dimension of LU $(3,q)$ to be $(q^3 - 2q^2 + 3q - 2)/2$ when q is an odd prime power and prove that it is at least $(q^3 - 2q^2 + 3q - 2)/2$ when q is an odd prime. When q is odd we apparently have a family of codes whose rates approach $1/2$.

We examined some LU (m,q) codes for $m = 4, 5, 6$, and 7 and we give our observations. We give a lower bound on the minimum weight of LU (m,q) in terms of q and m for odd m using Tanner's bound [3].

A *stopping set* in an LDPC code is the support of a binary vector having the length of the code that does not have exactly one 1 in common with any row of the parity-check matrix. A minimum stopping set is a nonzero stopping set with minimum weight. In the following, we identify the support of a binary vector with the vector. Note that any codeword is a stopping set, and therefore the minimum weight of a code is at least the

Manuscript received June 13, 2003; revised May 5, 2004. This work was supported in part by the Caesarea Edmond Benjamin de Rothchild Foundation Institute of Interdisciplinary Application of Computer Science at the University of Haifa to U.N. Peled. The material in this paper was presented in part at the 40th Allerton Conference on Communication, Control and Computing, Monticello, IL, October 2002.

J.-L. Kim is with the Department of Mathematics, University of Nebraska–Lincoln, Lincoln, NE 68588-0323, USA (e-mail: jlkim@math.unl.edu).

U. N. Peled, I. Perepelitsa, V. Pless, and S. Friedland are with the Department of Mathematics, Statistics, and Computer Science, University of Illinois–Chicago, Chicago, IL 60607-7045, USA (e-mail: uripeled@uic.edu, irina@math.uic.edu; pless@math.uic.edu; friedlan@uic.edu).

Communicated by S. Litsyn, Associate Editor for Coding Theory.

Digital Object Identifier 10.1109/TIT.2004.834760

0018-9448/04$20.00 © 2004 IEEE

IEEE Proof

weight of the minimum stopping set. The weight of the minimum stopping set is an important measure of the performance of a code with iterative decoding over the binary erasure channel [7]. We show that for LU $(2, q)$ the weight of the minimum stopping set is at least $q+2$. It follows from [3] that the weight of the minimum stopping set of LU $(3, q)$ is at least $2q$. We show that equality is achieved for LU $(3, q)$ obtained from $H(3, q)$.

We use a new technique, the partial row construction, to obtain codes with larger rate than LU (m, q) codes but not smaller girth. We give lists of interesting codes found in this way.

The parity-check matrices of LU codes are block matrices where blocks are powers of permutation matrices and are related to array codes [8]. A high girth code can be obtained from an array code by a proper choice of the powers as suggested in [8] or from a lattice code by a selection of slopes [9]. Milenkovic *et al.* [10] gave an explicit construction of high girth LDPC codes with the structure similar to LU codes using cycle-invariant difference sets.

A preliminary version of this paper appeared in [11]. We withdraw Proposition 1 of that paper as it is incorrect.

II. LU $(2, \mathrm{Q})$ Codes

Definition 1 ([4]): In $D(2, q)$ a point (a, b) is on a line $[x, y]$ if and only if $y = ax + b$, where a, b, x, y are in GF (q).

We label the rows and columns of $H(2, q)$ with the pairs $[x, y]$ and (a, b) ordered lexicographically under a fixed ordering of GF (q). If q is a prime, this is the usual ordering; if q is a prime power, we order the elements of GF (q) in some way, say as powers of a primitive element, with the element 0 first. It can be seen that $H(2, q)$ consists of q^2 $q \times q$ permutation matrices, where each permutation matrix corresponds to a fixed a and a fixed x. If q is a prime, these permutation matrices are circulants. So the first q rows of $H(2, q)$ consist of q permutation matrices, similarly for the next q rows, etc.

We call a *row block* the set of all rows with fixed x, and a *column block* the set of all columns with fixed a.

Proposition 1 ([4]): Any two rows (columns) of $H(m, q)$ have at most one 1 in common, i.e., in the same column (row).

Proposition 2: No two rows in a row block have a 1 in common. Any two rows from different row blocks have exactly one 1 in common. Similarly for columns.

Proof: This follows from Definition 1. □

Example.

$$H(2,3)=\{H_{ij}\}=\left(\begin{array}{ccc|ccc|ccc} 1&0&0&1&0&0&1&0&0\\ 0&1&0&0&1&0&0&1&0\\ 0&0&1&0&0&1&0&0&1\\ \hline 1&0&0&0&0&1&0&1&0\\ 0&1&0&1&0&0&0&0&1\\ 0&0&1&0&1&0&1&0&0\\ \hline 1&0&0&0&1&0&0&0&1\\ 0&1&0&0&0&1&1&0&0\\ 0&0&1&1&0&0&0&1&0 \end{array}\right)$$

where i, j run over the index set

$$\{00, 01, 02, 10, 11, 12, 20, 21, 22\}.$$

We also note that the code whose parity-check matrix is $H(2,3)^T$ is the same as the one with parity-check matrix $H(2, 3)$.

Theorem 1: For $q > 2$, all $D(2, q)$ have girth 6. Also, all $D(2, q)$ have diameter 4.

Proof: By Proposition 1, the girth of $D(2, q)$ is at least 6. We show that we can find a cycle of length 6. The first row r_1 of $H(2, q)$ has a common 1 with the first row r_2 in the second row block in a column c_1. There is another column c_2 with a 1 in r_2. Column c_2 has a 1 in a unique row r_3 of the third row block. Row r_3 must have a common 1 with row r_1, but not in c_1 (or else r_2 and r_3 would have two common 1's) and not in c_2 (or else r_1 and r_2 would have two common 1's). So there is a third column c_3 having common 1's with r_1 and r_2. Then $r_1 - c_1 - r_2 - c_2 - r_3$ $c_3 - r_1$ is a cycle of length 6 in $D(2, q)$.

Two rows in different row blocks have distance 2 from each other. Similarly for columns. A row and a column have distance 1 or 3, and two rows or columns in the same row or column block have distance 4. Hence, the diameter of $D(2, q)$ is 4. □

Theorem 2: If q is odd, the two LU $(2, q)$ codes derived from $H(2, q)$ and $H(2, q)^T$ are the same $[q^2, q-1, 2q]$ code, whose group has order $(q!)^{q+1}$.

Proof: We construct a canonical spanning set of LU $(2, q)^{\perp}$. If we add all the rows in any row block of $H(2, q)$, we obtain the all-one vector. If we add up all the rows in $H(2, q)$ that have 1 in a fixed column, we will be adding one row from each row block. If, for example, the column is the first column, the resulting sum will be

$$\underbrace{10\ldots0}_{q}\underbrace{11\ldots1}_{q}\ldots\underbrace{11\ldots1}_{q}.$$

This is so since no two rows in a row block have a 1 in common by Proposition 2 and since q is odd. Hence, LU $(2, q)^{\perp}$ contains all the rows of the following matrix:

$$A = \begin{pmatrix} E & 0 & \ldots & \ldots & 0 \\ 0 & E & 0 & \ldots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \ldots & E \\ 1 & 1 & 1 & \ldots & 1 \end{pmatrix}$$

where $E = I + J$ with I the $q \times q$ identity matrix and J the $q \times q$ all-one matrix, and where 1 is the all-one row vector of length q.

As E has rank $q - 1$, A generates a code of dimension $q(q-1)+1$ (the all-one vector of odd weight is not equal to any sum of previous rows, as all such sums have even weight). It is not hard to see that the rows of A span LU $(2, q)^{\perp}$, as we can express any row of $H(2, q)$ as a sum of these rows. Hence, for q odd, $\dim(\mathrm{LU}\,(2, q)) = q^2 - (q(q-1)+1) = q - 1$.

From the generating set A of LU $(2, q)^{\perp}$, we see that the group of this code consists of $\mathrm{Sym}(q)$ operating independently on each column block of q elements, and another $\mathrm{Sym}(q)$ permuting the q column blocks. Hence, for q odd, the group of LU $(2, q)$ has order $(q!)^{q+1}$.

We can also determine the minimum weight of LU $(2, q)$ by looking at A. The dual of each E is the all-one vector of length q. But as the all-one vector of length q^2 is in LU $(2, q)^{\perp}$, every

IEEE Proof

vector in LU$(2,q)$ has even weight. So the minimum weight of LU$(2,q)$ is $2q$. LU$(2,q)$ can be regarded as all even-weight row vectors made out of all-0 and all-1 blocks of length q. As we also get A as above for $H(2,q)^T$, the two LU$(2,q)$ codes are in fact the same. □

When q is even, we get interesting results.

Lemma 1: $H(2,2^s)$ is the incidence matrix of 2^{2s} points and 2^{2s} lines consisting of parallel classes from the affine plane AG$(2,2^s)$. Further, the code C generated by $H(2,2^s)$ contains all the lines of this affine plane. The same results hold for $H(2,2^s)^T$.

Proof: Each row of $H(2,2^s)$ has weight 2^s, the weight of a line in an affine geometry from a projective plane PG$(2,2^s)$ of order 2^s. We regard these rows as lines of the geometry. By Proposition 2, each row block is a parallel class of lines. There are 2^s such blocks in $H(2,2^s)$. The affine plane has 2^s+1 parallel classes of lines. This last parallel class consists of the 2^s row vectors each of which is the all-one vector in a fixed column block and zero outside the block. We show in what follows that these vectors are in C. If we add up all the rows of $H(2,2^s)$ that have a 1 in their first position, we get

$$\underbrace{0\ldots0}_{2^s}\underbrace{1\ldots1}_{2^s}\cdots\underbrace{1\ldots1}_{2^s}$$

by Proposition 2 and since 2^s is even. Adding the all-one vector, which is the sum of the rows in any row block, we get

$$\underbrace{1\ldots1}_{2^s}\underbrace{0\ldots0}_{2^s}\cdots\underbrace{0\ldots0}_{2^s}$$

which is a line in the missing parallel class. We can get the rest of the lines similarly. The fact that this affine plane comes from PG$(2,2^s)$ follows from the equations in Definition 1. The same proof works for $H(2,2^s)^T$. □

Theorem 3: LU$(2,2^s)$ are $[2^{2s}, 2^{2s}-3^s, 2^s+2]$ codes.

Proof: We only consider $H(2,2^s)$. It is known [12] that the incidence matrix of an affine plane of order 2^s generates a $[2^{2s}, 3^s]$ binary code C. By Lemma 1, LU$(2,2^s)$ is the code $C^{\perp}$. We generate an incidence matrix of a projective geometry PG$(2,2^s)$ by starting from $H(2,2^s)$ and adding 2^s+1 new columns representing the points at ∞. All lines in the same parallel class will have the same point at ∞ and any two lines in different parallel classes will have different points at ∞. We further add a new row representing the line at ∞ whose points are the points at ∞. We also add 2^s rows representing the missing parallel class of lines as described in Lemma 1, each containing a different point at ∞. It is known [13, Theorem 8.6.6] that the ovals of PG$(2,2^s)$ are precisely the supports of the codewords of weight 2^s+2 in $C(\mathrm{PG}(2,2^s))^{\perp}$, the dual code of the code generated by PG$(2,2^s)$; and furthermore, the minimum weight of $C(\mathrm{PG}(2,2^s))^{\perp}$ is at least 2^s+2. As there exist ovals disjoint from the line at ∞, the minimum weight of LU$(2,2^s)$ is at most 2^s+2. For the reverse inequality, take any codeword w in LU$(2,2^s)$ and extend it with 2^s+1 zeroes. We get a vector orthogonal to the incidence matrix of PG$(2,2^s)$, because as shown in Lemma 1, the rows in the missing parallel class are spanned by the rows of $H(2,2^s)$. Therefore, by the "furthermore" part, the weight of w is at least 2^s+2. Hence, LU$(2,2^s)$ is a $[2^{2s}, 2^{2s}-3^s, 2^s+2]$ code. □

Theorem 4: The weight of the minimum stopping set of LU$(2,q)$ is at least $q+2$.

Proof: We denote by r_i and c_i the ith row and the ith column of $H(2,q)$, respectively. Let v be a minimum stopping set of LU$(2,q)$. Pick some component of v that is equal to 1, say $v_1=1$. The column c_1 has q 1's, say in rows $r_1,\ldots,r_q$. Since $r_1,\ldots,r_q$ have a common 1 with v in c_1, each of them has at least one other common 1 with v, and no two of them can have the other common 1 with v in the same column by Proposition 1. Therefore, we may assume that r_i has a common 1 with v in c_{i+1} for $i=1,\ldots,q$. For each $i=2,\ldots,q+1$, c_i has a common 1 with c_1 in r_{i-1}, and, therefore, by Proposition 2 the c_i belong to different column blocks than the column block containing c_1. There are only q column blocks, and therefore two of $c_1,\ldots,c_{q+1}$ are in the same column block. By the above, both of them are distinct from c_1, so we may assume that c_q and c_{q+1} are in the same column block. By Proposition 2, c_{q+1} does not have a common 1 with c_q. Column c_{q+1} must have 0's in $r_1,\ldots,r_{q-1}$, otherwise, it would have two common 1's with c_1. Since it has weight q, we may assume that it has 1's in $r_{q+1},\ldots,r_{2q-1}$. Each of the $q-1$ rows $r_{q+1},\ldots,r_{2q-1}$ has a common 1 with v in c_{q+1}, and therefore must have another common 1 with it, but not in c_1 (since c_1 already has its q 1's in $r_1,\ldots,r_q$), and not in c_q (since c_{q+1} and c_q do not have common 1's). Furthermore, no two of these $q-1$ rows can have a common 1 with v in the same column (since both of them already have a common 1 with it in c_{q+1}). Therefore, at most $q-2$ of them can have a common 1 with v in $c_2,\ldots,c_{q-1}$, and one of them must have a common 1 with v outside $c_1,\ldots,c_{q+1}$, say in c_{q+2}. Thus, $q+2$ components of v are 1. □

It follows from Theorems 3 and 4 that for q even, the weight of the minimum stopping set of LU$(2,q)$ is $q+2$.

In [14], families of LDPC codes with girth 6 were constructed from finite geometries. One of these families of Euclidean geometry codes has parameters $[2^{2s}-1, 2^{2s}-3^s, 2^s+1]$. We extended two of these codes for $s=2$ and $s=3$ and (using Magma [15]) found that they are equivalent to LU$(2,4)$ and LU$(2,8)$. This will be so in general since both families of codes are constructed from PG$(2,2^s)$. However, the two families could have different belief-propagation decoding performance as the parity-check matrices used are different. In fact, the parity-check matrices in [14] are cyclic, whereas ours are not. We note that when q is prime, LU$(2,q)$ codes are array codes.

III. LU$(3,q)$ Codes

Definition 2 ([4]): In $D(3,q)$, a point (a,b,c) is incident with a line $[x,y,z]$ if and only if $y=ax+b$ and $z=ay+c$, where a,b,c,x,y,z are in GF(q).

We investigated the parameters of the LU$(3,q)$ codes for $q=2$ up to $q=25$ by Magma. By [4], all the Tanner graphs of the LU$(3,q)$ codes have girth at least $3+5=8$. We give a simple proof that the girth is exactly 8. By [6], $D(3,q)$ has diameter 6 for $q\geq 3$. $D(3,2)$ is disconnected; it is a union of two 8-cycles.

IEEE Proof

TABLE I
PARAMETERS OF LU $(3,q)$ CODES FOR $q = 3,4,5$

q	3	4	5
H	[27,8,6]	[64,22,8]	[125,44,10]
H^T	[27,8,8]	[64,22,8]	[125,44,20]

So LU $(3,2)$ is the direct sum of two $[4,1,4]$ codes, each of which is an LU $(2,2)$ code.

Theorem 5 ([6]): $D(3,q)$ has girth 8. Its diameter is 6 if $q > 2$.

Proof: Since by [4] we know that the girth of $D(3,q)$ is at least 8, finding one 8-cycle shows that the girth is 8. It is not hard to check that $(000) - [000] - (100) - [111] - (011) - [011] - (110) - [-100] - (000)$ is an 8-cycle in $D(3,q)$. $D(3,q)$ has diameter 6 for $q > 2$ [6, Theorem 3.9]. □

Theorem 6: For p an odd prime, LU $(3,p)$ is a $[p^3,k]$ code with $k \geq (p^3 - 2p^2 + 3p - 2)/2$.

Proof: See Appendix . □

Conjecture : For odd q, LU $(3,q)$ is a $[q^3,(q^3 - 2q^2 + 3q - 2)/2]$ code.

We verified this for all of the LU $(3,q)$ codes for all odd q from 3 until 25. If this is true, then the rates of these codes approach $1/2$ as the odd q gets large. We noticed that for $q = 3$ and $q = 5$, the two LU $(3,q)$ codes we obtain from $H(3,q)$ and its transpose have different minimum weights. We checked by Magma that for $q = 4$ the two codes are equivalent. See Table I. For $q \geq 7$, we were unable to determine the minimum weight of LU $(3,q)$ derived from H^T.

Theorem 7: The minimum weight and the weight of the minimum stopping set of LU $(3,q)$ are at least $2q$.

Proof: The bound on the minimum weight follows from [3, Theorem 2] since we know that the girth of LU$(3,q)$ is 8. However, Tanner's proof in [3] also holds for the minimum stopping set. □

Theorem 8: The minimum weight of LU $(3,q)$ obtained from H is $2q$. Consequently, the weight of the minimum stopping set of LU $(3,q)$ obtained from H is also $2q$.

Proof: By Theorem 7, the minimum weight of LU $(3,q)$ is at least $2q$. Therefore, finding a codeword of weight $2q$ in LU $(3,q)$ obtained from H will complete the proof of the theorem.

Let α be a primitive element of GF (q). Consider a word W containing the following points:

1) $(\alpha^{-2},0,0)$, which lies only on lines of the form $[x,\alpha^{-2}x,\alpha^{-4}x]$;
2) $(\alpha^{-2},\alpha^k,\alpha^{k-1})$, $0 \leq k \leq q-2$, which lies only on lines of the form $[x,\alpha^{-2}x+\alpha^k,\alpha^{-4}x+\alpha^{k-2}+\alpha^{k-1}]$;
3) $(\alpha^{-1},0,0)$, which lies only on lines of the form $[x,\alpha^{-1}x,\alpha^{-2}x]$;
4) $(\alpha^{-1},\alpha^{l+2},\alpha^l)$, $0 \leq l \leq q-2$, which lies only on lines of the form $[x,\alpha^{-1}x+\alpha^{l+2},\alpha^{-2}x+\alpha^{l+1}+\alpha^l]$.

These $2q$ points are distinct, so W has weight $2q$. We show that W is a codeword.

Lines of the form 1) and 2) never coincide. Lines of the form 3) and 4) never coincide. A line of the form 1) coincides with a line of the form 3) if and only if $x = 0$; it coincides with a line of the form 4) if and only if $x = \frac{\alpha^{l+4}}{1-\alpha}$. A line of the form 2) coincides with a line of the form 3) if and only if $x = \frac{\alpha^{k+2}}{1-\alpha}$; it coincides with a line of the form 4) if and only if $x = \frac{\alpha^{l+4}-\alpha^{k+2}}{1-\alpha}$. Now let L be a line of the form 1). If $x = 0$, then L is also of the form 3), but not of the forms 2) or 4). So L contains only two points of W, namely, $(\alpha^{-2},0,0)$ and $(\alpha^{-1},0,0)$. If $x \neq 0$, then L coincides with a unique line of the form 4) given by the unique l such that $x = \frac{\alpha^{l+4}}{1-\alpha}$, but not with any line of the form 2) or 3). So L contains only two points of W, namely $(\alpha^{-2},0,0)$ and $(\alpha^{-1},\alpha^{l+2},\alpha^l)$. Let L be a line of the form 2). Then L does not coincide with any line of the form 1). If $x \neq 0$, then L coincides with a unique line of the form 3) given by the unique k such that $x = \frac{\alpha^{k+2}}{1-\alpha}$; in that case, L cannot coincide with a line of the form 4), since lines of the forms 3) and 4) never coincide. So L contains only two points of W, namely, $(\alpha^{-2},\alpha^k,\alpha^{k-1})$ and $(\alpha^{-1},0,0)$. If $x = 0$, then L cannot coincide with a line of the form 3), but it does coincide with a unique line of the form 4) given by $l = k-2$, so again L contains only two points of W. Let L be a line of the form 3). If $x = 0$, then L coincides with a unique line of type 1) and no line of type 2) or 4). If $x \neq 0$, then L coincides with a unique line of type 2) and no line of type 1) or 4). In any case, L contains only two points of W. Let L be a line of type 4). If $x \neq 0$, then L coincides with a unique line of type 1) and no line of type 2) or 3). If $x = 0$, then L coincides with a unique line of type 2) and no line of type 1) or 3). In any case, L contains only two points of W. We have shown that each line containing a point of W contains precisely two points of W. Therefore, W is a codeword. □

From the preceding examples for $q = 3$ and $q = 5$, it seems that for odd q, LU $(3,q)$ derived from H^T has minimum weight larger than $2q$.

IV. THE PARTIAL ROW CONSTRUCTION

In investigating the LU $(3,q)$ codes, we found many that have low rates. We decided to consider those codes whose parity-check matrices consist of the first i rows of $H(m,q)$, where $i < q^m$ (we order the rows and columns lexicographically as in Section II). We call this the partial row construction. If we consider a code C whose parity-check matrix consists of the first i rows of $H(m,q)$, then the rate of C may stay the same or be higher than that of LU (m,q), the girth of its Tanner graph may stay the same or go up, but the minimum weight might go down. We found a number of interesting LDPC codes by the partial row construction for $m = 2$, which we list in Table II.

When $q = 8$ and the number of rows is 64, this code is LU $(2,8)$. Note that the $[9,4,4]$, $[16,9,4]$, and $[64,37,10]$ codes are optimal (i.e., have the highest minimum weight for their length and dimension), whereas the $[25,12,6]$ and $[81,32,16]$ codes are just 2 short of being optimal [16]. The other two codes have minimum weight 4 less than the optimal codes. The parity-check matrix for the $[9,4,4]$ code consists of the first six rows of $H(2,3)$ given in the example in Section II.

IEEE Proof

TABLE II
LDPC CODES OBTAINED BY THE PARTIAL ROW CONSTRUCTION FROM LU $(2,q)$ CODES

q	$[n,k,d]$	(girth, diameter)	# of rows of $H(2,q)$
3	[9,4,4]	(8,4)	6
4	[16,9,4]	(8,4)	8
5	[25,12,6]	(6,4)	14–15
7	[49,24,8]	(6,4)	27–28
8	[64,37,10]	(6,4)	57–64
9	[81,32,16]	(6,4)	53–54
11	[121,84,8]	(6,4)	39

TABLE III
CODES FROM LU $(3,q)$ CODES BY THE PARTIAL ROW CONSTRUCTION USING $H(3,q)$ OR $H^T(3,q)$

q	$[n,k,d]$	(girth, diameter)	matrix	# of rows
3	[27,12,4]	(16,10)	H	15
3	[27,10,6]	(12,8)	H	18
4	[64,35,4]	(8,10)	H^T	33
5	[125,54,14]	(8,6)	H^T	85
5	[125,47,20]	(8,6)	H^T	105

We also improve the rate while maintaining the minimum weight, girth, and diameter for LU $(2,q)$ codes by the partial row construction. We list them below as follows:

$$\begin{array}{llll} \text{old} & [25,4,10] & [49,6,14] & [81,8,18] \\ \text{new} & [25,6,10] & [49,10,14] & [81,14,18]. \end{array}$$

We obtain interesting LDPC codes from LU $(3,q)$ codes by the partial row construction. They are listed in Table III. Many have larger girths than the LU $(3,q)$ code. We list only those where we were able to find the minimum weight.

V. THE CASES $m = 4,5,6,7$

The equations for $D(m,q)$ for $m = 4,5,6,7$ are considerably more complicated than for $m = 2,3$. They can be found in [4].

$D(m,2)$ is disconnected for $m = 3,4,5,6$, and 7. In [4], the authors state that they and A. J. Woldar proved that for $m \geq 6$, all $D(m,q)$ are disconnected. In fact, in [6, p. 79] it is shown that for $q = 3$ and for $q > 4$, $D(m,q)$ has q^{t-1} connected components, where $t = \lfloor \frac{m+2}{4} \rfloor$, and for $m \geq 4$ $D(m,4)$ has 4^t connected components. So even though the graphs $D(m,q)$ have large girth (at least $2\lceil m/2 \rceil + 4$), the large length of the code and the disconnectedness makes them more difficult to use as Tanner graphs of LDPC codes. We do know the following.

Theorem 9: When $D(m,q)$ is disconnected, it is a union of isomorphic connected subgraphs. In this case, LU (m,q) is a direct sum of equivalent codes each of which has its parity-check matrix from the incidence matrix of a connected component subgraph.

Proof: When $D(m,q)$ is disconnected, it is a union of isomorphic connected subgraphs since the group of $D(m,q)$ is edge transitive [4]. This is so because if an automorphism of a graph maps an edge e into an edge f, then it maps the connected component of e onto the connected component of f. So, if for every two edges of $D(m,q)$ there is an automorphism mapping one onto the other, then for every two connected components there is an automorphism mapping one onto the other.

We can reorder the rows and the columns of $H(m,q)$ by putting the rows and the columns of the first connected component first, the rows and the columns of the second connected component second, etc. From this we can see that LU (m,q) is a direct sum of codes. Codes corresponding to distinct connected components are equivalent, since the connected components are isomorphic. □

We found directly that LU $(4,4)$, a $[256,88,8]$ code, is a direct sum of four $[64,22,8]$ codes of girth 8 and diameter 6; and that LU $(5,4)$, a $[1024,216]$ code, is a direct sum of four $[256,54]$ codes of girth 10 and diameter 8.

Since we have a lower bound of $2\lceil m/2 \rceil + 4$ on the girth, a lower bound on the minimum weight can be obtained.

Theorem 10: The minimum weight d of LU (m,q) satisfies

$$d \geq \begin{cases} 2\frac{(q-1)^{\lfloor m/4 \rfloor+1}-1}{q-2}, & \text{if } m \equiv 0 \bmod 4, \\ 2\frac{(q-1)^{\lfloor m/4 \rfloor+2}-1}{q-2}, & \text{if } m \equiv 3 \bmod 4, \\ 2\frac{(q-1)^{\lfloor m/4 \rfloor+1}-1}{q-2} + \frac{2}{q}(q-1)^{\lfloor m/4 \rfloor+1}, & \text{otherwise.} \end{cases}$$

When $q = 2$, the fraction $\frac{(q-1)^{\lfloor m/4 \rfloor+1}-1}{q-2}$ is understood to be $\lfloor m/4 \rfloor + 1$, and $\frac{(q-1)^{\lfloor m/4 \rfloor+2}-1}{q-2}$ to be $\lfloor m/4 \rfloor + 2$. The same bound holds for the weight of the minimum stopping set.

Proof: This bound on the minimum weight follows directly from [3, proof of Theorem 2], using the fact that the column sums of $H(m,q)$ are q. However, Tanner's proof in [3] also holds for the minimum stopping set. □

In particular, $d \geq 2q$ for $m = 3,4$; $d \geq 4q - 3$ for $m = 5,6$; $d \geq 2(q^2 - q + 1)$ for $m = 7,8$; and $d \geq 4(q-1)^2 + 4$ for $m = 9,10$, and $q > 2$.

VI. SIMULATION RESULTS

Some of our codes were simulated with help of Dr. Marc Fossorier and Chris Hruby. We give some explanation about our simulation result appearing in Figs. 1 through 5. For $m = 2$, we considered a $[64,37,10]$ code, denoted $LU28c$, which was constructed by the partial row construction (see Table II). For $m = 3$, we tested four codes LU $(3,q)$, denoted $LU3qt$ where $q = 7,8,9$, and 11, all of which come from the transpose of $H(3,q)$. For our codes $LU28c$ and $LU3qt$, we considered the sum product/belief propagation (BP) algorithm which produces the best error performance under pure iterative decoding, a version of belief propagation based on ordered statistics (BP-OSD1) described in [17], and maximum-likelihood decoding (MLD). We considered both word-error rate (WER) and bit-error rate (BER) with a maximum of 500 iterations for BP and a maximum of 50 iterations for OSD1. The simulations were done over the additive white Gaussian noise (AWGN) channel. We compared $LU3qt$ with random codes defined below using BP with a maximum of 500 iterations. Our random codes are denoted by $R3, R4, R5$, and $R6$ where the attached number means that the corresponding parity-check matrix has the constant column weight 3, 4, 5, and 6, respectively. Each random code has the same length as our compared code and has either

IEEE Proof

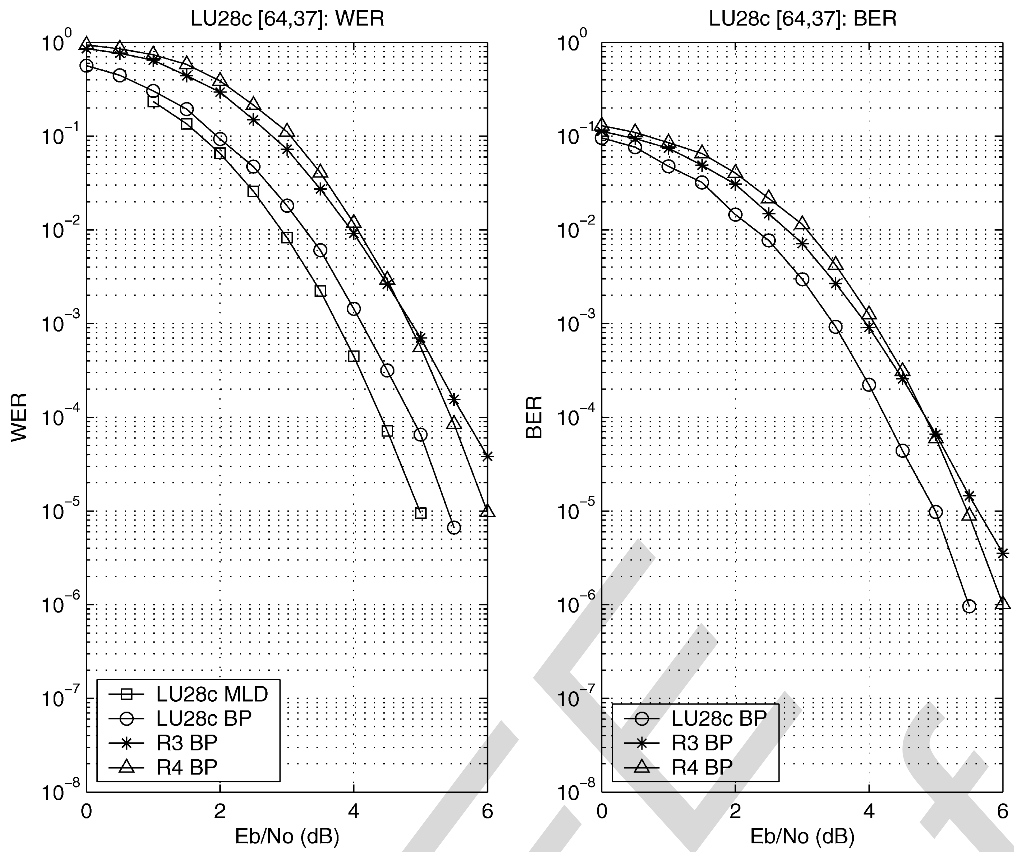

Fig. 1. A $[64, 37, 10]$ code $LU28c$ from LU $(2, 8)$ by partial row construction, maximum of 500 (50) iterations for BP (MLD), $R3$ $(R4)$ is a $[64, 37]$ ($[64, 38]$) code both with 64×27 HMatrix, HMatrix of $R3$ $(R4)$ has three (13) rows of wt 8 (10) and 24 (14) rows of wt 7 (9), respectively.

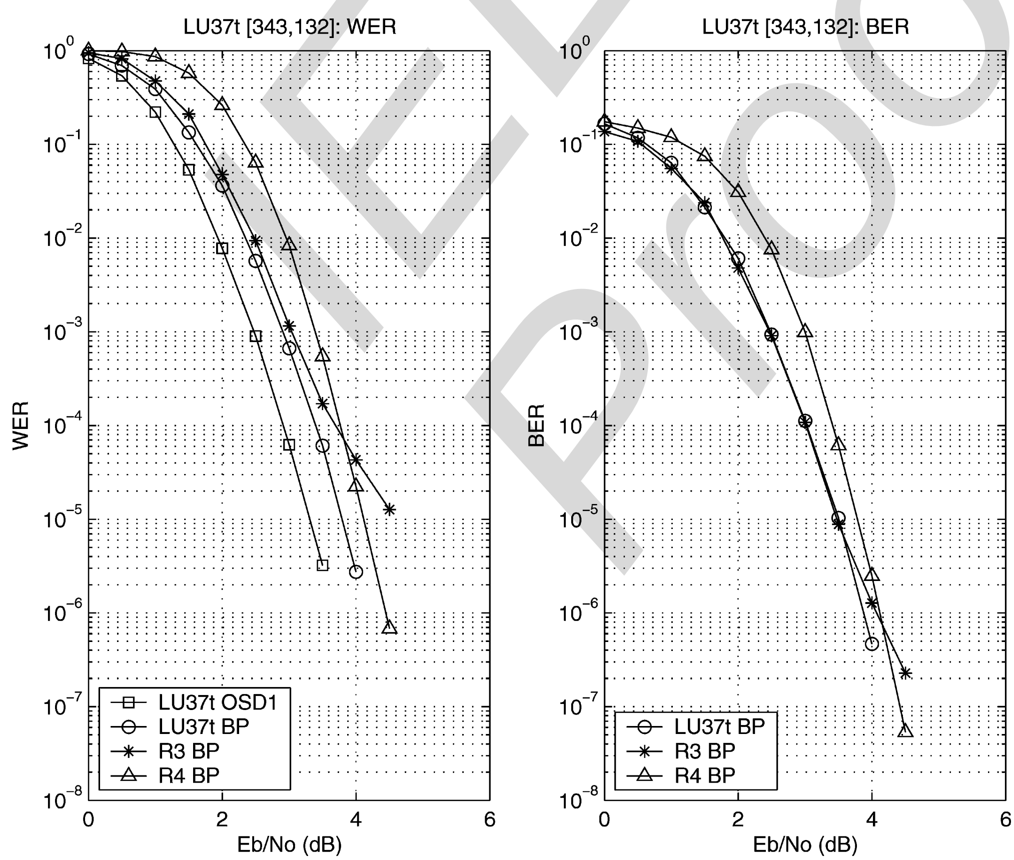

Fig. 2. LU $(3, 7)$ code from $H(3, 7)^T$, maximum of 500 (50) iterations for BP (OSD1), $R3$ $(R4)$ is a $[343, 132]$ ($[343, 133]$) code both with 343×211 HMatrix, HMatrix of $R3$ $(R4)$ has 185 (106) rows of wt $5(7)$, and 26 (105) rows of wt $4(6)$, respectively.

IEEE Proof

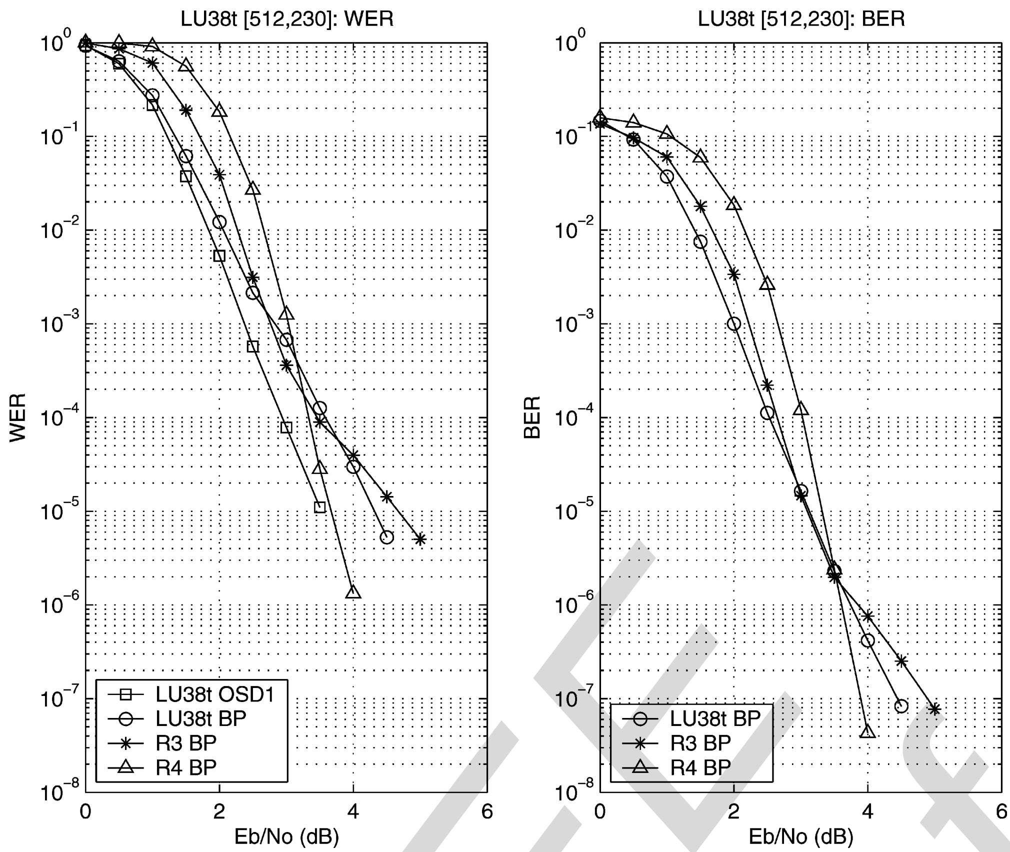

Fig. 3. LU $(3, 8)$ code from $H(3, 8)^T$, maximum of 500 (50) iterations for BP (OSD1), $R3$ ($R4$) is a $[512, 230]$ ($[512, 231]$) code both with 512×282 HMatrix, HMatrix of $R3$ ($R4$) has 126 (74) rows of wt $6\ (8)$ and 156 (208) rows of wt $5\ (7)$, respectively.

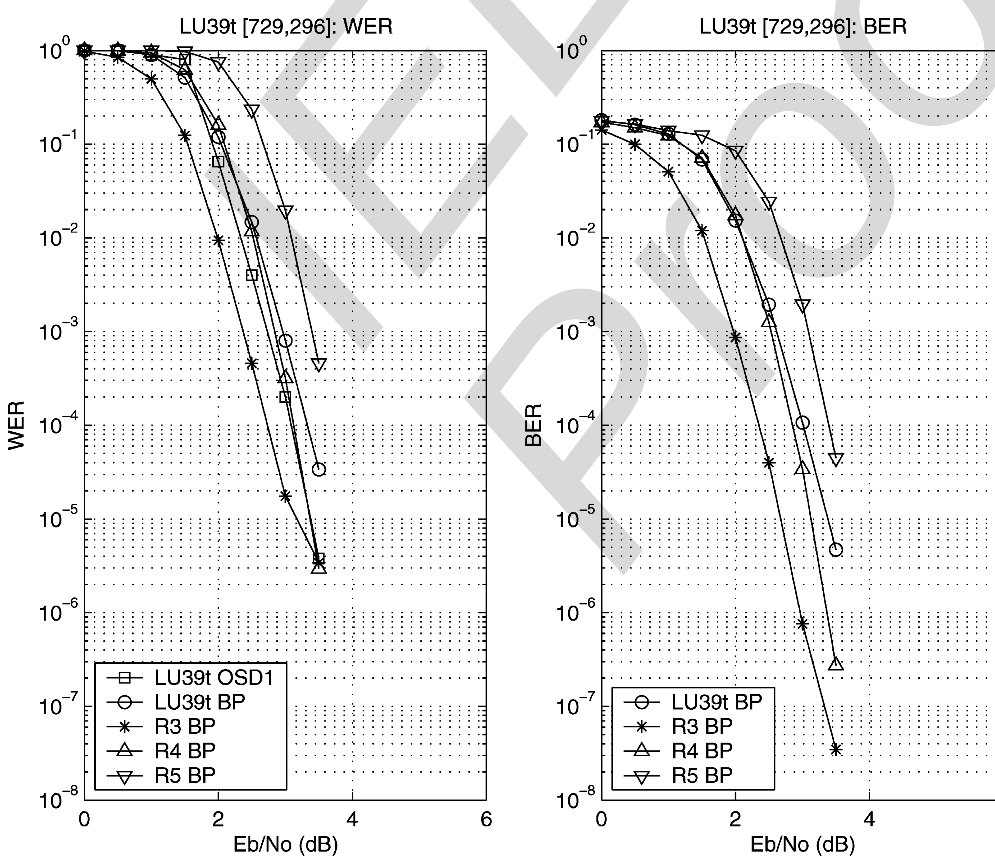

Fig. 4. LU $(3, 9)$ code from $H(3, 9)^T$, maximum of 500 (50) iterations for BP (OSD1), $R3$ and $R5$ ($R4$) are $[729, 296]$ ($[729, 297]$) codes all with 729×433 HMatrix, HMatrix of $R3$ ($R4$, $R5$) has 22 (318, 181) rows of wt $6(7,\ 9)$ and 411 (115, 252) rows of wt $5\ (6, 8)$, respectively.

IEEE Proof

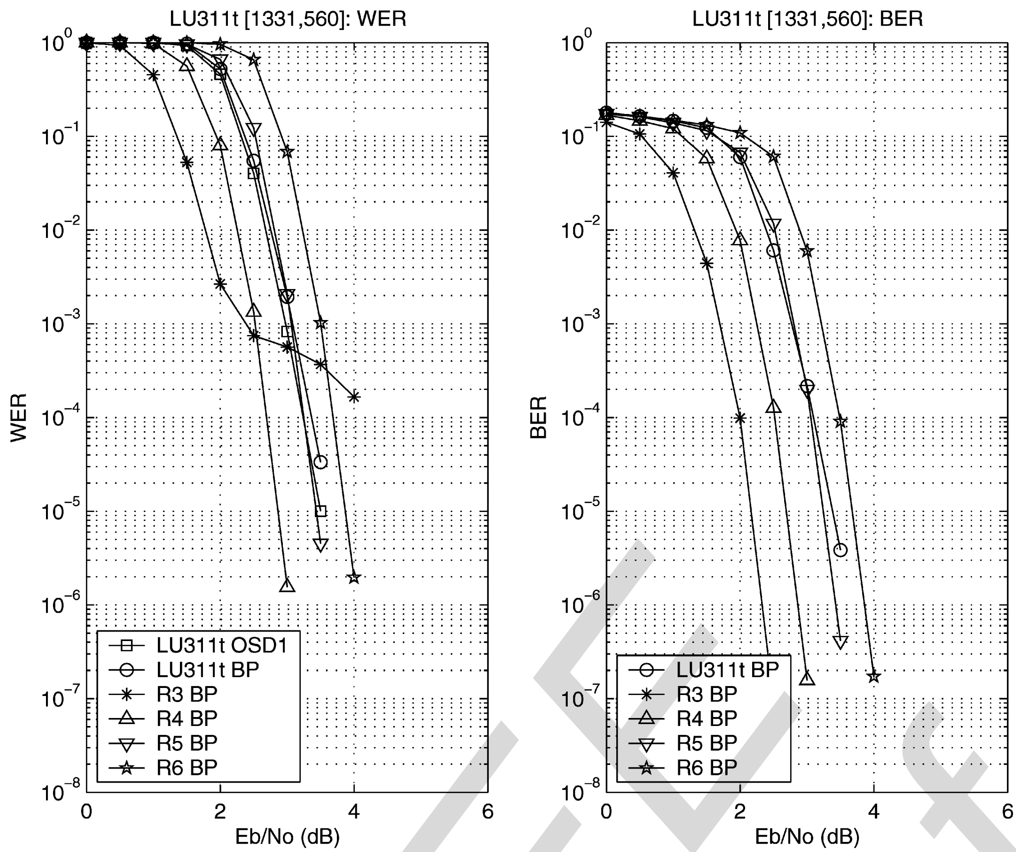

Fig. 5. LU $(3,11)$ code from $H(3,11)^T$, maximum of 500 (50) iterations for BP (OSD1), $R3$ and $R5$ ($R4$ and $R6$) are $1331, 560]$[([$1331, 561$]) codes all with 1331×771 HMatrix, HMatrix of $R3$ ($R4$, $R5$, $R6$) has 138\; (698, 487, 276) rows of wt 6 $(7,9,11)$ and 633 (73, 284, 495) rows of wt 5 $(6,8,10)$, respectively.

the same dimension as our compared code or one more. Random codes were not eliminated based on their girth.

It is seen that the codes $LU28c$, $LU37t$, and $LU38t$ perform better than random codes with respect to both WER and BER, whereas $R3$ (in Fig. 4) performs better than $LU39t$ and $R4$ (in Fig. 5) performs better than $LU311t$ with respect to both WER and BER, even though $R3$ (in Fig. 5) performs much better than $LU311t$ for 1 dB less than 2.5 with respect to WER.

We remark that since our $H(3,q)^T$ are N by N matrices, whereas the random codes are M by N $(M < N)$, the BP algorithm has to do more calculations for the LU $(3,q)$ codes than for the random codes due to more rows in the $H(3,q)^T$ matrix. Although some random codes perform better that LU codes, LU codes being constructive have implementation advantages.

Appendix
Proof of Theorem 6

We begin by a series of lemmas determining the ranks of certain matrices. Then we proceed to obtain an upper bound on the rank of $H(3,p)$ when p is an odd prime, using the previous results.

Lemma 2: Let $x_1,\dots,x_m$ be indeterminates, and consider the $m \times m$ matrix

$$A(x_1,\dots,x_m) = (a_{ij})_1^m, \quad a_{ij} = (x_j)^i - 1$$

over $\mathbb{Z}$. Then

$$\det A(x_1,\dots,x_m) = \prod_{0\le i<j\le m} (x_j - x_i), \text{ where } x_0 = 1. \quad (1)$$

Proof: Consider the $(m+1)\times(m+1)$ Vandermonde matrix with variables $x_0, x_1, \dots, x_m$, and substitute $x_0 = 1$. The determinant of the resulting matrix is given by the right-hand side of (1). If we subtract the first row from all other rows and then expand the determinant by the first column, we see that it is also equal to the left-hand side of (1). □

Lemma 3: If t is an indeterminate, then

$$\det(t^{i\cdot j} - 1)_1^m = \prod_{0\le i<j\le m} (t^j - t^i). \quad (2)$$

Proof: This is a special case of Lemma 2, where $x_j = t^j$ for all $j = 1,\dots,m$. □

Lemma 4: Let $\zeta \in \mathbb{C}$ be a primitive sth root of unity, and consider the matrix $A(m,\zeta) = (\zeta^{ij} - 1)_1^m$. Then the rank of $A(m,\zeta)$ is $\min(s-1, m)$.

Proof: This is trivial for $s=1$, where $\zeta=1$ and $A(m,\zeta)=0$, so we assume $s > 1$. Our first case is $m \le s-1$. Then $\zeta^0,\dots,\zeta^m$ are all distinct, and so Lemma 3 shows that the rank of $A(m,\zeta)$ is m. Our second case is $m \ge s$. Then row i of $A(m,\zeta)$ vanishes for each $1 \le i \le m$ that is divisible by s. If $1 \le i \le m$ is not divisible by s, we write $i = sq + r$ with $1 \le r < s$, and then row i of $A(m,\zeta)$ is equal to row r. It follows that the row-space of $A(m,\zeta)$ is spanned by the first $s-1$

IEEE Proof

rows, which are linearly independent by the first case. Hence, the rank of $A(m,\zeta)$ is $s-1$. □

For a positive integer q, we denote by I_k an identity matrix of order q whose rows are cyclically shifted k positions to the right, i.e., $(I_k)_{i,j} = 1$ if $j - i \equiv k \bmod q$, 0 otherwise. For example, with $q = 5$, we have

$$I_2 = \begin{pmatrix} 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \end{pmatrix}.$$

Note that $I_k = I_1^k$ for all integers k (not necessarily positive, so, for example, I_2 above is equal to I_{-3}). For positive integers m and q, we denote by M the block matrix with m block rows and m block columns, where the (i,j) block is $I_{i\cdot j} - I_0$ of order q. For example, with $m = 3$, we have

$$M = \begin{pmatrix} I_1 - I_0 & I_2 - I_0 & I_3 - I_0 \\ I_2 - I_0 & I_4 - I_0 & I_6 - I_0 \\ I_3 - I_0 & I_6 - I_0 & I_9 - I_0 \end{pmatrix}$$

where the subscripts in the I_k can be reduced $\bmod\ q$ if desired. Recall that the Euler function $\phi(n)$ is defined by

$$\phi(n) = |\{k \in \mathbb{Z} \mid 1 \le k \le n,\ \gcd(k,n) = 1\}|.$$

Lemma 5: With M defined above, the rank of M over $\mathbb{C}$ is

$$\sum_{\substack{1 \le s \le q \\ s \mid q}} \phi(s) \min(s-1, m). \quad (3)$$

Proof: If ζ is a qth root of unity, then $(1, \zeta, \ldots, \zeta^{q-1})^T$ is an eigenvector of I_1 with eigenvalue ζ. Therefore, if $X = (\zeta_i^{j-1})_{i,j=1}^q$ is the Vandermonde matrix corresponding to all the qth roots of unity $\zeta_1, \ldots, \zeta_q$, then

$$I_1 = XDX^{-1}, \qquad \text{where } D = \mathrm{diag}(\zeta_1, \ldots, \zeta_q). \quad (4)$$

Let X_m be the $m \times m$ block-diagonal matrix $\mathrm{diag}(X, \ldots, X)$. The matrix $X_m^{-1} M X_m$ has the same rank as M. By (4), the (i,j)th block of $X_m^{-1} M X_m$ is the $q \times q$ diagonal matrix $\mathrm{diag}(\zeta_1^{ij} - 1, \ldots, \zeta_q^{ij} - 1)$. By permuting the rows of $X_m^{-1} M X_m$ so that rows $1, q+1, \ldots, (m-1)q+1$ come first, then rows $2, q+2, \ldots (m-1)q+2$, and so on, and likewise for columns, we see that $X_m^{-1} M X_m$ is permutationally similar to the block-diagonal matrix

$$\bigoplus_{k=1}^{q} (\zeta_k^{ij} - 1)_{i,j=1}^m \quad (5)$$

($m \times m$ blocks, q block rows, and q block columns). Thus, the rank of M is the sum of the ranks of the diagonal blocks in (5). To find the rank of the kth diagonal block, let ζ_k be a primitive sth root of unity, so that $s|q$. By Lemma 4, the rank of the kth diagonal block is $\min(s-1, m)$. Since there are exactly $\phi(s)$ primitive sth roots of unity, the sum of the ranks of the diagonal blocks is given by (3). □

We now consider M as a binary matrix, so that its (i,j) block can be written as $I_{ij} + I_0$.

Lemma 6: If q is an odd positive integer, then the binary rank of M defined above is again given by (3).

Proof: Consider the polynomial $f(t) = t^q - 1$ over GF(2). Since q is odd, we have $f'(t) = qt^{q-1} = t^{q-1}$, so f and f' are relatively prime in GF(2)[t], and so the roots of f are simple. Let $\mathbb{F}$ be a finite extension field of GF(2) such that $f(t)$ splits over $\mathbb{F}$: $f(t) = (t-\zeta_1)\cdots(t-\zeta_q)$. Thus, $\zeta_1, \ldots, \zeta_q$ are qth roots of unity in $\mathbb{F}$. They are distinct since f has simple roots, so they comprise all the qth roots of unity in $\mathbb{F}$. We can then repeat the entire argument from Lemma 2 through Lemma 5 in $\mathbb{F}$ instead of in $\mathbb{C}$, and we obtain that the rank of M over $\mathbb{F}$ is given by (3). However, the rank over $\mathbb{F}$ is the same as the binary rank, since the entries of M are in GF(2), and the rank is the largest order of a nonzero minor. □

Lemma 7: If p is an odd prime and $1 \le m \le p-1$, then the binary rank of M defined above is $m(p-1)$.

Proof: This is a special case of Lemma 6. □

We now shift our attention to $H(3,q)^T$. Its rows are indexed by triples (a,b,c) with $a,b,c \in$ GF(q), and we let $R(a,b,c)$ denote the row indexed by (a,b,c). Similarly, the columns are indexed by triples $[x,y,z]$ with $x,y,z \in$ GF(q), and we let $C[x,y,z]$ denote the corresponding column. As before, we call a *row block* the set of all q^2 rows $R(a,b,c)$ with the same a, and we also call a *row subblock* a set of all q rows $R(a,b,c)$ with the same (a,b). Similarly, for *column blocks* and *column subblocks*.

Recall from Definition 2 that $R(a,b,c)$ meets $C[x,y,z]$ (i.e., $H(3,q)^T$ has a 1 in this row and column) if and only if $y = ax + b$ and $z = ay + c$. It follows that the $q \times q$ intersection of a row subblock and a column subblock is either zero or a permutation matrix. In the latter case, we say that the row subblock and the column subblock *meet*. Moreover, each row subblock meets exactly one column subblock of each column block.

Lemma 8: For each (a,b,c) and each $a' \ne a$, one has

$$\sum_{b'} R(a', b', ab' - a'b + c) + \sum_{b''} R(a, b'', a'(b'' - b) + c) = 0. \quad (6)$$

Proof: We need to show that each column $C[x,y,z]$ meets an even number of rows involved in the left-hand side of (6). Column $C[x,y,z]$ meets $R(a', b', ab' - a'b + c)$ if and only if $y = a'x + b'$ and $z = a'y + ab' - a'b + c$. These two equations can be satisfied by at most one value of b', and such b' exists if and only if

$$z = a'y + a(y - a'x) - a'b + c.$$

Similarly, $C[x,y,z]$ meets $R(a, b'', a'(b'' - b) + c)$ if and only if $y = ax + b''$ and $z = ay + a'(b'' - b) + c$. Again, these two equations can be satisfied by at most one value of b'', and such b'' exists if and only if

$$z = ay + a'(y - ax - b) + c.$$

Since the conditions of existence of b' and of b'' are equivalent, $C[x,y,z]$ meets exactly zero or exactly two rows involved in the left-hand side of (6). □

IEEE Proof

From now on we assume that p is an odd prime. Then any nonzero intersection of a row subblock and a column subblock has the form of a circulant I_c of order p.

Definition 3: A vector of the form $\sum_c R(a,b,c)$, i.e., the sum of the rows in a given row subblock, is said to be of Type I. A vector of the form $R(a,b,c)$ with $a+b \le p-1$ and $c \neq 0$ is said to be of Type II.

Lemma 9: The span of all p^2 vectors of Type I has dimension p^2-p+1.

Proof: Since p is odd, and since each row subblock meets exactly one column subblock of each column block, a vector of Type I is the all-one vector in exactly one column subblock of each column block, and is zero in all other column subblocks. Therefore, the rank of the matrix A whose rows are all the p^2 vectors of Type I is the same as the rank of the matrix of order p^2 obtained from A by suppressing all but one column in each column subblock. But by Definitions 1 and 2, the latter matrix is precisely $H(2,p)^T$, whose rank is p^2-p+1 by Theorem 2. □

Let B be the set of vectors consisting of all vectors of Type II and a basis of the span of the vectors of Type I.

Lemma 10: B consists of $(p^3+2p^2-3p+2)/2$ vectors.

Proof: There are $(p+1)p(p-1)/2$ vectors of Type II, and by Lemma 9 there are p^2-p+1 vectors in the basis of the span of the vectors of Type I, totaling $(p^3+2p^2-3p+2)/2$ vectors. □

Lemma 11: B spans the row-space of $H(3,p)^T$.

Proof: Consider a row subblock (a,b) satisfying $a+b \le p-1$. Since all its rows $R(a,b,c)$ with $c \neq 0$ are of Type II, and since $\sum_c R(a,b,c)$ is of Type I and thus in span B, it follows that all the rows of this subblock are in span B. Therefore, it is enough to prove that all rows $R(a,b,c)$ with $a+b \ge p$ are spanned by the rows $R(a,b,c)$ with $a+b \le p-1$ and the vectors of Type I. We do this by induction on a. In fact, we prove that for each a, all the rows $R(a,b,c)$ with $a+b \ge p$ are spanned by the rows of the form $R(a',\cdot,\cdot)$ with $a' \le a-1$, the rows of the form $R(a,b',\cdot)$ with $a+b' \le p-1$, and the vectors of Type I of the form $R(a,b,0)$ with $a+b \ge p$. We denote by $\mathcal{S}$ the span of the latter rows.

The basis of the induction for $a=1$ follows directly from Lemma 8. We assume now that $a \ge 2$, and apply Lemma 8 with $a' \le a-1$. Since the first summation in (6) is in $\mathcal{S}$, so is the second

$$\text{for } a' \le a-1, \qquad \sum_{b''} R(a,b'',a'(b''-b)+c) \in \mathcal{S}. \quad (7)$$

In (7), let a' take two values in turn: $a'=0$ and $a'=a'_2$ with $1 \le a'_2 \le a-1$, then add the two resulting equations to obtain: for $1 \le a'_2 \le a-1$

$$\sum_{b''} R(a,b'',c) + \sum_{b''} R(a,b'',a'_2(b''-b)+c) \in \mathcal{S}. \quad (8)$$

When b'' takes the value b in both summations of (8), the two terms cancel out. Furthermore, the terms involving b'' such that $a+b'' \le p-1$ are in $\mathcal{S}$, and so: for $1 \le a'_2 \le a-1$

$$\sum_{\substack{p-a \le b'' \le p-1 \\ b'' \neq b}} [R(a,b'',c)+R(a,b'',a'_2(b''-b)+c)] \in \mathcal{S}. \quad (9)$$

Now given a and $a'_2 \in \{1,\ldots,a-1\}$, choose $b=p-a$. Then (9) represents p linear equations (one equation for each value of c) in the $p(a-1)$ unknown rows $R(a,b'',\cdot)$ with $b'' \in \{p-a+1,\ldots,p-1\}$. If we let a'_2 take each value in $\{1,\ldots,a-1\}$, we obtain a total of $p(a-1)$ equations in our $p(a-1)$ unknown rows. It is not hard to check that the coefficient matrix of these equations is the matrix M appearing in Lemma 6.

For example, suppose $p=5$ and $a=3$. For $a'_2=1$ and $c=0$, (9) reads

$$R(3,3,0)+R(3,3,1)+R(3,4,0)+R(3,4,2) \in \mathcal{S};$$

for $a'_2=1$ and $c=1$ (9) reads

$$R(3,3,1)+R(3,3,2)+R(3,4,1)+R(3,4,3) \in \mathcal{S};$$

and so on. The coefficient matrix M of all these equations is displayed at the bottom of the page, where each column labeled by (a,b'',c) (where $b''=3,4$, $c=0,1,2,3,4$) represents one of the $5(3-1)=10$ unknowns $R(a,b'',c)$, and each row labeled

		a	3	3	3	3	3	3	3	3	3	3
		b''	3	3	3	3	3	4	4	4	4	4
a'_2	c	c	0	1	2	3	4	0	1	2	3	4
1	0		1	1				1		1		
1	1			1	1				1		1	
1	2				1	1				1		1
1	3					1	1	1			1	
1	4		1				1		1			1
2	0		1		1			1				1
2	1			1		1		1	1			
2	2				1		1		1	1		
2	3		1			1				1	1	
2	4			1			1				1	1

.

IEEE Proof

by (a_2', c) (where $a_2' = 1, 2$, $c = 0, 1, 2, 3, 4$) represents one of the $5(3-1) = 10$ equations. It is seen that in this example

$$M = \begin{pmatrix} I_0 + I_1 & I_0 + I_2 \\ I_0 + I_2 & I_0 + I_4 \end{pmatrix}$$

confirming the general form of the matrix M in Lemma 6.

By Lemma 6, the rank of M is $(p-1)(a-1)$ in general. Our unknown rows also satisfy the additional $a-1$ linear equations

$$\text{for } b'' = b+1, \ldots, b+a-1, \qquad \sum_c R(a, b'', c) \in \mathcal{S} \quad (10)$$

expressing the fact that the sum on the left is a vector of Type I. The coefficient matrix N of the (10) has $a-1$ rows, each having the all-one vector in one block column and zero in all other block columns. In our above example, where $q = 5$, $a = 3$

$$N = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & & & & & \\ & & & & & 1 & 1 & 1 & 1 & 1 \end{pmatrix}.$$

Clearly, the rows of N are linearly independent, and furthermore, they are not spanned by the rows of M, since the rows of N have odd weights and the rows of M have even weights. So the combined coefficient matrix of the linear (9) and (10) in our $p(a-1)$ unknown rows has rank

$$(p-1)(a-1) + (a-1) = p(a-1).$$

Therefore, (9) and (10) express all the unknown rows of the form $R(a, b'', \cdot)$ with $b'' \in \{p-a+1, \ldots, p-1\}$ as members of $\mathcal{S}$.

The remaining unknown rows for the given a have the form $R(a, p-a, \cdot)$. To deal with them, we make another choice of b in (9), namely, $b = p-1$. When b was $q-a$ and we let b'' run over its allowed values in (9), $b'' - b$ ran over $1, \ldots, a-1$ in order; now that $b = p-1$, we see that $b'' - b$ runs over $-a+1, \ldots, -1$ in order. In our example, where $q = 5$, $a = 3$, the matrix of coefficients of the resulting equations is given by

$$M' = \begin{pmatrix} I_0 + I_{-2} & I_0 + I_{-1} \\ I_0 + I_{-4} & I_0 + I_{-2} \end{pmatrix}$$

and, in general, M' has the same shape of M, but its (i, j) block is $I_0 + I_{-i(a-1-j)}$. It follows that M' is obtained from M by reversing the order of the block columns, as well as the order of the columns in each block column and the order of the rows in each block row. Therefore, M and M' have the same rank, and the previous argument shows that all the unknown rows of the form $R(a, b'', \cdot)$ with $b'' \in \{p-a, \ldots, p-2\}$ are also members of $\mathcal{S}$. □

Proof of Theorem 6: The proof follows from Lemmas 10 and 11 and the fact that $H(3, p)^T$ has p^3 rows. □

ACKNOWLEDGMENT

We wish to thank Keith Mellinger for calling our attention to [6] and a referee for pointing out that some LU codes are array codes. We also thank Marc Fossorier at the University of Hawaii at Manoa and Chris Hruby at the University of Nebraska at Lincoln for simulating some of our codes (see Section VI) and answering our questions.

REFERENCES

[1] R. G. Gallager, "Low density parity check codes," *IRE Trans. Infom. Theory*, vol. IT-8, pp. 21–28, Jan. 1962.
[2] D. J. C. MacKay and R. M. Neal, "Near Shannon limit performance of low density parity check codes," *Electron. Lett.*, vol. 32, no. 18, pp. 1645–1646, 1996.
[3] R. M. Tanner, "A recursive approach to low complexity codes," *IEEE Trans. Inform. Theory*, vol. IT–27, pp. 533–547, Sept. 1981.
[4] F. Lazebnik and V. A. Ustimenko, "Explicit construction of graphs with arbitrary large girth and of large size," *Discr. Appl. Math.*, vol. 60, pp. 275–284, 1997.
[5] F. Lazebnik and A. J. Woldar, "General properties of some families of graphs defined by systems of equations," *J. Graph Theory*, vol. 38, pp. 65–86, 2001.
[6] R. Viglione, "Properties of some algebraically defined graphs," Ph.D. dissertation, Univ. Delaware, Newark, 2002.
[7] C. Di, D. Proietti, İ. E. Telatar, T. J. Richardson, and R. L. Urbanke, "Finite-length analysis of low-density parity-check codes on the binary erasure channel," *IEEE Trans. Infom. Theory*, vol. 48, pp. 1570–1579, June 2002.
[8] J. L. Fan, "Array codes as low-density parity-check codes," in *Proc. 2nd Int. Symp. Turbo Codes and Related Topics*, Brest, France, 2000, pp. 543–546.
[9] B. Vasic, "A class of codes with orthogonal parity checks and its application in partial responce channels with iterative decoding," in *Proc. 40th Allerton Conf. Communication, Control and Computing*, Monticello, IL, Oct. 2–4, 2002.
[10] O. Milenkovic, K. Prakash, and B. Vasic, "Regular and irregular low density parity check codes for iterative decoding based on cycle-invariant difference sets," in *Proc. 41st Allerton Conf. Communication, Control and Computing*, Monticello, IL, Oct. 1–3, 2003.
[11] J.-L. Kim, U. N. Peled, I. Perepelitsa, and V. Pless, "Explicit construction of families of LDPC codes of girth at least six," in *Proc. 40th Allerton Conf. Communication, Control and Computing*, P. G. Voulgaris and R. Srikant, Eds., Monticello, IL, Oct. 2–4, 2002, pp. 1024–1031.
[12] E. F. Assmus Jr. and J. D. Key, *Designs and Their Codes*. Cambridge, U.K.: Cambridge Univ. Press, 1992.
[13] W. C. Huffman and V. Pless, *Fundamentals of Error-Correcting Codes*. Cambridge, U.K.: Cambridge Univ. Press, 2003.
[14] 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*, vol. 47, pp. 2711–2736, Nov. 2001.
[15] J. Cannon and C. Playoust, *An Introduction to Magma*. Sydney, Australia: Univ. Sydney Press, 1994.
[16] A. E. Brouwer, "Bounds on the size of linear codes," in *Handbook of Coding Theory*, V. S. Pless and W. C. Huffman, Eds. Amsterdam, The Netherlands: Elsevier, 1998, pp. 295–452.
[17] M. P. C. Fossorier and S. Lin, "Soft-decision decoding of linear block codes based on ordered statistics," *IEEE Trans. Inform. Theory*, vol. 41, pp. 1379–1396, Sept. 1995.

IEEE Proof

Jon-Lark Kim (S'01–A'03–M'04) received the B.S. degree in mathematics from Pohang University of Science and Technology (POSTECH), Pohang, Korea, in 1993, the M.S. degree in mathematics from Seoul National University, Seoul, Korea, in 1997, and the Ph.D. degree in mathematics from the University of Illinois at Chicago, in 2002.

Since fall 2002, he has been with the Department of Mathematics at the University of Nebraska-Lincoln as a Research Assistant Professor. He visited the Department of Pure Mathematics and Computer Algebra at the Ghent University, Ghent, Belgium in June/July, 2003. His areas of interest include algebraic coding theory with connections to combinatorics, graph theory, finite geometry, number theory, and algebraic geometry, as well as cryptography using error-correcting codes or elliptic curves. He is also interested in quantum information theory.

Uri N. Peled is a Professor of Mathematics and Computer Science in the Department of Mathematics, Statistics, and Computer Science at the University of Ilinois at Chicago. He has been there since 1982, following a position at Columbia University, New York, NY. He has been a Visiting Professor at the University of Rome, Rome, Italy; École Polytechnique Fédérale de Lausanne, Lausanne, Switzerland; Northeastern University, Boston, MA; the Fields Institute, Chicago, IL (**is this location OK? If not, please give location. Thank you**); and the University of Haifa, Haifa, Israel. He was a Long-Term Visitor of the Caesarea Edmond Benjamin de Rothchild Foundation Institute of Interdisciplinary Application of Computer Science at the University of Haifa. He is the author (with N.V.R. Mahadev) of *Threshold Graphs and Related Topics* (amsterdam, The Netherlands: Elsevier, 1995). His areas of interest include graph theory, combinatorial optimization, and combinatorics.

Irina Perepelitsa received the B.S. and M.S. degrees in mathematics from Novosibirsk State University, Novosibirsk, Russia.

Currently she is working toward the Ph.D. degree at the University of Illinois at Chicago. Her areas of interest include coding theory, graph theory, and combinatorics.

Vera Pless (M'74-SM'98) has been a Professor of Mathematics and Computer Science in the Department of Mathematics, Statistics and Computer Science at the University of Illinois at Chicago since 1975. She was a Visiting Professor at Dartmouth College, Hanover, NH; the California Institute of Technology, Pasadena; and the University of Wisconsin-Madison. She has been a Lady Davis Professor of Computer Science at the Technion–Israel Institute of Technology, Haifa. She is on the editorial boards of the *Journal of Combinatorial Theory (A)*, *Finite Fields and Their Applications*, and the *SIAM Journal on Discrete Mathematics*. She is the author of *Introduction to the Theory of Error-Correcting Codes* (3rd ed) (New York: Wiley, 1998) and was the editor (with W.C. Huffman) of *Handbook of Coding Theory* (Amsterdam, The Netherlands: Elsevier, 1998). She coauthored (W.C. Huffman) *Fundamentals of Error-Correcting Codes* (Cambridge, U.K.: Cambridge Univ. Press, 2003). Her areas if interest include error-correcting codes and combinatorics.

Shmuel Friedland has been a Professor of Mathematics and Computer Science in the Department of Mathematics, Statistics and Computer Science at the University of Illinois at Chicago since 1985. Prior to that he was a Professor at the Hebrew University in Jerusalem, Israel. He was also a Visiting Professor in Stanford University, Stanford, CA; the Institute for Advanced Study, Princeton, NJ; University of Wisconsin-Madison; Cornell University, Ithaca, NY; IHES **(au: Please spell out the name of the institution and cite city in France. Thank you)** in France. He was the Lady Davis Professor at the Technion–Israel Institute of Technology, Haifa, and New Direction Professor in the Institute for Mathematics and its Application at the University of Minnesota, Minneapolis. He is on the editorial boards of the *Journal of Linear Algebra and its Applications* and *Electronic Journal of Linear Algebra*. His professional interests are in matrices and their applications, dynamical systems, and entropy computations in statistical mechanics.

Prof. Friedland is a recipient of the first Hans Schneider prize in Linear Algebra (1993).

IEEE Proof