involve
a journal of mathematics

The truncated and supplemented Pascal matrix and applications

Michael Hua, Steven B. Damelin, Jeffrey Sun and Mingchao Yu

msp

2018 vol. 11, no. 2

INVOLVE 11:2 (2018)
dx.doi.org/10.2140/involve.2018.11.243

The truncated and supplemented Pascal matrix and applications

Michael Hua, Steven B. Damelin, Jeffrey Sun and Mingchao Yu

(Communicated by Jim Haglund)

In this paper, we introduce the $k \times n$ (with $k \leq n$) truncated, supplemented Pascal matrix, which has the property that any k columns form a linearly independent set. This property is also present in Reed–Solomon codes; however, Reed–Solomon codes are completely dense, whereas the truncated, supplemented Pascal matrix has multiple zeros. If the maximum distance separable code conjecture is correct, then our matrix has the maximal number of columns (with the aforementioned property) that the conjecture allows. This matrix has applications in coding, network coding, and matroid theory.

1. Introduction

Finite field linear algebra is an import branch of linear algebra. Instead of using the infinite field $\mathbb{R}$, it uses linearly independent vectors consisting of a finite number of elements, which can be represented by a finite number of bits. It has thus motivated many practical coding techniques, such as Reed–Solomon codes [1960] and linear network coding [Li et al. 2003; Ho et al. 2006]. It is also closely related to structural matroid theory through matroid representability [Oxley 2011; Oxley et al. 1996; El Rouayheb et al. 2010; Yu et al. 2014].

One of the most important problems in finite field linear algebra is finding the size of the largest set of vectors over a k-dimensional finite field such that every subset of k vectors is linearly independent [Ball 2012; Ball and De Beule 2012]. From a matrix perspective, the problem is described as:

Problem 1.1. *Consider a finite field $\mathbb{F}_q$, where $q = p^h$, for p a prime and h a nonnegative integer. Given a positive integer k, what is the largest integer n such that there exists a $k \times n$ matrix $\boldsymbol{H}$ over $\mathbb{F}_q$, in which every set of k columns is linearly independent?*

MSC2010: primary 05B30, 05B35, 94B25; secondary 05B05, 05B15, 11K36, 11T71.
Keywords: matroid, Pascal, network, coding, code, MDS, maximum distance separable.
Hua and Sun gratefully acknowledge support from the National Science Foundation under grants 0901145, 1160720, 1104696. Damelin was supported by the American Mathematical Society.

Such a matrix, upon its existence, could be the generator matrix of an $[n, k]$ maximum distance separable (MDS) code [Lin and Costello 2004], which can correct up to $d = n - k$ bits of erasures or $t = d/2$ bits of errors. We will thus refer to $\boldsymbol{H}$ as an MDS matrix. Its existence also determines the representability of uniform matroids, which we will discuss in detail in Section 4C. The maximal value of n, according to the MDS conjecture, is $q + 1$, unless $q = 2^h$ and $k = 3$ or $k = q - 1$, in which case $n \leq q + 2$. This conjecture has been recently proved for any $q = p$ in [Ball 2012; Ball and De Beule 2012], but a complete proof of it remains open.

Therefore, it is crucial to understand the construction of $k \times (q+1)$ MDS matrices. In coding theory literature, many construction algorithms have been proposed to meet certain coding requirements. However, their computational complexity is not necessarily satisfactory. On one hand, multiplications and additions over large finite fields are required in the matrix construction. On the other hand, the resultant MDS matrix may have low sparsity (or high density), which is measured by the number of zeros in the matrix. Low sparsity can be translated into higher encoding and decoding complexity. It is an open question how these algorithms can be generalized and provide new insights into related fields, such as network coding theory and matroid theory.

In this paper, we investigate the above problems by first proposing in Section 2 a new type of MDS matrix called a *supplemented Pascal matrix*. A supplemented Pascal matrix can be generated by additions and, in particular, without multiplications. It also has guaranteed number of zero entries for high sparsity. We will prove that a supplemented Pascal matrix is an MDS matrix in Section 3. We will then extend our results into a general code construction framework in Section 4A, and then discuss its applications to network coding theory and matroid theory in Sections 4B and 4C, respectively.

2. Definitions

For clarity we should first label the elements of a finite field. Henceforth, let p be a prime and h be a nonnegative integer. A finite field $\mathbb{F}_q$ contains $q = p^h$ elements, each represented by a polynomial $g(x) = \sum_{i=0}^{h-1} \beta_i x^i$, whose coefficients are $\{\beta_i\}_{i=0}^{h-1} \in [0, p - 1]$. The elements $g(x)$ take on distinct values between 0 and $q - 1$ at $x = p$, which can be used as an intuitive index of the elements. Specifically, we define a index function $\sigma_q(n)$:

Definition 2.1. For any integer $n \in [0, q - 1]$, $\sigma_q(n)$ is the element of $\mathbb{F}_q$ whose polynomial coefficients satisfy $\sum_{i=0}^{h-1} \beta_i p^i = n$.

For example, given $q = 2^3$, we have $\sigma_q(0) = 0$, $\sigma_q(1) = 1$, and $\sigma_q(5) = x^2 + 1$.

Based on $\sigma_q(n)$, we define a finite field binomial polynomial $f_{m,q}(n)$:

$$f_{m,q}(n) = \begin{cases} 1 = [\sigma_q(n)]^m, & m = 0, \\ \displaystyle\prod_{i=1}^{m} \frac{\sigma_q(n) - \sigma_q(i-1)}{\sigma_q(i)}, & m > 0, \end{cases} \tag{1}$$

where $\{m, n\} \in [0, q-1]$ are nonnegative integers. Intuitively, $f_{m,q}(n)$ is a polynomial in $\sigma_q(n)$ of degree m.

Based on $f_{m,q}(n)$, we introduce the key matrix in this paper, called the *Pascal matrix*:

Definition 2.2. Define the matrix $\boldsymbol{P}_q$ over $\mathbb{F}_q$ as the $q \times q$ matrix with elements $\boldsymbol{P}_q(m, n) = f_{m,q}(n)$:

$$\boldsymbol{P}_q = \begin{bmatrix} f_{0,q}(0) & f_{0,q}(1) & \cdots & f_{0,q}(q-1) \\ f_{1,q}(0) & f_{1,q}(1) & \cdots & f_{1,q}(q-1) \\ \vdots & \vdots & \ddots & \vdots \\ f_{q-1,q}(0) & f_{q-1,q}(1) & \cdots & f_{q-1,q}(q-1) \end{bmatrix}. \tag{2}$$

Note that $f_{m,q}(n) = 0$ for $m > n$ and so $\boldsymbol{P}_q$ is an upper-triangular Pascal matrix. For brevity, we simply call it the Pascal matrix.

Note that the matrix index starts from 0.

Example 2.3. When $q = 2^2 = 4$, we have

$$\boldsymbol{P}_4 = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 & x & x+1 \\ 0 & 0 & 1 & x+1 \\ 0 & 0 & 0 & 1 \end{bmatrix}.$$

Our considered matrix $\boldsymbol{P}_q$ is named after Pascal because its entries are binomial coefficients, which is the same as the traditional Pascal matrix, except that the field applied here is $\mathbb{F}_q$, as opposed to $\mathbb{Z}_{\geq 0}$ in the traditional case. Indeed, when $q = p$, the matrix $\boldsymbol{P}_p$ is equal to the traditional Pascal matrix modulo p.

Example 2.4. When $q = p = 5$, the traditional Pascal matrix $\boldsymbol{P}_{5,T}$ and our Pascal matrix $\boldsymbol{P}_5$ are given by

$$\boldsymbol{P}_{5,T} = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 2 & 3 & 4 \\ 0 & 0 & 1 & 3 & \mathbf{6} \\ 0 & 0 & 0 & 1 & 4 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix} \quad \text{and} \quad \boldsymbol{P}_5 = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 2 & 3 & 4 \\ 0 & 0 & 1 & 3 & \mathbf{1} \\ 0 & 0 & 0 & 1 & 4 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}.$$

Indeed, the construction of the Pascal matrix over $\mathbb{F}_p$ shares the same additive formula as the traditional Pascal matrix. Explicitly, $\boldsymbol{P}_p(m,n) = \boldsymbol{P}_p(m-1, m-1) + \boldsymbol{P}_p(m, n-1)$ for every pair of $\{m, n\} \in [1, q-1]$ (note that addition is modulo p). This idea appears in Section 4B.

Definition 2.5. The truncated Pascal matrix $\boldsymbol{P}_{q,k}$ is the Pascal matrix $\boldsymbol{P}_q$ truncated to the first k rows.

Example 2.6. Consider the matrix $\boldsymbol{P}_5$ given in Example 2.4. The truncated Pascal matrix $\boldsymbol{P}_{5,2}$ is given by

$$\boldsymbol{P}_{5,2} = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 2 & 3 & 4 \end{bmatrix}.$$

Definition 2.7. A *supplemented Pascal matrix*, denoted by $\boldsymbol{H}_{q,k}$, is a truncated Pascal matrix $\boldsymbol{P}_{q,k}$ appended with a column vector $\boldsymbol{s}_k$, which has a one in the bottom entry and zeros everywhere else:

$$\boldsymbol{H}_{q,k} = \left[\begin{array}{c|c} & 0 \\ & \vdots \\ U_{q,k} & 0 \\ & 1 \end{array}\right]. \tag{3}$$

Example 2.8. Supplementing the matrix $\boldsymbol{P}_{5,2}$ in Example 2.6 gives

$$\boldsymbol{H}_{5,2} = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 1 & 2 & 3 & 4 & 1 \end{bmatrix}.$$

Our supplemented Pascal matrix has a desirable property, namely:

Theorem 2.9. *Any k columns of $\boldsymbol{H}_{q,k}$ are linearly independent.*

3. Proof of Theorem 2.9

We will first prove the following property of $\boldsymbol{P}_{q,k}$, and then prove that $\boldsymbol{H}_{q,k}$ preserves this property.

Lemma 3.1 (truncation lemma). *Any k columns of $\boldsymbol{P}_{q,k}$ are linearly independent.*

Proof. We first note that $\boldsymbol{P}_q$ (and thus $\boldsymbol{P}_{q,k}$) has the important property that all the entries in the m-th row (recall m begins at 0) are defined by the same polynomial $f_{m,q}(n)$, which is a polynomial in $\sigma_q(n)$ of degree m. Recall also that $\boldsymbol{P}_q$ (and thus $\boldsymbol{P}_{q,k}$) is upper-triangular. Indeed, we have that $f_{m,q}(n)$ has m roots in $\mathbb{F}_q$ (counting multiplicity). Consequently, the first m entries of the m-th row are all zeros.

Given a truncated Pascal matrix $\boldsymbol{P}_{q,k}$, suppose there exist k distinct values of n such that the columns $\{n_0, n_1, \ldots, n_{k-1}\}$ of $\boldsymbol{P}_{q,k}$ constitute a linearly dependent set. In other words, there exists a $k \times k$ submatrix $\boldsymbol{M}$ of $\boldsymbol{P}_{q,k}$,

$$\boldsymbol{M} = \begin{bmatrix} f_{0,q}(n_0) & f_{1,q}(n_1) & \cdots & f_{1,q}(n_{k-1}) \\ f_{1,q}(n_0) & f_{2,q}(n_1) & \cdots & f_{2,q}(n_{k-1}) \\ \vdots & \vdots & \ddots & \vdots \\ f_{k-1,q}(n_0) & f_{k-1,q}(n_1) & \cdots & f_{k-1,q}(n_{k-1}) \end{bmatrix}, \tag{4}$$

whose rank is smaller than k.

If this is the case, then there must exist a nonzero vector $[a_0, a_1, \ldots, a_{k-1}] \in \mathbb{F}_q$ such that $\boldsymbol{aM} = \boldsymbol{z}$, where $\boldsymbol{z} = [z_0, z_1, \ldots, z_{k-1}] = [0, 0, \ldots, 0]$:

$$[a_0, a_1, \ldots, a_{k-1}]\boldsymbol{M} = [0, 0, \ldots, 0].$$

Recall that the m-th row of $\boldsymbol{P}_{q,k}$ (and thus $\boldsymbol{M}$) is defined by $f_{m,q}(n)$. Correspondingly, $\boldsymbol{z}$ is defined by

$$f'_q(n) \triangleq \sum_{m=0}^{k-1} \alpha_m f_{m,q}(n),$$

where $0 = \boldsymbol{z}(i) = f'_q(n_i) = 0$ for all $i \in [0, k-1]$. We also note that the degree of $f'_q(n)$ is at most $k-1$, because the highest degree of its summands is the degree of $f_{k-1,q}(n)$ with a value of $k-1$.

Therefore if the columns $\{n_0, n_1, \ldots, n_{k-1}\}$ of $\boldsymbol{P}_{q,k}$ constitute a linearly dependent set, then we will obtain a polynomial $f'_q(n)$ such that

- its degree is at most $k-1$;
- it has k roots, whose values are $\{\sigma_q(n_0), \sigma_q(n_1), \ldots, \sigma_q(n_{k-1})\}$.

However, with a degree of at most $k-1$, $f'_q(n)$ can only have at most $k-1$ roots unless $f'_q(n) = 0$, which is not the case because $\boldsymbol{a}$ is nonzero. Hence, $f'_q(n)$ does not exist, and thus our hypothesis is invalid. Therefore, every k columns of $\boldsymbol{P}_{q,k}$ are linearly independent. Thus Lemma 3.1 is proved. □

Since $\boldsymbol{H}_{q,k}$ is constructed by appending $\boldsymbol{s}_k$ to $\boldsymbol{P}_{q,k}$, to prove Theorem 2.9 we only need to prove that any $k-1$ columns of $\boldsymbol{P}_{q,k}$ and $\boldsymbol{s}_k$ together never constitute a linearly dependent set. To see this, we can simply use $\boldsymbol{s}_k$ to linearly cancel the first q entries in the last row of $\boldsymbol{H}_{q,k}$. This will transform $\boldsymbol{H}_{q,k}$ from (3) into

$$\boldsymbol{H}'_{q,k} = \left[\begin{array}{ccc|c} & & & 0 \\ & \boldsymbol{P}_{q,k-1} & & 0 \\ & & & \vdots \\ 0 & \cdots & 0 & 1 \end{array}\right], \tag{5}$$

which indicates that $\boldsymbol{s}_k$ is orthogonal to all the other columns of $\boldsymbol{H}'_{q,k}$. Then, by applying the truncation lemma to $\boldsymbol{P}_{q,k-1}$, we know that every $k-1$ out of the first q columns of $\boldsymbol{H}'_{q,k}$ are linearly independent. Adding $\boldsymbol{s}_k$ to them will yield a linearly independent set of k. Theorem 2.9 is thus proved.

4. Applications

4A. *Coding theory.* The truncation lemma can be immediately generalized to any appropriately defined $k \times n$ matrix over $\mathbb{F}_q$ that satisfies (1) $n \le q$, and (2) the m-th row ($m \in [0, k-1]$) is defined by a polynomial of degree m. For example, by setting $f_{m,q}(n) = \sigma_q(n)^{m-1}$, we can obtain a $k \times n$ matrix over $\mathbb{F}_q$ such that every set of k columns is a linearly independent set. Indeed, this matrix is the generator matrix $\boldsymbol{G}$ of an $[n, k]$ Reed–Solomon code:

$$\begin{bmatrix} \sigma_q(1)^0 & \sigma_q(2)^0 & \cdots & \sigma_q(n)^0 \\ \sigma_q(1) & \sigma_q(2) & \cdots & \sigma_q(n) \\ \sigma_q(1)^2 & \sigma_q(2)^2 & \cdots & \sigma_q(n)^2 \\ \vdots & \vdots & \ddots & \vdots \\ \sigma_q(1)^{k-1} & \sigma_q(2)^{k-1} & \cdots & \sigma_q(n)^{k-1} \end{bmatrix}.$$

Then by appending $\boldsymbol{s}_k$, we can obtain an $[n+1, k]$ extended Reed–Solomon code. Therefore, our polynomial approach is a general approach of constructing *nontrivial* $[n, k]$ MDS codes. It also indicates that the maximum length of any MDS code is at least $q+1$ for any $k \leqslant q$. This result is in agreement with the MDS conjecture [Ball 2012; Ball and De Beule 2012].

Among all the possible constructions, the supplemented Pascal matrix $\boldsymbol{H}_{q,k}$ enjoys a high sparsity, which is the number of zeros in the matrix. Higher sparsity is advantageous, because it generally leads to easier encoding/decoding. However, the sparsity has an upper bound. In the following lemma, we will prove that $\boldsymbol{H}_{q,k}$ approximates this bound with a factor of $\frac{1}{2}$:

Lemma 4.1 (matrix sparsity). *The number of zeros in the supplemented Pascal matrix $\boldsymbol{H}_{q,k}$ is $\frac{1}{2}$ of the maximum sparsity of any $[n, k]$ code.*

Proof. Since any $k \times k$ submatrix of $\boldsymbol{G}$ has a rank of k, there is no all-zero row in this matrix. Hence, there are at most $k-1$ zeros in each row of $\boldsymbol{G}$, and at most k^2-k zeros in total. Recall that in $\boldsymbol{H}_{q,k}$ the m-th row has $m+1$ zeros for $m \in [0, k-2]$ and the $(k-1)$-th row has $k-1$ zeros. The total number of zeros is $\frac{1}{2}(k^2+k-2)$. □

4B. *Network coding theory.* Network coding (NC) is a class of packet-based coding techniques. Consider a block of $K \ge 1$ data packets $\{\boldsymbol{x}_k\}_{k=0}^{K-1}$, each containing L bits of information. NC treats these data packets as K variables, and sends in the u-th ($u \in \mathbb{Z}_{\ge 0}$) transmission a linear combination $\boldsymbol{y}_u$ of all of them:

$$\boldsymbol{y}_u = \sum_{k=0}^{K-1} \alpha_{k,u} \boldsymbol{x}_k, \tag{6}$$

where coefficients $\{\alpha_{k,u}\}_{k=0}^{K-1}$ are elements of a finite field $\mathbb{F}_q$.

Ideally, NC is able to allow any receiver that has received any K coded packets to decode all the K data packets by solving a set of K linear equations. To this end, the associated coefficient matrix $\boldsymbol{C}$, where

$$\boldsymbol{C} = \begin{bmatrix} \alpha_{0,0} & \alpha_{0,1} & \cdots \\ \alpha_{1,0} & \alpha_{1,1} & \cdots \\ \vdots & \vdots & \\ \alpha_{K-1,0} & \alpha_{K-1,1} & \cdots \end{bmatrix}, \tag{7}$$

must satisfy that every set of K columns of it is a linearly independent set. Once this condition is met, NC is able to achieve the optimal throughput in wireless broadcast scenarios [Yu et al. 2014].

However, it is highly nontrivial to meet this condition, which hinders the implementation of NC. First, to guarantee the linear independence, the sender chooses coefficients randomly from a sufficiently large $\mathbb{F}_q$ [Lucani et al. 2009; Heide et al. 2009] or regularly collects receiver feedback to make online coding decisions [Fragouli et al. 2007]. While a large $\mathbb{F}_q$ incurs heavy computational loads, collecting feedback could be expensive or even impossible in certain circumstances, such as time-division-duplex satellite communications [Lucani et al. 2009]. Second, to enable the decoding, coding coefficients must be attached to each coded packet, which constitute $\lceil K \log_2 q \rceil$ bits of overhead in each transmission. When q is large and L is small, the throughput loss due to the overhead may overwhelm all the other benefits of NC.

These practical shortages of NC can be easily overcome by the proposed supplemented Pascal matrix. By choosing a sufficiently large p and letting $\boldsymbol{C} = \boldsymbol{H}_{p,K}$, we obtain an NC that is both computational friendly (only operations modulo p) and feedback-free. Moreover, for the receivers to retrieve the coding coefficients, the sender only needs to attach the index u to the u-th packet, rather than attaching the complete coefficients. Furthermore, the additive formula for Pascal matrix may enable efficient progressive coding/decoding algorithms, which could be our future research direction.

4C. *Matroid theory.* A matroid $\mathcal{M} = (E, \mathcal{I})$ is a finite collection of elements called the ground set, E, paired with its comprehensive set of independent subsets, $\mathcal{I}$. A uniform matroid U_n^k has $|E| = n$ and the property that *any* subset of size k of E is an element of $\mathcal{I}$ and *no* subset of size $k+1$ is in $\mathcal{I}$. U_n^k is called q-representable if there is a $k \times n$ matrix such that every k columns of it are linearly independent over $\mathbb{F}_q$.

Corollary 4.2 (representability of uniform matroid). *Any uniform matroid U_n^k that satisfies $n \leqslant q+1$ is q-representable by any n columns of $\boldsymbol{H}_{q,k}$.* □

It is known that any uniform matroid U_n^k that satisfies $n \leqslant q+1$ is q-representable [Oxley 2011; Ball 2015; Reed and Solomon 1960]; one can obtain another construction from Reed–Solomon codes. $\boldsymbol{H}_{q,k}$ is just another, sparse example.

5. Conclusion

In this paper, we proposed the supplemented Pascal matrix, whose first k rows are an MDS matrix over $\mathbb{F}_q$ for any prime power q and positive integer $k \leqslant q$. Our construction can be potentially generalized to a framework that enables low-complexity MDS code constructions and encoding/decoding as well. Our matrix can overcome some practical shortages of network coding and, thus, enables high-performance wireless network coded packet broadcast. Our matrix is in agreement with existing results on the representability of uniform matroids, while also providing new insights into this topic. In the future, we intend to study Pascal-based network coding algorithms. We are also interested in applying our results to other fields such as projective geometry and graph theory.

References

[Ball 2012] S. Ball, "On sets of vectors of a finite vector space in which every subset of basis size is a basis", *J. Eur. Math. Soc.* **14**:3 (2012), 733–748. MR Zbl

[Ball 2015] S. Ball, *Finite geometry and combinatorial applications*, London Mathematical Society Student Texts **82**, Cambridge Univ. Press, 2015. MR Zbl

[Ball and De Beule 2012] S. Ball and J. De Beule, "On sets of vectors of a finite vector space in which every subset of basis size is a basis, II", *Des. Codes Cryptogr.* **65**:1-2 (2012), 5–14. MR Zbl

[El Rouayheb et al. 2010] S. El Rouayheb, A. Sprintson, and C. Georghiades, "On the index coding problem and its relation to network coding and matroid theory", *IEEE Trans. Inform. Theory* **56**:7 (2010), 3187–3195. MR

[Fragouli et al. 2007] C. Fragouli, D. Lun, M. Medard, and P. Pakzad, "On feedback for network coding", pp. 248–252 in *CISS '07*, Annual Conference on Information Sciences and Systems **41**, IEEE, Piscataway, NJ, 2007.

[Heide et al. 2009] J. Heide, M. V. Pedersen, F. H. P. Fitzek, and T. Larsen, "Network coding for mobile devices: systematic binary random rateless codes", pp. 1–6 in *IEEE International Conference on Communications Workshops* (Dresden, 2009), IEEE, Piscataway, NJ, 2009.

[Ho et al. 2006] T. Ho, M. Médard, R. Koetter, D. R. Karger, M. Effros, J. Shi, and B. Leong, "A random linear network coding approach to multicast", *IEEE Trans. Inform. Theory* **52**:10 (2006), 4413–4430. MR Zbl

[Li et al. 2003] S.-Y. R. Li, R. W. Yeung, and N. Cai, "Linear network coding", *IEEE Trans. Inform. Theory* **49**:2 (2003), 371–381. MR Zbl

[Lin and Costello 2004] S. Lin and D. J. Costello, *Error control coding, fundamentals and applications*, 2nd ed., Pearson, Upper Saddle River, NJ, 2004. Errata by E. Agrell available at arXiv 1101.2575. Zbl

[Lucani et al. 2009] D. E. Lucani, M. Medard, and M. Stojanovic, "Random linear network coding for time-division duplexing: field size considerations", pp. 1–6 in *GLOBECOM 2009: IEEE Global Telecommunications Conference* (Honolulu, 2009), edited by M. Ulema, IEEE, Piscataway, NJ, 2009.

[Oxley 2011] J. Oxley, *Matroid theory*, 2nd ed., Oxford Graduate Texts in Mathematics **21**, Oxford Univ. Press, 2011. MR Zbl

[Oxley et al. 1996] J. Oxley, D. Vertigan, and G. Whittle, "On inequivalent representations of matroids over finite fields", *J. Combin. Theory Ser. B* **67**:2 (1996), 325–343. MR Zbl

[Reed and Solomon 1960] I. S. Reed and G. Solomon, "Polynomial codes over certain finite fields", *J. Soc. Indust. Appl. Math.* **8**:2 (1960), 300–304. MR Zbl

[Yu et al. 2014] M. Yu, P. Sadeghi, and N. Aboutorab, "On deterministic linear network coded broadcast and its relation to matroid theory", pp. 536–540 in *2014 IEEE Information Theory Workshop* (Hobart, 2014), IEEE, Piscataway, NJ, 2014.

Received: 2016-02-17 Revised: 2016-07-21 Accepted: 2016-12-15

mikwa@umich.edu *Department of Nuclear Engineering and Radiological Sciences and Department of Mathematics, University of Michigan, Ann Arbor, MI, United States*

damelin@umich.edu *Mathematical Reviews, The American Mathematical Society, Ann Arbor, MI, United States*

jeffjeff@umich.edu *Department of Mathematics, University of Michigan, Ann Arbor, MI, United States*

ming.yu@anu.edu.au *College of Engineering and Computer Science, Australian National University, Canberra, Australia*

involve
msp.org/involve

INVOLVE YOUR STUDENTS IN RESEARCH

Involve showcases and encourages high-quality mathematical research involving students from all academic levels. The editorial board consists of mathematical scientists committed to nurturing student participation in research. Bridging the gap between the extremes of purely undergraduate research journals and mainstream research journals, *Involve* provides a venue to mathematicians wishing to encourage the creative involvement of students.

See inside back cover or msp.org/involve for submission instructions. The subscription price for 2018 is US $190/year for the electronic version, and $250/year (+$35, if shipping outside the US) for print and electronic. Subscriptions, requests for back issues and changes of subscriber address should be sent to MSP.

Involve (ISSN 1944-4184 electronic, 1944-4176 printed) at Mathematical Sciences Publishers, 798 Evans Hall #3840, c/o University of California, Berkeley, CA 94720-3840, is published continuously online. Periodical rate postage paid at Berkeley, CA 94704, and additional mailing offices.

Involve peer review and production are managed by EditFLOW® from Mathematical Sciences Publishers.

PUBLISHED BY

mathematical sciences publishers

nonprofit scientific publishing

http://msp.org/

involve

2018 vol. 11 no. 2