An Analytic Approach to the Problem of Matroid Representibility: Summer REU 2015

D. Capodilupo*[1], S. Freedman†[1], M. Hua‡[1], and J. Sun§[1]

[1]Department of Mathematics, University of Michigan

Abstract

A central problem in matroid theory—and by extension coding theory and finite geometry—is the problem of constructing matrices with a maximal number of columns such that every square submatrix formed by a subset of the columns is nonsingular. In this project, we apply the tools of analysis to this problem and demonstrate the value of such an approach. First, we introduce various quantities that can be defined for an arbitrary matroid, and show that certain conditions on these quantities imply that a matroid is not representable over $\mathbb{F}_q$. In particular, for a matroid of rank r, we examine the proportion of size-$(r-k)$ subsets that are dependent, and give bounds, in terms of the cardinality of the matroid and q a prime power, for this proportion, below which the matroid is not representable over $\mathbb{F}_q$. Using an observation about the reduced form of a uniform matrix, we explore connections between the quantities we define. Further, we demonstrate that the defined quantities can be used to prove that random matrices have high proportions of subsets of independent columns. In addition, we construct a uniform matroid using a method analogous to the construction of Pascal's Triangle, generalized for finite fields of non-prime order.

We extend our thanks to Dr Steve Damelin and Dr Ming Yu for their guidance in this project.

The following people also contributed to the discussions regarding the Pascal triangle work and we are thankful to them for their input and to fruitful discussions: Karl Winsor, Sam Tenka and Bar Roytman.

This research was funded by NSF grants: 0901145, 1160720, 1104696.

REU webpage: http://www.ima.umn.edu/∼ damelin/REU.html

1 Introduction of Quantities

By a subset of a matrix we will mean a subset of its columns, and by its size we will mean the total number of columns it has. We will say a matroid is q-representable if it has a matrix representation over $\mathbb{F}_q$.

*dcapo@umich.edu

†samjfree@umich.edu

‡mikwa@umich.edu

§jeffjeff@umich.edu

1.1 A Generalization of Uniformity

First, we generalize a basic definition.

Definition 1.1. *A matroid M of rank r is said to be **uniform** if every size-r subset of M is independent.*

Definition 1.2. *We define the k-**dependence** of a matroid of rank r as the proportion of its size-$(r-k)$ subsets that are dependent. When a matrix has k-dependence 0, we call it k-**independent**, otherwise we call it k-**dependent**. For a matroid M, we will denote rank by $r(M)$, cardinality by $s(M)$, and k-dependence by $d(M,k)$.*

Note that, by these definitions, a matroid M is uniform if $d(M,0) = 0$, i.e., if it is 0-independent.

1.2 Optimal Representable Matrices

It is natural to try to optimize some property of a matroid given given certain constraints, especially q-representability. We use the following symbols to denote optimal achievable quantities:

Definition 1.3.

- *By $Ind_q(r,k,d)$, we mean the largest s such that there exists some full-rank $r \times s$ matrix M over $\mathbb{F}$ with k-dependence $\leq d$. Equivalently, it is the size of the largest q-representable rank-r matroid with k-dependence $\leq d$.*
- *By $D_q(r,k,s)$, we mean the smallest d such that there exists some full-rank $r \times s$ matrix M over $\mathbb{F}_q$ with k-dependence $\leq d$. Equivalently, it is the smallest k-dependence of any q-representable rank-r matroid of size s.*

These quantities prove useful because we can use them to say the following:

Theorem 1.4. *Let M be a matroid. If, for some k,*

- *If $Ind_q(r(M),k,d(M,k)) \leq s(M)$ or*
- *If $D_q(r(M),k,s(M)) \leq d(M,k)$ for some k,*

then M is not q-representable.

2 Equivalences of Bounds

An equivalence between bounds on Ind and on D exist due to the following:

Lemma 2.1. *As a function of s, $D_q(r,k,s)$ is non-decreasing.*

Proof. Let M be a minimally k-dependent q-representable matroid of size s. That is, because we are dealing with finite sets and infima are always achievable,

$$d(M) = D_q(r(M), k, s(M)).$$

Then, for every matroid M' obtained by deletion of one element from M,

$$d(M') \geq D_q(r(M'), k, s(M')) = D_q(r(M) - 1, k, s(M) - 1).$$

Thus, because each size-$(n-k)$ subset is counted an equal number of times in the measurement of the $d(M')$,

$$D_q(r(M), k, s(M)) \geq D_q(r(M) - 1, k, s(M) - 1).$$

□

The equivalence between bounds can be stated thus:

Theorem 2.2.

- *If, for some $q, r, k, d, Ind_q(r, k, d) < s$, then, for any $s' \geq s$, it holds that*

$$D_q(r, k, s') > d.$$

- *If, for some $q, r, k, s, D_q(r, k, s) > d$, then, for any $d' \leq d$, it holds that*

$$Ind_q(r, k, d') < s.$$

3 Explicit Bounds

We give various explicit bounds on Ind and D, on whichever of the two the explanation of the bound is simplest. In each case, the equivalent statement on the other function is implied.

Theorem 3.1. $Ind_q(r, k, 0) \leq q^{k+1}(r - k - 1)$

Proof. Suppose some matroid M is q-representable. Then some $r(M) \times s(M)$ matrix M' over $\mathbb{F}_q$ can be constructed with all size-$(n-k)$ subsets independent.

We treat the columns of M' as vectors in $\mathbb{F}_q^r$, and assume that none of them are the zero vector.

Observe that at most $r - k - 1$ columns of M' can lie within a $(r - k - 1)$-plane. This implies that the proportion between $(r - k - 1)$ and the number of points in an $(r - k - 1)$-plane bounds the proportion of the total number of vectors in $\mathbb{F}_q^r$ that are represented as columns in M'.

Explicitly, this proportion is

$$\frac{r - k - 1}{q^{r-k-1}}$$

out of

$$q^r$$

vectors in the space. Thus, the total number of columns is bounded by

$$q^r \frac{r - k - 1}{q^{r-k-1}} = q^{k+1}(r - k - 1).$$

□

Theorem 3.2. *For some integer n, $D_q(r, k, n\frac{q^n-1}{q-1})$ is minimized by the matrix M consisting of n copies of each unique nonzero vector in $\mathbb{F}_q^r$ up to scaling.*

That is, the matrix consists of exactly n representatives of each point in the projective space.

Proof. Let M as above. The claim is clearly true for $k = n - 2$, in which case M is the only vector of the required size that is $(n-2)$-dependent. We proceed inductively. Let M as above, $\vec{v} \in M$. We can view M as a multiset of points in the projective space $\mathbb{P}^{r-1}(\mathbb{F}_q)$. Let $\mathbb{P}^{r-2}$ be some hyperplane in $\mathbb{P}^{r-1}(\mathbb{F}_q)$. Then a set S including one copy of $\vec{v}$ is independent if and only if the projection of $S \setminus \{\vec{v}\}$ from $\vec{v}$ onto $\mathbb{P}^{r-2}$ is independent. A set containing two copies of $\vec{v}$ is dependent. Thus, removing all copies of $\vec{v}$ from M, we can count the number of independent size-$(n-k)$ sets containing $\vec{v}$ by counting the number of independent size-$(n-k-1)$ points of the projection of the remaining members of M onto $\mathbb{P}^{r-2}$ as above. If M contains one column for each vector in $\mathbb{F}_q^r$, then exactly $q+1$ vectors will be projected to each point in the hyperplane. The $(k-1)$-dependence for that arrangement of vectors in the hyperplane, by the inductive hypothesis, is optimal. □

4 k-extensions

By putting k-independent matrices in a certain form, we can obtain a necessary and sufficient condition for k-independence.

Definition 4.1. *Let M be an $r \times s$ matrix of full rank. Rearrange the columns so that the first r are linearly independent, and form an invertible matrix A. Multiply M by A^{-1}. None of these operations affect which subsets of M are independent. Now, M should be of the form $[Id|M']$, where Id is the identity matrix, and M' is called the "extension". If M is k-independent, we call M' a k-extension.*

In many ways, it turns out to be easier to directly examine the extension of a matrix. For example,

Theorem 4.2. *A matrix M is a k-independent if and only if every $(n+k) \times n$ submatrix of its extension is full-rank, for every n.*

Proof. First, let M' be an $r \times (r + \ell)$ systematic k-dependent matrix constructed with extension M. Because it is k-dependent, there exists some set of $r - k$ columns of M' that sum to zero. Let us say that n of these columns are in the extension, and $(r-k)-n$ of them are in the identity part. Then the n columns combine to a vector with zeroes where all the $k-n$ columns have zeroes, which is in $r - ((r-k)-n) = k+n$ places. Take the submatrix of M that consists of the n columns and the $k+n$ rows that they combine to zero on. Then this submatrix does not have full rank because its columns are dependent.

Next, suspending any requirement on M' other than its size and that the first r columns form an identity matrix, let there exist some $(k+n) \times n$ submatrix of M that is not full-rank. Then its columns combine to the zero vector. In that case, extending this submatrix to the full height r, the n columns combine to a vector $\vec{v}$ with $n+k$ zeroes. Thus, these columns, together with the $r-(n+k)$ columns of the identity with ones where $\vec{v}$ does not necessarily have zeroes, combine to zero. These columns number $r-(n+k)+n = r-k$, and so M' is k-dependent. □

For the case $k = 0$, this was pointed out by [4].
This has many interesting implications:

- Every $r \times (r - k)$ submatrix is full-rank, meaning that any bunch of $n - k$ parallel column n-vectors within the matrix are independent.
- Every $(r + k) \times r$ submatrix S contains an invertible matrix as a subset of its rows. This bounds the number of possible sets of r rows of S that are dependent. It also bounds the number of sets of r rows of any submatrix that are dependent. Looking at the submatrix sideways, this is a condition on dependent columns.
- For the $k = 0$ case, where we are discussing extensions of a uniform matroid, the condition is that all submatrices are of full rank. Equivalently, it is that all square submatrices are invertible. This property is closed under transpose, and so given a uniform matrix matroid, putting it in systematic form (which is always possible), the dual matroid can be constructed by simply taking the transpose of the extension and appending a larger identity matrix. We check that this takes a matrix of size $n \times (n + l)$, with extension of size $n \times l$, and produces a matrix with extension size $l \times n$, of size $l \times (n + l)$.
- Many methods are suggested by this property for making $(k+1)$-extensions out of k-extensions, possibly the simplest being the addition of a zero row to the k-extension. This gives inductive lower bounds on the maximal sizes of k-extensions.
- This implies that any submatrix of a k-extension is a k-extension.
- There are many equivalent ways to state this condition. For example, out of a matrix M, construct the block matrix $M'' = [M|0_k]$, where 0_k stands for the matrix with k zero columns. Then M is a k-extension if and only if every $r \times r$ submatrix of M'' has rank at least $r - k$.
- If the MDS conjecture is true, then the sizes of the 0-extensions are precisely those that can fit in the top triangle of a $q \times q$ matrix.
- A study of the overlapping behavior of k-extensions could be fruitful. That is, whether there are k-extensions that overlap on some submatrix, or whether they are totally overlapping, meaning that they overlap on a submatrix with height the minimum of the heights of the two matrices, and the same with width. If there is sufficient overlapping of k-extensions, then a large matrix with a staircase-shaped nonzero region can be constructed, every rectangular submatrix of whose nonzero region is a k-extension. In the $k = 0$ case, [4] presents such triangles for $p \in \{5, 7\}$
- Similarly, if you can start with an $n \times (q-n)0-$extension which admits either a row addition or a column addition, the MDS conjecture (for that n) is equivalent to being unable to fill in the last entry in the corner not covered by the new row or column. This is because, without the final entry, every submatrix of the matrix with the new column and row is either a submatrix of the row-added matrix or the column-added matrix, so the row-added column-added matrix fulfils the submatrix-rank condition.

- It suggests a generalization of k-dependence to $k < 0$, in which the width of the required full-rank matrices exceed their height. Note that under the transpose, k-extensions are taken to $(-k)$-extensions. This is consistent with 0-extensions being taken to 0-extensions.

5 Random Matrices

Defining two more quantities, this approach can be used to prove that, with very high probability, a very high proportion of the subsets of a certain size of a random matrix are independent.

By "random matrix," we mean a matrix whose columns are randomly chosen nonzero vectors.

Definition 5.1. *Let $Ind_q(r, k, d, p)$ be the largest s, or $D_q(r, k, s, p)$ the smallest d, or $P_q(r, k, d, s)$ the smallest p, such that, with probability $1 - p$, a random $r \times s$ matrix has k-dependence $\leq d$.*

Lemma 5.2. *Denote the probability that $(r - k)$ nonzero vectors chosen randomly from $\mathbb{F}_q^r$ are independent by $\pi_{q,r,k}$. Then,*

$$\pi_{q,r,k} = \prod_{i=0}^{r-k} \frac{q^r - q^i}{q^r - 1}.$$

Proof. Each term of the product divides the number of points outside an i-plane by the number of nonzero points in the space. This is the probability that, given that we have already picked i independent vectors, that the next one we pick will lie outside the span of those i. □

Theorem 5.3.

$$D_q(r, k, s) \leq 1 - \pi_{q,r,k}.$$

Proof. Take a certain choice of $(r - k)$ distinct integers between 1 and r. These correspond to a single size-$(r - k)$ subset of a matrix of size s. Then, the proportion of this particular subset of all size-s matrices that are independent is equivalently $\pi_{q,r,k}$. Since this proportion is equal for any choice of subset, we have that the proportion of all size-$(r - k)$ subsets of all matrices of size s is $\pi_{q,r,k}$. Thus, some matrix achieves this proportion. □

Corollary 5.4. *$1 - \pi_{q,r,k}$ is the mean k-dependence of all $r \times s$ matrices without zero columns.*

Because $\pi_{q,r,k}$ is in general very close to one, viewing p as a proportion of the set of all $r \times s$ matrices, we can get bounds on $D_q(r, k, s, p)$. Specifically,

Theorem 5.5. *For any q, r, k, s, p,*

$$D_q(r, k, s, p) \leq \frac{1 - \pi_{q,d,k}}{p}.$$

Corollary 5.6. *For any q, r, k, s, d,*

$$P_q(r, k, s, d) \leq \frac{1 - \pi_{q,d,k}}{d}.$$

Note that these quantities do not depend on s.

6 Pascal Matrices

Let q be a power of a prime p. In this section, all matrices will be assumed to take entries over F_q. The map σ will be a bijection from $N_{\leq q-1} \cup \{0\}$ to F_q that takes $N_{\leq p-1} \cup \{0\}$ to the prime subfield in the canonical way.

For simplicity, examples will focus on the prime case.

Definition 6.1. *Let F_p denote the prime subfield of F_q. For $n \in F_q, k \in F_p$ we define*

$$\binom{n}{k} = \frac{1}{k!} \prod_{i=0}^{k-1} (n-i)$$

Note that, as a function of n, this is a polynomial of degree k.

Definition 6.2. *The **pascal matrix** U_q is the $q \times q$ matrix with*

$$\{U_q\}_{i,j} = \begin{cases} \binom{\sigma(j-1)}{i-1}, & i \geq j \\ 0, & \text{otherwise.} \end{cases}$$

Example 6.3.

$$U_7 = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 2 & 3 & 4 & 5 & 6 \\ 0 & 0 & 1 & 3 & 6 & 10 & 15 \\ 0 & 0 & 0 & 1 & 4 & 10 & 20 \\ 0 & 0 & 0 & 0 & 1 & 5 & 15 \\ 0 & 0 & 0 & 0 & 0 & 1 & 6 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

Definition 6.4. *Suppose q is a prime power and m is an integer with $0 \leq m \leq q$. The **truncated pascal matrix** $U_{q,m}$ is the pascal matrix U_q truncated to m rows.*

Example 6.5.

$$U_{7,3} = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 2 & 3 & 4 & 5 & 6 \\ 0 & 0 & 1 & 3 & 6 & 10 & 15 \end{bmatrix}$$

Definition 6.6. *A **supplemented pascal matrix**, denoted by $H_{q,m}$, is a truncated pascal matrix $U_{q,m}$ appended with the vector $\vec{s}_m$ with a one in the bottom entry and zeroes everywhere else.*

$$H_{q,m} = \left[\begin{array}{c|c} & 0 \\ U_{q,m} & \vdots \\ & 0 \\ & 1 \end{array}\right]$$

Example 6.7.

$$H_{7,3} = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 1 & 2 & 3 & 4 & 5 & 6 & 0 \\ 0 & 0 & 1 & 3 & 6 & 10 & 15 & 1 \end{bmatrix}$$

6.1 Linear Independence

First we prove that any m columns of $U_{q,m}$ are linearly independent for prime power q. Then we prove that the addition of the vector $(0, 0, ..., 0, 1) = \vec{s}_m$ preserves the property.

Lemma 6.8 (Truncation Lemma)**.** *Any m columns of $U_{q,m}$ are linearly independent.*

Proof. Recall that the entries of the k^{th} row of $U_{q,m}$ are defined by the polynomial $\binom{\sigma(j)}{k}$ of degree $k-1$. In particular, the j^{th} entry is the value of that polynomial at $\sigma(j)$.

Suppose some set of m columns are linearly dependent. Then the rows of the $m \times m$ submatrix they comprise can be combined to zero with at least one nonzero coefficient. However, this implies that the polynomials defining the rows can be combined to a polynomial with m zeros. Since the polynomials are each of degree at most $m-1$, the resulting polynomial would have to be identically zero. Since each polynomial in the combination is of a different degree, this implies that the linear combination has no nonzero coefficients, a contradiction. □

Theorem 6.9. *Any m columns of $H_{q,m}$ are linearly independent.*

Proof. The truncation lemma covers most cases; in fact, we can reduce this to two cases: the case when $\vec{s}_m$ is included in the m-subset, and the case when it is not. In the latter, we are taking a m-subset of $H_{q,m} \setminus \{\vec{s}_m\} = U_{q,m}$. We know this subset is linearly independent by the truncation lemma.
In the former case, we have a $[m \times m]$ matrix with $\vec{s}_m$ as a column. To show the linear independence of the this set, we can show that this submatrix is non-singular. Without loss of generality, we can assume that $\vec{s}_m$ is the mth column, and we can expand along this column. We are then done by the truncation lemma: any $m-1$ columns of $U_{p,m-1}$ are linearly independent. . □

Remark 6.10. *The proofs also work to show that any square submatrix of $H_{q,q}$ is invertible, provided that there is no zero row or column.*

6.2 Coding Theory

Reed-Solomon codes are a class of error-correcting codes. An example of a simple Reed-Solomon code is:

$$\begin{bmatrix} 1 & 1 & \cdots & 1 \\ 1 & 2 & \cdots & q \\ 1^2 & 2^2 & \cdots & q^2 \\ \vdots & \vdots & \ddots & \vdots \\ 1^k & 2^k & \cdots & q^k \end{bmatrix}$$

Note that $(0, \ldots, 0, 1)$ can be appended. It is established in [2],[1] that $H_{q,k}$ is equivalent to a $[k \times q + 1]$ Reed-Solomon code. This code involves multiplication and taking field elements to different powers. The $H_{q,k}$ offers a simpler construction based on addition; it retains the additive structure of Pascal's triangle.

The truncated pascal matrices leads to an efficient, memory-non-intensive network coding algorithm for prime q, especially in the binary case. Set c and t to be variable vectors of length n and s,

respectively. Take d to be the length s vector of data. The following algorithm is an example of a non-memory-intensive encoding process, where shift is taken to be the operation that moves each entry in an array to the next entry, and set the first entry to zero:

```
for i < s:
   t += d[i]*c;
   c += c.shift();
return t
```

References

[1] S. Ball, *On large subsets of a finite vector space in which every subset of a basis size is a basis*, Journal European Math. Soc, J. Eur. Math. Soc, 2012, 14(3): 733-748.

[2] S. Ball and J. De Beulle, *On sets of vectors of a finite vector space in which every subset of basis size is a basis II*, Des. Codes Cryptogr. 65 (2012), no. 1-2, 514.

[3] S. Ball, C. Padro, Z. Weiner and C. Xing, *On the representibility of the bi-uniform matroid*, arXiv 1407.7283v1.

[4] F. J. McWilliams, N. J .A. Sloane, *The Theory of Error Correcting Codes*, Amsterdam, The Netherlands: North Holland, 1977, pp. 323.

[5] K. A. Bush, *Orthogonal arrays of index unity*, Ann. Math. Statist., 23 (1952) 426434.

[6] J. W. P. Hirschfeld, *Maximum sets in finite projective spaces*, Surveys In Combinatorics, London Math. Soc. Lecture Note Series 82, Cambridge University Press, Cambridge, 1983, pp. 5576.

[7] J. W. P. Hirschfeld and G. Korchmaros, *On the embedding of an arc into a conic in a finite plane*, Finite Fields Appl., 2 (1996) 274292.

[8] J. W. P. Hirschfeld and L. Storme, *The packing problem in statistics, coding theory and finite projective spaces, update 2001*, in Developments in Mathematics, 3, Kluwer Academic Publishers. Finite Geometries, Proceedings of the Fourth Isle of Thorns Conference, pp. 201-246.

[9] M. Hu, D. Capodilupo, S. B. Damelin, S. Freeman, J. Sun and M. Yu, *A Note on Truncated Pascal Coding Matrices and Lower Bounds for the Number of Linearly Independent Vectors of Fixed Length over F_q*, submitted.

[10] M. Hua and J. Sun, *Personal Communication*, May 2015.

[11] R. Lidl and H. Niederreiter, *Finite Fields*, Sec. Ed., Encyclo. Math. and Appl., Vol. 20, Cambridge Univ. Press, 1997.

[12] J. Oxley, *Matroid Theory*, Oxford University Press, 1992.

[13] B. Segre, *Introduction to Galois geometries*, Atti Accad. Naz. Lincei Mem., 8 (1967) 133-236.

[14] G. Tallini, *Le geometrie di Galois e le loro applicazioni alla statistica e alla teoria dellinformazione*, Rendiconti di Matematica (3-4), 19(1960), pp. 379-400.

[15] J. F. Voloch, *Complete arcs in Galois planes of non-square order*, in: Advances in Finite Geometries and Designs, Oxford University Press, Oxford, 1991, pp. 401-406.

[16] M. Yu, P. Sadeghi and N. Aboutorab, *On Deterministic linear network codes braodcast and its relation to matroid theory*,

[17] M. Yu and S. B. Damelin *Overview of independent number, matroid theory, and network coding*, Notes, January 2015.