AN INTRODUCTION TO MATROID THEORY

A Dissertation submitted in partial fulfillment of the

requirementfor the award of

DEGREE OF MASTER OF SCIENCE

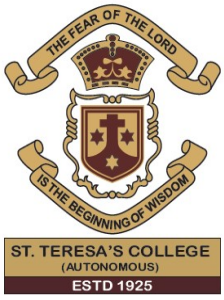
IN MATHEMATICS

By

ANGEL ISSAC

REGISTER NO: SM16MAT002

(2016 – 2018)



DEPARTMENT OF MATHEMATICS

ST.TERESA'S COLLEGE, (AUTONOMOUS)

ERNAKULAM, KOCHI - 682011

APRIL 2018

DEPARTMENT OF MATHEMATICS

ST.TERESA'S COLLEGE (AUTONOMOUS), ERNAKULAM

CERTIFICATE

This is to certify that the dissertation entitled "AN INTRODUCTION TO MATROID THEORY "is a bonafide record of the work done by ANGEL ISSAC under my guidance as partial fulfillment of the award of the degree of Master of Science in Mathematics at St.Teresa's College (Autonomous), Ernakulam affiliated to Mahatma Gandhi University, Kottayam. No part of this work has been submitted for any other degree elsewhere.

Ms.Mary Runiya (Supervisor)

Assistant Professor

Department Of Mathematics

St.Teresa's College,(Autonomous)

Ernakulam

Smt Teresa Felitia (HOD)

Associate Professor

Department of Mathematics

St. Teresa's College (Autonomous)

Ernakulam

External Examiners:

1. ..... **2. .....**

DECLARATION

I hereby declare that the work presented in this project is based on the original work done by me under the guidance of Ms.MARY RUNIYA, Assistant Professor, Department of Mathematics, St Teresa's College (Autonomous) Ernakulam and has not been included in any other project submitted previously for the award of any degree.

ERNAKULAM

APRIL 2018

ANGEL ISSAC

REGISTER NO: SM16MAT002

ACKNOWLEDGEMENT

I bow my head before God Almighty who showered His abundant grace on me to make this project a success.

With great pleasure I express my sincere gratitude to my guide Ms.MaryRuniya ,Assistant Professor ,Department of Mathematics , St.Teresa's College (Autonomous),Ernakulam
for successful completion of this work.

I further express my sincere gratitude to Dr.Sajimol Augustine M, Principal, Rev,Sr.Dr.Celine E, Director, smt.TeresaFelitia Head of the Department of Mathematics, St.Teresa's College, Ernakulam and other teachers of the Department for their encouragement, suggestions and assistance in taking up this dissertation.

I am most graceful to the Library staff for the help extended in accomplishing this work.

I finally thank my parents,friends and all my wellwishers who had supported me during the project.

ERNAKULAM

APRIL 2018

Angel Issac

REGISTER NO: SM16MAT002

INTRODUCTION

Matroid is a structure that generalizes the properties of Independence.Relevant applications are found in graph theory and Linear Algebra.

There are several ways to define a matroid,each relate to the concept of independence. Many results of graph theory extend or simplify in the theory of matroids.

Several difficult theorems about graphs have found easier proofs using matroids.

We can define matroids in terms of bases,the rank function, independent sets,circuits.

We can obsrve that how both graphs and matrices can be viewed as matroids. Then we translate linear to graph theory and vice versausing the language of matroids.

Matroids arise in many contexts but are special enough to have rich combinatorial structure.

When a result from graph theory generalises to matroids it can be interpreted in other special cases.

The matroid theory is a powerful tool in order to study several classes endowed with algebraic structures such as affine spaces, vector spaces, algebraic independacne, graph theory and so on.

A distinctive aspect of elementary theory of matroids is that they can be described in many equivalent ways.

BASIC CONCEPTS

GRAPH: A graph is pair of sets (V,E),where V is the set of vertices and E is the set of edges, formed by pair of vertices.

LOOP: A loop is an edge whose endpoints are equal.Multiple edges are the edges having the same pair of end points.

SIMPLE GRAPH:It is graph having no loops or multiple edges.

COMPLETE GRAPH: A simple graph G is said to be complete if its each pair of distinct vertices is joint by edges.A complete graph with n vertices is denoted by Kn

PATH: A path is a simple graph whose verices can be ordered so that two vertices are adjacent if and only if they are consecutive in the list.

CYCLE: A cycle is a graph with an equal number of vertices and edges whose vertices can be placed around a circle so that two vertices are adjacent if and only if they appear consecutively along the circle.

CONNECTED GRAPH: A graph is connected if each pair of vertices in G belongs to a path. Otherwise it is disconnected.

CIRCUIT: A graph is Eulerian if it has a closed trial containing all edges. A closed trial is a circuit when we do not specify the first vertex but keep the list in cyclic order.

INDEPENDENT SET:An independant set or stable set in a graph G is a set of pair wise non adjacent vertices.

CLIQUE: A clique in graph is a set of pair wise adjacent vertices.

MAXIMAL PATH: It is a path P in a graph G that is not contained in a longer path.

BIPARTITE GRAPH: A graph is bipartite if its vertex set can be partitioned into two non empty subsets X and Y such that each edge has one end in X and other end in Y.

TREE: A tree is a connected graph containing no cycles.

SPANNING TREE: A spanning tree is a spanning subgraph that is a tree.

FOREST: A forest is an acyclic graph.

SUBGRAPH : A subgraph of a graph G is a graph H such that V(H) $\subseteq$ V(G) and E(H) $\subseteq$ E(G) and the assignment of endpoints to edges in H is the same as in G.

ADJACENCY MATRIX: Let G be a loopless graph with vertex V(G) = {$V1$,.....Vn} and edge set E(G) = {e1,.....en}.
The adjacency matrix of G written A(G) is the n $\times$ n matrix in which a[i] , j is the numberif edges in G with endpoints {Vi , Vj}.

INCIDENCE MATRIX: The incidence matrix M(G) is the n$\times$m matrix in which entry mi,j is 1 if vi is an endpoint of ej and otherwise 0.
If vertex V ia an endpoint of edge e then V and e are incident. The degree of the vertex V is the number of incident edges.

WALK: It is a list V0 , e1 , V1 , ...ek , Vk of vertices and edges such that for 1 $\leq$ i $\leq$ k , the edge ei has endpoints Vi - 1 and Vi. A trial is a walk with no repeated edge.
A walk or trial is closed if its endpoints are the same.

SPAN: Given a vector space V over a field K the span of a set S of vectors is defined to be the intersection W of all subspace of V that contain S.W is referred to as the subspace spanned by S or by the vectors in S.Conversely S is called a spanning set of W and we say that S spans W.

BASIS : A set of elements in a vector space V is called a basis, or a set of vectors if the vectors are linearly independent and every vectors in the vector space is a linear combination of this set.

DIRECTED GRAPH : A directed graph or digraph D consist of a finite non empty set V of points together with a prescribed collection E of ordered pairs of distinct points. The elements of E are directed lines or arcs.

DEFINITIONS OF MATROIDS.

HEREDITARY SYSTEMS: A hereditary family or ideal is a collection of sets F such that every subset of a set in F is also in F.
A hereditary system M on E consists of a non empty ideal IM of subsets of E and the various ways of specifying that ideal called aspects of M.
The elements of IM are the independent setsof M.The other subsets of E are dependent. The bases are maximal independent sets and the circuits are the minimal dependent sets.
BM and CM denote these families of subsets.
The rank of a subset of E is the maximum size of an independent set in it.
The rank function rM is defined by r(X) = $\max\{|Y| : Y \subseteq X, Y \in I\}$

The diagram illustrates the relationships among the input sets,bases,circuits and independent sets of a hereditary system. The bases are the maximal elements of the family I and the circuits are the maximal elements not in I. In every hereditary system ϕ belongs to I.If every set is input then there is no circuits but there is always at least one base.

• Sets in the hereditary family are called independent sets of M
• The family of subsets of a set E other than those in Im is denoted by Dm and called the family of dependent sets of M.
• An independent set is maximal if it is not proper subset of another independent set.
A maximal independent set is called a bases. The family of all bases is denoted by Bm.
An independent set is always contained in a bases.
• A dependent set is minimal if no dependent set is its proper subset.
A minimal dependent set is called a circuit.
A dependent set always contains a circuit.
• A circuit consisting of only one element is called a loop.
Elements of a circuit with two elements are called parallel.
• The rank of a subset F of E is the largest size of an independent set contained in F..

Aspects of hereditary systems

A hereditary system M is determined by any of Im, Bm, Cm, rm..because each aspects specifies the others. We have expressed Bm, Cm, rm in terms of Im.
conversely if we know Bm, then Im consists of the sets contained in members of Bm.
If we know Cm, then Im consists of the sets containing no member of Cm.
If we know rm then Im = $\{X \subseteq E : r\ \mathrm{m(x)} = |x|\ \}$
Hereditary systems are too general to behave nicely. We restrict our attention to hereditary systems having an additional property and these we call matroids
We can translate any restriction on Im into a corresponding restriction on some other aspect of the hereditary system
Because hereditary systems can be specified in many ways.

Definitions of Matroid

Bases

A matroid M consists of a finite set E and a non empty collection B of subsets of E called bases satisfying the following property;
B1: No base properly contains another base.
B2 : If B1 , and B2 are bases and if {e} is any element of B1, then there is an element f of B2 such that (B1 - {e}) $\cup$ {f} is also a base.
This is known as exchange property.
This property states that if an element is removed from B1 then there exist an element in B2, such that a new base B3 is formed when that element is added to B1.
We can use the property B2 to show that every base in a matroid has the same number of elements.

Theorem : Every base of a matroid has the same number of elements.

Proof : First assume that two bases of matroid M, B1 and B2 contain different number of elements such that $|B\ 1\ | < |B\ 2\ |$
Now suppose there is some element {e} $\in$ M such that e $\in$ B1 but e $\notin$ B2.
If we remove {e} from B1 then by property B2 , we know there is some element f $\in$ B2 but f $\notin$ B1 such that B3 = B1 $\setminus$ ({e} $\cup$ {f}) where B3 is a base in M.
Therefore $|B\ 1\ | = |B\ 3\ |$, but $|B\ 2\ | \neq |B\ 1\ | = |B\ 3\ |$.
If we continue the process of exchanging elements defined by the property B2 k number of times , then there will be no element initially in B1 that is not in the base Bk.
Therefore for all e $\in$ Bk, the element e is also in B2 and thus B$k \subseteq$ B2.
From property B1 , we know that no base properly contains another base.
This is a contradiction.
Therefore we know that every base has the same number of elements.

An example in Linear Algebra

Let A = $\begin{bmatrix} 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$

In A these columns form a matroid.
Here we will take the base of a matroid to be a maximal linearly independent set that span the column space.

Let B1 = { 2 , 4 , 6 , 8}

B2 = { 2 , 5 , 7 , 8}

Now if we remove the second vector in B1, then we can replace it with the second vector in B2 to get a new base B3.

B3 = { 2 , 5 , 6 , 8}

For this case B2 is satisfied.
We would find the same results if we continued this process with all possible bases of A and we know that no bases of A properly contains another bases.

An example in graph theory

G :

Here we take a base of our matroid to be a spanning tree of G.

That is,
{ a, b, c, d }

{ a, e, d, c }

{b, c, d, e }

{ b, a, e, d }

{ c, g, f, e }

{ c, b, a, e }

{ c, b, f, e }

{ c, d, f, a }

{ c, g, a, e }

Here B1 is satisfied because no base properly contains another base.
Let a base B1 = { a, b, c, d } and
Bj ={ c, g, a, e } then the spanning trees are ;

Bi :

Bj :

We can prove B2 by removing an element { a } from B1 and then there exist an element in B2 such that a new base is created.

B3 = B 1 \ ({a} ∪ {e})

B3 :

Independent sets

A matroid is a pair M = (E, I) consisting of a finite set E and a non empty collection I of its subsets called independent sets satisfying the axioms :

• Any subset of an independent is independent.
• If X and Y are independent and $|Y| > |X|$,then there is an element e contained in Y but not in X such that X ∪ {e} is independent.

An example in Graph theory

We will take the independent sets of a graph to be the set of edges in a graph that do not contain a cycle. It can also be defined in terms of forest.

G :

The independent sets of a graph are the edge sets of the forests contained in the graph.

An example of a forest contained in G :

The first property can be shown because a set is independent if it is contained within a base .
Therefore independent sets must be contained with a spanning tree of a graph which means that rank of an independent set must be less than or equal to the rank of the graph.
The forest contained in graph G are ;
{a} , {b} , {c} ,{d} , {e}
{f} , {g} , {a,b} , {b,c}
{c,d} ,{d,e} , {e,f} , {f,g}
{g,a} , {a,f} , {e,f} , {d,f}
{b,f} , {b,g} , {c,g} , {d,g}
{a,b,c} , {a,b,g} , {a,e,d}
{a,f,d} , {a,g,c} , {a,g,d}
{b,c,d} , {b,g,d} , {b,f,d}
{b,f,e}, {c,d,e} , {c,g,d}
{c,d,f} , {e,f,e} , {a,f,g}
{a,b,c,d}, {a,c,d,e}, {b,c,d,e
{b,a,d,e}, {c,b,a,e}, {c,b,f,e}
{c,d,f,a}, {c,g,a,e}, {c,g,f,e}

From observing the table of forests, we can see that the forests are contained within the spanning trees which are the bases listed in the last three rows.
Now we will demonstrate why the exchange axiom for independent sets requires that two independent sets K and L must satisfy the inequality $|K| > |L|$
Let K and L0 be two forest from above.

K :

L0 :

$|K| = |L| = 3$
We find that there is an element e contained in K but not in L such that L $\cup$ {e} is independent.If we let L1 = L0 $\setminus$ {c} so that $|L\ 1\ | = 2 < |K| = 3$ then we necessarily have an element let it be {d} such that d $\in$ K but in L1. Therefore the independent set L1 $\cup$ {d} .

In linear algebra

We will take the independent sets of a matroid M of column vectors. I is independent in M if I is linear independent.

Circuits

A matroid is a pair M = (E,C) consisting of a finite set E and a non empty collection C of its subsets called circuits satisfying
• No proper subset of a circuit is a circuit.
• If C1 and c2 are distinct circuits and C $\in$ C1 $\cap$ C2 then
(C1 $\cup$ C2) - C contains a circuit.

Rank function

A matroid is a pair M = (E,r) consisting of a finite set E and a function r,rank assigning a number to a subset of E satisfying;
• The rank of an empty set is zero.
• For any subset X and any element y $\notin$ X,

$$r(\ X \cup \{y\}) = r(X) \text{ or } r(X) + 1$$

• For any subset X and two elements y,z not in X,
if r (X $\cup$ y) = r (X $\cup$ z) = r (X) then r (X $\cup$ { y,z }) = r(X)

Theorem :

If M is a hereditary system of the set E then,

1) r(ϕ) = 0

2) For any subset of E and any element e, r(F) $\leq$ R (F+e) $\leq$ r (F) + 1

Proof : Thee first case is trivial.
We need to prove the second case
Since F + e contains those independent sets that are contained F, we have r(F + e) $\geq$ r(F).
On the other hand possible independent subsets of F + e not contained in F may only consist of an independent subset of F and e so $\leq$ r(F) + 1.
$\Rightarrow$ r(F) $\leq$ r (F + e) $\leq$ r(F) + 1.

CHAPTER 2 :
TYPES OF MATROIDS

Trivial matroids

Given any non empty finite set E. We can define on it a matroid whose only independent set is the empty set ϕ. This matroids is known as he trivial matroid.
This matroid is the trivial matroid on E and has rank 0.

Discrete matroids

E is a finite set, every subset of E is independent. Discrete matroid on E has only 1 base E itself and that sank of any subset A is the number of elements in A

Linear matroid

Let F be a field, A $\in$ F AN m $\times$ n matrix over F, S = { 1,2,....n } be set of columns of A. Then I $\subseteq$ S is independent if he corresponding columns are linearly independent.

Cycle matroids

A matroid E can be associated with any graph G by letting E as the set of edges and taking as bases the edges as spanning forest of G.
This matroid is called the cycle matroid and denoted M(G).
The cycle matroid M(G) of a graph G is the hereditary system on E(G) whose circuits are the cycles of G.
Graphs may have loops and multiple edges. In cycle matroids they lead to circuits of sizes 1 and 2.

Graphic matroids

A hereditary system that is M(G) for some graph G is a graphic matroid.
Let G be a graph and let c be the set of cycles of G.
Then C is the set of circuits of a matroid on E and denoted by M(G).
A matroid obtained on this way is called graphic matroid.

Not every matroid is graphic, but all matroid on there elements are graphic. Every graphic matroid is regular.

Vectorial matroid

The vectorial matroid on a set E of vectors in a vector space is the system whose independent sets are the linearly independent subsets of vectors in E. An important example of a matroid define in this way is the Fano matroid.

Column matroid

The column matroid M(A) of a matrix A is the vectorial matroid defined on its columns.

Fano matroid

The Fano matroid is a rank three matroid derived from the fano plane, a finite geometry with seven points and seven lines.
It is a linear matroid whose elements may be described as the seven non zero points in three dimensional vector space over a finite field.

The Fano matroid F is the matroid defined on the set
E = { 1, 2, 3, 4, 5, 6, 7 } whose bases are all those subsets of E with three elemetns except,
{ 1, 2, 3 }, { 2, 3, 5 }, { 3, 4, 6 }, { 4, 5, 7 }, { 5, 6, 1 },
{ 6, 7, 2 },and { 7,1,3 }.

Here the bases are those set of three elements that do not lie on a line.
The cycles of Fano matroid are the lines such as { 1, 2, 4 } and the complements of the lines such as { 1, 2, 3, 6 }.

Bond matroid

The circuits of B(G) are the minimal edge cuts also known as bonds of G. These are minimal collections of the edges of G which when removed from G increase the connected components

Representable matroids

A matroid that is equivalent to a vector matroid although it may be presented differently is called representable or linear. If M is equivalent to a vector matroid over s field F, then we say M is representable if it is representable over the real numbers.
For instance a graphic matroids is presented in terms of a graph, it is also representable by vectors over any field.

Regular matroids

A matroid that is representable over all possible fields is called a regular matroid.
Every graphic matroid is regular.

Uniform matroids

Let E be a finite set and K be a natuaral number. One may define a matroid on E by taking every k element subset of E to a bases.
This is known as the uniform matroid of rank k.
A uniform matroid with rank k and with n elements is denoted by Uk, n.
A subset of the elements is independent if and only if it contains atmost k elements.
A subset is a bases if it has exactly k elements and it is a circuit if it has exactly r + 1 elements. A matroid of rank k is uniform if and only if all of its circuits exactly have r + 1 elements.
All uniform matroids of rank atleast two are simple. The uniform matorid of rank two on n points is called the n - point line.Direct sums of uniform matroids are called partition matroids.
Discrete matroids are the special cases of the k-uniform matroid on E whose bases are those subsets of E with exactly k elements.
The trivial matroid on E is 0-uniform and the discrete matorid is E-uniform.

Cographic matroid

We have already seen how to define a graphic or cycle matroid for any graph G.There is also another matroid, the cographic matroid of G, which is likewise defined on the edges of E. The circuits in the cographic matroid are the cut-sets of G, where a cut-set is a collection of edges C, such that when the edges in C are deleted from G, the number of connected components of G increases by one. So if G is connected then a cut-set is a group of edges which separate G into two connected haves.

Bicircular matroids

We can assign yet another matroid to a graph G, using a slight modification to the definition of graphic or cycle matroid. In the cycle matroid of G, the independent sets were the sets of acyclic edges, that is the forest.
In the bycircular matroid, the independent sets are the pseudoforests where a pseudoforest is a graph in which there is atmost one cycle in each connected component it is easy to see that the number of edges in a pseudoforest P is equal to the number of vertices in P minus the number of acyclic connected componets of P.

A maximal Pseudoforest P in a connected graph G will necessarily have a cycle in each component of P unless G is itself acyclic. Furthermore if the pseudoforest is truly maximal, its edges must cover all the verices in G. Therefor the size of a maximal pseudoforest is the number of vertices in G, or one less if G is acyclic. Then if G is not connected, the size of a maximal pseudoforest is the total number of vertices in G minus the number of acyclic connected components of G.Since this doesnt depend on the pseudoforest, we see that the maximal pseudoforest in any graph are all the same size.Therefore if S is a set of edges in a graph and we define a set of edges to be independent iff it is a pseudoforest, then the maximal independent subsets of S are all the same size . The resulting matroid is called a bicircular matroid. Unlika graphic matroids these are not necessarily representable over all fields, though they are always representable over Q.

CHAPTER 3
OPERATIONS MATROIDS

Duality

An important concept in matroid theory is the notion of duality. To each matroid M on a set E there is dual matroid defined on the same set E. The simplest definition is though bases Let M be a matroid, the dual matroid M^* to a matroid M is the matroid with bases that are complements of the bases M.

$B(M^*) = \{ E - B \setminus B \in B(M) \}$.
An element of B^* is called a cobase of M. tahe rank function of the dual M^* is given by
$r^*(X) = |x| + r(E - X) - r(M)$

We have already seen an example of a pair of dual matroids. If G is a graph then the graphic and cographic matroids of G are dual to each other we can also talk aoubt an abstract dual of a graph G which is another graph G^*, whose edges are identified with the edges of G such that the circuits of G are the cut-sets of G^* stated in terms of matroid theory, this tells us that if a matroid N is graphic and its dual M^* is also graphic then, M is the cycle matroid of a planar graph.
Such matroids are called planar matroids.

• In the uniform matroid of rank k on a set of size n, Uk, n, the bases are exactly the size k. There for the bases in the dual matroid are exactly the sets of size n - k, so the dual matroid is just $Un - k, n$.

• If a matoid M is representable over a field, then so its dual M^*.
The duals of representable matroids can be also understood geometrically through hyperplanes, as Whitney noted in his original paper.

Remark : The dual matroid of a discrete matroid is trivial.

Proof : The only base of a discrete matroid on E is E itself. So the only base of its dual is empty set. Thus the dual matroid is trivial matroid on E.

Restriction

Restriction of M to X, ($X \subset E$) is the matroid M^* with ground set X and independent sets I we denote it as $M \mid X$.

Deletion and submatroids

If M is a matroid on set E and E^0 is any subset of E then we can define a matroid on E^0 by taking a subset of E^0 to be independent iff it was independent in the original matroid.
In other words we simply restrict the notion of independence and dependence to the subsets of E^0. This is clearly still as matroid, as it satisfies the axioms for independence. This new matroid M^0 is a sub matroid of M called the restriction of M to E^0. We can define the sub matroid in terms of rank, bases, circuits. The rank function on the sub matroid will just be the restriction of the rank function from the original matorid. The circuits in the submatroid are just the original circuits that were contained in E. If M is a matroid and $x \in M$, then the submatroid on the set $E \mid \{x\}$ is called the matroid obtained by deleting x. We can also delete a subset S of E which is same as restricting to the complement S.

Contraction

The operation of deletion above has a dual notion of contraction. It is the dual operation of deletion.

$M \setminus T = (M^* \setminus T)^*$

APPLICATIONS

Matroids are structures that abstract certain fundamental properties of dependence common to graphs and vector spaces. The theory of matroids has its origin in graph theory and linear algebra and its most successful applications in the past have been in the areas of combinatorial optimization and network theory.
Recently however there has been a flurry of new applications of this theory in the fields of information and coding theory.It is only natural to expect matroid theory to have an influence on theory of error correcting codes, as matrices over finite fields are objects of fundamental importance in both these areas of mathematics.
Indeed as far as back as 1976 , Greene re-derived the MacWilliams identities which relate the Hamming weight enumerators of a linear code and its dual as special cases of an identity for the Tutte polynomial of a matroid.However aside from such use of tools from matroid theory to re-derive results in coding theory that had already been proved by other means, each field has had surprisingly little impact on the other , until very recently.Coding theory, information theory , secret sharing, network coding, and information i inequalities have seen a recentinflux of ideas from matroid theory and combinatorial optimization.

coding theory

The serious study of channel or coding theory started with Shannon's monumental 1948 paper[9].Shannon stated the result that reliable communication is possible at rates up to channel capacity , meaning that for any desired symbol or block error probability there exist a channel code and a decoding algorithm that can achieve this symbol or block error probability as long as the rate of the channel code is smaller than the channel capacity. On the other hand Shannon showed that if the rate is larger than the capacity and the symbol and the block error probability must be bounded away from zero. Unfortunately the proof of the above achievability result is non constructive meaning that if shows only the existence of such channel codes ans decoding algorithms. Therefore since the appearance of Shannon's theorem the quest has been on to find codes with practical encoding and decoding algorithms that fulfill Shannon promise.

The codes and decoding schemes that people have come up can broadly be classified into two classes: traditional schemes and modern schemes. In the traditional schemes codes were proposed that have some desirable properties like large minimum Hamming distance. However given a code it was usually unclear how to decode it efficiently. Often it took quite some time until such a decoding algorithm was found if at all.
In modern schemes the situation is reversed. Given and iterative decoding algorithm like the sum-product algorithm, the question is what codes work well together with such an iterative decoding algorithm. Actually codes and decoding algorithm in the spirit of modern schemes were already described in the early 1960s by Gallager.
He proposed to define codes in terms of graphs. Such graphs are now known as Tanner graphs: they are bipartite graphs where one class of vertices corresponds to codeword symbols and where the other class of vertices corresponds to parity-checks that are imposed on the adjacent codeword symbols.
Decoding is then based on repeatedly sending messages with estimates about the value of the codeword symbols along edges and to locally process these messages at vertices in order to produce new messages that are again sent along the e of the shares in every secret sharing scheme realizing edges.

Secret sharing

The second major application of matroid theoretic ideas that we mention here is with respect to secret sharing schemes. A secret-sharing scheme is a method to distribute shares of a secret value among a certain number of participants such that qualified subsets of participants can recover the secret from there joint shares.
Secret sharing schemes were originally motivated by the problem of secure storage of cryptographic keys. In a secret sharing scheme the collection of qualified subsets of participants is called the access structure of the scheme. It is known that for any monotone increasing collection Γ , of a finite set, one can define a secret sharing scheme with access structure Γ.
Γ is said to be an ideal access structure if it admits an ideal secret-sharing scheme..

Brickell and Davenport began a line of working relating ideal secret sharing schemes to matroids. They showed that any ideal access structure is

induced by a matorid in a very specific sense. However it is also known that not every matroid gives rise to an ideal access structure, for example, the access structures induced by the vamos matroid are not ideal. Characterizing the matroids that give rise ideal access structures has remained an open problem.
In a talk based on joint works presented the use of non Shannon information inequality of lower bounds on the size of an access structure induced by the vamos matroid. This is the first result showing the existence of an access structure induced by a matroid which is not nearly ideal.

Network coding

Another novel application of matroid theory and combinatorial obtimisation within the realm of information theory is in the area of network coding.

CONCLUSION

Matroids seem to be fairly interesting mathematical objects, if only for the sake of novelty. They unite concepts from linear algebra, projective, geometry, graph theory, combinatorial optimization. The most distinctive feature of matroids seems to be the diversity of definitions of one concept. Moreover matroids provide a frame work for generalizing results from graph theory and linear algebra. For example a theorem about a graph can be defined in terms of cycles, bases, spanning trees then the statement can be translated into the frame work of matroids and we can ask weather the new statement holds for all matroids, or for some interesting class of matroids. One example of a problem which was sold by generalizing from graphd to matroids was the Shannon Edge Switching game. In this game to players called Short and Cut alternatively choose ans edge in a graph, either contracting it or deleting it respectively. There is also a special edge linking the source and sink, which neither player can choose. In the end, short wins by connecting the source and sink and cut wins by preventing this. This haves an obvious generalization of duals in terms of closure, that cut wins exactly by co-spanning the designated edge.So matroid theory reveals the symmetry between the two players the roles of the two players are exactly dual. Moreover matroid theory was used by Alfred Lehman to solve the game in full generality. Only later the solution translated back into a graph theoretic construct, for the case of the edge switching game.

REFERENCES

• Introduction to Graph Theory, ROBIN J WILSON

• K. V. Adaricheva , V. A. Gorbunov and V. I Tumanou, Join-semi distributive lattices and convex geometries, Advances in mathematics 173 (2003), 1-49.

• Eugene Lawler, combinatorial optimization; networks and matroids, Holt, Rhinehart and winston, Newyork, 1976