Hassler Whitney

Gian-Carlo Rota

Polymatroids, Part 1, Wednesday, Feb. 10 at 10:00

A **set system**, (E,F), on finite ground set E
with a non-empty family F of subsets of E,
is called an independence system if every subset of a member of F (called an independent set) is a member of F.

Where E is the edge-set of a graph G, and the independent sets are the matchings in G, the independence system (E,F) is not a matroid.
Where the independent sets are the edge-sets of forests in G, the system (E,F) is a matroid.
More generally where E is the set of columns of a matrix over a field, and the independent sets are the linearly independent sets, (E,F) is a matroid.
We will see sources of many other matroids.

Here are two convenient definitions of matroid:
(3.1) An independence system, M = (E,F), such that
any independent set together with another element contains
at most one minimal dependent subset (called a circuit).
Or
(3.2) An independence system, M = (E,F), such that
for any subset S of E, every maximal (not meaning largest)
independent subset of S (called a **basis** of S) is the same size,
called the rank r(S) of S in M..

Definition (3.2) is a well-known theorem
for the linearly independent subsets of a set of vectors.
Definition (3.1) is obvious for a set of vectors when it is stated in
the obviously equivalent form: (3.1') For two circuits, C1 and C2,
of M, and any e ε C1 ∩ C2, the set {(C1 ∩ C2) – e} is dependent.

Hence proving that (3.1) and (3.2) are equivalent
is a fun way to derive a bit of linear algebra.

A non-empty set F of non-negative integer-valued d-tuples (with coordinates indexed by E) is called an (integer) **lower ideal** when ($a \leq b$ ε F) => (a ε F). (There is probably a better term for it but that's the one that comes to mind.)

(3.3) An **polymatroid** is a lower ideal F such that,
for any non-negative integer d-tuple, s, every maximal x,
such that $x \leq s$ and x ε F, has the same sum (of entries),
called the rank r(s) of s in the ideal F.

Notice, where the members of F consist of 0's and 1's,
a polymatroid is the same thing as a matroid.
It turns out that any polymatroid, is exactly the same as the set of integer solutions of a special kind of system of linear inequalities.

A real valued function, f, of subsets of a set E
is called **submodular** when $f(A \cup B) + f(A \cap B) \leq f(A) + f(B)$.
It's **supermodular** when the inequalities are reversed,
and **modular** when the inequalities are equations.
Any modular set function takes the form $x(S) \equiv \sum(x(j): j \in S)$.

A **polymatroid set-function** is a submodular function which is integer-valued, non-decreasing, non-negative, and 0 for the empty set. Any integer submodular function can be represented as a polymatroid function plus a modular function.

(3.4) Theorem. For any polymatroid set function, f,
the integer points of polytope
$P(f) = \{x \geq 0\text{: for every subset } S \text{ of } E,\ x(S) \leq f(S)\}$
is a polymatroid, F, whose rank function is,
for every $a \geq 0$, $r(a) = \min\,\{f(S) + a(E - S)\text{: } S \text{ is a subset of } E\}$

Conversely,
(3.5) Theorem. For any polymatroid F on E,
let $f(S) \equiv \max\{x(S): x \in F\}$.
Then f is a polymatroid function such that $P(f) = F$.

It follows immediately from the definition of polymatroid that for any polymatroid, P, the integer points $x \in P$ such that $x \leq \mathbf{1}$ are the 0,1 incidence vectors of a matroid.
Hence Theorem (3.3) has as a corollary
the following way of getting matroids,
which is dramatically different from linear dependence.

(3.6) Theorem. For any polymatroid function f on subsets of E,
let F consist of the subsets J of E such that,
for every subset S of E, $|J \cap S| \leq f(S)$.
Then (E,F) is a matroid with rank function,
$r(A) = \min\{f(S) + |A - S| : S \text{ is a subset of } A\}$.

(3.7) For example, let $\{(E, F(i)) : i \in K\}$
be any multi-set of matroids, each on ground set E.
They could be matroids of linear independence over various fields.

Since the rank function of any matroid is a polymatroid function,
$f(S) = \sum(r(S, i): i \in K)$ is a polymatroid function,
and so by (3.6) gives a new matroid, (E,F),
not necessarily a matroid of linear independence over any field.

Assuming that we have oracles which recognize whether or not
a set is independent in each of the matroids (E,F(i)),
Theorem (3.6) gives us a good way to recognize
when a set J is not in F. We need only to see
that one of the inequalities of (3.6) is not satisfied.
But what is good way to recognize when a set J **is** independent?

The answer is given by the following Matroid Partition Theorem.
(3.7) A set J satisfies the all the inequalities of (3.6),
where f(S) is as in (3.7), if and only if
J can be partitioned into sets, J(i), $i \in K$, such that $J(i) \in F(i)$.

This is a way of saying:
(3.8) Theorem. The Minkowski sum of a multi-set of polymatroids,
P(i), each coordinatized by E is an polymatroid.

The **Minkowski sum** of any sets F(i), $i \in K$,
of d-tuples coordinatized by E,
means the set $F = \{x = \sum x(i) : x(i) \in F(i), i \in K\}$.

We have a polytime algorithm for deciding whether or not a set J can be partition into sets J(i) which are independent respectively in matroids (E,F(i)).

More generally we have a polytime algorithm for the so-called
“sum-set inverse problem”,
popular among additive number theorists, for expressing,
if possible, a given integer-valued d-tuple x
as the sum of d-tuples, x(i),
contained respectively in the sets, P(i), of d-tuples.
I expect (3.8) to have applications in additive number theory.
Of course, it **is** additive number theory.