Generic Matroids

Athan Clark

July 26, 2015

Abstract

Matroids are a great tool for optimization - say we have a set of elements, and some function to measure each element. If we want to maximize the *total* measure of a subset of the input, we can do so quickly with matroids. The principal is simple - if we first have all paths to potential solutions at hand (the matroid itself), and a function to take elements of our set and give us some unit that we can compare each other against (for instance, the *Ord* type class in Haskell), then we can find the subset with a maximum total very quickly.

Here we assert the properties and definition of matroids, to better formalize and demonstrate their utility.

1 Overview

A Matroid can be seen as the "road map" to every possible solution. The potential solutions are based on an input set, and the set of all potential solutions are the roads. Formally, a matroid consists of a **ground** set E (the input), and a "family" I of **independent** subsets of E (the roads):

$$E : Set\ \ \delta,\ \ I : Set\ \ (Set\ \ \delta)\ \text{ where }\ I \subseteq \rho E$$

for some element type δ. I is a subset of the power set of E; I is a set of subsets of E.

2 Properties

For I to be seen as the routes we can take to a solution, we need some closure properties. An independence system supports the potential routes from an empty set to a solution, and the augmentation property lets us grow from a smaller solution to a larger one:

$$\forall i \in I.\ i \subseteq E \tag{MATROID-SUBSET}$$

$$\forall i \in I.\ \rho i \subseteq I \tag{MATROID-HEREDITARY}$$

$$\begin{aligned} &\forall i, j \text{ where } |i| < |j| \in I. \\ &\quad \exists e \in i - j.\ i \cup \{e\} \in I \end{aligned} \tag{MATROID-GROWTH}$$

MATROID-SUBSET and MATROID-HEREDITARY satisfy what is known as an "Independence System", a "Hereditary Subset System", or "Abstract Simplical Complex". This gives us the knowledge that for every subset $i \subseteq E$ in I, any *smaller variant* of i is also in I. MATROID-GROWTH is the "Augmentation Property" for matroids, letting us grow from a smaller element to a larger element, by implementing atomic inclusion of additional elements via union.

With these properties, not only can we leverage matroids as a means to check if a subset of E is a potential solution (in I), but we can also easily *add to* our solution, and see if that is also satisfactory. The *greedily* function relies on this, inductively proving that it strongly normalizes to a maximum "weight". That is, when using a *weigh* function as a metric for each element of type δ in E, *greedily* can find the subset of E that maximizes the total of this weight metric.

This is the nature of I - it is exhaustive in every opportinity that a subset of E can have to become a larger solution - all subsets of a potential solution will be a potential solution, and through augmentation we can approach a larger solution from a smaller one.

3 Weights

Matroids let us find optimal subsets of a particular set, with respect to a particular *metric*. We need some form of *weigh* function, which gives a measure for each element in E:

$$weigh \ : \ \delta \to \psi$$

For our purposes, we will also need some way to get a "total" value of any number of ψ values - in *any order*, too. This means that we need a binary $\otimes$ function, which satisfies an *abelian semigroup* over ψ:

$$\otimes : \psi \to \psi \to \psi$$

$$\forall a, b \in \psi.\ a \otimes b \equiv b \otimes a \tag{PSI-COMM}$$

$$\forall a, b, c \in \psi.\ (a \otimes b) \otimes c \equiv a \otimes (b \otimes c) \tag{PSI-ASSOC}$$

In the circumstance that we want to find the subset of E that *maximizes* the *total*[1], then ψ obviously needs to form a partial order. If we are to greedily

[1] Where *total* is akin to *concat* from Haskell, in any order.

find our maximum subset, then $\otimes$ should also be strictly increasing value when combining terms:

$$\begin{aligned}
\forall p \in \psi.\ & p \leq p && \text{(PSI-REFL)} \\
\forall p, q \in \psi.\ & p \leq q \wedge q \leq p \Rightarrow p \equiv q && \text{(PSI-ANTI)} \\
\forall p, q, r \in \psi.\ & p \leq q \wedge q \leq r \Rightarrow p \leq r && \text{(PSI-TRANS)} \\
\forall p, q \in \psi.\ & p \leq p \otimes q && \text{(PSI-INC)}
\end{aligned}$$

Where PSI-REFL, PSI-ANTI and PSI-TRANS form the partial order, and PSI-INC shows that the total of any number terms should be larger than or equal to the total of any subset of those terms.

ψ then serves as an auxiliary type, with enough behaviour to ensure that $greedilyMax$ will find our maximum subset.

4 Optimization

$greedilyMax$ works by making successive "*pivots*", moving the maximum element from the ground set to the temporary result (only if the new result is in I). Put simply, $pivotMax$ mutates the temporary result directly, and is stateful in the ground set:

$$\begin{aligned}
pivotMax\ &:\ (\ MonadState\ (Set\ \delta)\ m \\
&\quad\ ,\ MonadReader\ (Set\ (Set\ \delta))\ m \\
&\quad\ ) \Rightarrow Set\ \delta \rightarrow m\ (Set\ \delta) \\
pivotMax\ x\ &=\ \text{do}\ \ e \leftarrow takeMaximumWith\ weigh \\
&\qquad\quad\ \ i \leftarrow ask \\
&\qquad\quad\ \ \text{if}\ \ x \cup e \in i\ \ \text{then}\ \ \text{return}\ \ x \cup e \\
&\qquad\qquad\qquad\qquad\quad \text{else}\ \ \text{return}\ \ x
\end{aligned}$$

$greedilyMax$ is then the partial fixpoint of $pivotMax$ - until there is nothing left in the copy of E:

$$\begin{aligned}
&greedilyMax\ \ :\ \ (Set\ \delta,\ \ Set\ \ (Set\ \delta)) \rightarrow Set\ \delta \\
&greedilyMax\ \ (e,\ \ i)\ \ :=\ \ runReader\ \ (runStateT\ \ go\ \ e)\ \ i \\
&\quad \text{where}\ \ go\ \ :=\ \ almostFixM\ \ (null\ \ {=}{<}{<}\ \ get)\ \ pivotMax\ \ \emptyset
\end{aligned}$$

In this way, $greedilyMax$ finds the maximum subset.

Theorem 1 (Maximum Total)**.** *$greedilyMax$ finds the subset $X \in I, X \subseteq E$ such that $\sum(fmap\ \ weigh\ \ X)$ is maximal compared to all other elements in $I \subseteq \rho E$.*

Proof. We first prove that *go* approaches the unique, maximum-sized subset $E_\Omega \subseteq E\ E_\Omega \in I$. We also prove that for any n, the *total* of any set sized $n+1$ will be larger than or equal to n. From these, we can prove that $total\ \ E_\Omega$ will be maximal compared to all $i \in I$.

By MATROID-SUBSET and MATROID-HEREDITARY, we can see that *for any* $i \in I$, we can reach i from the empty set, as $\rho i \subseteq I$. Also, through MATROID-GROWTH we can reach *any larger* $j \in I$. From this, it is clear to see that we can reach *the larget set* in I from the empty set, especially from the fact that $\forall i \in I.\ \rho i. \in I$.

The second proof follows directly from PSI-INC - if we have any additional term, then the product will be greater than or equal to the original. This follows directly to n-sized concatenation:

$$\begin{gathered}\forall xs \subseteq ys : Set\ \ \phi \text{ where } |xs| \leq |ys|.\\ total\ \ xs\ \ \leq total\ \ ys\end{gathered}$$

Thus, $total\ \ E_\Omega$ is maximal. ■

Theorem 2 (Eager Maximum)**.** *$X_{n+1} \leftarrow pivotMax\ \ X_n$ eagerly finds the most maximal subset $X_n \in I, X_n \subseteq E$ such that for any other $i \in I$ where $|i| = n$, then total $X_n \geq$ total i.*

Proof. By structural induction. We rely that the initial state for the $MonadState$ component of $pivotMax$ is E, and also that the initial value supplied as the third argument to $almostFixM$ is the empty set. From this, we can start our induction.

$takeMaximumWith$ in $pivotMax$ removes and returns the element of it's input set with a maximum value from the function provided. From this, we can see that for the first case, $n := 1$, that the result is the singleton set $\{e_\Omega\}$, and the new state $E - \{e_\Omega\}$. At this stage, it is easy to show

$$\forall e' \in E - \{e_\Omega\}.\ \ weigh\ \ e' \leq weigh\ \ e_\Omega$$

as that is the definition for the maximum. To be more precise, we must show

$$\begin{gathered}\forall E' \subseteq E \text{ where } |E'| = 1.\\ totalMap\ \ weigh\ \ E' \leq totalMap\ \ weigh\ \ \{e_\Omega\}\end{gathered} \tag{1}$$

For the successor case, we also need to show that the solution S_n is maximal compared to all other subsets of size n, for any n. Lastly, by showing that $S_n \subseteq S_{n+1}$, we have proven that the result at n is maximal compared to all other subsets of that size. Formally, we need to show that

$$\begin{gathered}\forall n : Nat,\ \ E' \subseteq E \text{ where } \ |E'| = n.\\ totalMap\ \ weigh\ \ E' \leq totalMap\ \ weigh\ \ S_n\end{gathered} \tag{2}$$

$$\forall n : Nat.\ S_n\ \subseteq\ S_{n+1} \tag{3}$$

are both true.

Like said before, (1) is easy to show - as there are no other elements in the set initially (we start with the empty set $\emptyset$), and we begin with E, we *remove* the largest element e_Ω from E, and add it to our accumulator. From this initial state, it is easy to show that e_Ω is larger than any other individual element in $E - \{e_\Omega\}$, and transitively that the set total value of $\{e_\Omega\}$ is larger than any other subset with the size 1 (any other singleton set).

The more general case, where the total of S_n is maximal compared to every other subset of E with size n, relies on the fact that S_{n-1} was also maximal compared to every other subset of size $n-1$, inductively back down to the base case - in that this proof uses structural induction. Assuming we know that S_{n-1} was maximal, it is easy to show that we *maintain* this maximal state, as for each pivot, we remove the *maximum*, top element in the state, thus retaining maximality when using $\otimes$.

More formally, if S_n is the solution set at pivot n, and $E_{\gamma,n}$ is the *state* of the temporary copy of E at pivot n, then

$$\begin{aligned} \forall n : Nat.\ & S_n \subseteq S_{n+1} \\ \forall n : Nat.\ & E_{\gamma,n} \supseteq E_{\gamma,n+1} \\ E_{\gamma,0} := E, \qquad & S_0 := \emptyset \end{aligned}$$

Should all be obvious. We omit the rest of the proof for brevity. ■

For an asymptotically faster version of *greedilyMax*, we turn our condition and statefulness into a fold:

$$\begin{aligned} greedilyMax'\ (e,\ i)\ &:=\ foldr\ go\ \emptyset\ (sortBy\ weigh\ e) \\ \text{where}\quad go\ x\ acc\ &:=\ \text{if}\ acc \cup \{x\} \in I\ \text{then}\ acc \cup \{x\} \\ &\qquad\qquad\qquad\qquad\qquad \text{else}\ acc \end{aligned}$$

5 Bases and Circuits

If we do some analysis on a matroid, we can see clear semantics regarding independent and dependent sets, in the context of ordering and inclusion.

Say I have some solution $\lceil S \rceil \subseteq E \in I$. Then this solution is a *basis* if and only if it is the largest subset in I:

$$\forall i \in I.\ i \subseteq \lceil S \rceil$$

Likewise, we could also say that any additional element added to $\lceil S \rceil$ is now not independent:

$$\forall e \in E - \lceil S \rceil.\ \lceil S \rceil \cup \{e\} \notin I$$

We carry this logic orthogonally to *circuits*. A circuit $\lfloor \hat{S} \rfloor \subseteq E$ is the minimal dependent set in our matroid - such that every other dependent set is a superset of a circut, and that any smaller subset is independent:

$$\forall i' \subseteq E \notin I.\ \ \lfloor \hat{S} \rfloor \subseteq i'$$
$$\forall s \in \lfloor \hat{S} \rfloor.\ \ \lfloor \hat{S} \rfloor - \{s\} \in I$$

We use the hat symbol (ˆ) to disambiguate a dependent set from an independent one, and use the floor and ceiling operators intuitively as "maximum" and "minimum".

Circuts and bases, in their own right, are enough to define matroids. A subset $i \subseteq E$ is independent if and only if it is a subset of $\lceil S \rceil$, and not a superset of $\lfloor \hat{S} \rfloor$:

$$i \in I \iff i \subseteq \lceil S \rceil \ \wedge\ i \not\supseteq \lfloor \hat{S} \rfloor$$

Likewise, the same proposition can be made for dependent sets:

$$i \notin I \iff i \not\subseteq \lceil S \rceil \ \wedge\ i \supseteq \lfloor \hat{S} \rfloor$$

Where we evade the hereditary property, while leveraging the definition of the circuit. Thus $\lceil S \rceil$ and $\lfloor \hat{S} \rfloor$ form a matroid over E.

6 Ranks

Now that we have an intuition for how maximal independent sets, and minimal dependent sets form a matroid, we can direct our focus toward *ranks* - a measure of matroids.

The rank of a matroid is the size of its basis - such that the rank function $r : E \to \mathbb{N}$ is defined as follows:

$$r(E) := \lceil S \rceil \subseteq E.\ \ |\lceil S \rceil|$$

Where $|\lceil S \rceil|$ is the size of the basis in E. From there, it is easy to show that

$$r(E) \ \leq\ |E|$$

because $\lceil S \rceil \subseteq E$. Also, because elements *added* to a set may not be independent, we can make a transitivity rule as well:

$$\forall A \subseteq E,\ \ e \in E.\ \ \ r(A) \ \leq\ r(A \cup \{e\}) \ \leq\ r(A) + 1$$

which follows to

$$\forall A, B, C \ \text{ where }\ A \subset B \subset C.\ \ \ r(A) \ \leq\ r(B) \ \leq\ r(C)$$

such that r is monotonic. Lastly, r is submodular:

$$\forall A, B \subseteq E. \quad r(A \cup B) + r(A \cap B) \quad \leq \quad r(A) + r(B)$$

Which makes sense in terms of our bases - the basis of $A \cup B$ *could* be only as large as A or B.

From these, we can see that if $r(A) = |A|$, the A is its own basis. Further, if I have a subset $A' \subseteq A$ that also is its own basis, then that implies their bases are subsets:

$$A' \subseteq A \ \ \wedge \ \ r(A) = |A| \ \ \wedge \ \ r(A') = |A'| \ \ \Rightarrow \ \ \lceil S \rceil_{A'} \subseteq \lceil S \rceil_A$$

Which is orthogonal to MATROID-HEREDITARY, and if $\lceil S \rceil_A$ is the largest basis in E, then we also satisfy MATROID-GROWTH. Thus, r forms a matroid over E, where elements in I are formed by self-basis:

$$\forall i \in I. \ r(i) = |i|$$

From this persepctive, we can also intuit *submatroids*, where (E', r) is a submatroid of (E, r) iff. $E' \subseteq E$.