ФІЗИКО-МАТЕМАТИЧНІ НАУКИ

Avdieiev O.D.
Student,
Kharkiv National University of Radio Electronics

GREEDY ALGORITHM

Algorithms designed to solve optimization problems are usually a sequence of steps, each of which is given a set of choices. Determining the best choice, guided by the principles of dynamic programming, in many optimization tasks resembles shooting from a cannon on sparrows; in other words, more simple and effective algorithms are better suited for these tasks.

This article outlines an elegant theory of greedy algorithms. It is useful when you need to determine when a greedy method provides the optimal solution. This theory contains combinatorial structures known as «matroids».

A matroid is an ordered pair M = (S, I) satisfying the conditions stated below:

1. The set S is finite.

2. I is a non-empty family of subsets of the set S (which are called independent subsets) such that if $B \in I$ and $A \subseteq B$, then $A \in I$. If the family I satisfies this property, it is called hereditary. Note that the empty set $\emptyset$ necessarily belongs to the family I.

3. If $A \in I$, $B \in I$ and $| A | <| B |$, then there exists an element $x \in A - B$ such that $A \cup \{x\} \in I$. It is said that the structure M satisfies the exchange property.

A matroid is an arbitrary pair $M = [E, \mathfrak{I}]$, where E is a finite set and $\mathfrak{I}$ is a nonempty family of subsets of the set E satisfying the conditions: (M1) from ($A \in \mathfrak{I}$, $B \subset A$) that $B \in \mathfrak{I}$; (M2) $\forall$ A, $B \in \mathfrak{I}$, such that $| A | <| B |$, there is always $e \in B \setminus A$: $A \cup \{e\} \in \mathfrak{I}$. The sets of the family $\mathfrak{I}$ are called independent sets, and all other subsets of E are dependent sets of the matroid M. It follows from (M1) and the nonemptiness, that $\emptyset \in \mathfrak{I}$ in any matroid.

The base of the matroid is any maximal independent inclusion in the inclusion. A cycle of a matroid is any minimal dependent set.

A dependent set is a subset of the matroid carrier that is not independent. We represent the matroid over the field F if it is isomorphic to some vector matroid over this field. If we represent a matroid over any field, it is called regular. A matroid that is representable over a two-element field GF (2) = {0,1} (a field is a set of elements on which two operations are defined: addition and multiplication, even if these operations are not ordinary operations of addition and multiplication, and also subtraction and division by any non-zero element) is called a binary matroid. A matroid that is representable over a field GF (3) = {0,1,2} of three elements is called a ternary matroid.

A dual matroid is a matroid whose carrier coincides with the carrier of the given matroid, and bases are the complements of the bases of the given matroid to the carrier, that is, X * = X, and the set of bases of the dual matroid is the set of B * such that B * = X \ B, where B is the base of the given matroid. Suppose that the matrix G of the ideal scheme for dividing the secret with the matroid M is determined by the dual matroid M * through the list of its cycles as a list of its dependent sets. Therefore, if we represent the matroid M over a finite field F, then M * defines the generating matrix G of the code linear with respect to the field F with the verification matrix H given by cycles of the matroid M, this code is the code of this CPC.

The rank of a matroid is the power of its bases. The rank of the trivial matroid is zero.

Matroids are widely used in problems related to combinatorial optimization, as well as problems whose solution is based on greedy algorithms. Greedy method has enough power and is well suited for a fairly wide class of tasks.

Many problems for which a greedy approach allows us to obtain an optimal solution can be formulated in terms of searching for an independent subset with the maximum weight in a weighted matroid.

The weighted matroid is a matroid, on elements of the set E a positive weight function w is given.

So, we have a weighted matroid M = (S, I) and we need to find an independent set A ∈ I for which w (A) is maximal. We call such a maximal independent subset with the maximum possible weight an optimal subset of the matroid. Since the weight w (x) of each element x∈S is positive, the optimal subset is always a maximal independent subset, which always helps to make the set A as large as possible.

For example, in the minimal-spanningtree problem, a connected undirected graph G = (V, E) and a function of length w are defined such that w (e) is a (positive) edge length e. (The term «length» is used here to refer to the initial weight corresponding to the edge of the graph, the term «weight» is reserved for the weights in the corresponding matroid.) It is necessary to find a subset of edges that connect all the vertices and have a minimum total length. To represent this problem in the form of the problem of finding the optimal subset of the matroid, consider the weighted matroid MG with the weight function w, where w (e) = w0 – w (e), and w0 exceeds the maximum edge length.

In such a weighted matroid, any weight is positive, and the optimal subset is a spanning tree, each maximal independent subset of A corresponds to a spanning tree, and since for every maximal independent subset A the following relation holds: w (A) = (| V | – 1) w0 – w (A), then the independent subset that maximizes w (A) must minimize w (A). Thus, any algorithm that allows us to find the optimal subset A of an arbitrary matroid also allows us to solve the minimal spanning tree problem.

A greedy algorithm is an algorithm that consists in making locally optimal decisions at each stage, assuming that the final solution will also be optimal. It is known that if the structure of the problem is set by the matroid, then the application of the greedy algorithm will produce a global optimum, which will have success.

References:

1. Жадные алгоритмы [Электронный ресурс]. – Режим доступа: http://www.williamspublishing.com/PDF/5-8459-0857-4/part.pdf
2. Сорокина С. В., Титов С. С. Матроиды, двойственные к бинарным, и их схемы разделения секрета // Безопасность в информационной сфере. – 2014. – № 4. – С. 36-39.
3. Асанов М. О. и др. Дискретная математика: графы, матроиды, алгоритмы. – Ижевск: ННЦ «Регулярная и хаотическая динамика», 2001. – С. 56-72.

Шинкарюк А.Т.
студент,
Коледж Чернівецького національного університету
імені Юрія Федьковича

ЙМОВІРНІСТЬ ОДНА – ПІДХОДИ РІЗНІ

В зв’язку з тим, що на сьогодні немає такої галузі знань, де б не використовувалися досягнення математики. Фізики, хіміки, астрономи, біологи, економісти, навіть мовознавці та історики використовують математичний апарат. Часто доводиться мати справу з явищами реального світу, які залежать від невідомих обставин, що не піддаються обліку. Формулювання задач з різних галузей знань містять не математичні поняття і якщо математик розв’язує таку задачу, то він прагне перекласти її на математичну мову, тобто мову виразів, формул, рівнянь тощо.

Одним з таких понять, який викликав різні суперечки серед вчених починаючи з XVII століття стало поняття ймовірності, що призвело до виникнення теорії ймовірності, як цілого розділу математичної науки. Становлення і розвиток теорії ймовірностей висвітлено в працях П’єра Лапласа (1749–1827), Ріхарда Мізеса (1893-1953), Д. Кардано (1501–1576), Б.Паскаля (1623–1662), особливого значення набули праці математика А.М. Колмогорова (1903–1987).

Українська математична наука подарувала світові імена видатних фахівців у галузі теорії ймовірностей. Імена Б.В. Гніденка, А.В. Скорохода, М.Й. Ядренка, М.І. Жалдака відомі математикам усього світу.

Вислів Б.В. Гніденка «Теорія ймовірності подібно до інших розділів математики, розвинулася з потреб практики; в абстрактні формі вона відображає закономірності властиві подіям масового характеру» [1, с. 13].

В зв’язку з бурхливим розвитком природничих наук апарат теорії ймовірностей перетворився в чітку математичну дисципліну з власними проблемами та методами доведень. Суперечки між математиками виникали при подачі означення математичної ймовірності. Число різних означень математичної ймовірності, що пропонувалося різними авторами дуже різноманітне і багате. Але інтерес до логічно обгрунтованого означення теорії ймовірностей виник значно пізніше, ніж вміння проводити обчислення в парктичній діяльності і в наукових дослідженнях.