УДК 004.056:519.854

Использование радиуса устойчивости оптимизационных задач для скрытия и проверки корректности информации

© Э.Н. Гордеев

МГТУ им. Н.Э. Баумана, Москва, 105005, Россия

Рассматриваются возможности применения теории устойчивости оптимизационных задач для скрытия информации и проверки корректности получаемой информации при передаче ее по открытым каналам. Для этого используется связь между исследованием устойчивости решений дискретных экстремальных задач и методами решения обратных задач. (В обратной задаче требуется построить условие задачи на основе заданного решения или множества решений.) Приводится общее описание двух методов, а также дается краткое описание некоторых результатов теории устойчивости, на основе которых описанные методы могут быть реализованы. Первый подход базируется непосредственно на связи методов решения обратных задач и результатов теории устойчивости. Второй подход посвящен возможностям восстановления искаженной информации на основе знания радиуса устойчивости некоторой дискретной экстремальной задачи.

Ключевые слова: *дискретная оптимизация, радиус устойчивости, обратная задача, восстановление информации.*

Введение. В работах [1–7] рассматривались различные подходы к исследованию устойчивости в задачах дискретной оптимизации. Суть их состоит в следующем.

Рассматривается класс задач дискретной оптимизации, который описывается следующей моделью. Пусть $E = (e_1, ..., e_n)$ – некоторое множество, $D_n = \{\tau_1, ..., \tau_m\}$ $m > 1$, – система подмножеств множества E, называемых траекториями. Характеристический вектор траектории τ будем обозначать через $H(\tau) = (h_1(\tau), ..., h_n(\tau))$, т. е.

$$h_i(\tau) = \begin{cases} 1, & e_i \in \tau; \\ 0, & e_i \notin \tau. \end{cases}$$

Элементам из E приписаны веса $w(e_1) = a_1, ..., w(e_n) = a_n$. И пусть вектор $A = (a_1, ..., a_n)$, берется из R^n. На каждой траектории определяется функционал $\tau(A)$ – длина траектории при взвешивании A. Функционал может быть задан различными способами, наиболее известные из которых – линейный функционал:

$$\tau(A) = \sum_{e_i \in \tau} a_i \qquad (1)$$

и функционал задачи на узкие места:

$$\tau(A) = \max_{e_i \in \tau} a_i.$$

Под дискретной оптимизационной задачей будем понимать тройку (E, D_n, A) с определенным на ней типом функционала. Будем обозначать через Z_A индивидуальную задачу массовой задачи (E, D_n, A), определяемую путем задания вектора A.

Решениями задачи называются траектории, доставляющие экстремум, например, минимум функционалу (оптимальные траектории). В указанную схему укладываются все задачи, так называемой, комбинаторной оптимизации, в частности, все оптимизационные задачи на графах, что подчеркивается выделением в определении задания множества D_n.

Множество номеров оптимальных траекторий задачи при взвешивании A обозначим через $\varphi(A)$, а длину оптимальной траектории — $m(A)$. Через $S_\Delta(A)$ обозначим открытый шар в R^n с центром в A и радиуса Δ.

Под обратной задачей будем понимать тройку $(E, D_n, \varphi(A))$. Решением обратной задачи будет матрица A, для которой заданный набор траекторий φ является множеством оптимальных траекторий (или множество всех таких матриц $W(A)$). Будем обозначать через Z^*_φ индивидуальную задачу массовой задачи $(E, D_n, \varphi(A))$, определяемую путем задания множества φ.

Пусть $R_0 = \{A: A \in R^n, |\varphi(A)| = m\}$ и в пространстве R^n задана норма. Назовем задачу Z_A ε-устойчивой, если для любого $B \in R^n$, $\|B\| < \varepsilon$, выполняется условие $\varphi(A + B) \subseteq \varphi(A)$. Радиус устойчивости задачи Z_A, $A \in R_0$, полагаем по определению равным нулю, в противном случае радиусом устойчивости назовем *sup* ε, где *sup* берется по всем ε, для которых Z_A является ε-устойчивой. Обоснование, подробный анализ введенных определений, а также исследование устойчивости многих известных оптимизационных задач как с линейным, так и с минимаксным функционалом при различных типах норм в R^n можно найти, например, в [1–7].

Таким образом, радиус устойчивости задает предел возмущений элементов весового вектора задачи Z_A, при которых не расширяется множество оптимальных решений.

В [6] рассматривались задачи на матроидах и пересечении матроидов для случая чебышевской метрики в R^n. Для случая единственной оптимальной траектории формула для радиуса устойчивости при некотором дополнительном условии получена в [5].

Устойчивость и обратные оптимизационные задачи. Предлагаемая здесь методика базируется на связи исследования устойчивости с обратными оптимизационными задачами. Эта тема исследовалась, например, в работах [3–5].

Показано, что знание радиуса устойчивости и его оценок при определенных условиях позволяет решать такие задачи. В работе [5] этому посвящен отдельный раздел, где в общем случае и на примере задачи коммивояжера рассмотрена связь проблематики устойчивости с подходами по решению обратных задач.

Рассмотрим возможность применения этих результатов для передачи информации по открытым каналам.

Пусть имеется канал связи, по которому работают пользователи A и B и злоумышленник Z имеет к нему доступ.

Для скрытия информации используется некоторая *NP*-полная задача большой размерности, например, задача коммивояжера на графе с n вершинами. На сегодня при достаточно больших n нет эффективных алгоритмов ее решения.

Типовым случаем (при вероятностном подходе «с вероятностью единица») является ситуация $|\varphi(A)| = 1$ (см., например, [8] и [4]). При решении обратной задачи по заданной траектории нужно уметь строить вектор (матрицу) A, где заданная траектория является оптимальной.

Пусть злоумышленнику известно n и тип используемой задачи. Как показано, например, в работах [3–5] решение обратной задачи базируется на задании некоторого множества параметров, связанных с комбинаторикой задачи. При этом одним из главных (а в ряде случаев ключевым) является радиус устойчивости той прямой задачи (E, D_n, A), для которой найдено $\varphi(A)$. Обозначим этот набор параметров через $P(\varphi)$.

Зная этот набор параметров A и B скрывают свою информацию с помощью элементов оптимальной траектории, например, в случае задачи коммивояжера передаваемая информация содержится только в n элементах минимального гамильтонова цикла, а остальные элементы вектора (матрица) A используются для ее сокрытия.

Не зная оптимальной траектории, злоумышленник информацию из сообщения извлечь не может по той же причине, что и в алгоритмах *RSA*. Точное решение *NP*-трудных задач большой размерности невозможно получить «за разумное время». В то же время A и B передают друг другу матрицу с известной оптимальной траекторией. При этом за счет варьирования параметрами множества $P(\varphi)$ матрицы могут быть разными.

Если к этому добавить какой-нибудь алгоритм открытого распределения ключей, то по нему можно передавать саму оптимальную траекторию, тем самым постоянно ее меняя.

Конечно, тематика обратных задач – известная серьезная проблема дискретной оптимизации. Мы же лишь с помощью результатов [3–5] указываем на возможность использования в определенных задачах и в определенных методах параметра под названием «радиус устойчивости».

Далее на простом примере проиллюстрируем еще одну возможность применения радиуса устойчивости.

Алгоритм восстановления информации с помощью радиуса устойчивости. Вновь рассмотрим канал обмена информацией между пользователями A и B при наличии доступа злоумышленника Z к этому каналу. Пусть, как и выше, пользователи A и B используют решение траекторной задачи для сокрытия информации. Пусть размерность этой задачи, а также ее тип известны и злоумышленнику.

Неизвестно лишь то, что при этом A и B используют радиус устойчивости. Рассмотрим один из примеров такого использования. Алгоритмы и формулы для радиуса устойчивости и сходных с ним параметров разработаны для многих комбинаторных задач с различными типами функционалов, различными метриками в векторном пространстве весовых векторов, с различными типами и правилами возмущений.

Если метрика чебышевская, функционал линейный и задача на минимум, то в [6] показано, что

$$\rho(A) = \min_{j \notin \varphi(A)} \max_{i \in \varphi(A)} |\tau_i(A) - \tau_j(A)| / (|\tau_i| + |\tau_j| - 2|\tau_i \cap \tau_j|), \qquad (2)$$

а величина $r_{ij}(A) = |\tau_i(A) - \tau_j(A)| / (|\tau_i| + |\tau_j| - 2|\tau_i \cap \tau_j|)$ обладает тем свойством, что при добавлении ее ко всем элементам τ_i и вычитании из всех элементов τ_j длины этих траекторий сравняются. При этом мы считаем, что все элементы вектора (матрицы) A возмущаются независимо. Там же, в частности, показано, что для любой пары τ_i и τ_j оптимальной и неоптимальной траекторий возмущения элементов на величины, меньшие $r_{ij}(A)$, не может привести к выравниванию длин.

Отсюда следует, что при увеличении всех элементов A, кроме элементов из оптимальной траектории, на величину, равную половину радиуса, радиус устойчивости новой задачи с новой матрицей уменьшится вдвое.

Пусть теперь используется задача не обязательно *NP*-трудная и необязательно большой размерности.

Отправитель генерирует произвольную матрицу (вектор) A и решает на ней задачу, находя при этом не только оптимальную траекторию τ_i, но и радиус устойчивости $\rho(A)$. Как уже говорилось выше, с вероятностью единица оптимальная траектория единственна, поэтому в редком случае ее неединственности отправитель просто генерирует новую задачу.

Далее, для сокрытия информации отправитель использует все элементы A, кроме элементов оптимальной траектории. При этом можно использовать не сами элементы, а их веса.

Затем отправитель увеличивает веса всех элементов кроме весов элементов оптимальной траектории, например, на величину, равную половине радиуса устойчивости. И эта новая «возмущенная» матрица A' отправляется получателю.

Получатель для восстановления информации должен просто решить задачу и найти радиус устойчивости. После этого он вычитает его значение из всех элементов матрицы, кроме элементов оптимальной траектории. Таким образом восстанавливается исходная (невозмущенная) матрица.

Злоумышленник, зная тип и размерность задачи, не сможет восстановить информацию без знания процедуры применения радиуса устойчивости.

Заключение. Первая из предложенных методик основана на невозможности эффективного решения *NP*-трудной задачи. Вторая же, наоборот, предполагает решение полиномиально разрешимой задачи, однако требует и наличия эффективного алгоритма поиска радиуса устойчивости.

Как правило, для полиномиально разрешимых задач и радиус устойчивости находится за полиномиальное время, хотя степень полинома, характеризующего трудоемкость его вычисления, может быть выше, чем степень аналогичного полинома для алгоритма решения самой задачи.

Задачи на матроидах и пересечении матроидов сами решаются с полиномиальной сложностью и алгоритмы нахождения радиуса устойчивости тоже полиномиальны. (Сюда входит задача о кратчайшем остове. Задача о назначениях и многие другие известные оптимизационные задачи).

Для некоторых потоковых задач и частных случаев задачи о кратчайшем пути также существуют полиномиальные алгоритмы нахождения радиуса устойчивости. Однако, в общем случае, с точки зрения исследования устойчивости, задача о кратчайшем пути требует на сегодня экспоненциального алгоритма [7]. Так как в данном случае наличие циклов отрицательной длины не может быть исключено.

ЛИТЕРАТУРА

[1] Sotskov Yu.N., Leontev V.K., Gordeev E.N.Some concepts of stability analysis in combinatorial optimization. *Discrete Applied Mathematics,* 1995, vol. 58, pp. 169–190.

[2] Гордеев Э.Н., Леонтьев В.К. Общий подход к исследованию устойчивости решений в задачах дискретной оптимизации. *Журнал выч. мат. и мат. физ.*, 1996, т. 36, с. 66–72.

[3] Леонтьев В.К. Устойчивость в линейных дискретных задачах. В кн.: *Проблемы кибернетики*. Москва, Наука, 1979, вып. 35, с. 169–185.
[4] Леонтьев В.К., Гордеев Э.Н. Качественное исследование траекторных задач. Кибернетика, 1986, № 5, с. 82–90.
[5] Леонтьев В.К. *Устойчивость решений в дискретных экстремальных задачах*. Дис. … докт. физ.-мат. наук. Москва, 1981, 228 с.
[6] Гордеев Э.Н. Алгоритмы полиномиальной сложности для вычисления радиуса устойчивости в двух классах траекторных задач. *Журнал выч. мат. и мат. физ*., 1987, № 7, с. 984–992.
[7] Гордеев Э.Н. Устойчивость решений в задаче о кратчайшем пути на графе. *Дискретная математика*, 1989, № 3, с. 39–46.
[8] Гордеев Э.Н., Липкин Л.И. О единственности решения в задачах выбора. *Дискретный анализ*, Новосибирск, 1990.

Статья поступила в редакцию 28.06.2013

Ссылку на эту статью просим оформлять следующим образом:
Гордеев Э.Н. Использование радиуса устойчивости оптимизационных задач для скрытия и проверки корректности информации. *Инженерный журнал: наука и инновации*, 2013, вып. 11. URL: http://engjournal.ru/catalog/it/hidden/993.html

Гордеев Эдуард Николаевич родился в 1954 г., окончил Московский физико-технический институт в 1977 г. Д-р физ.-мат. наук, профессор кафедры «Информационная безопасность» МГТУ им. Н.Э. Баумана. Автор более 70 научных работ в области прикладной математики, информатики.