УДК 510.1

О СУЩЕСТВОВАНИИ ОДНОСТОРОННИХ ФУНКЦИЙ

Плотников А. Д.

ON THE EXISTENCE OF ONE-WAY FUNCTION

Plotnokiv A.

Формулируется теорема существования и устанавливаются свойства, которым должна удовлетворять односторонняя функция, используемая в криптологии. Приводится пример такой функции.

Ключевые слова: *криптология, односторонняя функция, класс P, класс NP.*

1 Постановка задачи

В криптологии используется понятие односторонней функции. Полагают, что функция y = f (x) является односторонней, если значение y для заданного x вычисляется "легко", а значение x для заданного y вычисляется "трудно". В настоящее время имеется некоторая неопределенность в существовании односторонних функций и не имеется точного критерия, который позволял бы определенно утверждать, что рассматриваемая функция является односторонней.

Вопрос о существовании односторонних функций увязывают с проблемой взаимоотношения классов P и NP. В связи с решением этой задачи (см. [1]) появилась возможность сформулировать критерий существования такой функции.

Цель данной работы — сформулировать теорему существования односторонней функции и указать ее теоретико-множественные свойства.

2 Подклассы класса NP

Уточним понятия "легкости" и "трудности" для односторонней функции.

В теории вычислительной сложности определяют класс задач NP [2, 3]. Говорят, что задача Z принадлежит классу NP, если:

1. задача может быть задана конечным числом символов n;

2. решение задачи также может быть представлено конечным числом m символов, где m есть полиномиальная функция от n: m = f(n);

3. время верификации полученного решения t есть некоторая полиномиальная функция от n: t = φ(n).

Множество задач из NP, имеющих полиномиально-временной решающий алгоритм, образует класс P, где P $\subset$ NP. Элементарным примером задачи класса P является задача поиска наибольшего элемента массива длины n. Ясно, что для этого надо рассмотреть все элементы массива, т.е. время поиска решения в этом случае равно O(n).

Общепринятой моделью вычислительного процесса решения любой задачи является машина Тьюринга [1]. Сущность этого процесса состоит в том, что исходные данные (параметры) индивидуальной задачи по¬следовательно преобразуются такт за тактом (шаг за шагом). Результатом таких преобразований является получение решения задачи, если оно имеется, или ответ, что решения данной задачи не существует. Все результаты вычислительного процесса решения задачи машиной Тьюринга до получения окончательного ответа, очевидно, следует рассматривать как промежуточные результаты, вычислений.

Чтобы вычислительный процесс был направлен на получение правильного результата, необходимо на каждом шаге вычислений проверять промежуточный результат на его принадлежность хотя бы какому-то допустимому решению задачи.

Например, если находится решение задачи Выполнимость, то на каждом шаге выбора различных литералов (значений булевых переменных), составляющих допустимое решение, эти результаты должны удовлетворять условию непротиворечивости, т.е. нельзя в промежуточное решение выбирать одновременно переменную x и ее отрицание X. И возможность такого выбора в данной задаче легко проверяется.

В определении задачи класса NP процедура проверки промежуточного результата никак не оговаривается. Поэтому в классе NP мы выделим класс задач, для которых время проверки промежуточного результата есть полиномиальная функция от размерности задачи n. Множество всех таких задач обозначим UF. Любую задачу класса UF будем называть *задачей без предвидения*.

Таким образом, из определения задачи без предвидения следует, что в задачах, принадлежащих множеству NP \ UF, время проверки хотя бы одного промежуточного решения есть экспоненциальная функция от размерности задачи. Приведем пример оптимизационной задачи из класса NP \ UF в распознавательной форме.

Тяжелый набор (TH)

Условие. Заданы конечное множество X = $\{x_1,x_2,..., x_п\}$ булевых переменных, бент-функция $f(x_1,x_2,... ,x_n) \in \{0; 1\}$, функция $w(x_1,x_2,..., x_п) \in Z^+$ и граница $E \in Z^+$, которая может быть представлена конечным числом символов m, где m есть полиномиальная функция от n: m= ω (n). Полагаем, что функции f(X), w(X) вычисляются за

полиномиальное время и функция w(X) не является константой.

Вопрос. Существует ли набор значений булевых переменных X такой, что f(X)=1 и значение w(X) не меньше E?

Теорема 1. *Задача ТН принадлежит классу NP.*

Доказательство. В самом деле, исходные данные задачи ТН и решения конечны и решение имеет линейный размер от размерности задачи. Кроме того, полученный набор (решение) может быть проверено за полиномиальное время. Поэтому TH$ $\in$ NP.

Теорема 2. *Задача ТН не может быть решена за полиномиальное время.*

Доказательство. В задаче ТН имеется неявное требование перебора всех наборов, на которых бент-функция f(X) равна 1. Отсюда следует, что набор максимального веса можно найти только рассмотрев все элементы массива таких наборов. Так как одно из свойств бент-функции состоит в том, что ровно на половине наборов X ее значение равно 1, а на другой половине наборов равно 0, то верификация промежуточных результатов возможна лишь после просмотра весов всех наборов, на которых f(X) = 1. Так как число таких наборов равно 2n-1, отсюда следует справедливость сделанного утверждения.

Теорема 3. *Задача ТН принадлежит классу NP \ UF.*

Доказательство. Нетрудно видеть, что максимальный вес текущего набора X булевых переменных (промежуточный результат) проверяется за экспоненциальное время, т.е. требует O(2n-1) единиц времени.

Следствие 4. NP\UF $\neq \emptyset$.

Следствие 5. UF $\neq$ NP.

3 Свойства односторонних функций

В теории сложности вычислений понятие "легкости" и "эффективности" вычисления означают, что время вычисления t некоторой функции y = f (x) есть полиномиальная функция от размерности задачи n: t = λ (n). Тогда понятие "трудности" вычисления означает, что время вычисления T функции x = f-1(y), когда она существует, является экспоненциальной функцией от размерности задачи n: T = Λ (n). Таким образом, имеет место следующее утверждение.

Теорема 6. *Если y = f (x) есть односторонняя функция, то она принадлежит классу P, а функция x = f $^{-1}$(y) существует и принадлежит множеству NP \ UF.*

Доказательство. Справедливость сделанного утверждения следует из определения понятия односторонней функции.

С теоретико-множественной точки зрения мы можем рассматривать функцию y = f (x) как отображение R: Dom(R) $\rightarrow$ Ran(R), где x $\in$ Dom(R) и y $\in$ Ran(R). Ясно, что для каждого элемента x $\in$ Dom(R) отображение x $\rightarrow$ Ran(R) должно содержать полиномиальное число элементов. С другой стороны функция x = f^{-1}(y) есть отображение R^{-1}: Dom(R^{-1}) $\rightarrow$ Ran(R^{-1}) или, равносильно, Ran(R) $\rightarrow$ Dom(R). Для того, чтобы функция y = f(x) была односторонней, необходимо, чтобы отображение элемента y $\rightarrow$ Dom(R) содержало экспоненциальное число элементов.

Примером односторонней функции может служить бент-функция f(x_1, . . . , $x_п$) из задачи ТН. В этой задаче вычисление “прямой” функции f(X)и веса w(X) происходит, по условию, за полиномиальное время от n, а обратная задача --- поиск набора наибольшего веса, на котором f(X)=1 – происходит за экспоненциальное время от n.

Таким образом, мы доказали следующее утверждение.

Теорема 7. *Класс Q $\subset$ NP односторонних функций не пустой и каждая, односторонняя, функция,*
y = f (x) обладает следующими свойствами:

- *аргумент x может быть записан конечным числом символов n;*
- *значение функции y может быть записано m символами, где m есть полиномиальная функция от n: m = π (n);*
- *время вычисления t функции y есть полиномиальная функция от и: t = $\wp$ (n);*
- *время вычисления какого-либо промежуточного значения функции x = f^{-1}(y) (или его длина) есть экспоненциальная функция от n.*

4 Заключение

Из данной работы следует, что криптосистема будет теоретически стой¬кой, если использует функцию шифрования, удовлетворяющую Теореме 7, а не опирается на трудности работы с громадными числами.

Литература

1. Plotnikov, A. D. On the relationship between classes P and NP / A, D, Plotnikov, // Journal of Computer Science— 2011,— № 7(8).— 1036-1040.

2. Гэри, М. Вычислительные машины и труднорешаемые задачи: пер. с англ. / М. Гэри, Д. Джонсон. — М.: Мир, 1982. — 416 с.

3. Рейнгольд, Э. Комбинаторные алгоритмы: пер. с англ. / Э. Рейн¬гольд, Ю. Нивергельт, Н. Део. — М.: Мир, 1980. — 476 с.

References

1. Plotnikov, A. D. On the relationship between classes P and NP / A, D, Plotnikov, // Journal of Computer Science— 2011,— № 7(8).— 1036-1040.

2. Gjeri, M. Vychislitel'nye mashiny i trudnoreshaemye zadachi: per. s angl. / M. Gjeri, D. Dzhonson. — M.: Mir, 1982. — 416 p.

3. Rejngol'd, Je. Kombinatornye algoritmy: per. s angl. / Je. Rejn¬gol'd, Ju. Nivergel't, N. Deo. — M.: Mir, 1980. — 476 p.

Плотніков О. Д.

ПРО ІСНУВАННЯ ОДНОСТОРОННІХ ФУНКЦІЙ

Формулюється теорема існування і встановлюються властивості, яким повинна задовольняти односторонння функція, яка використовується в криптології. Наводиться приклад такої функції.

Ключові слова: *кріптологія, односторо-ня функція, клас P, клас NP.*

Plotnokiv A.

ON THE EXISTENCE OF ONE-WAY FUNCTION

The theorem of existence and set the properties to be satisfied by a one-way function used in cryptology. The example of such a function.

Keywords: *cryptology, one-way function, class P, class NP.*

Плотников А. Д. – к.т.н., профессор, ВНУ им. В. Даля, Луганск.

Рецензент: Петров Олександр Степанович – докт. техн. наук, професор, завідувач кафедри безпеки інформаційних систем, Східноукраїнський національний університет імені Володимира Даля, м. Луганськ.