ISSN 2076-2429 (print)
ISSN 2223-3814 (on line)

КОМП'ЮТЕРНІ Й ІНФОРМАЦІЙНІ МЕРЕЖІ І СИСТЕМИ

АВТОМАТИЗАЦІЯ ВИРОБНИЦТВА

COMPUTER AND INFORMATION NETWORKS AND SYSTEMS

MANUFACTURING AUTOMATION

УДК 004.67:519.714

В.Ю. Гнатенко, инженер,
В.С. Ситников, д-р техн. наук, проф.,
П.В. Ступень, канд. техн. наук,
Одес. нац. политехн. ун-т

НАХОЖДЕНИЕ ДЕЛИТЕЛЕЙ ЦЕЛОГО ЧИСЛА ПУТЕМ РЕШЕНИЯ БУЛЕВА УРАВНЕНИЯ

В.Ю. Гнатенко, В.С. Ситніков, П.В. Ступень. **Знаходження дільників цілого числа шляхом вирішення булева рівняння.** Описано загальну структуру булева рівняння для знаходження дільників цілого числа. Запропоновано послідовність вирішення булева рівняння за допомогою одержання функції кількості одиничних значень булевої функції та бисекції.
Ключові слова: визначення подільності, факторизація.

В.Ю. Гнатенко, В.С. Ситников, П.В. Ступень. **Нахождение делителей целого числа путем решения булева уравнения**. Описана общая структура булева уравнения для нахождения делителей целого числа. Предложена последовательность решения булева уравнения посредством получения функции количества единичных значений булевой функции и бисекции.
Ключевые слова: определение делимости, факторизация.

V.Yu. Gnatenko, V.S. Sitnikov, P.V. Stupen. **Finding divisors of the integer by solving Boolean equations**. A general structure of the Boolean equation for finding divisors of an integer is described. A solution sequence of the Boolean equation by obtaining the function of unit values of the Boolean function and bisection is proposed.
Keywords: divisibility determination, factorization.

Одна из важных задач при сохранении информации в компьютерных системах — оценка криптостойкости алгоритмов шифрования. В основе криптостойкости некоторых алгоритмов шифрования с открытым ключом, например RSA (аббревиатура от фамилий Rivest, Shamir и Aldeman) [1], лежит вычислительная сложность задачи факторизации.

В зависимости от длины факторизуемого числа в бинарном представлении существуют алгоритмы факторизации экспоненциальной и субэкспоненциальной сложности [1]. Под факторизацией подразумевается разложение натурального числа в произведение простых множителей.

Сложность алгоритма Шора [2] полиномиальна, однако, квантовых компьютеров пригодных для его реализации для больших чисел, пока нет.

© Гнатенко В.Ю., Ситников В.С., Ступень П.В., 2012

Вопрос о существовании алгоритма факторизации с полиномиальной сложностью на компьютере с классической архитектурой является одной из важных открытых проблем современной теории чисел [1].

Отсутствие алгоритмов факторизации полиномиальной сложности посредством решения каких-либо булевых уравнений обусловливает необходимость рассмотрения вопросов определения структур соответствующих булевых уравнений и выбора стратегий их решения.

Факторизацию произвольного натурального числа можно свести к решению булева уравнения. При этом необходимо определить структуру этого уравнения и пути его решения.

Пусть число, делители которого нужно найти,

$$C=\sum_{i=0}^{n}(2^i c_i),\ C_{\text{в}}=\sum_{i=0}^{2n}(2^i c_{\text{в}i}),\ A=\sum_{i=0}^{n}(2^i a_i),\ B=\sum_{i=0}^{n}(2^i b_i)$$

где n — старший разряд C (0 — младший разряд C),

$C_{\text{в}}$ — произведение неизвестных A и B,

a_i, b_i — разряды неизвестных A и B, соответственно;

C, $C_{\text{в}}$, A, $B \in N$;

N — множество натуральных чисел,

$c_i=\begin{cases} c_i,\ i \le n; \\ 0,\ i > n. \end{cases}$ — значение i-го разряда C,

$c_{\text{в}i}=\begin{cases} c_{\text{в}i},\ i \le n; \\ 0,\ i > n. \end{cases}$ — булева функция от разрядов неизвестных A и B, представленных в двоичной системе счисления.

Значение i-го разряда $C_{\text{в}}$ согласно правил умножения чисел в двоичной системе счисления —

$$c_{\text{в}i}=\bigoplus_{j=0}^{i}(a_i b_{i-j})\oplus\bigoplus_{j=0}^{\frac{i(i-1)}{2}}P_{ij},$$

где $P_{ij-1}=\begin{cases} c_{\text{чв}i-1j-1}a_j b_{i-1-j},\ 1 \le j < i; \\ c_{\text{чв}i-1j-1}P_{i-1j},\ i \le j < i+\dfrac{i(i-1)}{2},\ i > 2, \end{cases}$

$c_{\text{чв}ij}=\begin{cases} \bigoplus\limits_{j=0}^{m}a_j b_{i-j},\ 0 \le m \le i; \\ \bigoplus\limits_{j=0}^{i}a_j b_{i-j}\oplus\bigoplus\limits_{j=0}^{m}P_{ij},\ 0 \le m < \dfrac{i(i-1)}{2}-1, \end{cases}$ — частичное значение $c_{\text{в}i}$;

$a_j=\begin{cases} a_j\ ,\ j \le n; \\ 0,\ j > n \end{cases}$;

$b_j=\begin{cases} b_j\ ,\ j \le n; \\ 0,\ j > n. \end{cases}$

Можно получить булево уравнение

$$\prod_{i=0}^{2n}(c_i \oplus c_{\text{в}i}\oplus 1)=1, \tag{1}$$

решениями которого являются искомые разряды неизвестных делителей A и B числа C.

Решение булева уравнения в общем виде

$$f(x_0,\ ...,\ x_n)=1, \tag{2}$$

где $f(x_0, ..., x_n)$ — булева функция булевых аргументов, может быть получено в результате перебора значений функции $f(x_0, ..., x_n)$ — левой части уравнения (2), полученных при подстанов-

 ISSN 2076-2429 (print)
ISSN 2223-3814 (on line)

ке всех возможных комбинаций ее аргументов x_0, ..., x_n. В этом случае для решения уравнения (2) требуется экспоненциальное количество действий.

Задача перебора значений функции $f(x_0, ..., x_n)$ на заданном множестве M комбинаций ее аргументов x_0, ..., x_n аналогична задаче подсчета количества единичных значений $f(x_0,...,x_n)$ на множестве M. Для корректной постановки задачи подсчета количества единичных значений $f(x_0, ..., x_n)$ на множестве M необходимо выбрать способ упорядочения этого множества — установить соответствие значений элементов множества M присвоенным им индексам k.

Применяя $F(k)$ — функцию количества единичных значений $f(x_0,...,x_n)$ для k последовательно расположенных элементов упорядоченного множества M, можно решить уравнение (2) методом, аналогичным бисекции [4].

Пусть $k_{\min}$, $k_{\max}$ — индексы элементов на границах множества M. Если множество M содержит более одного решения уравнения, следует определить дополнительные критерии поиска решения, к примеру — искомое решение должно быть минимальным.

Если $F(k) = 0$ при $k = k_{\max}$, то уравнение (2) не имеет решения. В противном случае диапазон индексов $[k_{\min}, ..., k_{\max}]$ делится пополам. При заданном дополнительном критерии “поиск минимального решения”, если левая часть диапазона содержит решения уравнения (2), то выбирается эта часть диапазона для дальнейшего деления, иначе — выбирается правая часть диапазона. Деление выбираемого диапазона продолжается до тех пор, пока диапазон содержит более одного индекса.

За количество итераций K деление пополам осуществляется K раз, поэтому длина конечного диапазона в 2^K раз меньше длины исходного. При этом сложность решения уравнения (2) определяется сложностью вычисления $F(k)$.

Сложность вычисления $F(k)$ для заданного класса булевых функций определяется свойствами, присущими этому классу, и способами представления $F(k)$.

Представление $F(k)$ зависит от способа упорядочения ее области определения множества M. В частности, в результате реализации одного из способов упорядочения множества M функция $F(k)$ может быть представлена в результате преобразования $f(x_0, ..., x_n)$ в булеву последовательность и получения интеграла этой последовательности [3].

В связи с этим один из путей оценки сложности решения обобщенного для натурального числа C любой длины уравнения (1) — решение вопроса существования полиномиальной сложности формулы вычисления интеграла булевой последовательности [3], полученной из левой части уравнения (1). При этом определенность структуры булевой последовательности — необходимое условие поиска структуры ее интеграла полиномиальной сложности.

Таким образом, предложенная последовательность вычислений любого разряда произведения двух натуральных чисел, представленных в двоичной системе счисления, позволяет упростить его представление и рассмотреть возможность нахождения делителей натурального числа полиномиальной сложности путем решения булева уравнения.

Литература

1. Ян, С.Й. Криптоанализ RSA / С.Й. Ян; пер. с англ. Ю.Айдарова. — М.; Ижевск: НИЦ Регулярная и хаотическая динамика; Ижев. ин-т компьютер. исслед., 2011. — 312 с.
2. Shor, P.W., Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer / P.W. Shor // SIAM J. Comput Vol. 26(5). — P.1484 — 1509.
3. Гнатенко, В.Ю. Аналитическое представление сумм булевых последовательностей / В.Ю. Гнатенко, В.С. Ситников, П.В. Ступень // Пр. Одес. політехн. ун-ту. — Одеса, 2012. — Вип. 1(38). — С.147 — 152.
4. Волков, Е.А. Численные методы: Учеб. пособие для вузов. — 2-е изд., испр. — М.: Наука, 1987.— 248 с.

References

1. Jan, S.J. Kriptoanaliz RSA [Cryptanalysis RSA]/ S.J. Jan; per. s angl. Ju.Ajdarova [Transl. from Eng. by Yu. Aydarov] — M.; Izhevsk: NIC Reguljarnaja i haoticheskaja dinamika, Izhev. in-t komp’juter. issled. [Research Center “Regular and Chaotic Dynamics”, Izhevsk Inst. of Comp. Studies], 2011. — 312 s.

2. Shor, P.W., Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer / P.W. Shor // SIAM J. Comput Vol. 26(5) — P. 1484 — 1509.
3. Gnatenko, V.Yu. Analiticheskoje predstavlenije summ bulevih posledovatel'nostey [Analytical Representation of Sums of Boolean Sequences] / V.Yu. Gnatenko, V.S. Sitnikov, P.V. Stupen // Pr. Odes. politeh. un-ty [Proc. of the Odesa Polytech. Univ.]. — Odesa, 2012. — Vip. 1(38). — S. 147 — 152.
4. Volkov, E.A. Chislennie metody: Ucheb. posobie dlya vuzov [Numerical Methods: Study Guide for Univ.]. — 2-e izd., ispr.— M.: Nauka,1987. — 248 s.

Рецензент д-р техн. наук, проф. Одес. нац. политехн. ун-та Паулин О.Н.

Поступила в редакцию 29 сентября 2012 г.