УДК 004.67:519.714

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

АНАЛИТИЧЕСКОЕ ПРЕДСТАВЛЕНИЕ СУММ БУЛЕВЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ

В.Ю. Гнатенко, В.С. Ситніков, П.В. Ступень. **Аналітичне подання сум булевих послідовностей**. Розглянуто поняття булевої послідовності. Описано й обгрунтовано основні способи аналітичного подання сум булевих послідовностей в канонічному вигляді.

Ключові слова: сумма булевої послідовності.

В.Ю. Гнатенко, В.С. Ситников, П.В. Ступень. **Аналитическое представление сумм булевых последовательностей.** Рассмотрено понятие булевой последовательности. Описаны и обоснованы основные способы аналитического представления сумм булевых последовательностей в каноническом виде.

Ключевые слова: сумма булевой последовательности.

V.Yu. Gnatenko, V.S. Sitnikov, P.V. Stupen. **Analytical representation of Boolean sequences sums**. The notion of a Boolean sequence is considered. The basic methods of Boolean sequences analytic representation in the canonical form are described and justified.

Keywords: boolean sequence sum.

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 (буквенная аббревиатура от фамилий Rivest, Shamir и Aldeman) [1], лежит вычислительная сложность задачи факторизации.

Существуют алгоритмы факторизации экспоненциальной и субэкспоненциальной сложности в зависимости от длины факторизуемого числа в бинарном представлении [1]. Факторизация — разложение натурального числа в произведение простых делителей.

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

Вопрос о существовании алгоритма факторизации с полиномиальной сложностью на компьютере с классической архитектурой является одной из важных открытых проблем современной теории чисел [1]. Одно из направлений решения этой проблемы состоит в минимизации представления некоторой функции.

Пусть задан показатель делимости числа x на число y без остатка —

$$\text{функция } f_{\text{res}}(x,y) = \begin{cases} 1, & \text{mod}_y\, x = 0; \\ 0, & \text{mod}_y\, x \neq 0. \end{cases}$$

где сумма $F_{\text{res}}(x,z) = \sum_{y=1}^{z} f_{\text{res}}(x,y)$,

$z \le x$,

$y \in N$,

N — множество натуральных чисел.

Реализация дихотомического алгоритма факторизации, сложность которого линейно зависит от количества разрядов факторизуемого числа, представленного в двоичной системе счисления, и меры сложности $F_{\text{res}}(x,z)$, очевидна. Для доказательства существования или несуще-

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

ствования формы реализации $F_{\text{res}}(x,z)$ полиномиальной сложности необходимо в первую очередь представить $F_{\text{res}}(x,z)$ в каноническом виде.

$f_{\text{res}}(x,y)$ — функция целочисленных аргументов, принимающая булевы значения, т.е. булева последовательность (БП). БП является подмножеством целочисленных функций. Булева функция (БФ) — подмножество БП.

Предлагается систематизация аналитического представления сумм булевых последовательностей (СБП) по произвольным аргументам.

Виды аналитического представления СБП в канонической форме можно разделить по способу получения полинома СБП из полинома БП:

первый вид — с поразрядным получением СБП; второй — инвариантный и третий, зависимый от порядка следования принимаемых аргументами БП значений — виды без поразрядного получения СБП.

Второй вид представления СБП реализуется на основе методов, применяемых в логико-вероятностном исчислении (ЛВИ) [3]. При этом каноническое представление суммируемой БП — целочисленный полиномом ее аргументов $Y(x_1, \ldots, x_i, \ldots, x_m)$. Полином СБП получается путем замены каждого аргумента x_i суммой принимаемых им значений X_i. То есть суммирование значений производится для всех возможных комбинаций заданных аргументов $Y(x_1, \ldots, x_i, \ldots, x_m)$, порядок следования комбинаций в этом случае не важен.

При реализации третьего вида представления СБП суммируемая БП $Y(el_1(x), \ldots, el_i(x), \ldots, el_m(x))$ представляется полиномом элементарных БП (ЭБП)

$$el_i(x) = \begin{cases} 1,\ 0 \le \operatorname{mod}_{T_i}(x) \le \dfrac{T_i}{2} - 1; \\ 0,\ \dfrac{T_i}{2} - 1 < \operatorname{mod}_{T_i}(x) \le T_i - 1, \end{cases} \quad (1)$$

где $i, x \in N$,

$T_i = 2^{i+1}$ — величина периода i-й ЭБП.

Для получения СБП элементарного полинома — произведения произвольных ЭБП — предлагается следующий алгоритм:

— создать и сортировать в порядке возрастания значений элементов массив I индексов ЭБП, составляющих произведение; индексация элементов массива I начинается с 0;

— задать начальное значение верхнего предела суммирования — z, произведения — П и i_{cur} — текущего индекса массива I;

$z = z_{\max}$;

П = 0;

$i_{\text{cur}} = \text{length}(I) - 1$.

Пока $i_{\text{cur}} \ge 1$ Цикл

$$\Pi = \Pi + \frac{T_{I(i_{\text{cur}})}}{2^{i_{\text{cur}}+1}} \operatorname{Int}\left(\frac{z}{T_{I(i_{\text{cur}})}}\right).$$

Если $\operatorname{mod}_{T_{I(i_{cur})}}(z) \ge \dfrac{T_{I(i_{\text{cur}})}}{2}$, тогда

$$\Pi = \Pi + \frac{T_{I(i_{\text{cur}})}}{2^{i_{\text{cur}}+1}}.$$

Конец вычислений

Иначе

$z = \operatorname{mod}_{T_{I(i_{\text{cur}})}}(z)$;

$i_{\text{cur}} = i_{\text{cur}} + 1$.

Конец Цикла.

Если $\text{mod}_{T_{I(i_{\text{cur}})}}(z) \geq \frac{T_{I(i_{\text{cur}})}}{2}$, тогда

$\Pi = \Pi + \frac{T_{I(i_{\text{cur}})}}{2}$.

Конец вычислений.

Иначе

$z = \text{mod}_{T_{I(i_{\text{cur}})}}(z)$.

$\Pi = \Pi + z$.

Конец вычислений.

При этом Int(z) — целая часть числа z, $T_{I(i_{\text{cur}})}$ — длина периода $el_{I(i_{\text{cur}})}(z)$, length($I$) — длина массива I.

Получение СБП для всех составляющих полином $Y(el_1(x), \ldots, el_i(x), \ldots, el_m(x))$ произведений определяет СБП всего полинома.

Предложенный алгоритм обусловлен следующим свойством ЭБП:

— на числовом промежутке, кратном периоду ЭБП с максимальным индексом в произведении ЭБП, количество единичных значений зависит только от количества множителей в произведении;

— первую половину периода каждой ЭБП составляют единичные значения, что определяет порядок подсчета количества единиц на участках, выходящих за границы числового промежутка, кратного периоду ЭБП с максимальным индексом в произведении ЭБП.

Рассмотрим первый вид представления СБП с поразрядным преобразованием.

Для суммы значений y_i БП Y, $y_i \in \{0,1\}$, $0 \leq i \leq n$, справедливо выражение

$$\sum_{i=0}^{n}(y_i) = \sum_{j=0}^{k}\left(2^j \bigoplus_{i=j}^{n}(p_{ij})\right) \tag{2}$$

где $k = \text{Int}(\log_2(n))$ — вес старшего разряда двоичной суммы,

$i, n \in N$;

$p_{ij} = p_{ij-1} \bigoplus_{i=j}^{i-1}(p_{i\,j-1})$ — значение i-го переноса из j–1-го разряда в j-й, для $j > 0$;

$p_{i0} = y_i$,

$\bigoplus_{i=j}^{n}(p_{ij})$ — значение j-го разряда суммы $\sum_{i=0}^{n}(y_i)$, сумма по модулю 2 ($\oplus$) переносов из j–1-го разряда суммы $\sum_{i=0}^{n}(y_i)$ в j-й, для $j > 0$.

Полагая младший разряд $\bigoplus_{i=j}^{n}(p_{ij})$ суммы (2) алгебраической функцией $P_0(i)$, рассмотрим взаимосвязь функции каждого последующего разряда $P_{l+1}(i)$ от функции предыдущего $P_l(i)$, т.е.

$$P_{l+1}(i) = P_l(i) \oplus \bigoplus_{j=0}^{i}[P_l(j)\Delta_{\oplus}(P_l(j))], \tag{3}$$

где $\Delta_{\oplus}(P_{l+1}(j)) = P_{l+1}(i) \oplus P_{l+1}(i-1)$ — “производная” по модулю 2 функции $P_{l+1}(i)$,

$\bigoplus_{j=0}^{i}[P_l(j)\Delta_{\oplus}(P_l(j))]$ — “интеграл” по модулю 2 .

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

Доказательство.

Очевидно $P_{l+1}(i) = \bigoplus_{j=0}^{i}[\Delta_{\oplus}(P_{l+1}(j))]$ для всех $l \geq 0$.

Согласно правилам сложения чисел в двоичной системе счисления

$$\Delta_{\oplus}(P_{l+1}(i)) = P_l(i-1)\Delta_{\oplus}(P_l(i)) .$$

Согласно определению "производной" по модулю 2 функции $P_l(i)$

$$P_l(i-1) = P_l(i) \oplus \Delta_{\oplus}(P_l(i)) .$$

Следовательно,

$$\Delta_{\oplus}(P_{l+1}(i)) = \Delta_{\oplus}[P_l(i) \oplus P_l(i)\Delta_{\oplus}(P_l(i))] . \quad (4)$$

Учитывая аддитивность суммирования по модулю 2, проинтегрируем по модулю 2 обе части выражения (4). Тогда

$\bigoplus_{j=0}^{i}[\Delta_{\oplus}(P_{l+1}(j))] = P_{l+1}(i)$ — для левой части,

$$\bigoplus_{j=0}^{i}[\Delta_{\oplus}(P_l(i) \oplus P_l(i)\Delta_{\oplus}(P_l(i)))] = \bigoplus_{j=0}^{i}[\Delta_{\oplus}(P_l(i)] \oplus \bigoplus_{j=0}^{i}[P_l(i)\Delta_{\oplus}(P_l(i))] =$$

$= P_l(i) \oplus \bigoplus_{j=0}^{i}[P_l(i)\Delta_{\oplus}(P_l(i))]$ — для правой,

что и требовалось доказать.

Рассмотрим суммирование и дифференцирование по модулю 2 произведений ЭБП.

Будем полагать длину области определения заданного произведения ЭБП t, равной 2^m, где $m \in N$.

ЭБП с максимальным индексом для заданного t будет $el_{m-1}(x)$.

Суммой по модулю 2 всех ЭБП на области t будет функция, в которой все значения — единицы,

$$\bigoplus_{i=0}^{n}\left[\prod_{j=0}^{m-1} el_j(i)\right] = 1 , \; 0 \leq n \leq t. \quad (5)$$

Если в произведении присутствуют все ЭБП с индексами 0, …, l, то они заменяются на ЭБП с индексом l+1, т.е.

$$\bigoplus_{i=0}^{n}\left[\prod_{j=0}^{l} el_j(i)\right] = el_{l+1}(n) , \; l < m-1. \quad (6)$$

Для дифференцирования по модулю 2 совершаются обратные действия.

Представив любую БП в базисе "И", "ИСКЛЮЧАЮЩЕЕ ИЛИ" ($\oplus$) в канонической форме, с учетом аддитивности суммирования по модулю 2, путем аналитических преобразований на основе соотношений (3), (5) и (6) можно получать формулы для подсчета количества ее единичных значений.

Рассмотрим получение СБП для БП

$$Y(x) = \text{НЕ}\left(el_0(x) \text{И} el_1(x)\right) \text{И} el_2(x) , \; 0 \leq x \leq 7.$$

В базисе $\oplus$ логическое И, канонической форме

$$Y = \left(el_0(x) \text{И} el(x)_1 \oplus 1\right) \text{И} el_2(x) = el_0(x) \text{И} el_1(x) \text{И} el_2(x) \oplus el_2(x) ,$$

$$P_0(i) = \bigoplus_{j=0}^{i}[el_0(x) \text{И} el_1(x) \text{И} el_2(x) \oplus el_2(x)] = 1 \oplus el_0(x) \text{И} el_2(x) ,$$

$$P_1(i) = P_0(i) \oplus \bigoplus_{j=0}^{i}[P_0(j)\Delta_{\oplus}(P_0(j))],$$

$$P_0(j)\Delta_{\oplus}(P_0(j) = \left(1 \oplus el_0(x)Иel_2(x)\right)И\left(el_0(x)Иel_1(x)Иel_2(x) \oplus el_2(x)\right) =$$
$$el_2(x) \oplus el_0(x)Иel_2(x),$$

$$\bigoplus_{j=0}^{i}[P_0(j)\Delta_{\oplus}(P_0(j))] = el_0(x)Иel_2(x) \oplus el_1(x)Иel_2(x),$$

$$P_1(i) = 1 \oplus el_1(x)Иel_2(x),$$

$$P_2(i) = P_1(i) \oplus \bigoplus_{j=0}^{i}[P_1(j)\Delta_{\oplus}(P_1(j))],$$

$$P_1(j)\Delta_{\oplus}(P_1(j) = \left(1 \oplus el_1(x)Иel_2(x)\right)И\left(el_0(x)Иel_1(x)Иel_2(x) \oplus el_0(x)Иel_2(x)\right) =$$
$$= el_0(x)Иel_1(x)Иel_2(x) \oplus el_0(x)el_2(x),$$

$$\bigoplus_{j=0}^{i}[P_1(j)\Delta_{\oplus}(P_1(j))] = 1 \oplus el_1(x)Иel_2(x),$$

$$P_2(i) = 0.$$

Булева последовательность $Y(x)$ и СБП $Y(x)$ представлены в таблице.

Значения $el_0(x)$, $el_1(x)$, $el_2(x)$,СБП $Y(x)$, $P_0(x)$, $P_1(x)$

x	0	1	2	3	4	5	6	7
$el_0(x)$	1	0	1	0	1	0	1	0
$el_1(x)$	1	1	0	0	1	1	0	0
$el_2(x)$	1	1	1	1	0	0	0	0
$Y(x)$	0	1	1	1	0	0	0	0
СБП $Y(x)$	0	1	2	3	3	3	3	3
$P_0(x)$	0	1	0	1	1	1	1	1
$P_1(x)$	0	0	1	1	1	1	1	1

Таким образом, проведена систематизация способов аналитического представления любых СБП в канонической форме, позволяющая корректно формулировать СБП для минимизации, с учетом правил представления функций натурального аргумента посредством булевых функций для реализации на компьютере с классической архитектурой. Это открывает возможность поиска свойств конкретных СБП, применимых для факторизации, позволяющих получить их формы представления полиномиальной сложности либо доказать отсутствие таких свойств.

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, SIAM J. Comput. 26 (5): 1484 — 1509.
3. Рябинин, И.А. Надежность и безопасность структурно-сложных систем / И.А. Рябинин. — СПб.: Изд-во С.-Петерб. ун-та, 2007. — 276 с.

References

1. Yan, S.Y. Kriptoanaliz RSA [Cryptanalysis of RSA] / S.Y. Yan; per. s angl. Yu. Aydarova [transl. from English by Yu.Aydarov] — M.; Izhevsk: NIC Regulyarnaya i khaoticheskaya dinamika, Izhev. in-t komp'yuter. issled.[SRC Regular and Chaotic Dynamics, Izhev. Inst. comput. res.], 2011. — 312 p.
2. Shor, P.W. Polynomial-time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer, SIAM J. Comput. 26 (5): 1484 — 1509.

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

3. Ryabinin, I.A. Nadezhnost’ i bezopasnost’ strukturno-slozhnykh system [Reliability and Safety of Structurally-Complex Systems] / I.A. Ryabinin. — St.-Peterburg, 2007. — 276 p.

Рецензент д-р техн. наук, проф. Одес. нац. политехн. ун-та Дрозд А.В.

Поступила в редакцию 15 ноября 2011 г.