Ежегодная международная научно-практическая конференция
«РусКрипто’2024»

О сложности алгоритмов последовательного опробования (АПО)

Фомичёв Владимир Михайлович
д.ф.-м.н., профессор,
научный консультант, ООО «Код Безопасности»,
ведущий научный сотрудник, ФИЦ ИУ РАН.
e-mail: fomichev.2016@yandex.ru

КОД безопасности

Общая задача решения системы уравнений

Сложность общей задачи поиска *всех решений* системы m булевых уравнений от n неизвестных имеет порядок $m2^n$ опробований в худшем случае и 2^{n+1} в среднем, если вероятность выполнения любого уравнения на случайном наборе равна 1/2.

$$\{f_j(x_1, \dots, x_n) = a_j, j = 1, \dots, m\}, \qquad (1)$$

Существо АПО – групповая отбраковка

Обозначим $S(j)$ множество номеров существенных переменных $f_j(x_1, \dots, x_n), j = 1, \dots, m$. Если $\{1, \dots, j\} = S(j) \subset S(j+1) = \{1, \dots, j+1\}$, то при *m=n* треугольную систему (2) решим n-шаговым АПО.

$$
\begin{gathered}
f_1(x_1) = a_1, \\
f_2(x_1, x_2) = a_2, \\
\dots \\
f_{n-1}(x_1, x_2, \dots, x_{n-1}) = a_{n-1}, \\
f_n(x_1, x_2, \dots, x_n) = a_n.
\end{gathered}
\qquad (2)
$$

Для треугольных систем средняя сложность АПО достигает $2n$.

Основной результат доклада

Многие системы, где некоторые уравнения зависят не от всех переменных, можно приблизить к треугольной системе перестановкой уравнений, что снижает среднюю сложность АПО в естественной вероятностной модели вычислений.

Для системы (1) предложен алгоритм поиска наилучшей перестановки уравнений, учитывающий структуру множеств существенных переменных уравнений, оценена средняя сложность АПО.

Очередность уравнений при решении системы

Задача: решить систему (1) m-шаговым АПО, где в левой части каждая переменная существенная для некоторых функций и некоторые функции зависят не от всех переменных.

Перестановку $Q_m^m = (q_1, \dots, q_m)$ чисел $1, \dots, m$ назовем **маркером** алгоритма решения системы (1). Маркер Q_m^m однозначно определяет перестановку уравнений системы (1).

Обозначим: $Q_m^r = (q_1, \dots, q_r)$ - бесповторная упорядоченная выборка r чисел из $\{1, \dots, m\}$, $r = 1, \dots, m$;

$\{Q_m^r\} = \{q_1, \dots, q_r\}$ – множество элементов выборки Q_m^r.

Условия анализа сложности АПО

Для случайной системы (1) среднюю сложность АПО оценим числом опробований наборов переменных при подстановке в уравнения системы.

Условия оценки средней сложности:

1) случайный набор значений существенных переменных удовлетворяет любому уравнению с вероятностью ½;
2) разные наборы значений существенных переменных независимо удовлетворяют или не удовлетворяют любому уравнению;
3) любой набор значений переменных независимо удовлетворяет или не удовлетворяет разным уравнениям системы (1).

Характеристики АПО с маркером $(q_1, \dots, q_m)$

$S^{\langle m \rangle} = \{S(1), \dots, S(m)\}$ – частично упорядоченное множество (ч.у.м.) по отношению теоретико-множественного включения.

Обозначим при маркере $Q_m^m = (q_1, \dots, q_m)$:

$\Delta(Q_m^1) = S(q_1)$; $\Delta(Q_m^r) = S(q_r) \backslash \left(S(q_1) \cup \dots \cup S(q_{r-1})\right), r > 1$;

$n_r = |\Delta(Q_m^r)|, r = 1, \dots, m$; если $\Delta(Q_m^r) = \emptyset$, то $n_r = 0$;

T – средняя сложность а.п.о.;

T_r - среднее число операций на шаге r;

M_r – среднее число не отбракованных наборов переменных после шага r.

Алгоритм АПО с маркером $(q_1, \dots, q_m)$

1-й шаг. Опробуются все наборы значений n_1 переменных с номерами из $S(q_1)$, ложные наборы бракуются по уравнению с номером q_1.

r-й шаг, $r > 1$. Каждый не отсеянный на $(r-1)$-м шаге набор:

а) при $\Delta(Q_m^r) = \emptyset$ бракуется по уравнению с номером q_r;

б) при $\Delta(Q_m^r) \neq \emptyset$ пополняется 2^{n_r} наборами значений переменных с номерами из $\Delta(Q_m^r)$, и пополненные наборы значений переменных бракуются по уравнению с номером q_r.

$(x_1, \dots, x_n)$ - решение системы (1), если не отсеян на шаге m.

Средняя сложность АПО

При данных обозначениях:

$$\sum_{1\le r\le m} n_r = n; \qquad (3)$$

$$T_r = M_{r-1}2^{n_r};\ M_r = M_{r-1}2^{n_r-1},\ 1 \le r \le m, \text{ где } M_0 = 1.$$

По определению $T = \sum_{1\le r\le m} T_r$, тогда

$$T = \sum_{1\le r\le m} M_{r-1}2^{n_r}. \qquad (4)$$

Средняя сложность T зависит от разбиения числа n на $n_1, \dots, n_m$ и, следовательно, от маркера $(q_1, \dots, q_m)$.

Задача поиска оптимального маркера

Задача: для системы (1) найти маркер $(q_1, \dots, q_m)$ АПО, при котором средняя вычислительная сложность АПО наименьшая.

Такой маркер назовем оптимальным маркером (о.м.) для системы уравнений (1).

Комбинаторные свойства разбиений числа

Обозначим: R_n^m - множество разбиений числа n на m целых неотрицательных чисел; $\bar{n} = (n_1, \dots, n_m) \in R_n^m$, $\bar{n}' = (v_1, \dots, v_m) \in R_n^m$.

$\angle$ - лексикографический линейный порядок на R_n^m;

$\rho(\bar{n}, \bar{n}')$ - метрика на R_n^m: $\rho(\bar{n}, \bar{n}') = \sum_{1 \le i \le m} |n_i - v_i|$.

Разбиения $\bar{n}$ и $\bar{n}'$ назовем соседними, если $\rho(\bar{n}, \bar{n}') = 2$; для соседних разбиений $\{n_1 - v_1, \dots, n_m - v_m\}$ содержит одну «1», одну «-1» и «0».

Зададим бинарное отношение на R_n^m при $t > 1$: $\bar{n} \le \bar{n}' \Leftrightarrow$ имеется цепь $\left(\bar{n}^{(1)}, \dots, \bar{n}^{(t)}\right)$, где $\bar{n} = \bar{n}^{(1)}$, $\bar{n}' = \bar{n}^{(t)}$, $\bar{n}^{(j)}$ и $\bar{n}^{(j+1)}$ - соседние, и $\bar{n}^{(j)} \angle \bar{n}^{(j+1)}$, $j = 1, \dots, t-1$.

Теоремы и алгоритм поиска о.м.

Обозначим: MINX множество минимальных элементов ч.у.м. X.

Теорема 1. Если $\bar{n}(Q) \leq \bar{n}(Q')$ для маркеров Q и Q', то $T(Q) < T(Q')$.

Теорема 2. При о.м. $(q_1, \dots, q_m)$: $\bar{n} = (|S(q_1)|, n_2, \dots, n_m)$, $S(q_1) \in \mathrm{MIN}S^{\langle m \rangle}$.

Алгоритм поиска о.м.: 1. Находим q_1, где $S(q_1) \in \mathrm{MIN}S^{\langle m \rangle}$.

2. Для q_1 находим q_2, где $S(q_2) \in \mathrm{MIN}\left\{S^{\langle m \rangle} \backslash \{S(q_1)\}\right\}$ ...

$2 < r < m$. Для $(q_1, \dots, q_{r-1})$ находим q_r, где

$$S(q_r) \in \mathrm{MIN}\left\{S^{\langle m \rangle} \backslash (S(q_1) \cup \dots \cup S(q_{r-1}))\right\}.$$

m. Для $(q_1, \dots, q_{m-1})$ находим $q_m \neq q_1, \dots, q_{m-1}$.

Многозначность и сложность поиска о.м.

Сложность поиска о.м. тем ниже, чем меньше многозначность поиска минимального элемента ч.у.м. (см. решение треугольной системы, слайд 3).

Многозначность и сложность поиска о.м. снижается если:

1) на шаге $r > 1$ при $Q_m^{r-1} \neq Q_m^{r-1\prime}$ получены односоставные выборки $\{Q_m^r\} = \{Q_m^{r\prime}\}$ (отличаются лишь перестановкой);
2) в $S^{\langle m \rangle}$ содержатся одинаковые множества, т.е. $S(i) = S(j)$, $1 \leq i < j \leq m$.

Пример, m=n=5

Сложность решения полным перебором системы 5 уравнений от 5 переменных равна: в среднем 62; в худшем случае ≈ 160.

j	1	2	3	4	5
$S(j)$	{1,2}	{1,2,4}	{3,5}	{3,4,5}	{3,4,5}

№	маркер $(q_1, \dots, q_5)$	разбиение $\overline{5}$	T а.п.о.
1	(12345) ≅ (12354)	2+1+2+0+0	22
2	(13452) ≅ (13542)	2+2+1+0+0	26
3	(31245) ≅ (31254)	2+2+1+0+0	26
4	(31452) ≅ (31542)	2+2+1+0+0	26
5	(34512) ≅ (35412)	2+1+0+2+0	16

СПАСИБО
за
ВНИМАНИЕ!