ОБОЗРЕНИЕ
ПРИКЛАДНОЙ И ПРОМЫШЛЕННОЙ
Том 20 **МАТЕМАТИКИ** **Выпуск 2**
2013

В. О. Мironкин (Москва, ТВП). **Методы восстановления неизвестного подмножества при действии случайного отображения специального вида.**

Пусть $A = \{0,1\}^r$, $r \in \mathrm{N}$, и пусть на множестве A заданы равномерная мера $p(a_i) = 2^{-r}$, $i = 1, 2, \ldots, 2^r$, и число $\varepsilon \in \mathrm{N}$. Зафиксируем некоторый элемент $s \in A$. Положим $\Theta = \{x \in A\colon \|s \oplus x\| \leqslant \varepsilon\}$, где $\|s \oplus x\| = \sum_{j=1}^{r}(s_j \oplus x_j)$ есть расстояние между элементами s и x в метрике Хэмминга, $|\Theta| = k = k(\varepsilon) = \sum_{j=0}^{\varepsilon}\binom{r}{j}$.

З а м е ч а н и е. Множество Θ однозначно определяется своим центром s и параметром ε.

Пусть далее $B = V_q$, $q \in \mathrm{N}$, и элемент $b \in B$ фиксирован. Рассмотрим множество всех отображений $\mathfrak{I} = \{f\colon A \to B \,|\, f(\Theta) = b\}$. Зададим на $\mathfrak{I}$ равномерную меру. При каждой реализации f выбирается случайно. Задача состоит в восстановлении множества Θ при условии, что параметры A, B, ε известны и для любого $a \in A$ значение $f(a)$ легко вычислимо.

В работе, представленной данным докладом, предложены следующие методы восстановления неизвестного множества Θ, основанные на частичном опробовании: метод префиксного частичного опробования; метод усеченного разреженного опробования весовых групп.

Метод префиксного частичного опробования. Пусть $A_k = \{a \in A\colon \|a\| = k\}$, $k = 0, 1, \ldots, r$, $\Theta_k = A_k \cap \Theta$, положим $M = \max_{0\leqslant k\leqslant r}\{k \,|\, \Theta_k \neq \varnothing\}$ и $m = \min_{0\leqslant k\leqslant r}\{k \,|\, \Theta_k \neq \varnothing\}$. Положим C_l — множество двоичных векторов вида $(0, \ldots, 0, a_{l+1}, \ldots, a_r)$, где $a_i \in \{0,1\}$, $i = l+1, l+2, \ldots, r$, $l = 0, 1, \ldots, r-1$.

Предложение 1. *Для определения некоторого элемента множества Θ достаточно перебрать элементы множества C_ε.*

Следующие предложения устанавливают связь между строением центра s и способом опробования подвекторов. Обозначим $\oplus$ поразрядное сложение по модулю 2.

Предложение 2. *Пусть среди первых ε координат центра $s = (s_1, s_2, \ldots, s_r)$ множества Θ имеется k нулей, $0 \leqslant k \leqslant \varepsilon$, тогда множеству Θ будут принадлежать векторы из множества $\{(0, \ldots, 0, s_{\varepsilon+1}, \ldots, s_r) \oplus \beta \,|\, \beta \in C_\varepsilon,\ \|\beta\| \leqslant k\}$.*

Предложение 3. *Пусть среди первых ε координат центра $s = (s_1, s_2, \ldots, s_r)$ множества Θ имеется k нулей, $0 \leqslant k \leqslant \varepsilon$, тогда для определения вектора, принадлежащего множеству Θ, достаточно опробовать векторы из множества $C_{\varepsilon+k}$.*

В силу предложения 3, опробование векторов следует осуществлять в лексикографическом порядке.

Алгоритм 1

1. Опробуем последовательно векторы a из множества C_ε в лексикографическом порядке и l раз вычисляем значение $f(a)$. Если произошло событие $H = \{\text{при всех } l \text{ реализациях } f(a) = b\}$, то считаем, что вектор $a \in \Theta$, и переходим к шагу 2, в противном случае опробуем следующий вектор.

2. Если $\|a\| = \varepsilon$, то полагаем $u = (1, 1, \ldots, 1)$ и переходим к шагу 3. Если $\|a\| \geqslant 3\varepsilon$, то полагаем $u = (0, 0, \ldots, 0)$ и переходим к шагу 3.

3. Пусть множество различающихся координат элементов a и u есть $\{j_1, j_2, \ldots, j_k\}$. Изменяем последовательно значения этих координат у элемента a на противоположные до тех пор, пока не произойдет событие $\overline{H}$. Элемент a без учета последнего изменения обозначаем v. Если $\binom{r}{k} < \binom{r}{\varepsilon}^2$, где $k = \|v\|$, то переходим к шагу 4, в противном случае — к шагу 5.

4. Опробуем A_k, находим Θ_k. Если $u = (1, 1, \ldots, 1)$, то вычисляем $s = \&_{a\in\Theta_k} a$; если $u = (0, 0, \ldots, 0)$, то вычисляем $s = \vee_{a\in\Theta_k} a$. Завершаем алгоритм.

5. Для каждого элемента $a' \in A$: $\|a' \oplus a\| = \varepsilon$ проверяем условие: для всех $a'' \in A$: $\|a'' \oplus a'\| = \varepsilon$ произошло событие H. Элемент $a'' \in A$, для которого выполнилось соответствующее условие, есть центр Θ. Завершаем алгоритм.

Среднее значение трудоемкости алгоритма

$$T = \sum_{k=0}^{\varepsilon} \sum_{t=1}^{r-\varepsilon-k} T_{k,t} P(H_{k,t}) = 3^{\varepsilon-1}(2^{r-3\varepsilon-1} - 2^{-r-1}).$$

Вероятность успеха алгоритма асимптотически близка к 1.

Метод усеченного разреженного опробования весовых групп. Далее рассмотрим метод опробования элементов весовых групп, построенных из усеченных векторов множества C_ε. Зададим $D_{l,k}(t)$ $(t \in \{1, 2, \ldots, r-1\})$ — множество таких двоичных векторов вида $(a_1, a_2, \ldots, a_r)$, что $\|a_1, a_2, \ldots, a_t\| = l$, $\|a_{t+1}, \ldots, a_r\| = k$, $l + k \leqslant r$, где $a_i \in \{0, 1\}$, $1 \leqslant i \leqslant r$. В случае $t = \varepsilon$ положим по определению $D_{l,k} \equiv D_{l,k}(\varepsilon)$.

Пусть $1 \leqslant t \leqslant r-1$, $l + k \leqslant r$, тогда

$$|D_{l,k}(t)| = \binom{t}{l}\binom{r-t}{k}. \qquad (*)$$

Предложение 4. *Пусть $\varepsilon \leqslant k \leqslant r - \varepsilon$ и $D_{0,k} \cap \Theta = \varnothing$, тогда для центра s множества Θ справедливо соотношение $s \notin \bigcup_{i=0}^{\varepsilon} \bigcup_{j=-\varepsilon+i}^{\varepsilon-i} D_{i,k+j}$.*

Предложение 5. *Пусть для некоторого k, $\varepsilon \leqslant k \leqslant r - \varepsilon$, $D_{0,k} \cap \Theta = \varnothing$, $D_{\varepsilon,k-\varepsilon} \cap \Theta = \varnothing$ и $D_{0,k+2\varepsilon} \cap \Theta = \varnothing$, $D_{\varepsilon,k+\varepsilon} \cap \Theta = \varnothing$, тогда справедливо соотношение $\Theta \cap \bigcup_{l=k}^{k+2\varepsilon} A_l$.*

Таким образом, опробование очередных двух множеств усеченных векторов вида $D_{0,k+j\varepsilon} \cap \Theta = \varnothing$, $D_{\varepsilon,k+(j-1)\varepsilon} \cap \Theta = \varnothing$ позволяет исключить из алгоритма опробования 2ε весовых групп.

На основе полученного результата строится алгоритм разреженного усеченного опробования.

Алгоритм 2

1. Последовательно для каждого значения $k = \varepsilon, r - \varepsilon, 3\varepsilon, r - 3\varepsilon, \ldots, \varepsilon + 2\varepsilon([r/(4\varepsilon)] - 1), r - \varepsilon - 2\varepsilon([r/(4\varepsilon)] - 1), [r/2] - \varepsilon, [r/2] + \varepsilon$ опробуем множества векторов $D_{0,k}$, $D_{\varepsilon,k-\varepsilon}$ и l раз вычисляем значение $f(a)$. Если произошло событие $H = \{\text{при всех } l \text{ реализациях } f(a) = b\}$, то считаем, что вектор $a \in \Theta$ и переходим к шагу 2 в алгоритме 1, в противном случае опробуем следующий вектор.

2. Если $\|a\| = \varepsilon$, то полагаем $u = (1, 1, \ldots, 1)$ и переходим к шагу 3. Если $\|a\| \geqslant 3\varepsilon$, то полагаем $u = (0, 0, \ldots, 0)$ и переходим к шагу 3.

3. Пусть множество различающихся координат элементов a и u есть $\{j_1, j_2, \ldots, j_k\}$. Изменяем последовательно значения этих координат у элемента a на противоположные до тех пор, пока не произойдет событие $\overline{H}$. Элемент a без учета последнего изменения обозначаем через v. Если $\binom{r}{k} < \binom{r}{\varepsilon}^2$, где $k = \|v\|$, то переходим к шагу 4, в противном случае — к шагу 5.

4. Опробуем A_k, находим Θ_k. Если $u = (1, 1, \ldots, 1)$, то вычисляем $s = \&_{a\in\Theta_k} a$, если $u = (0, 0, \ldots, 0)$, то вычисляем $s = \vee_{a\in\Theta_k} a$. Завершаем алгоритм.

5. Для каждого элемента $a' \in A:\ \|a' \oplus a\| = \varepsilon$ проверяем условие: для всех $a'' \in A:\ \|a'' \oplus a'\| = \varepsilon$ произошло событие H. Элемент $a'' \in A$, для которого выполнилось соответствующее условие, есть центр Θ. Завершаем алгоритм.

Согласно $(*)$, трудоемкость алгоритма не превосходит величины $2l \sum_{k=0}^{2h+1} \binom{r-\varepsilon}{\varepsilon k}$. Вероятность успеха алгоритма также близка к 1.