ОБОЗРЕНИЕ
ПРИКЛАДНОЙ И ПРОМЫШЛЕННОЙ
Том 20 МАТЕМАТИКИ Выпуск 4
2013

В. О. Миронкин (Москва, ТВП). **О методе связного опробования элементов неизвестного подмножества при действии случайного отображения специального вида.**

Пусть $A = \{0,1\}^r$, $r \in \mathrm{N}$, и на множестве A задана равномерная мера $p(a) = 2^{-r}$, $\forall a \in A$.

Пусть задано $\varepsilon \in \mathrm{N}$. Зафиксируем некоторый элемент $s = (s_1, s_2, \ldots, s_r) \in A$ — центр множества Θ. Положим $\Theta = \Theta(\varepsilon) = \{x \in A\colon \ \|s \oplus x\| \leqslant \varepsilon\}$. Очевидно, $|\Theta| = \sum_{j=0}^{\varepsilon} \binom{r}{j}$.

Пусть далее $B = \{0,1\}^q$, $q \in \mathrm{N}$ и зафиксирован произвольный элемент $b \in B$. Рассмотрим множество всех отображений $\mathrm{Im} = \{f\colon \ A \to B | f(\Theta) = b\}$ и зададим на Im равномерную меру.

Рассмотрим задачу восстановления множества Θ при условии, что значение ε известно и для любого $a \in A$ значение $f(a)$ легко вычислить. При каждом вычислении значения $f(a)$ отображение f выбирается случайно $\forall a \in A$.

В работах [1, 2] было показано, что для восстановления множества Θ достаточно определить его произвольный элемент. В работе, представленной данным докладом, предлагается новый подход к восстановлению произвольного элемента множества Θ.

Метод связного опробования. Ранее в работе [2] автором рассматривался подход частичного опробования при восстановлении произвольного элемента множества Θ, заключающийся в опробовании усеченных векторов множества A. Напомним, что суть подхода частичного опробования заключается в опробовании элементов множества C_ε, где C_l — множество двоичных векторов вида $(0, \ldots, 0, a_{\varepsilon+1}, \ldots, a_r)$, $a_i \in \{0,1\}$, $0 \leqslant l < i \leqslant r$.

Действительно, в работе [2] показано, что если центр множества Θ имеет вид $s = (s_1, s_2, \ldots, s_r)$, то вектор вида $(0, \ldots, 0, s_{\varepsilon+1}, \ldots, s_r)$ будет заведомо лежать во множестве Θ.

Обозначим X_l множество двоичных векторов вида $(1, \ldots, 1, a_{l+1}, \ldots, a_r)$.

Определение. Будем говорить, что множества C_l и X_l *опробуются связным образом*, если для каждого элемента вида $(s_{l+1}, \ldots, s_r)$ одновременно опробуются элементы $(0, \ldots, 0, s_{l+1}, \ldots, s_r)$ и $(1, \ldots, 1, s_{l+1}, \ldots, s_r)$.

Предложение 1. *Для определения произвольного элемента множества Θ достаточно связным образом опробовать элементы множеств $C_{2\varepsilon+1}$ и $X_{2\varepsilon+1}$.*

Средняя трудоемкость такого опробования оценивается величиной $(2^{r-2\varepsilon-1} + 2^{r-2\varepsilon-1})/2 = 2^{r-2\varepsilon-1}$.

Замечание. Значение длины нулевого и единичного подвекторов, указанное в предложении 1, не может превышать $2\varepsilon + 1$.

О структуре множества Θ. В работе [2] изучались соотношения между центром множества Θ и множествами $D_{l,k}(t)$, $l + k \leqslant r$, $1 \leqslant t \leqslant r - 1$. Напомним, что $D_{l,k}(t)$ обозначалось множество таких двоичных векторов $(a_1, a_2, \ldots, a_r) \in A$, что $\|(a_1, a_2, \ldots, a_t)\| = l$, $\|(a_{t+1}, \ldots, a_r)\| = k$, $l + k \leqslant r$.

О п р е д е л е н и е. Обозначим $D_{m,l,k}(t_1,t_2)$, $t_1+t_2<r$, множество таких двоичных векторов $(a_1,a_2,\dots,a_r)\in A$, что $\|(a_1,a_2,\dots,a_{t_1})\|=m$, $\|(a_{t_1+1},\dots,a_{t_2})\|=l$, $\|(a_{t_2+1},\dots,a_r)\|=k$, $m+l+k\leqslant r$.

Согласно введенному определению, имеем $|D_{m,l,k}(t_1,t_2)|=\binom{t_1}{m}\binom{t_2}{l}\binom{r-t_1-t_2}{k}$, где $t_1+t_2<r$, $m+l+k\leqslant r$.

Для более компактной записи последующих результатов используем следующие обозначения: $p=\min\{\varepsilon,t_1\}$, $p_i=\min\{\varepsilon,i\}$, $q_i=\min\{\varepsilon-p_i,t_2\}$, $i=0,1,\dots,p$.

Предложение 2. *Пусть* $t_1+t_2<r$, $0\leqslant k\leqslant r-t_1-t_2$. *Тогда если* $\Theta\bigcap D_{0,0,k}(t_1,t_2)=\varnothing$, *то* $s\notin\bigcup_{i=0}^{p}\bigcup_{j=0}^{q_i}\bigcup_{l=k-\varepsilon+i+j}^{k+\varepsilon-i-j}D_{i,j,l}(t_1,t_2)$. *Если* $\Theta\bigcap D_{0,t_2,k}(t_1,t_2)=\varnothing$, *то* $s\notin\bigcup_{i=0}^{p}\bigcup_{j=t_2-q_i}^{t_2}\bigcup_{l=k-\varepsilon+t_2+i-j}^{k+\varepsilon-t_2-i+j}D_{i,j,l}(t_1,t_2)$.

Предложение 3. *Пусть* $t_1+t_2<r$, $0\leqslant k\leqslant r-t_1-t_2$. *Тогда если* $\Theta\bigcap D_{t_1,0,k}(t_1,t_2)=\varnothing$, *то* $s\notin\bigcup_{i=0}^{p}\bigcup_{j=0}^{q_i}\bigcup_{l=k-\varepsilon+i+j}^{k+\varepsilon-i-j}D_{t_1-i,j,l}(t_1,t_2)$. *Если* $\Theta\bigcap D_{t_1,t_2,k}(t_1,t_2)=\varnothing$, *то* $s\notin\bigcup_{i=0}^{p}\bigcup_{j=t_2-q_i}^{t_2}\bigcup_{l=k-\varepsilon+t_2+i-j}^{k+\varepsilon-t_2-i+j}D_{t_1-i,j,l}(t_1,t_2)$.

Следствие 1. *Пусть* $2\varepsilon+1<r$, $0\leqslant k\leqslant r-2\varepsilon-1$. *Тогда если* $\Theta\bigcap D_{0,0,k}(\varepsilon+1,\varepsilon)=\varnothing$, *то* $s\notin\bigcup_{i=0}^{\varepsilon}\bigcup_{j=0}^{\varepsilon-i}\bigcup_{l=k-\varepsilon+i+j}^{k+\varepsilon-i-j}D_{i,j,l}(\varepsilon+1,\varepsilon)$. *Если* $\Theta\bigcap D_{0,\varepsilon,k}(\varepsilon+1,\varepsilon)=\varnothing$, *то* $s\notin\bigcup_{i=0}^{\varepsilon}\bigcup_{j=i}^{\varepsilon}\bigcup_{l=k+i-j}^{k-i+j}D_{i,j,l}(\varepsilon+1,\varepsilon)$.

Следствие 2. *Пусть* $2\varepsilon+1<r$, $0\leqslant k\leqslant r-2\varepsilon-1$. *Тогда если* $\Theta\bigcap D_{\varepsilon+1,0,k}(\varepsilon+1,\varepsilon)=\varnothing$, *то* $s\notin\bigcup_{i=0}^{\varepsilon}\bigcup_{j=0}^{\varepsilon-i}\bigcup_{l=k-\varepsilon+i+j}^{k+\varepsilon-i-j}D_{\varepsilon-i,j,l}(\varepsilon+1,\varepsilon)$. *Если* $\Theta\bigcap D_{\varepsilon+1,\varepsilon,k}(\varepsilon+1,\varepsilon)=\varnothing$, *то* $s\notin\bigcup_{i=0}^{\varepsilon}\bigcup_{j=i}^{\varepsilon}\bigcup_{l=k+i-j}^{k-i+j}D_{\varepsilon-i,j,l}(\varepsilon+1,\varepsilon)$.

Предложение 4. *Пусть* $2\varepsilon+1<r$, $\varepsilon\leqslant k\leqslant r-2\varepsilon-1$. *Тогда если* $\Theta\bigcap D_{0,0,k}(varepsilon+1,\varepsilon)=\varnothing$ *и* $\Theta\bigcap D_{0,\varepsilon,k-\varepsilon}(\varepsilon+1,\varepsilon)=\varnothing$, *то* $s\notin\bigcup_{i=k-\varepsilon}^{k+\varepsilon}D_{0,i}(\varepsilon+1)$. *Если* $\Theta\bigcap D_{\varepsilon+1,0,k}(\varepsilon+1,\varepsilon)=\varnothing$ *и* $\Theta\bigcap D_{\varepsilon+1,\varepsilon,k-\varepsilon}(\varepsilon+1,\varepsilon)=\varnothing$, *то* $s\notin\bigcup_{i=k-\varepsilon}^{k+\varepsilon}D_{\varepsilon+1,i}(\varepsilon+1)$.

Определение центра множества Θ. Напомним понятие весовой группы $A_k=\{a\in A\colon\ \|a\|=k\}$, $k=0,1,\dots,r$, введенное в работе [1].

В работе [2] были предложены алгоритмы, позволяющие определить центр s множества Θ в случае, когда известен произвольный элемент $a\in\Theta_m\bigcup\Theta_M$, где, $\Theta_k=A_k\bigcap\Theta$, $k=0,1,\dots,r$. Рассмотрим вопрос определения центра s множества Θ в случае, когда известный элемент $a\notin\Theta_m\bigcup\Theta_M$.

Приведем предложение из работы [1], описывающее распределение числа элементов множества Θ в зависимости от веса центра s.

Предложение 5. *Пусть* $\varepsilon\leqslant r/2$, $s\in A$ *и* $\|s\|=k$, $k\in\{0,1\dots,r\}$. *Тогда для любого* j, $0\leqslant j\leqslant\varepsilon$

$$\left|A_{k+j}\bigcap\Theta\right|=\sum_{t=0}^{[(\varepsilon-j)/2]}\binom{r-k}{j+t}\binom{k}{t},\quad \left|A_{k-j}\bigcap\Theta\right|=\sum_{t=0}^{[(\varepsilon-j)/2]}\binom{k}{j+t}\binom{r-k}{t}.$$

Предположим, что при опробовании весовой группы $A_k=\{a\in A\colon\ \|a\|=k\}$, $k=0,1,\dots,r$, справедливо соотношение $|A_k\bigcap\Theta|=m$, $m\in\mathrm{N}$. Тогда согласно предложению 5 можно записать две системы уравнений относительно переменных (i,j), $0\leqslant i\leqslant r$, $0\leqslant j\leqslant\varepsilon$:

$$\left\{\begin{array}{c}\displaystyle\sum_{t=0}^{[(\varepsilon-j)/2]}\binom{r-i}{j+t}\binom{i}{t}=m,\\ k=i+j,\end{array}\right.\quad\Leftrightarrow\quad\left\{\begin{array}{c}\displaystyle\sum_{t=0}^{[(\varepsilon-j)/2]}\binom{r+j-k}{j+t}\binom{k-j}{t}=m,\\ i=k-j,\end{array}\right.\tag{1}$$

$$\left\{\begin{array}{c}\displaystyle\sum_{t=0}^{[(\varepsilon-j)/2]}\binom{i}{j+t}\binom{r-t}{t}=m,\\ k=i-j,\end{array}\right.\quad\Leftrightarrow\quad\left\{\begin{array}{c}\displaystyle\sum_{t=0}^{[(\varepsilon-j)/2]}\binom{j+k}{j+t}\binom{r-j-k}{t}=m,\\ i=j+k.\end{array}\right.\tag{2}$$

Для полученного решения (i,j) системы (1) или (2) возможны два случая. Если $i-\varepsilon\geqslant 0$, то опробуем элементы весовой группы $A_{i-\varepsilon}$ и находим множество $\Theta_{i-\varepsilon}$.

Тогда $s = \bigvee_{a \in \Theta_{i-\varepsilon}} a$. Если же $i - \varepsilon < 0$, то опробуем элементы весовой группы $A_{i+\varepsilon}$ и находим множество $\Theta_{i+\varepsilon}$. Тогда $s = \&_{a \in \Theta_{i+\varepsilon}} a$.

СПИСОК ЛИТЕРАТУРЫ

1. *Миронкин В. О.* Восстановление подмножества области определения при отображении специального вида. — Обозрение прикл. и промышл. матем., 2012, т. 19, в. 3, с. 413–415.
2. *Миронкин В. О.* Методы восстановления неизвестного подмножества при действии случайного отображения специального вида. — Обозрение прикл. и промышл. математем., 2013, т. 20, в. 2, с. 144–146.