ОБОЗРЕНИЕ
ПРИКЛАДНОЙ И ПРОМЫШЛЕННОЙ
Том 19 МАТЕМАТИКИ Выпуск 3
2012

В. О. Миронкин (Москва, ТВП). **Восстановление подмножества области определения при отображении специального вида.**

Пусть $A = \{0,1\}^r$, $r \in \mathbf{N}$, и на множестве A задана равномерная мера $p(a_i) = 2^{-r}$, $i = 1, 2, \ldots, 2^r$.

Пусть задано $\varepsilon \in \mathbf{N}$. 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 $B = V_q$, $q \in \mathbf{N}$, элемент $b \in B$ фиксирован. Рассмотрим множество всех отображений $\mathcal{T} = \{f \colon A \to B \,|\, f(\Theta) = b\}$. Зададим на $\mathcal{T}$ равномерную меру. При каждой реализации f выбирается случайно. Задача состоит в восстановлении множества Θ при условии, что параметр ε известен и для любого $a \in A$ можно вычислить значение $f(a)$.

Рассмотрим метод разреженного опробования весовых групп, в котором определяется некоторый элемент множества Θ, после чего определяются все элементы минимального или максимального веса и на основе них вычисляется центр множества Θ.

Следующее предложение показывает, как связан центр s с элементами минимального и максимального веса множества Θ.

Обозначим $A_k = \{a \in A \colon \|a\| = k\}$, $k = 0, 1, \ldots, r$, $\Theta_k = A_k \cap \Theta$. Пусть $M = \max_{0 \leqslant k \leqslant r}\{k \,|\, \Theta_k \neq \varnothing\}$, $m = \min_{0 \leqslant k \leqslant r}\{k \,|\, \Theta_k \neq \varnothing\}$. Обозначим $\vee, \&$ поразрядные дизъюнкцию и конъюнкцию.

Предложение 1. *Пусть* $m > 0$, *тогда* $s = \vee_{a \in \Theta_m} a$; *пусть* $M < r$, *тогда* $s = \&_{a \in \Theta_M} a$.

Следующее предложение позволяет определить элемент из Θ минимального или максимального веса не более, чем за ε опробований, если известен произвольный элемент из множества Θ и произвольный элемент из дополнения $A \backslash \Theta$.

О п р е д е л е н и е. Пусть $u, v \in A$ и $\{j_1, j_2, \ldots, j_k\}$ — множество различающихся координат элементов u и v, $k \leqslant r$. Тогда *путем* $\overline{u,v}$ длины k из u в v назовем некоторую последовательность $(\alpha_1, \alpha_2, \ldots, \alpha_k)$, $\alpha_i \in A$, где $\alpha_1 = u$, $\alpha_k = v$ и $\alpha_1, \alpha_2, \ldots, \alpha_k$ попарно различны и α_i, α_{i+1}, $i = 1, 2, \ldots, k-1$, отличаются ровно в одной из координат $\{j_1, j_2, \ldots, j_k\}$.

Предложение 2. *Пусть* $u \in \Theta$, $v \notin \Theta$ *и* $\overline{u,v} = (\alpha_1, \alpha_2, \ldots, \alpha_k)$ *— некоторый путь длины* k *из* u *в* v, $k \leqslant r$. *Пусть далее* α_i *— первый элемент пути, удовлетворяющий условию* $\alpha_i \notin \Theta$, $i = 2, 3, \ldots, k$. *Тогда элемент* α_{i-1} *лежит на границе множества* Θ, *т. е.* $\|\alpha_{i-1} \oplus s\| = \varepsilon$.

Следующий **алгоритм** использует предложения 1 и 2.

1. Последовательно для каждого $k = \varepsilon, r - \varepsilon, 3\varepsilon, r - 3\varepsilon, \ldots, \varepsilon + 2\varepsilon([[r/2]/(2\varepsilon)] - 1), r - \varepsilon - 2\varepsilon([r/2]/(2\varepsilon)] - 1), [r/2] - \varepsilon, [r/2] + \varepsilon$ опробуем все элементы весовой группы

A_k. Если для некоторого $a \in A_k$ и некоторого фиксированного l произошло событие

$$H = \{\text{при всех } l \text{ реализациях } f(a) = b\},$$

то считаем, что $a \in \Theta$, и переходим к шагу 2, в противном случае переходим к следующему значению k.

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

3. Пусть множество различающихся координат элементов a и u равно $\{j_1, j_2, \dots, j_k\}$. 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 и переходим к шагу 4.

4. Опробуем A_k и находим Θ_k, где $k = \|v\|$. Если $u = (1, 1, \dots, 1)$, то вычисляем $s = \&_{a \in \Theta_k} a$, если $u = (0, 0, \dots, 0)$, то вычисляем $s = \vee_{a \in \Theta_k} a$. Алгоритм завершает работу.

Следующее предложение показывает, как распределены элементы множества Θ по весовым группам в зависимости от веса s.

Предложение 3. *Пусть* $\varepsilon \leqslant r$, $s \in A = V_r$ *и* $\|s\| = k$, $k = \varepsilon, \varepsilon + 1, \dots, r - \varepsilon$. *Тогда для любого* $j = 0, 1, \dots, \varepsilon$

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

Согласно предложению 3, для трудоемкости метода справедлива оценка

$$Q \leqslant 2l \sum_{k=0}^{[r/2]-\varepsilon-1} \binom{r}{k} + l\binom{r}{[r/2]-\varepsilon}.$$

Для вероятности успеха по наихудшему случаю имеем

$$\pi \geqslant \prod_{i=1}^{t} (1 - \mathbf{P}\{H_i | a_i \notin \Theta\}) = (1 - 2^{-ql})^t \to 1 \text{ при } l \to \infty,$$

где

$$t = 2 \sum_{k=0}^{[r/2]-\varepsilon-1} \binom{r}{k} + \binom{r}{[r/2]-\varepsilon} - \binom{[r/2]}{\varepsilon}.$$