

В. А. А р б у з о в (Москва, ЗАО «Закрытые технологии»). **Вероятностный метод определения принадлежности двоичного вектора к подмножеству двоичных векторов.**

Рассмотрим произвольное непустое подмножество $M = \{\mathbf{v}_i\}$ векторов из пространства $\mathbf{V}_n$ двоичных векторов размерности n . Мощность подмножества M равна N , $|M| = N$. Зададим натуральное число k , $k \ll N$.

Для определения принадлежности произвольного двоичного вектора $\mathbf{v}$ к подмножеству M предлагается использовать следующий метод.

На первом этапе выбирается способ построения отображения $F : \mathbf{V}_n \longrightarrow \mathbf{V}_{N+k}$ из пространства векторов $\mathbf{V}_n$ в пространство векторов большей размерности $\mathbf{V}_{N+k}$:

Преобразование F подбирается таким образом, чтобы максимизировать ранг матрицы $F(M)$, где i -я строка матрицы $F(M)$ равна $F(\mathbf{v}_i)$.

На втором этапе определяется r — ранг матрицы $F(M)$, и матрица $F(M)$ произвольно дополняется до матрицы A_{N+k} полного ранга произвольными строками-векторами из множества V_{N+k} : $\mathbf{u}_1, \mathbf{u}_2, \dots, \mathbf{u}_k, \dots, \mathbf{u}_{k+N-r}$.

На третьем этапе решается k систем линейных уравнений $A_{N+k} \mathbf{Y} = \mathbf{X}_i$, $1 \leq i \leq k$, для правых частей следующего вида:

$$\begin{cases} X_{i,j} = 0, & \text{если } 1 \leq j < r \text{ или } (r < j \text{ и } j \neq i), \\ X_{i,j} = 1, & \text{если } r < j \leq N+k \text{ и } j = i. \end{cases}$$

На четвертом этапе полученные k решений $\{\mathbf{Y}_1, \dots, \mathbf{Y}_k\}$ систем линейных уравнений используются для определения принадлежности произвольного двоичного вектора $\mathbf{v}$ к подмножеству M .

Утверждение. Если при случайном равновероятном векторе $\mathbf{v}$ из пространства $\mathbf{V}_n$ хотя бы одно из скалярных произведений $(\mathbf{Y}_i, F(\mathbf{v}))$, $i = 1, 2, \dots, k$, в поле $\mathbf{GF}(2)$ не равно нулю, то вектор $\mathbf{v}$ не принадлежит множеству M с вероятностью не менее $p = 1 - 2^{-k}$.

Реализация данного метода с использованием программируемой логики имеет регулярную структуру, которая не зависит от векторов подмножества M .