ОБОЗРЕНИЕ
ПРИКЛАДНОЙ И ПРОМЫШЛЕННОЙ
Том 19 МАТЕМАТИКИ Выпуск 3
2012

Н. В. Бессуднова, В. В. Мкртичян (Ростов-на-Дону, ФГНУ НИИ «Спецвузавтоматика»). **О вычислении размерности q-ичного кода Рида–Маллера.**

Помехоустойчивые q-ичные коды Рида–Маллера, являющиеся, в частности, обобщением двоичных кодов Рида–Маллера и кодов Рида–Соломона, активно исследуются и применяются в задачах теории помехоустойчивого кодирования и криптографии (см., например, [1–3]). Для них строятся перспективные декодеры, в частности, списочные (см., например, [1] и [2]). С точки зрения теории помехоустойчивого кодирования, интерес представляет задача вычисления размерности q-ичного кода Рида–Маллера.

Рассмотрим $\mathbf{F}_q[X_1, X_2, \ldots, X_m]$ – кольцо полиномов от m переменных над полем Галуа $\mathbf{F}_q$. Пусть $n = q^m$, $P_0, P_1, \ldots, P_{n-1}$ — упорядоченное множество точек векторного пространства $\mathbf{F}_q^m$. Введем в рассмотрение q-ичный код Рида–Маллера с натуральными параметрами m и u вида

$$\mathrm{RM}_q(u, m) = \{(f(P_0)), (f(P_1)), \ldots, f(P_{n-1}) \,|\, f \in \mathbf{F}_q[X_1, X_2, \ldots, X_m],\ \deg(f) \leqslant u\},$$

где $u \leqslant m(q-1)$ [3].

Теорема. *Размерность кода* $\mathrm{RM}_q(u, m)$ *вычисляется по формуле*

$$k = \sum_{i=0}^{u} \sum_{j=0}^{\lfloor i/q \rfloor} (-1)^j C_m^j \, C_{i-jq+m-1}^{m-1}.$$

Доказательство теоремы основано на теории полей Галуа, комбинаторике и результатах работ [2] и [3]. Рассматривается матричный и полиномиальный способ задания кода $\mathrm{RM}_q(u, m)$ и устанавливается взаимно-однозначное соответствие между этими способами. Наряду с понятием степени многочлена рассматривается понятие приведенной степени многочлена для фиксированного поля Галуа $\mathbf{F}_q$. Размерность блока кодовой матрицы кода $\mathrm{RM}_q(u, m)$ рассчитывается как количество мономов, у которых степень фиксирована и совпадает с приведенной степенью. Размерность кода $\mathrm{RM}_q(u, m)$ рассчитывается как сумма размерностей блоков кодовой матрицы. Таким образом, получена формула для вычисления размерности q-ичного кода Рида–Маллера $\mathrm{RM}_q(u, m)$. (Доказательство теоремы публикуется отдельно.)

СПИСОК ЛИТЕРАТУРЫ

1. *Думер И. И.*, *Кабатянский Г. А.*, *Тавернье С.* Списочное декодирование двоичных кодов Рида–Маллера первого порядка. — Проблемы передачи информации, 2007, т. 43, № 3, с. 66–74.

2. *Pellikaan R.*, *Wu X.-W.* List Decoding of q-ary Reed–Muller Codes. — IEEE Trans. Inform. Theory, 2004, v. 50, № 4, p. 679–682.
3. *Евпак С. А.*, *Мкртичян В. В.* Исследование возможности применения q-ичных кодов Рида–Маллера в схемах специального широковещательного шифрования. — Изв. ВУЗов. Северо-Кавказский регион. Естественные науки, 2011, № 5, с. 5–15.