УДК 512 624: 003.26

О вычислении минимального расстояния квадратично-вычетных кодов

Королёва М. Н. (БНТУ), Липницкий В. А. (ВА РБ)
Белорусский национальный технический университет

Квадратично-вычетные коды (КВ-коды) весьма перспективны для практических приложений, т.к. имеют большое минимальное расстояние. Теория КВ-кодов, их задание и обработка, строятся на полиномиальном языке. Помехоустойчивое кодирование опирается на теорию конечных полей. Покажем влияние этой теории на исследование и обработку КВ-кодов. Рассмотрим один из формально существующих четырех классов взаимосвязанных двоичных КВ-кодов. **Предложение.** Всякий двоичный КВ-код $C_{q(x)}$ имеет простую длину $n = p = 8k \pm 1$, определен над полем $GF(2^m)$ минимальным расширением поля $Z/2Z$, содержащим все корни p-й степени из 1, является обобщённым БЧХ-кодом, то есть линейным кодом с проверочной матрицей $H = [\beta^i, \beta^{li}, ..., \beta^{si}]^T$ и с конструктивным расстоянием $\delta = 2t+1$, где $(p-1)/2 = mt$ и t натуральных чисел 1, l,… ,s лежат в различных циклотомических классах по модулю p, определяющих всё многообразие квадратичных вычетов; $q(x) = \prod_{i \in Q}(x - \beta^i)$; β - примитивный корень p-ой степени из 1 в поле $GF(2^m)$; Q - циклическая подгруппа квадратов (квадратичных вычетов по модулю p) мультипликативной группы $GF(p)^*$ порядка $(p-1)/2$, она содержит и 1 и 2 и группу $<2>$ порождённую классом вычетов 2. Минимальное расстояние *d* КВ-кода $C_{q(x)}$ длиной *p* удовлетворяет неравенству: $d \geq \sqrt{p}$. Определение точного значения минимального расстояния КВ-кодов остаётся сложной задачей, не имеющей до настоящего времени полного и точного решения. С XX века сохранился подход, предполагающий переход к расширенному КВ-коду. Расширение получается дополнением проверкой на чётность. Это увеличивает длину кода и его минимальное расстояние на 1, а группу автоморфизмов кода – до группы дробно-линейных преобразований. Тщательные расчеты с этой дробно-линейной группой, изучение её силовских подгрупп позволяют найти точное значение минимального расстояния расширенного КВ-кода. Данное предложение открывает путь к прямым синдромным методам определения минимального расстояния КВ-кодов.