В. Н. Думачев (Воронеж, ВИ МВД России)**. О коррекции ошибок в** $\mathrm{GF}(2^m)$**.**

В работе, представленной данным докладом, предлагается алгоритм построения совершенного недвоичного кода $[n,k] = [2^m+1, 2^m-1]$ над полем Галуа $\mathrm{GF}(2^m)$. Этап кодирования не отличается от алгоритма построния циклического кода. Представим информационную последовательность $a = (a_1, a_2, \ldots, a_k)$ в виде полинома $u(x) = \sum_{i=1}^{k} a_i x^{k-i}$. Сдвинем информационную последовательность на $r = 2$ разряда влево, для этого умножим информационный полином $u(x)$ на x^r: $m(x) = x^r u(x)$, и запишем его в виде $m(x) = C(x)\, g(x) + R(x)$, где $g(x) = x^r + \sum_{i=0}^{r-1} b_i x^i$ есть порождающий полином. Искомым кодом является прямая конкатенация коэффициентов информационного полинома $u(x)$ и полинома остатков $R(x)$: $F = (a||e)$, где $e_1 = (c\, a)$ и $e_2 = (d\, a)$.

Допустим, что принятая кодовая комбинация $\overline{F}(x)$ имеет 1 ошибку. Для декодирования совершенного кода необходимо иметь дополнительно таблицу локализации, определяемую лидером смежного класса по величине ошибки. Для ее построения вычислим новые значения проверочных разрядов $\overline{e}_1, \overline{e}_2$ для $\overline{F}(x)$. По коэффициентам проверочных разрядов построим вектор локаторов ошибки. Для этого введем полиномы локаторов λ и нормированные полиномы локаторов ошибки $\widehat{\lambda}$: $\lambda_k = c_k x + d_k$, $\widehat{\lambda}_k = x + c_k^{-1} d_k = x + \Lambda_k$. Вектор локаторов ошибки обозначим $\Lambda_k = c_k^{-1} d_k$. С другой стороны, складывая старые и новые проверочные разряды $\binom{\Delta e_1}{\Delta e_2} = \binom{e_1}{e_2} + \binom{\overline{e}_1}{\overline{e}_2}$, получим полиномы локаторов μ и нормированные полиномы локаторов ошибки $\widehat{\mu}$: $\mu = \Delta e_1 x + \Delta e_2$, $\widehat{\mu} = x + (\Delta e_1)^{-1} \Delta e_2 = x + \Lambda$, и по таблице вектора локаторов находим Λ_k, т. е. локализуем ошибку, которая находится в символе a_k. Теперь для символа a_k выписываем локатор единичной ошибки $\lambda = c_k x + d_k$ и, сравнивая с $\mu = \Delta e_1 x + \Delta e_2$, заметим, что $\mu = \mathbf{E}\,\lambda$, т. е. величина ошибки $\mathbf{E}$ вычисляется по формулам $\Delta e_1 = \mathbf{E}\, c_k$, $\Delta e_2 = \mathbf{E}\, d_k$, или $\mathbf{E} = c_k^{-1} \Delta e_1 = d_k^{-1}\, \Delta e_2$. Складывая побитно $a_k + \mathbf{E}$, получаем исправленную кодовую комбинацию и восстанавливаем информационную последовательность. В докладе приведены таблицы коэффициентов проверочных символов c_i, d_i и локаторов Λ_i кода для $\mathrm{GF}(2^2)$, $\mathrm{GF}(2^3)$, $\mathrm{GF}(2^4)$.

В заключение заметим, что если ошибка произошла в проверочном символе e_1, то полином локаторов будет иметь вид $\mu = \mathrm{const}\, x$, а если ошибка произошла в проверочном символе e_2, то полином локаторов имеет вид $\mu = \mathrm{const}$. В любом из этих случаев нам должно быть совершенно безразлично значение ошибки, поскольку информационные символы остались без искажения.