# НОРМЕННЫЙ МЕТОД РЕШЕНИЯ УРАВНЕНИЙ В ПОЛЯХ ГАЛУА

**В.А. Липницкий** [1], **И.В. Иванейчик** [2]

[1] БГУИР, Бровки 6, 220013, Минск, Беларусь
valipnitski@yandex.ru

[2] Белгосуниверситет, механико-математический факультет, Независимости 4, 220050 Минск, Беларусь
ivan-chik@yandex.ru

К разряду важнейших проблем компьютерной математики относится проблема разработки эффективных алгоритмов решения уравнений в полях Галуа характеристики 2. Актуальность ее мотивирована широкими применениями в цифровой обработке сигналов, помехоустойчивом кодировании, защите информации, атомной физике и т. д. Здесь даже для простейшего случая квадратных уравнений стандартные формулы не работают, поскольку деление на 2 невозможно. Интенсивный штурм данной проблемы во второй половине XX-го века привел к неутешительному результату — применению переборных методов типа процедуры Чэня [1]. В помехоустойчивом кодировании разработана теория норм синдромов [2, 3], которая позволяет обойти трудно реализуемую аппаратно процедуру решения уравнений. В дальнейшем выяснилось, что норменный метод можно применить и для решения

алгебраических уравнений над полями Галуа $GF(2^m)$. Практическая реализация этого метода решения уравнений требует применения средств компьютерной математики — пакета *MATHEMATICA* или ему подобных пакетов.

Пусть $x^t+b_1x^{t-1}+\ldots+b_{t-1}x+b_t=0$ — произвольное уравнение степени $t>1$ над полем $GF(2^m)$. Можно считать, что его корни однократные и не равны нулю, так как известны несложные процедуры сведения уравнения к такому виду. Корни $x_1, x_2, \ldots, x_t$ данного уравнения являются локаторами $t$-кратной ошибки $\bar{e}$ в примитивном БЧХ-коде с проверочной матрицей $H=(\alpha^i, \alpha^{3i}, \ldots, \alpha^{(2t-1)i})^T$, где $\alpha$ — примитивный элемент поля Галуа $GF(2^m)$. С математической точки зрения кодек БЧХ-кода для определения ошибочной составляющей $\bar{e}$ принятого сообщения $\bar{x}=\bar{c}+\bar{e}$ ($\bar{c}$ — истинное сообщение) решает систему уравнений:

$$\begin{cases} x_1+x_2+\ldots+x_t=s_1, \\ x_1^3+x_2^3+\ldots+x_t^3=s_2, \\ \ldots \\ x_1^{2t-1}+x_2^{2t-1}+\ldots+x_t^{2t-1}=s_t. \end{cases}$$

Теорема Виета связывает коэффициенты уравнения с элементарными симметрическими полиномами от его корней $b_i=\sigma_i(x_1,\ldots,x_t)$, а формулы Ньютона [4] устанавливают взаимно однозначное соответствие между элементарными и степенными симметрическими многочленами, то есть позволяют вычислить синдром $S(\bar{e})=(s_1,\ldots,s_t)$, а затем и норму синдрома $\bar{N}(S(\bar{e}))$ по формулам из [2, 3]. Декодируемые ошибки весом $t$ по теории норм синдромов группируются в $\Gamma$-орбиты $\langle\bar{e}_i\rangle$ относительно группы $\Gamma$ циклических сдвигов координат векторов $\bar{e}_i$. Норма синдрома $\bar{N}(S(\bar{e}))$ инвариантна на каждой $\Gamma$-орбите. Составим список $\Pi$ норм $\bar{N}(S(\bar{e}_i))$ всех $\Gamma$-орбит $\langle\bar{e}_i\rangle$ ошибок весом $t$. Вычисленная норма $\bar{N}(S(\bar{e}))$ сравнивается с этим списком. Если $\bar{N}(S(\bar{e}))=\bar{N}_j\in\Pi$, то вектор-ошибка $\bar{e}$ является циклическим сдвигом вектора $\bar{e}_j$ и легко находится. Координаты $\bar{e}$ однозначно указывают на элементы первой строки матрицы $H$ — корни решаемого уравнения.

**Литература**

1. *Мак-Вильямс Ф.Ж., Слоэн Н.ДЖ.А.* Теория кодов, исправляющих ошибки. М.. Связь, 1979. 744 с.

2. *Конопелько В.К., Липницкий В.А.* Теория норм синдромов и перестановочное декодирование помехоустойчивых кодов Мн.: БГУИР, 2000. 242 с.; 2-е издание· М.УРСС, 2004 176 с

3. *Липницкий В.А., Конопелько В К.* Норменное декодирование помехоустойчивых кодов и алгебраические уравнения. Мн.. "Издательский центр БГУ", 2007 240 с.

4. *Курош А.Г.* Курс высшей алгебры. Изд. 9-е М. Наука, 1968. 432 с.