ПОШУК КОРЕНІВ ПОЛІНОМУ ЛОКАТОРІВ ПОМИЛОК БЧХ КОДІВ

Крилова В. А., Котко Р. О.
Національний технічний університет «Харківський політехнічний інститут», м. Харків

Найбільш трудомістким розрахунком процедури декодування БЧХ кодів є процедура Ченя, яка виконується за допомогою арифметики кінцевих полів Галуа та залежить від кількості операцій добутку та множення. Тому питання у розробці швидкісних алгоритмів пошуку коренів полінома локаторів помилок, які б забезпечували мінімальне число арифметичних операцій в полях Галуа, є актуальним.

Розв'язання задачі пошуку коренів полінома локаторів помилок, коефіцієнти якого належать кінцевому полю $GF(2^m)$, використовуючи алгоритм Берлекемпа базується на спеціальному класі багаточленів. Ці многочлени, коріння яких може бути знайдено значно простіше, називаються *p*-многочленами. Якщо розмістити (упорядкувати) елементи кінцевого поля $GF(2^m)$ в такий спосіб, щоб сусідні вектора розрізнялися у однієї позиції. Тоді на кожному кроці алгоритму пошуку коренів багаточлена локаторів помилок, обчислення зводяться до одного додавання – попереднього значення та значення *p*-многочлена в точках стандартного базису $F(\alpha^0)\ F(\alpha^1)\ \ldots..\ F(\alpha^{m-1})$ кінцевого поля $GF(2^m)$. Таким чином, для того щоб обчислити всі значення полінома локаторів помилок, представлений як афінний многочлен

$$\sigma(x) = F(x) + \sigma_0, \quad \sigma_0 \in GF(2^m) \tag{1}$$

у всіх точках кінцевого поля необхідно виконати

$$F(\beta^i) = F(\beta^{i-1}) + F_j(\alpha^j) \tag{2}$$

де $\alpha^j = \beta^i \oplus \beta^{i-1}$ – відповідає одному з базисних елементів поля $GF(2^m)$.

Вираз (2) задає процедуру знаходження набору значень багаточлена $\sigma(x)$ у всіх точках $\alpha^i \in GF(2^m)$. Обчислення вимагає впорядкування всіх елементів поля, наявність попереднього значення $F(\beta^{i-1})$ та заздалегідь знайдених значень базисних векторів $L(\alpha^i)$. Для оцінки реальної ефективності запропонованого модифікованого алгоритму обчислення коренів багаточлена локаторів помилок було реалізовано програмне моделювання мовою C++. Розрахунок в кінцевих полях $GF(2^8)$ для методу Ченя було здійснено за допомогою таблиць логарифмів та антилогарифмів. Обчислення коренів та порівняння результатів виконувались тільки для *p*-многочленів помилок та для елементів поля α^0, α^1, …, α^{254}. Застосування модифікованого алгоритму для пошуку коренів поліномів локаторів помилок, представлених як *p*-многочлени, дозволяє досягти виграшу за швидкодією в 1,5 рази більше порівняно з методом пошуку Ченя.

Література:

1. Фрейман В.І. (2019). Дослідження характеристик кодів Ріда-Соломона для реалізації у пристроях систем керування. Радіоелектроніка, інформатика, управління. Запоріжжя. № 3. 143–151. DOI: 10.15588/1607-3274-2019-3-1.