XXXI Неделя науки СПбГПУ. Материалы межвузовской научной конференции. Ч. VI: С.189-190, 2003.

УДК 621.391.15

П.В. Трифонов (6 курс, кафедра РВКС), С.В. Федоренко к.т.н., доц.

БЫСТРЫЙ АЛГОРИТМ ВЫЧИСЛЕНИЯ СИНДРОМНОГО МНОГОЧЛЕНА ПРИ ДЕКОДИРОВАНИИ КОДОВ РИДА-СОЛОМОНА

В связи с бурным развитием телекоммуникационных систем в настоящее время остро стоит проблема эффективной реализации алгоритмов поддержки помехоустойчивого кодирования, использование которых необходимо для обеспечения приемлемого качества связи. Применение при программной или аппаратной реализации алгоритмов с высокой сложностью приводит к большим величинам задержки сообщения или громоздким микросхемам. В данной работе предлагается алгоритм, позволяющий существенно снизить сложность одного из этапов декодирования некоторых широко используемых кодов.

Как известно, декодирование кодов БЧХ, Рида-Соломона, Гоппы и многих других состоит из следующих этапов:

1. Вычисление синдромного многочлена $S(x)$
2. Поиск решения ключевого уравнения, связывающего многочлен синдрома S(x) с многочленами локаторов ошибок $\sigma(x)$ и значений ошибок $\xi(x)$
3. Поиск корней многочлена $\sigma(x)$, значения которых указывают на местоположение искаженных при передаче символов
4. Поиск значений ошибок (в случае использования недвоичных кодов)
5. Коррекция ошибок

На всех этих этапах вычисления производятся в некотором конечном поле $GF(2^m)$. Наибольшую вычислительную сложность имеют первый и четвертый этапы; традиционно, они реализуются с помощью методов, основанных на схеме Горнера. Проблема быстрого поиска корней многочлена локаторов ошибок была рассмотрена в работах [1], [2]. В данной работе предлагается алгоритм быстрого вычисления синдромного многочлена.

В работе [3] был предложен алгоритм вычисления быстрого преобразования Фурье над конечными полями. Алгоритм записывается как

$$F = AL f, \qquad (1)$$

где A – матрица с элементами из поля $GF(2)$, L – блочно-диагональная матрица, элементы которой являются циркулянтами, составленными из элементов нормальных базисов всех подполей $GF(2^m)$; Известно, что умножение на циркулянтные матрицы эквивалентно вычислению циклических сверток, поэтому алгоритм (1) сводится к набору циклических сверток и последующих сложений. Ввиду того, что проблема вычисления синдромного многочлена может рассматриваться как вычисление неполного преобразования Фурье, описанный алгоритм может быть непосредственно применен для решения этой задачи. При этом следует ожидать, что сложность алгоритма может быть снижена за счет того, что не требуется вычислять некоторые компоненты ДПФ, Однако, очевидный подход, состоящий в отбрасывании строк матрицы A, соответствующих ненужным компонентам ДПФ, не дает уменьшения общего числа вычислительно сложных операций умножения в алгоритме.

Известно, что ДПФ обладает свойством симметрии, т.е. алгоритмы прямого и обратного преобразования совпадают с точностью до перестановки компонентов выходного вектора. Поэтому выражение (1) может быть переписано в эквивалентной форме как

$$F' = A^{-1}L^{-1} f', \qquad (1)$$

где X' означает соответствующую перестановку. Данное преобразование сохраняет структуру алгоритма [3]. Таким образом, задача вычисления неполного преобразования Фурье сводится к следующим этапам:

1. Выбор блоков матрицы L^{-1}, соответствующих искомым компонентам ДПФ.

2. Построение алгоритмов циклической свертки для этих блоков.

3. Как правило, оказывается, что не требуется вычислять все коэффициенты циклической свертки. Существующие алгоритмы быстрого вычисления циклических сверток [4] могут оказаться неоптимальными в этой ситуации. В ряде случаев, сложность может быть сокращена путем циклического сдвига коэффициентов свертки.

4. Построение последовательности предварительных сложений, реализующих умножение на матрицу A.

Применение описанного подхода позволило построить алгоритм вычисления синдромного многочлена для кода RS (255,239,17) , содержащий 80 умножений и 2862 сложений, что лучше, у всех известных авторам аналогов.

ЛИТЕРАТУРА:

1. S.V. Fedorenko, P.V. Trifonov. Finding roots of polynomials over finite fields, IEEE Transactions on Communications, 50(11), 2002.

2. S.V. Fedorenko, P.V. Trifonov, E. Costa, H. Haas. Improved hybrid algorithm for finding roots of error-locator polynomials, Submitted to European Transactions on Telecommunications, 2002.

3. S.V. Fedorenko, P.V. Trifonov. On Computing the Fast Fourier Transform over Finite Fields, In Proceedings of ACCT'02, pp. 108 – 111, 2002.

4. Р. Блейхут. Теория и практика кодов, контролирующих ошибки. М.: Мир, 1986.