XXXII Неделя науки СПбГПУ. Материалы межвузовской научно-технической конференции. Ч.V : С.180-181

УДК 621.391.1:681.3

Н.Л.Чурков (3 курс, каф. РВиКС), С.В.Федоренко, к.т.н., доц.

МЕТОД ПОСТРОЕНИЯ ЦИКЛИЧЕСКИХ СВЕРТОК СОСТАВНОЙ ДЛИНЫ НАД КОНЕЧНЫМИ ПОЛЯМИ

Во многих областях используется дискретное преобразование Фурье (ДПФ). Известно множество алгоритмов быстрого преобразования Фурье (БПФ). Один из таких методов использует циклические свертки (ЦС) над конечными полями – циклотомический алгоритм [1]. Этот метод состоит в разбиении исходного многочлена на сумму линеаризованных и вычислении их значений в наборе базисных точек с последующим комбинированием с коэффициентами из простого подполя. При выборе в качестве базиса поля нормального вычисление линеаризованных многочленов сводится к вычислению циклических сверток с фиксированным сомножителем.

Использование циклических сверток наталкивает на необходимость разработки методов построения быстрых ЦС. Известны алгоритмы построения сверток над полями вещественных и комплексных чисел, использующие особенности этих полей, но над конечными полями характеристики 2 они или не работают, или не дают выигрыша.

Предлагается метод вычисления ЦС составной длины путем разбиения задачи на подзадачи меньшей размерности, равной делителю длины данной ЦС. Разбиение проводится по векторам и матрицам в матричной записи свертки. При этом свертка исходной длины над элементами поля сводится к свертке длины, равной делителю исходной длины, – уже над матрицами и векторами из элементов того же поля. То есть, один из сомножителей – вектор матриц, а другой – вектор из векторов. Результат свертки – вектор из векторов. При вычислении этой свертки меньшей размерности операциями будут сложение матриц и векторов и умножение матрицы на вектор. Последнее представляет собой умножение теплицевой матрицы на вектор. Более того, часть таких умножений являются циклическими свертками (в матричной записи) над элементами исходного поля, так как некоторые теплицевы матрицы будут циркулянтными. В общем случае не известно оптимального алгоритма перемножения теплицевой матрицы и вектора, который бы имел мультипликативную сложность циклической свертки, но такое не исключено, а на размерности 2 это выполняется.

В отличие от метода Агарвала-Кули уменьшения размерности задачи [4] в предлагаемом методе нет ограничения на взаимную простоту делителей длины свертки. Это позволяет ускоренно вычислять свертки на длинах, содержащих степени простых чисел. На длинах, равных степени 2, алгоритм не хуже известных, а при условии фиксированного сомножителя их превосходит. Алгоритм дает возможность построения циклических сверток любой длины, путем сведения их к ЦС на длинах, равных простым делителям заданной длины.

Циклическая свертка длины 8 получается из сверток длин 4 и 2. В качестве примера рассмотрим свертку длины 4 над конечным полем характеристики 2, которая получается из свертки длины 2, выполненной с матрицами и векторами размерности 2 над этим же полем. Используемая свертка длины 2 имеет мультипликативную сложность 3, 2 из которых тривиальны в случае фиксированного сомножителя. При подстановке в свертку векторов и матриц (размерности 2) нетривиальные умножения заменяется умножениями теплицевой матрицы на вектор, а тривиальные – умножениями циркулянтной матрицы на вектор

(вычисляются как циклические свертки длины 2 над элементами поля). Умножение же теплицевой 2x2-матрицы на вектор длины 2 имеет мультипликативную сложность 3.

$$\mathbf{C}=\begin{pmatrix}\begin{pmatrix}c_0\\c_1\end{pmatrix}\\\begin{pmatrix}c_2\\c_3\end{pmatrix}\end{pmatrix}=\begin{pmatrix}\mathbf{C}_0\\\mathbf{C}_1\end{pmatrix}=\begin{pmatrix}\begin{pmatrix}b_0&b_3\\b_1&b_0\end{pmatrix}&\begin{pmatrix}b_2&b_1\\b_3&b_2\end{pmatrix}\\\begin{pmatrix}b_2&b_1\\b_3&b_2\end{pmatrix}&\begin{pmatrix}b_0&b_3\\b_1&b_0\end{pmatrix}\end{pmatrix}\times\begin{pmatrix}\begin{pmatrix}a_0\\a_1\end{pmatrix}\\\begin{pmatrix}a_2\\a_3\end{pmatrix}\end{pmatrix}=\begin{pmatrix}\mathbf{B}_0&\mathbf{B}_1\\\mathbf{B}_1&\mathbf{B}_0\end{pmatrix}\times\begin{pmatrix}\mathbf{A}_0\\\mathbf{A}_1\end{pmatrix}=\mathbf{B}\times\mathbf{A}$$

Итак, матричная свертка длины 2 использует 1 умножение на теплицеву 2x2-матрицу и 2 умножения на циркулянтную, первое требует 3 умножения в поле, а второе в случае фиксированного сомножителя – одно умножение. Получаем вычисление ЦС длины 4 за 2*2+1*1=5 умножений (всего – 9 умножений, но 2*2=4 из них тривиальные).

Свертка длины 8 получается, если уже в полученной циклической свертке длины 4 вместо элементов поля поставить 2x2-матрицы и вектора длины 2. Матричная свертка длины 4 использует 5 умножений на теплицеву 2x2-матрицу и 4 умножения на циркулянтную, опять же первое требует 3 умножения в поле, а второе в случае фиксированного сомножителя – одно умножение. Получаем вычисление циклической сверки длины 8 за 5*3+4*1=19 умножений (всего – 27 умножений, но 4*2=8 из них тривиальные).

Циклотомический алгоритм БПФ длины 255 использует 30 раз циклическую свертку длины 8 с фиксированным сомножителем. Известна свертка длины 8, требующая 27 умножений [2]. Но при фиксированном сомножителе она редуцируется лишь до 22 умножений. А свертка, вытекающая из работы Захаровой [3], – до 21 умножения.

Таким образом, получена циклическая свертка длины 8 над полем характеристики 2, требующая в случае фиксированного сомножителя всего 19 умножений, что на 2 умножения меньше, чем в свертке, ранее использовавшейся при построении БПФ длины 255. Это приводит к уменьшению мультипликативной сложности циклотомического алгоритма БПФ длины 255 на 60 умножений.

Замена известных ранее методов построения сверток предложенным приводит к существенному уменьшению мультипликативной сложности БПФ.

ЛИТЕРАТУРА:

1. П.В.Трифонов, С.В.Федоренко. Метод быстрого вычисления преобразования Фурье над конечным полем. Проблемы передачи информации, 2003. Т.39. Вып.3. с. 3-10.
2. Э.М.Габидулин, В.Б. Афанасьев. Кодирование в радиоэлектронике. М.: Радио и связь, 1986.
3. Т.Г.Захарова. Вычисление преобразования Фурье в полях характеристики 2. Проблемы передачи информации, 1992. Т.28. Вып.2. с. 62-77.
4. Блейхут Р. Теория и практика кодов, контролирующих ошибки. М.: Мир, 1986.