Министерство образования и науки Российской Федерации

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«САРАТОВСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИМЕНИ Н.Г. ЧЕРНЫШЕВСКОГО»

Кафедра теоретических основ компьютерной безопасности и криптографии

**Дискретное преобразование Фурье**

ОТЧЕТ ПО ДИСЦИПЛИНЕ

«ТЕОРЕТИКО-ЧИСЛОВЫЕ МЕТОДЫ В КРИПТОГРАФИИ»

Лабораторная работа №3

студентки 5 курса 531 группы

специальности 10.05.01 «Компьютерная безопасность»

факультета компьютерных наук и информационных технологий

Громовой Наталии Викторовны

|  |  |  |
| --- | --- | --- |
| Преподаватель  профессор | \_\_\_\_\_\_\_\_\_\_ | В.А. Молчанов |
|  | подпись, дата |  |

Саратов 2018

**Цель работы**: изучение свойств дискретного преобразования Фурье.

**Теоретическая часть**

Пусть имеется многочлен n-ой степени:

 A(x) = a_0 x^0 + a_1 x^1 + \ldots + a_{n-1} x^{n-[...]

Не теряя общности, можно считать, что n является степенью 2. Если в действительности n не является степенью 2, то мы просто добавим недостающие коэффициенты, положив их равными нулю.

Из теории функций комплексного переменного известно, что комплексных корней n-ой степени из единицы существует ровно n. Обозначим эти корни через w_{n,k}, k = 0 \ldots {n-1}, тогда известно, что w_{n,k} = e^{ i \frac{ 2 \pi k }{ n } }. Кроме того, один из этих корней w_n = w_{n,1} = e^{ i \frac{ 2 \pi }{ n } } (называемый главным значением корня n-ой степени из единицы) таков, что все остальные корни являются его степенями: w_{n,k} = (w_n)^k.

 {\rm DFT}(a_0, a_1, \ldots, a_{n-1}) = (y_0, y_1,[...]Тогда дискретным преобразованием Фурье (ДПФ) (discrete Fourier transform, DFT) многочлена A(x) (или, что то же самое, ДПФ вектора его коэффициентов (a_0, a_1, \dots, a_{n-1})) называются значения этого многочлена в точках x = w_{n,k}, т.е. это вектор:

 = (A(w_n^0), A(w_n^1), \ldots, A(w_n^{n-1})). 

Аналогично определяется и обратное дискретное преобразование Фурье (InverseDFT). Обратное ДПФ для вектора значений многочлена (y_0, y_1, \ldots y_{n-1})— это вектор коэффициентов многочлена (a_0, a_1, \ldots, a_{n-1}):

 {\rm InverseDFT}(y_0, y_1, \ldots, y_{n-1}) = (a_[...]

Таким образом, если прямое ДПФ переходит от коэффициентов многочлена к его значениям в комплексных корнях n-ой степени из единицы, то обратное ДПФ — наоборот, по значениям многочлена восстанавливает коэффициенты многочлена.

**Быстрое преобразование Фурье** (fast Fourier transform) — это метод, позволяющий вычислять ДПФ за время O(n \log n). Этот метод основывается на свойствах комплексных корней из единицы (а именно, на том, что степени одних корней дают другие корни).

Основная идея БПФ заключается в разделении вектора коэффициентов на два вектора, рекурсивном вычислении ДПФ для них, и объединении результатов в одно БПФ.

Итак, пусть имеется многочлен A(x) степени n, где n — степень двойки, и n>1:

 A(x) = a_0 x^0 + a_1 x^1 + \ldots + a_{n-1} x^{n-[...]

Разделим его на два многочлена, один — с чётными, а другой — с нечётными коэффициентами:

 A_1(x) = a_1 x^0 + a_3 x^1 + \ldots + a_{n-1} x^{[...] A_0(x) = a_0 x^0 + a_2 x^1 + \ldots + a_{n-2} x^{[...]

Нетрудно убедиться, что:

 A(x) = A_0(x^2) + x A_1(x^2). ~~~~~~~(1) 

Многочлены A_0 и A_1 имеют вдвое меньшую степень, чем многочлен A. Если мы сможем за линейное время по вычисленным {\rm DFT}(A_0) и {\rm DFT}(A_1)вычислить {\rm DFT}(A), то мы и получим искомый алгоритм быстрого преобразования Фурье (т.к. это стандартная схема алгоритма "разделяй и властвуй", и для неё известна асимптотическая оценка O(n \log n)).

Итак, пусть мы имеем вычисленные вектора \{ y_k^0 \}_{k=0}^{n/2-1} = {\rm DFT}(A_0) и \{ y_k^1 \}_{k=0}^{n/2-1} = {\rm DFT}(A_1). Найдём выражения для \{ y_k \}_{k=0}^{n-1} = {\rm DFT}(A).

Во-первых, вспоминая (1), мы сразу получаем значения для первой половины коэффициентов:

 y_k = y_k^0 + w_n^k y_k^1, ~~~~k = 0 \ldots n/2-1[...]

 y_{k+n/2} = A(w_n^{k+n/2}) = A_0(w_n^{2k+n}) + w_[...]Для второй половины коэффициентов после преобразований также получаем простую формулу:

 = A_0(w_n^{2k}) - w_n^k A_1(w_n^{2k}) = y_k^0 - w[...]

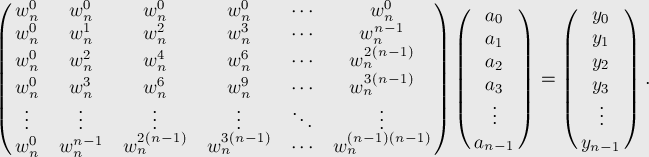
(Здесь мы воспользовались (1), а также тождествами w_n^n = 1 и  w_n^{n/2} = -1.)

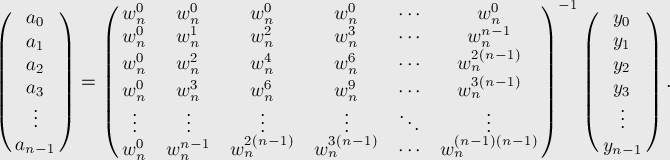
Итак, в результате мы получили формулы для вычисления всего вектора \{ y_k \}:

 y_{k+n/2} = y_k^0 - w_n^k y_k^1, \ \ \ \ k = 0 \l[...] y_k = y_k^0 + w_n^k y_k^1, \ \ \ \ k = 0 \ldots n[...]

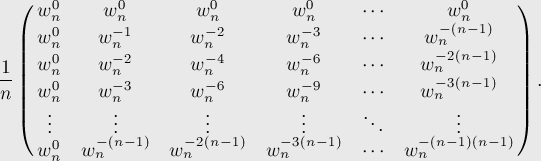
**Обратное БПФ**

Итак, пусть дан вектор (y_0, y_1, \ldots, y_{n-1}) — значения многочлена A степени n в точках x = w_n^k. Требуется восстановить коэффициенты (a_0, a_1, \ldots, a_{n-1})многочлена. Эта известная задача называется **интерполяцией**, для этой задачи есть и общие алгоритмы решения, однако в данном случае будет получен очень простой алгоритм (простой тем, что он практически не отличается от прямого БПФ).

ДПФ мы можем записать, согласно его определению, в матричном виде:

Тогда вектор (a_0, a_1, \ldots, a_{n-1}) можно найти, умножив вектор (y_0, y_1, \ldots, y_{n-1}) на обратную матрицу к матрице, стоящей слева (которая, кстати, называется матрицей Вандермонда):

Непосредственной проверкой можно убедиться в том, что эта обратная матрица такова:



Таким образом, получаем формулу:

 a_k = \frac{1}{n} \sum_{j=0}^{n-1} y_j w_n^{-kj}.[...]

Сравнивая её с формулой для y_k:

 y_k = \sum_{j=0}^{n-1} a_j w_n^{kj}, 

мы замечаем, что эти две задачи почти ничем не отличаются, поэтому коэффициенты a_k можно находить таким же алгоритмом "разделяй и властвуй", как и прямое БПФ, только вместо w_n^k везде надо использовать w_n^{-k}, а каждый элемент результата надо разделить на n.

Таким образом, вычисление обратного ДПФ почти не отличается от вычисления прямого ДПФ, и его также можно выполнять за время O(n \log n)

Алгоритм БПФ (аналогичный для обратного БПФ, но *w* меняем на *w-1(* mod *m),*а на шаге 3 полагаем .

