УДК 517.9

БЫСТРОЕ ПРЕОБРАЗОВАНИЕ ФУРЬЕ И РЕШЕНИЕ СВЁРТОЧНЫХ УРАВНЕНИЙ НА ГРУППЕ ГЕЙЗЕНБЕРГА НАД ПРОСТЫМ ПОЛЕМ ГАЛУА

Деундяк В. М., Леонов Д. А.

FFT AND SOLVING OF CONVOLUTION EQUATIONS ON HEISENBER GROUP OVER PRIME GALUA FIELD

Deundyak V. M., Leonov D. A.

Southern Federal University, Rostov-on-Don, 344090, Russia
e-mail: tori_92@inbox.ru

Abstract. Fourier method has been used for a long time in many fields of mathematics, physics and engineering sciences on commutative groups. The development of the fast Fourier transform that can significantly speed up the solution of important practical problems is of particular interest. But in comparison with the commutative variant the construction of the fast Fourier transforms for non-commutative groups is more difficult because of the complexity of the dual objects group in terms of which this transformation is constructed.

This paper studies Fourier method of solution of convolution equations on finite Heisenberg group $\mathbb{H}(\mathbb{F}_p)$ over Galois field $\mathbb{F}_p$ of a prime power. The fast Fourier transform on this group is built on the basis of reduction to the fast Fourier transform on the cyclic groups, the explicit formulas for forward and inverse transformations are obtained. On the basis of proved formulas an effective algorithm has been developed for solution of convolution equations with the complexity $O(n^{\frac{4}{3}})$, where $n = p^3$ is the power of $\mathbb{H}(\mathbb{F}_p)$. Obtained theoretical results allowed us on the basis of the programming language $C\#$ to develop a software implementation of the numerical method for solution of convolution equations on $\mathbb{H}(\mathbb{F}_p)$. The results of numerical experiments are presented in the paper.

Keywords: Heisenberg group, convolution equations, Fourier method, fast Fourier transformation.

Введение

Метод Фурье на некоммутативных группах имеет широкое применение, в частности, в области анализа ранжированной информации, при разработке методов кодирования в каналах и сетях передачи данных [1], в теории фильтров и анализе изображений [2], в задаче дифракции на телах с некоммутативной группой симметрий [3]. Хорошо известно, что группа Гейзенберга $\mathbb{H}_n(\mathbb{F})$ и теория преобразования Фурье на этой группе в случае, когда поле $\mathbb{F}$ равно полю вещественных чисел $\mathbb{R}$ или полю комплексных чисел $\mathbb{C}$, играет важную роль в теоретической физике, теории дифференциальных и интегральный уравнений на группах Ли [4]. Конечная группа Гейзенберга $\mathbb{H}_n(\mathbb{F}_p)$ над полями Галуа используется при решении задач случайных блужданий [5], а также в теории и практике радиообнаружения и дальнометрии [6].

В случае конечных коммутативных групп для более эффективных вычислений давно интенсивно применяется быстрое преобразование Фурье (БПФ) со сложностью $O(n \log n)$, где n — мощность группы. Однако для некоммутативных групп разработка БПФ существенно затрудняется из-за проблем, связанных с теорией представлений. В настоящий момент для некоторых классов конечных некоммутативных групп известны быстрые алгоритмы преобразования Фурье с невысокой сложностью вплоть до $O(n \log n)$ [7–10]. Разработка более эффективных алгоритмов

Деундяк Владимир Михайлович, канд. физ.-мат. наук, доцент кафедры алгебры и дискретной математики института математики, механики и компьютерных наук имени И. И. Воровича Южного федерального университета; e-mail: vlade@math.rsu.ru.

Леонов Дмитрий Александрович, аспирант первого года обучения по специальности математика и механика, кафедры алгебры и дискретной математики института математики, механики и компьютерных наук имени И. И. Воровича Южного федерального университета; e-mail: tori_92@inbox.ru.

БПФ для различных классов некоммутативных групп активно ведётся и сейчас.

Целью настоящей работы является разработка и программная реализация алгоритма быстрого преобразования Фурье на группе Гейзенберга $\mathbb{H}(\mathbb{F}_p)$, где $\mathbb{F}_p$ — поле Галуа с простым p, решение на этой основе свёрточных уравнений и проведение численных экспериментов.

1. Сверточные уравнения и преобразование Фурье на конечных некоммутативных группах

Пусть $\mathbb{G}$ — конечная группа с атомарной мерой, а $\mathbb{C}\mathbb{G}$ — групповая алгебра над полем $\mathbb{C}$ [11]. Групповая алгебра $\mathbb{C}\mathbb{G}$ естественно изоморфна алгебре $L_1(\mathbb{G})$, операция умножения в которой является левой свёрткой. Далее будем отождествлять алгебры $\mathbb{C}\mathbb{G}$ и $L_1(\mathbb{G})$. Напомним, что левая свертка и правая свертка функций φ и ψ из $L_1(\mathbb{G})$ обозначаются соответственно $\varphi *_l \psi$ и $\varphi *_r \psi$ и определяются формулами:

$$(\varphi *_l \psi)(y) = \sum_{x\in\mathbb{G}} \varphi(yx^{-1})\psi(x),$$

$$(\varphi *_r \psi)(y) = \sum_{x\in\mathbb{G}} \varphi(x^{-1}y)\psi(x),$$

где $y \in \mathbb{G}$. Оператор левой свёртки $C_a^{(l)} : L_1(\mathbb{G}) \to L_1(\mathbb{G})$ задаётся равенством

$$(C_a^{(l)} f)(y) = (a *_l f)(y),\ y \in \mathbb{G},$$

функция a называется ядром оператора $C_a^{(l)}$. Аналогично определяется оператор правой свёртки $C_a^{(r)}$

$$(C_a^{(r)} f)(y) = (a *_r f)(y),\ y \in \mathbb{G}.$$

В случае коммутативной группы операторы левой и правой свёртки совпадают.

Преобразование Фурье $F : L_1(\mathbb{Z}_n) \to \to L_1(\mathbb{Z}_n)$ для циклической группы $\mathbb{Z}_n$ определяется равенством

$$(Ff)(k) = \sum_{l=0}^{n-1} f(l) e^{i\frac{2\pi kl}{n}}, \qquad (1.1)$$

$k, l \in \mathbb{Z}_n$, а обратное преобразование Фурье F^{-1} действует по формуле

$$(F^{-1}f)(l) = \frac{1}{n}\sum_{k=0}^{n-1} f(k) e^{-i\frac{2\pi kl}{n}}, \qquad (1.2)$$

$k, l \in \mathbb{Z}_n$ [11].

Чтобы определить преобразование Фурье на произвольной конечной группе $\mathbb{G}$ понадобятся дополнительные определения [12]. Далее будем рассматривать унитарные представления группы $\mathbb{G}$ в линейном пространстве $\mathbb{C}^n$, т.е. гомоморфизмы $\mathbb{G}$ в группу унитарных матриц $U(n)$. Отметим, что представления могут иметь разные размерности, через d_ρ обозначим размерность представления ρ. Характером группы $\mathbb{G}$ называется произвольный гомоморфизм этой группы в мультипликативную группу $\mathbb{T} = \{z \in \mathbb{C} : |z| = 1\}$. Характер χ_T конечномерного представления $\mathbf{T}$ группы $\mathbb{G}$ определяется с помощью следа

$$\chi_T(g) = \mathtt{tr}(T(g)).$$

Представления $\mathbf{T}$, $\mathbf{T}'$ называются эквивалентными, если существует такая обратимая матрица $\mathbf{Q}$, что $\mathbf{T}(g) = \mathbf{Q}^{-1}\mathbf{T}'(g)\mathbf{Q}$ для любого $g \in \mathbb{G}$. Множество классов эквивалентности унитарных неприводимых представлений группы $\mathbb{G}$ обозначают $\hat{\mathbb{G}}$ и называют двойственным объектом группы $\mathbb{G}$. В каждом классе эквивалентности зафиксируем представитель (представление группы $\mathbb{G}$) и далее, не теряя общности, под $\hat{\mathbb{G}}$ будем понимать множество таких представителей. Если группа $\mathbb{G}$ коммутативна, то все неприводимые унитарные представления одномерны и двойственный объект является группой. В некоммутативном случае дуальный объект для группы $\mathbb{G}$ не является группой и построить его труднее [13].

Пусть $\mathbb{G}$ — конечная группа, $\hat{\mathbb{G}}$ — двойственный объект группы $\mathbb{G}$. Преобразование Фурье на конечной группе $\mathbb{G}$ ставит в соответствие каждой функции f на $\mathbb{G}$ операторную функцию $\hat{f}$ на множестве $\hat{\mathbb{G}}$, причём

$$\forall \rho \in \hat{\mathbb{G}} : \hat{f}(\rho) \in L(d_\rho, \mathbb{C}),$$

где символом $L(d_\rho, \mathbb{C})$ обозначена алгебра квадратных $d_\rho \times d_\rho$ матриц над полем $\mathbb{C}$, а d_ρ — размерность неприводимого представления ρ. Через $\mathfrak{G}(\hat{\mathbb{G}})$ обозначим прямое произведение матричных алгебр $L(d_\rho, \mathbb{C})$ для всех $\rho \in \hat{\mathbb{G}}$. Отметим, что $\mathfrak{G}(\hat{\mathbb{G}})$ — алгебра с покомпонентно определенными операциями [13].

Прямое преобразование Фурье $F : \mathbb{C}\mathbb{G} \to \mathfrak{G}(\hat{\mathbb{G}})$ является алгебраическим

изоморфизмом и определяется следующим образом [12]:

$$(F(f))(\rho) = \sum_{x\in\mathbb{G}} f(x)\rho(x), \qquad (1.3)$$

где $\rho \in \hat{\mathbb{G}}$, а обратное преобразование Фурье $F^{-1} : \mathfrak{G}(\hat{\mathbb{G}}) \to \mathbb{C}\mathbb{G}$

$$(F^{-1}(g))(x) = \frac{1}{|\mathbb{G}|}\sum_{\rho\in\hat{\mathbb{G}}} d_\rho \mathrm{tr}(g(\rho)\rho(x^{-1})), \qquad (1.4)$$

$x \in \mathbb{G}$. (Здесь и далее для произвольного конечного множества X через $|X|$ будем обозначать его мощность.) Иногда для удобства будем использовать обозначения $F = F_{\mathbb{G}}$, $F(f) = \hat{f}$ и $F^{-1}(g) = \check{g}(x)$.

С помощью M_φ будем обозначать оператор умножения на матрицу—функцию $\boldsymbol{\varphi} \in \mathfrak{G}(\hat{\mathbb{G}})$, который действует в $\mathfrak{G}(\hat{\mathbb{G}})$.

Теперь рассмотрим оператор $C_a^{(l)}$. Символом этого оператора будем называть $F(a)$ — преобразование Фурье ядра.

Теорема 1. Свёрточный оператор $C_a^{(l)}$ обратим тогда и только тогда, когда для всех $\rho \in \hat{\mathbb{G}}$ выполняется

$$(F(a))(\rho) \in GL(d_\rho, \mathbb{C}), \qquad (1.5)$$

где d_ρ — размерность представления.

Рассмотрим уравнение

$$C_a^{(l)}\boldsymbol{\varphi} = b_0, \quad a, b_0 \in L_1(\mathbb{G}) \qquad (1.6)$$

относительно неизвестной $\boldsymbol{\varphi} \in L_1(\mathbb{G})$. Найти неизвестную функцию φ из уравнения (1.6), для которого выполняется условие (1.5), можно следующим образом:

1) подействовать на обе части уравнения (1.6) преобразованием Фурье

$$F(a)F(\varphi) = F(b_0);$$

2) умножить полученное уравнение слева на обратный элемент к $(F(a))(x)$

$$F(\varphi) = (F(a))^{-1}F(b_0);$$

3) воспользоваться обратным преобразованием Фурье

$$\varphi = F^{-1}((F(a))^{-1}F(b_0)).$$

Эта схема решения свёрточного уравнения хорошо известна и широко применяется для коммутативных групп. Для некоммутативных групп она становится сложнее из-за того, что для каждой группы нужно находить неприводимые представления и строить свой дуальный объект.

2. БПФ на группе $\mathbb{H}(\mathbb{F}_p)$

Приведем в удобном виде необходимые сведения о группе Гейзенберга $\mathbb{H}(\mathbb{F}_p)$, где $\mathbb{F}_p$ — поле Галуа мощности p, а p — произвольное простое число. Дискретная группа $\mathbb{H}(\mathbb{F}_p)$ определяется как множество матриц 3×3 вида

$$\begin{pmatrix} 1 & x & z \\ 0 & 1 & y \\ 0 & 0 & 1 \end{pmatrix}, \quad x, y, z \in \mathbb{F}_p,$$

с обычной операцией умножения матриц. Для удобства элементы $\mathbb{H}(\mathbb{F}_p)$ будем обозначать тройками (x, y, z). Тогда умножение принимает следующий вид:

$$(x, y, z)(x', y', z') = (x + x', y + y', z + z' + xy'),$$

а обратный элемент вычисляется по формуле

$$(x, y, z)^{-1} = (-x, -y, xy - z).$$

Отметим, что $|\mathbb{H}(\mathbb{F}_p)| = p^3$. Матрицу размера $p \times p$, у которой все элементы, кроме диагональных, равны нулю, будем обозначать как

$$\mathrm{diag}[a_{1,1}, a_{2,2}, a_{3,3}, \ldots, a_{p,p}].$$

Для определения преобразования Фурье понадобятся все неприводимые унитарные представления $\mathbb{H}(\mathbb{F}_p)$. Дискретная группа $\mathbb{H}(\mathbb{F}_p)$ имеет 2 типа представлений [6]:

1) p^2 одномерных представлений $\rho_{a,b}$, определяемых по формуле

$$\rho_{a,b}(x, y, z) = e^{\frac{2\pi i(ax+by)}{p}}, \quad a, b \in \mathbb{F}_p;$$

2) $p - 1$ представлений ρ_s размерности p вида

$$\rho_s(x, y, z) = e^{\frac{2\pi i(sz)}{p}}\mathbf{D}(sy)\mathbf{W}(x), \qquad (2.1)$$

где $s \in \mathbb{F}_p\backslash\{0\}$, $\mathbf{D}(\lambda)$ — диагональная матрица размера $p \times p$, вида

$$\mathbf{D}(\lambda) = \mathrm{diag}\left[e^{\frac{2\pi i(\lambda b_0)}{p}}, e^{\frac{2\pi i(\lambda b_1)}{p}}, \ldots, e^{\frac{2\pi i(\lambda b_{p-1})}{p}}\right],$$

$\lambda, b_i \in \mathbb{F}_p$, а $\mathbf{W}(x)$ — матрица сдвига

$$\mathbf{W}(x) = \begin{pmatrix} 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ \vdots & \vdots & \vdots & \dots & \vdots \\ 0 & 0 & 0 & \dots & 1 \\ 1 & 0 & 0 & \dots & 0 \end{pmatrix}^{\widetilde{x}},$$

где $\widetilde{x} \in \mathbb{N}$ соответствует $x \in \mathbb{F}_p$. Пусть $\sigma_{a,b}$ и σ_s — классы эквивалентности унитарных представлений группы $\mathbb{H}(\mathbb{F}_p)$, содержащие представления $\rho_{a,b}$ и ρ_s соответственно, где $a, b \in \mathbb{F}_p$, $s \in \mathbb{F}_p \backslash \{0\}$. Множество таких представлений обозначим $\hat{\mathbb{H}}(\mathbb{F}_p)$, оно имеет вид

$$\hat{\mathbb{H}}(\mathbb{F}_p) = \{\rho_{0,0}, \dots, \rho_{p-1,p-1}, \rho_1, \dots, \rho_{p-1}\}.$$

Аддитивную группу поля $\mathbb{F}_p$ отождествим с группой $\mathbb{Z}_p$, а группу $\mathbb{F}_p^3$ с группой $\mathbb{Z}_p^3$. Алгебра $L_1(\mathbb{F}_p^3)$ является тензорным произведением алгебр $L_1(\mathbb{F}_p)$, т.е.

$$L_1(\mathbb{F}_p^3) = L_1(\mathbb{F}_p) \otimes L_1(\mathbb{F}_p) \otimes L_1(\mathbb{F}_p).$$

Отметим, что для $f \in L_1(\mathbb{F}_p^3)$

$$(F_{\mathbb{F}_p^3} f)(x_1, x_2, x_3) = \\ = ((F^{(1)} \otimes F^{(2)} \otimes F^{(3)}) f)(x_1, x_2, x_3),$$

где $F^{(k)} : L_1(\mathbb{F}_p) \to L_1(\mathbb{F}_p)$ — преобразование Фурье на группе $\mathbb{F}_p$ по k-й переменной, $k = 1, 2, 3$. Через $I^{(k)}$ будем обозначать тождественный оператор действующий в $L_1(\mathbb{F}_p)$ по k-й переменной, $k = 1, 2, 3$.

Теорема 2. Пусть $\mathbb{H}(\mathbb{F}_p)$ — группа Гейзенберга и $\hat{\mathbb{H}}(\mathbb{F}_p)$ — двойственный объект для $\mathbb{H}(\mathbb{F}_p)$. Тогда:

I. На одномерных представлениях $\{\rho_{a,b}\}_{a,b \in \mathbb{F}_p}$ значения преобразования Фурье функции $f \in L_1(\mathbb{H}(\mathbb{F}_p))$ можно вычислить по формуле

$$\widehat{f}(\rho_{a,b}) = ((F^{(1)} \otimes F^{(2)})\varphi)(a, b), \qquad (2.2)$$

где $\varphi(x, y) = \sum_{z=0}^{p-1} f(x, y, z)$.

На представлениях $\{\rho_s\}_{s \in \mathbb{F}_p \backslash \{0\}}$ размерности p значения преобразования Фурье $\widehat{f}(\rho_s)$ задаются в виде $(p \times p)$–матрицы

$$(((I^{(1)} \otimes F^{(2)} \otimes F^{(3)}) f)(j - i, is, s))_{i,j=0}^{p-1}. \quad (2.3)$$

II. Быстрое преобразование Фурье на группе $\mathbb{H}(\mathbb{F}_p)$ может быть построено с помощью быстрого преобразования Фурье на циклической группе $\mathbb{Z}_p$, его сложность составляет $O(p^3 \log p)$, где p — мощность поля $\mathbb{F}_p$.

Доказательство. Рассмотрим преобразование Фурье на $\mathbb{H}(\mathbb{F}_p)$ на одномерных представлениях $\rho_{a,b}$

$$\widehat{f}(\rho_{a,b}) = (F_{\mathbb{H}(\mathbb{F}_p)} f)(\rho_{a,b}) = \sum_{g \in \mathbb{H}(\mathbb{F}_p)} f(g)\rho_{a,b}(g) = \\ = \sum_{x \in \mathbb{F}_p} \sum_{y \in \mathbb{F}_p} \sum_{z \in \mathbb{F}_p} f(x, y, z)\rho_{a,b}(x, y, z) = \\ = \sum_{x=0}^{p-1} \sum_{y=0}^{p-1} \sum_{z=0}^{p-1} f(x, y, z) e^{\frac{2\pi i(ax+by)}{p}} = \\ = \sum_{x=0}^{p-1} e^{\frac{2\pi iax}{p}} \sum_{y=0}^{p-1} e^{\frac{2\pi iby}{p}} \sum_{z=0}^{p-1} f(x, y, z).$$

Просуммируем функцию $f(x, y, z)$ по z и обозначим $\varphi(x, y) = \sum_{z=0}^{p-1} f(x, y, z)$, тогда

$$\widehat{f}(\rho_{a,b}) = \sum_{x=0}^{p-1} e^{\frac{2\pi iax}{p}} \sum_{y=0}^{p-1} e^{\frac{2\pi iby}{p}} \varphi(x, y).$$

Вторая сумма в последней формуле — преобразование Фурье на циклической группе $\mathbb{Z}_p$ по переменной y, т.е.

$$\widehat{f}(\rho_{a,b}) = \sum_{x=0}^{p-1} e^{\frac{2\pi iax}{p}} ((I^{(1)} \otimes F^{(2)})\varphi)(x, b),$$

оставшаяся сумма является преобразованием Фурье по переменной x, т.е.

$$\widehat{f}(\rho_{a,b}) = ((F^{(1)} \otimes F^{(2)})\varphi)(a, b),$$

где $a, b = 0,1, \dots, p-1$. Формула (2.2) доказана.

Рассмотрим преобразование Фурье на $\mathbb{H}(\mathbb{F}_p)$ для представлений ρ_s размерности p и построим быстрое преобразование Фурье

$$\widehat{f}(\rho_s) = (F_{\mathbb{H}(\mathbb{F}_p)} f)(\rho_s) = \sum_{g \in \mathbb{H}(\mathbb{F}_p)} f(g)\rho_s(g) = \\ = \sum_{x \in \mathbb{F}_p} \sum_{y \in \mathbb{F}_p} \sum_{z \in \mathbb{F}_p} f(x, y, z)\rho_s(x, y, z) = \\ = \sum_{x=0}^{p-1} \sum_{y=0}^{p-1} \sum_{z=0}^{p-1} f(x, y, z) e^{\frac{2\pi i(sz)}{p}} \mathbf{D}(sy)\mathbf{W}(x),$$

Сумма по z является преобразованием Фурье на циклической группе функции $f(x,y,z)$ по переменной z, с учётом этого вторая сумма представляет собой диагональную матрицу, у которой на диагонали расположены элементы вида $\sum\limits_{y=0}^{p-1}((I^{(1)}\otimes I^{(2)}\otimes F^{(3)})f)(x,y,s)e^{\frac{2\pi isyk}{p}}$, где $k\in\mathbb{F}_p$, но

$$\sum_{y=0}^{p-1}((I^{(1)}\otimes I^{(2)}\otimes F^{(3)})f)(x,y,s)e^{\frac{2\pi isyk}{p}} = \\ =((I^{(1)}\otimes F^{(2)}\otimes F^{(3)})f)(x,sk,s),$$

где $k\in\mathbb{F}_p$, $s\in\mathbb{F}_p\backslash\{0\}$. Далее просуммировав матрицы по переменной x мы получим матрицу элементы которой вычисляются по формуле (2.3).

Положение I доказано. □

Так как в формуле (2.2) требуется вычислить два преобразования Фурье на циклической группе, то с учётом того, что сложность быстрого преобразования Фурье на циклической группе $\mathbb{Z}_p$ равна $O(p\log p)$, следует, что для вычисления значений преобразования Фурье функции $f\in L_1(\mathbb{H}(\mathbb{F}_p))$ от одномерных представлений по формуле (2.2) понадобится $O(p^2\log p)$, где p — количество операций умножения в поле комплексных чисел.

Для того, чтобы получить быстрое преобразование Фурье на группе $\mathbb{H}(\mathbb{F}_p)$ нужно применить быстрое преобразования Фурье для каждого элемента матрицы. Сложность одного быстрого преобразования Фурье составляет $O(p\log p)$, получаем, что сложность преобразования Фурье на группе $\mathbb{H}(\mathbb{F}_p)$ составит $O(p^3\log p)$ т.е. $O(|\mathbb{H}(\mathbb{F}_p)|\log|\mathbb{H}(\mathbb{F}_p)|)$, где p — мощность поля $\mathbb{F}_p$.

Положение II доказано. □

Теорема 3. Пусть $\mathbb{H}(\mathbb{F}_p)$ — группа Гейзенберга и $\hat{\mathbb{H}}(\mathbb{F}_p)$ — двойственный объект для $\mathbb{H}(\mathbb{F}_p)$. Тогда:

I. Преобразование Фурье функции $\varphi\in\mathfrak{G}(\hat{\mathbb{H}}(\mathbb{F}_p))$ можно вычислить по формуле

$$\check{\varphi}((x,y,z)^{-1}) = \frac{1}{p^3}((F^{(1)}\otimes F^{(2)})\psi)(x,y)+ \\ +\frac{1}{p^2}((I^{(1)}\otimes F^{(2)}\otimes F^{(3)})a)(x,sy,z), \quad (2.4)$$

где

$$\psi(a,b)=\varphi(\rho_{a,b}),\quad a,b\in\mathbb{F}_p,$$

$a(x,k,s)$ — диагональные элементы матрицы $\boldsymbol{\varphi}(\rho_s)\mathbf{D}(sy)\mathbf{W}(x)$, $x,y,k,z\in\mathbb{F}_p$, $s\in\mathbb{F}_p\backslash\{0\}$.

II. Быстрое обратное преобразование Фурье на группе $\mathbb{H}(\mathbb{F}_p)$ может быть построено с помощью быстрого обратного преобразования Фурье на циклической группе $\mathbb{Z}_p$, его сложность составляет $O(p^3\log p)$, где p — мощность поля $\mathbb{F}_p$.

Доказательство. Рассмотрим формулу обратного преобразования Фурье (1.4) функции $\varphi\in\mathfrak{G}(\hat{\mathbb{H}}(\mathbb{F}_p))$ от элемента $(x,y,z)^{-1}$ и преобразуем ее

$$\check{\varphi}((x,y,z)^{-1}) = (F^{-1}_{\mathbb{H}(\mathbb{F}_p)}\varphi)((x,y,z)^{-1}) = \\ =\frac{1}{|\mathbb{H}(\mathbb{F}_p)|}\sum_{\rho\in\widetilde{\mathbb{H}}(\mathbb{F}_p)} d_\rho\operatorname{tr}(\varphi(\rho)\rho(x,y,z)) = \\ =\frac{1}{p^3}\sum_{\rho_{a,b}\in\widetilde{\mathbb{H}}(\mathbb{F}_p)} d_{\rho_{a,b}}\operatorname{tr}(\varphi(\rho_{a,b})\rho_{a,b}(x,y,z))+ \\ +\frac{1}{p^3}\sum_{\rho_s\in\widetilde{\mathbb{H}}(\mathbb{F}_p)} d_{\rho_s}\operatorname{tr}(\varphi(\rho_s)\rho_s(x,y,z)),$$

так как $d_{\rho_{a,b}}=1$, $d_{\rho_s}=p$ и

$$\operatorname{tr}(\varphi(\rho_{a,b})\rho_{a,b}(x,y,z)) = \varphi(\rho_{a,b})\rho_{a,b}(x,y,z),$$

то

$$\check{\varphi}((x,y,z)^{-1}) = \\ =\frac{1}{p^3}\sum_{\rho_{a,b}\in\widetilde{\mathbb{H}}(\mathbb{F}_p)}\varphi(\rho_{a,b})\rho_{a,b}(x,y,z)+ \\ +\frac{1}{p^2}\sum_{\rho_s\in\widetilde{\mathbb{H}}(\mathbb{F}_p)}\operatorname{tr}(\varphi(\rho_s)\rho_s(x,y,z)). \quad (2.5)$$

Рассмотрим отдельно первую сумму и будем обозначать $\psi(a,b)=\varphi(\rho_{a,b})$

$$\frac{1}{p^3}\sum_{\rho_{a,b}\in\widetilde{\mathbb{H}}(\mathbb{F}_p)}\psi(a,b)\rho_{a,b}(x,y,z) = \\ =\frac{1}{p^3}\sum_{a=0}^{p-1}\sum_{b=0}^{p-1}\psi(a,b)e^{\frac{2\pi i(ax+by)}{p}} = \\ =\frac{1}{q^3}\sum_{a=0}^{p-1}e^{\frac{2\pi iax}{p}}\sum_{b=0}^{p-1}\psi(a,b)e^{\frac{2\pi iby}{p}},$$

сумма по b является преобразованием Фурье функции $\psi(a,b)$ на циклической группе $\mathbb{Z}_p$,

а сумма по a — преобразование Фурье суммы $\sum_{b=0}^{p-1}\psi(a,b)e^{\frac{2\pi iby}{p}}$ на циклической группе $\mathbb{Z}_p$, т.е.

$$\frac{1}{p^3}\sum_{a=0}^{p-1}e^{\frac{2\pi iax}{p}}\sum_{b=0}^{p-1}\psi(a,b)e^{\frac{2\pi iby}{p}} = \frac{1}{p^3}\sum_{a=0}^{p-1}e^{\frac{2\pi iax}{p}}((I^{(1)}\otimes F^{(2)}\psi)(a,y) = \frac{1}{p^3}((F^{(1)}\otimes F^{(2)})\psi)(x,y).$$

Рассмотрим вторую сумму формулы (2.5)

$$\frac{1}{p^2}\sum_{\rho_s\in\widetilde{\mathbb{H}}(\mathbb{F}_p)}\operatorname{tr}(\boldsymbol{\varphi}(\rho_s)\rho_s(x,y,z)) = \frac{1}{p^2}\sum_{s=1}^{p-1}e^{\frac{2\pi i(sz)}{p}}\operatorname{tr}(\boldsymbol{\varphi}(\rho_s)\mathbf{D}(sy)\mathbf{W}(x)).$$

Так как $\boldsymbol{\varphi}(\rho_s)$ — матрица размера $p\times p$, обозначим её элементы как

$$\boldsymbol{\varphi}(\rho_s) = (a_{k,j}(s))_{k,j=0}^{p-1},$$

тогда

$$\boldsymbol{\varphi}(\rho_s)\mathbf{D}(sy) = (a_{k,j}(s)e^{\frac{2\pi i(syk)}{p}})_{k,j=0}^{p-1}.$$

Для вычисления следа нужны только диагональные элементы матрицы. Матрица $\mathbf{W}(x)$ является матрицей сдвига, поэтому умножение всех матриц $\boldsymbol{\varphi}(\rho_s)\mathbf{D}(sy)\mathbf{W}(x)$ может быть выполнено за $O(|\mathbb{H}(\mathbb{F}_p)|) = O(p^3)$ операций. Диагональные элементы примут вид $a_{k,k-x}(s)e^{\frac{2\pi i(syk)}{p}}$, где $x,k = 0,1,\ldots,p-1$, $s = 1,\ldots,p-1$, обозначим эти элементы $a(x,k,s) = a_{k,k-x}(s)$, тогда след можно записать следующим образом:

$$\operatorname{tr}(\boldsymbol{\varphi}(\rho_s)\mathbf{D}(sy)\mathbf{W}(x)) = \sum_{k=0}^{p-1}a(x,k,s)e^{\frac{2\pi i(syk)}{p}} = (I^{(1)}\otimes F^{(2)}\otimes I^{(3)})a)(x,sy,s).$$

Вернемся ко второй сумме формулы (2.5)

$$\frac{1}{p^2}\sum_{\rho_s\in\widetilde{\mathbb{H}}(\mathbb{F}_p)}\mathtt{tr}(\boldsymbol{\varphi}(\rho_s)\rho_s(x,y,z)) = \frac{1}{p^2}\sum_{s=1}^{p-1}((I^{(1)}\otimes F^{(2)}\otimes I^{(3)})a)(x,sy,s)e^{\frac{2\pi i(sz)}{p}} = \frac{1}{p^2}((I^{(1)}\otimes F^{(2)}\otimes F^{(3)})a)(x,sy,z).$$

Таким образом, преобразование Фурье функции φ для элемента $(x,y,z)^{-1}$ можно вычислить по формуле (2.4).

Положение I доказано. □

При использовании алгоритма БПФ на циклической группе для вычисления значений первой суммы в формуле (2.4) для всех (x,y,z) понадобится $O(p^2\log p)$.

Учитывая, что умножение всех матриц $\boldsymbol{\varphi}(\rho_s)\mathbf{D}(sy)\mathbf{W}(x)$ может быть выполнено за $O(p^3)$ операций, то для вычисления значений второй суммы в формуле (2.4) для всех (x,y,z) понадобится $O(p^3\log p)$. Таким образом, сложность обратного преобразования Фурье на $\mathbb{H}(\mathbb{F}_p)$ составит $O(p^3\log p)$, где p — мощность поля $\mathbb{F}_p$.

Положение II доказано. □

3. Решение свёрточных уравнений на группе $\mathbb{H}(\mathbb{F}_p)$

В разделе 2 для группы $\mathbb{H}(\mathbb{F}_p)$, приведен алгоритм сложность которого $O(p^3\log p)$. Рассмотрим подробнее алгоритм решения свёрточного уравнения на конечной группе, приведенный в конце раздела 1. На первом шаге нам требуется найти БПФ от функций $a, b_0\in L_1(\mathbb{H}(\mathbb{F}_p))$, сложность вычисления составит $O(p^3\log p)$. На втором шаге приведенного алгоритма вычисляется произведение двух преобразований Фурье, для одного из которых нужно найти обратный элемент $(F(a)(\rho))^{-1}$. В случае представления ρ_s, где $s = 1,2\ldots,p-1$, элемент $(F(a))(\rho_s)$ является матрицей размера $p\times p$, обращение которой можно выполнить со сложностью $O(p^3)$, тогда обращение всех $p-1$ матриц потребует $O(p^4)$ операций. На третьем шаге применяется обратное БПФ, сложность которого также составляет $O(p^3\log p)$. Несмотря на использование построенного алгоритма БПФ, сложность которого — $O(p^3\log p)$, т.е $O(|\mathbb{H}(\mathbb{F}_p)|\log|\mathbb{H}(\mathbb{F}_p)|)$, сложность решения

Таблица 1. Время работы алгоритмов ПФ и БПФ на $\mathbb{H}(\mathbb{F}_p)$

№1	$\lvert\mathbb{G}\rvert$	343	1331	2197	4913	6859
1	t (прямое ПФ, $\mathbb{H}(\mathbb{F}_p)$)	0,012	0,136	0,388	1,842	2,896
2	t (обратное ПФ, $\mathbb{H}(\mathbb{F}_p)$)	0,013	0,198	0,547	2,93	6,198
3	t (прямое БПФ, $\mathbb{H}(\mathbb{F}_p)$)	0,007	0,025	0,028	0,095	0,132
4	t (обратное БПФ, $\mathbb{H}(\mathbb{F}_p)$)	0,005	0,022	0,029	0,102	0,118
5	t (прямое БПФ, $\mathbb{Z}_{p^3}$)	0,004	0,022	0,029	0,095	0,096
6	t (обратное БПФ, $\mathbb{Z}_{p^3}$)	0,004	0,022	0,028	0,096	0,102

Таблица 2. Время решения свёрточного уравнения с помощью ПФ и БПФ

№2	$\lvert\mathbb{G}\rvert$	343	1331	2197	4913	6859
1	t (ПФ, $\mathbb{H}(\mathbb{F}_p)$)	0,033	0,444	1,107	5,626	11,172
2	t (БПФ, $\mathbb{H}(\mathbb{F}_p)$)	0,014	0,059	0,084	0,322	0,404
3	t (БПФ, $\mathbb{Z}_{p^3}$)	0,013	0,058	0,084	0,25	0,275

свёрточного уравнения составит $O(p^4)$, т.е. $O(|\mathbb{H}(\mathbb{F}_p)|^{\frac{4}{3}})$.

С помощью построенного программного средства для решения свёрточного уравнения на $\mathbb{H}(\mathbb{F}_p)$ проведены эксперименты и проанализирована зависимость времени работы программы от мощности группы.

Результаты экспериментов представлены в табл. 1 и 2, при этом в табл. 1 содержатся данные численных экспериментов работы алгоритмов ПФ и БПФ на группе $\mathbb{H}(\mathbb{F}_p)$ и равномощной ей циклической группе $\mathbb{Z}_{p^3}$, а в табл. 2 — численных экспериментов решения свёрточных уравнений на группах $\mathbb{H}(\mathbb{F}_p)$ и $\mathbb{Z}_{p^3}$. Диапазон мощностей групп в обеих таблицах — от 343 до 6859. В первой и второй строках табл. 1 указано время работы алгоритмов прямого и обратного преобразования Фурье. В третьей и четвёртой строках табл. 1 — время работы алгоритмов быстрого прямого и обратного преобразования Фурье соответственно. Для сравнения, в пятой и шестой строках табл. 1 приведено время работы алгоритмов быстрого прямого и обратного преобразования Фурье на $\mathbb{Z}_{p^3}$ соответственно. В первой строке табл. 2 указано время решения свёрточного уравнения на $\mathbb{H}(\mathbb{F}_p)$ с помощью алгоритма ПФ, во второй — с помощью алгоритма БПФ, в третьей — решение свёрточного уравнения на группе $\mathbb{Z}_{p^3}$.

Полученные численные результаты демонстрируют преимущество решения свёрточного уравнения с применением БПФ, при этом время работы алгоритма на группе $\mathbb{H}(\mathbb{F}_p)$ несущественно отличается от времени его работы на равномощной группе $\mathbb{Z}_{p^3}$. Но время работы алгоритма БПФ решения свёрточного уравнения для группы $\mathbb{H}(\mathbb{F}_p)$ отличается от времени для равномощной группы $\mathbb{Z}_{p^3}$, что связано это с обращением матриц из представлений, о которых сказано в начале раздела.

Численные эксперименты проводились на ОС Windows 7 Professional, Service Pack 1, 64bit, процессор Intel Core 2 Quad CPU Q6600 2.4GHz, ОЗУ 4.00 Gb. Программное средство реализовано с помощью языка программирования *C#*.

Заключение

На конечной дискретной группе Гейзенберга $\mathbb{H}(\mathbb{F}_p)$, где $\mathbb{F}_p$ — поле Галуа с простым p, построено быстрое преобразование Фурье. Разработана программная реализация численного метода решения свёточных уравнений на $\mathbb{H}(\mathbb{F}_p)$ с применением построенного быстрого преобразования Фурье, приведены результаты численных экспериментов и представлен анализ полученных результатов.

Литература

1. *Rockmore D.* Recent Progress and Applications in Group FFTs // Computational Noncommutative Algebra and Applications. 2004. Vol. 136. P. 227–254.
2. *Leinz R.* Using representations of the dihedral groups in the design of early vision filters // Acoustics, Speech, and Signal Processing. 1993. Vol. 5. P. 165–168.
3. *Загороднов И. А., Тарасов Р. П.* Задача дифракции на телах с некоммутативной конечной группой симметрий и численное ее реше-

ние // Журн. вычисл. математики и матем. физики. 1997. Т. 37. № 10. С. 1246—1262.
4. *Howe R.* On The role of the Heisenberg group in harmonic analysis // Bulletin of the American Mathematical Society. 1980. Vol. 3. № 2. P. 821–843.
5. *Bump D., Diaconis P., Hicks A., Miclo L., Widom H.* An exercise (?) in Fourier analysis on the Heisenberg group // ArXiv e-prints. 2015. P. 1–24.
6. *Terras A.* Fourier analysis on finite groups and applications. Cambridge University Press, 1999. 456 с.
7. *Beth T.* On the Computational Complexity of the General Discrete Fourier Transform // Theor. Comp. Sci. 1987. Vol. 51. P. 331–339.
8. *Clausen M.* Fast Generalized Fourier Transforms // Theor. Comp. Sci. 1989. Vol. 67. № 1. P. 55–63.
9. *Rockmore D.* Efficient computation of Fourier Inversion for finite groups // J. of the ACM. 1994. Vol. 41. № 1. P. 31–66.
10. *Деундяк В. М., Леонов Д. А.* Применение быстрого преобразования Фурье для решения сверточных уравнений на диэдральных группах // Вестник САФУ. 2015. № 3. С. 97–107.
11. *Кириллов А. А.* Элементы теории представлений. М.: Наука, 1978. 343 с.
12. *Кириллов А. А.* Введение в теорию представлений и некоммутативный гармонический анализ // Итоги науки и техн. Сер. Соврем. пробл. мат. Фундам. направления. 1988. Т. 22. С. 5–162.
13. *Хьюитт Э., Росс К.* Абстрактный гармонический анализ. М.: Наука, Т. 2. 1975. 900 с.

References

1. Rockmore D. Recent Progress and Applications in Group FFTs. *Computational Noncommutative Algebra and Applications*, 2004, vol. 136, pp. 227–254.
2. Leinz R. Using representations of the dihedral groups in the design of early vision filters. *Acoustics, Speech, and Signal Processing*, 1993, vol. 5, pp. 165-168.
3. Zagorodnov I. A., Tarasov R. P. Zadacha difraktsii na telakh s nekommutativnoy konechnoy gruppoy simmetriy i chislennoe ee reshenie [The Problem of Diffraction on Bodies with Non-Commutative Finite Group of Symmetries and Numerical Solution]. *Zhurnal Vychislitel'noi Matematiki i Matematicheskoi Fiziki*, 1997, vol. 37, no. 10, pp. 1246–1262.
4. Howe R. On The role of the Heisenberg group in harmonic analysis. *Bulletin of the American Mathematical Society*, 1980, vol. 3, no. 2, pp. 821–843.
5. Bump D., Diaconis P., Hicks A., Miclo L., Widom H. An exercise(?) in Fourier analysis on the Heisenberg group. *ArXiv e-prints*, 2015, pp. 1–24.
6. Terras A. *Fourier analysis on finite groups and applications*. Cambridge University Press, 1999, 456 p.
7. Beth T. On the Computational Complexity of the General Discrete Fourier Transform. *Theor. Comp. Sci.*, 1987, vol. 51, pp. 331–339.
8. Clausen M. Fast Generalized Fourier Transforms. *Theor. Comp. Sci.*, 1989, vol. 67, no. 1, pp. 55–63.
9. Rockmore D. Efficient computation of Fourier Inversion for finite groups. *J. of the ACM*, 1994, vol. 41, no. 1, pp. 31–66.
10. Deundyak V. M., Leonov D. A. Primenenie bistrogo preobrazovania Fourier dlya reshenia svertochnih uravneni' na diedral'nih groppah [Fast Fourier Transform for solution of convolution equations on Dihedral Groups]. *Vestnik NARFU*, 2015, no. 3, pp. 97—107.
11. Kirillov A. A. *Elementy teorii predstavleniy* [Elements of Theory of Representations]. Moscow, Science, 1978, 343 p.
12. Kirillov A. A. Vvedenie v teoriu predstavleni' i nekommutativni' garmonicheski' analis [Introduction to the theory of representations and noncommutative harmonic analysis]. *Itogi nauki i techn. Ser. Sovrem. probl. mat. Fundam. napravleniya*, 1988, vol. 22, pp. 5–162.
13. Hewitt E., Ross K. *Abstract Harmonic Analysis*. Moscow, Science, vol. 2, 1975, 900 p.

Статья поступила 22 марта 2016 г.