Г. А. Маргулис, Явные конструкции расширителей, *Пробл. передачи информ.*, 1973, том 9, выпуск 4, 71–80

ПРОБЛЕМЫ ПЕРЕДАЧИ ИНФОРМАЦИИ

Том IX *1973* *Вып. 4*

УДК 621.395.34:513.83

ЯВНЫЕ КОНСТРУКЦИИ РАСШИРИТЕЛЕЙ

Г. А. Маргулис

При решении некоторых задач теории коммутации и теории кодирования возникает необходимость в построении конструкций, аналогичных тем, которые в настоящей работе называются расширителями. Несмотря на то что существование расширителей довольно легко доказывается из вероятностных соображений, их явное построение оказывается затруднительным. В настоящей работе с помощью теории представлений групп решается задача о явном построении расширителей.

§ 1. Формулировка задачи

1.1. Пусть нам нужно создать конструкцию, обладающую некоторым свойством. В теории информации и близких к ней вопросах одним из наиболее распространенных является следующий путь: сначала строится некоторый класс конструкций, а потом доказывается, что в этом классе почти все конструкции (в некотором смысле) являются «хорошими» (т. е. обладающими требуемым свойством). Но при этом зачастую оказывается: несмотря на то что «хороших» конструкций очень много, явно построить хотя бы одну из них очень трудно. Задача, о которой будет идти речь в настоящей работе, как раз связана с такого рода конструктиями.

1.2. В этом пункте будут даны определения, необходимые для постановки задачи. Пусть A и B — некоторые конечные множества. Элементы множества A назовем входами, а элементы множества B — выходами. Пусть каждый вход *непосредственно* соединен с некоторым числом выходов. Любой полученный таким образом граф будем называть *соединителем.* Если в соединителе число элементов в множестве A равно числу элементов в множестве B, то такой соединитель назовем равномерным. Пусть H — *равномерный соединитель. Емкостью* соединителя H назовем число элементов в множестве A (или, что то же, в множестве B), *весом* — число ребер в H, а *плотностью* — отношение веса к емкости. В дальнейшем для любого равномерного соединения H через $c(H)$, $w(H)$ и $d(H)$ будем обозначать соответственно емкость, вес и плотность этого соединителя.

Пусть H — равномерный соединитель, а X — подмножество множества A. Тогда через X_H обозначим подмножество множества B, состоящее из тех и только тех выходов, которые соединены хотя бы с одним из входов, принадлежащих подмножеству X.

Для любого подмножества X множества A (или множества B) через $r(X)$ будем обозначать число элементов в X, а отношение $c(X)/c(A)$ будем называть плотностью подмножества X. Пусть теперь c и α — положительные числа, причем $c>1$, а $\alpha<1$. Тогда равномерный соединитель H назовем (c, α)-расширителем, если выполнено следующее условие: для любого подмножества X множества A, плотность которого меньше α, имеет место неравенство

$$\frac{c(X_H)}{c(X)}>c.$$

1.3 Постановка задачи. Для любых таких положительных c и α, что $c>1$, $\alpha<1$ и $c\alpha<1$ требуется явно построить такую бесконечную последовательность $H_1, \ldots, H_i, \ldots$ равномерных соединителей, чтобы выполнялись следующие условия:

1) при любом i $(1\leqslant i<\infty) H_i$ является (c, α)-расширителем;

2) если i стремится к бесконечности, то емкость соединителя H_i стремится к бесконечности, т. е. $\lim\limits_{i\to\infty} c(H_i)=\infty$;

3) плотности всех соединителей H_i ограничены в совокупности некоторой константой D, т. е. для любого $i(1\leqslant i\leqslant\infty)$ верно неравенство $d(H_i)<D$, где D не зависит от i.

Несмотря на то что *существование* искомой последовательности равномерных соединителей довольно легко доказывается из вероятностных соображений, *явное* построение такой последовательности оказывается затруднительным.

1.4. Вопросы, близкие к тому, который был сформулирован в пункте 1.3, возникают в ряде задач теории коммутации и теории кодирования. Например, представляет интерес (см. работу М. С. Пинскера [1]) построение последовательности соединителей $H_1, \ldots, H_i \ldots$, у которых число входов пропорционально с некоторой константой k числу выходов, и являющихся (c, α)-расширителями (для соединителей, не являющихся равномерными, понятие (c, α)-расширителя определяется так же, как и для равномерных соединителей). При этом, естественно, надо потребовать соблюдение неравенства $c\alpha<1/k$. Покажем, как можно решить эту задачу для целых k и $\alpha<1/k$, если заранее решить задачу, сформулированную в пункте 1.3. Действительно, так как число входов (т. е. $c(A)$) пропорционально числу выходов (т. е. $c(B)$) с целочисленной константой k, то мы можем разбить A на k непересекающихся подмножеств $A_1, \ldots, A_k$, мощность каждого из которых равна мощности множества B (т. е. $c(A_i)=c(B)$ при любом $1\leqslant i\leqslant k$). После этого для любого $i(1\leqslant i\leqslant k)$ построим $(c, \alpha k)$-расширитель, у которого A_i является множеством входов, а B — множеством выходов (здесь мы используем решение задачи из п. 1.3). Затем объединим все полученные k соединителей в один. Чтобы показать, что полученный таким образом соединитель H является (c, α)-расширителем, достаточно заметить, что для любого $X\subset A$ выполняется неравенство $\dfrac{c(X\cap A_i)}{c(A_i)}>k\dfrac{c(X)}{c(A)}$ хотя бы при одном i, и после этого использовать то, что H состоит из $(c, \alpha k)$-расширителей.

Для практических вопросов, в которых встречается задача из пункта 1.3, важно, чтобы константа D была достаточно мала. По-видимому, приводимые ниже конструкции удовлетворяют этому условию. К сожалению, автор доказывать это не умеет. Будет лишь доказано существование D.

§ 2. Построение конструкции и формулировка утверждений, из которых вытекает, что построенная конструкция является искомой

2.1. Обозначения. Для любого натурального m через Z_m будем обозначать кольцо вычетов по модулю m. Для любых X и Y через $X\times Y$ будем обозначать прямое произведение X и Y.

2.2. Конструкция. Пусть m — произвольное натуральное число. Положим $A_m=Z_m\times Z_m$ и $B_m=Z_m\times Z_m$. Таким образом, элементами как множества A_m, так и множества B_m являются пары (x, y), где $x\in Z_m$ и $y\in Z_m$. Построим теперь соединитель H_m следующим образом: каждый элемент (x, y) множества A_m соединяется со следующими пятью элементами множества B_m: 1) (x, y), 2) $(x+1, y)$, 3) $(x, y+1)$, 4) $(x, x+y)$, 5) $(-y, x)$.

2.3. Теорема. *Существует такая положительная константа d, не зависящая от m, что для любого натурального m построения в п. 2.2 соединитель H_m является $(1+d(1-\alpha),\ \alpha)$-расширителем при любом α, удовлетворяющем неравенству $0<\alpha<1$.*

Доказательство теоремы будет приведено в § 3.

2.4. Пусть H_1 и H_2 — два равномерных соединителя с одинаковой емкостью, т. е. у H_1 и H_2 одинаковое число входов (и выходов). Тогда между выходами соединителя H_1 и входами соединителя H_2 можно установить взаимно однозначное соответствие. Иначе говоря мы можем считать, что выходы соединителя H_1 являются входами соединителя H_2. Определим теперь произведение $H_2 \circ H_1$ соединителей H_2 и H_1 следующим образом:

1) входами соединителя $H_2 \circ H_1$ являются входы соединителя H_1, а выходами — выхода соединителя H_2;

2) вход x соединителя $H_2 \circ H_1$ тогда и только тогда соединен с выходом соединителя $H_2 \circ H_1$, когда найдется такой выход z соединителя H_1 (он же вход соединителя H_2), который соединен как с x, так и с y.

2.5. Из определения произведения соединителей и определения (c, α)-расширителя сразу следует

Лемма. *Если H_1 является (c_1, α)-расширителем, а H_2 — $(c_2, c_1\alpha)$-расширителем, то $H_2 \circ H_1$ является (c_1c_2, α)-расширителем.*

Замечание. Строго говоря, определение произведения соединителей H_2 и H_1 зависит от способа отождествления выходов соединителя H_1 с входами соединителя H_2. Тем не менее только что сформулированная лемма остается верной независимо от этого способа.

2.6. Для любого соединителя H и любого натурального k через H^k будем обозначать произведение $\overbrace{H\circ \ldots \circ H}^{k \text{ раз}}$. Тогда из определения соединителя H_m и определения произведения соединителей сразу вытекает, что для любых натуральных m и k каждый вход соединителя $H_m{}^k$ соединен не более чем с 5^k выходами этого соединителя. Поэтому верна

Лемма. *Для любых натуральных m и k плотность соединителя $H_m{}^k$ не превосходит 5^k.*

2.7. Из теоремы 2.3 и леммы 2.5 сразу следует

Лемма. *Пусть c и α — такие положительные числа, что $\alpha<1$, $c>1$, и $c\alpha<1$. Тогда найдется такое k, что для любого m соединитель $H_m{}^k$ является (c, α)-расширителем.*

2.8. *Замечание.* Леммы 2.6 и 2.7 дают ответ на задачу, поставленную в п. 1.3.

§ 3. Доказательство теоремы 2.3

3.1. Настоящий параграф состоит из двух частей. В первой части (пункты 3.2—3.8) теорема 2.3 будет сведена к лемме 3.7. Во второй части (пункты 3.9—3.23) лемма 3.7 будет доказана с помощью методов теории представлений групп.

3.2. Сохраним обозначения пункта 2.2. Определим теперь преобразования T_1, T_2, T_3 и T_4 множества $A_m = Z_m \times Z_m$ по следующим формулам:

$$T_1(x, y) = (x+1, y),$$

$$T_2(x, y) = (x, y+1).$$

$$T_3(x, y) = (x+y, y),$$

$$T_4(x, y) = (-y, x),$$

где $x \in Z_m$ и $y \in Z_m$.

3.3. Как и прежде, для любого X через $c(X)$ будем обозначать число элементов в X. Кроме того, для любого подмножества X множества A и любого $i\,(1\leqslant i\leqslant 4)$ через $T_i(x)$ будем обозначать образ X под действием преобразования T_i (т. е. $T_i(X)=\bigcup\limits_{x\in X} T_i(x)$).

Лемма. *Существует такая положительная константа d, что для любого натурального m и любого α, удовлетворяющего неравенству $0<\alpha<1$, верно следующее: если $X\subset A_m=Z_m\times Z_m$ и $c(X)<\alpha c(A_m)=\alpha m^2$, то для некоторого $i\,(1\leqslant i\leqslant 4)$ имеет место неравенство $c(T_i(X)\cup X)>(1+d(1-\alpha))c(X)$.*

Из определения соединителя H_m и преобразований T_1, T_2, T_3 и T_4 видно, что из только что сформулированной леммы 3.3 сразу следует теорема 2.3. Поэтому мы в дальнейшем будем доказывать именно эту лемму.

3.4. Введем в пространстве комплекснозначных функций на A_m скалярное произведение по следующей формуле:

$$(f_1,f_2)=\sum_{a\in A_m} f_1(a)\overline{f_2(a)},$$

где f_1 и f_2 — функции, а черта над $f_2(a)$ означает комплексное сопряжение. Легко видеть, что пространство комплекснозначных функций на A_m с только что введенным скалярным произведением является конечномерным евклидовым пространством, которое мы обозначим через $L^2(A_m)$. Введем в $L^2(A_m)$ норму, а именно для $f\in L^2(A_m)$ положим $\|f\|=\sqrt{(f,f)}$.

3.5. Пусть T — произвольное взаимно однозначное отображение множества A_m на себя. Сопоставим T линейный оператор $\tilde{T}$ в пространстве $L^2(A_m)$ следующим образом: если $f\in L^2(A_m)$, то для любого $a\in A_m$

$$\tilde{T}f(a)=f(T^{-1}a),$$

где T^{-1} означает отображение, обратное к T. Из взаимной однозначности T и того, как было определено скалярное произведение в $L^2(A_m)$, вытекает, что $\tilde{T}$ является в $L^2(A_m)$ унитарным оператором (для любых $f_1, f_2\in L^2(A_m)$ верно равенство $(\tilde{T}f_1,\tilde{T}f_2)=(f_1,f_2)$).

3.6. Обозначим через $S(A_m)$ подпространство в $L^2(A_m)$, состоящее из всех функций f, для которых $\sum\limits_{a\in A_m} f(a)=0$. Иначе говоря, $S(A_m)$ является ортогональным дополнением к одномерному пространству константы (функций, постоянных на всем A_m). Легко видеть, что $S(A_m)$ является в $L^2(A_m)$ подпространством коразмерности 1, т. е. $\dim L^2(A_m)-\dim S(A_m)=1$. Заметим еще, что для любого взаимно однозначного отображения T множества A_m в себя пространство $S(A_m)$ инвариантно относительно $\tilde{T}$.

3.7. Пусть T_1, T_2, T_3 и T_4 означают то же, что и в пунктах 3.2 и 3.3.

Лемма. *Существует такая положительная константа d, не зависящая от m, что для любого $f\in S(A_m)$ найдется такое $i\,(1\leqslant i\leqslant 4)$, что*

$$\frac{(\tilde{T}_i f,f)}{(f,f)}<1-d.$$

3.8. Доказательство леммы 3.7 будет приведено ниже. А пока покажем, как из нее вытекает лемма 3.3.

Пусть X — произвольное * подмножество множества A_m. Определим на A_m функцию f_X следующим образом:

$$f_X(a)=c(A_m)-c(X),\ \text{если } a\in X,$$

$$f_X(a)=-c(X),\ \text{если } a\notin X,$$

где $c(A)$ и $c(X)$, как и прежде, означает число элементов в A и X. Из определения функции f_X сразу видно, что $f_X\in S(A_m)$. Поэтому, согласно лемме 3.7, найдется такое i $(1\leqslant i\leqslant 4)$, что выполняется неравенство

$$\frac{(\widetilde{T}_i f_X, f_X)}{(f_X, f_X)}<1-d. \tag{1}$$

Из определения функции f_X и оператора $\widetilde{T}_i$ непосредственными вычислениями (которые мы опускаем ввиду их тривиальности) получаем следующие равенства:

$$(f_X, f_X)=c(X)c(A_m)(c(A_m)-c(X)) \tag{2}$$

и

$$(\widetilde{T}_i f_X, f_X)=c(A_m)[c(X\cap T_iX)c(A_m)-c^2(X)]. \tag{3}$$

Из (1)—(3) следует, что

$$\frac{c(X\cap T_iX)c(A_m)-c^2(X)}{c(X)(c(A_m)-c(X))}<1-d. \tag{4}$$

Так как $c(X)>0$ и $c(A_m)-c(X)>0$ (так как $X\neq\varnothing$ и $X\neq A_m$), то, обозначив $\dfrac{c(X)}{c(A_m)}$ через α_X, из (4) получаем, что

$$\begin{aligned} c(X\cap T_iX)&<\frac{(1-d)c(X)(c(A_m)-c(X))+c^2(X)}{c(A_m)}=\\ &=\frac{c(X)c(A_m)-c^2(X)-dc(X)c(A_m)+dc^2(X)+c^2(X)}{c(A_m)}=\\ &=c(X)-dc(X)+c(X)d\alpha_X=c(X)(1-d+d\alpha_X). \end{aligned} \tag{5}$$

Так как T_i — взаимно однозначное отображение, то $c(T_iX)=c(X)$. Поэтому

$$c(X\cup T_iX)=c(X)+c(T_iX)-c(X\cap T_iX)=2c(X)-c(X\cap T_iX). \tag{6}$$

Из (5) и (6) следует, что

$$c(X\cup T_iX)>c(X):[1+d(1-\alpha_X)]. \tag{7}$$

Из неравенства (7) сразу вытекает лемма 3.3.

3.9. Этот и следующие пункты будут посвящены доказательству леммы 3.7. Это доказательство будет основано на методах теории представлений групп, а более точно, на методах, связанных с свойством T, изучавшимся Д. А. Кажданом (см. [2, 3]). Мы здесь не будем давать определений из теории представлений групп, так как это заняло бы слишком много места. Отметим только, что эти определения могут быть почерпнуты из [2–4].

3.10 Обозначения. Обозначим через H группу всех унимодулярных ** матриц вида $\begin{pmatrix} a & b & u\\ c & d & v\\ 0 & 0 & 1\end{pmatrix}$, а через S — группу матриц вида $\begin{pmatrix} 1 & 0 & u\\ 0 & 1 & v\\ 0 & 0 & 1\end{pmatrix}$, где

* Мы исключим случаи, когда X — пустое множество и когда $X=A_m$.

** Матрица называется унимодулярной, если ее определитель равен 1.

a, b, c, d, u, v пробегают поле вещественных чисел. Через $H_Z \subset H$ ($S_Z \subset S$) обозначим подгруппу, состоящую из всех принадлежащих $H(S)$ матриц с целочисленными коэффициентами.

3.11. Для любого целого числа a и любого элемента x кольца Z_m через ax будем обозначать произведение a на x (если $a>0$, то ax по определению есть $\overbrace{x+\ldots+x}^{m\ \text{раз}}$, если $a<0$, то $ax=-[(-a)x]$, если $a=0$, то $ax=0$).

Пусть m — произвольное натуральное число. Сопоставим теперь каждому элементу $g=\begin{pmatrix} a & b & u \\ c & d & v \\ 0 & 0 & 1\end{pmatrix}$ группы H_Z преобразование $T_m(g)$ множества $A_m = Z_m \times Z_m$ следующим образом: если $(x,y) \in Z_m \times Z_m$, то $T_m(g)(x,y) = (ax+by+u,\ cx+dy+v)$. Непосредственными вычислениями проверяется, что для любых $g_1, g_2 \in H_Z$ верно равенство

$$(8) \qquad T_m(g_1g_2) = T_m(g_1)T_m(g_2).$$

3.12. Так как H_Z — группа, то из (8) следует, что для любого $g \in H_Z$ преобразование $T_m(g)$ взаимно однозначно. Поэтому $T_m(g)$ можно сопоставить (см. пункт 3.5) линейный унитарный оператор в пространстве $L^2(A_m)$. Обозначим этот оператор через $\tilde{T}_m(g)$. Из (8) и определения операторов $\tilde{T}_m(g)$ следует, что для любых $g_1, g_2 \in H_Z$ верно равенство

$$(9) \qquad \tilde{T}_m(g_1g_2) = \tilde{T}_m(g_1)\tilde{T}_m(g_2)$$

(при этом надо использовать тот легко проверяемый факт, что для любых двух взаимно однозначных отображений T_1 и T_2 верно равенство $\tilde{T}_1 \circ \tilde{T}_2 = \widetilde{T_1 \circ T_2}$).

Из равенства (9) и унитарности операторов $\tilde{T}_m(g)$ следует, что $\tilde{T}_m$ является унитарным представлением группы H_Z.

3.13. Выберем в группе H_Z следующие четыре элемента:

$$g_1=\begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1\end{pmatrix}, \qquad g_2=\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1\end{pmatrix},$$

$$g_3=\begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1\end{pmatrix}, \qquad g_4=\begin{pmatrix} 0 & -1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1\end{pmatrix}.$$

Из определения преобразований $T_m(g)$ (пункт 3.11) и преобразований T_1, T_2, T_3 и T_4 (пункт 3.2) сразу следуют равенства

$$(10) \qquad T_m(g_i) = T_i$$

при любом i ($1 \leqslant i \leqslant 4$). Из равенства (10), определения операторов $\tilde{T}_i$ ($1 \leqslant i \leqslant 4$) (см. пункт 3.5) и определения представлений $\tilde{T}_m$ (см. пункт 3.12) следует равенство

$$(11) \qquad \tilde{T}_m(g_i) = \tilde{T}_i.$$

при любом i ($1 \leqslant i \leqslant 4$).

3.14. Определение. Унитарное представление T группы H_Z в пространстве X назовем существенно нетривиальным на S_Z, если в X не найдется ненулевого вектора, инвариантного относительно $T(S_Z)$ (т. е. для любого $x \in X (x \neq 0)$ найдется такой элемент $s \in S_Z$, что $T(s)x \neq x$).

Определение. Унитарное представление T группы H в пространстве X назовем существенно нетривиальным на S, если в X не найдется ненулевого вектора, инвариантного относительно $T(S)$.

3.15. Лемма. *Существует такая положительная константа d, что если T — произвольное унитарное представление группы H_Z в гильбертовом пространстве L, существенно нетривиальное на S_Z, а x — любой ненулевой элемент из L, то найдется такое $i (1 \leqslant i \leqslant 4)$, что*

$$\frac{(T(g_i)x, x)}{(x, x)} < 1 - d,$$

где x, y означает скалярное произведение в пространстве L.

3.16. Доказательство леммы 3.15 будет приведено ниже. А пока покажем, как из леммы 3.15 следует лемма 3.7.

Как было отмечено в пункте 3.6, для любого взаимно однозначного отображения множества T в себя пространство $S(A_m)$ инвариантно относительно $\tilde{T}$. Поэтому $S(A_m)$ является для представления $\tilde{T}_m$ инвариантным подпространством. Обозначим через T_m' ограничение представления $\tilde{T}_m$ на подпространство $S(A_m)$. Так как $\tilde{T}_m$ — унитарное представление (см. пункт 3.12), то T_m' также унитарное представление. Покажем теперь, что T_m' существенно нетривиально на S_Z. Действительно, если бы T_m' не было существенно нетривиально на S_Z, то, как легко видеть, в $S(A_m)$ нашлась бы ненулевая функция f инвариантная относительно $T_m'(S_Z)$. Но тогда ввиду определения представления T_m' для любых x, y, u, $v \in Z_m$ верно равенство

$$f(x+u, y+v) = f(x, y). \tag{12}$$

Так как x, y, $v \in Z_m$ произвольны, то из (12) следует, что f постоянна на A_m. Но $f \in S(A_m)$, т. е. $\sum_{a \in m} f(a) = 0$. Следовательно, $f \equiv 0$. Таким образом, мы показали, что T_m' существенно нетривиально на S_Z. Из этого утверждения, унитарности представления T_m' и леммы 3.15 вытекает, что для любой ненулевой функции $f \in S(A_m)$ найдется такое $i (1 \leqslant i \leqslant 4)$, что

$$\frac{(T_m'(g_i)f, f)}{f, f} < 1 - d. \tag{13}$$

Так как $T_m'(g_i)f = \tilde{T}_m(g_i)f$ для любых $i (1 \leqslant i \leqslant 4)$ и $f \in S(A_m)$ (по определению T_m'), то из (13) и (11) следует лемма 3.7.

3.17. Пусть G — локально-компактная группа. Обозначим через $\tilde{G}$ множество унитарных представлений группы G. Пусть $T \in \tilde{G}$, $\varepsilon > 0$, K — компакт в G, X — вектор из пространства представления T. Обозначим через $V(X, K, \varepsilon)$ множество всех таких $T' \in \tilde{G}$, что в пространстве представления T найдется такой вектор Y, что для любого $g \in K$ выполняется неравенство $((T'(g)Y, Y) - (T(g)X, X)) < \varepsilon$. Введем теперь в G топологию, для которой множества $V(X, K, \varepsilon)$ образуют базис окрестностей представления T.

3.18. Лемма. *У единичного представления группы H_Z найдется такая окрестность U, что любое унитарное представление группы H_Z, существенно нетривиальное на S_Z, не лежит в U.*

3.19. Доказательство леммы 3.18 будет приведено ниже. А пока покажем, как лемма 3.15 сводится к лемме 3.18. Это сведение будет основано на лемме, доказательство которой будет приведено в пункте 3.20.

Лемма. *Элементы g_1, g_2, g_3 и g_4 из пункта 3.13 являются образующими группы H_Z.*

Сведение леммы 3.15 к лемме 3.18. Так как H_z — дискретная группа, то любой компакт $K\subset H_Z$ является конечным подмножеством. Поэтому из леммы 3.18 следует существование такого $\varepsilon>0$ и такого конечного подмножества $K\subset H_Z$, что для любого унитарного представления T' группы H_Z, существенно нетривиального на S_Z, верно следующее: если x элемент пространства представления T', то для некоторого $h\in K$ имеет место неравенство

$$(14)\qquad \frac{(T'(h)x, x)}{(x, x)}<1-\varepsilon.$$

Из унитарности оператора $T'(h)$ и теоремы Пифагора вытекает, что неравенство (14) эквивалентно неравенству

$$(15)\qquad \frac{\|x-T'(h)x\|}{\|x\|}>\sqrt{2\varepsilon-\varepsilon^2}.$$

Приведем теперь без доказательства следующее простое

Утверждение. *Пусть A_1 и A_2 — два унитарных оператора, действующих в одном и том же гильбертовом пространстве L, а $x\in L$. Тогда $\|x-T_1T_2x\|\leqslant\|x-T_1x\|+\|x-T_2x\|$ (унитарность T_1 и T_2 существенна).*

Так как K — конечное подмножество в H_Z, а g_1, g_2, g_3 и g_4 являются образующими в H_Z, то найдется такое натуральное m, что любой элемент $h\in K$ представляется в виде слова от g_1, g_2, g_3 и g_4, длина которого не превосходит m *. Отсюда, из неравенства (15) и приведенного только что утверждения вытекает, что для любого x из пространства представления T' найдется такое i, что

$$(16)\qquad \frac{\|T'(g_i)x-x\|}{\|x\|}<\frac{\sqrt{2\varepsilon-\varepsilon^2}}{m}.$$

Из унитарности оператора $T'(g_i)$ и теоремы Пифагора вытекает, что неравенство (16) эквивалентно неравенству

$$17)\qquad \frac{(T'(g_i)x, x)}{(x, x)}<\sqrt{1-\frac{2\varepsilon-\varepsilon^2}{m^2}}.$$

Теперь остается положить d, равным $1-\sqrt{1-\dfrac{2\varepsilon-\varepsilon^2}{m^2}}$ и заметить, что из (17) следует лемма 3.15.

3.20. Доказательство леммы 3.19. Обозначим через A_Z группу, состоящую из целочисленных унимодулярных матриц вида

$$\begin{pmatrix} a & b & 0 \\ c & d & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Обозначим через f отображение H_Z в A_Z, сопоставляющее матрице $\begin{pmatrix} & & \\ c & d & v \\ & & \end{pmatrix}$ матрицу $\begin{pmatrix} a & b & 0 \\ c & d & 0 \\ 0 & 0 & 1 \end{pmatrix}$. Непосредственными вычислениями про-

---

* Т. е. $h=g_{i_1}^{m_1}g_{i_2}^{m_2}\ldots g_{i_l}^{m_l}$, где $1\leqslant i_j\leqslant 4$ и $\sum_{j=1}^{l}|m_j|<m$ (m_j могут быть отрицательными).

веряется, что для любого $g \in H_Z$ имеет место равенство

(18) $$g = f(g) \cdot s,$$

где $s \in S_Z$. Сделаем теперь следующие два замечания:

Замечание 1. Как легко следует из § 2 в [5] (см. замечание в [5] после теоремы 1 из § 2), группа A_Z порождается элементами g_3 и g_4 (определение g_3 и g_4 см. пункт 3.13).

Замечание 2. Непосредственно проверяется, что для любых целых m и n верно следующее равенство:

(19) $$\begin{pmatrix} 1 & 0 & m \\ 0 & 1 & n \\ 0 & 0 & 1 \end{pmatrix} = g_1^m g_2^n,$$

где g_1 и g_2 — из пункта 3.13. Из (19) вытекает, что g_1 и g_2 являются образующими группы S_Z.

Из замечаний 1 и 2 и равенства (18) вытекает утверждение леммы 3.19.

3.21. Пусть μ — правоинвариантная мера Хаара * на группе H. Тогда μ естественным образом индуцирует на фактор-пространстве H / H_Z меру, которую мы обозначим через $\tilde{\mu}$.

Лемма. *Мера всего фактор-пространства H / H_Z относительно меры $\tilde{\mu}$ конечна* (*т. е.* $\tilde{\mu}(H/H_Z) < \infty$).

Доказательство. Прежде всего отметим, что относительно определений, которые будут использоваться в этом доказательстве, надо смотреть [6]. После этого сделаем следующие замечания:

Замечание 1. Из определения арифметической подгруппы алгебраической группы сразу следует, что H_Z является в H арифметической подгруппой.

Замечание 2. Обозначим через A подгруппу группы H, состоящую из вещественных унимодулярных матриц вида $\begin{pmatrix} a & b & 0 \\ c & d & 0 \\ 0 & 0 & 1 \end{pmatrix}$. Легко видеть, что H является полупрямым произведением A и S (определение S см. пункт 3.10). С другой стороны, 1) так как A, как легко видеть, изоморфна $SL(2, \mathbf{R})$ (группа вещественных унимодулярных матриц второго порядка), а $SL(2, \mathbf{R})$, как хорошо известно (см., например, [8]) — простая группа, то A — простая группа, 2) S — унипотентная группа. Из последних двух предложений вытекает, что H не имеет нетривиальных рациональных характеров.

Из замечаний 1 и 2 и теоремы 9.4 в [6] следует утверждение леммы.

3.22. Лемма. *У единичного представления группы H найдется такая окрестность V, что любое унитарное представление группы H, нетривиальное на S, не лежит в V.*

Доказательство. Из лемм 2 и 3 работы [2] сразу следует, что у единичного представления группы H найдется такая окрестность V, что любое *неприводимое* унитарное представление группы H, нетривиальное на S, не лежит в V. Отсюда, из теоремы о разложении любого унитарного представления в прямой интеграл неприводимых (см. [9]) и определения существенно нетривиального на S представления группы H (см. пункт 3.14) легко следует утверждение леммы.

3.23. Доказательство леммы 3.18. Как и прежде, для любой локально-компактной группы G через $\tilde{G}$ будем обозначать пространство унитарных представлений с топологией, описанной в пункте 3.17.

* Определение меры Хаара см. в [7].

Рассмотрим отображение φ: $\hat{H}_Z \to \hat{H}$ — индуцирование в смысле Фробениуса (или в терминологии [3] — индуцирование в смысле Макки). Лемма 3.18 немедленно следует из двух свойств этого отображения:

а) φ непрерывно,

б) если $p \in \hat{H}_Z$ существенно нетривиально на S_Z, то $\varphi(p)$ существенно нетривиально на S.

Свойство а) легко вытекает из леммы 3.19 и результатов работы [10] (см. также [2, 3]).

Свойство б) сразу следует из определения φ.

ЛИТЕРАТУРА

1. Pinsker M. S. On the Complexity of a Concentrator. 7th International Teletraffic Congress. Stockholm, 1973.
2. Каждан Д. А. О связи дуального пространства группы со строением ее замкнутых подгрупп. Функциональный анализ и его приложения, 1967, **1**, *1*, 71—74.
3. Delaroche C. et Kirillov A. Sur les relations entre l'espace dual d'un groupe et la structure de ses sous-groupes fermes, Sem. Bourbaki, N 343, Juin 1968.
4. Гельфанд И. М., Граев М. Н., Виленкин Н. Я. Интегральная геометрия и связанные с ней вопросы теории представлений. Обобщенные функции, **5**, М., Физматгиз, 1962.
5. Ганнинг Р. К. Лекции о модулярных формах. Математика (сб. перев.), 1964, **8**, *6*, 3—68.
6. Борель А., Хариш-Чандра. Арифметические подгруппы алгебраических групп. Математика (сб. перев.), 1964, 8, *2*, 19—71.
7. Понтрягин Л. С. Непрерывные группы. М., Гостехиздат, 1954.
8. Семинар «Софус Ли». Теория групп Ли, топология групп Ли. М., Изд-во иностр. лит., 1962.
9. Dixmier J. Les C^*-algebras et leurs representations. Gauthier — Villars, Paris, 1964.
10. Fell M. G. Weak Containment and Induced Representation of Groups. Canadien J. Math., 1962, **14**, *2*, 237—262.

Поступила в редакцию
2 июня 1972 г.