S©MR ISSN 1813-3304

СИБИРСКИЕ ЭЛЕКТРОННЫЕ
МАТЕМАТИЧЕСКИЕ ИЗВЕСТИЯ

Siberian Electronic Mathematical Reports
http://semr.math.nsc.ru

Том 12, стр. 960–966 (2015) УДК 519.147
DOI 10.17377/semi.2015.12.082 MSC 05C50

ОЦЕНКИ РАЗМЕРА НОСИТЕЛЯ ВЕКТОРОВ В КООРДИНАТНО-ТРАНЗИТИВНЫХ ЛИНЕЙНЫХ ПРОСТРАНСТВАХ

С.В. АВГУСТИНОВИЧ, О.Г. ПАРШИНА

Abstract. We discuss the minimum distance problem of some transitive linear spaces. A minimal support of vectors in monogenerated coordinate-transitive spaces problem is solved for ones generated by a vector of weight 2. In the case of generating vector of weight 3 some conjectures are provided by computer experiments. Attainable lower bound on the support cardinality with respect to dimension of linear space is obtained. Also a connection between full-rank criterion for vector and tilings of groups is mentioned.

Keywords: transitive linear spaces, support of a vector, code distance, minimum distance problem.

1. Введение

Хорошо известно [1, 2], что проблема определения размера минимального носителя ненулевых векторов произвольного линейного пространства (над $GF(2)$, над $\mathbb{Z}$ или над $\mathbb{R}$ — в равной степени) является NP-трудной. В некотором смысле эта задача эквивалентна определению кодового расстояния линейного кода, заданного своей порождающей матрицей. Кроме прочего, является естественным желание задать базис линейного пространства максимально компактным образом. Во многих значимых случаях упомянутое пространство априорно имеет богатую группу автоморфизмов. Скажем, собственные пространства транзитивных графов именно таковы. Таким образом задача поиска

Avgustinovich, S.V., Parshina, O.G., On vectors of minimal support in transitive linear spaces.

Исследование выполнено за счет гранта Российского научного фонда (проект №14-11-00555).

Поступила 26 ноября 2015 г., опубликована 11 декабря 2015 г.

векторов с минимально возможным носителем в транзитивных линейных пространствах представляется нам актуальной.

Пусть L произвольное линейное подпространство размерности k в евклидовом пространстве E^n, координаты которого проиндексированы множеством $M = \{0, 1, 2, \ldots, n-1\}$. Группой автоморфизмов $Aut(L)$ пространства L будем считать множество всех подстановок на M, оставляющих L на месте. В том случае, когда $Aut(L)$ действует на M транзитивно, будем говорить, что L является координатно транзитивным пространством. Для построения координатно транзитивного линейного пространства можно действовать следующим образом. Рассмотрим транзитивную группу подстановок G, регулярно действующую на множестве $M = \{0, 1, 2, \ldots, n-1\}$. В этом случае можно считать, что M является просто множеством номеров элементов группы G. Для произвольного вектора v из E^n определим линейное замыкание $L_G(v)$ как линейную оболочку вектора v и всех его образов (эти образы мы будем называть сдвигами вектора v) под действием элементов группы G. Заметим, что G является подгруппой группы $Aut(L_G(v))$, а обратное верно не всегда. Везде в дальнейшем мы будем иметь дело с координатно-транзитивными линейными пространствами, полученными вышеописанным способом, называя их однопорожденными. Нас будет интересовать вопрос о размере минимального носителя ненулевых векторов произвольного однопорожденного координатно транзитивного линейного пространства для фиксированных группы G и вектора v. Забегая вперед скажем, что сложностной статус этой проблемы нам неизвестен, хотя и кажется, что она может иметь отношение к проблеме изоморфизма графов Кэли.

2. Некоторые свойства координатно транзитивных линейных пространств

Назовем *весом* $W(v)$ вектора $v = (v_0, v_1, v_2, ..., v_{n-1})$ число его ненулевых координат (фактически — размер носителя). Не теряя общности везде в дальнейшем будем считать, что $v_0 = 1$. Обозначим через $P_G(v)$ минимальный вес векторов из $L_G(v)$. Вектор называется *однородным*, если все его ненулевые компоненты равны 1, и *полуоднородным*, если компоненты из множества $\{0, +1, -1\}$. Во всех остальных случаях векторы неоднородные. Каждому однородному вектору v можно поставить в соответствие подмножество $B(v)$ элементов группы G, отвечающих единичным компонентам. В некотором смысле v является характеристическим вектором для множества $B(v)$. Замкнув $B(v)$ относительно групповой операции, получим подгруппу $O(v)$ группы G, и будем ее называть *орбитой* вектора v. В случае, когда $B(v)$ совпадает с орбитой, такой вектор назовем *орбитным*.

Довольно очевидно, что вопрос о минимальном носителе вектора сводится к тому же вопросу в рамках его орбиты.

Вектор будем называть *уравновешенным*, если сумма всех его компонент равна нулю. Легко понять, что множество уравновешенных векторов образует линейное пространство (обозначим его U_n), размерность которого на 1 меньше размерности всего пространства. Ясно также, что ни один орт не принадлежит U_n, а все полуоднородные векторы веса 2 принадлежат, поэтому размер минимального носителя векторов в U_n равен 2. Будем говорить, что вектор v — *полного ранга*, если $L_G(v) = E^n$, $L_G(v)$ в таком случае *полноранговое*. В противном случае ранг вектора неполон.

Нам также понадобится дополнительное определение. Вектор будем называть *редуцируемым*, если в $L_G(v)$ найдется вектор меньшего веса, чем $W(v)$. Изучение $P_G(v)$ будет обычно сводиться к следующему. Если v полноранговый, то $P_G(v) = 1$, в противном случае встает вопрос о его редуцируемости к вектору промежуточного веса.

Заметим, что $L_G(v)$ порождается ровно n векторами (сдвигами v), а это означает, что любая нетривиальная линейная зависимость этих векторов влечет неполноранговость $L_G(v)$.

3. Случай векторов веса два

Если вектор v имеет вес два, то вопрос о мощности носителя порождаемого им линейного подпространства $L_G(v)$ сводится к тому, является ли оно полноранговым. Заметим, что в произвольной группе G орбита вектора v веса два циклическая, поскольку $B(v)$ содержит, кроме единичного, еще ровно один элемент, который и порождает циклическую подгруппу. В случае, когда вектор v имеет полный ранг, $P_G(v) = 1$, иначе $P_G(v) = 2$, и, в отличие от случая, когда вектор имеет вес $s \geq 3$, других возможных вариантов нет.

Везде в дальнейшем, говоря о циклической группе мы будем считать, что ее элементы пронумерованы числами от 0 до $n-1$, а групповая операция аддитивна.

Теорема 1. *Пусть G — циклическая группа порядка $n = 2^k \cdot q$, где q — нечётно. Рассмотрим однородный вектор v веса 2 такой, что $v_0 = v_a = 1$. Тогда*

$$P_G(v) = \begin{cases} 1, & \text{если } 2^k | a, \\ 2, & \text{иначе.} \end{cases}$$

Доказательство. Пусть $A \leq G$ - подгруппа, порожденная элементом a. $A =< a >= \{0, a, 2a, ..., (|A|-1)a\}$. Рассмотрим набор представителей смежных классов по этой подгруппе в G: $0 = b_0, b_1, ..., b_t$, где $t = |G|/|A|$. Группа G может быть представлена в виде объединения смежных классов по подгруппе A: $G = (b_0 + A) \bigcup (b_1 + A) \bigcup ... \bigcup (b_t + A)$.

Пусть $2^k \nmid a$. В этом случае необходимо показать, что существует нетривиальная линейная комбинация векторов множества $L_G(v)$, равная нулю. Для этого приведем два подходящих вектора для v: l и w, где $l = (1/2, 1/2, ..., 1/2)$,

$$w_x = \begin{cases} 1, & x = b_i + s \cdot a, s \text{ - чет}, i = 0, 1, \ldots, t, \\ 0, & \text{иначе.} \end{cases}$$

Каждый из этих векторов вместе с вектором v образует линейную комбинацию, равную единичному вектору $\overline{\mathbf{1}}$. Вычтем первую линейную комбинацию из второй и получим искомую нетривиальную нулевую линейную комбинацию векторов. Таким образом пространство, порожденное вектором v, неполноранговое, а значит, не существует линейной комбинации векторов из $L_G(v)$, образующей орт, т. е. вектор веса 1.

Пусть теперь $2^k | a$. Рассматривая знакопеременную сумму циклических сдвигов вектора v, несложно убедиться в том, что эта сумма образует орт. □

Из теоремы 1 вытекает, что для распознавания полноранговости вектора веса 2 в поизвольной группе достаточно выяснить четность его орбиты.

Заметим также, что неоднородный вектор веса два в любой группе имеет полный ранг, а полуоднородный всегда неполноранговый.

4. О полноранговости векторов веса три в циклическом случае

Рассмотрим множество $L_G(v)$, где $v = (v_1, v_2, ..., v_n)$ — однородный вектор. Нетрудно видеть, что $L_G(v) = E^n$ тогда и только тогда, когда определитель следующей матрицы отличен от нуля:

$$V = \begin{pmatrix} v_1 & v_2 & ... & v_n \\ v_n & v_1 & ... & v_{n-1} \\ \vdots & \vdots & \ddots & \vdots \\ v_2 & v_3 & \dots & v_1 \end{pmatrix}$$

Матрица V носит название *циркулянт*, её определитель (см., например, [3]) равен $\prod\limits_{k=0}^{n-1} f(\varepsilon_k)$, где $f(x) = \sum\limits_{l=0}^{n-1} v_{l+1} \cdot x^l$, $\varepsilon_k = \cos(\frac{2\pi k}{n}) + i\sin(\frac{2\pi k}{n})$, k — целое.

Вопрос о полноранговости порождаемого некоторым вектором v подпространства сводится к вопросу о невырожденности соответствующей ему матрицы V. Для того, чтобы определитель V был равен нулю, необходимо равенство нулю хотя бы одного из значений $f(\varepsilon_k)$. Рассмотрим данный полином для некоторого $\varepsilon_k = \cos(\frac{2\pi k}{n}) + i\sin(\frac{2\pi k}{n}) = e^{i\cdot\frac{2\pi k}{n}}$. Без ограничения общности считаем, что $v_1 = 1$, тогда $f(\varepsilon_k) = 1 + \sum\limits_{l=1}^{n-1} v_{l+1} \cdot e^{i\cdot\frac{2\pi k}{n} l} = 1 + \sum\limits_{l=1}^{n-1} v_{l+1} \cdot e^{i\cdot\frac{2\pi kl}{n}} = 0, v_l \in \{0, 1\}$. Для выполнения равенства необходимы следующие условия:

1. $\sum\limits_{l=1}^{n-1} v_{l+1} \sin(\frac{2\pi kl}{n}) = 0$;
2. $\sum\limits_{l=1}^{n-1} v_{l+1} \cos(\frac{2\pi kl}{n}) = -1$.

Если эти условия не выполняются, то определитель матрицы отличен от нуля, пространство $L_G(v)$ полноранговое, а значит содержит орт — вектор веса 1. В случае выполнения данных условий можно лишь утверждать, что размер минимального носителя $L_G(v)$ не меньше 2.

Для случая, когда вес вектора v равен 3, эти условия принимают более простой вид. Пусть $B(v) = \{0, l, h\}$, тогда определитель соответствующей вектору v циркулянтной матрицы равен $f(x) = 1 + e^{i\cdot\frac{2\pi kl}{n}} + e^{i\cdot\frac{2\pi kh}{n}}$, $1 < l < h \leq n$.

Условия 1. и 2. в этом случае можно переписать следующим образом:

1. $\sin(\frac{2\pi kl}{n}) + \sin(\frac{2\pi kh}{n}) = 0 \Leftrightarrow 2\sin(\frac{\pi k(h+l)}{n})\cos(\frac{\pi k(h-l)}{n}) = 0$
$\Leftrightarrow \sin(\frac{\pi k(h+l)}{n}) = 0 \Leftrightarrow \frac{\pi k(h+l)}{n} = \pi s, s \in \mathbb{Z} \Leftrightarrow k = \frac{ns}{h+l}$;

2. $\cos(\frac{2\pi kl}{n}) + \cos(\frac{2\pi kh}{n}) = -1 \Leftrightarrow \cos(\frac{\pi k(h+l)}{n})\cos(\frac{\pi k(h-l)}{n}) = -\frac{1}{2}$
$\Leftrightarrow \cos(\pi s)\cos(\frac{\pi k(h-l)}{n}) = -\frac{1}{2}$.

Далее в пункте 2. возможны два варианта:

2.а. s - нечётно, $\cos(\frac{\pi k(h-l)}{n}) = \frac{1}{2} \Leftrightarrow \frac{\pi k(h-l)}{n} = \pm\frac{\pi}{3} + 2\pi r, r \in \mathbb{Z}$
$\Leftrightarrow \frac{s(h-l)}{h+l} = \pm\frac{1}{3} + 2r \Leftrightarrow s = \frac{(h+l)(6r\pm1)}{3(h-l)} \in \mathbb{Z} \Leftrightarrow 3|(h+l)$.

2.b. s — четно, $\cos(\frac{\pi k(h-l)}{n}) = -\frac{1}{2} \Leftrightarrow \frac{\pi k(h-l)}{n} = \pm\frac{2\pi}{3} + 2\pi r, r \in \mathbb{Z}$
$\Leftrightarrow s = \frac{(h+l)(6r\pm 2)}{3(h-l)} \Leftrightarrow 3|(h+l)$.

Нетрудно видеть, что полученные из пунктов 1. и 2. условия $3|(h+l)$ и $k = \frac{ns}{h+l}$ эквивалентны следующим:

1') $3|n$;
2') $l \equiv 1 \bmod 3$, $h \equiv 2 \bmod 3$.

В группе Z_n, где n кратно трем, рассмотрим подгруппу H порядка $n/3$. Однородный вектор v веса 3 называется *репрезентативным*, если множество $B(v)$ содержит ровно по одному представителю каждого смежного класса подгруппы H, иначе вектор *нерепрезентативный*.

Используя введенную выше терминологию, условия 1'), 2') можно переформулировать следующим образом:

Теорема 2. *Пусть n кратно трем. Однородный вектор веса три имеет полный ранг над группой Z_n тогда и только тогда, когда он не является репрезентативным.*

Заметим, как следствие, что для некратных трем n любой вектор веса три над группой Z_n имеет полный ранг.

5. О редуцируемости векторов веса 3

Как показано в предыдущем параграфе, все нерепрезентативные векторы веса 3 являются полноранговыми и редуцируются к векторам веса 1. Осталось рассмотреть случай репрезентативных векторов и исследовать вопрос их редуцируемости к векторам веса 2.

Нетрудно показать, что все орбитные векторы в Z_n являются нередуцируемыми. Действительно, сдвиги такого вектора либо совпадают с ним самим, либо имеют непересекающийся с ним носитель.

Вычисления с помощью стандартных компьютерных программ показали, что все остальные неполноранговые однородные векторы редуцируются к полуоднородным векторам веса 2 для циклических групп вплоть до порядка $n = 18$. Мы предполагаем, что данная ситуация в циклических группах сохраняется для всех остальных порядков.

6. Заключение

В предыдущем параграфе было замечено, что орбитные векторы являются нередуцируемыми в циклической группе. Ясно, что и в произвольной группе это свойство орбитных векторов сохранится. Мы можем сказать больше.

Предложение 1. *Пусть L — произвольное координатно транзитивное линейное подпространство размерности k в E^n. Тогда минимальный размер $P(L)$ нетривиального носителя векторов из L удовлетворяет неравенству*

$$P(L) \geq n/k \tag{1}$$

Доказательство. Рассмотрим вектор v из L минимального веса и квадратную матрицу M порядка n, строками которой являются все образы вектора v под действием элементов группы G. Некоторые строки могут совпадать. Если $P(L) < n/k$, то мы без труда выберем в нашей матрице больше k линейно независимых векторов, следя за тем, чтобы каждый новый вектор своими ненулевыми координатами покрывал какую-либо новую координату. Заметим, при таком подходе равенство в (1) достигается лишь тогда, если носители всех выбранных векторов не пересекаются между собой. Это в свою очередь возможно лишь если L порождено вектором, носитель которого соответствует некоторому однородному орбитному вектору. □

Завершая заметку, хотелось бы сделать ряд замечаний. Каждому однородному вектору v можно поставить в соответствие граф Кэли группы G с множеством порождающих $B(v)$. Граф этот будет ориентированным и связным на орбите вектора v и ее смежных классах. Из общих соображений ясно, что для решения рассматриваемой нами задачи могут оказаться полезными инварианты описанного графа, и в частности - его собственных пространств и ориентированных совершенных раскрасок. Также нам представляется интересным ответить на следующий вопрос. Пусть v и w - два произвольных вектора одинаковой длины. Как распознать совпадение или изоморфизм порожденных ими линейных пространств $L_G(v)$ и $L_G(w)$? Как минимум, такое совпадение не произойдет, если размеры минимальных носителей векторов в этих пространствах различны.

В наших рассмотрениях практически отсутствовали пространства, порожденные неоднородными векторами. В этом случае пришлось бы иметь в виду совокупную рациональную сравнимость компонент таких векторов, что значительно усложняет анализ.

Кажется естественным исследовать поведение минимального носителя для циркулянтных матриц и однородных порождающих векторов. В этом случае прослеживается определенная связь с понятием тайлинга циклической группы [4, 5]. Действительно, дополняемость вектора до тайлинга автоматически означает его неполноранговость.

Пара (A, T) подмножеств группы G образует ее *тайлинг*, если каждый элемент $g \in G$ может быть однозначно представлен в виде $g = t + a$, где $t \in T, a \in A$. Два вектора образуют тайлинг группы G, если их представители образуют тайлинг.

Вектор v *дополняемый*, если существует такой вектор w, что пара (v, w) образует тайлинг группы G. Вектор w назовем *дополняющим* для вектора v.

Предложение 2. *Если вектор v дополняемый, то его ранг неполон.*

Доказательство. Пусть существует вектор w такой, что пара (v, w) — тайлинг группы G. Это значит, что существует линейная комбинация элементов множества $L_G(v)$, порождающая единичный вектор $\overline{\mathbf{1}} = (1, 1, ...1)$: $\sum_{i=1}^{n} \alpha_i \cdot v^{g_i} = \overline{\mathbf{1}}$. Так как речь идет об однородных векторах, $\alpha_i \in \{0, 1\}$. Подействовав на данное равенство неединичным элементом h группы G, получим: $\sum_{i=1}^{n} \alpha_i \cdot v^{h(g_i)} = \overline{\mathbf{1}}$

Разность этих равенств дает нетривиальную линейную зависимость сдвигов вектора v, а это значит, что он имеет неполный ранг. □

References

[1] A. Vardy, *Algoritmic complexity in coding theory and the minimum distance problem.* STOC '97 (El Paso, TX), 92–109 (electronic), ACM, New York, 1999. MR1715628

[2] E.R. Berlekamp, R.J. McEliece, H.C. A.van Tilborg, *On the inherent intractability of certain coding problems.* IEEE Trans. Inform. Theory, **24** (1978), 384–386. MR0495180

[3] D.M. Cvetković, M.Doob, H.Sachs, *Spectra of Graphs. Theory and Application.* Second edition. VEB Deutscher Verlag der Wissenschaften, Berlin, 1982. 368 pp. MR0690768

[4] M. Dinitz, *Full rank tilings of finite abelian groups.* SIAM J. Discrete Math., **20** (2006), 160–170. MR2257253

[5] D.K. Zhukov, *Tilings of p-ary cyclic groups.* Siberian Electronic Mathematical Reports, **10** (2013), 562–565. MR3262315

Sergey Vladimirovich Avgustinovich
Sobolev Institute of Mathematics,
pr. Koptyuga, 4,
630090, Novosibirsk, Russia
E-mail address: avgust@math.nsc.ru

Olga Gennad'evna Parshina
Sobolev Institute of Mathematics,
pr. Koptyuga, 4,
630090, Novosibirsk, Russia
E-mail address: parolja@gmail.com