ДИСКРЕТНЫЙ АНАЛИЗ И ИССЛЕДОВАНИЕ ОПЕРАЦИЙ
Октябрь–декабрь 2022. Т. 29, № 4. С. 104–123

УДК 519.115.5 DOI 10.33048/daio.2022.29.747

О СУЩЕСТВОВАНИИ РАЗБИЕНИЙ, ПРИМИТИВНЫХ ПО АГИЕВИЧУ

Ю. В. Тарannиков[1, 2]

[1] Московский государственный университет им. М. В. Ломоносова, Ленинские горы, 1, 119991 Москва, Россия

[2] Московский центр фундаментальной и прикладной математики Ленинские горы, 1, 119991 Москва, Россия

E-mail: yutarann@gmail.com

Аннотация. Доказано, что для любого натурального m существует наименьшее натуральное $N = N_q(m)$ такое, что при $n > N$ не существует A-примитивных разбиений пространства $\mathbf{F}_q^n$ на q^m аффинных подпространств размерности $n - m$. Получены нижние и верхние оценки на величину $N_q(m)$. Доказано, что $N_q(2) = q + 1$. Результаты того же типа установлены для разбиений на грани. Библиогр. 16.

Ключевые слова: аффинное подпространство, разбиение пространства, оценка, бент-функция, координатное подпространство, грань, ассоциативный блок-дизайн.

Введение

Пусть q — степень простого числа. Достаточно широко известна задача разбиения пространства $\mathbf{F}_q^n$ на линейные подпространства L_i:

$$\{L_i\}\colon \bigsqcup_i (L_i \setminus \{0\}) = \mathbf{F}_q^n \setminus \{0\},$$

где L_i — линейные подпространства, как правило, одинаковой размерности, но рассматривались и наборы различных размерностей. Задача эта не такая простая, но интересная, с большим числом приложений и активно изучавшаяся (см., например, [1, 2]). Исследователей интересовало в основном существование разбиений и их структура; количество разбиений, как правило, не оценивалось.

Исследование выполнено при финансовой поддержке Министерства науки и высшего образования России в рамках программы Московского центра фундаментальной и прикладной математики (соглашение № 075–15–2022–284).

В отличие от упомянутой выше задачи, практически не изучалась задача о разбиении $\mathbf{F}_q^n$ на аффинные подпространства $E_i = L_i + b_i$, где L_i — линейное подпространство, $b_i \in \mathbf{F}_q^n$:

$$\{E_i\}\colon \bigsqcup_i E_i = \mathbf{F}_q^n.$$

Возможно причина в том, что она имеет тривиальное решение: достаточно взять все $L_i = L$, а в качестве b_i — представителей классов смежности (такое разбиение указано в начале работы [3], где в роли L выступает q-ичный код Хэмминга, после чего рассмотрение переходит к разбиению $\mathbf{F}_q^n$ на неэквивалентные совершенные коды — тоже достаточно популярной теме). Поскольку задача тривиальна и не было приложений, требующих нетривиальных разбиений, её не рассматривали.

В 2008 г. такое приложение обнаружил Агиевич, исследуя построения бент-функций в работе [4]; там же он исследовал некоторые количественные и структурные свойства разбиений $\mathbf{F}_q^n$ на аффинные подпространства.

В последние пару лет появилось несколько новых публикаций на эту тему: в [5, 6] получены оценки на число разбиений $\mathbf{F}_2^n$ на аффинные подпространства, а в [7] найдена асимптотика логарифма числа разбиений $\mathbf{F}_2^n$ на аффинные подпространства размерности два, что позволило улучшить асимптотическую нижнюю оценку на логарифм числа булевых бент-функций и превзойти асимптотику логарифма числа бент-функций из пополненного семейства Майораны — МакФарланда, которое до этого считалось самым большим из известных. Подробнее о бент-функциях и других криптографически важных функциях см. в [8].

В [4] Агиевич ввёл понятие примитивного разбиения. Рассмотрим разбиение $\{E_i\}$: $\bigsqcup_i E_i = \mathbf{F}_q^n$, где E_i — аффинные подпространства пространства $\mathbf{F}_q^n$, $E_i = L_i + b_i$, L_i — соответствующие линейные подпространства пространства $\mathbf{F}_q^n$, $b_i \in \mathbf{F}_q^n$. Положим $W = \bigcap_i L_i$. Агиевич назвал разбиение $\{E_i\}$ *примитивным,* если $W = \{0\}$.

С нашей точки зрения в данном контексте использование термина «примитивный» небесспорно, поскольку он характеризует скорее некоторую невырожденность разбиения. Кроме того, подобного рода невырожденность можно определять разными способами, а слово «примитивный» в математике вообще перегружено. В то же время предлагать другой термин тоже представляется неправильным, поэтому будем в дальнейшем называть такое разбиение *примитивным по Агиевичу* или *A-примитивным.*

Обратим также внимание на ещё одну серию публикаций. Как упомянуто выше, в ряде работ рассматривались разбиения пространства $\mathbf{F}_q^n$

на совершенные коды (как правило, при $q = 2$). Поскольку совершенные коды могут быть нелинейными, это несколько другая задача. Однако в части статей изучались разбиения только на сдвиги линейных совершенных кодов (т. е. кодов Хэмминга), а это уже подзадача задачи о разбиении на аффинные подпространства с ограничением на вид L_i. При этом в [9] Хеден и Соловьёва рассматривали разбиение на взаимно непараллельные коды Хэмминга; под *взаимной непараллельностью* понималось требование $L_i \neq L_j$ при $i \neq j$. Кротов пошёл ещё дальше и изучал в [10] разбиения на максимально непараллельные коды Хэмминга, ставя задачей максимизацию величины $\min\limits_{i \neq j}(\dim\langle L_i \cup L_j\rangle - \dim L_i)$.

Заметим, что свойства A-примитивности и взаимной непараллельности не вкладываются друг в друга. Так, увеличивая n на 1 и добавляя ко всем подпространствам взаимно непараллельного разбиения новый базисный вектор, получим снова взаимно непараллельное разбиение, которое не будет A-примитивным. При этом некоторые из A-примитивных разбиений, приводимых ниже, будут содержать повторяющиеся L_i, т. е. не будут взаимно непараллельными.

Ещё одним частным случаем разбиений на аффинные подпространства, получившим внимание исследователей, являются ассоциативные блок-дизайны (АБД). Нам будет удобнее обсудить их в разд. 3.

В настоящей статье главное внимание уделяется вопросу существования A-примитивных разбиений. Основные результаты представлены в аннотации.

1. Технические сведения и вспомогательные результаты

Приведём необходимые определения, а определения, данные во введении, повторять не будем.

Пусть q — степень простого числа. Конечное поле порядка q обозначается через $\mathbf{F}_q$, линейное пространство векторов длины n над $\mathbf{F}_q$ — через $\mathbf{F}_q^n$, сумма векторов u и v из $\mathbf{F}_q^n$ — через $u+v$, а произведение вектора u на константу $\lambda \in \mathbf{F}_q$ — через λu. Если L — линейное подпространство пространства $\mathbf{F}_q^n$, а $b \in \mathbf{F}_q^n$, то под аффинным подпространством $E = L + b$ понимается множество всех векторов вида $u + b$, где $u \in L$.

Для любой пары $u = (u_1, \ldots, u_n)$ и $v = (v_1, \ldots, v_n)$ векторов из $\mathbf{F}_q^n$ их *внутреннее*[1] *произведение,* обозначаемое через (u, v), определяется так:

$$(u, v) = u_1 v_1 + \cdots + u_n v_n, \tag{1}$$

[1] Внутреннее произведение также очень часто называют скалярным, но над конечным полем или кольцом такое произведение не является в полном смысле скалярным, поскольку не выполнено свойство «квадрат равен нулю только на нулевом векторе».

где умножение и сложение выполняются над $\mathbf{F}_q$. Говорят, что векторы u и v *ортогональны*, и пишут $u \perp v$, если $(u, v) = 0$. Если L — линейное подпространство в $\mathbf{F}_q^n$, то через $L^\perp$ обозначается множество всех таких векторов v, что $v \perp u$ для любого $u \in L$. Легко понять и широко известно, что $L^\perp$ само является линейным подпространством в $\mathbf{F}_q^n$. Подпространство $L^\perp$ называется *ортогональным* к L. Напомним, что для пространств над конечными полями ортогональное подпространство не обязательно является ортогональным дополнением, в отличие, например, от евклидова случая.

Если C — произвольное подмножество $\mathbf{F}_q^n$, то его *линейной оболочкой* (или *линейным замыканием*) $\langle C \rangle$ называется множество всех векторов, представимых в виде линейных комбинаций над $\mathbf{F}_q$ векторов из C. Легко понять, что $\langle C \rangle$ является линейным подпространством пространства $\mathbf{F}_q^n$.

Следующая лемма широко известна, но мы докажем её для полноты изложения.

Лемма 1. *Пусть q — степень простого числа, L — линейное подпространство пространства $\mathbf{F}_q^n$, $u \notin L^\perp$. Тогда внутреннее произведение (x, u) при x, пробегающем L, принимает каждое из q значений одинаковое число раз.*

Доказательство. Из $u \notin L^\perp$ следует, что существует $x_0 \in L$ такое, что $(x_0, u) = \mu_0 \neq 0$. Тогда для любого $\mu \in \mathbf{F}_q$, $\mu \neq 0$, отображение $x \to \mu x$ переводит L в себя, причём внутреннее произведение $(x, u) = \mu_0$ переходит в $(\mu x, u) = \mu\mu_0$. Отсюда следует, что любое ненулевое значение внутреннего произведения встречается не реже, чем любое другое ненулевое значение, поэтому все ненулевые значения принимаются как результат внутреннего произведения одинаковое число раз.

Далее, рассмотрим отображение $x \to x - x_0$. Это отображение переводит L в себя, причём внутреннее произведение $(x, u) = \mu_0$ переходит в $(x - x_0, u) = \mu_0 - \mu_0 = 0$. В свою очередь, отображение $x \to x + x_0$ переводит L в себя, причём внутреннее произведение $(x, u) = 0$ переходит в $(x + x_0, u) = \mu_0$. Отсюда следует, что нулевое значение внутреннего произведения встречается столько же раз, сколько любое ненулевое, и, таким образом, внутреннее произведение (x, u) при x, пробегающем L, принимает каждое из q значений одинаковое число раз. Лемма 1 доказана.

Из леммы 1 немедленно получаем

Следствие 1. *Пусть q — степень простого числа, $E = L + b$ — аффинное подпространство пространства $\mathbf{F}_q^n$ и $u \notin L^\perp$. Тогда внутреннее произведение (x, u) при x, пробегающем E, принимает каждое из q значений одинаковое число раз.*

2. A-примитивные разбиения

В этом разделе получим результаты о существовании A-примитивных разбиений.

Лемма 2. *Пусть q — степень простого числа, $\{E_i = L_i + b_i\}$ — A-примитивное разбиение пространства $\mathbf{F}_q^n$. Тогда* $\dim \left\langle \bigcup\limits_{i=1}^{q^m} L_i^\perp \right\rangle = n$.

Доказательство. Предположим, напротив, что $\dim \left\langle \bigcup\limits_{i=1}^{q^m} L_i^\perp \right\rangle < n$. Тогда найдётся ненулевой вектор $u \in \mathbf{F}_q^n$ такой, что $u \perp \left\langle \bigcup\limits_{i=1}^{q^m} L_i^\perp \right\rangle$. Значит, u принадлежит всем L_i, что противоречит A-примитивности разбиения $\{E_i\}$. Лемма 2 доказана.

Теорема 1. *Пусть q — степень простого числа. Для любого натурального m существует наименьшее натуральное $N = N_q(m)$ такое, что при $n > N$ не существует A-примитивных разбиений $\mathbf{F}_q^n$ на q^m аффинных подпространств размерности $n - m$.*

Доказательство. Пусть $\{E_i = L_i + b_i\}$ — A-примитивное разбиение пространства $\mathbf{F}_q^n$. Из леммы 2 следует, что $n = \dim \left\langle \bigcup\limits_{i=1}^{q^m} L_i^\perp \right\rangle \leqslant mq^m$. Теорема 1 доказана.

Следствие 2. $N_q(m) \leqslant mq^m$.

Заметим, что Агиевич в [4] фактически доказал, что $N_q(1) = 1$ для любого q, равного степени простого числа, и $N_2(2) = 3$.

Для дальнейшего усиления верхней оценки на $N_q(m)$ сформулируем два дополнительных соображения.

Лемма 3. *Пусть $\{E_i\}$ — разбиение пространства $\mathbf{F}_q^n$ на q^m аффинных подпространств размерности $n - m$, $n \geqslant 2m$. Тогда для любых $i \neq j$ выполнено $L_i^\perp \cap L_j^\perp \neq \{0\}$.*

Доказательство. Предположим противное. Пусть $L_i^\perp \cap L_j^\perp = \{0\}$ для некоторых i, j. Если $L_i^\perp = \langle \{l^{i,1}, \ldots, l^{i,m}\} \rangle$, $L_j^\perp = \langle \{l^{j,1}, \ldots, l^{j,m}\} \rangle$, то $E_i \cap E_j$ есть множество решений системы из $2m$ уравнений с n неизвестными:

$$\{(x - b_i, l^{i,t}) = 0,\ t = 1, \ldots, m;\ (x - b_j, l^{j,t}) = 0,\ t = 1, \ldots, m\}.$$

В силу линейной независимости системы векторов $\{l^{i,t}, l^{j,t}\}$, $t = 1, \ldots, m$, и условия $n \geqslant 2m$ (неизвестных не меньше чем уравнений) эта система имеет решение. Следовательно, аффинные подпространства E_i и E_j

пересекаются, что противоречит тому, что они входят в разбиение. Полученное противоречие доказывает лемму. Лемма 3 доказана.

Лемма 4. *Пусть $\{E_i\}$ — разбиение пространства $\mathbf{F}_q^n$ на q^m аффинных подпространств размерности $n-m$. Тогда для любого $u \in \mathbf{F}_q^n$ число содержащих вектор u ортогональных подпространств $L_i^\perp$ делится на q.*

Доказательство. Нулевой вектор, очевидно, принадлежит всем q^m подпространствам $L_i^\perp$. Пусть $u \in \mathbf{F}_q^n$, $u \neq 0$. Если $u \notin L_i^\perp$, то внутреннее произведение (x,u) при x, пробегающем E_i, в силу следствия 1 принимает каждое из q значений одинаковое число раз. Если же $u \in L_i^\perp$, то внутреннее произведение (x,u) при x, пробегающем E_i, принимает фиксированное значение, и, стало быть, при $y = x + b_i$, пробегающем E_i, внутреннее произведение (y,u) принимает также фиксированное значение. В силу того, что $u \notin (\mathbf{F}_q^n)^\perp = \{0\}$, по лемме 1 внутреннее произведение (x,u) при x, пробегающем $\mathbf{F}_q^n$, принимает каждое из q значений одинаковое число раз. Отсюда число $L_i^\perp$, содержащих u, должно делиться на q. Лемма 4 доказана.

Теорема 2. *Пусть q — степень простого числа. Тогда $N_q(m) \leqslant mq^{m-1}$.*

Доказательство. Пусть $\{E_i\}$ — A-примитивное разбиение $\mathbf{F}_q^n$ на q^m аффинных подпространств размерности $n-m$. В силу леммы 2 выполнено $\dim \left\langle \bigcup\limits_{i=1}^{q^m} L_i^\perp \right\rangle = n$. Построим базис $U = \{u_1, \ldots, u_n\}$ пространства $\mathbf{F}_q^n$ следующим образом. Будем последовательно просматривать подпространства $L_j^\perp$, $j = 1, 2, \ldots$, и если $\dim \left\langle \bigcup\limits_{i=1}^{j} L_i^\perp \right\rangle - \dim \left\langle \bigcup\limits_{i=1}^{j-1} L_i^\perp \right\rangle = \delta > 0$, то в U добавим δ линейно независимых векторов, принадлежащих $L_j^\perp$, но не принадлежащих $\left\langle \bigcup\limits_{i=1}^{j-1} L_i^\perp \right\rangle$.

По построению каждый из базисных векторов $u_1, \ldots, u_n$ принадлежит хотя бы одному $L_i^\perp$ и, стало быть, по лемме 4 принадлежит не менее чем q подпространствам $L_i^\perp$. Тем самым общее число вхождений базисных векторов из U в $\bigcup\limits_{i=1}^{q^m} L_i^\perp$ не меньше чем qn. С другой стороны, каждое $L_i^\perp$ содержит не более чем m векторов из U. Отсюда для числа S вхождений векторов из U в $\bigcup\limits_{i=1}^{q^m} L_i^\perp$ имеем

$$qn \leqslant S \leqslant mq^m$$

и, следовательно,

$$n \leqslant mq^{m-1}.$$

Теорема 2 доказана.

Лемма 5. *Пусть q — степень простого числа. Тогда $N_q(2) \leqslant q+1$.*

Доказательство. Пусть $\{E_i\}$ — А-примитивное разбиение $\mathbf{F}_q^n$ на q^2 аффинных подпространств размерности $n-2$. В силу леммы 2 выполнено $\dim \left\langle \bigcup\limits_{i=1}^{q^2} L_i^\perp \right\rangle = n$. Поменяем, если нужно, нумерацию подпространств $L_j^\perp$, $j = 1, \ldots, q^2$, так, чтобы для первых j, пока это возможно, возрастало значение величины $\dim \left\langle \bigcup\limits_{i=1}^{j} L_i^\perp \right\rangle$, т. е. выполнялось условие

$$\dim \left\langle \bigcup_{i=1}^{j} L_i^\perp \right\rangle - \dim \left\langle \bigcup_{i=1}^{j-1} L_i^\perp \right\rangle > 0.$$

Ввиду леммы 3 получим $\dim(L_j^\perp \cap L_1^\perp) > 0$ при $j \geqslant 2$, поэтому при $j = 2, \ldots, n-1$ подпространство $L_j^\perp$ будет иметь вид $L_j^\perp = \langle v_{j,1}, v_{j,2} \rangle$, где $v_{j,1} \in (L_1^\perp \setminus \{0\})$, $v_{j,2} \notin \left\langle \bigcup\limits_{i=1}^{j-1} L_i^\perp \right\rangle$.

Подпространство $L_1^\perp$ содержит q^2-1 ненулевых векторов, каждое из подпространств $L_2^\perp, \ldots, L_{n-1}^\perp$ по построению содержит q^2-q векторов, не содержащихся в уже рассмотренных подпространствах. Значит, объединение подпространств $\bigcup\limits_{i=1}^{n-1} L_i^\perp$ содержит не менее чем $(q^2-1)+(n-2)\times(q^2-q)$ различных ненулевых векторов из $\mathbf{F}_q^n$, поэтому по лемме 4 общее число вхождений ненулевых векторов из $\mathbf{F}_q^n$ в $\bigcup\limits_{i=1}^{q^2} L_i^\perp$ не меньше чем $q((q^2-1)+(n-2)(q^2-q))$. С другой стороны, каждое $L_i^\perp$ содержит в точности q^2-1 ненулевых векторов из $\mathbf{F}_q^n$, поэтому для числа S вхождений ненулевых векторов из $\mathbf{F}_q^n$ в $\bigcup\limits_{i=1}^{q^2} L_i^\perp$ имеем

$$q((q^2-1)+(n-2)(q^2-q)) \leqslant S = (q^2-1)q^2,$$

откуда

$$n \leqslant q + 2 - \frac{1}{q}.$$

Учитывая целочисленность n, получаем

$$n \leqslant q+1.$$

Лемма 5 доказана.

Заметим, что непосредственное применение техники доказательства леммы 5 позволяет улучшить и оценку теоремы 2, но незначительно,

поэтому не будем приводить соответствующие достаточно громоздкие рассуждения и выкладки.

Справедливо следующее рекуррентное неравенство.

Теорема 3. *Пусть q — степень простого числа. Тогда*

$$N_q(m+1) \geqslant q \cdot N_q(m) + 1.$$

Доказательство. Обозначим через $\mathbf{F}_q = \{a_0, a_1 \ldots, a_{q-1}\}$ элементы поля $\mathbf{F}_q$. Пусть $\{E_i\} = \{L_i + b_i\}$, $i = 1, \ldots, q^m$, — A-примитивное разбиение $\mathbf{F}_q^n$ на q^m аффинных подпространств размерности $n - m$. Построим A-примитивное разбиение $\{E_i\}$ пространства $\mathbf{F}_q^{qn+1}$ на q^{m+1} аффинных подпространств размерности $qn-m$. Множество базисных векторов пространства $\mathbf{F}_q^{qn+1}$ обозначим через $U = \{e_1, \ldots, e_{qn+1}\}$.

Определим $\mathbf{S}_j$, $j \in \{0, 1, \ldots, q-1\}$, как копию пространства $\mathbf{F}_q^n$, натянутую на множество базисных векторов $U_j = \{e_{jn+1}, e_{jn+2}, \ldots, e_{(j+1)n}\}$ и являющуюся подпространством пространства $\mathbf{F}_q^{qn+1}$ (во всех компонентах, не вошедших в U_j, все векторы из $\mathbf{S}_j$ имеют нулевые значения).

Подпространство L и вектор b, взятые в j-й копии $\mathbf{S}_j$ пространства $\mathbf{F}_q^n$, будем обозначать $L[\mathbf{S}_j]$ и $b[\mathbf{S}_j]$ соответственно. Сами $L[\mathbf{S}_j]$ и $b[\mathbf{S}_j]$ будем рассматривать как лежащие уже в $\mathbf{F}_q^{qn+1}$.

Определим $\widehat{\mathbf{S}}_j$, $j \in \{0, 1, \ldots, q-1\}$, как копию пространства $\mathbf{F}_q^{(q-1)n}$, натянутую на множество базисных векторов $\widehat{U}_j = U \setminus (U_j \cup e_{qn+1})$ и являющуюся подпространством пространства $\mathbf{F}_q^{qn+1}$ (во всех компонентах, не вошедших в $\widehat{U}_j$, все векторы из $\mathbf{S}_j$ имеют нулевые значения).

Зададим совокупность из q^{m+1} аффинных подпространств:

$$\{E_{i,j}\} = \{L_{i,j} + b_{i,j}\}, \quad L_{i,j} = \langle L_i[\mathbf{S}_j], \widehat{\mathbf{S}}_j \rangle, \quad b_{i,j} = b_i[\mathbf{S}_j] + a_j e_{qn+1},$$
$$i = 1, \ldots, q^m,\ j = 0, 1, \ldots, q-1.$$

По построению каждое из заданных подпространств имеет размерность $(n-m) + (q-1)n = qn - m$.

Пусть $(i', j') \neq (i'', j'')$. Если $j' \neq j''$, то аффинные подпространства $E_{i',j'}$ и $E_{i'',j''}$ не пересекаются, потому что в последней $(qn+1)$-й компоненте все векторы из $E_{i',j'}$ имеют значение $a_{j'}$, а все векторы из $E_{i'',j''}$ — значение $a_{j''}$. Если же $j' = j'' = j$ и $i' \neq i''$, то аффинные подпространства $E_{i',j}$ и $E_{i'',j}$ не пересекаются, поскольку совокупность аффинных подпространств $\{E_i\}$ является разбиением $\mathbf{F}_q^n$. Следовательно, совокупность аффинных подпространств $\{E_{i,j}\}$ действительно является разбиением $\mathbf{F}_q^{qn+1}$.

Покажем теперь, что никакой ненулевой вектор w из $\mathbf{F}_q^{qn+1}$ не принадлежит одновременно всем $\{L_{i,j}\}$. У ненулевого вектора w есть ненулевая компонента. Можно считать, что эта компонента не последняя, потому

что по построению у всех векторов из всех $L_{i,j}$ последняя компонента нулевая. Тогда ненулевая компонента вектора w принадлежит какому-то множеству компонент U_j, $j \in \{0, 1, \ldots, q-1\}$. Вектор w при ограничении на множество компонент U_j даёт ненулевой вектор $\widetilde{w}$ длины n. Из A-примитивности разбиения $\{E_i\}$ следует, что некоторое L_i не содержит $\widetilde{w}$. Отсюда вытекает, что линейное подпространство $L_{i,j}$ не содержит вектора w. Это доказывает, что разбиение $\{E_{i,j}\}$ A-примитивно. Теорема 3 доказана.

Из рекуррентной оценки теоремы 3 вытекает нижняя оценка на величину $N_q(m)$.

Теорема 4. *Пусть q — степень простого числа. Тогда*

$$N_q(m) \geqslant \frac{q^m - 1}{q - 1}.$$

Доказательство. В качестве основания индукции можно взять значение $L_q(1) = 1$ [4] или даже $L_q(0) = 0$ (очевидно, хотя и вычурно).

Индуктивный переход заключается в использовании теоремы 3. Пусть $N_q(m) \geqslant \frac{q^m-1}{q-1}$. Тогда

$$N_q(m+1) \geqslant q \cdot N_q(m) + 1 \geqslant q \cdot \frac{q^m - 1}{q - 1} + 1 = \frac{q^{m+1} - 1}{q - 1}.$$

Теорема 4 доказана.

Заметим, что в конструкции из теоремы 3 можно сделать множества U_j пересекающимися. Тогда при переходе от m к $m+1$ размерность пространства можно увеличить с n до любого числа из отрезка от $n+1$ до $qn+1$. Отсюда легко следует

Теорема 5. *Пусть q — степень простого числа, m — натуральное число. Тогда A-примитивное разбиение пространства $\mathbf{F}_q^n$ на q^m аффинных подпространств размерности $n-m$ существует при любом натуральном n в отрезке от m до $\frac{q^m-1}{q-1}$.*

Заметим, что при $n > \frac{q^m-1}{q-1}$ отсутствие «дырок» в множестве значений размерности пространств, для которых существует A-примитивное разбиение, не является априори очевидным.

Полученные результаты позволяют установить точное значение величины $N_q(2)$ для любого q, являющегося степенью простого числа (напомним, в [4] Агиевич фактически сделал это для $q = 2$).

Теорема 6. *Пусть q — степень простого числа. Тогда*

$$N_q(2) = q + 1.$$

Доказательство немедленно следует из леммы 5 и теоремы 4.

3. A-примитивные разбиения на грани

Аффинное подпространство $E = L + b$ называется *координатным* (и известно также как *грань*), если базисные векторы подпространства L содержатся среди фиксированных базисных векторов $e_1, \ldots, e_n$ всего пространства $\mathbf{F}_q^n$.

Предполагается, что базис $\{e_1, \ldots, e_n\}$ пространства $\mathbf{F}_q^n$ задан и зафиксирован. Тогда линейное подпространство L размерности $n-m$ определяется выбором $n-m$ из n базисных векторов. Для задания аффинного подпространства нужно дополнительно задать вектор $b \in \mathbf{F}_q^n$. Несложно понять, что b можно выбрать таким образом, чтобы он имел нули во всех компонентах, соответствующих базисным векторам подпространства L.

Разбиение на грани является частным случаем разбиения на аффинные подпространства, но разбиение на грани можно рассмотреть и для q, не являющегося степенью простого числа. Действительно, базисные векторы $\{e_1, \ldots, e_n\}$ не содержат компонент, отличных от 0 и 1, поэтому в их линейных комбинациях не используется умножение, отличное от умножения на 0 и 1. Ортогональным к координатному линейному подпространству L объявляется координатное линейное подпространство $L^\perp$, базис которого состоит из тех и только тех векторов из $\{e_1, \ldots, e_n\}$, которые не входят в базис L (и поэтому для координатных подпространств, в отличие от произвольных подпространств, ортогональное подпространство можно называть ортогональным дополнением). Внутреннее произведение двух q-значных векторов при q, не являющемся степенью простого, в общем случае не для всех целей может быть задано соотношением (1), поскольку умножение не будет групповым, но при проверке ортогональности векторов u и v, $u \in L$, $v \in L^\perp$, формулу (1) можно использовать, поскольку при её применении не возникнет произведения ненулевых элементов.

Исходя из сказанного выше, можно говорить о разбиении на аффинные координатные подпространства (грани) и при q, не являющемся степенью простого, только рассматриваться эти подпространства будут не в $\mathbf{F}_q^n$, а в $\mathbf{Z}_q^n$. Также можно применять использовавшуюся в предыдущих разделах технику работы с ортогональными подпространствами.

Каждую грань $E = L + b$ размерности $n - m$ в $\mathbf{Z}_q^n$ можно задать как набор длины n из звёздочек и чисел из $\mathbf{Z}_q$, причём чисел в точности m. Звёздочки стоят в компонентах, соответствующих базисным векторам подпространства L, числа стоят в остальных компонентах, причём число, стоящее в j-й компоненте, равно значению j-й компоненты набора b.

Разбиение $\{E_i\}$ пространства $\mathbf{Z}_q^n$ на грани можно задать матрицей размера $q^m \times n$. Для того чтобы такая матрица задавала разбиение, она должна удовлетворять

критерию непересечения граней: *для каждой пары строк должен быть столбец с разными числами в этих строках.*

Действительно, все наборы, содержащиеся в грани, можно получить произвольными доопределениями всех звёздочек строки числами из $\mathbf{Z}_q^n$. Для того чтобы из двух строк доопределениями не получился один набор (и тем самым эти две грани не пересеклись бы), как раз необходим и достаточен критерий непересечения граней.

То, что каждый набор из $\mathbf{Z}_q^n$ попадёт в какую-то грань, гарантируется числом строк в матрице. В матрице в точности q^m строк, каждая задаёт грань с q^{n-m} наборами, все грани вместе содержат $q^m q^{n-m} = q^n$ наборов, грани не пересекаются, поэтому каждый набор попадёт ровно в одну грань и, таким образом, матрица действительно задаст разбиение на грани.

Для того чтобы разбиение, задаваемое матрицей, было A-примитивным, матрица должна удовлетворять

критерию A-примитивности: *в матрице не должно быть столбца из одних звёздочек.*

Действительно, если j-й столбец матрицы состоит из одних звёздочек, то базисный вектор e_j принадлежит всем L_i, поэтому разбиение не будет A-примитивным. Если же i-я строка матрицы содержит в j-м столбце число, то базисный вектор e_j не принадлежит L_i вместе со всеми линейными комбинациями базисных векторов, в которые он входит с ненулевым коэффициентом (напомним, умножения на 0 и 1 у нас разрешены).

Заметим, что частным случаем разбиения на грани являются *ассоциативные блок-дизайны* (АБД), которые были введены Ривестом [11] для использования в алгоритмах хэширования и изучались в ряде работ (см., например, [12, 13]). АБД — это разбиение $\mathbf{Z}_2^n$ на грани одинаковой размерности с дополнительным требованием: в матрице разбиения каждый столбец содержит одно и то же число звёздочек. Из определения очевидно, что АБД является A-примитивным разбиением.

При переносе результатов со случая разбиения $\mathbf{F}_q^n$ на аффинные подпространства на случай разбиения $\mathbf{Z}_q^n$ на грани небольшую техническую трудность представляет использование внутреннего произведения. Будем продолжать его использование в соответствии с формулой (1), следя за тем, чтобы не возникало произведения элементов $\mathbf{Z}_q$, одновременно отличных и от нуля, и от единицы. В последующих леммах этого раздела под L_i и $L_i^\perp$ понимаются только координатные линейные подпространства.

Лемма 6. *Пусть $q \geqslant 2$ — натуральное число, L — линейное координатное подпространство пространства $\mathbf{Z}_q^n$, а $u \in \mathbf{Z}_q^n \setminus L^\perp$ — вектор, все*

компоненты которого принимают только значения из множества $\{0,1\}$. *Тогда внутреннее произведение* (x,u) *при* x, *пробегающем* L, *принимает каждое из* q *значений одинаковое число раз.*

Доказательство. Из того, что $u \notin L^{\perp}$, следует, что существует компонента j, в которой значение вектора u равно 1, а $e_j \in L$. Сгруппируем наборы координатного подпространства L в группы по q наборов, отличающихся только в j-й компоненте. Пусть G — одна из таких групп. Тогда легко видеть, что при x, пробегающем G, внутреннее произведение (x,u) принимает каждое из q значений ровно один раз. Рассмотрев все группы, получаем, что при x, пробегающем L, внутреннее произведение (x,u) принимает каждое из q значений одинаковое число раз. Лемма 6 доказана.

Из леммы 6 немедленно получаем

Следствие 3. *Пусть* $q \geqslant 2$ — *натуральное число,* $E = L + b$ — *аффинное координатное подпространство пространства* $\mathbf{Z}_q^n$, *а* $u \in \mathbf{Z}_q^n \setminus L^{\perp}$ — *вектор, все компоненты которого принимают только значения из множества* $\{0,1\}$. *Тогда внутреннее произведение* (x,u) *при* x, *пробегающем* E, *принимает каждое из* q *значений одинаковое число раз.*

Лемма 7. *Пусть* $\{E_i\}$ — *разбиение пространства* $\mathbf{Z}_q^n$ *на* q^m *координатных аффинных подпространств размерности* $n-m$, *а* $u \in \mathbf{Z}_q^n$ — *вектор, все компоненты которого принимают только значения из множества* $\{0,1\}$. *Тогда число содержащих набор* u *ортогональных подпространств* $L_i^{\perp}$ *делится на* q.

Доказательство. Нулевой набор, очевидно, принадлежит всем q^m подпространствам $L_i^{\perp}$. Пусть $u \neq 0$. Если $u \notin L_i^{\perp}$, то внутреннее произведение (x,u) при x, пробегающем E_i, в силу следствия 3 принимает каждое из q значений одинаковое число раз. Если же $u \in L_i^{\perp}$, то внутреннее произведение (x,u) при x, пробегающем E_i, принимает фиксированное значение и, стало быть, при $y = x + b_i$, пробегающем E_i, внутреннее произведение (y,u) принимает также фиксированное значение. В силу того, что $u \notin (\mathbf{Z}_q^n)^{\perp} = \{0\}$, по лемме 6 внутреннее произведение (x,u) при x, пробегающем $\mathbf{Z}_q^n$, принимает каждое из q значений одинаковое число раз. Отсюда число $L_i^{\perp}$, содержащих u, должно делиться на q. Лемма 7 доказана.

Лемма 8. *Пусть* $\{E_i\}$ — *разбиение пространства* $\mathbf{Z}_q^n$ *на* q^m *координатных аффинных подпространств размерности* $n-m$, *а* $u \in \mathbf{Z}_q^n$. *Тогда число содержащих набор* u *ортогональных подпространств* $L_i^{\perp}$ *делится на* q.

Доказательство. По вектору u построим набор $\delta(u)$, заменив все ненулевые компоненты вектора u на 1. Для вектора $\delta(u)$ заключение леммы 8 справедливо в силу леммы 7. Легко видеть, что наборы u и $\delta(u)$ принадлежат или не принадлежат каждому из координатных линейных подпространств $L_i^\perp$ одновременно. Следовательно, заключение леммы 8 справедливо и для вектора u. Лемма 8 доказана.

Следствие 4. *Пусть $\{E_i = L_i + b_i\}$ — разбиение пространства $\mathbf{Z}_q^n$ на грани одинаковой размерности. Тогда множество $\{L_i\}$ соответствующих этому разбиению координатных линейных подпространств распадается на группы из q совпадающих.*

Доказательство. Пусть $E = L + b$ — грань из разбиения $\{E_i\}$. Рассмотрим вектор u, равный 0 в компонентах, соответствующих базисным векторам подпространства L, и равный 1 в компонентах, соответствующих базисным векторам подпространства $L^\perp$. По построению $u \in L^\perp$. По лемме 7 вектор u должен содержаться в делящемся на q числе подпространств $L_i^\perp$, но, очевидно, в силу того, что u имеет m ненулевых компонент, он не может содержаться ни в каком координатном линейном подпространстве размерности m кроме $L^\perp$, поэтому подпространство L входит в $\{L_i\}$ делящееся на q число раз. Следствие 4 доказано.

Следствие 5. *Не существует взаимно непараллельных разбиений пространства $\mathbf{Z}_q^n$ на грани одинаковой размерности.*

Утверждение следствия 4 ранее сформулировано и доказано Потаповым [14, предложение 4] для $q = 2$, но доказательство дословно подходит для любого q. Ещё раньше аналогичное утверждение было сформулировано и доказано для АБД в [15, теорема 9.7(4)], доказательство дословно подходит для любого разбиения на грани и для любого q.

Заметим, что утверждения, аналогичные следствиям 4 и 5, не будут верными для разбиений пространства $\mathbf{F}_q^n$ на произвольные (не обязательно координатные) аффинные подпространства в силу того, что в рассуждениях из доказательства утверждения 4 вектор u может содержаться в этом случае в разных подпространствах $L_i^\perp$.

Пример 1. Существует взаимно непараллельное A-примитивное разбиение пространства $\mathbf{F}_2^3$ на 2^2 аффинных подпространств размерности $3 - 2 = 1$:

$$E_1 = \{(000), (001)\} = \langle e_3 \rangle,$$
$$E_2 = \{(100), (110)\} = \langle e_2 \rangle + e_1,$$
$$E_3 = \{(011), (111)\} = \langle e_1 \rangle + e_2 + e_3,$$
$$E_4 = \{(010), (101)\} = \langle e_1 + e_2 + e_3 \rangle + e_2.$$

Рекурсивно подставляя это разбиение в конструкцию из теоремы 3, получаем взаимно непараллельные A-примитивные разбиения пространства $\mathbf{F}_2^n$ на 2^m аффинных подпространств размерности $n-m$ для $n = 2^m - 1$, $m = 2, 3, \ldots$.

Для удобства будущих ссылок сформулируем в явном виде утверждения предыдущих разделов, перенесённые на разбиения на грани.

Лемма 9. *Пусть $\{E_i = L_i + b_i\}$ — A-примитивное разбиение пространства $\mathbf{Z}_q^n$ на грани. Тогда* $\dim \left\langle \bigcup\limits_{i=1}^{q^m} L_i^{\perp} \right\rangle = n$.

Теорема 7. *Пусть $q \geqslant 2$. Для любого натурального m существует наименьшее натуральное $N = N_q^{\mathrm{coord}}(m)$ такое, что при $n > N$ не существует A-примитивных разбиений $\mathbf{Z}_q^n$ на q^m граней размерности $n - m$.*

Поскольку при q, являющемся степенью простого числа, разбиение на грани будет частным случаем разбиения на аффинные подпространства, справедливо

Утверждение 1. *Пусть q — степень простого числа. Тогда*

$$N_q^{\mathrm{coord}}(m) \leqslant N_q(m).$$

Теорема 8. *Пусть $q \geqslant 2$. Тогда $N_q^{\mathrm{coord}}(m) \leqslant mq^{m-1}$.*

Доказательство аналогично доказательству теоремы 2 с использованием леммы 8. При формировании множества U дополнительно требуем, чтобы в множество U включались только базисные векторы пространства. Таким образом, после окончания процедуры формирования множества U получим $U = \{e_1, \ldots, e_n\}$. Теорема 8 доказана.

Можно переформулировать доказательство теоремы 8 на языке матрицы разбиения на грани. Зададим A-примитивное разбиение на грани матрицей размера $q^m \times n$. В каждой строке ровно m чисел, всего чисел в матрице mq^m, в матрице нет столбца из одних звёздочек, а количество чисел в каждом столбце делится на q, поэтому число столбцов не превышает mq^{m-1}.

Несложно видеть, что конструкция теоремы 3 сохраняет свойство разбиения быть координатным. Тем самым такая же рекуррентная оценка верна и для разбиения на грани.

Теорема 9. *Пусть $q \geqslant 2$. Тогда $N_q^{\mathrm{coord}}(m+1) \geqslant q \cdot N_q^{\mathrm{coord}}(m) + 1$.*

Теорема 10. *Пусть $q \geqslant 2$. Тогда $N_q^{\mathrm{coord}}(m) \geqslant \frac{q^m-1}{q-1}$.*

Теорема 11. *Пусть $q \geqslant 2$, m — натуральное число. Тогда A-примитивное разбиение пространства $\mathbf{Z}_q^n$ на q^m граней размерности $n - m$ существует при любом натуральном n в отрезке от m до $\frac{q^m-1}{q-1}$.*

Лемма 10. *Пусть $q \geqslant 2$. Тогда $N_q^{\mathrm{coord}}(2) \leqslant q+1$.*

Доказательство. Можно действовать аналогично доказательству леммы 5 с использованием леммы 8, в качестве базисных векторов подпространств $L_i^{\perp}$ выбирая базисные векторы пространства, а можно поступить проще. По следствию 4 множество из всех q^2 граней разобьётся на q групп из q параллельных граней в каждой группе. Первая из этих групп даст вклад в $\dim \langle \cup L_i^{\perp} \rangle$, равный 2, каждая из последующих групп в силу критерия непересечения граней будет добавлять к этой величине не более единицы. Отсюда $n \leqslant q+1$. Лемма 10 доказана.

Теорема 12. *Пусть $q \geqslant 2$. Тогда $N_q^{\mathrm{coord}}(2) = q+1$.*

Доказательство немедленно следует из леммы 10 и теоремы 10.

Из доказательства леммы 10 несложно видеть, что максимальное значение $N_q^{\mathrm{coord}}(2) = q+1$ будет достигаться только на таких разбиениях $\mathbf{Z}_q^n$ на грани размерности $n-2$, в которых все $L_i^{\perp}$ содержат общий базисный вектор пространства $\mathbf{Z}_q^n$, а каждый из остальных $n-1 = q$ базисных векторов $\mathbf{Z}_q^n$ является вторым базисным вектором в точности в q подпространствах $L_i^{\perp}$.

Заметим, что для АБД при $m > 3$ доказано неравенство $n \leqslant \binom{m}{2}$ [16]. Сравнение этой квадратичной по m верхней оценки с экспоненциальной нижней оценкой $N_2^{\mathrm{coord}}(m) \geqslant 2^m - 1$ теоремы 10 представляется сильным аргументом в пользу того, что в матрицах разбиений на грани, на которых достигаются величины $N_q^{\mathrm{coord}}(m)$, распределение звёздочек по столбцам очень неравномерно.

4. О числе разбиений на аффинные подпространства

Пусть q — степень простого числа. В [4] приведена формула для числа различных неупорядоченных разбиений пространства $\mathbf{F}_q^n$ на q^m аффинных подпространств размерности $n-m$:

$$c_q(n,m) = \sum_{d=0}^{n-m} \binom{n}{d}_q c_q^*(n-d,m), \tag{2}$$

где $c_q(n,m)$ — число различных неупорядоченных разбиений пространства $\mathbf{F}_q^n$ на q^m аффинных подпространств размерности $n-m$; $c_q^*(n,m)$ — число различных неупорядоченных A-примитивных разбиений пространства $\mathbf{F}_q^n$ на q^m аффинных подпространств размерности $n-m$; $\binom{n}{d}_q$ — число различных d-мерных подпространств пространства $\mathbf{F}_q^n$. Хорошо известно, что

$$\binom{n}{d}_q = \frac{\prod\limits_{i=0}^{d-1}(q^n - q^i)}{\prod\limits_{i=0}^{d-1}(q^d - q^i)}. \tag{3}$$

Делая в (2) замену $h = n-d$, учитывая, что $\binom{n}{d}_q = \binom{n}{n-d}_q$ (поскольку d-мерное подпространство однозначно задаётся ортогональным к нему $(n-d)$-мерным подпространством, и наоборот), а также принимая во внимание, что по теореме 1 при $n > N_q(m)$ не существует A-примитивных разбиений $\mathbf{F}_q^n$ на q^m аффинных подпространств размерности $n-m$, получаем

$$c_q(n,m) = \sum_{h=m}^{N_q(m)} \binom{n}{h}_q c_q^*(h,m). \tag{4}$$

Заметим, что при фиксированных q и m сумма в (4) содержит конечное число слагаемых.

Пусть q (степень простого числа) и m фиксированы, $n \to \infty$. Легко видеть, что $\binom{n}{h}_q = o\left(\binom{n}{h'}_q\right)$ при фиксированных натуральных $h < h'$, откуда

$$c_q(n,m) \sim \binom{n}{N_q(m)}_q c_q^*(N_q(m),m). \tag{5}$$

Раскрывая число подпространств в (5) по формуле (3) и переходя к асимптотике, устанавливаем следующий факт.

Теорема 13. *Пусть q (степень простого числа) и m фиксированы, $n \to \infty$. Тогда*

$$c_q(n,m) \sim C q^{n \cdot N_q(m)},$$

где $C = \frac{c_q^*(N_q(m),m)}{q^{(N_q(m))^2}\left(\frac{1}{q};\frac{1}{q}\right)_{N_q(m)}}$, а величина $\left(\frac{1}{q};\frac{1}{q}\right)_{N_q(m)} = \prod\limits_{i=1}^{N_q(m)}\left(1-\frac{1}{q^i}\right)$ известна как q-символ Почхаммера.

Как видим, асимптотика числа разбиений пространства $\mathbf{F}_q^n$ на q^m аффинных подпространств одинаковой размерности при $m = \text{const}$, $n \to \infty$ в огромной степени определяется величиной $N_q(m)$, что является ещё одним аргументом в пользу её изучения.

Для разбиений на грани аналогично получаем формулу

$$c_q^{\text{coord}}(n,m) = \sum_{h=m}^{N_q^{\text{coord}}(m)} \binom{n}{h} c_q^{\text{coord}*}(h,m), \tag{6}$$

где $c_q^{\mathrm{coord}}(n,m)$ — число различных неупорядоченных разбиений $\mathbf{Z}_q^n$ на q^m граней размерности $n-m$; $c_q^{\mathrm{coord}*}(n,m)$ — число различных неупорядоченных A-примитивных разбиений пространства $\mathbf{Z}_q^n$ на q^m граней размерности $n-m$; $\binom{n}{h}$ — обычный биномиальный коэффициент.

Заметим, что при фиксированных q и m сумма в (6) содержит конечное число слагаемых.

Пусть q и m фиксированы, $n\to\infty$. Легко видеть, что $\binom{n}{h}=o\bigl(\binom{n}{h'}\bigr)$ при фиксированных натуральных $h<h'$. Отсюда

$$c_q^{\mathrm{coord}}(n,m)\sim\binom{n}{N_q^{\mathrm{coord}}(m)}c_q^{\mathrm{coord}*}(N_q^{\mathrm{coord}}(m),m),$$

и мы устанавливаем следующую теорему.

Теорема 14. *Пусть q и m фиксированы, $n\to\infty$. Тогда*

$$c_q^{\mathrm{coord}}(n,m)\sim C' n^{N_q^{\mathrm{coord}}(m)},$$

где $C'=\frac{c_q^{\mathrm{coord}*}(N_q^{\mathrm{coord}}(m),m)}{N_q^{\mathrm{coord}}(m)!}$.

Как видим, величину $N_q^{\mathrm{coord}}(m)$ мы тоже изучали не зря.

Автор благодарит коллег из МГУ им. М. В. Ломоносова и Института математики им. С. Л. Соболева за содержательные обсуждения, а также анонимного рецензента за полезные замечания, способствовавшие улучшению качества статьи.

ЛИТЕРАТУРА

1. **Heden O.** A survey of the different types of vector space partitions // Discrete Math. Algorithms Appl. 2012. V. 4, No. 1. P. 1–14.
2. **Akman F., Sissokho P. A.** Reconfiguration of subspace partitions // J. Comb. Des. 2022. V. 30, No. 1. P. 5–18.
3. **Августинович С. В., Соловьёва Ф. И., Хеден У.** О разбиениях n-куба на неэквивалентные совершенные коды // Пробл. передачи информ. 2007. Т. 43, № 4. С. 45–50.
4. **Agievich S. V.** Bent rectangles // Boolean functions in cryptology and information security. Amsterdam: IOS Press, 2008. P. 3–22. (NATO Sci. Peace Secur. Ser. D: Inf. Commun. Secur.; V. 18).
5. **Баксова И. П., Таранников Ю. В.** Об одной конструкции бент-функций // Обозрение прикл. и промышл. математики. 2020. Т. 27, № 1. С. 64–66.
6. **Баксова И. П., Таранников Ю. В.** Оценки числа разбиений пространства $\mathbf{F}_2^m$ на аффинные подпространства размерности k // Вестн. Моск. ун-та. Сер. 1. Математика, механика. 2022. № 3. С. 21–25.

7. **Potapov V. N., Taranenko A. A., Tarannikov Yu. V.** Asymptotic bounds on numbers of bent functions and partitions of the Boolean hypercube into linear and affine subspaces. Ithaca, NY: Cornell Univ., 2021. (Cornell Univ. Libr. e-Print Archive; arXiv:2108.00232).
8. **Логачёв О. А., Сальников А. А., Смышляев С. В., Ященко В. В.** Булевы функции в теории кодирования и криптологии. М.: Ленард, 2021. 576 с.
9. **Heden O., Solov'eva F.** Partitions of $\mathbf{F}^n$ into non-parallel Hamming codes // Adv. Math. Commun. 2009. V. 3, No. 4. P. 385–397.
10. **Krotov D. S.** A partition of the hypercube into maximally nonparallel Hamming codes // J. Comb. Des. 2014. V. 22, No. 4. P. 179–187.
11. **Rivest R. L.** On hash-coding algorithms for partial-match retrieval // Proc. 15th Annu. Symp. Switching Automata Theory (New Orleans, USA, Oct. 14–16, 1974). Piscataway: IEEE, 1974. P. 95–103.
12. **Brouwer A. E.** On associative block designs // Combinatorics. Amsterdam: North-Holland, 1978. P. 173–184. (Colloq. Math. Soc. J. Bolyai; V. 18).
13. **Van Lint J. H.** $\{0, 1, *\}$-Distance problems in combinatorics // Surveys in Combinatorics. Inv. Pap. 10th British Comb. Conf. (Glasgow, UK, July 22–26, 1985). Cambridge: Camb. Univ. Press, 1985. P. 113–135. (Lond. Math. Soc. Lect. Notes Ser.; V. 103).
14. **Potapov V. N.** DP-colorings of uniform hypergraphs and splittings of Boolean hypercube into faces // Electron. J. Comb. 2022. V. 29, No. 3, ID P3.37. 7 p.
15. **Van Lint J. H., Wilson R. M.** A course in combinatorics. Cambridge: Camb. Univ. Press, 2001. 620 p.
16. **La Poutré J. A.** A theorem on associative block designs //Discrete Math. 1986. V. 58, No. 2. P. 205–208.

Таранников Юрий Валерьевич

Статья поступила
11 июля 2022 г.
После доработки —
28 июля 2022 г.
Принята к публикации
28 июля 2022 г.

DISKRETNYI ANALIZ I ISSLEDOVANIE OPERATSII
/DISCRETE ANALYSIS AND OPERATIONS RESEARCH/
October–December 2022. Vol. 29, No. 4. P. 104–123

UDC 519.115.5 DOI 10.33048/daio.2022.29.747

ON THE EXISTENCE OF AGIEVICH-PRIMITIVE PARTITIONS

Yu. V. Tarannikov[1,2]

[1] Lomonosov Moscow State University, Faculty of Mechanics and Mathematics,
1 Leninskie Gory, 119991 Moscow, Russia

[2] Moscow Center for Fundamental and Applied Mathematics,
1 Leninskie Gory, 119991 Moscow, Russia

E-mail: yutarann@gmail.com

Abstract. We prove that for any positive integer m there exists the smallest positive integer $N = N_q(m)$ such that for $n > N$ there are no Agievich-primitive partitions of the space $\mathbf{F}_q^n$ into q^m affine subspaces of dimension $n - m$. We give lower and upper bounds on the value $N_q(m)$ and prove that $N_q(2) = q + 1$. Results of the same type for partitions into coordinate subspaces are established. Bibliogr. 16.

Keywords: affine subspace, partition of a space, bound, bent function, coordinate subspace, face, associative block design.

REFERENCES

1. **O. Heden,** A survey of the different types of vector space partitions, *Discrete Math. Algorithms Appl.* **4** (1), 1–14 (2012).
2. **F. Akman** and **P. A. Sissokho,** Reconfiguration of subspace partitions, *J. Comb. Des.* **30** (1), 5–18 (2022).
3. **S. V. Avgustinovich, F. I. Solov'eva,** and **O. Heden,** Partitions of an n-cube into nonequivalent perfect codes, *Probl. Peredachi Inf.* **43** (4), 45–50 (2007) [Russian] [*Probl. Inf. Transm.* **43** (4), 310–315 (2007)].
4. **S. V. Agievich,** Bent rectangles, in *Boolean Functions in Cryptology and Information Security* (IOS Press, Amsterdam, 2008), pp. 3–22 (NATO Sci. Peace Secur. Ser. D: Inf. Commun. Secur., Vol. 18).
5. **I. P. Baksova** and **Yu. V. Tarannikov,** On a construction of bent functions, *Obozr. Prikl. Prom. Mat.* **27** (1), 64–66 (2020) [Russian].

This research is supported by the Ministry of Science and Higher Education of Russia as part of the program of the Moscow Center for Fundamental and Applied Mathematics (Agreement 075–15–2022–284).

English version: Journal of Applied and Industrial Mathematics **16** (4) (2022).

6. **I. P. Baksova** and **Yu. V. Tarannikov,** The bounds on the number of partitions of the space $\mathbf{F}_2^m$ into k-dimensional affine subspaces, *Vestn. Mosk. Univ., Ser. 1. Mat. Mekh.,* No. 3, 21–25 (2022) [Russian] [*Mosc. Univ. Math. Bull.* **77** (3), 131–135 (2022)].
7. **V. N. Potapov, A. A. Taranenko,** and **Yu. V. Tarannikov,** Asymptotic bounds on numbers of bent functions and partitions of the Boolean hypercube into linear and affine subspaces (Cornell Univ., Ithaca, NY, 2021) (Cornell Univ. Libr. e-Print Archive, arXiv:2108.00232).
8. **O. A. Logachev, A. A. Salnikov, S. V. Smyshlyaev,** and **V. V. Yashchenko,** *Boolean Functions in Coding Theory and Cryptography* (Lenard, Moscow, 2021) [Russian].
9. **O. Heden** and **F. I. Solov'eva,** Partitions of $\mathbf{F}^n$ into non-parallel Hamming codes, *Adv. Math. Commun.* **3** (4), 385–397 (2009).
10. **D. S. Krotov,** A partition of the hypercube into maximally nonparallel Hamming codes, *J. Comb. Des.* **22** (4), 179–187 (2014).
11. **R. L. Rivest,** On hash-coding algorithms for partial match retrieval, in *Proc. 15th Annu. Symp. Switching Automata Theory, New Orleans, USA, Oct. 14–16, 1974* (IEEE, Piscataway, 1974), pp. 95–103.
12. **A. E. Brouwer,** On associative block designs, in *Combinatorics* (North-Holland, Amsterdam, 1978), pp. 173–184 (Colloq. Math. Soc. J. Bolyai, Vol. 18).
13. **J. H. van Lint,** $\{0, 1, *\}$-distance problems in combinatorics, in *Surveys in Combinatorics* (Inv. Pap. 10th British Comb. Conf., Glasgow, UK, July 22–26, 1985) (Camb. Univ. Press, Cambridge, 1985), pp. 113–135 (Lond. Math. Soc. Lect. Notes Ser., Vol. 103).
14. **V. N. Potapov,** DP-colorings of uniform hypergraphs and splittings of Boolean hypercube into faces, *Electron. J. Comb.* **29** (3), ID P3.37, 7 p. (2022).
15. **J. H. van Lint** and **R. M. Wilson,** *A Course in Combinatorics* (Camb. Univ. Press, Cambridge, 2001), 620 p.
16. **J. A. La Poutré,** A theorem on associative block designs, *Discrete Math.* **58** (2), 205–208 (1986).

Yuriy V. Tarannikov

Received July 11, 2022
Revised July 28, 2022
Accepted July 28, 2022