Министерство образования и науки Российской Федерации

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«САРАТОВСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ИМЕНИ Н.Г. ЧЕРНЫШЕВСКОГО»

Кафедра Компьютерной алгебры и теории чисел

Применение полиномиального метода

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА

студента (ки) 4 курса 421 группы

направление (специальность) 02.03.01 Математика и компьютерные науки

Механико-математического факультета

Казанцева Максима Николаевича

Научный руководитель
к.ф-м.н., доцент А. М. Водолазов

Зав. кафедрой
зав.каф., к.ф-м.н., доцент А. М. Водолазов

Саратов 2017

ВВЕДЕНИЕ

Конечные поля стали изучаться в начале XIX в. Этому предшествовали исследования выдающихся математиков XVII и XVIII в. Но бесспорные заслуги в формировании этого понятия принадлежат Гауссу и Галуа. Длительное время конечные поля изучались и находили применение только в алгебре и теории чисел, однако в последние десятилетия грани соприкосновения теории конечных полей с разными областями математики и ее прикладными разделами существенно расширились. Теория чисел, теория полей, теория групп, алгебраическая геометрия, комбинаторика, теория кодирования - вот далеко не полный перечень разделов математики, с которыми теория успешно взаимодействует. Конечные поля обладают такими свойствами, которые присущи далеко не всем алгебраическим объектам.

В первой главе работы излагаются все необходимые алгебраические основы включающие в себя основные понятия теории групп, колец, полей, многочленов и т.д. Во второй главе подробно рассмотрено строение конечных полей, будут доказаны основные леммы и теоремы, которые понадобятся нам в дальнейшем, так же будут рассмотрены способы представления элементов конечных полей.

Во второй главе, которая является ключевой в данной работе, будет рассмотрена следующая задача: какого количества точек в $n-$мерном пространстве над конечным полем $\mathbb{F}_3$ достаточно, чтобы в нем заведомо нашлась арифметическая прогрессия длины три? Знаменитая теорема Рота говорит, что достаточно $o(3^n)$ точек. Недавно с помощью полиномиального (построения многочлена от многих переменных, зануляющегося на множестве $A \subseteq \mathbb{F}_4$ без прогрессий длины три) доказали что хватает c^n точек для некоторого $c < 3$, сначала Крут, Лев и Пах, где сделано для поля из четырех элементов, чуть позднее Эленберг и независимо от него Гийсвийт, доказали, что делается еще короче и для поля из трех элементов, рассмотрим подробнее их результаты в соответствующей главе, в которой мы так же убедимся в справедливости данной теории с помощью компьютерной программы.

Последняя глава направлена на более лучшее понимание задачи, в ней мы переформулируем основной вопрос при помощи карточной игры «Set» придуманная Маршей Фалко и выпущенная компанией Set Enterprises в 1991 году. Игра имеет богатую математическую структуру связывающую её с комбинаторикой проективных пространств и теорией исправления ошибок в коде,

будут рассмотрены частные случаи данной задачи для двумерного, трехмерного и четырехмерного векторного пространств над полем $\mathbb{F}_3$, и подтверждающие их правоту компьютерные программы, подробнее о правилах игры будет рассказано соответствующей главе.

ОСНОВНОЙ РАЗДЕЛ

В первом разделе рассматриваются основные определения и теоремы, которые используются в последующих разделах. Поскольку основным инструментом данной работы являются именно поля, то особое внимание мы обратим на определение этого понятия. Прежде всего поле есть множество F, на котором заданы две операции, называемые сложением и умножением и которое содержит два выделенных элемента 0 и e, причем $0 \neq e$. Далее, поле F - абелева группа по сложению, единичным элементом которой является 0, а элементы из F, отличные от 0, образуют абелеву группу по умножению, единичным элементом которой является e. Две операции, сложение и умножение, связаны законом дистрибутивности $a(b+c) = ab + bc$. Второй закон дистрибутивности $(b+c)a = ba + ca$ выполняется автоматически в силу коммутативности умножения. Элемент 0 называется нулевым элементом (или просто нулем), а e - единичным элементом (или просто единицей) поля F. Так же незаменимым инструментом являются многочлены, поэтому приведем необходимые определения:

Определение 16. Многочлены:

$$f(x) = \sum_{i=0}^{n} a_i x^i \text{ и } g(x) = \sum_{i=0}^{n} b_i x^i$$

Над R считаются равными тогда и только тогда, когда $a_i = b_i$ для $0 \leq i \leq n$. Определим сумму многочленов $f(x)$ и $g(x)$ равенством

$$f(x) + g(x) = \sum_{i=0}^{n} (a_i + b_i) x^i,$$

а произведение многочленов

$$f(x) = \sum_{i=0}^{m} a_i x^i \text{ и } g(x) = \sum_{j=0}^{n} b_j x^j$$

равенством

$$f(x)g(x) = \sum_{k=0}^{m+n} c_k x_k, \text{ где } c_k = \sum_{\substack{i+j=k \\ 0 \leq i \leq m, 0 \leq j \leq n}} a_i b_j.$$

Определение 17. Кольцо, образованное многочленами над кольцом R с введенными выше операциями, называется кольцом многочленом над R и обозначается через $R[x]$.

Определение 18. Многочлен $f \in F[x]$ называется неприводимым (точнее, неприводимым над полем F или в кольце $F[x]$), если он имеет положительную степень и равенство $f = gh$, $g, h \in F[x]$, может выполняться лишь в том случае, когда либо g, либо h является постоянным многочленом.

Во втором разделе излагаются основные свойства конечных полей и описываются методы построения конечных полей. Основными теоремами в данном разделе являются:

Теорема 2 (существование и единственность конечных полей). Для каждого просто числа p и каждого натурального числа числа n существует конечное поле из p^n элементов. Любое конечное поле из $q = p^n$ элементов изоморфно полю разложения многочлена $x^q - x$ над полем $\mathbb{F}_p$.

Теорема 3 (критерий подполя). Пусть $\mathbb{F}_q$ - конечное поле из $q = p^n$ элементов (p - простое число). Тогда каждое подполе поля $\mathbb{F}_q$ имеет порядок p^m, где m является положительным делителем числа n. Обратно, если m - положительный делитель числа n, то существует ровно одно подполе поля $\mathbb{F}_q$ из p^m элементов.

Лемма 5. Пусть $f \in \mathbb{F}_q[x]$ - неприводимый многочлен степени m над $\mathbb{F}_q$. Тогда $f(x)$ делит многочлен $x^{q^n} - x$ в том и только том случае, если число m делит n.

Теорема 6. Если $f \in \mathbb{F}_q[x]$ - неприводимый многочлен степени m, то в поле $\mathbb{F}_q^m$ содержится любой корень α многочлена f. Более того, все корни многочлена f просты и ими являются m различных элементов $\alpha, \alpha^q, \alpha^{q^2}, \ldots, \alpha^{q^{m-1}}$ поля $\mathbb{F}_q^m$.

Теорема 11. Пусть $n \in N$ и K - поле характеристик p, тогда

(i) Если p не делит n, то множество $E^{(n)}$ является циклической подгруппой порядка n мультипликативной группы поля $K^{(n)}$.

(ii) Если p делит n и $n = mp^e$, где $m, e \in N$ и p не делит m, то $K^{(n)} = K^{(m)}$, $E^{(n)} = E^{(m)}$ и корнями многочлена $x^n - 1$ в поле $K^{(n)}$ являются

m элементов множества $E^{(m)}$, каждый из которых имеет кратность p^e.

Теорема 12. Пусть $n \in N$ и K - поле характеристик p, тогда

(i) Если p не делит n, то множество $E^{(n)}$ является циклической подгруппой порядка n мультипликативной группы поля $K^{(n)}$.

(ii) Если p делит n и $n = mp^e$, где $m, e \in N$ и p не делит m, то $K^{(n)} = K^{(m)}$, $E^{(n)} = E^{(m)}$ и корнями многочлена $x^n - 1$ в поле $K^{(n)}$ являются m элементов множества $E^{(m)}$, каждый из которых имеет кратность p^e.

Теорема 13. Круговое поле $K^{(n)}$ является простым алгебраическим расширением поля K. Кроме того,

(i) Если $K = Q$, то $[K^{(n)} : K] = \varphi(n)$, причем круговой многочлен Q_n неприводим над K (здесь φ - функция Эйлера).

(ii) Если $K = \mathbb{F}_q$ и НОД $(q, n) = 1$, то $[K^{(n)} : K] = d$, где d - наименьшее натуральное число, такое,что $q^d \equiv 1(modn)$.При этом круговой многочлен Q_n разлагается в произведение $\varphi(n)/d$ различных нормированных неприводимых многочленов из $K[x]$ одной и той же степени d и $K^{(n)}$ является полем разложения каждого из этих многочленов.

Так же приведем примеры представления элементов конечных полей. Первый принцип основан на принципах изложенных в предыдущей главе. Заметим, что в силу теоремы 5 поле $\mathbb{F}_q$ является простым алгебраическим расширением простого поля $\mathbb{F}_p$. Действительно, если $f-$неприводимый многочлен степени n из $\mathbb{F}_p[x]$, то по теореме 6 любой корень α этого многочлена принадлежит полю $\mathbb{F}_{p^n} = \mathbb{F}_q$, и поэтому $\mathbb{F}_q = \mathbb{F}_p(\alpha)$. Значит, ввиду теоремы 2 первой главы каждый элемент поля $\mathbb{F}_q$ можно однозначно представить в виде значения некоторого многочлена от x над $\mathbb{F}_p$ степени, не превосходящей $n - 1$, при $x = \alpha$. Мы можем также рассматривать поле $\mathbb{F}_q$ как факторкольцо $\mathbb{F}_p[x]/f$.

Пример 4. Чтобы представить таким способом элементы поля $\mathbb{F}_9$, будем рассматривать $\mathbb{F}_9$ как простое алгебраическое расширение степени 2 поля $\mathbb{F}_3$, получаемое присоединением корня α неприводимого квадратного многочлена над $\mathbb{F}_3$, скажем $f(x) = x^2 + 1 \in \mathbb{F}_3[x]$. Тогда $f(\alpha) = \alpha^2 + 1 = 0$ в $\mathbb{F}_9$, и девять элементов поля $\mathbb{F}_9$ можно задать в виде $a_0 + a_1\alpha$, где $a_0, a_1\ in\mathbb{F}_3$. Точнее, $\mathbb{F}_9 = \{0, 1, 2, \alpha, 1+\alpha, 2+\alpha, 2\alpha, 1+2\alpha, 2+2\alpha\}$. Таблицы операций для $\mathbb{F}_9$ можно построить так же, как и в примере 1.62, причем корень α играет здесь ту же

роль, какую там играл класс вычетов $[x]$.

Другую возможность представления элементов поля $\mathbb{F}_q$ дает применение теорем 11 и 12. Поскольку поле $\mathbb{F}_q$ является $(q-1)-$круговым полем над $\mathbb{F}_p$, мы можем построить его, найдя разложение $(q-1)$-кругового многочлена $Q_{q-1} \in \mathbb{F}_p[x]$ на неприводимые сомножители в $\mathbb{F}_p[x]$ (все они имеют одну и ту же степень). Любой корень каждого из этих многочленов тогда является первообразным корнем $(q-1)-$й степени из единицы над $\mathbb{F}_p$, а значит, и примитивным элементом поля $\mathbb{F}_q$. Таким образом, поле $\mathbb{F}_q$ состоит из нуля и степеней этого примитивного элемента.

Пример 5. тобы применить этот способ для построения поля $\mathbb{F}_9$, заметим, что $\mathbb{F}_9 = \mathbb{F}_3^(8)$, т.е. поле $\mathbb{F}_9$ является 8-круговым полем над $\mathbb{F}_3$. Далее, следуя примеру 2.46, получаем, что $Q_8(x) = x^4 + 1 \in \mathbb{F}_3[x]$. Разложение многочлена Q_8 на неприводимые сомножители в $\mathbb{F}_3[x]$ выглядит так:

$$Q_8(x) = (x^2 + x + 2)(x^2 + 2x + 2).$$

Пусть $\xi-$корень многочлена $x^2 + x + 2$; тогда он является первообразным корнем 8-й степени из единицы над $\mathbb{F}_3$. Поскольку $\mathbb{F}_9 = \mathbb{F}_3(\xi)$, то каждый ненулевой элемент поля $\mathbb{F}_9$ можно представить подходящей степенью элемента ξ, так что $\mathbb{F}_9 = \{0, \xi, \xi^2, \xi^3, \xi^4, \xi^5, \xi^6, \xi^7, \xi^8\}$. Мы можем свести ненулевые элементы поля $\mathbb{F}_9$ в так называемую таблицу индексов, в которой указывается значение степени ξ^i, соответствующее показателю i. Для установления связи с предыдущим представлением (Пример 2) заметим, что корнем многочлена $x^2 + x + 2 \in \mathbb{F}_3[x]$ является элемент $\xi = 1 + \alpha$, где $\alpha^2 + 1 = 0$ (т.е. $\alpha-$ корень многочлена $x^2 + 1$, как и в примере 2). Поэтому таблица индексов для поля $\mathbb{F}_9$ имеет следующий вид:

i	ξ^i	i	ξ^i
1	$1+\alpha$	5	$2+2\alpha$
2	2α	6	α
3	$1+2\alpha$	7	$2+\alpha$
4	2	8	1

Из таблицы видно, что мы получаем, конечно, те же самые элементы, что и в примере 2, только в другом порядке.

Третий способ представления элементов конечного поля $\mathbb{F}_q$ осуществляется с помощью матриц. Пусть $f(x) = a_0 + a_1x + \ldots + a_{n-1}x^{n-1} + x^n$ -

нормированный многочлен положительной степени n над некоторым полем (не обязательно конечным). Его сопровождающей матрицей называется следующая квадратная матрица порядка n:

$$A = \begin{pmatrix} 0 & 0 & 0 & \dots & 0 & -a_0 \\ 1 & 0 & 0 & \dots & 0 & -a_1 \\ 0 & 10 & 0 & \dots & 0 & -a_2 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & 1 & -a_{n-1} \end{pmatrix}$$

Из линейной алгебры известно, что матрица A удовлетворяет уравнению $f(A) = O$, где $f(A)-$значение многочлена $f(x)$ при $x = A$ (будем называть его многочлен от матрицы A), т.е.

$$a_0 I + a_1 A + \ldots + a_{n-1} A^{n-1} + A^n = 0,$$

где I - единичная, а O - нулевая квадратные матрицы порядка n. Таким образом, если A - сопровождающая матрица нормированного неприводимого многочлена f степени $n \in N$ над простым конечным полем $\mathbb{F}_p$, то $f(A) = O$, и потому матрица A может играть роль корня многочлена f. Отсюда следует, что элементы поля $\mathbb{F}_{p^n}$ представляются всевозможными многочленами над $\mathbb{F}_p$ от матрицы A степеней, меньших n.

Пример 6. Как и в примере 2, пусть задан многочлен $f(x) = x^2 + 1 \in \mathbb{F}_3[x]$. Сопровождающей матрицей этого многочлена является матрица

$$A = \begin{pmatrix} 0 & 2 \\ 1 & 0 \end{pmatrix}.$$

Следовательно, поле $\mathbb{F}_9$ можно представить так:

$$\mathbb{F}_9 = \{O, I, 2I, A, I + A, 2I + A, 2A, I + 2A, 2I + 2A\}.$$

Или, в явном виде,

$$O = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \quad I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad 2I = \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}, \quad A = \begin{pmatrix} 0 & 2 \\ 1 & 0 \end{pmatrix},$$

$$I+A=\begin{pmatrix}1&2\\1&1\end{pmatrix},\quad 2I+A=\begin{pmatrix}2&2\\1&2\end{pmatrix},\quad 2A=\begin{pmatrix}0&1\\2&0\end{pmatrix},\quad I+2A=\begin{pmatrix}1&1\\2&1\end{pmatrix},$$

$$2I+2A=\begin{pmatrix}2&1\\2&2\end{pmatrix}.$$

Если поле $\mathbb{F}_9$ задано таким образом, то вычисления в этом поле проводятся по обычным правилам алгебры матриц. Например,

$$(2I+A)(I+2A)=\begin{pmatrix}2&2\\1&2\end{pmatrix}\begin{pmatrix}1&1\\2&1\end{pmatrix}=\begin{pmatrix}0&1\\2&0\end{pmatrix}=2A.$$

В третьем разделе рассматривается следующий вопрос теории чисел: какого количества точек в $n-$мерном пространстве над конечным полем $\mathbb{F}_3$ достаточно чтобы в нем заведомо нашлась арифметическая прогрессия длины три. Знаменитая теорема Рота говорит, что хватает $O(3^n)$ точек. Недавно с помощью полиномиального метода (построение многочлена от многих переменных, зануляющегося на множестве A без прогрессий длины три) была доказана.

Теорема 14 (Крут-Лев-П.Пах, 2016). Пусть $A\subseteq\mathbb{F}_4^n$ не имеет прогрессий длины три. Тогда $|A|\ll 4^{0.927n}$.

Этот метод был перенесен Элленбергом-Гийсвийтом на все группы $\mathbb{F}_q^n$. Сформулируем их результат в случае $q=3$.

Теорема 15 (Элленберг-Гийсвийт, 2016). Пусть $A\subseteq\mathbb{F}_3^n$ не имеет прогрессий длины три. Тогда $|A|\ll(2.756)^n$.

Мы же воспользуемся доказательством Федора Петрова, которое дает ту же оценку что и у Элленберга и Гийсвийта, но можно более понятно и кратко уложить. Для начала нам понадобится следующая лемма.

Лемма 6. Пусть $\mathbb{F}$ это поле, U- конечный набор и X $k-$мерное линейное подпространство пространства $\mathbb{F}^U$ функций на U. Тогда в пространстве X найдется вектор имеющий хотя бы k не нулевых координат.

Обозначим за $d(\alpha)$ количество точек в $\{0,1,2\}^n$ сумма координат которых не превосходит α, $d(\alpha)$- это размерность пространства π_α многочленов над конечным полем $\mathbb{F}_3$ (степени не выше 2 по каждой переменной) и суммарной степени не выше α.

Теорема 16. Предположим что $A \subset \mathbb{F}_3^n$ не содержащее трех разных элементов сумма которых равна нулю. Также Предположим что $N := |A| > 2d(\alpha) + d(2n - 2\alpha - 1)$ при некотором $\alpha < n$ (минимум достигается, понятно, при α примерно $2n/3$).

В последнем разделе мы переформулируем данный вопрос при помои карточный игры, правило которой подробно описаны в соответствующем разделе выпускной квалификационной работы. Сразу зададим вопрос: какое максимальное количество сар в $\mathbb{F}_3^4$. Каждой точке в этом пространстве соответствует карта, как показано на следующем примере:

(2,1,3,2) $\longleftrightarrow$ 

Первая из координат говорит нам, что на данной карте 2 фигуры, вторая указывает на заполнение, третья на цвет, и четвертая на форму. Ответ на данный вопрос нам поможет дать компьютерная программа, в ней мы рассмотрим случай для $\mathbb{F}_3^2$, в данном случае мы будем иметь 9 векторов, каждому из которых будет соответствовать своя карта, в нашем случае это будут карты красного цвета и все буду иметь форму овала, все эти карты приведены на следующем рисунке:

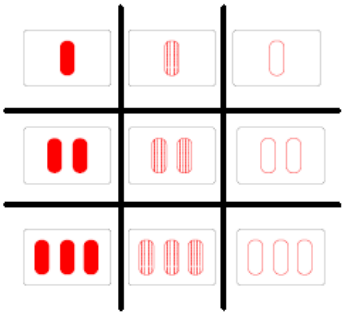

Рисунок 1

Как можно увидеть из Рисунка 5 соответствующей главы данной работы, это будут точки расположенные в углах, приведем программное доказательство

данного факта (листинг программы и его описание приведены в приложении к данной работе):

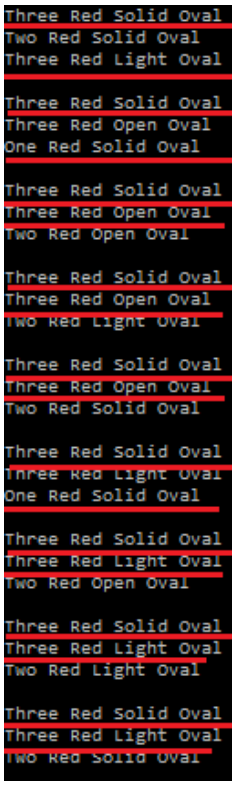

Рисунок 2

Да данном рисунке представлены тройки карт не образующие наборы, можно заметить что что подчеркнутые карты - являются искомыми, что завершает доказательство.

ЗАКЛЮЧЕНИЕ

В настоящей выпускной работе был рассмотрен одно из значимых открытий в теории чисел XXI века. В первых двух главах мы познакомились с основными понятиями теории групп, колец, полей и многочленов, так же были введены в курс строения конечных полей, теория конечных полей очень обширна, в данной работе мы ограничились, только тему понятиями которые необходимы нам при решении поставленной задачи. Так же была реализована программа, которая помогла нам наглядно убедиться в справедливости поставленной задачи. В последней главе мы переформулировали исходную задачу при помощи карточной игры, убедились в справедливости изложенных в соответствующей главе фактов при помощи реализованных компьютерных программ. Таким образом можно сказать что основная цель выпускной работы, а именно осветить одну из знаменитых задач теории чисел, в её современной интерпретации была достигнута, а поставленные задачи решены.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1 J. Bierbrauer and Y. Edel. Bounds on affine caps. J. Combin. Des., 10(2):111–115, 2002.

2 R. C. Bose. Mathematical theory of the symmetrical factorial design. Sankhy?a, 8:107–166, 1947

3 A. R. Calderbank and P. C. Fishburn. Maximal three-independent subsets of $\{0, 1, 2\}^n$. Des. Codes Cryptogr., 4(3):203–211, 1994.

4 Y. Edel. Extensions of generalized product caps. Preprint available from http://www.mathi.uni-heidelberg.de/?yves/.

5 C. J. Colbourn and A. Rosa. Triple systems. Oxford Mathematical Mono?graphs. The Clarendon Press Oxford University Press, New York, 1999.

6 Y. Edel, S. Ferret, I. Landjev, and L. Storme. The classification of the largest caps in AG(5, 3). Journal of Combinatorial Theory, Series A, 99:95–110, 2002.

7 W. Fulton and J. Harris. Representation theory, A first course. Readings in Mathematics. Springer-Verlag, New York, 1991.

8 M. Hall, Jr. Automorphisms of Steiner triple systems. IBM J. Res. Develop, 4:460–472, 1960

9 M. Hall, Jr. Steiner triple systems with a doubly transitive automorphism group. J. Combin. Theory Ser. A, 38(2):192–202, 1985.

10 R. Hill. On the largest size of cap in S5, 3. Atti Accad. Naz. Lincei Rend. Cl. Sci. Fis. Mat. Natur. (8), 54:378–384 (1974), 1973.

11 R. Hill. Caps and codes. Discrete Math., 22(2):111–137, 1978.

12 R. Hill. On Pellegrino's 20-caps in S4,3. In Combinatorics '81 (Rome, 1981), pages 433–447. North-Holland, Amsterdam, 1983.

13 R. Hill. A first course in coding theory. The Clarendon Press Oxford University Press, New York, 1986.

14 W. M. Kantor. Homogeneous designs and geometric lattices. J. Combin. The?ory Ser. A, 38(1):66–74, 1985

15 J. D. Key and E. E. Shult. Steiner triple systems with doubly transitive au?tomorphism groups: a corollary to the classification theorem for finite simple groups. J. Combin. Theory Ser. A, 36(1):105–110, 1984.

16 D. Knuth. Programs setset, setset-all, setset-random. Available from http://sunburn.stanford.edu/?knuth/programs.html

17 Roy Meshulam. On subsets of finite abelian groups with no 3-term arithmetic progressions. J. Combin. Theory Ser. A, 71(1):168–172, 1995.

18 G. Pellegrino. Sul massimo ordine delle calotte in S4,3. Matematiche (Catania), 25:149–157 (1971), 1970.

19 J. H. van Lint and R. M. Wilson. A course in combinatorics. Cambridge Uni?versity Press, Cambridge, second edition, 2001

20 Лидл Р., Нидеррайтер Г. J155 Конечные поля: В 2-х т. Т. 1. Пер. с англ. - М.: Мир, 1988. - 430 с.