УДК 20.53.23; 49.31.00

НОВЫЙ СПОСОБ ПОСТРОЕНИЯ CFF

А. В. Афанасьева
аспирантка
Санкт-Петербургский государственный университет аэрокосмического приборостроения

Предложен новый подход к построению CFF с использованием кодов, исправляющих ошибки. Показано, что для достижения оптимальных параметров CFF в этом случае необходимо использовать коды, лежащие на границе Грайсмера.

The new approach of CFF construction with use of correcting mistakes codes is offered. It is shown, that for achievement of optimum CFF parameters is necessary to use the codes laying on Graismer's border.

Введение

CFF (cover-free families) рассматривались в теории информации, комбинаторике и групповых тестах. Впервые данный объект был введен в работе [1] в 1964 году для рассмотрения неслучайных наложенных двоичных кодов. Позднее появилось множество работ, посвященных этим кодам и соответственно CFF. В 1985 году была опубликована статья [2], где к описанию CFF был применен комбинаторный подход, и построены первые оценки для соотношения параметров схемы. В 1987 году авторы работы [4] ввели понятие CFF и рассмотрели его применение для создания групповых тестов. С тех пор по данной теме было опубликовано множество работ, которые относились к различным областям, применяли разные методики построения CFF и получения оценок для них. Многие результаты были несколько раз «переоткрыты», а теоремы «передоказаны». Наиболее полный обзор, обобщающий все имеющиеся результаты по данной теме, приведен в работе [5]. Там же можно более подробно ознакомиться с существующими подходами к построению CFF. Само понятие CFF было обобщено различными способами для использования в прикладных областях. Каждое обобщение требовало изменения или разработки новых способов построения, уточнения оценок и т. п. Самое первое и наиболее узкое определение, на которое мы и будем в дальнейшем ориентироваться, звучит следующим образом.

Пусть (X, A) – система множеств, где $X = \{x_1, x_2, \ldots, x_v\}$ и $A = \{A_i \subseteq X : i = \overline{1, \ldots, N}\}$, A_i – некоторые подмножество X. Система множеств (X, A) будет r-CFF (v, N) в том случае, если для любого подмножества $B \subseteq A$ такого, что $B \leq r$, и для любого $A_j \in A \setminus B$ верно утверждение $A_j \not\subset \bigcup_{A_i \subseteq B} A_i$.

Иначе говоря, в r-CFF (v, N) объединение любых r блоков не покрывает ни одного другого блока.

В данной работе представлен новый способ построения CFF именно в такой формулировке, поэтому не рассматриваются различные обобщения, которые можно встретить в работе [5].

Способы построения CFF

В общей сложности все ранее предложенные подходы к построению CFF можно разделить на три направления: комбинаторный подход, кодовая теория и вероятностные методы.

1. Комбинаторный подход. Первым и наиболее изученным является комбинаторный метод. В работах [1–3] были предложены различные схемы построения r-CFF на базе t-схем. Подробное описание этих схем мы здесь приводить не будем, напомним только полученные в данных работах оценки на параметры CFF.

Используя свойства блок-схем, можно вывести следующие соотношения между параметрами CFF, полученными на их основе: $v = O(r^2)$, $N = O(v^{t/2})$. Однако есть серьезное ограничение на использование подобных конструкций, связанное с тем, что на данный момент не существует блок-схем с $t \geq 6$.

В работе [8] предложен другой подход: построение r-CFF на базе разделяющих семейств хеш-функций (separating hash families). Данный подход позволяет получить значительно лучшие результаты и не имеет таких серьезных ограничений, как t-схемы. В этой же работе получены следующие результаты для CFF: для любого положительного r можно построить r-CFF (v, N), такое, что $N = O(v^{\log(r+1)})$, $v = O(r^2)$.

2. Коды, исправляющие ошибки. Кодовый подход при построении CFF начал применяться несколько позднее комбинаторного, и ему посвящено

значительно меньше публикаций [2, 6, 7]. В первой из них предлагалось использовать обычные и укороченные коды Рида – Соломона. Еще две работы [6, 7] посвящены использованию алгебро-геометрических кодов (Гоппы и Garcia –Stichtenoth) для построения CFF. Перечислим полученные в указанных работах оценки; более подробно способ построения будет раскрыт ниже в описании нашего подхода к построению CFF.

Для кодов Рида – Соломона было доказано, что для $r > 2$ более эффективно использование укороченных кодов. Также доказано, что для таких кодов $v = O(r^2 \log^2 N)$. Коды Garcia – Stichtenoth уступают в эффективности кодам Рида – Соломона.

3. Вероятностный подход использовался во многих работах, как для получения теоретических границ, так и при попытках построить конкретные схемы. Все полученные результаты приблизительно схожи между собой, поэтому воспользуемся результатами из работы [10]. В ней доказано, что для некоторых v, r и k, таких, что $v > 2k$, существует система множеств с постоянным размером блока k и параметром t, с $N \le e^{2(k+kp-1)^2/k-t}$ и $p = 1 - \frac{(v-k)^r}{v^r}$, где вероятность того, что данная система не является r-CFF(v, N), не превосходит e^{-t}.

Границы CFF

Здесь представлены неконструктивные границы, которые были доказаны, но еще не были получены примеры, удовлетворяющие данным границам.

Первая верхняя граница для количества блоков r-CFF с постоянным размером блока k была построена в работе [2]:

$$N \le \binom{v}{\lceil \frac{k}{r} \rceil} \Big/ \binom{k-1}{\lceil \frac{k}{r} \rceil - 1}.$$

Наилучшая нижняя оценка на размер алфавита приведена в работе [11]:

$$v \ge c \frac{r^2}{\log r} \log N,$$

где c – некоторая константа. В рассматриваемой работе [2] $c \approx 1/2$, позднее были получены другие оценки: $c \approx 1/4$ [12] и $c \approx 1/8$ [13].

При сравнении различных методов построения CFF заметно, что наилучшие и ближайшие к теоретическим границам результаты можно получить при использовании кодов, исправляющих ошибки (таблица).

Таким образом, остается только подобрать наиболее подходящий тип кодов, позволяющий строить оптимальные CFF.

Сводная таблица границ для CFF

Методы построения CFF	Размер алфавита (v)
Комбинаторный подход:	
на блок-схемах	$O(N)$, $N > r^2$
на Латинских квадратах и прямоугольниках	$O(Nr^2)$
Кодовый подход	$O(r^2 \log N)$
Теоретическая граница	$c \frac{r^2}{\log r} \log N$

Предлагаемая схема использования кодов для построения CFF

Пусть C – некоторый $(n, M, d)_q$-код, где n – длина кодового слова; M – количество слов в коде; d – расстояние кода; q – поле, над которым построен код. Тогда можно построить r-CFF(nq, M), где $r = \frac{n-1}{n-d}$ [3]. Блоки CFF строятся из слов кода, каждому слову ставится в соответствие блок. Блоки формируют пары (i, α_i), где i – номер позиции кодового слова; а α_i – элемент, стоящий на этой позиции. Таким образом, длина блока равна длине кодового слова n, а размер алфавита, составленного из всех возможных пар $\{(i, \alpha) : i = \overline{1,n},\ \alpha = \overline{0,q-1}\}$, соответственно равен $q \times n$.

Чтобы получить оптимальную схему CFF, надо построить схему с минимальным размером алфавита при максимальном числе блоков и максимальной величине r. Для этого необходимо найти код с максимальным d при минимальном nq для минимизации размера алфавита. Данное соотношение достижимо для кодов, лежащих на границе Синглтона [2, 7]. И естественно, что данные коды давали наилучшие результаты среди кодовых подходов. Однако из таких кодов известны только коды Рида–Соломона, у которых длина не превосходит размера поля. Это приводит к серьезному ограничению: на небольших полях нельзя построить схемы CFF с произвольным r. Размер поля существенно ограничивает наши возможности.

Так как $n \le q$, то можно записать

$$n = q - s;$$

$$r(n-d) = n-1.$$

Согласно границе Синглтона

$$n = d + k - 1,$$

поэтому

$$r(k + d - 1 - d) = n - 1;$$

$$r(k-1) + 1 = n;$$

$$q - s = r(k-1) + 1;$$

$$q - s = rk - r + 1.$$

Так как число блоков CFF совпадает с количеством кодовых слов, то

$$N = M = q^k,$$

следовательно:

$$rk = r\log_q N = r\frac{\log_2 N}{\log_2 q};$$

$$q - s = r\log_q N - r + 1 = r\frac{\log_2 N}{\log_2 q} - r + 1;$$

$$q\log_2 q = r\log_2 N - (r - s + 1)\log_2 q.$$

Если $s \geq r - 1$, то

$$q\log_2 q \geq r\log_2 N,$$

иначе, если $0 \leq s < r - 1$, то

$$q\log_2 q \geq r\log_2 N - r\log_2 q.$$

Эти соотношения ограничивают величины r и N сверху при заданном q, что не позволяет построить на определенном поле любую схему.

Следовательно, для того чтобы добиться выигрыша, необходимо перейти к другому классу кодов, близкому по соотношению параметров и не имеющему таких ограничений на длину. Это позволит при меньших значениях поля получить бóльшие длины кодов и расстояния, а следовательно, уменьшить алфавит при прочих равных значениях.

Коды на границе Грайсмера

Граница Грайсмера является верхней границей для параметров кодов, следовательно, коды, лежащие на данной границе, имеют минимальную длину при заданных значениях d, k, q. Некоторые из кодов на границе Грайсмера не удавалось построить, для других доказано, что они не существуют, но если рассматривать существующие коды на границе Грайсмера, они имеют оптимальные параметры, по сравнению с любыми другими кодами.

Граница Грайсмера [14] уточняет границу Синглтона и выражается следующей формулой:

$$n \geq \sum_{i=0}^{k-1}\left\lceil \frac{d}{q^i} \right\rceil,$$

где n – длина кода; k – размерность кода; d – расстояние кода; q – размер поля, над которым задан код. Для кодов, лежащих на границе Грайсмера, выполняется равенство. Таких кодов известно достаточно много и существуют конструктивные способы их построения [15–18]. Так, существуют алгебро-геометрические коды, построенные на эллиптических кривых, лежащие на этой границе. Легко показать, что при $0 \leq d \leq q$ граница Грайсмера совпадает с границей Синглтона.

Таким образом, при построении CFF на кодах, лежащих на границе Грайсмера, можно получить лучшие значения параметров по сравнению с уже существующими способами построения.

Полученные результаты

Еще раз напомним все введенные ранее обозначения, которыми и воспользуемся для сравнения полученных нами результатов с уже существующими схемами: v – размер алфавита CFF; r – количество блоков, не покрывающих больше ни один блок; N – количество блоков; q – размер поля, на котором построен код; d – расстояние кода; n – длина кодового слова; k – размерность кода; c, a – произвольные константы; z – произвольная целочисленная константа.

Теоретическая граница на размер алфавита (v), приведенная в работе [11] связывает эти параметры:

$$v = c\frac{r^2}{\log r}\log N.$$

Теорема 1. Для получения оптимальных параметров CFF с использованием кодов, лежащих на границе Грайсмера, необходимо выбирать коды с $d < q^2$.

Доказательство. Пусть $d = aq^z$ ($z < k$ и $a < q$), тогда

$$n = \sum_{i=0}^{k-1}\left\lceil \frac{d}{q^i} \right\rceil = d + \frac{d}{q} + \frac{d}{q^2} + \ldots + \frac{d}{q^{k-1}} =$$

$$= b(\underbrace{q^z + q^{z-1} + \ldots + q + 1}_{z+1} + \underbrace{1 + \ldots + 1}_{k-1-z}) = a\left(\frac{q^{z+1} - 1}{q - 1} + k - 1 - z\right).$$

Таким образом,

$$n = a\left(\frac{q^{z+1} - 1}{q - 1} + k - 1 - z\right).$$

Для любых кодовых конструкций CFF известно:

$$r = \frac{n - 1}{n - d},$$

отсюда

$$r = \frac{a\left(\frac{q^{z+1} - 1}{q - 1} + k - 1 - z\right)}{a\left(\frac{q^{z+1} - 1}{q - 1} + k - 1 - z\right) - aq^z} =$$

$$= \frac{\frac{q^{z+1} - 1}{q - 1} + k - 1 - z}{\frac{q^{z+1} - 1}{q - 1} + k - 1 - z - q^z} =$$

$$= \frac{q^{z+1} - zq + z + kq - k - q}{q^z - zq + z + kq - k - q} < q, \text{ для } k < q.$$

Размер алфавита CFF равен

$$v = nq = a\left(\frac{q^{z+1} - 1}{q - 1} - z + k - 1\right)q =$$

$= a(q^{z+1} + q^z + q^{z-1} + \ldots + q^2 + q \cdot (k - z))$, $z < k < q$.

Следовательно, чтобы рост размера алфавита не превосходил $O(r^2 \log N)$, необходимо, чтобы выполнялось условие $z \le 1$, т. е. $d = aq < q^2$.

Как уже упоминалось, при $d < q$ мы получаем обычный МДС код и результаты, уже известные для кодов Рида – Соломона. Поэтому имеет смысл рассматривать только коды, у которых $q < d < q^2$, т. е. $d = aq$, где $1 < a < q$ – некоторая константа.

Теорема 2. Оптимальные параметры CFF, построенных на кодах, лежащих на границе Грайсмера, можно получить при использовании кода с $d = (k-2)q$.

Доказательство. Пусть $d = aq$ $(1 < a < q)$, тогда

$$n = \sum_{i=0}^{k-1} \left\lceil \frac{d}{q^i} \right\rceil = d + \frac{d}{q} + \frac{d}{q^2} + \ldots + \frac{d}{q^{k-1}} = aq + a + k - 2;$$

$$n = aq + a + k - 2.$$

Следовательно,

$$r = \frac{n-1}{n-d} = \frac{aq + a + k - 3}{a + k - 2};$$

$$ar + kr - 2r = aq + a + k - 3;$$

$$q = \frac{ar + kr - 2r - a - k + 3}{a} =$$

$$= \frac{a(r-1) + r(k-2) - (k-2) + 1}{a} =$$

$$= \frac{a(r-1) + (r-1)(k-2) + 1}{a} =$$

$$= \frac{(r-1)(a + k - 2) + 1}{a} > \frac{(r-1)(a + k - 2)}{a},$$

а размер алфавита равен

$$v = nq = (aq + a + k - 2)q \le$$

$$\le \left((r-1)(a + k - 2) + (a + k - 2)\right)\frac{(r-1)(a + k - 2)}{a} =$$

$$= r(a + k - 2)\frac{(r-1)(a + k - 2)}{a} = r(r-1)\frac{(a + k - 2)^2}{a}.$$

Для получения оптимальных параметров CFF необходимо минимизировать размер алфавита. Попытаемся найти экстремум полученной функции размера алфавита от переменной a:

$$v' = r(r-1)\left(\frac{2(a + k - 2)}{a} - \frac{(a + k - 2)^2}{a^2}\right) =$$

$$= r(r-1)\frac{(a + k - 2)(2a - a - k + 2)}{a^2} =$$

$$= r(r-1)\frac{(a + k - 2)(a - k + 2)}{a^2};$$

$$v^{\downarrow} = 0;$$

$$r(r-1)\frac{(a + k - 2)(a - k + 2)}{a^2} = 0;$$

$$a = k - 2 \text{ или } a = 2 - k.$$

В точке $a = k - 2$ размер алфавита достигает своего минимума, а в точке $a = 2 - k$ – максимума.

Следовательно, для получения CFF на кодах, исправляющих ошибки, с минимальным достижимым размером алфавита необходимо брать коды, лежащие на границе Грайсмера, с расстоянием $d = (k-2)q$.

Оценим размер алфавита, получаемого при использовании кодов, лежащих на границе Грайсмера, с расстоянием $d = (k-2)q$:

$$n = (k-2)q + k - 2 + k - 2 =$$

$$= (k-2)q + 2(k-2) = (k-2)(q+2);$$

$$r = \frac{n-1}{n-d} = \frac{(k-2)(q+2) - 1}{(k-2)(q+2) - (k-2)q} = \frac{(k-2)(q+2) - 1}{2(k-2)} =$$

$$= \frac{q+2}{2} - \frac{1}{2(k-2)} \le \frac{q+2}{2} - 1 = \frac{q}{2};$$

$$q \ge 2r;$$

$$v = nq = (k-2)(q+2)q \ge (k-2)(2r+2)2r =$$

$$= 4r(r+1)(k-2) = 4r(r+1)\frac{\log N}{1 + \log r}.$$

Полученный результат совпадает с теоретической границей, которая приведена в начале параграфа, с точностью до константы. Следовательно, используя коды, лежащие на границе Грайсмера, мы можем получить оптимальные, с точки зрения размера алфавита, CFF схемы.

Практически, на эллиптических кривых можно построить следующие коды для конкретных параметров: $q = 64$, $k = 13$, $d = 66$, $n = 79$. Из этого кода можно получить CFF с параметрами 6-CFF(5056, 2^{78}): $q = 53$, $k = 14$, $d = 81$, $n = 97$. Соответственно, из этого кода можно получить CFF с параметрами 6-CFF(5141, 2^{80}). Лучшая известная до сих пор схема на кодах Рида–Соломона дает код $q = 73$, $k = 13$, $d = 61$, $n = 73$. Из этого кода можно получить CFF с параметрами 6-CFF(5329, 2^{80}).

Способы построения кодов на границе Грайсмера

Существует несколько подходов к построению кодов на границе Грайсмера. В 1965 году авторы работы [15] предложили способ построения целого класса кодов, лежащих на границе Грайсмера, с использованием процедуры вычеркивания столбцов из порождающей матрицы симплекс-кода. Позднее, в 1974 году, этот подход был обобщен В. И. Беловым [16] и построен еще один класс кодов. Другой подход, который был предложен в 1981 году и развит в 1983 году в работах [17, 18], заключался в новом методе комбинирования порождающих матриц симплекс-кодов и добавлении к ним новых элемен-

тов. Более поздние работы связаны с попытками применения понятий проективной геометрии в построении кодов, таких как проективные плоскости [19].

К сожалению, все предложенные в данных работах коды двоичные, для q-ичного случая в общем виде не было предложено ни одной конструктивной процедуры построения. Кроме того, все предложенные коды строятся на базе симплекс-кодов или различными комбинациями кодов, поэтому все они имеют очень большие длины, а следовательно, и большой размер алфавита. По этим причинам все рассмотренные ранее конструкции нам не подходят, и необходимо воспользоваться каким-либо иным способом построения кода.

Мы предлагаем способ построения кодов, который не дает возможности гарантированного построения целого класса кодов, но позволяет получать отдельные экземпляры кодов, лежащих на границе Грайсмера или очень близко к ней. Будем строить алгебро-геометрические коды. Данный способ построения рассматривался во многих работах и гарантирует получение кодов с длиной $n \le k + d - 1 + g$ [28], где g – род кривой. Так как границу Грайсмера можно представить в виде

$$n \ge d + k - 1 + \sum_{i=1}^{k-1} \left\lfloor \frac{d}{q^i} \right\rfloor,$$

то нетрудно подобрать параметры кривой для построения кода, лежащего на границе Грайсмера. Можно было бы говорить о построении целого класса кодов, у которых $g \le \sum_{i=1}^{k-1} \left\lfloor \frac{d}{q^i} \right\rfloor$, но, к сожалению, при выборе параметров приходится учитывать еще одно ограничение на коды, построенные с использованием кривых $n \le q + g\left\lfloor 2\sqrt{q} \right\rfloor$ [28]. Данное ограничение не позволяет увеличивать длину кода до бесконечности, следовательно, мы можем говорить только о построении отдельных экземпляров кодов. Для нашей схемы можно воспользоваться любым из предложенных ранее подходов или разработать новый, но данный способ позволяет получить некоторые примеры для их наглядного сравнения с уже существующими схемами построения CFF.

Применение CFF

CFF может применяться в различных приложениях. Множество работ посвящено описанию взаимосвязи между различными комбинаторными объектами. В этих работах показано, каким образом можно построить различные комбинаторные схемы на базе CFF. Существует также множество работ, которые предлагают использовать CFF в различных криптографических приложениях, таких как цифровая подпись [20], управление ключами [21, 22], Frame proof [23, 24], Broadcast encryption [7, 26], Traitor tracing [27]. Кроме того, были широко распространены исследования по применению CFF в построении схем группового тестирования [4, 28]. Все опубликованные работы по данной тематике показывают актуальность разработки новых способов построения CFF. Предложенная нами схема может быть применена в любой из рассмотренных ранее работ.

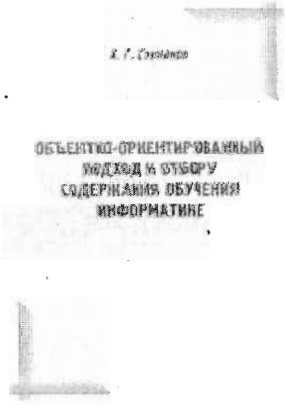
Литература

1. **Kautz W. H., Singleton R. C.** Nonrandom binary superimposed codes// IEEE Transactions on Information Theory. – 1964. – N. 10. – P. 363–377.
2. **Erdös P., Frankl P., Füredi Z.** Families of finite sets in which no set is covered by the union of r others// Israel Journal of Mathematics. – 1985. – N 51. – P. 75-89.
3. **Stinson D. R., Wei R.** Combinatorial properties and constructions of traceability schemes and frameproof codes // SIAM Journal on Discrete Mathematics. – 1998. – N 11. – P. 41–53.
4. **Hwang K. F., Sтs V. T.** Non-adaptive hypergeometric group testing // Studia Sci. Math. Hungar. – 1987. – N 22. – P. 257–263.
5. **Wei R.** On cover-free families: Preprint.
6. **Garcia A., Stichtenoth H.** A tower of Artin-Schreier extensions of function fields attaining the Drinfeld-Vladut bound // Invent. Math. – 1995. – N 121. – P. 211–222.
7. **Kumar R., Rajagopalan S., Sahai A.** Coding constructions for blacklisting problems without computational assumptions // Advances in Cryptology – Crypto '99: Lecture Notes in Computer Scienc. – 1999. – N 1666. – P. 609–623.
8. **Stinson D. R., van Trung Tran, Wei R.** Secure frameproof codes, key distribution patterns, group testing algorithms and related structures // Journal of Statistical Planning and Inference. – 2000. – N 86. – P. 595–617.
9. **Staddon J. N., Stinson D. R. and Wei R.** Combinatorial properties of frameproof and traceability codes// IEEE Transactions on Information Theory. – 2001. – N 47. – P. 1042–1049.
10. **Stinson D. R., Wei R.** Generalized cover-free families: Preprint.
11. **Дьячков А. Г., Рыков В. В.** Границы на длину разделяющих кодов// Проблемы передачи информации. – 1982. – Вып. 18. – С. 7–13.
12. **Füredi Z.** On r-cover-free families// Journal of Combinatorial Theory. – 1996. – A 73. – P. 172–173.
13. **Ruszinko M.** On the upper bound of the size of the r-cover-free families // Journal of Combinatorial Theory. – 1994. – A 66. – P. 302–310.
14. **MacWilliams F. J., A. Sloane N. J.** The Theory of Error-Correcting Codes. – Amsterdam: North-Holland, 1977.
15. **Solomon G., Stiffler J. J.** Algebraically punctured cyclic codes // Inform. Contr., Apr. – 1965. – Vol. 8. – P. 170–119.
16. **Белов В. И., Логачев В. Н., Сандимиров В. П.** Построение класса линейных двоичных кодов, достигающих границы Варшамова-Гилберта// Проблемы передачи информации. – 1974. – Вып. 3. – С. 36–44.
17. **Helleseth T., A van Tilborg H. C.** A new class of codes meeting the Griesmer bound // IEEE Trans. Inform. Theory. – Sept. 1981. – Vol. IT-27. – P. 548–555.

18. **Helleseth T.** New Constructions of Codes Meeting the Griesmer Bound// IEEE Transactions on Information Theory. – May 1983. – Vol. IT-29. – N 3. – P. 434–439.
19. **Storme L.** Linear codes meeting the Griesmer bound, minihypers and geometric applications: Preprint.
20. **Pieprzyk J., Wang H., Xing C.** Multiple-time signature schemes secure against adaptive chosen message attacks // 10th Workshop on Selected Areas in Cryptography: Lecture Notes in Computer Science, 2003.
21. **Chan Aldar C.F.** Distributed Symmetric Key Management for Mobile Ad Hoc Networks // IEEE INFOCOM, 2004.
22. **Dyer M., Fenner T., Frieze A., Thomason A.** On key storage in secure networks // J. Cryptology. – 1995. – N 8. – P. 189–200.
23. **Stinson D. R., Wei R.** Combinatorial properties and constructions of traceability schemes and frameproof codes// SIAM Journal on Discrete Mathematics. – 1998. – N 11. – P. 41–53.
24. **Stinson D. R., van Trung Tran, Wei R.** Secure frameproof codes, key distribution patterns, group testing algorithms and related structures// Journal of Statistical Planning and Inference. – 2000. – N 86. – P. 595–617.
25. **Stinson D. R., Wei R.** Key reassigned traceability schemes for broadcast encryption// Selected Areas in Cryptology – SAC '98: Lecture Notes in Computer Science. – 1999. – N 1556. – P. 144–156.
26. **Chor B., Fiat A., Naor M., Pinkas B.** Tracing traitors // IEEE Transactions on Information Theory. – 2000. – N 46. – P. 893–910.
27. **Knill E., Bruno W. J., Torney D. C.** Non-adaptive group testing in the presence of error // Discrete Appl. Math. – 1998. – N 88. – P. 261–290.
28. **Tsfasman M.A., Vlădut S.G.** Algebraic-geometric codes// Dordrecht: Kluwer, 1991.
29. **Hamada N. A.** Characterization of some [*n*; *k*; *d*; *q*]-codes meeting the Griesmer bound using a minihyper in a finite projective geometry // Discrete Math. – 1993. – Vol. 116. – N 1–3. – P. 229–268.

А. Г. Степанов

Объектно-ориентированнйй подход к отбору содержания обучения информатике: Монография/ СПб.: Политехника, 2005. -287 с.: ил. ISBN 5-7325-0856-2



Монография посвящена разработке модели информатики как предмета обучения на основе анализа существующих представлений об информатике как науке. В качестве основы построения модели предлагается объектно-ориентированный подход. Модель строится с помощью методов концептуальной кластеризации с использованием теории прототипов на основе анализа существующего состояния обязательного содержания профильного обучения информатике.

Материалы монографии представляют интерес для специалистов, занимающихся вопросами преподавания информатики в средней и высшей школе, а также административных работников системы образования. Представленные в приложениях дидактические материалы могут использоваться как систематизированные справочные данные, характеризующие текущее содержание обучения вопросам информатики в высшей школе России.

Предложенная модель информатики как предмета обучения может быть использована для разработки перспективных Государственных стандартов образования существующих и вновь открываемых специальностей и направлений подготовки средней и высшей школы.