2008 Теоретические основы прикладной дискретной математики № 1(1)

DOI 10.17223/20710410/1/3
УДК 519.1

КОДЫ, КОМПОЗИЦИИ И РЕШЕТКИ

А.М. Кутьин

Сибирский федеральный университет, г. Красноярск

E-mail: maglinetc@mail.ru

Обсуждаются вопросы теории кодирования, связанные с ее центральной проблемой. Рассмотрена основная модель теории кодирования и криптографии – дистрибутивная решетка, исследованы ее связи с композициями чисел и *c*-матроидами. Построены решеточные коды. Указаны границы кодов в метрике Хемминга.

Ключевые слова: *код*, *композиции чисел*, *решетка*, *метрика*, *s-множество*, *c-матроид*

Теория кодирования и криптографии призвана решить относящиеся к ней задачи общей проблемы безошибочной передачи данных с обеспечением их защиты от несанкционированного доступа. Одной из теоретических основ их решения, как показано ниже, является теория решеток и s-множеств [1 – 7].

Напомним, что решетка как алгебра обозначается обычно $L = < M; +, \cdot >$ или $L = < M; \vee, \wedge >$, $M \neq \varnothing$.

Центральная проблема теории кодирования имеет немалое число формулировок. Приведем лишь две из них. При заданных n и d найти $A(n, d)$, равное максимальному числу кодовых слов в равномерном (n, M, d)-коде, где M – объем кода, см. [8]. Другая формулировка [9]: найти равномерные коды с большим $R = k/n$ для эффективности, так как R – скорость, и большим d для надежности: чем больше d, тем больше ошибок можно исправить (здесь k – число информационных символов). Мы предпочитаем следующую формулировку.

Найти аналитическую формулу для функции $A(m, l, d)$, где $A(m, l, d)$ – максимальная мощность кодов из слов v равной длины $l(v) = n$ над алфавитом мощности m с расстоянием ρ между кодовыми словами не менее наперёд заданного d; в отсутствие точной формулы найти неулучшаемые верхние и нижние границы.

1. Кодирование и *L*-кодирование

Рассмотрим сначала равномерные коды (кратко Р-коды). Возьмем алфавит $A = \{a_0, \ldots, a_m\}$ и построим множество W всех слов v равной длины $l(v) = n$ над A; получаем простой равномерный код (ПРК, или ПР-код) над A. Слово $u = x_1 \ldots x_n$ можно рассматривать и как вектор $\boldsymbol{u} = <x_1, \ldots, x_n>$ конечного n-мерного пространства, $x_i \in A$, $i = 1, \ldots, n$. Поэтому можно говорить о координатах или компонентах в векторах (словах) и символах в словах (векторах). Исходным фактом теории L-кодирования, который объясняет ее название, является следующая теорема 1.

Теорема 1. Любое множество W слов v равной длины $l(v) = n$, в частности простой равномерный код, над линейно упорядоченным алфавитом $A = \{a_0, \ldots, a_m\}$ объема $m+1$ при векторном отношении порядка $\leq$ на W, индуцированном порядком на A, является конечной дистрибутивной самодвойственной решеткой $L_A = \langle W, \leq \rangle$, порожденной c-элементами вида $c_{i\,j} = (a_0, \ldots, a_0, a_j, a_0, \ldots, a_0)$, где a_j стоит на j-м месте. При этом:

1) L_A – градуированная решетка, число уровней которой равно $nm+1$, представляет собой прямое произведение цепей C_i равной длины $l(C_i)$ числом n: $L_A = \Pi_1^n C_i$, каждая из которых состоит только из c-элементов указанного вида, а всякий c-элемент принадлежит соответствующей цепи C_i, и только ей;

2) число n всех цепей C_i равно $n = l(v)$ – длине слова v (равносильно – длине кода), а длина $l(C_i)$ любой цепи C_i равна $m = l(C_i)$, где $m+1 = |A|$ – объем алфавита A, причем $l(L_A) = l(\Pi_1^n C_i) = \Sigma_1^n\, l(\mathrm{C}_i) = nm$;

3) число всех c-элементов равно $nm+1$, причем $c_{ik} \wedge c_{jt} = \hat{0}$ при $i \neq j$, а любое слово v Р-кода представимо единственной суммой $v = \vee\, c_{km}$ c-элементов, в этом слове содержащихся: $v \geq c_{km}$ для всех c_{km} из суммы $\vee\, c_{km}$;

4) множество всех c-элементов есть у-подмножество в решетке L_A всех $\vee$-неприводимых элементов из L_A, являющееся $\wedge$-полурешеткой ранга m и c-матроидом, а при добавлении к ним всех элементов из L_A рангов, соответствующих рангам c-элементов, оказывается также и суперматроидом.

Обратно, любая конечная решетка L, разложимая в прямое произведение цепей $L = \Pi_1^n C_i$ равной длины m, являясь самодвойственной дистрибутивной решеткой, порожденной $\vee$-неприводимыми элементами, изоморфна решетке L_A слов равной длины n над алфавитом $A = \{0, 1, \ldots, m\}$. ■

В этом контексте удобно L_A обозначать через $L_{\text{ПРК}}(m, n)$, $m+1 = |A|$ или через $L_{\text{ПРК}}(n)$ при фиксированном m, а в c_{ik} удалить индекс k, так что далее c_i обозначает просто некоторый c-элемент.

Определим ранг-метрику ρ_r: $\rho_r(v, u) = r(v \vee u) - r(v \wedge u)$, где $v, u \in L_A$, $r(x)$ – ранговая функция на L_A (по сути, $r(x)$ – это высота элемента x в L_A), и H-метрику ρ_H: пусть $w_H(x)$ – вес Хемминга вектора x, тогда $\rho_H(x, y) = w_H(x - y)$ выражает число позиций, в которых отличаются векторы x и y; значит, в любой L_A всегда $\rho_H \le n$, где n – длина Р-кода, а $\rho_H = n$ – максимальное значение функции ρ_H.

Следствие 1. Группа автоморфизмов решетки $L_{\text{ПРК}}(n)$ изоморфна симметрической группе S_n перестановок, где n – длина кода над односортным алфавитом A, а используя перестановки из S_n и/или из симметрической группы $S(A)$ перестановок на A, и/или элементы из группы антиизоморфизмов решетки $L_{\text{ПРК}}(n)$, можно все слова Р-кода преобразовать в другие, тем самым шифруя закодированное сообщение.

Решетка L_A при любом алфавите A допускает ранг-метрику ρ_r и H-метрику ρ_H. Пара $<L_A, \rho_r>$, как и пара $<L_A, \rho_H>$, является дискретным метрическим пространством при любом алфавите A. ■

Теорема 1 позволяет изучать коды независимо от их происхождения: созданы ли они над полями, или другими алгебрами, или являются геометрическими кодами и т.д. Например, на рис. 1 представлен ПРК над кольцом классов вычетов по модулю 3, а на рис. 2 в [1] – ПРК над симметрической полугруппой перестановок S_n.

Тем самым теория L-кодирования инвариантна относительно источников происхождения кодов, и одновременно она позволяет использовать все факты, полученные иным путем, так как все, что определено и доказано для множества слов W равной длины над любым алфавитом A и его подмножества кодовых слов, конечно же, определено и доказано для L_A. Поэтому здесь и не приведены известные факты теории кодирования, кроме тех, что понадобятся далее для целей изложения.

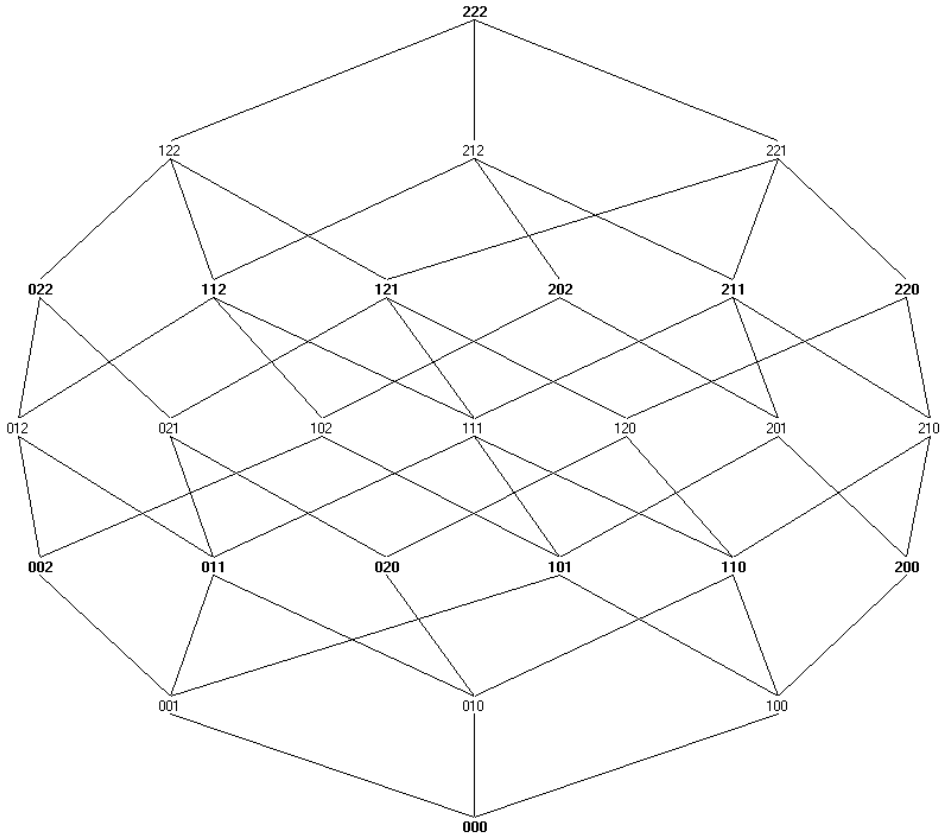

Рис. 1. Решётка слов длины 3 над алфавитом $A = \{0, 1, 2\}$. Слова кода кусочно-постоянного веса (либо 6, либо 4, либо 2, либо 0) с минимальным кодовым расстоянием $d_0 = 2$ выделены

Как видим, при $A = \{0, 1\}$ получаем булеву решетку, называемую в случае двоичных Р-кодов еще и n-мерным кубом, так что $L_{\text{ПРК}}(m, n)$ можно назвать n-мерным параллелепипедом, так как цепи C_i в общем случае можно брать различной длины, см. [1]. Булеву подрешетку двоичного ПР-кода с 2^3 словами длины 3 над алфавитом $A = \{0, 1\}$ с наименьшим в ней элементом-словом 000 и наибольшим в ней элементом-словом 111 см. на рис. 1, так что и в общем случае (при соблюдении естественного условия на длины кодов) вложение $A_1 \subseteq A_2$ алфавита A_1 в A_2 влечет вложение кода длины n над A_1 в код длины $n + k$ над A_2, $k \ge 0$, в частности, при $k = 0$ ПР-код длины n над $A_1 = \{1, \ldots, m\} \subseteq \{0, 1, \ldots, m\} = A_2$ есть подрешетка с наименьшим в ней элементом-словом 1…1 и наибольшим в ней элементом-словом $m…m$; точнее, эта подрешетка есть интервал $I = [1…1, m…m]$, изоморфный $L_{\text{ПРК}}(n, m)$ над алфавитом $A_1 = \{1, \ldots, m\}$: $I \cong L_{\text{ПРК}}(n, m)$.

Решетка на рис. 1 – это одновременно

- решетка композиций чисел от 0 до $nm = 9$ с ограничениями: 1) все $a_i \le m$ в сумме $\sum a_i = j$, здесь j – это j-уровень, $0 \le j \le nm$ (соответственно $3 \le j \le nm$); 2) число слагаемых в $\sum a_i = j$ равно n;
- решетка конечного линейного векторного пространства размерности 3, оси которого и есть цепи C_i, $i = 1, 2, 3$;
- решетка кольца (над кольцом классов вычетов по модулю 3) с покомпонентными сложением и умножением;
- решетка делимости, называемая также решеткой НОД-НОК или же решеткой упорядоченных разложений в произведение степеней простых чисел p_i^{ki}, так как компоненты элементов решетки, изображенные на рис. 1, можно интерпретировать как показатели степеней k_i этих чисел;
- решетка всех размещений с повторениями, так что их число в данном случае равно $m^n = 3^3 = 27$.

Ясно, что любая решетка $L_{\text{ПРК}}(m, n)$ обладает всеми только что перечисленными свойствами (указанные в примере конкретные значения n и m относятся именно к нему, а в общем случае их из свойств нужно, конечно, удалить).

Р-код, образуя у-подмножество в решетке $L_{\text{ПРК}}(m, n)$, не образует, вообще говоря, подрешетку в ней. Однако верно

Предложение 1. Решеточные коды, т.е. коды, являющиеся подрешетками решетки $L_{\text{ПРК}}(n)$, существуют, более того, существуют корректирующие решеточные коды.

Доказательство. Простые решеточные коды существуют – ими являются все ПРК. Покажем, что существуют корректирующие решеточные коды в любой $L_{\text{ПРК}}(m, n)$ с ранг-метрикой. Возьмем лишь те c-элементы c_i, c_j решетки $L_{\text{ПРК}}(n)$, которые находятся друг от друга на расстоянии $\rho_r(c_i, c_j) \ge d_0$ – наименьшего подходящего кодового расстояния. Найдем все элементы вида $v_k = \vee c_i$, затем все элементы вида $u_t = \wedge v_k$, потом вида $w_s = \vee u_t$ и т.д. По окончании построения множества всех таких элементов получим решеточный Р-код. В этом Р-коде для любых его кодовых слов $v = \vee c_i$ и $u = \vee c_j$ выполняется $\rho_r(v, u) \ge d_0$, потому что имеет место следующая лемма 1.

Лемма 1. Пусть $v = \vee c_i$, $u = \vee c_j$ и $\rho_r(c_i, c_j) \ge d_0$ хоть для одной пары c_i, c_j. Тогда $\rho_r(v, u) \ge \rho_r(c_i, c_j) \ge d_0$. ■

Полученный в ходе доказательства предложения 1 Р-код – это корректирующий код при $d_0 \ge 2$, так как для любых его кодовых слов $v \ne u$ выполняется $\rho_r(v, u) \ge d_0$. Например, взяв в $L_{\text{ПРК}}(2, 3)$ элементы 200, 020, 002 (см. рис. 1) и найдя все $\wedge c_i$, $\vee c_i$ и т.д., получим решеточный Р-код 000, 200, 020, 002, 220, 202, 022, 222, для любых кодовых слов v и u которого выполняется $\rho_r(v, u) \ge d_0 = 2$, так что этот код обнаруживает одну ошибку.

Все решеточные корректирующие коды того же типа для любой $L_{\text{ПРК}}(m, n)$, $m \ge 2$, с ранг-метрикой суть 00…0, m0…0, 0m…0, 0…0m, mm0…0, …, $mm...m$, а так как $\rho_r(v, u) \ge d_0 = m$, то при $m \ge 3$ эти коды не только обнаруживают, но и исправляют ошибки. Решеточные коды этого типа можно использовать для шифрования, например, двоичных ПР-кодов типа 00…0, 10…0, 01…0, 0…01, 110…0, …, 11...1, превращая их в коды m0…0, 0m…0, 0…0m, mm0…0, …, $mm...m$; при этом, хотя решетки этих кодов изоморфны, они при $m \ge 2$ существенно различны: полученный код – это корректирующий код, а исходный двоичный код таковым, конечно, не является.

Если же взять подходящие вложения $L_{\text{ПРК}}(m, n)$ в $L_{\text{ПРК}}(m+k, n)$ или в $L_{\text{ПРК}}(m+k, n+t)$, $k, t \ge 1$, то, исходя из кодов указанного типа в $L_{\text{ПРК}}(m, n)$, можно построить решеточные коды и другого типа соответственно в $L_{\text{ПРК}}(m+k, n)$ и $L_{\text{ПРК}}(m+k, n+t)$.

2. *L*-модель равномерных кодов

С учетом сказанного в п. 1 введем следующую L-модель ПР- и Р-кодов.

Основное определение. Множество всех элементов решетки $L(m, n) = \Pi_1^n C_i$, $l(C_i) = m$, назовем ПР-кодом, считая, что $L(m, n)$ есть $L_{\text{ПРК}}(m, n)$, а любое непустое подмножество элементов решетки $L(m, n) = L_{\text{ПРК}}(m, n)$ назовем Р-кодом.

Цепи и антицепи. **Уровневые числа**. Наиболее удобной решеткой $L_{\text{ПРК}}(m, n)$ для дальнейшего исследования является решетка, построенная над алфавитом $A = \{0, 1, \ldots, m\}$, так как тогда любое целое j, определяющее j-уровень этой решетки, равно весу $\omega(v)$ любого слова v этого j-уровня: $j = \omega(v)$, $0 \le j \le nm$.

Один из основных классов кодов – коды с постоянным весом строятся на основе групп перестановок. Взяв $L_{\text{ПРК}}(m, n)$, можно построить коды с кусочно-постоянным весом, пример одного из которых мы и предъявляем на рис. 1. Ясно, что коды с постоянным весом – частный случай кодов с кусочно-постоянным весом.

В дополнение к аналогам $h(\Pi_1^k P_i) = \Sigma_1^k h(P_i)$ и $l(\Pi_1^k C_i) = \Sigma_1^k l(C_i)$, см. [1], основного свойства логарифмической функции: $\ln(x \cdot y) = \ln(x) + \ln(y)$ приведем также следующий аналог этого свойства. Пусть $Ach(j)$ – антицепь, являющаяся j-уровнем решетки $L = \Pi_{i=1}^n C_i$ и $ach(j) = |Ach(j)| = w_j$ – уровневые числа (числа Уитни).

Лемма 2. При $0 \le j \le m$ и $n \ge 2$ для любой антицепи $Ach(j)$ j-уровня решетки $L = \Pi_{i=1}^n C_i$, $l(C_i) = m$, $i = 1, \ldots, n$, справедливо

$$ach(j, \Pi_{i=1}^n C_i) = \Sigma_{t=0}^j ach(t, \Pi_{i=1}^{n-1} C_i), \text{ равносильно } w_j(\Pi_{i=1}^n C_i) = \Sigma_{t=0}^j w_t(\Pi_{i=1}^{n-1} C_i). \blacksquare$$

Объемы шаров и границы. Пусть $A(n, m, d_0)$ – равномерный код (подмножество кодовых слов множества W всех слов равной длины $l = n$ над алфавитом объема $m + 1$), любые два слова которого находятся на расстоянии $\rho(v, w) \le d_0$ – минимального кодового расстояния. Пусть далее $Sh(r, z):=\{x: \rho(x, z) \le r\}$ – шар радиуса $r \ge 0$ и с центром z, z – некоторое слово, например кодовое, внутренность шара $Int(Sh(r, z)):= \{x: \rho(x, z) < r, r \ge 1\}$, сфера $Sf(r, z):= Sh(r, z) \setminus Int(Sh(r, z)) = \{x: \rho(x, z) = r\}$ и $Vsh(r, z):=|Sh(r, z)|$ – объем шара. Тогда

$$Vsh(r, z) = |Sf(r, z) \cup Int(Sh(r, z))| = |Sf(r, z)| + |Int(Sh(r, z))| \text{ при } r \ge 1.$$

При $r = 0$ считаем по определению, что шар $Sh(0, z)$ совпадает со своей внутренностью, а площадь его сферы равна 0.

Ясно, что минимальный объем шара $Sh(r, z)$ в $L(n, m)$ при $r \ge 1$ и кодовом слове z не может быть меньше 2, так как он должен содержать хотя бы 2 элемента, а чтобы код мог обнаруживать хоть одну ошибку, нужно, чтобы $d_0 \ge 2$, а тогда $r \le d_0/2$.

Объемы шаров в ранг-метрике одного и того же радиуса r, вообще говоря, различны (см. рис. 1), поэтому говорим о минимальном значении объемов шаров $Vsh_{\min}(r)$, максимальном $Vsh_{\max}(r)$ и среднем значении $Vsh_{sr}(r)$ объемов шаров. Тогда в общем случае непосредственно получаем следующие неравенства и границы

$$m^n / Vsh_{\max}(r) \le m^n / Vsh_{sr} \le m^n / Vsh_{\min}, \ (m+1)^n / Vsh_{\max}(r) \le \max|A(n,m,d_0)| \le \lceil (m+1)^n / d_0 \rceil. \blacksquare$$

Здесь и ниже $m + 1$ – объем алфавита $A = \{0, \ldots, m\}$ и $\lceil\ \rceil$ – целая часть числа сверху, например, $\lceil 25:2 \rceil = 13$.

В частном случае двоичного алфавита $A = \{0, 1\}$, $m = 1$, имеем

$$2^n / Vsh_{\max}(r) \le \max|A(n, m, d_0)| \le \lceil 2^n / d_0 \rceil.$$

Очевидно, что точное значение $\max|A(n, m, d_0)|$ находится в ряду чисел

$$\lceil m^n / Vsh_{\max}(r) \rceil, 1+\lceil m^n / Vsh_{\max}(r) \rceil, 2+\lceil m^n / Vsh_{\max}(r) \rceil, \ldots, \lceil m^n / d_0 \rceil.$$

Оказалось, что хотя объемы шаров в ранг-метрике одного и того же радиуса r, вообще говоря, различны, существуют максимальные Р-коды объема $\max|A(n, m, d_0)| = \lceil m^n : d_0 \rceil$, так что указанная верхняя граница $\lceil m^n : d_0 \rceil$ достигается. Приведем из них простейший код объема $\max|A(2, 5, 2)| = 13$ с $d_0 = 2$, обнаруживающий любую одну ошибку: 00, 11, 02, 20, 22, 13, 31, 33, 04, 40, 24, 42, 44, где взят алфавит {0, 1, 2, 3, 4}, а каждый шар имеет радиус $r = 1$; это же значение объема кода получаем согласно формуле $\max|A(n, m, d_0)| = \lceil m^n : d_0 \rceil$ при $n = 2$, $m = 5$ и $d_0 = 2$.

Так как в случае H-метрики длина Р-кода n – это максимальное значение функции ρ_H, то в этом случае шары, центры которых – кодовые слова, а внутренности не пересекаются, есть смысл брать лишь с радиусом r для $0 \le r < n$.

Если на $L(n, m)$ задана H-метрика, то площади сфер одного и того же радиуса r равны, а шары одного и того же радиуса r равнообъёмны, так что при фиксированном радиусе r соответственно имеем

$$\text{площадь любой сферы } |Sf(r, z)| = C_n^r m^r, \text{ объём любого шара } Vsh(r, z) = 1 + \sum_{ri=1}^{r} C_n^{ri} m^{ri}.$$

Поэтому, в случае H-метрики при $m = 1$ с учётом равнообъёмности шаров одного того же радиуса r получаем

$$2^n / (1 + \sum_{ri=1}^{r} C_n^{ri}) \le \max|A(n, m, d_0)| \le \lceil 2^n / d_0 \rceil.$$

***L*(*m*,*n*) как решетки композиций чисел от 0 до *nm* с ограничениями.** Как известно [10, Гл.1, п.2С], упорядочение множества разложений целого положительного числа n в суммы $n_1 + n_2 + \ldots + n_k$ целых положительных неупорядоченных слагаемых (так что, например, 1+2 = 2+1) приводит к у-множеству $D(n)$ – *доминирующему порядку*. Если же и слагаемые в сумме также упорядочены, так что, например, $1+2 \ne 2+1$, то получаем решетку $D_{\le}(n)$ композиций числа n (см. диаграммы $D(5)$ и $D_{\le}(5)$ на рис. 2).

Утверждение 1.

1. $D(n)$ является ранжированной модулярной мультирешеткой [3, 5, 11].

2. $D_{\le}(n)$ – булева решетка, точнее: $D_{\le}(n) \cong Bool(n–1)$.

3. Каждому элементу вида $n_1 + n_2 + \ldots + n_k$ из $D(n)$ соответствует свой класс эквивалентности из $D_{\le}(n)$, получаемый из $n_1 + n_2 + \ldots + n_k$ всеми перестановками этих слагаемых, так что существует биекция между классами эквивалентности на множестве элементов k-уровня из $D_{\le}(n)$ и множеством элементов k-уровня из $D(n)$, $0 \le k \le n$.

Существует монотонная сюръекция $sur(D_{\le}(n)) = D(n)$.

Решетка Юнга J имеет следующую связь с $D(n)$: $|D(n)| =$ |множество элементов уровня n решетки J|.

Имеет место следующая связь между $D_{\le}(n)$ композиций числа n и ПР-кодами над алфавитом $A = \{0, \ldots, n\}$: мощность множества слов длины $n + k$ и веса $\omega \le n$, $0 < \omega$, в $L_{ПРК}(m, n+k)$ полностью определяется всеми подходящими расстановками нулей в элементах из $D_{\le}(i)$, $1 \le i \le n$. Поэтому существует сюръекция $n+k$-уровня и веса $\omega \le n$ решетки $L_{ПРК}(m, n+k)$ на $D_{\le}(n)$. ■

В свете вышесказанного становится очевидным, что теория L-кодирования не ограничена рамками проблематики лишь равномерных кодов, потому что, например, элементы любой решетки $D_{\le}(n)$ композиций, как и доминирующего порядка $D(n)$, могут быть взяты и как слова неравной длины, а потому и как неравномерный код постоянного веса (см. рис. 2).

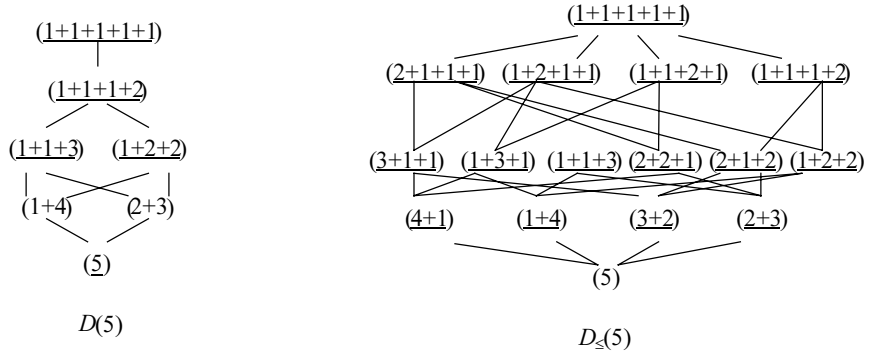

Рис. 2

К тому же изоморфизм $D_{\leq}(n) \cong Bool(n–1)$ можно использовать для кодирования с переходом от слов 11…1, 21…1, …, 1…12,…, *n*–11, *n* соответственно длины от *n* до 1 над алфавитом {1, …, *n*} к словам равной длины *n*–1 над алфавитом {0, 1}, а также для обратного перехода. Можно также использовать вложения решетки $D_{\leq}(n)$ в подходящую решетку $D_{\leq}(n + k)$, $k = 1, \ldots$, при расширении кода и обратно: использовать наложения $D_{\leq}(n + k)$ на $D_{\leq}(n)$ при сжатии (сужении) кода, выкалывании и т.п.; эти же приемы, естественно, можно использовать для $L_{\text{ПРК}}(m, n)$ при вложениях ее в $L_{\text{ПРК}}(m+k, n)$ или $L_{\text{ПРК}}(m+k, n+t)$, $k, t \geq 1$, или при их наложениях на $L_{\text{ПРК}}(m, n)$. Тем самым получаем различные способы и кодирования, и шифрования (точнее, кодошифрования – шифрования закодированного сообщения).

3. Структуры матроидного типа: матроиды и *c*-матроиды

Множество *S* вместе с оператором замыкания $A \to \bar{A}$ называется матроидом [10, 11], если для всех $A \subseteq S$ и любых $p, q \in S$ выполняются аксиомы замены Штейница и конечного базиса.

Как известно [10, гл. II, § 3, теорема 2.29 (Биркгоф – Уитни)], множество точек $T = \{p: p \in L_\gamma\}$ геометрической решетки L_γ вместе с оператором замыкания $\varphi: T' \to \bar{T}' = \{p: p \leq \sup(T'),\ p \in T, \varnothing \neq T' \subseteq T\}$ и аксиомой замены Штейница является простым матроидом.

В частности, из этого предложения и теоремы 1 извлекаем следующее утверждение.

Утверждение 2. Множество *T* точек булевой решетки двоичного ПР-кода над алфавитом $A = \{0, 1\}$ с оператором замыкания φ и аксиомой замены Штейница является простым матроидом. Если к *T* добавить о и взять пару: множество $T \cup \{o\}$ вместе с отношением порядка ≤, являющимся ограничением порядка булевой решетки на $T \cup \{o\}$, то пара $<T \cup \{o\}, \leq>$ превращается в суперматроид (определение суперматроида и его свойства см. в [12, 13]). ■

Определение [2]. Множество всех *c*-элементов $C \subseteq L$ вместе с оператором замыкания φ называется *c*-матроидом, если для всех $C' \subseteq C$, $C' \neq \varnothing$, и любых $c_1, c_2 \in C$ выполняется следующая аксиома замены:

из $c_1 \notin \varphi(C')$ и $c_1 \in \varphi(C' \cup c_2)$ следует существование такого c_2', что $o < c_2' \leq c_2$ и $c_2' \in \varphi(C' \cup c_1)$.

Как указано в теореме 1, множество всех *c*-элементов решетки L_A является *c*-матроидом, а при добавлении к ним всех элементов рангов, соответствующих рангам *c*-элементов, оказывается суперматроидом.

Исследование *c*-матроидов связано также с 25-й проблемой Скорнякова [14]: исследовать дедекиндовы структуры, в которых каждый элемент представляется в форме $a = \sum_{i=1}^{n(a)} La_i$, где La_i – цепи, в частности конечные (дедекиндовы структуры – это модулярные решетки), см. [2].

Заключение. Структуры других моделей

Приведем здесь кратко факты, подтверждающие, что и многие другие модели, используемые в кодировании и криптографии, имеют структуры, являющиеся *s*-множествами, в частности решетками.

Геометрические коды, как известно, строятся над геометриями. С геометриями, в которых две различные точки определяют единственную прямую (однозначные геометрии), выпуклыми геометриями, матроидами и антиматроидами ассоциированы геометрические и слабо полудистрибутивные решетки [15]. По этому поводу отметим следующее. Неоднозначные геометрии (две различные точки не обязательно определяют единственную прямую, например, как в геометрии Мебиуса) ассоциированы не с решетками, а с геометрическими *ML*-решетками и *p*-матроидами [2, 3].

О структурах моделей дискретных систем, в том числе автоматов и ассоциированных с ними языков, см. [16 – 18], где показано, что эти структуры являются решетками или полурешетками.

О семиотических моделях информации, моделях неопределенности и соответствующих им *s*-множествах и решетках см. [7, 19, 20].

Проблемы и вопросы теории кодирования и криптографии приведены в [8, 9], см. также [1, 3 – 5, 10].

ЛИТЕРАТУРА

1. *Кутьин А.М.* Коды и решетки // Вестник ТГУ. Приложение. 2006. № 17. С. 30 – 34.
2. *Кутьин А.М.* Р-матроиды // Дискретная математика. 2005. Т. 17. Вып. 3. С. 146 – 160.
3. *Кутьин А.М.* Проблемы теории кодирования и теория геометрий // Проблемы информатизации региона. Красноярск: Изд-во КТГУ, 2001. С. 90 – 103.
4. *Кутьин А.М.* Открытые вопросы теории кодирования и криптографии. I // Проблемы информатизации региона. Красноярск: Изд-во КТГУ, 2001. С. 74 – 91.
5. *Кутьин А.М.* Информация, безопасность, кодирование и решетки. III // Проблемы информатизации региона: Шестая Всерос. науч.-практич. конф.: Доклады. Красноярск: Изд-во КТГУ, 2000. С. 74 – 79.
6. *Кутьин А.М.* Вопросы теории кодирования и решетки // Безопасность информационных технологий. М.: МИФИБ, 2001. № 4. С. 79 – 84.
7. *Кутьин А.М.* О моделях информации. II // Информационная реальность и цивилизация. Красноярск: Изд-во САА, 1998. С. 73 – 81.
8. *Конвей Дж.*, *Слоэн Н.* Упаковки шаров, решетки и группы. Т. 1. М.: Мир, 1990.
9. *Мак-Вильямс Ф.Дж.*, *Слоэн Н.Дж.А*. Теория кодов, исправляющих ошибки. М.: Связь, 1979.
10. *Айгнер М.* Комбинаторная теория. М.: Мир, 1982. 558 с.
11. *Биркгоф Г.* Теория решеток. М.: Мир, 1984.
12. *Емеличев В.А*., *Ковалев М.М*., *Кравцов М.К*. Многогранники, графы, оптимизация. М.: Наука, 1981.
13. *Ковалев М.М.* Матроиды в дискретной оптимизации. Минск: Изд-во Университетское, 1987.
14. *Скорняков Л.А*. Дедекиндовы структуры с дополнениями и регулярные кольца. М.: Физматгиз, 1961.
15. *Горбунов В.А.* Алгебраическая теория квазимногообразий. Новосибирск: Научная книга, 1999.
16. *Агибалов Г.П.* Дискретные автоматы на полурешетках. Томск: Изд-во Том. ун-та, 1993.
17. *Богомолов А.М.*, *Салий В.Н.* Алгебраические основы теории дискретных систем. М.: Наука, 1997.
18. *Салий В.Н*. Представление языков в решеточных автоматах // Методы и системы техн. диагностики. 1992. № 17. С. 33 – 36.
19. *Кутьин А.М.* К теории неопределенности: модели и структуры // Вестник КГТУ. Математические методы и моделирование. 2003. № 30. С. 14 – 27.
20. *Кутьин А.М.* Теория направленных *s*-множеств // Вестник КГТУ. 2001. Вып. 26. С. 117 – 126.