Компьютерная математика

УДК 519.854

В.П. ШИЛО, В.А. РОЩИН, Д.А. БОЯРЧУК, П.В. ШИЛО

АЛГОРИТМ ТОЧНОГО РЕШЕНИЯ ЗАДАЧИ ПОСТРОЕНИЯ ПОМЕХОЗАЩИЩЕННОГО КОДА МАКСИМАЛЬНОГО ОБЪЕМА ДЛЯ *Z*-КАНАЛА

Для точного решения задачи построения помехозащищенного кода максимального объема для Z-канала, которая сводится к задаче нахождения максимального независимого множества вершин графа, предложен алгоритм ветвей и границ. Предложенный способ ветвления с использованием специфики рассматриваемых графов дает возможность резко сократить объем вычислений в разработанном алгоритме.

Введение. Интерес к задачам получения надежных кодов, позволяющих корректировать искажения информации при ее передаче, вызван развитием современных средств связи, Интернета, различных компьютерных технологий. Нередко при исследовании проблем теории кодирования возникают задачи, математические модели которых описываются в терминах дискретного программирования. Такими являются, например, задачи построения помехозащищенных кодов, нахождения оценок их объема.

Постановка задачи. Пусть B^n – множество n-мерных векторов $x = (x_1, \ldots, x_n)$, координаты которых принимают значения 0 или 1. Двоичным кодом C называется произвольное подмножество множества B^n, под объемом |C| кода подразумевается мощность этого подмножества. Число n будем называть длиной кода.

Предположим, что вектор $x^i \in B^n$ из-за ошибок при передаче информации может переходить в один из элементов произвольного множества $R(x^i)$, $i = 1, \ldots, 2^n$.

Двоичный код $C \subset B^n$ называется помехозащищенным, если для любых $x, y \in B^n$, $x \neq y$, выполняется условие $(R(x) \cup \{x\}) \cap (R(y) \cup \{y\}) = \varnothing$.

Задача построения помехозащищенного кода максимального объема сводится к задаче нахождения максимального независимого множества вершин графа [1]. Подмножество $I \subset V$ вершин графа $G(V, E)$ называется независимым, если никакие две его вершины не связаны ребром. Независимое множество $I_{\max}$ называется максимальным независимым, если для любого независимого множества I выполняется соотношение $|I_{\max}| \geq |I|$.

Лексикографически упорядочим векторы $x \in B^n$ по возрастанию: $x^1 = (0,...,0) \prec x^2 \prec ... \prec x^k = (1,...1), k = 2^n$. Тем самым определим взаимно-однозначное преобразование подмножества $\{1,...,2^n\}$ множества натуральных чисел в векторы $x \in B^n : \chi(i) \to x^i, i = 1,...,2^n$. Определим граф $G(V, E)$ следующим образом. Предположим, что множество V вершин графа состоит из 2^n вершин и ребро $(v_i, v_j) \in E$ тогда и только тогда, когда $(R(\chi(v_i)) \cup \{\chi(v_i)\}) \cap (R(\chi(v_j)) \cup \{\chi(v_j)\}) \neq \varnothing$. Если найдено независимое множество I в $G(V, E)$, то очевидно, что тем самым построен помехозащищенный код C. Он состоит из двоичных векторов, соответствующих вершинам независимого множества $I : C = \{\chi(v) : v \in I\}$.

Обозначим $\alpha(G)$ – число элементов в максимальном независимом множестве $I_{\max}$ ($\alpha(G) = |I_{\max}|$). Задачу нахождения максимального независимого множества вершин графа можно сформулировать как задачу целочисленного программирования с булевыми переменными. Поставим в соответствие каждой вершине $v_j \in V$ заданного графа $G(V, E)$ переменную $x_j \in \{0,1\}$, $j = 1,…, k$, а произвольному вектору $x = (x_1,..., x_k)$ – множество $I(x) = \{v_j \in V : x_j = 1, j = 1,..., k\}$. Тогда математическая модель задачи нахождения максимального независимого множества вершин графа описывается таким образом: найти

$$\max\left\{ f(x) = \sum_{i=1}^{k} x_i \prod_{j:(v_i, v_j)\in E} (1 - x_j) : x \in B^k \right\}. \quad (1)$$

Если множество $I(x)$ – независимое, то значение целевой функции $f(x)$ равно количеству его элементов.

Использование специфики графов. Предположим, что P – множество всех перестановок $p = (p_1,..., p_n)$ целых чисел от 1 до n. Для произвольной перестановки $p \in P$ рассмотрим следующие преобразования $B^n \Rightarrow B^n$:

$$x = (x_1,..., x_n) \Rightarrow y = (x_{p_1},..., x_{p_n}), \quad (2)$$

$$x = (x_1,..., x_n) \Rightarrow y = (\bar{x}_{p_1},..., \bar{x}_{p_n}). \quad (3)$$

Множество всех таких преобразований обозначим Ψ, $|\Psi| = 2n!$.

Определение. Преобразование $\psi\in\Psi$ будем называть правильным, если из условия $(v_i, v_j)\notin E$ следует, что $(\chi^{-1}(\psi(\chi(v_i))), \chi^{-1}(\psi(\chi(v_j))))\notin E$.

В дальнейшем для простоты изложения вместо $\chi^{-1}(\psi(\chi(v)))$ будем использовать запись $\psi(v)$. Обозначим Q – множество всех правильных преобразований. Пусть $I(v)$ – независимое множество, в которое входит вершина $v\in V$. Обозначим $\alpha(G,v)$ – число элементов в максимальном независимом множестве $I_{\max}(v)$ ($\alpha(G,v) = |I_{\max}(v)|$).

Справедлива теорема [2].

Теорема 1. Пусть $\psi \in Q$. Тогда имеет место неравенство $\alpha(G, v) \leq \alpha(G, \psi(v))$.

Предположим, что $\psi \in C$. Тогда справедливо неравенство $\alpha(G, v) \leq \alpha(G, \psi(v))$.

Для произвольной вершины $v\in V$ рассмотрим множество вершин графа $M(v) = \{u\in V : u = \psi(v),\ \psi\in C\}$. Из теоремы 1 следует, что если $\alpha(G, v) \leq k$, то тем самым установлено, что $\alpha(G, u) \leq k$, $u \in M(v)$.

Для произвольного двоичного вектора x определим величину $w(x) = \sum_{j=1}^{n} x_j$ – его вес. Вес вершины v определим как вес вектора $\chi(v)$: $w(v) = w(\chi(y))$, $y \in B^n$.

Имеет место

Лемма 1. Для любой пары вершин $v_i, v_j \in V$ выполняется соотношение $\left| w(v_i) - w(v_j) \right| = \left| w(\psi(v_i)) - w(\psi(v_j)) \right|$.

Доказательство. В случае, если преобразование ψ относится к типу (2), то очевидно, что $w(\chi(x)) = w(\psi(\chi(x)))$ для любого $x\in V$, а если – к типу (3), то $w(\chi(x)) = n - w(\psi(\chi(x)))$ для любого $x\in V$. Это и доказывает справедливость леммы.

Для практики особый интерес представляют помехозащищенные коды для Z-канала, схема которого показана на рисунке. Z-канал – это асимметрический двоичный канал. При передаче информации в нем вероятность ошибки – перехода 1 в 0 равна p, а вероятность ошибки – перехода 0 в 1 равна 0.

В работе [3] введено асимметрическое расстояние $d_A(x, y) = \max(N(x, y), N(y, x))$ между векторами x, $y \in B^n$, где $N(x, y) = \left| \{ i : x_i = 0 \wedge y_i = 1 \} \right|$.

Оно связано с расстоянием по Хеммингу $d_H(x,y) = \sum_{i=1}^{n} |x_i - y_i| = N(x, y) + N(y, x)$ следующим соотношением:

$$2\,d_A(x,y) = d_H(x,y) + |\,w(x) - w(y)\,|\,. \qquad (4)$$

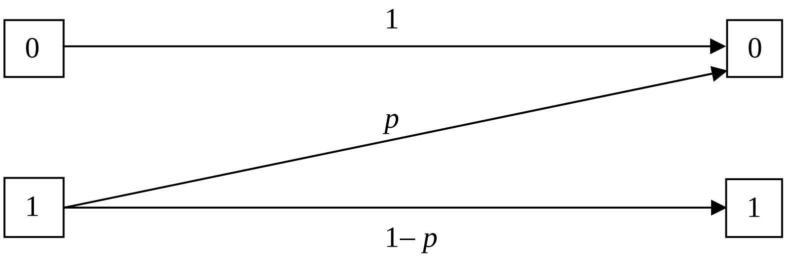

РИСУНОК. Схема *Z*-канала

Для кода $C \subset B^n$ определим минимальное асимметрическое расстояние

$$\Delta = \min\{d_A(x,y) : x, y \in C,\ x \neq y\}.$$

Доказано [3], что код C с минимальным асимметрическим расстоянием Δ может корректировать не более $(\Delta - 1)$ асимметрических ошибок (переходов 1 в 0). Далее будем рассматривать коды с минимальным асимметрическим расстоянием $\Delta = 2$.

Пусть в графе $G(V, E)$ ребро $(v_i, v_j) \in E$, $i, j = 1, \ldots n$, тогда и только тогда, когда $d_A(\chi(v_i), \chi(v_j)) < \Delta$.

Справедливы следующие утверждения [2]

Лемма 2. Если любая пара вершин $v_i,\ v_j \in V$, то для нее имеет место соотношение $d_A(\chi(v_i), \chi(v_j)) = d_A(\psi(\chi(v_i)), \psi(\chi(v_j)))$.

Из леммы 2 следует, что для графа $1zc$ все преобразования $\psi \in \Psi$ – правильные. Вершины $x, y \in V$ назовем эквивалентными, если $\alpha(G, x) = \alpha(G, y)$.

Теорема 2. Пусть произвольные вершины $v_i, v_j \in V$, такие, что $w(v_i) = w(v_j)$ или $w(v_i) + w(v_j) = n$. Тогда они эквивалентны в графе $1zc2^n$.

Изучим структуру графа $1zc2^n$. Из равенства (4) следует, что вершины $v_i,\ v_j \in V$ связаны ребром, если выполняется неравенство

$$d_H(\chi(v_i), \chi(v_j)) + |w(\chi(v_i)) - w(\chi(v_j))| \leq 2\,. \qquad (5)$$

Из соотношения (5) следует лемма.

Лемма 3. В графе $1zc2^n$ могут быть связаны ребром только те вершины, абсолютная величина разности весов которых не превосходит 1.

Для каждой вершины $v_i \in V$ определим вершину $\overline{v}_i$: $x = \chi(v_i), \overline{v}_i = = \chi^{-1}(y), y : y_j = 1 - x_j, i, j = 1,...,n$. Легко видеть, что справедлива

Лемма 4. В любом графе $1zc2^n$ не существует ребер $(v_i, \overline{v}_i), v_i \in V$. Доказательство леммы следует из соотношения (5) и способа определения вершины $\overline{v}_i$.

Покажем, что имеет место следующая теорема.

Теорема 3. Пусть $v_i, v_j \in V,\ i, j = 1,...,n$. Тогда:

1) если ребро $\left(v_i, v_j\right) \in / \notin E$, то и ребро $\left(\overline{v}_i, \overline{v}_j\right) \in / \notin E$;

2) если ребро $\left(v_i, v_j\right) \in E$, то ребро $\left(v_i, \overline{v}_j\right) \notin E$.

Доказательство. Первая часть утверждения – следствие леммы 2. Если $\left(v_i, v_j\right) \in E$, то $d_H(\chi(v_i), \chi(v_j)) = 1$ и, следовательно, $d_H(\chi(v_i), \chi(\overline{v}_j)) = n - 1$, $d_A(x, y) = n/2$.

Правильное преобразование $\psi \in \Psi$ называется совершенным, если выполняются условия:

1) $v_i \neq \psi(v_i), v_i = \psi\left(\psi(v_i)\right)$;

2) ребро $\left(v_i, \psi(v_i)\right) \notin E, v_i \in V$;

3) если ребро $\left(v_i, v_j\right) \in / \notin E$, то и ребро $\left(\psi(v_i), \psi(v_j)\right) \in / \notin E$;

4) если ребро $\left(v_i, v_j\right) \in E$, то ребро $\left(v_i, \psi(v_j)\right) \notin E$.

Очевидно, что множество совершенных преобразований не пусто, так как в него входят преобразования, переводящие вершины $v_i \in V$ графа в $\overline{v}_i$.

Пусть $\psi \in \Psi$ – совершенное преобразование.

Рассмотрим следующий алгоритм преобразования множества.

Шаг 1. Предположим, что S – некоторое подмножество множества V вершин графа. Полагаем $r = 0$.

Шаг 2. Из множества S выбираем произвольную вершину v_{i_r} и вершину $\psi(v_{i_r})$. Если это невозможно, алгоритм заканчивает работу.

Шаг 3. Удаляем из множества S вершины $v_{i_r}, \psi(v_{i_r})$ и все вершины, связанные с ними ребром.

Шаг 4. Если множество S не пусто, полагаем $r = r + 1$ и переходим на шаг 2. В противном случае алгоритм заканчивает работу.

Назовем множество S разложимым, если алгоритм заканчивает его рассмотрение на шаге 4. Легко показать, что имеет место следующая теорема.

Теорема 4. Множество S, состоящее из всех вершин графа $1zc2^n$, разложимо. Пары $(v_{i_r}, \psi(v_{i_r}))$, $r = 1,\ldots,R$, полученные в результате работы алгоритма, образуют независимое множество.

Вышеприведенные утверждения дают основания для существенного уменьшения числа узлов (кандидатов) для ветвления в предлагаемом точном алгоритме ветвей и границ, базирующийся на использовании неявного перебора пар вершин $(v_i, \psi(v_i))$ графа. Если выбрана какая-то пара $(v, \psi(v))$, то все вершины, соединенные с ней ребром, удаляются из рассматриваемого графа.

Алгоритм

Шаг 1. **Инициализация.** $l = 0$, $V_l = V$, $E_l = E$, $mis_l = 0$. По некоторому правилу выбираем совершенное преобразование $\psi \in \Psi$ и набор пар $P_l = \{(v_{i_r}, \psi(v_{i_r}))\}$, $v_{i_r}, \psi(v_{i_r}) \in V_l, r = 1,\ldots,q_l$, обладающий свойством $Est(V_l \setminus P_l) \le l\_mis - mis_l$ ($Est()$ – функция оценки) $p_l = 0$.

Шаг 2. **Ветвление *l*-го уровня.** $V_{l+1} = V_l$, $E_{l+1} = E_l$. Из графа $G(V_{l+1}, E_{l+1})$ удаляем вершины $(v_{i_r}, \psi(v_{i_r}))$, $r = 1,\ldots, p_l$. Полагаем $p_l = p_l + 1$ и выбираем пару $(v_{i_{p_l}}, \psi(v_{i_{p_l}}))$. Из графа $G(V_{l+1}, E_{l+1})$ удаляем вершины, связанные ребром с вершинами пары $(v_{i_{p_l}}, \psi(v_{i_{p_l}}))$, и вершины этой пары (если $v \in V_{l+1}$ и $(v, v_{i_{p_l}}) \in E_{l+1}$ или $(v, \psi(v_{i_{p_l}})) \in E_{l+1}$, вершина v удаляется).

Шаг 3. **Оценка *l*-го уровня.** $mis_{l+1} = mis_l + 2$. Если $l\_mis < mis_{l+1}$, полагаем $l\_mis = mis_{l+1}$. Если $Est(V_{l+1}) \le l\_mis - mis_{l+1}$, переходим на шаг 4. Иначе полагаем $l = l + 1$ и переходим на шаг 2.

Шаг 4. Если $p_l < q_l$, переходим на шаг 2. Иначе полагаем $l = l - 1$ и при l ñ 0 переходим на шаг 2. Иначе останов.

Интересным является свойство графов $1zc2^n$. В них переменные, соответствующие вершинам с весом $n/2$ (при четном n) или переменные, соответствующие вершинам с весом $(n-1)/2$ и $1 + (n-1)/2$ (при нечетном n), – связывающие в задаче (1). То есть, если задать им какие-то значения, то задача (1) распадается на две независимые симметрические подзадачи вида (1) с переменными, соответствующими вершинам с весом, меньшим $n/2((n-1)/2)$ и переменными, соответствующими вершинам с весом, большим $n/2(1 + (n-1)/2)$.

Имеет место следующая теорема.

Теорема 5. Алгоритм ветвей и границ, основанный на использовании неявного перебора пар вершин, успешно заканчивает работу и находит в графе $1zc2^n$ замкнутое к включению независимое множество вершин с мощностью, равной четному числу.

Справедливость теоремы следует из вышеприведенных утверждений.

Выводы. Предложенный в данной работе способ неявного перебора пар вершин использует специфику рассматриваемых графов и позволяет намного уменьшить объем вычислений в разработанном алгоритме ветвей и границ. С помощью программной реализации этого алгоритма на PC Intel CoreTM i7-3770 CPU 3.40 GHz и 8.0GB RAM за 1757 минут улучшена верхняя оценка для графа 1zc1024 с 117 до 113 (при известном решении 112).

В.П. Шило, В.О. Рощин, Д.О. Боярчук, П.В. Шило

АЛГОРИТМ ТОЧНОГО РОЗВ'ЯЗАННЯ ЗАДАЧІ ПОБУДОВИ ЗАВАДОЗАХИЩЕНОГО КОДУ МАКСИМАЛЬНОГО ОБ'ЄМУ ДЛЯ *Z*-КАНАЛУ

Для точного розв'язання задачі побудови завадозахищеного коду максимального об'єму для *Z*-каналу, яка зводиться до задачі знаходження максимальної незалежної множини вершин графу, запропоновано алгоритм гілок і меж. Запропонований спосіб розгалуження з використанням специфіки розглянутих графів дає можливість суттєво зменшити об'єм обчислень у розробленому алгоритмі.

V.P. Shylo, V.A. Roshchyn, D.A. Boyarchuk, P.V. Shylo

EXACT ALGORITHM FOR FINDING THE LARGEST CORRECTING CODES PROBLEM FOR *Z*-CHANNEL

Branch and bound algorithm for exact solving the problem of construction of error-correcting codes for Z-channel, which can be transformed into maximum independent set problem, is proposed.
The proposed branching technique using the specificity of the graphs being considered provides a significant reduction of calculations in the developed algorithm.

1. *Сергиенко И.В., Шило В.П.* Задачи дискретной оптимизации: проблемы, методы решения, исследования. Киев: Наук. думка, 2003. 264 с.
2. *Шило В.П.* Точное решение задачи построения помехозащищенного кода максимального объема. *Компьютерная математика*. Киев: Ин-т кибернетики имени В.М. Глушкова НАН Украины, 2005. № 2. С. 147 – 156.
3. *Rao T.R.N., Chawla A.S.* Asymmetric error codes for some LSI semiconductor memories. *Southeastern Symp. System Theory*. 1975. P. 170 – 171.

Получено 03.05.2017

Об авторах:

Шило Владимир Петрович,
доктор физико-математических наук, профессор, ведущий научный сотрудник
Института кибернетики имени В.М. Глушкова НАН Украины,
E-mail: v.shylo@gmail.com

Рощин Валентина Алексеевна,
кандидат физико-математических наук, старший научный сотрудник
Института кибернетики имени В.М. Глушкова НАН Украины,
E-mail: v.roshin@gmail.com

Боярчук Дмитрий Алексеевич,
научный сотрудник Института кибернетики имени В.М. Глушкова НАН Украины,
E-mail: dopt135@gmail.com

Шило Петр Владимирович,
младший научный сотрудник Института кибернетики имени В.М. Глушкова НАН Украины.
E-mail: petershylo@gmail.com