Математика и ее приложения : ЖИМО. 2013. Вып. 1 (10). С. 43–46

УДК 512.543

А. А. Толстопятов[1]

Кодирующее уравнение и выбор порождающих при булевом сжатии файлов

Ключевые слова: разбиение файла, булевы полиномы.

Рассмотрен вопрос о зависимости существования решений кодирующего уравнения от выбора порождающих булевых полиномов. Получено уравнение, позволяющее построить кодирующее уравнение, систему порождающих и замену аргументов кодирующего уравнения на порождающие.

Key words: boolean compress, boolean Polynomial.

Considered the question of the dependence of the existence of solutions of a coding equations from the choice of generating Boolean polynomials. Equation is obtained, which helps you build encoder equation, the system of generators and a replacement arguments encoding equations on generating.

Предложенный в [1] подход к сжатию файлов основан на разбиении файла на кортежи равной длины, объединении, вообще говоря, разного числа кортежей в буферы и сопоставлении кортежам, входящим в отдельный буфер булева уравнения, решениями которого эти кортежи являются. Такой подход позволяет использовать для сжатия файла не только линейные зависимости между буферами, которые можно рассматривать как элементы 2-х мерного линейного векторного пространства над GF(2), но нелинейные зависимости между булевыми полиномами, кодирующими поля принадлежности каждого буфера. Для построения кода файла надо выбрать систему порождающих булевых полиномов. выразить через них булевы полиномы, кодирующие поля принадлежности и построить кодирующее уравнение, из которого эти полиномы могут быть получены. В работах [2] и [3] было показано, как отделить эти две задачи друг от друга. В [2] была получена формула, определяющая число порождающих булевых полиномов и высказаны соображения, что за редчайшим исключением это число совпадает с числом булевых переменных, от которых зависят полиномы, кодирующие поля принадлежности. Но это число есть длина кортежа.

Далее, если число порождающих равно длине кортежа, то естественно в качестве этих порождающих взять сами булевы переменные, от которых зависят полиномы, кодирующие поля принадлежностей. Но в этом случае кодирующее уравнение может не иметь решений, а значит построение кода будет невозможно.

[1]Ивановский государственный университет; E-mail: khash2@mail.ru Работа выполнена при финансовой поддержке РФФИ (проект 13-07-00628a)

В данной работе рассматривается вопрос о том, может ли повлиять замена порождающих без изменения их числа на существование решений кодирующего уравнения.

Для ответа на этот вопрос достаточно получить уравнение на параметры, задающие кодирующее уравнение, порождающие булевы полиномы и подстановку вместо аргументов кодирующего уравнения тех или иных полиномов из системы порождающих. Тогда решение (или его отсутствие) этого уравнения дает ответ на поставленный выше вопрос.

Введем следующие обозначения:
1. x_i – булевы переменные; $i = 1, \ldots, n$.
2. n – длина кортежа.
3. L – число буферов.
4. $f_l(x_i)$ – булев полином, кодирующий поле принадлежности l-го буфера
5. P – число булевых полиномов в системе порождающих.
6. $\varphi_p(x_i),\ p = 1, \ldots, P$ – p-й булев полином из системы порождающих.
7. I – число аргументов полинома кодирующего уравнения.
8. $l_k,\ k = 1, \ldots, I$ – k-й аргумент кодирующего уравнения.
9. $F(e_k)$ – полином кодирующего уравнения.
10. $L_j(x_i)$ – j-й полином Лагранжа от булевых переменных x_i, $i = 1, \ldots, n$, $j = 0, \ldots, 2^n - 1$.
11. $L_s(e_k)$ – s-й полином Лагранжа от булевых переменных e_k, $k = 1, \ldots, I$, $s = 0, \ldots, 2^I - 1$.

Пусть

$$f_l(x_i) = \sum_{j=0}^{2^n-1} C_{lj} L_j(x_i)\ , \tag{1}$$

В (1) $L_j(x_i)$ – полиномы Лагранжа, определяемые согласно:

$$L_j(x_i) = \prod_{k=1}^{n} L_{jk}(x_k)\ , \tag{2}$$

где $j_k \in \{0, 1\}$ определяется из

$$j = \sum_{k=1}^{n} j_k 2^{k-1}\ , \tag{3}$$

а $L_0(x)$ и $L_1(x)$ есть:

$$L_0(x) = x + 1, \quad L_1(x) = x\ . \tag{4}$$

Отметим, что согласно (3) и (4), справедливо

$$L_{jk}(x_k) = x_k + j_k + 1\ . \tag{5}$$

Из (2) нетрудно получить, что:

$$\sum_{j=0}^{2^n-1} L_j(x_i) = 1\ . \tag{6}$$

Полиномы Лагранжа $L_k(e)$ могут быть введены и для булевых переменных $e_i, i = 1, \ldots, I$, являющихся аргументами полинома кодирующего уравнения $F(e_s)$, согласно

$$L_k(e_s) = \prod_{s=1}^{I} L_{k_s}(e_s) \ , \tag{7}$$

где

$$k = \sum_{s=1}^{I} k_s 2^{s-1} \ , \tag{8}$$

причем из (4) и (10) следует, что:

$$L_k(e_s) = e_s + k_s + 1 \ . \tag{9}$$

Полином кодирующего уравнения $F(e_s)$ может быть разложен по полиномам Лагранжа $L_k(e_s)$:

$$F(e_s) = \sum_{k=0}^{2^I-1} A_k L_k(e_s) \ , \tag{10}$$

или, используя (9) и (11), можно записать (12) так:

$$F(e_s) = \sum_{k=0}^{2^I-1} A_k \prod_{s=1}^{I} L_{k_s}(e_s) \ , \tag{11}$$

Булевы полиномы $\varphi_p, \ p = 1, \ldots, P$ из системы порождающих можно разложить по полиномам Лагранжа $L_j(x)$:

$$\varphi_p = \sum_{j=0}^{2^n-1} b_{pj} L_j(x) \ . \tag{12}$$

Кодирующее уравнение есть

$$F(e_s^l) = f_e(x_i) \ , \tag{13}$$

где e_s^l один из полиномов, порождающих φ_p, который для l-го буфера ставится в полином кодирующего уравнения вместо e_s. Эта подстановка может быть представлена как:

$$e_s^l = \sum_{p=1}^{P} a_{sp}^l \varphi_P \ , \tag{14}$$

где L матрица a_{sp} размерностью $I \times P$ в каждой из I строк имеют одну 1 и $I - 1$ нулей.

Подставляя (14) в (16), далее (16) в (13), и (13) в (15). При этом учтем, что, согласно (6) будем иметь, что:

$$k_s + 1 = \sum_{j=0}^{2^n-1} (k_s + 1) L_j(x) \ . \qquad (15)$$

Кроме того, в полученном выражении можно переставить произведение по s и сумму по j, а затем переставить суммы по k и по j. В результате будем иметь:

$$\sum_{j=0}^{2^n-1} \left\{ \sum_{k=0}^{2^I-1} A_k \left[\prod_{s=1}^{I} \left(\sum_{p=1}^{P} a_{sp}^l b_{pj} + k_s + 1 \right) \right] + C_{l_j} \right\} L_j(x) = 0. \qquad (16)$$

Из определения полиномов Лагранжа (2) и (4) следует, что:

$$L_i L_j = L_j \delta_{ij}. \qquad (17)$$

Из (19) следует, что полиномы Лагранжа линейно независимы. Но тогда (18) будут выполнятся только, если в ноль обращаются все коэффициенты при $L_j(x)$:

$$\sum_{k=0}^{2^I-1} A_k \left[\prod_{s=1}^{I} \left(\sum_{p=1}^{P} a_{sp}^l b_{pj} + k_s + 1 \right) \right] + C_{l_j} = 0. \qquad (18)$$

В системе булевых уравнений заданы величины C_{lj}, а следующие переменные:

1. A_k – задающие полином кодирующего уравнения $F(e_s)$.
2. b_{pj} – задающие p-ый полином системы порождающих.
3. a_{sp}^l – задающие подстановку полиномов системы порождающих вместо.

являются используемыми булевыми переменными.

Так как из уравнений (20) коэффициенты b_{pj} разложения (14) не исчезли, то это значит, что выбор системы порождающих может повлиять на существование кодирующего уравнения и его решений.

Однако, при таком подходе задачи о построении кодирующего уравнения и порождающих не отделены друг от друга.

Список литературы

1. *Толстопятов А. А.* О возможности использования булевых уравнений для сжатия файлов // Вестник Иван. гос. ун-та. 2003. Вып 3. С. 82–84.

2. *Толстопятов А. А.* Построение системы порождающих полиномов при булевом сжатии файлов // Математика и ее приложения : журн. Иван. мат. о-ва. 2010. Вып. 1(7). С. 59–68.

3. *Толстопятов А. А.* Построение кодирующего уравнения при булевом сжатии файлов // Математика и ее приложения : журн. Иван. мат. о-ва. 2010. Вып. 1(7). С. 69–82.

Поступила в редакцию 26.11.2013.