УДК 512.45; 621.391

Л. П. БЕДРАТЮК
Хмельницький національний університет

ВАГОВІ ФУНКЦІЇ САМОДУАЛЬНОГО КОДУ

Розроблено критерій перевірки чи довільний многочлен від двох змінних є ваговою функцією деякого парного самодуального бінарного коду.

1. Розглянемо простір Хеммінга F_q^n і лінійний код C в F_q^n розмірності k, де F_q - скінченне поле характеристики $p, q = p\hat{}k$. Спектром коду C називається набір цілих чисел A_0, A_1, … A_n, де A_i -- кількість векторів з C які мають вагу i. Традиційно спектр коду зображується ваговим многочленом

$$W_C(x,y) = \sum_{i=0}^{n} A_i x^{n-i} y^i.$$

Вагові многочлени $W_C(x,y)$, $W_{C^\perp}(x,y)$ коду C і дуального йому коду $C^\perp$ зв'язані співвідношенням Мак-Вільямс [1]:

$$W_C(x,y) = q^{k-n} W_{C^\perp}(x+(q-1)y, x-y).$$

Нагажаємо, що код C називається самодуальним, якщо $C = C^\perp$. Багато хороших кодів є самодуальними, наприклад код Голея, деякі квадратично-лишкові коди. Для бінарного ($p = 2$) самодуального коду співвідношення Мак-Вільямс набуває вигляду

$$W_C(x,y) = W_C\left(\frac{x+y}{\sqrt{2}}, \frac{x-y}{\sqrt{2}}\right).$$

Отже, ваговий многочлен самодуального коду є інваріантом деякої групи перетворень, що накладає сильне обмеження на можливий аналітичний вираз для таких многочленів. Для бінарних самодуальних кодів має місце теорема Глісона, див. [2], яка стверджує, що довільний ваговий многочлен парного самодуального бінарного коду є многочленом від двох многочленів W_1 і W_2, де

$$W_1 = x^8 + 14x^4y^4 + y^8,$$

$$W_2 = x^{24} + 759x^{16}y^8 + 2576x^{12}y^{12} + 759x^8y^{16} + y^{24}.$$

Многочлени W_1 і W_2 є в ваговими многочленами розширеного (8,4,4)-коду Хеммінга і (24,12,8)-коду Голея відповідно.

В той же час, питання чи даний многочлен від двох змінних може бути ваговим многочленом деякого самодувального коду є відкритою алгоритмічною проблемою. Це повязано з тим, що для кілець многочленів не існує ефективного алгоритму перевірки належності елемента підкільцю. В даній роботі знайдено необхідні умови яким задовольняє ваговий многочлен бінарного самодуального коду.

2. В кільці многочленів $\mathsf{Z}[x,y]$, де Z - кільце цілих чисел, розглянемо підкільце W породжене многочленами W_1 і W_2. Для довільного многочлена $f \in \mathsf{Z}[x,y]$ питання його належності до кільця W може бути розв'язане при допомозі відомого алгоритму, який грунтується на теорії базисів Грьобнера, див. [3]. Більш детально розглянемо допоміжне кільце $\mathsf{Z}[x,y,z,t,s]$ і його ідеал

$$I = (f - z, t - W_1, s - W_2).$$

Побудуємо базис Грьобнера $GB(I)$ ідеалу I. Добре відомо, що коли перетин

$$GB(I) \cap \mathsf{Z}[z,t,s]$$

є порожньою множиною, то тоді многочлен f не належить до кільця W. Іншими словами, у цьому випадку многочлен f не може бути ваговим многочленом самодуального коду. Проте, коли степінь многочлена є досить високим, то цей алгоритм непридатний для використання навіть для сучасних систем комп'ютерної алгебри.

Тому застосуємо інший підхід для розв'язання цієї задачі. Нехай $f, g \in \mathsf{Z}[x,y]$ і розглянемо підкільце

$\mathsf{Z}[f,g]$, породжене многочленами f,g. Визначемо диференціювання

$$D_{f,g}:\mathsf{Z}[x,y]\to\mathsf{Z}[x,y],$$

наступним чином:

$$D_{f,g}=\frac{1}{J(f,g)}((g_{y'}-f_{y'})\partial_x+(f_{x'}-g_{x'})\partial_y),$$

тут $J(f,g)=f'_xg'_y-f'_yg'_x$ -- якобіан многочленів f і g.

Нагадаємо, що диференціюванням кільця називається всяке лінійне відображення, яке задовольняє правило Лейбніца.

Має місце наступна теорема.

Теорема 1. (і) Ядро $Z[x,y]^{D_{f,g}}$ диференціювання $D_{f,g}$ рівне $Z[f-g]$;

(ii) диференціювання $D_{f,g}$ є локально нільпотентним диференціюванням на кільці $Z[f,g]$.

Доведення. (і) Нагадаємо, що ядром довільного диференціювання називається множина многочленів які перетворюються в 0 при дії цього диференціювання. Для випадку кільця многочленів від двох зміних, добре відомо [4], що ядро диференціювання або тривіальне, або породжене одним многочленом. Знайдемо дію $D_{f,g}$ на породжуючі многочлени f,g:

$$D_{f,g}(f)=\frac{1}{J(f,g)}((g_{y'}-f_{y'})f'_x+(f_{x'}-g_{x'})f'_y)=\frac{1}{J(f,g)}(f'_xg_{y'}-f'_yg_{x'})=1.$$

Аналогічно знаходимо

$$D_{f,g}(g)=\frac{1}{J(f,g)}((g_{y'}-f_{y'})g'_x+(f_{x'}-g_{x'})g'_y)=\frac{1}{J(f,g)}(f'_xg_{y'}-f'_yg_{x'})=1.$$

В силу лінійності диференціювання $D_{f,g}$ отримаємо

$$D_{f,g}(f-g)=D_{f,g}(f)-D_{f,g}(g)=0.$$

Отже, многочлен $f-g$ лежить в ядрі диференціювання $D_{f,g}$. Оскільки, ядро диференціювання кільця від двох змінних не може породжуватися більше ніж одним многочленом, то звідси і випливає перше твердження теореми.

(ii) Диференціювання D називається локально нільпотентним на кільці $\mathsf{Z}[f,g]$, якщо для довільного многочлена F, існує таке ціле число $n(F)$, для якого виконується співвідношення $D^{n(F)}(F)=0$. Оскільки $D_{f,g}(f)=D_{f,g}(g)=1$, то обмеження диференціювання $D_{f,g}$ на кільце $\mathsf{Z}[f,g]$ має вигляд $\partial_f+\partial_g$. Але, кожне з диференціювань ∂_f, ∂_g є, очевидно, локально нільпотентним на $\mathsf{Z}[f,g]$, тому локально нільпотетною буде і їхня сума.

Теорема доведена.

Тепер ми можемо встановити ефективний критерій належності довільного многочлена з $\mathsf{Z}[x,y]$ до кільця $\mathsf{Z}[f,g]$:

Теорема 2. Многочлен $F\in\mathsf{Z}[x,y]$ належить кільцю $\mathsf{Z}[f,g]$, тоді і лише тоді коли існує ціле число $n(F)$ для якого виконується $D^{n(F)}_{f,g}(F)=0$.

Доведення. Якщо належить кільцю $\mathsf{Z}[f,g]$, то його можна записати як деякий многочлен від f,g. Оскільки обмеження диференціювання $D_{f,g}$ на $\mathsf{Z}[f,g]$ є локально нільпотентним, то звідси і випливає, що існує такие ціле $n(F)$ для якого має місце рівність $D^{n(F)}_{f,g}(F)=0$. Якщо ж для многочлена F існує таке $n(F)$, що $D^{n(F)}_{f,g}(F)=0$, то звідси випливає нільпотентність диференціювань диференціювань ∂_f, ∂_g, що є рівносильнив, див.[4], належності F до $\mathsf{Z}[f,g]$.

Теорема доведена.

Зауважимо - якщо многочлен F належить кільцю $\mathsf{Z}[f,g]$, то, очевидно, що тоді і

$D^k_{f,g}(F) \in \mathbb{Z}[f,g]$ для всіх додатніх $k \in \mathbb{Z}$.

3. Отже, тепер ми маємо можливість перевіряти, чи даний многочлен може бути ваговою функцією самодуального бінарного коду. В кільці $\mathbb{Z}[x,y]$, розглянемо підкільце $\mathbb{Z}[W_1,W_2]$, і відповідне диференціювання $D := D_{W_1,W_2}$:

$$D := \frac{1}{J(W_1,W_2)}((1518x^{15}y^8 + 3864x^{11}y^{12} + 759x^7y^{16} - 7x^3y^4 + 3x^{23} - x^7)\partial_y +$$

$$+ (y^7 - 759x^{16}y^7 - 3864x^{12}y^{11} - 1518x^8y^{15} + 7x^4y^3 - 3y^{23})\partial_x),$$

Тут

$$J(W_1,W_2) = 1344x^{27}y^3 + 92736x^{19}y^{11} - 92736x^{11}y^{19} - 48384y^7x^{23} + 48384y^{23}x^7 - 1344x^3y^{27},$$

- якобіан многочленів W_1 і W_2.

Проілюструємо вищесказане і з'ясуємо, чи многочлен $F = 14x^4y^4(x^4 - y^4)^4$ може бути ваговим многочленом самодуального бінарного коду. Прямими обчисленнями отримуємо

$$D(F) = x^{16} + 28x^{12}y^4 + 198x^8y^8 + 28x^4y^{12} + y^{16} - \frac{1}{3},$$
$$D^2(F) = 2x^8 + 28x^4y^4 + 2y^8,$$
$$D^3(F) = 2,$$
$$D^4(F) = 0.$$

Неважко показати, що

$$F = \frac{W_1^2 - W_2}{588}.$$

Отже, F лежить в $\mathbb{Z}[W_1,W_2]$, тобто може бути ваговою функцією самодуального бінарного коду. Питання, чи існує код з такою ваговою функцією потребує окремого дослідження і вимагає методів, які виходять за межі даної роботи.

Розглянемо тепер многочлен $F = (x^4 - y^4)^8$. Прямими обчисленнями знаходимо

$$D(F) = -\frac{4(3x^{16} + 756x^{12}y^4 + 4626x^8y^8 + 756x^4y^{12} - 8 + 3y^{16})(x^4 - y^4)^4}{21(x^8 - 34x^4y^4 + y^8)}$$

Якби многочлен F належав до кільця $\mathbb{Z}[W_1,W_2]$, то і $D(F)$ мав би належати до $\mathbb{Z}[W_1,W_2]$. Але, очевидно, що $D(F)$ навіть не належить до $\mathbb{Z}[x,y]$, Звідси робимо висновок, що і F не належить до $\mathbb{Z}[W_1,W_2]$. Отже, F не може бути ваговою функцією самодуального коду.

4. Порівняємо ефективність роботи запропонованого алгоритму із стандартним алгоритмом який використовує теорію базисів Грьобнера. В наступній таблиці подано машиний час який небхідний для перевірки того, що многочлен F не може бути ваговою функцією самодуального коду. Перевірка здійснювалася стандартним алгоритмом (Алгоритм 1) і алгоритмом запропонованим у даній роботі (Алгоритм 2) в системі символьних обчислень Maple.

Многочлен	Алгоритм 1	Алгоритм 2
$F = x^4y^4(x^4 - y^4)^{10}$	0.625c	0.001c
$F = x^4y^4(x^4 - y^4)^{12}$	0.906c	0.001c
$F = x^4y^4(x^4 - y^4)^{14}$	3.391c	0.016c
$F = x^4y^4(x^4 - y^4)^{16}$	2.999c	0.062c
$F = x^4y^4(x^4 - y^4)^{18}$	5.704c	0.076c

Отже, запопонований алгоритм є більш ефективним, ніж стандартний алгоритм.

Список використаних джерел

1. Мак-Вильямс Ф. Дж., Слоэн Н. Д. А. Теория кодов исправляющих ошибки. – М.: Связь, 1979. –

572 с.

2. Gleason A. Weight polynomials of self-dual codes and the MacWilliams identities // Actes Congr. internat. Math. 1970, 3. – P. 211 – 215.

3. Аржанцев И. В. Базисы Грёбнера и системы алгебраических уравнений. – М.: МЦНМО, 2003. – 65 с.

4. Nowicki A. Polynomial derivation and their Ring of Constants. Torun, UMK, 1994. – 170 p.