1 Разложение функций

Рассмотрим функции

$$h = hx^{k-1} + tx^{k-2} + \cdots + tx + t$$
$$t = tx^{k-1} + ehx^{k-2} + \cdots + ehx + eh, \text{ где}$$

e – некоторый коэффициент.

Через C_{hi}^{hd} обозначим коэффициент у функции h при x^i, при функции h, поляризация d.

Через C_{ti}^{hd} обозначим коэффициент у функции h при x^i, при функции t, поляризация d.

Через C_{hi}^{td} обозначим коэффициент у функции t при x^i, при функции h, поляризация d.

Через C_{ti}^{td} обозначим коэффициент у функции t при x^i, при функции t, поляризация d.

$$C_{hi}^{hd} = \binom{k-1}{i}(-d)^{k-1-i}$$

$$C_{ti}^{hd} = \sum_{j=i}^{k-2}\binom{j}{i}(-d)^{j-i}$$

$$C_{hi}^{td} = \sum_{j=i}^{k-2} e\binom{j}{i}(-d)^{j-i}$$

$$C_{ti}^{td} = \binom{k-1}{i}(-d)^{k-1-i}$$

Заметим, что $\binom{k-1}{i} \neq 0 \pmod{k}$, тогда у функции h при любой поляризации присутствует слагаемое с h, а у функции t при любой поляризации присутствует слагаемое с t.

Пусть $f_a = h + at$, где $a \in [1..k-1]$.

Теорема 1. *Для любых d и a у полинома функции $f_a^{(d)}$ k слагаемых, если e – квадратичный невычет по модулю k.*

Доказательство. Пусть существуют a, d, i такие, что $f_a^{(d)}[i] = 0$, тогда C_{hi}^{hd} должно быть равно $-aC_{hi}^{td}$, а C_{ti}^{hd} должно быть равно $-aC_{ti}^{td}$.

$$\begin{cases} \binom{k-1}{i}(-d)^{k-1-i} &= -a\sum\limits_{j=i}^{k-2} e\binom{j}{i}(-d)^{j-i} \\ \sum\limits_{j=i}^{k-2}\binom{j}{i}(-d)^{j-i} &= -a\binom{k-1}{i}(-d)^{k-1-i} \end{cases}$$

$\sum_{j=i}^{k-2} \binom{j}{i}(-d)^{j-i} \neq 0$ так как $\binom{k-1}{i}(-d)^{k-1-i} \neq 0$. Следовательно

$$a^{-1}\sum_{j=i}^{k-2}\binom{j}{i}(-d)^{j-i} = a\sum_{j=i}^{k-2} e\binom{j}{i}(-d)^{j-i}$$

Значит $e = (a^{-1})^2$, что противоречит с тем, что e – квадратичный невычет по модулю k. □

2 Функции одной переменной

Рассмотрим теперь следующие функции h и t одной переменной:

$$h = ex^{k-1} + (x-1)^{k-1}$$
$$t = x^{k-1} + e(x-1)^{k-1}$$

Они выглядят так:

$$h = (e+1)x^{k-1} + x^{k-2} + \cdots + x + 1$$
$$t = (e+1)x^{k-1} + ex^{k-2} + \cdots + ex + e$$

Через C_i^{hd} обозначим коэффициент при x^i у функции h при поляризации d.

Через C_i^{td} обозначим коэффициент при x^i у функции t при поляризации d.

$$C_i^{hd} = \tbinom{k-1}{i}(-d)^{k-1-i} + \sum_{j=i}^{k-2} e\tbinom{j}{i}(-d)^{j-i}$$
$$C_i^{hd} = e\tbinom{k-1}{i}(-d)^{k-1-i} + \sum_{j=i}^{k-2} \tbinom{j}{i}(-d)^{j-i}$$

Теорема 2. *Для любой поляризации d, для любого i у любой пары f и g функций из $\{h, t, h+at\}$ $(\forall a \in [1..k-1])$ коэффициенты при x^i не могут быть равны 0 одновременно.*

Доказательство. 1) Рассмотрим случай, когда f и $g \in \{h, t\}$. Предположим, что $C_i^{hd} = 0$ и $C_i^{td} = 0$. Тогда, так как $\binom{k-1}{i}(-d)^{k-1-i} \neq 0$, то и $\sum_{j=i}^{k-2} \binom{j}{i}(-d)^{j-i} \neq 0$. А также

$$e\sum_{j=i}^{k-2}\binom{j}{i}(-d)^{j-i} = e^{-1}\sum_{j=i}^{k-2}\binom{j}{i}(-d)^{j-i}$$

Следовательно $e^2 = 1$, но $e \in [2..k-2]$ чего не может быть так как у 1 только два корня 1 и -1.

2) Пусть $f = h + at$, а $g \in \{h, t\}$.

$$C_i^{fd} = C_i^{hd} + aC_i^{td}.$$

Если $C_i^{gd} = 0$, то в C_i^{fd} всего 1 слагаемое и, в силу предыдущего пункта, оно отлично от 0.

3) Последний случай: $f = h + at$, $g = h + bt$.

$$C_i^{fd} = C_i^{hd} + aC_i^{td},$$
$$C_i^{gd} = C_i^{hd} + bC_i^{td}.$$

Если $C_i^{td} \neq 0$, то $C_i^{fd} \neq C_i^{gd}$, а если $C_i^{td} = 0$, то из первого пункиа следует, что $C_i^{hd} \neq 0$.

□