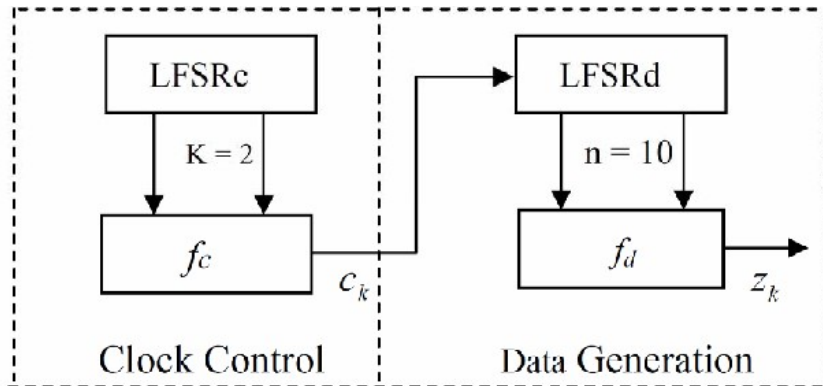
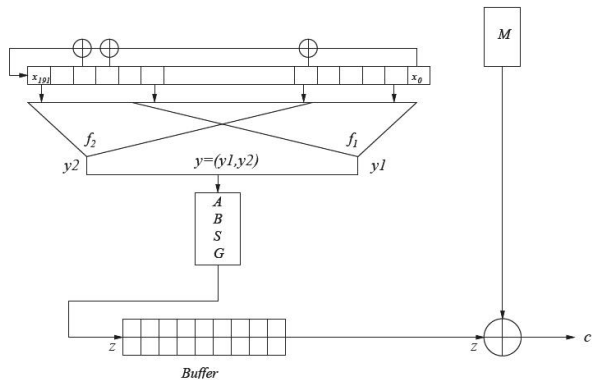


Оценки веса монотонных буюнктивных функций в связи с методом буюнктивных имплицент решения систем булевых уравнений

Работу выполнили: Тарасов А.В., Трубицин Н.М.

Москва 2025



Структура поточных шифров Decim и LILI-128.

Рассмотрим систему $\mathcal{S}$ булевых уравнений вида:

$$\{f_i(\bar{x}) = \gamma_i, \quad i \in \overline{1, t}. \quad (1)$$

Обозначим её множество решений через $Sol(\mathcal{S})$.

Основная идея метода имплицент состоит в построении по системе (1) системы $\mathcal{S}'$ булевых уравнений

$$\{g_j(\bar{x}) = 0, \quad j \in \overline{1, l}$$

такой, что $Sol(\mathcal{S}) \subset Sol(\mathcal{S}')$ и система $\mathcal{S}'$ решается эффективнее, чем система $\mathcal{S}$, например, лежит в одном из полиномиально решаемых классов.

В анализе шифров поточных
Криптограф знает, что всегда
С их нелинейной частью точно
Возникнет где-нибудь беда.
С проблемой нелинейных бедствий
Поможет новый инструмент:
Систему биюнктивных следствий
Построит метод имплицент.
Но чтобы метод перспективный
Принёс в анализе успех,
Нам нужен способ эффективный,
Который быстро без помех

Если система булевых уравнений порождается фильтрующим или комбинирующим генератором, то она имеет итеративный вид:

$$\{f(\bar{x}A^{i-1}) = \gamma_i, \quad i \in \overline{1, t}, \quad (2)$$

где $f(x_1, \dots, x_n)$ — булева функция от n переменных, $A \in GL(n, 2)$, $\gamma_i \in \{0, 1\}$, $i \in \overline{1, t}$.

При достаточно больших t система (2) имеет, как правило, единственное решение $\bar{x} = (c_1, \dots, c_n)$, а значит, её следствием является функция $x_1^{c_1} \dots x_n^{c_n}$, которая является буюнктивной, слабо положительной и слабо отрицательной.

Для разных буюнктивных функций

Оценки веса приведёт

Иль для системы из дизъюнкций

Число решений всех найдёт.

И в этой непростой задаче

Помогут графы без труда,

А также числа Фибоначчи

Нас выручат почти всегда.

И ряд таких оценок точных

Мы приведём в один момент,

Чтоб виды всех шифров поточных

Вскрывал наш метод имплицит! 🔍🔗

- 1) F_n — n -е число Фибоначчи, $n \in \mathbb{N}_0$;
 - 2) Bi'_n — множество монотонных биективных функций от n переменных, существенно зависящих от всех своих переменных и не имеющих аффинных имплицентов;
 - 3) $m_d(f)$ — минимальный импликативный ранг функции f ;
 - 4) $[f(x_1, \dots, x_n)]_{\langle S_n \rangle}$ — класс эквивалентности булевых функций с представителем f относительно симметрической группы S_n перестановок координат векторов из V_n ;
 - 5) $v(G)$ — число вершинных покрытий неориентированного графа G .
- Для функции $f \in Bi'_n$, минимальная и сокращённая 2-КНФ которой имеет вид:

$$f(x_1, \dots, x_n) = \bigwedge_{i=1}^t (x_{s_{i,1}} \vee x_{s_{i,2}}),$$

построим неориентированный граф $H = (VH, EH)$, где

$$VH = \{x_1, \dots, x_n\}, \quad EH = \{e_1 = (x_{s_{1,1}}, x_{s_{1,2}}), \dots, e_t = (x_{s_{t,1}}, x_{s_{t,2}})\}.$$

Теорема

Для буюнктивной функции $f(x_1, \dots, x_n)$, существенно зависящей от $n \geq 2$ переменных и не имеющей аффинных имплицент, существует функция $g(x_1, \dots, x_n) \in Bi'_n$ со свойствами $||f|| = ||g||$ и $m_d(f) \geq m_d(g)$.

Теорема

Для буюнктивной функции $f(x_1, \dots, x_n)$, существенно зависящей от $n \geq 2$ переменных и не имеющей аффинных имплицент, справедливо неравенство: $||f|| \geq 2^{n-m_d(f)} + m_d(f)$. При этом для любого возможного значения $m_d(f)$ оценка достижима на монотонной буюнктивной функции.

Теорема

При $n \geq 2$ для функции $f(x_1, \dots, x_n) \in M$ справедливо неравенство: $\|f\| \geq 2^{n-m} + m$, где $m = m_d(f) = \min_{\alpha \in E_f} \|\alpha\|$. При этом для любого возможного значения m оценка достижима на монотонной буюнктивной функции.

Следствие

Если m — мощность минимального вершинного покрытия простого неориентированного графа на n вершинах без изолированных вершин, то количество вершинных покрытий этого графа не меньше, чем $2^{n-m} + m$. При этом оценка достижима для любого возможного значения m .

Определение

Неориентированный граф $H = (V, E)$ без изолированных вершин состоит из попарно не пересекающихся графов $H_i = (V_i, E_i)$, $i \in \overline{1, t}$, множества вершин V' и множества рёбер E' , если в множестве V' нет смежных вершин и в наборах $V_1, \dots, V_t, V'$ и $E_1, \dots, E_t, E'$ множества попарно не пересекаются.

Теорема

Если граф H функции $f \in Bi'_n$ состоит из попарно не пересекающихся:

- | | |
|---|----------------------|
| 1) k простых цепей длин $t_1, \dots, t_k \geq 1$; | 3) m вершин; |
| 2) r простых циклов длин $l_1, \dots, l_r \geq 3$; | 4) $s \geq m$ рёбер, |

то для веса функции f справедливы следующие неравенства:

$$\left(\frac{3}{4}\right)^s \cdot 2^m \cdot \prod_{i=1}^k F_{t_i+3} \cdot \prod_{j=1}^r (F_{l_{j+1}} + F_{l_{j-1}}) \leq \|f\| \leq 2^m \cdot \prod_{i=1}^k F_{t_i+3} \cdot \prod_{j=1}^r (F_{l_{j+1}} + F_{l_{j-1}}).$$

При этом обе оценки достижимы тогда и только тогда, когда каждая переменная входит в 2-КНФ функции $f(x_1, \dots, x_n)$ не более двух раз.

Следствие

Число вершинных покрытий дерева G на n вершинах с диаметром d удовлетворяет неравенствам:

$$\left(\frac{3}{2}\right)^{n-d-1} \cdot F_{d+3} \leq v(G) \leq 2^{n-d-1} \cdot F_{d+3}.$$

Следствие

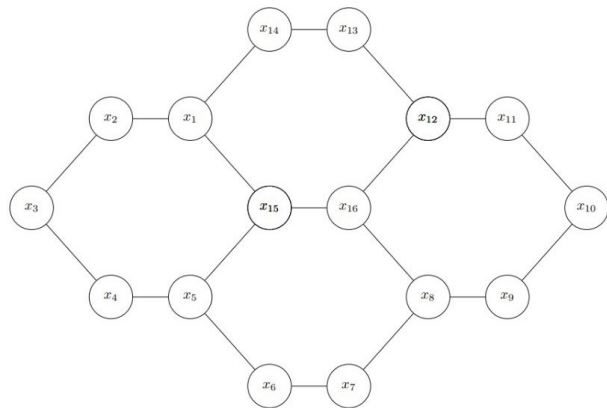
Число вершинных покрытий гамильтонового (n, m) -графа G удовлетворяет неравенствам:

$$\left(\frac{3}{4}\right)^{m-n} \cdot (F_{n+1} + F_{n-1}) \leq v(G) \leq F_{n+1} + F_{n-1}.$$

$$f(x_1, \dots, x_{16}) = (x_1 \vee x_{14})(x_1 \vee x_{15})(x_5 \vee x_{15})(x_{12} \vee x_{16})(x_8 \vee x_{16})(x_{15} \vee x_{16}) \wedge \bigwedge_{i=1}^{13} (x_i \vee x_{i+1})$$

Можно выделить следующие разбиения графа функции f :

- 1) 2 цикла длины 6: $(x_1, x_2, x_3, x_4, x_5, x_{15})$ и $(x_8, x_9, x_{10}, x_{11}, x_{12}, x_{16})$; 2 цепи длины 1: (x_{13}, x_{14}) и (x_6, x_7) ; 5 рёбер: (x_1, x_{14}) , (x_5, x_6) , (x_7, x_8) , (x_{12}, x_{13}) и (x_{15}, x_{16}) ;
- 2) цикл длины 14: $(x_1, x_2, \dots, x_{14})$; цепь длины 1: (x_{15}, x_{16}) ;
- 4 ребра: (x_1, x_{15}) , (x_5, x_{15}) , (x_8, x_{16}) и (x_{12}, x_{16}) ;
- 3) цепь длины 15: $(x_{16}, x_{15}, x_1, x_2, \dots, x_{14})$; 4 ребра: (x_1, x_{14}) , (x_8, x_{16}) , (x_{12}, x_{16}) и (x_5, x_{15}) ;
- 4) цикл длины 6: $(x_1, x_{14}, x_{13}, x_{12}, x_{16}, x_{15})$; цепь длины 9: $(x_2, x_3, \dots, x_{11})$; 4 ребра: (x_1, x_2) , (x_5, x_{15}) , (x_8, x_{16}) и (x_{11}, x_{12}) .



Соответствующие этим разбиениям графа оценки веса имеют вид:

$$1) \left(\frac{3}{4}\right)^5 \cdot 3^2 \cdot 18^2 = \left(\frac{3}{4}\right)^5 \cdot 3^2 \cdot (F_7 + F_5)^2 < \|f\| < 3^2 \cdot (F_7 + F_5)^2 = 3^2 \cdot 18^2 \Leftrightarrow 692 \leq \|f\| \leq 2915;$$

$$2) \left(\frac{3}{4}\right)^4 \cdot 3 \cdot 843 = \left(\frac{3}{4}\right)^4 \cdot 3 \cdot (F_{15} + F_{13}) < \|f\| < 3 \cdot (F_{15} + F_{13}) = 3 \cdot 843 \Leftrightarrow 801 \leq \|f\| \leq 2528;$$

$$3) \left(\frac{3}{4}\right)^4 \cdot 2584 = \left(\frac{3}{4}\right)^4 \cdot F_{18} < \|f\| < F_{18} = 2584 \Leftrightarrow 818 \leq \|f\| \leq 2583;$$

$$4) \left(\frac{3}{4}\right)^4 \cdot 18 \cdot 144 = \left(\frac{3}{4}\right)^4 \cdot (F_7 + F_5) \cdot F_{12} < \|f\| < (F_7 + F_5) \cdot F_{12} = 18 \cdot 144 \Leftrightarrow 821 \leq \|f\| \leq 2591.$$

Таким образом, $821 \leq \|f\| \leq 2528$. При этом настоящий вес функции находится примерно в центре полученного интервала. Кроме того, нижняя оценка составляет около половины реального значения, а верхняя превосходит его менее, чем в 1,5 раза.

Утверждение

Если $k \leq n$, функции $h(x_1, \dots, x_k)$ и $f(x_1, \dots, x_n)$ существенно зависят от всех своих переменных, и h — имплицента функции f , то справедливо неравенство $\|f\| \leq \|h\| \cdot 2^{n-k}$.

Лемма

Для любых $n, r, s_1, \dots, s_r \in \mathbb{N}$ таких, что $s_1 + \dots + s_r = n - r$, справедливо неравенство

$$(2^{s_1} + 1) \cdot \dots \cdot (2^{s_r} + 1) \leq 3^{r-1} \cdot (2^{n-2r+1} + 1),$$

обращающееся в равенство тогда и только тогда, когда среди натуральных чисел $s_1, \dots, s_r$ одно равно $n - 2r + 1$, а все остальные равны единице.

Лемма

При $n \geq 3$ и $r \in \overline{1, \lfloor \frac{n-1}{2} \rfloor}$ функция $h(r) = 3^{r-1} \cdot (2^{n-2r+1} + 1)$ монотонно убывает по переменной r .

Лемма

Для чисел Фибоначчи справедливо следующее неравенство:

$$F_{l_1+2} \cdot \dots \cdot F_{l_t+2} > F_n \quad \forall n, t, l_1, \dots, l_t \in \mathbb{N}, t \geq 2 : l_1 + \dots + l_t = n - 2.$$

Лемма

Для любых $n, r, s_1, \dots, s_r \in \mathbb{N}$ таких, что $s_1 + \dots + s_r = n - r$, справедливо неравенство

$$F_{s_1+2} \cdot \dots \cdot F_{s_r+2} \geq F_{q+3}^l \cdot F_{q+2}^{r-l},$$

где l — остаток от деления n на r , а $q = \lfloor \frac{n}{r} \rfloor$ — неполное частное.

Определение

Звездой степени n называется дерево на n вершинах с $n - 1$ листьями при $n \geq 3$ и единственное дерево на двух вершинах при $n = 2$.

Определение

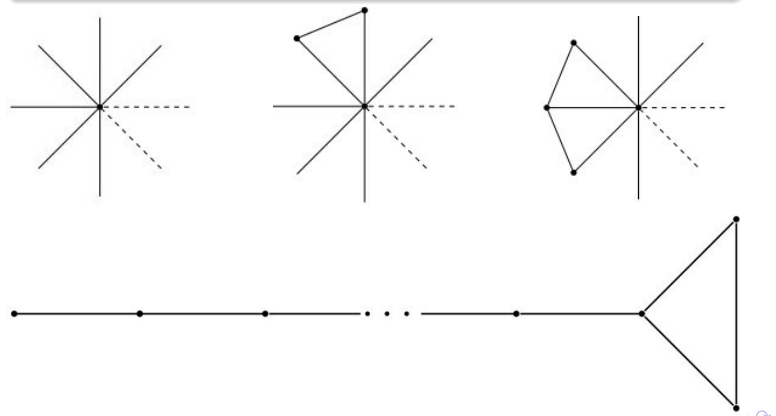
Пауком степени $n \geq 3$ называется простой связный (n, n) -граф, имеющий цикл длины 3, $n - 3$ листа и вершину степени $n - 1$.

Определение

Большим пауком степени $n \geq 4$ называется простой связный $(n, n+1)$ -граф, имеющий три простых цикла длин 3, 3 и 4, $n - 4$ листа и вершину степени $n - 1$.

Определение

Воздушным змеем степени $n \geq 4$ называется простой связный (n, n) -граф с циклом длины 3 и единственным листом.



Теорема

При $n \geq 2$ для неразложимой функции $f \in Bi'_n$ с длиной 2-КНФ $n - 1$ верно неравенство $\|f\| \geq F_{n+2}$, обращаясь в равенство только на функциях из класса

$$[(x_1 \vee x_2)(x_2 \vee x_3) \dots (x_{n-1} \vee x_n)]_{\langle S_n \rangle}.$$

Следствие

Для дерева G на $n \geq 2$ вершинах верно неравенство: $v(G) \geq F_{n+2}$. При этом оценка достигается только на простой цепи длины $n - 1$.

Теорема

При $n \geq 4$ для функции $f \in Bi'_n$ с длиной 2-КНФ $n + 1$ верно неравенство $\|f\| \leq 5 \cdot 2^{n-4} + 1$. При этом оно достигается только на функциях из классов

$$\left[\bigwedge_{i=1}^{n-1} (x_1 \vee x_{i+1}) \wedge (x_{n-2} \vee x_{n-1}) \wedge (x_{n-1} \vee x_n) \right]_{\langle S_n \rangle}, \quad n \geq 4,$$

$$[(x_1 \vee x_2)(x_1 \vee x_3)(x_1 \vee x_4)(x_2 \vee x_5)(x_3 \vee x_5)(x_4 \vee x_5)]_{\langle S_5 \rangle}.$$

Следствие

При $n \geq 4$ для простого $(n, n + 1)$ -графа G без изолированных вершин верно неравенство: $v(G) \leq 5 \cdot 2^{n-4} + 1$. При этом для $n = 4$ и $n \geq 6$ оценка достигается только на большом пауке степени n .

Теорема

При $n \geq 3$ для функции $f \in Bi'_n$ с длиной 2-КНФ n , верно неравенство $\|f\| \leq 3 \cdot 2^{n-3} + 1$. Если при этом f — неразложимая функция, то также верно неравенство $\|f\| \geq F_{n+1} + F_{n-1}$. При этом для $n \geq 5$ нижняя оценка достигается только на функциях из классов

$$\begin{aligned} &[(x_1 \vee x_2)(x_2 \vee x_3) \dots (x_{n-1} \vee x_n)(x_n \vee x_1)]_{\langle S_n \rangle}, \\ &[(x_1 \vee x_2)(x_2 \vee x_3) \dots (x_{n-1} \vee x_n)(x_1 \vee x_3)]_{\langle S_n \rangle}, \end{aligned}$$

а верхняя оценка — только на функциях из класса

$$\left[\bigwedge_{i=1}^{n-1} (x_1 \vee x_{i+1}) \wedge (x_2 \vee x_n) \right]_{\langle S_n \rangle}.$$

При $n \in \{3, 4\}$ верхняя и нижняя оценки совпадают и достигаются на всех неразложимых функциях из класса Bi'_n с длиной 2-КНФ n .

Следствие

При $n \geq 3$ для простого $(n, n+1)$ -графа G без изолированных вершин верно неравенство $v(G) \leq 3 \cdot 2^{n-3} + 1$. Если G — связный граф, то также верно неравенство $v(G) \geq F_{n+1} + F_{n-1}$. При этом для $n \geq 5$ нижняя оценка достигается только на простом цикле длины n и воздушном змее степени n , а верхняя оценка — только на пауке степени n . При $n \in \{3, 4\}$ верхняя и нижняя оценки совпадают и достигаются на всех простых связных (n, n) -графах без изолированных вершин.

Теорема

При $n \geq 3$ для функции $f \in Bi'_n$ с длиной 2-КНФ $\lceil \frac{n}{2} \rceil \leq m \leq n - 1$ справедливо неравенство: $\|f\| \leq 3^{n-m-1} \cdot (2^{2m-n+1} + 1)$, обращающееся в равенство для любых допустимых значений m и n только на функциях из класса

$$\left[\bigwedge_{i=1}^{n-m-1} (x_i \vee x_{i+n-m-1}) \wedge \bigwedge_{j=2n-2m}^n (x_{2n-2m-1} \vee x_j) \right]_{\langle S_n \rangle}.$$

Если при этом граф функции f является лесом с r нетривиальными компонентами связности, то для неё верно неравенство $\|f\| \geq F_{q+3}^l \cdot F_{q+2}^{r-l}$, где l — остаток от деления n на r , а $q = \lfloor \frac{n}{r} \rfloor$ — неполное частное. Оно обращается в равенство для любых допустимых значений m и n на функциях, эквивалентных относительно группы S_n функции

$$\bigwedge_{i=1}^l ((x_i \vee x_{i+l}) \dots (x_{i+(q-1)l} \vee x_{i+ql})) \wedge \bigwedge_{j=1}^{r-l} ((x_{j+(q+1)l} \vee x_{ql+r+j}) \dots (x_{n-j+1-r+l} \vee x_{n-j+1})).$$

Следствие

При $n \geq 3$ и $\lceil \frac{n}{2} \rceil \leq m \leq n - 1$ простой (n, m) -граф G без тривиальных компонент связности удовлетворяет неравенству: $v(G) \leq 3^{n-m-1} \cdot (2^{2m-n+1} + 1)$. При этом оценка достижима только на лесе, состоящем из $n - m - 1$ звёзд степени 2 и одной звезды степени $2m - n + 2$ при любых допустимых значениях m и n .

Таким образом, при $n \geq 4$ вес функции $f \in Bi'_n$ с длиной 2-КНФ m не превосходит

$$T(n, m) = \begin{cases} 5 \cdot 2^{n-4} + 1, & \text{если } m = n + 1; \\ 3 \cdot 2^{n-3} + 1, & \text{если } m = n; \\ 3^{n-m-1} \cdot (2^{2m-n+1} + 1), & \text{если } \lceil \frac{n}{2} \rceil \leq m \leq n - 1. \end{cases}$$

При этом для любых значений m и n , кроме $(n, m) = (4, 4)$ и $(n, m) = (5, 6)$, указанная оценка достижима на единственном классе эквивалентности относительно группы S_n .

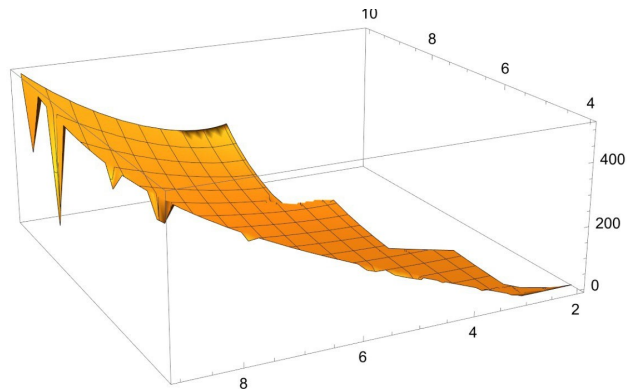
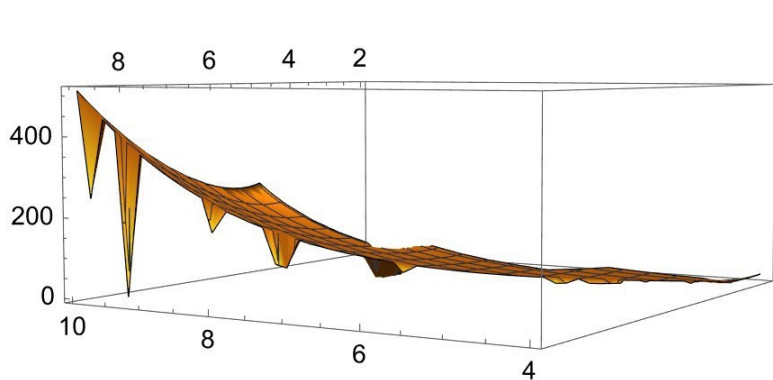


График функции $T(n, m)$ при $n \leq 10$ и $\lceil \frac{n}{2} \rceil \leq m \leq n + 1$.

Теорема

Справедливы следующие утверждения:

1) при $n \geq 2$ число неразложимых функций из класса Bi'_n с длиной 2-КНФ $n - 1$ и наименьшим весом F_{n+2} равно

$$\left| [(x_1 \vee x_2)(x_2 \vee x_3) \dots (x_{n-1} \vee x_n)]_{\langle S_n \rangle} \right| = \frac{n!}{2};$$

2) при $n \geq 4$ число неразложимых функций из класса Bi'_n с длиной 2-КНФ n и наименьшим весом $F_{n+1} + F_{n-1}$ равно $\frac{(n+1)(n-1)!}{2}$, причём

$$\left| [(x_1 \vee x_2) \dots (x_{n-1} \vee x_n)(x_n \vee x_1)]_{\langle S_n \rangle} \right| = \frac{(n-1)!}{2}, \quad \left| [(x_1 \vee x_2) \dots (x_{n-1} \vee x_n)(x_1 \vee x_3)]_{\langle S_n \rangle} \right| = \frac{n!}{2};$$

3) при $n \geq 6$ число функций из класса Bi'_n с длиной 2-КНФ $n + 1$ и наибольшим весом $5 \cdot 2^{n-4} + 1$ равно

$$\left| \left[\bigwedge_{i=1}^{n-1} (x_1 \vee x_{i+1}) \wedge (x_{n-2} \vee x_{n-1}) \wedge (x_{n-1} \vee x_n) \right]_{\langle S_n \rangle} \right| = \frac{n(n-1)(n-2)(n-3)}{2};$$

Теорема (продолжение)

4) при $n \geq 5$ число функций из класса Bi'_n с длиной 2-КНФ n и наибольшим весом $3 \cdot 2^{n-3} + 1$ равно

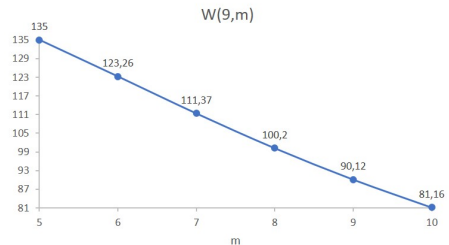
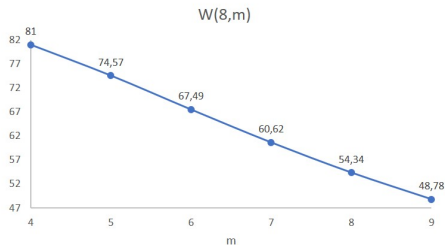
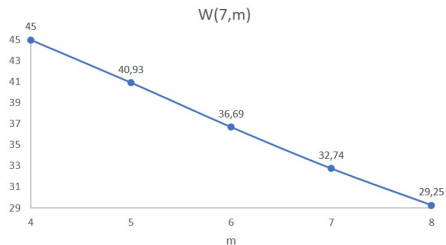
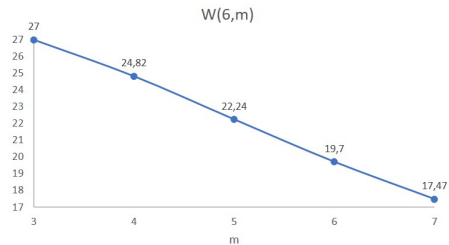
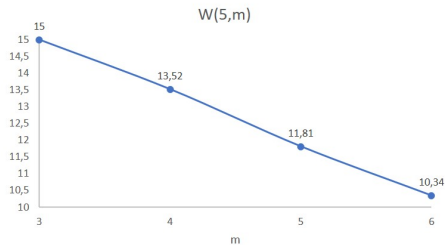
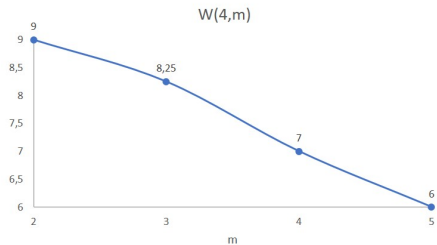
$$\left| \left[\bigwedge_{i=1}^{n-1} (x_1 \vee x_{i+1}) \wedge (x_2 \vee x_n) \right]_{\langle S_n \rangle} \right| = \frac{n(n-1)(n-2)}{2};$$

5) при чётном $n \geq 4$ число функций из класса Bi'_n с длиной 2-КНФ $\frac{n}{2}$ и наибольшим весом $3^{\frac{n}{2}}$ равно

$$\left| \left[\bigwedge_{i=1}^{n/2} (x_i \vee x_{i+\frac{n}{2}}) \right]_{\langle S_n \rangle} \right| = 2^{-\frac{n}{2}} \cdot A_n^{\frac{n}{2}};$$

6) при $n \geq 4$ и $\lceil \frac{n}{2} \rceil \leq m \leq n-1$, за исключением случая $m = \frac{n}{2}$ при чётных n , число функций из класса Bi'_n с длиной 2-КНФ m и наибольшим весом $3^{n-m-1} \cdot (2^{2m-n+1} + 1)$ равно

$$\left| \left[\bigwedge_{i=1}^{n-m-1} (x_i \vee x_{i+n-m-1}) \wedge \bigwedge_{j=2n-2m}^n (x_{2n-2m-1} \vee x_j) \right]_{\langle S_n \rangle} \right| = \frac{2^{m+1-n} \cdot A_n^{m+1}}{(2m-n+1)!}.$$



Теорема

Справедливы следующие утверждения:

- 1) при $n \geq 5$ наименьшее значение веса среди функций из класса Bi'_n с длиной 2-КНФ $n - 1$ достигается только на разложимых функциях;
- 2) при $n \geq 6$ наименьшее значение веса среди функций из класса Bi'_n с длиной 2-КНФ n достигается только на разложимых функциях.

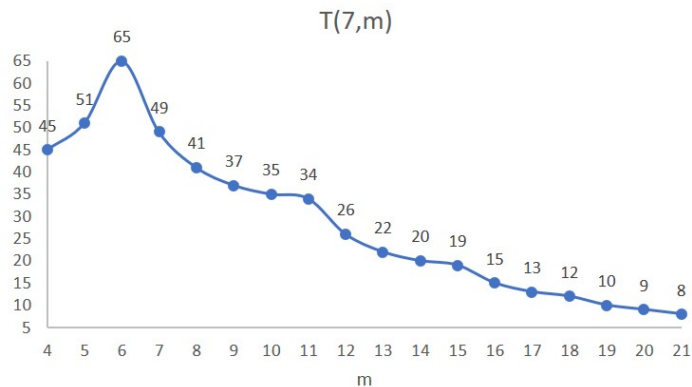
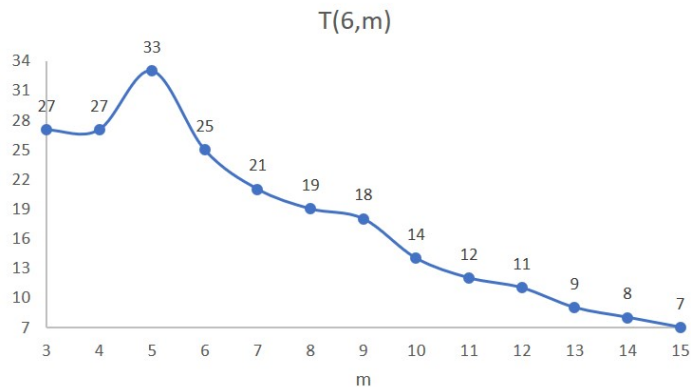
Следствие

Справедливы следующие утверждения:

- 1) при $n \geq 5$ наименьшим количеством вершинных покрытий среди простых $(n, n - 1)$ -графов обладают только несвязные графы;
- 2) при $n \geq 6$ наименьшим количеством вершинных покрытий среди простых (n, n) -графов обладают только несвязные графы.

Максимальные веса монотонных биективных функций, существенно зависящих от 6 и 7 переменных, при всех возможных значениях длины 2-КНФ

24/25



Графики функции $T(n, m)$ при $n \in \{6, 7\}$ и $\lceil \frac{n}{2} \rceil \leq m \leq C_n^2$.

Оценки веса монотонных буюнктивных функций в связи с методом буюнктивных имплицент решения систем булевых уравнений

Работу выполнили: Тарасов А.В., Трубицин Н.М.

Москва 2025