UNIVERSITAS COMENIANA
ACTA MATHEMATICA UNIVERSITATIS COMENIANAE
XLVIII—XLIX — 1986

ОЦЕНКИ СЛОЖНОСТИ ДИЗЪЮНКТИВНЫХ НОРМАЛЬНЫХ ФОРМ СЛУЧАЙНЫХ БУЛЕВЫХ ФУНКЦИЙ

МАРТИН ШКОВИЕРА, Братислава

1. Введение и основные понятия

В настоящей работе излагаются некоторые оценки сложности дизъюнктивных нормальных форм (ДНФ) и с тем связанных других параметров случайных булевых функций. В частности, дается асимптотика длины совершенной и наибольшей длины тупиковых ДНФ, и асимптотика логарифма длины сокращенной ДНФ и числа тупиковых ДНФ случайной булевой функции.*).

Под случайной булевой функцией n переменных понимается отображение $D^n \to D$, где $D = \{0, 1\}$, принимающее значения 1 и 0 с вероятностью p_n и $1 - p_n$, соответственно, независимо на различных точках множества D^n.

Известно, что всякая булева функция может быть представлена, как правило, несколькими различными ДНФ. Минимизация — это процесс построения для данной функции ДНФ минимальной сложности. Сложностью ДНФ обычно понимают или число слагаемых или общее число букв в ДНФ.

Известные алгоритмы минимизации выполняются на нескольких этапах. Сначала строят сокращенную ДНФ используя то или иное задание булевой функции. Чаще всего булеву функцию задают таблицей, или, что ровносильно, своей совершенной ДНФ. Удаляя излишние члены из сокращенной ДНФ различными способами, получают тупиковые ДНФ. Наконец, перебирая все тупиковые ДНФ, находят ДНФ минимальной сложности (в том или ином отношении).

В предлагаемой работе мы предпочитаем «геометрическую» трактов-

*) Полные доказательства будут опубликованы в другом месте.

ку задачи минимизации. Область определения булевой функции — множество D^n — понимается как множество вершин графа Q_n n-мерного единичного куба, в котором два набора $\alpha, \beta \in D^n$ соединены ребром тогда и только тогда, когда они различаются точно в одном разряде. Булева функция f отождествляется с подграфом индуцированным на множестве $Nf = \{\alpha \in D^n; f(\alpha) = 1\}$.

Существует взаимно однозначное соответствие между ДНФ функции f и покрытиями множества Nf гранями (= подкубами) куба D^n, содержащимися в Nf (такие подкубы называются интервалами функции f).

Таким образом, совершенная ДНФ соответствует покрытию множества Nf 0-мерными интервалами, сокращенная ДНФ — покрытию всеми максимальными интервалами (подкуб $K \subseteq Nf$ называется максимальным интервалом, если не существует такого подкуба L, что $K \subset L \subseteq Nf$) и тупиковые ДНФ отвечают таким покрытиям $\mathcal{U}$ максимальными интервалами, что для каждого $K \in \mathcal{U}$ множество $\mathcal{U} - \{K\}$ уже перестанет быть покрытием. Число $|\mathcal{U}|$ называется длиной покрытия $\mathcal{U}$ и ему соответствующей ДНФ.

Итак, изучение булевых функций тесно связано с изучением случайных индуцированных подграфов графа Q_n и всякий результат относительно случайных булевых функций можно перевести на язык такого рода случайных графов и обратно.

Вероятность p_n того, что вершина $\alpha \in D^n$ принадлежит множеству Nf считается зависящей от числа переменных функции f. Разумно предполагать, что получаемая таким образом последовательность $(p_n)_{n=1}^{\infty}$ сходится к некоторому p. Если $p = 0$ или $p = 1$, то необходимо налагать ограничения на скорость роста функций $\frac{1}{p_n}$ или $\frac{1}{1 - p_n}$, соответственно.

Перечислим важнейшие результаты работы.

С вероятностью стремящейся к 1 при $n \to \infty$ для случайной булевой функции верно следующее:

Если $\frac{1}{p_n} = o(n)$ и $\frac{1}{1 - p_n} = o(n)$, то

1. длина совершенной ДНФ асимптотически равна $p_n \cdot 2^n$;

2. двоичный логарифм от длины сокращенной ДНФ асимптотически равен $n + \log_2 n \cdot \log_2 \log_{1/p_n} n$.

Если $\frac{1}{p_n} = o\left(\frac{\sqrt{n}}{\log n}\right)$ и $\frac{1}{1 - p_n} = o(\log_2 \log_2 n)$, то

3. наибольшая длина тупиковой ДНФ асимптотически равна $p_n \cdot 2^n$;

4. двоичный логарифм от числа тупиковых ДНФ асимптотически равен $p_n \cdot 2^n \cdot \log_2 n \cdot \log_2 \log_{1/p_n} n$.

Основным средством для получения этих оценок являются неравенства Чебышева и в разд. 4 также метод условных вероятностей. Статья развивает идеи работ Глаголева [1] и Сапоженко [4], где, на самом деле, доказаны аналогичные результаты в традиционном случае $p_n = \frac{1}{2}$.

В заключении этого пункта приводим некоторые дальнейшие используемые нами обозначения.

Все предельные переходы и асимптотики считаются при $n \to \infty$, так что последний символ часто опускается. Последовательности, как правило, действительны и неотрицательны. Мы пользуемся o-символикой. Так $a_n = o(b_n)$ означает, что $\lim \frac{a_n}{b_n} = 0$; запись $a_n = O(b_n)$ значит, что последовательность $\frac{|a_n|}{|b_n|}$ ограничена. Говорят, что последовательности (a_n), (b_n) асимптотически равны, если $\lim \frac{a_n}{b_n} = 1$. В таком случае пишут $a_n \sim b_n$. Наконец, символ $\log x$ везде обозначает двоичный логарифм; в остальных случаях основание логарифма указано. Например, в символе $\log \log_a x$ внешний логарифм — двоичный, а внутренний имеет основание a.

Для более подробного ознакомления с понятиями касающимися булевых функций, их представления при помощи ДНФ, задачи минимизации и ее геометрической трактовки, рекомендуем читателю книги [2] и [3].

2. Вероятностные пространства

Случайные булевы функции образуют некоторое дискретное вероятностное пространство $(\boldsymbol{B}_n, \boldsymbol{P}_0)$, где $\boldsymbol{B}_n$ — множество всех булевых функций n переменных и $\boldsymbol{P}_0$ — вероятностная мера, которую мы определяем ниже. Вместе с ним в нашей работе используются и другие пространства на множествах (пар) булевых функций. Мы их строим из $(\boldsymbol{B}_n, \boldsymbol{P}_0)$ при помощи двух известных конструкций — произведения пространств и «подпространства» наделенного условной вероятностной мерой.

Чтобы определить $(\boldsymbol{B}_n, \boldsymbol{P}_0)$, представим себе случайный выбор функции $f \in \boldsymbol{B}_n$ как случайное разделение точек множества D^n до множеств Nf и $D^n - Nf$ по схеме Бернулли. Поскольку точку α до Nf выбираем с вероятностью p_n и до $D^n - Nf$ с вероятностью $1 - p_n$ независимо, то выбор функции f осуществляется с вероятностью $p_n^{|Nf|}(1 - p_n)^{2^n - |Nf|} = \boldsymbol{P}_0(\{f\})$. Для произвольного $A \subseteq \boldsymbol{B}_n$ имеем по определению $\boldsymbol{P}_0(A) = \sum_{f \in A} \boldsymbol{P}_0(\{f\})$.

Пользуясь теоремой о биноме нетрудно подсчитать, что верно следующее

Предложение 1. Пусть A, $B \subseteq D^n$ — два непересекающихся подмножества и $F = \{f \in B_n;\ A \subseteq Nf,\ B \subseteq D^n - Nf\}$. Тогда

$$\boldsymbol{P}_0(F) = p_n^{|A|}(1 - p_n)^{|B|}.$$

Если K — фиксированная k — мерная грань куба D^n, то отсюда вытекает, что $\boldsymbol{P}_0(K \subseteq Nf) = \boldsymbol{P}_0(\{f \in B_n;\ K \subseteq Nf\}) = p_n^{2^k}$.

Пространство $(B_n, \boldsymbol{P}_0)$ имеет существенное значение для наших рассуждений. Именно в нем мы интерсуемся отдельными свойствами булевых функций. Пусть S — некоторое свойство. Если $\lim \boldsymbol{P}_0(\{f \in B_n;$ f обладает свойством $S\}) = 1$, говорят, что случайная булева функция имеет свойство S, или что свойство S имеет место почти наверное. В случае, когда $p_n = \frac{1}{2}$, $n = 1, 2, \ldots$, обычно говорят, что почти все функции обладают свойством S.

Остальные вероятностные пространства используемые в нашей работе — второстепенного значения; они являются только техническим средством.

Пусть $B_n \times B_n$ — множество всех пар n-местных булевых функций. Возьмем на $B_n \times B_n$ вероятностную меру $\boldsymbol{P}_1 = \boldsymbol{P}_0 \times \boldsymbol{P}_0$ — произведение двух экземпляров меры $\boldsymbol{P}_0$. Таким образом для $f = (f_1, f_2) \in B_n \times B_n$ имеем $\boldsymbol{P}_1(\{f\}) = \boldsymbol{P}_0(\{f_1\}) \cdot \boldsymbol{P}_0(\{f_2\})$.

Через C_n обозначим подмножество множества $B_n \times B_n$ образованное такими парами (f_1, f_2), что $Nf_2 \subseteq Nf_1$. Мы будем рассматривать C_n как «подпространство» пространства $(B_n \times B_n, \boldsymbol{P}_1)$, т.е. множество C_n наделим мерой $\boldsymbol{P}_2 = \boldsymbol{P}_1(\cdot|C_n)$. Для произвольного $A \subseteq C_n$ тогда имеем

$$\boldsymbol{P}_2(A) = \frac{\boldsymbol{P}_1(A)}{\boldsymbol{P}_1(C_n)}.$$

Наконец, пусть C_n^a обозначает подмножество множества C_n состоящее из пар (f_1, f_2) таких, что $a \in Nf_1$; значит, $C_n^a = \{f \in B_n \times B_n;\ Nf_2 \subseteq Nf_1,\ a \in Nf_1\}$. Множество C_n^a наделим тоже условной вероятностной мерой $\boldsymbol{P}_3 = \boldsymbol{P}_1(\cdot|C_n^a)$. Если $A \subseteq C_n^a$, то $\boldsymbol{P}_3(A) = \dfrac{\boldsymbol{P}_1(A)}{\boldsymbol{P}_1(C_n^a)}$. Нетрудно видеть, что

$$\frac{\boldsymbol{P}_1(A)}{\boldsymbol{P}_1(C_n^a)} = \boldsymbol{P}_3(A) = \frac{\boldsymbol{P}_2(A)}{\boldsymbol{P}_2(C_n^a)}.$$

Используя опять только определения и простые приемы обращения с комбинаторными суммами (напр. теорему о биноме) находим следующие равенства.

Предложение 2.

$$\boldsymbol{P}_1(C_n) = (1 - p_n + p_n^2)^{2^n}$$

$$\boldsymbol{P}_1(C_n^\alpha) = p_n(1 - p_n + p_n^2)^{2^n - 1}$$

$$\boldsymbol{P}_2(C_n^\alpha) = \frac{p_n}{1 - p_n + p_n^2}.$$

Все изучаемые параметры булевых функций (или пар булевых функций) мы рассматриваем здесь как случайные величины на упомянутых выше пространствах.

Для получения асимптотических оценок этих параметров самым важным инструметом являются хорошо известные неравенства Чебышева. В их формулировке и в дальнейшем тексте используем букву $\boldsymbol{E}$ для математического ожидания и $\boldsymbol{D}$ для дисперсии случайных величин. Напомним, что $\boldsymbol{D}\xi = \boldsymbol{E}(\xi - \boldsymbol{E}\xi)^2 = \boldsymbol{E}(\xi^2) - (\boldsymbol{E}\xi)^2$ для любой случайной величины ξ.

Теорема А. [5] (1-ое неравенство Чебышева)
Если $\xi \geqslant 0$ — неотрицательная случайная величина и $\varepsilon > 0$ — любое положительное число, тогда

$$\boldsymbol{P}(\xi \geqslant \varepsilon) \leqslant \frac{\boldsymbol{E}\xi}{\varepsilon}.$$

Теорема Б. [5] (2-ое неравенство Чебышева)
Для любой случайной величины ξ и $\varepsilon > 0$ выполняется неравенство

$$\boldsymbol{P}(|\xi - \boldsymbol{E}\xi| \geqslant \varepsilon) \leqslant \frac{\boldsymbol{D}\xi}{\varepsilon^2}.$$

Кроме того мы пользуемся еще одним приемом, который позволяет нам то комбинировать свойства имеющие место почти наверное, то ограничиться в наших рассуждениях только существенной частью — с точки зрения рассматриваемого параметра — множества B_n и пренебречь оставшимися функциями. Мы его сформулируем в следующем просто доказываемом предложении.

Предложение 3. Пусть $(X_n, \mathscr{S}_n, \boldsymbol{Q}_n)_{n=1}^{\infty}$ — последовательность вероятностных пространств. Пусть дальше Y_n, $Z_n \in \mathscr{S}_n$ — такие события, что $\lim \boldsymbol{Q}_n(Y_n) = 1 = \lim \boldsymbol{Q}_n(Z_n)$ и $A_n \in \mathscr{S}_n$. Тогда

а) $\lim \boldsymbol{Q}_n(Y_n \cap Z_n) = 1$;

б) если $\lim \boldsymbol{Q}_n(A_n | Y_n) = 1$, то $\lim \boldsymbol{Q}_n(A_n) = 1$.

3. Длина совершенной и сокращенной ДНФ

Чтобы получить асимптотические оценки сложности совершенной, сокращенной и тупиковых ДНФ, начинаем с изучения структуры интервалов случайной булевой функции.

Пусть $i_{n,k}$ — случайная величина на B_n такая, что $i_{n,k}(f)$ равно числу k-мерных интервалов функции $f \in B_n$. Для каждой k-мерной грани K куба D^n введем случайную величину η_K (т. наз. индикатор) следующим способом:

$$\eta_K(f) = \begin{cases} 1, & \text{если } K \subseteq Nf \\ 0, & \text{в остальных случаях.} \end{cases}$$

Тогда $i_{n,k} = \sum_K \eta_K$; суммирование ведется по всем k-мерным граням $K \subseteq D^n$.

Так как число k-мерных граней n-мерного куба равно $\binom{n}{k} \cdot 2^{n-k}$ и

$$P_0(\eta_K = 1) = P_0(K \subseteq Nf) = p_n^{2^k}$$

в силу предложения 1, имеем

Предложение 4.

$$Ei_{n,k} = \binom{n}{k} \cdot 2^{n-k} \cdot p_n^{2^k}.$$

Используя равенство $Di_{n,k} = E(i_{n,k})^2 - (Ei_{n,k})^2$, выражение

$$(i_{n,k})^2 = \left(\sum_K \eta_K\right)^2 = \sum_{(K,L)} \eta_K \cdot \eta_L,$$

где суммирование ведется по всем упорядоченным парам k-мерных граней в D^n, и рассматривая возможные случаи относительно пресечения $K \cap L$ находим

Предложение 5.

$$Di_{n,k} \leqslant \binom{n}{k}^2 \cdot 2^{n-k} \cdot p_n^{2^k}.$$

Применим 2-ое неравенство Чебышева к случайной величине $i_{n,k}$ положив $\varepsilon = \varphi(n) \cdot \binom{n}{k} \cdot \sqrt{2_{n-k} \cdot p_n^{2^k}}$, причем $\dfrac{1}{\varphi(n)} = o(1)$. Поскольку

$$P_0(|i_{n,k} - Ei_{n,k}| \geqslant \varepsilon) \leqslant \frac{Di_{n,k}}{\varepsilon^2} \leqslant \frac{1}{\varphi(n)^2} \to 0,$$

мы получаем следующий результат.

Предложение 6. С вероятностью стремящейся к 1 при $n \to \infty$ для случайной булевой функции имеют место неравенства

$$\binom{n}{k}\left(2^{n-k}\cdot p_n^{2k} - \varphi(n)\sqrt{2^{n-k}\cdot p_n^{2k}}\right) < i_{n,k} < \binom{n}{k}\left(2^{n-k}\cdot p_n^{2k} + \varphi(n)\sqrt{2^{n-k}\cdot p_n^{2k}}\right).$$

Начиная с этого места мы будем предполагать, что p_n сходится и что

$$\frac{1}{p_n} = o(n) = \frac{1}{1-p_n}.$$

Подставляя в предыдущее неравенство $k = \left[\log n - \log\log\frac{1}{p_n}\right] + r$, $r \geqslant 2$, убеждаемся в том, что правая часть стремится к 0 если $n \to \infty$. С другой стороны, если $k \leqslant \left[\log n - \log\log\frac{1}{p_n}\right] - 1$, при подходящем выборе $\varphi(n)$ отношение $\frac{\varphi(n)}{\sqrt{2^{n-k}\cdot p_n^{2k}}} \to 0$. Из этого следует

Теорема 1. Пусть $\frac{1}{p_n} = o(n) = \frac{1}{1-p_n}$. С вероятностью стремящейся к 1 при $n \to \infty$ случайная булева функция не имеет интервалов размерности большей $\mu = \left[\log n - \log\log\frac{1}{p_n}\right] + 1$. Кроме того при $k \leqslant \left[\log n - \log\log\frac{1}{p_n}\right] - 1 = \mu - 2$ число k-мерных интервалов $i_{n,k}(f)$ случайной булевой функции f асимптотически равно $\binom{n}{k}\cdot 2^{n-k}\cdot p_n^{2k}$, т.е. $i_{n,k} \sim \binom{n}{k}\cdot 2^{n-k}\cdot p_n^{2k}$.

При $k = 0$ значение $i_{n,k}(f)$ равно числу точек множества Nf и тем самым сложности совершенной ДНФ.

Теорема 2. Число точек множества Nf и сложность совершенной ДНФ почти наверное асимптотически равны $p_n\cdot 2^n$.

Сложность сокращенной ДНФ равна числу максимальных интервалов функции. Пока мы получили только верхнюю границу размерности интервалов и тем самым оценку сверху для размерности максимальных интервалов. Теперь подсчитаем их среднее число.

Пусть $I_{n,k}(f)$ — число максимальных k-мерных интервалов функции f и $s(f)$ — сложность сокращенной ДНФ. Тогда $s(f) = \sum_{k=0}^{n} I_{n,k}(f)$. Примерно так как и предложение 4, вводя подходящие индикаторы, доказывается следующее

Предложение 7.

$$EI_{n,k} = \binom{n}{k} \cdot 2^{n-k} \cdot p_n^{2k} \cdot (1 - p_n^{2k})^{n-k}.$$

Рассматривая отношение $\dfrac{EI_{n,k}}{EI_{n,k+1}}$ мы убеждаемся в том, что для больших n оно при $k \leqslant \log\log_{1/p_n} n - 1$ больше единицы и для $k > \log\log_{1/p_n} n$ — меньше единицы. Значит, $EI_{n,k}$ как функция переменной k достигает своего максимума либо при $k = [\log\log_{1/p_n} n] = \lambda$ либо при $k = [\log\log_{1/p_n} n] + 1 = \lambda + 1$. Так как

$$Es = \sum_{k=0}^{n} EI_{n,k} \leqslant (n+1) \cdot \max_k \cdot EI_{n,k},$$

получаем следующую оценку.

Предложение 8.

$$Es \leqslant n^{(1+\varepsilon_1(n)) \cdot \log\log_{1/p_n} n} \cdot 2^n, \quad \lim \varepsilon_1(n) = 0.$$

Ограничимся теперь множеством A_n тех функций, максимальные интервалы которых имеют размерность не большуйю чем $\mu = \left[\log n - \log\log \dfrac{1}{p_n}\right] + 1$; ясно что $\lim P_0(A_n) = 1$. Руководствуясь весьма простыми соображенями получаем

Предложение 9. С вероятностью стремящейся к 1 при $n \to \infty$ выполнено неравенство

$$s(f) \geqslant \frac{i_{n,\lambda}(f)}{\binom{\mu}{\lambda} \cdot 2^{\mu-\lambda}},$$

$$\lambda = \left[\log\log n - \log\log \frac{1}{p_n}\right] = [\log\log_{1/p_n} n].$$

Теперь сформулируем основной результат.

Теорема 3. Пусть $\dfrac{1}{p_n} = o(n) = \dfrac{1}{1-p_n}$. Тогда с вероятностью стремящейся к 1 при $n \to \infty$ верны следующие оценки:

$$n^{(1-\varepsilon_2(n))\log\log_{1/p_n} n} \cdot 2^n \leqslant s(f) \leqslant n^{(1+\varepsilon_3(n))\log\log_{1/p_n} n} \cdot 2^n$$

причем $\lim \varepsilon_2(n) = 0 = \lim \varepsilon_3(n)$. Более того, если $\lim p_n = p \in (0, 1)$, то

$$\varepsilon_2(n) = O\left(\frac{1}{\log\log_{1/p_n} n}\right) = \varepsilon_3(n).$$

Верхняя оценка вытекает из предложения 8 и 1-ого неравенства Чебышева, полагая $\varepsilon = n$. Нижняя оценка является следствием предложения 9 и предложения 6.

Изучение поведения $EI_{n,k}$ как функции от k показывает, что $EI_{n,k}$ сначала растет, достигая своего максимума при k примерно равном $\log\log_{1/p_n} n$, а затем убывает. Можно ожидать, что в сокращенной ДНФ наиболее часто встречаться будут интервалы размерности близкой к $\log\log_{1/p_n} n$. Следующая теорема показывает, что это на самом деле так.

Чтобы сформулировать ее, обозначим через $I_{>k}$ ($I_{<k}$) сумму $\sum\limits_{l>k} I_{n,l}$ $\left(\sum\limits_{l<k} I_{n,l}\right)$. Пусть $H_{>k}$ ($H_{<k}$) — число точек множества Nf, покрываемых максимальными интервалами размерности большей (меньшей) k.

Теорема 4. Пусть

$$\frac{1}{p_n} = o(n) = \frac{1}{1-p_n} \quad \text{и} \quad \lambda_1 = \log\log_{1/p_n} n - 1,$$

$$\lambda_2 = \log\log_{1/p_n} n + \log\log\log_{1/p_n} n + \varepsilon, \qquad \varepsilon > 0.$$

Тогда с вероятностью стремящейся к 1 при $n \to \infty$

$$I_{<\lambda_1}(f) = o(2^n) = I_{>\lambda_2}(f)$$

$$H_{<\lambda_1}(f) = o(2^n) = H_{>\lambda_2}(f).$$

Таким образом подавляющую часть сокращенной ДНФ случайной булевой функции составляют интервалы размерностей не меньше λ_1 и не больше λ_2.

Для случая $p_n = \dfrac{1}{2}$ аналогичные оценки получены Глаголевым в [1].

4. Длина а число тупиковых ДНФ

Через $l(f)$ обозначим наибольшуйю длину тупиковой ДНФ функции $f \in B_n$. Известно [3, 4] и просто доказывается, что $l(f) \leqslant |Nf|$. В силу предложения 6 имеем

Предложение 10. С вероятностью стремящейся к 1 при $n \to \infty$ верно неравенство $l(f) \leqslant p_n \cdot 2^n + \varphi(n)\sqrt{p_n \cdot 2^n}$, где $\dfrac{1}{\varphi(n)} = o(1)$.

Верхняя оценка числа $\tau(f)$ тупиковых ДНФ случайной булевой функции является тоже следствием результатов предыдущего раздела. Ясно, в частности, что число тупиковых ДНФ не превосходит числа всех покрытий множества Nf максимальными интервалами. Поэтому

$$\tau(f) \leqslant \sum_{i \geqslant 1} \binom{s(f)}{i}.$$

Из этого вытекает

Предложение 11. С вероятностью стремящейся к 1 при $n \to \infty$ верна оценка

$$\tau(f) \leqslant 2^{p_n \cdot 2^n \cdot \log n \cdot \log\log_{1/p_n} n \cdot (1 + \varepsilon_4(n))}, \quad \lim \varepsilon_4(n) = 0.$$

В то время как верхние оценки доказываются довольно нетрудно, весь следующий аппарат используется для оценок снизу. Нам нужны более тонкие методы. Оценки вспомогательных параметров должны быть более точными. Ограничения налагаемые на последовательность (p_n) здесь также более строгие: начиная с этого места мы предполагаем, что

$$\frac{1}{p_n} = o\left(\frac{\sqrt{n}}{\log n}\right) \quad \text{и} \quad \frac{1}{1 - p_n} = o(\log\log n).$$

Мы используем идею основанную на рассмотрении функций f с некоторым выделенным подмножеством $Af \subseteq Nf$, принадлежащую Сапоженко [4]. На самом деле такие функции образуют множество

$$C_n = \{(f_1, f_2) \in B_n \times B_n;\ Nf_2 \subseteq Nf_1\}$$

упомянутое уже в разд. 1.

Сначала исследуем максимальные интервалы проходящие фиксированной вершиной $\alpha \in D^n$. На пространстве $(C_n^\alpha, \boldsymbol{P}_3)$, (см. разд. 2), рассмотрим случайную величину $M_{n,k}^\alpha$, которая определяется следующим способом: взяв $f = (f_1, f_2) \in C_n^\alpha$, пусть $M_{n,k}^\alpha(f)$ — число максимальных k-мерных интервалов $K \subseteq Nf_1$ таких, что $\alpha \in K$, $K - \{\alpha\} \subseteq Nf_2$. Для фиксированной k-мерной грани K, $\alpha \in K$, введем индикатор ζ_K определенный на C_n^α.

$$\zeta_K(f) = \begin{cases} 1, & \text{если } K \text{ — максимальный интервал функции } f_1 \text{ и } K - \{\alpha\} \subseteq Nf_2 \\ 0, & \text{в остальных случаях.} \end{cases}$$

Интервал K, для которого $\zeta_K(f) = 1$, $\alpha \in K$, называется погруженным в Nf_2, ср. [3, 4]. Очевидно, что $M_{n,k}^\alpha = \sum_K \zeta_K$, где суммирование ведется по всем k-мерным граням n-мерного куба D^n, содержащим точку α.

Используя для выражения максимальности интервала K формулу включений и исключений и затем неравенства Бонферрони [5], получаем

$$p_n^{2k+1}\cdot(1-p_n+p_n^2)^{2^n-2^k}-(n-k)\cdot p_n^{3\cdot 2^k}\cdot(1-p_n+p_n^2)^{2^n-2^{k+1}}\leqslant \boldsymbol{P}_1(\zeta_K(f)=1)\leqslant$$
$$\leqslant p_n^{2^{k+1}-1}\cdot(1-p_n+p_n^2)^{2^n-2^k}.$$

Отсюда имеем

Предложение 12.

$$\binom{n}{k}\left(\frac{p_n^2}{1-p_n+p_n^2}\right)^{2^k-1}\cdot\left(1-p_n(n-k)\left(\frac{p_n}{1-p_n+p_n^2}\right)^{2^k}\right)\leqslant$$
$$\leqslant \boldsymbol{E}M_{n,k}^{\alpha}\leqslant\binom{n}{k}\left(\frac{p_n^2}{1-p_n+p_n^2}\right)^{2^k-1}.$$

Предложение 13. Если

$$k\geqslant\left[\log\log_{1/p_n}n+\log\log\frac{1}{p_n^2}-\log\log\frac{1-p_n+p_n^2}{p_n}\right]=\varkappa,$$

то

$$\binom{n}{k}\left(\frac{p_n^2}{1-p_n+p_n^2}\right)^{2^k-1}\cdot\left(1-\frac{p_n}{n}\right)\leqslant \boldsymbol{E}M_{n,k}^{\alpha}\leqslant\binom{n}{k}\left(\frac{p_n^2}{1-p_n+p_n^2}\right)^{2^k-1}$$

и, следовательно,

$$\boldsymbol{E}M_{n,k}^{\alpha}\sim\binom{n}{k}\left(\frac{p_n^2}{1-p_n+p_n^2}\right)^{2^k-1}.$$

Заметим, что

$$\log\log\frac{1}{p_n^2}-\log\log\frac{1-p_n+p_n^2}{p_n}>0,$$

поскольку $\dfrac{1}{p_n^2}>\dfrac{1}{p_n}>\dfrac{1-p_n+p_n^2}{p_n}$ для больших n.

Чтобы подвинуться дальше, обозначим через ζ'_K индикатор на $(C_n^{\alpha}, \boldsymbol{P}_3)$

$$\zeta'_K(f)=\begin{cases}1, & \text{если } K\subseteq Nf_1 \text{ и } K-\{\alpha\}\subseteq Nf_2\\ 0 & \text{в остальных случаях.}\end{cases}$$

Ясно, что $\zeta_K\leqq\zeta'_K$ и следовательно

$$(M_{n,k}^{\alpha})^2=\left(\sum_K\zeta_K\right)^2\leqslant\left(\sum_K\zeta'_K\right)^2=\sum_{(K,L)}\zeta'_K\cdot\zeta'_L,$$

причем в последней сумме суммируется по всем упорядоченным парам k-мерных граней куба D^n, проходящих через вершину α. Рассматривая возможные пересечения $K\cap L$ этих пар получаем

$$E(M^a_{n,k})^2 \leqslant \sum_{(K,L)} E(\zeta'_K \cdot \zeta'_L) =$$

$$= \binom{n}{k}\left(\frac{p_n^2}{1-p_n+p_n^2}\right)^{2k+1-1} \cdot \sum_{l=0}^{k} \binom{k}{l}\binom{n-k}{k-l}\left(\frac{1-p_n+p_n^2}{p_n^2}\right)^{2l}.$$

Последнюю сумму нетрудно оценить сверху, так как

$$1 \leqslant \frac{1-p_n+p_n^2}{p_n^2} \quad \text{и} \quad \sum_{l=0}^{k}\binom{k}{l}\binom{n-l}{k-l} = \binom{n}{k}.$$

Однако, получаемая таким образом оценка

$$E(M^a_{n,k})^2 \leqslant \binom{n}{k}^2 \left(\frac{p_n^2}{1-p_n+p_n^2}\right)^{2k-1}$$

слишком груба и не выгодна для наших целей. Чтобы получить более точную оценку, заметим, что обозначая

$$\binom{k}{l}\binom{n-k}{k-l}\left(\frac{1-p_n+p_n^2}{p_n^2}\right)^{2l} = a_l,$$

при больших n и $k = \varkappa$ имеет место $a_1 \geqslant a_l$ $(l \geqslant 2)$. Отсюда вытекает

$$E(M^a_{n,k})^2 \leqslant \binom{n}{k}\left(\frac{p_n^2}{1-p_n+p_n^2}\right)^{2k+1-1} \cdot (a_0 + k \cdot a_1) \quad \text{и}$$

Предложение 14.

$$E(M^a_{n,k})^2 \leqslant \binom{n}{k}^2 \left(\frac{p_n^2}{1-p_n+p_n^2}\right)^{(2k-1)\cdot 2} \cdot \left(1 + O\left(\frac{1-p_n+p_n^2}{p_n} \cdot \frac{k^3}{n}\right)\right) \quad \text{при } k = \varkappa.$$

Для

$$\varkappa = \left[\log\log_{1/p_n} n + \log\log\frac{1}{p_n^2} - \log\log\frac{1-p_n+p_n^2}{p_n}\right]$$

обозначим $M^a_{n,\varkappa} = \zeta^a$. Соединяя предложение 13 и предложение 14 пользуясь 2-ым неравенством Чебышева, получаем

Предложение 15.

$$P_3\left(|\xi^a - E\xi^a| \geqslant \frac{1}{\varkappa} E\xi^a\right) = O\left(\frac{1-p_n+p_n^2}{p_n} \cdot \frac{\varkappa^5}{n}\right).$$

Следовательно, $\xi^a \geqslant \left(1 - \frac{1}{\varkappa}\right)E\xi^a$ с вероятностью стремящейся к 1, если $n \to \infty$.

Таким образом, для фиксированной вершины α почти наверное число интервалов погруженных в Nf_2 близко к математическому ожиданию; более точно, $|\xi^\alpha - \boldsymbol{E}\xi^\alpha| < \frac{1}{\varkappa}\boldsymbol{E}\xi^\alpha$.

Теперь исследуем число вершин в Nf_1, для которых последнее неравенство не выполнено. (Такие вершины принято называть плохими.) На этом месте переходим от пространства $(C_n^\alpha, \boldsymbol{P}_3)$ к пространству $(C_n, \boldsymbol{P}_2)$. Для любой пары $f \in C_n$ положим

$$Bf = \left\{\alpha \in Nf_1;\ |\xi^\alpha - \boldsymbol{E}\xi^\alpha| \geqslant \frac{1}{\varkappa}\boldsymbol{E}\xi^\alpha\right\}$$

и через ηf обозначим число $|Bf|$ плохих вершин пары f. Пусть η_α — индикатор свойства вершины $\alpha \in D^n$ «быть плохой», т.е.

$$\eta_\alpha(f) = \begin{cases} 1, & \text{если } |\xi^\alpha - \boldsymbol{E}\xi^\alpha| \geqslant \frac{1}{\varkappa}\boldsymbol{E}\xi^\alpha \\ 0 & \text{в остальных случаях; } f \in C_n. \end{cases}$$

Поскольку $\eta = \sum\limits_{\alpha \in D^n} \eta_\alpha$, имеем

$$\boldsymbol{E}\eta = 2^n \cdot \boldsymbol{E}\eta_{\tilde{1}} = 2^n \cdot \boldsymbol{P}_2\left(\tilde{1} \in Nf_1,\ |\xi^{\tilde{1}} - \boldsymbol{E}\xi^{\tilde{1}}| \geqslant \frac{1}{\varkappa}\boldsymbol{E}\xi^{\tilde{1}}\right) =$$
$$= 2^n \cdot \boldsymbol{P}_3\left(|\xi^{\tilde{1}} - \boldsymbol{E}\xi^{\tilde{1}}| \geqslant \frac{1}{\varkappa}\boldsymbol{E}\xi^{\tilde{1}}\right) \cdot \boldsymbol{P}_2(C_n^{\tilde{1}}).$$

Тем самым мы получили следующий результат.

Предложение 16.

$$\boldsymbol{E}\eta = 2^n \cdot O\left(\frac{\varkappa^2}{p_n \cdot n}\right).$$

Применив 1-ое неравенство Чебышева с $\varepsilon = 2^n \cdot \dfrac{\varkappa^6}{p_n \cdot n}$ находим

Предложение 17. Для всякой пары $f \in C_n$ число плохих вершин почти наверное выполняет неравенство

$$|Bf| \leqslant 2^n \cdot \frac{\varkappa^6}{p_n \cdot n}.$$

Возвращаясь на этом шагу к первоначальному пространству $(\boldsymbol{B}_n, \boldsymbol{P}_0)$ введем несколько обозначений:

$$T_n = \left\{f \in C_n;\ |Bf| \leqslant 2^n \cdot \frac{\varkappa^6}{p_n \cdot n}\right\}$$

$$U_n = \{g \in B_n;\ |Ng| = 2^{n-\nu}\}, \quad \nu = \left[\log\log n + \log\log\log n - 2\log\log \frac{1}{p_n}\right],$$

$$V_n = \{h \in B_n;\ \ g \in U_n\colon Ng \subseteq Nh \text{ и } (h, g) \in T_n\}.$$

Мы хотим убедиться в том, что $\lim P_0(V_n) = 1$, т. е. грубо говоря, какая бы ни была функция $g \in B_n$, существует такая пара $f \in C_n$, что $f_1 = g$, Nf_2 достаточно велико но число плохих вершин этой пары мало. Ради этой цели обозначим еще

$$W_n = B_n \times U_n$$

$$X_n = W_n \cap T_n.$$

Весьма просто доказывется, что

$$1 \geqslant P_0(V_n) \geqslant \frac{P_1(X_n)}{P_0(U_n)} \quad \text{и} \quad \lim \frac{P_1(X_n)}{P_0(U_n)} \geqq \lim \frac{P_1(W_n)}{P_1(W_n)} = 1.$$

Таким образом, мы получили

Предложение 18. С вероятностью стремящейся к 1 при $n \to \infty$ для всякой булевой функции $g \in B_n$ существует такая пара $f \in C_n$, что $f_1 = g$, $|Nf_2| = 2^{n-\nu}$, $\left(\nu = \left[\log\log n + \log\log\log n - 2\log\log \frac{1}{p_n}\right]\right)$, и $|Bf| \leqslant 2^n \cdot \frac{\varkappa^6}{p_n \cdot n}$.

Следующее вспомогательное утверждение касается числа наборов в Nf покрываемых интервалами определенной размерности в случайной булевой функции. Для $f \in B_n$ пусть $h_{n,k}(f)$ равно числу вершин в Nf покрываемых интервалами размерности k. Очевидно, что $h_{n,k}(f) \leqslant i_{n,k}(f) \cdot 2^k$. В силу 1-ого неравенства Чебышева и предложения 4 имеем

Предложение 19. С вероятностью стремящейся к 1 при $n \to \infty$ для $f \in B_n$ имеет место неравенство

$$h_{n,k}(f) \leqslant \varphi(n) \cdot \binom{n}{k} \cdot 2^n \cdot p_n^{2^k}, \quad \text{где} \quad \frac{1}{\varphi(n)} = o(1).$$

Теперь мы уже в близу цели. Все подготовлено для нижних оценок обеих основных теорем настоящего раздела.

Теорема 5. Пусть

$$\frac{1}{p_n} = o\left(\frac{\sqrt{n}}{\log n}\right) \quad \text{и} \quad \frac{1}{1 - p_n} = o(\log\log n).$$

С вероятностью стремящейся к 1 при $n \to \infty$ для случайной булевой функции имеют место следующие оценки:

$$p_n \cdot 2^n \cdot (1 - \varepsilon_5(n)) \leqslant l(f) \leqslant p_n \cdot 2^n + \varphi(n) \cdot \sqrt{p_n \cdot 2^n}, \quad \text{где } \varepsilon_5(n) \to 0.$$

Следовательно, $l(f) \sim p_n \cdot 2^n$. Более того, если $\lim p_n = p \in (0, 1)$, то

$$\varepsilon_5(n) = O\left(\frac{1}{\log \log_{1/p_n} n}\right).$$

Оценка $l(f)$ снизу использует конструкцию Сапоженко [4] покрытия множества Nf, где $f \in V_n$, содержащего тупиковое покрытие большой длины. В нашем случае она основана на предложениях 12—19 и осуществляется в три шага. Пусть $g \in V_n$. Тогда найдется $f \in C_n$, что $f_1 = g$, $|Nf_2| = 2^{n-\nu}$ и $|Bf| \leqslant 2^n \cdot \dfrac{\varkappa^6}{p_n \cdot n}$.

1. Пусть $\mathcal{U}_1$ — какое-нибудь тупиковое покрытие множества Bf. Можно доказать, что

$$\left|\bigcup \mathcal{U}_1\right| \leqslant 2^\nu \cdot |Bf| + h_{n,\nu}(f_1),$$

$$\nu = \left[\log\log n + \log\log\log n - 2\log\log \frac{1}{p_n}\right].$$

2. Пусть $\mathcal{U}_2$ — тупиковое покрытие множества $Nf_2 - \bigcup \mathcal{U}_1$ максимальными интервалами функции $g = f_1$ погруженными в Nf_2. Ясно, что

$$\left|\bigcup \mathcal{U}_2\right| \leqslant 2\,|Nf_2|.$$

3. Оставшиеся непокрытыми вершины станем покрывать максимальными интервалами размерности $\varkappa$ погруженными в Nf_2. Очевидно, что для покрытия всякой вершины

$$\alpha \in Nf_1 - \left(\bigcup \mathcal{U}_1 \cup \bigcup \mathcal{U}_2\right)$$

имеем $\xi^\alpha(f)$ возможностей. Пусть $\mathcal{U}_3$ — покрытие множества

$$Nf_1 - \left(\bigcup \mathcal{U}_1 \cup \bigcup \mathcal{U}_2\right)$$

образованное взятием для каждой вершины α ровно одного из $\xi^\alpha(f)$ возможных интервалов.

Множество $\mathscr{U}_1 \cup \mathscr{U}_2 \cup \mathscr{U}_3$ является покрытием множества $Ng = Nf_1$. Пусть $\mathscr{U}$ — любое тупиковое покрытие содержащееса в $\mathscr{U}_1 \cup \mathscr{U}_2 \cup \mathscr{U}_3$. Понятно, что $\mathscr{U}_3 \subseteq \mathscr{U}$. Таким образом, всякая функция g из

$$V_n \cap \{f \in B_n;\ |Nf| \geqslant p_n \cdot 2^n - \varphi(n) \cdot \sqrt{p_n \cdot 2^n}\} = V_n'$$

имеет тупиковуя ДНФ длины равной по крайней мере

$$|\mathscr{U}_3| = \left| Nf_1 - \bigcup (\mathscr{U}_1 \cup \mathscr{U}_2) \right| \geqslant$$

$$\geqslant |Ng| - 2^r |Bf| - h_{n,r}(f_1) - 2\,|Nf_2| \geqslant p_n \cdot 2^n (1 - o(1)).$$

При этом ясно, что $\lim P_0(V_n') = 1$ (предложения 3, 6).

Из выше сказанного вытекает, что число тупиковых ДНФ функции $g \in V_n'$ не меньше числа возможностей выбора покрытия $\mathscr{U}_3$. В силу предложения 15 последнее можно снизу ограничить выражением

$$\left(\left(1 - \frac{1}{\varkappa}\right) E\xi^{\alpha}\right)^{|Nf_1 - \cup (\mathscr{U}_1 \cup \mathscr{U}_2)|} \geqslant 2^{p_n \cdot 2^n \cdot \log n \cdot \log\log_{1/p_n} n \cdot (1 + o(1))}$$

Итак, имеет место

Теорема 6. Пусть

$$\frac{1}{p_n} = o\left(\frac{\sqrt{n}}{\log n}\right) \quad \text{и} \quad \frac{1}{1 - p_n} = o(\log\log n).$$

Тогда с вероятностью стремящейся к 1 при $n \to \infty$ верны оценки

$$2^{p_n \cdot 2^n \cdot \log n \cdot \log\log_{1/p_n} n \cdot (1 - \varepsilon_6(n))} \leqslant \tau(f) \leqslant 2^{p_n \cdot 2^n \cdot \log n \cdot \log\log_{1/p_n} n \cdot (1 + \varepsilon_7(n))},$$

где $\lim \varepsilon_6(n) = 0 = \lim \varepsilon_7(n)$. Если кроме того $\lim p_n = p \in (0, 1)$, то

$$\varepsilon_6(n) = O\left(\frac{1}{\log\log_{1/p_n} n}\right) \quad \text{и} \quad \varepsilon_7(n) = O\left(\frac{1}{\log n \cdot \log\log_{1/p_n} n}\right).$$

ЛИТЕРАТУРА

[1] Глаголев, В. В.: Некоторые оценки дизъюнктивных нормальных форм функций алгебры логики, Сб. Проблемы кибернетики, вып. 19 (1967), 75—94.

[2] Дискреная математика и математические вопросы кибернетики, т. 1., Сб. под ред. С. В. Яблонского и О. Б. Лупанова, М.: Наука, 1974.

[3] Сапоженко, А. А.: Дизъюнктивные нормальные формы (метрическая теория) М.: МГУ, 1975.

[4] Сапоженко, А. А.: О наибольшей длине тупиковой дизъюнктивной нормальной формы у почти всех булевых функций, Мат. заметки 4 (1969), № 6, 649—658.
[5] Феллер, В.: Введение в теорию вероятностей и ее приложения, т. 1., М.: Мир, 1967.

Адрес автора:
Martin Škoviera
MFF UK, Katedra teoretickej kybernetiky
Matematický pavilón
Mlynská dolina
Bratislava
842 15

Поступило: 8. 2. 1984

SÚHRN

ODHADY ZLOŽITOSTI DISJUNKTÍVNYCH NORMÁLNYCH FORIEM NÁHODNÝCH BOOLEOVSKÝCH FUNKCIÍ

Martin Škoviera, Bratislava

V článku sa skúma zložitosť rôznych typov disjunktívnych normálnych foriem (DNF) náhodných booleovských funkcií. Uvedené sú asymptotické odhady dĺžky úplnej DNF, skrátenej DNF, maximálnej dĺžky iredundatnej DNF a počtu iredundatných DNF náhodnej booleovskej funkcie.

SUMMARY

ESTIMATES OF COMPLEXITY OF DISJUNCTIVE NORMAL FORMS OF A RANDOM BOOLEAN FUNCTION

Martin Škoviera, Bratislava

Complexity of different types of disjunctive normal forms (DNF) of random Boolean functions is investigated. Asymptotic estimates of the length of the principal DNF, abbreviated DNF, the maximum length of an irredundant DNF and the number of irredundant DNFs of a random Boolean function are given.