UNIVERSITAS COMENIANA
ACTA MATHEMATICA UNIVERSITATIS COMENIANAE
XLVIII—XLIX — 1986

РЕЗУЛЬТАТИВНОСТЬ НЕКОТОРЫХ ЛОКАЛЬНЫХ АЛГОРИТМОВ УПРОЩЕНИЯ СЛУЧАЙНЫХ БУЛЕВЫХ ФУНКЦИЙ

ЭДУАРД ТОМАН, Братислава

В настоящей работе исследуется результативность некоторых локальных алгоритмов упрощения случайных булевых функций. Под случайной булевой функцией понимается функция алгебры логики, которая на вершинах единичного n-мерного куба принимает значение 1 с вероятностью p, $0 < p < 1$, и значение 0 с вероятностью $q = 1 - p$, независимо от значений в остальных вершинах куба. Вершины единичного n-мерного куба занумерованы.

В данной работе установливается, что в случайной булевой функции с вероятностью стремящейся к 1 при $n \to \infty$, д.н.ф. Квайна асимптотически равна сокращенной д.н.ф. и д.н.ф. сумма тупиковых д.н.ф. тоже асимп тотически равна сокращенной д.н.ф. Определения этих понятий можно найти напримерь в работе [2].

Аналогичные результаты получены в работе [1] для $p = 1/2$.

Основным средством для получения результатов является вычисление средних значений некоторых параметров и применение следующего очевидного неравенства Чебышева.

Лемма 1. Пусть $\{\xi_n\}_{n=1}^{\infty}$-последовательность случайных величин таких, что $\xi_n \geqslant 0$ с вероятностью 1. Пусть $\eta(n) \to \infty$ при $n \to \infty$, тогда с вероятностью стремящейся к 1, при $n \to \infty$

$$\xi_n < \eta(n) M_{\xi_n}.$$

Доказательство. Неравенство доказывают следующие соотношения

$$M_{\xi_n} \geqslant M(\xi_n, \xi_n \geqslant \eta(n)M_{\xi_n}) \geqslant \eta(n)M_{\xi_n}M(1, \xi_n \geqslant \eta(n)M_{\xi_n}) =$$
$$= \eta(n)M_{\xi_n}P(\xi_n \geqslant \eta(n)M_{\xi_n}),$$

отсюда

$$P(\xi_n \geqslant \eta(n) M_{\xi_n}) \leqslant \frac{1}{\eta(n)}.$$

Лемма доказана.

Определения и обозначения неприводимые здесь надо понимать в смысле работы [3].

§ 1. Оценка числа ядровых интервалов

Конъюнкцию будем называть ядровой если интервал, который ей соответствует содержит вершину не покрываемую никаким другим интервалом. Совокупность всех ядровых конъюнкций будем называть ядро. Тогда другими словами, конъюнкция входит в ядро, если она не поглощается совокупностью всех других конъюнкций.

Рассмотрим разложение $f(x_1, \ldots, x_n)$ по переменным $x_1, \ldots, x_{n-k}$;

$$(*)\ f(x_1, \ldots, x_n) = x_1 x_2 \ldots x_{n-k} f_0(x_{n-k+1}, \ldots, x_n) \vee \bar{x}_1 x_2 \ldots x_{n-k} f_1(x_{n-k+1}, \ldots, x_n) \vee$$
$$\vee\ x_1 \bar{x}_2 \ldots x_{n-k} f_2(x_{n-k+1}, \ldots, x_n) \vee \ldots \vee x_1 x_2 \ldots \bar{x}_{n-k} f_{n-k}(x_{n-k+1}, \ldots, x_n) \vee$$
$$\vee\ \bar{x}_1 \bar{x}_2 x_3 \ldots x_{n-k} f_{n-k+1}(x_{n-k+1}, \ldots, x_n) \vee \ldots \vee$$
$$\vee\ \bar{x}_1 \bar{x}_2 \ldots \bar{x}_{n-k} f_{2^{n-k}}(x_{n-k+1}, \ldots, x_n).$$

Лемма 2. Пусть $N_{x_1 \ldots x_{n-k}}$ является k-мерным интервалом случайной булевой функции $f(x_1, \ldots, x_n)$. Интервал $N_{x_1 \ldots x_{n-k}}$ является ядровым интервалом тогда и только тогда если в разложении $(*)$ $f_0(x_{n-k+1}, \ldots, x_n) \equiv 1$ и существует набор $(\alpha_{n-k+1}, \ldots, \alpha_n)$ такой, что $f_i(\alpha_{n-k+1}, \ldots, \alpha_n) = 0$ для всех $i = 1, 2, \ldots, n-k$.

Доказательство. Необходимое условие. Пусть максимальный интервал $N_{x_1 \ldots x_{n-k}}$ принадлежит ядру функции $f(x_1, \ldots, x_n)$. Тогда очевидно, что $f_0(x_{n-k+1}, \ldots, x_n) \equiv 1$, потому что конъюнкция $x_1 x_2 \ldots x_{n-k}$ принадлежит д.н.ф. $f(x_1, \ldots, x_n)$. Если бы для любого набора $(\alpha_{n-k+1}, \ldots, \alpha_n)$ существовала хотя бы одна функция $f_i(x_{n-k+1}, \ldots, x_n)$, $i = 1, 2, \ldots, n-k$ для которой бы $f_i(\alpha_{n-k+1}, \ldots, \alpha_n) = 1$, то потом существует ребро

$$N_{x_1 \ldots x_{i-1} x_{i+1} \ldots x_{n-k} x_{n-k+1} \ldots x_n} \not\subseteq N_{x_1 \ldots x_{n-k}}$$

которое содержит вершину $(1, \ldots, 1, \alpha_{n-k+1}, \ldots, \alpha_n)$ и содержится в каком то другом максимальном интервале. Это значит, что точка $(1, \ldots, 1, \alpha_{n-k+1}, \ldots, \alpha_n)$ покрывается максимальным интервалом различным от интервала $N_{x_1 \ldots x_{n-k}}$, это противоречит тому, что интервал $N_{x_1 \ldots x_{n-k}}$ входит в ядро.

Достаточное условие. Пусть $f_0(x_{n-k+1}, \ldots, x_n) \equiv 1$ и существует набор $(\alpha_{n-k+1}, \ldots, \alpha_n)$ такой, что $f_i(\alpha_{n-k+1}, \ldots, \alpha_n) = 0$ для всех $i = 1, 2, \ldots, n-k$. Пусть $N_{x_1 \ldots x_{n-k}}$ не принадлежит ядру $f(x_1, \ldots, x_n)$, потом существует вершина $(1, \ldots, 1, \alpha_{n-k+1}, \ldots, \alpha_n) \in N_{x_1 \ldots x_{n-k}}$ и хотя бы одно ребро

$$N_{x_1 \ldots x_{i-1} x_{i+1} \ldots x_{n-k} \alpha_{n-k+1}} \nsubseteq N_{x_1 \ldots x_{n-k}},$$

содержащее эту вершину и принадлежащее N_f, но потом $f_i(\alpha_{n-k+1}, \ldots, \alpha_n) = 1$, что противоречит предположению.

Пусть $c(f)$ — число ядровых интервалов случайной булевой функции $f(x_1, \ldots, x_n)$ и $M_{\xi_n^{(1)}}$ — среднее значение этого параметра.

Лемма 3.

$$M_{\xi_n^{(1)}} = \sum_{k=0}^{n} C_n^k 2^{n-k} p^{2^{2k}} (1 - (1 - (1-p)^{n-k})^{2^k}).$$

Доказательство. Пусть $P_{n,k}$ вероятность того, что фиксированная k-мерная грань n-мерного единичного куба является ядровым интервалом случайной булевой функции $f(x_1, \ldots, x_n)$. Очевидно, что

$$M_{\xi_n^{(1)}} = \sum_{k=0}^{n} C_n^k 2^{n-k} P_{n,k}.$$

Тогда сначала подсчитается вероятность того, что фиксированная грань размерности k является ядровым интервалом случайной булевой функции. В силу того, что свойство интервала быть ядровым интервалом данной функции сохраняется при перенумерации переменных, при замене переменной на отрицание, эта вероятность будет одна и та же для всех интервалов данной размерности. Поэтому достаточно подсчитать ее для фиксированного интервала $N_{x_1 \ldots x_{n-k}}$. В силу леммы 2 интервал является ядровым в том и только в том случае, когда он содержит точку, непокрываемую никаким другим максимальным интервалом. Рассматрим розложение (*) функции $f(x_1, \ldots, x_n)$. Вероятность того, что $f_0(x_{n-k+1}, \ldots, x_n) \equiv 1$ равна p^{2^k}, далее вероятность того, что существует хотя бы одна вершина принадлежащая интервалу $N_{x_1 \ldots x_{n-k}}$ и не покрываемая ни каким другим максимальным интервалом, равна $(1 - (1 - (1-p)^{n-k})^{2^k})$ и тогда

$$M_{\xi_n^{(1)}} = \sum_{k=0}^{n} C_n^k 2^{n-k} p^{2^k} (1 - (1 - (1-p)^{n-k})^{2^k}).$$

Теперь оценим среднее $M_{\xi_n^{(1)}}$.

Лемма 4. С вероятностью сремящейся к 1 при $n \to \infty$

$$M_{\xi_n^{(1)}} \leqslant n^{(1+\gamma_n)\log\log_{\frac{1}{p}} n}(2(1-p)^n),$$

где $\gamma_n \to 0$ при $n \to \infty$.

Доказательство. Оценим порядок величины $M_{\xi_n^{(1)}}$. С этой целью сумму из леммы 3 разобъем на два слагаемых S_1 и S_2 и оценим каждое отдельно. Выбирая целое число l так, чтобы $p^{2^l} < 1/3$, тогда получаем, что

$$S_1 = \sum_{k > \log n + l}^{n} C_n^k 2^{n-k} p^{2^k}(1 - (1 - (1-p)^{n-k})^{2^k}) \leqslant \sum_{k > \log n + l}^{n} C_n^k 2^{n-k} p^{2^k} \leqslant$$

$$\leqslant \sum_{k=0}^{n} C_n^k 2^{n-k} p^{2^k} \leqslant p^{2^{\log n + l}} \sum_{k=0}^{n} C_n^k 2^{n-k} = (3p^{2^l}) < 1.$$

Для оценки другого слагаемого найдем максимум величины $b_k = C_n^k 2^k 2^{n-k}(1-p)^{n-k} p^{2^k}$. Взяв отношение $b_{k+1}/b_k = (n-k)p^{2^k}/(k+1)(1-p)$ замечаем, что начиная с некоторого n, при $k \leqslant \log\log_{\frac{1}{p}} n - 1$ оно больше единицы, а при $k > \log\log_{\frac{1}{p}} n$ оно меньше единицы. Поэтому максимум b_k достигается либо при $k = \lambda$, либо при $k = \lambda + 1$ где $\lambda = [\log\log_{1/p} n]$. Отсюда иммем:

$$S_2 = \sum_{k \leqslant \log n + l} C_n^k 2^{n-k} p^{2^k}(1 - (1 - (1-p)^{n-k})^{2^k}) \leqslant$$

$$\leqslant \sum_{k \leqslant \log n + l} C_n^k 2^{n-k} p^{2^k}(1 - (1 - 2^k(1-p)^{n-k})) =$$

$$= \sum_{k \leqslant \log n + l} C_n^k 2^{n-k} p^{2^k}(1-p)^{n-k} \cdot 2^k \leqslant (\log n + l + 1) \max_{k \leqslant \log n + l} b_k \leqslant$$

$$\leqslant \frac{C_n^{\lambda+1}}{\sqrt{n}} c_1 \log^2 n(2(1-p))^n$$

где c_1 некоторая константа. С другой стороны

$$S_2 \geqslant C_n^\lambda 2^{n-\lambda} p^{2^\lambda}(1 - (1 - (1-p)^{n-\lambda})^{2^\lambda}) \geqslant$$

$$\geqslant C_n^\lambda 2^{n-\lambda} p^{2^\lambda}(1 - (1 - 2^\lambda(1-p)^{n-\lambda} + (2^\lambda(1-p)^{n-\lambda})^2) \geqslant$$

$$\geqslant C_n^\lambda 2^{n-\lambda} p^{2^\lambda} 2^\lambda (1-p)^\lambda (1 - 2^\lambda(1-p)^{n-\lambda}) \geqslant$$

$$\geqslant C_n^\lambda \frac{c_2 \log n}{n} 2^{n-\lambda}(1-p)^{n-\lambda} = C_n^\lambda \frac{c_2 \log n}{n}(2(1-p))^n,$$

где c_2 — некоторая константа. Таким образом

$$C_n^{\lambda}\frac{c_2\log n}{n}(2(1-p))^n \leqslant M_{\xi_n^{(1)}} \leqslant \frac{C_n^{\lambda+1}}{\sqrt{n}}c_1\log^2 n(2(1-p))^n + (3p^{2l})^n.$$

Из этих неравенств вытекает, что

$$M_{\xi_n^{(1)}} \leqslant n^{(1+\gamma_n)\log\log_{1/p}n}(2(1-p))^n,$$

где $\gamma_n \to 0$ при $n \to \infty$.

Замечание. При оценке S_2 мы воспользовались следующими неравенствами; для всякого натурального n и для $0 \leqslant x \leqslant 1$, имеет место

$$(1-nx) \leqslant (1-x)^n \leqslant (1-nx+n^2x^2).$$

Очевидным следствием предидущей леммы и неравенства Чебышева получаем следующее утверждение.

Лемма 5. С вероятностью стремящейся к 1 при $n \to \infty$ число ядровых интервалов случайной булевой функции $f(x_1, \ldots, x_n)$ $c(f)$ не превосходит

$$n^{(1+\gamma'_n)\log\log_{1/p}n}(2(1-p))^n,$$

где $\gamma'_n \to 0$ при $n \to \infty$.

§ 2. Оценка числа регулярных точек

Пусть $f(x_1, \ldots, x_n)$ — случайная булева функция n-переменных. Вершину $\tilde{\alpha} \in N_f$ назовем регулярной точкой случайной булевой функции f, если существует другая вершина $\tilde{\beta} \in N_f$ такая, что любой максимальный интервал проходящий через $\tilde{\beta}$, проходит и через $\tilde{\alpha}$. Вершину $\tilde{\beta}$ будем назвывать порождающей регулярную точку $\tilde{\alpha}$. Обозначим через $r(f)$ число регулярных точек функции $f(x_1, \ldots, x_n)$ и через $M_{\xi_n^{(2)}}$ — среднее число значения параметра $r(f)$.

Лемма 6. С вероятностью стремящейся к 1 при $n \to \infty$

$$r(f) < \varrho^n,$$

где ϱ константа, зависящая от p и $3/2 < \varrho < 2$.

Доказателство. Пусть $P_n(\tilde{\alpha})$ — обозначает вероятность того, что вершина $\tilde{\alpha}$ является регулярной точкой случайной булевой функции $f(x_1, \ldots, x_n)$. В силу того, что свойство точки быть регулярной точкой для случайной булевой функции $f(x_1, \ldots, x_n)$ сохраняется при замене переменной на отрицание, то вероятность того, что точка является регулярной будет одна и та же для всех $\tilde{\alpha}_j$, потому $M_{\xi_n^{(2)}} = 2^n P_n(\tilde{1})$, где $\tilde{1} = (1, \ldots, 1)$. Для произвольной вершины $\tilde{\beta}$ обозначим через $P_{n, \beta}(\tilde{1})$ вероятность того, что точка $\tilde{1}$ является регулярной и порождается точкой $\tilde{\beta}$. Так как это отношение между точками $\tilde{\beta}$ и $\tilde{1}$ сохраняется при перенумерации переменных, то $P_{n, \beta}(\tilde{1})$ будет одна и та же для всех точек $\tilde{\beta}$, находящихся от $\tilde{1}$ на данном растоянии k. Обоначим ее $P_{n, k}(\tilde{1})$.

Тогда

$$P_n(\tilde{1}) \leqslant \sum_{k=1}^{n} C_n^k P_{n, k}(\tilde{1})$$

(регулярная точка может иметь несколько порождающих).

Оценим $P_{n, k}(\tilde{1})$. Можно считать, что порождающей является точка

$$\tilde{\beta} = (\underbrace{1, \ldots, 1}_{n-k}, \underbrace{0, \ldots, 0}_{k}).$$

Рассмотрим разложение (*) из § 1. Для того, чтобы точка $\tilde{\beta}$ попрождала регулярную точку $\tilde{1}$, необходимо выполнение следующих условий:

(а) $f_0(x_{n-k+1}, \ldots, x_n) \equiv 1$;

(б) если $f_i(0, \ldots, 0) = 1$, то $f_i(x_{n-k+1}, \ldots, x_n) = 1$, $i = 1, 2, \ldots, n-k$.

Условие (а) очевидно. Чтобы убедиться в справедливости (б) заметим, что если $f_i(0, \ldots, 0) = 1$, то $\tilde{B}$ проходит интервал, содержающий ребро $N_{x_1 \ldots x_{i-1} x_{i+1} \ldots x_{n-k} \bar{x}_{n+k+1} \ldots \bar{x}_n}$. Так как этот интервал должен проходить через точку $\tilde{1}$, он содержит интервал $N_{x_1 \ldots x_{i-1} \bar{x}_i x_{i+1} \ldots x_{n-k}}$, а это означает, что $f_i(x_{n-k+1}, \ldots, x_n) \equiv 1$.

Вероятность того, что $f_0(x_{n-k+1}, \ldots, x_n) \equiv 1$ равна p^{2^k}, и вероятность того, чтобы выбрать коэфициенты $f_1, \ldots, f_{n=k}$ удовлетворяющее условию (б) равна $(1 - p + p^{2^k})^{n-k}$; либо $f_i \equiv 1$, либо f_i — одна из функций, обращающихся в нуль на нулевом наборе.

Имеем далее,

$$P_n(\tilde{1}) = \sum_{k=1}^{n} C_n^k (1 - p + p^{2^k})^{n-k} p^{2^k}$$

и тогда

$$M_{\xi_n^{(2)}} \leqslant 2^n \sum_{k=1}^{n} C_n^k (1 - p + p^{2^k})^{n-k} p^{2^k} = \sum_{k=1}^{n} C_n^k p^{2^k} (1 - p + p^{2^k})^{n-k} 2^{n-k} 2^k =$$

$$= \sum_{k=1}^{n} C_n^k (2p^{2^k/k})^k (1 - p + p^{2^k})^{n-k} 2^{n-k} \leqslant n 2^n p^2 (1 - p + p^2)^{n-1} +$$

$$+ \ldots + C_n^k (2p^{(2^{k_0}/(k_0))})^{k_0} (1 - p + p^{2^{k_0}})^{n-k_0} \cdot 2^{n-k_0} +$$

$$+ \sum_{k=0}^{n} C_n^k (2p^{2^{k_0+1}/(k_0+1)})^k (1 - p + p^{2^{k_0+1}})^{n-k} 2^{n-k} \leqslant cn 2^n (1 - p + p^2)^n (1 + o(1)),$$

где c — константа. Замечаем, что для всякого фиксированного p, $0 < p < 1$, существует такое k_0, что имеет место последнее неравенство. (Мы воспользовались тем, что при $k \geqslant k_0 + 1$, $p^{2k/k} \leqslant p^{2k_0+1/k_0+1}$ и $(1 - p + p^{2^k}) \leqslant$ $\leqslant (1 - p + p^{2^{k_0+1}})$).

Таким образом

$$M_{\xi_n^{(2)}} < cn2^n(1 - p + p^2)^n(1 + o(1)) = cn\varrho^n$$

где $3/2 < \varrho < 2$, ϱ — константа, зависящая от p. Используя неравенство Чебышева, получаем, что $r(f) < \varrho^n$.

§ 3. Основные результаты

То обстоятельство, что почти всегда ядровых интервалов сравнительно мало позволяет оценить эфективность применения к сокращенной д.н.ф. упрощения Квайна, смотри [2].

Будем рассматривать случайные булевы функции у которых размерность максимальных интервалов не превосходит $k = [\log_{1/p} n] + 1$ и что число $s(f)$ конъюнкций в сокращенной д.н.ф. находится в пределах

$$n^{(1-\delta_n')\log\log_{1/p} n}\cdot 2^n \leqslant s(f) \leqslant n^{(1+\delta_n'')\log\log_{1/p} n}\cdot 2^n,$$

и $\delta_n' \to 0$, $\delta_n'' \to 0$ при $n \to \infty$ и функции, на которые распространяется лемма 5 из первого параграфа.

В работе [5] показано, что случайная булева функция с вероятностью стремящейся к 1 при $n \to \infty$ обладает вышеуказанными свойствами.

Теорема 1. С вероятностью стремящейся к 1 при $n \to \infty$ длина д.н.ф. Квайна случайной булевой функции $f(x_1, \ldots, x_n)$ асимптотически равна длине ее сокращенной д.н.ф.

Доказательство. Так как размерность интервалов у рассмотриваемых функций не превосходит k, то у каждой функции число точек, принадлежащих ядровым интервалом не больше $c(f)\cdot 2^k$. Далее, через каждую точку приходит не более $\sum_{j=0}^{k} C_n^j$ граней, размерность которых не превосходит k. Чтобы оценить теперь число граней покрываемых ядровыми, заметим, что оно не больше числа граней, содержащих хотя бы одну точку принадлежащую ядровой грани, а это число в свою очередь не превосходит

$$c(f)\cdot 2^k \sum_{j=0}^{k} C_n^j \leqslant n^{(1-\gamma_n)\log\log_{1/p} n} 2^k(k+1)n^k(2(1-p))^n = o(s(f)).$$

В работе [2] показано, что для того, чтобы конъюнкция K из д.н.ф. сокращенной $D_C(f)$ не входила в д.н.ф. сумма тупиковых $D_{UT}(f)$, необходимо и достаточно, чтобы каждая вершина соответствующего интервала была регулярной относительно $(K, D_C(f))$.

Теорема 2. С вероятностью стремящейся к 1 при $n \to \infty$, длина д.н.ф. сумма тупиковых случайной булевой функции $f(x_1, \ldots, x_n)$ асимптотически равна длине сокращенной д.н.ф.

Доказательство. Подобно тому как при доказательстве предидущей теоремы, заключаем, что для функций, у которых размерность максимальных интервалов не превосходит k, число максимальных интервалов, содержащих хотя бы одну регулярную точку, небольше $r(f) \sum_{j=0}^{k} C_n^j$. Утверждение теоремы вытекает теперь из неравенства леммы 6 и утверждений преведенных в начале этого параграфа.

ЛИТЕРАТУРА

[1] Глаголев, В. В.: Некоторые оценки д.н.ф. функций алгебры логики, Проблемы кибернетики, вып. 19, Москва: Наука, 1967, 73—94.

[2] Журавлев, Ю. И.: Теоретико-множественные методы в алгебре логики, Проблемы кибернетики, вып. 8, Москва: Физматгиз, 1962, 5—44.

[3] Яблонский, С. В.: Функциональные построения в k-значной логике, Труды МИАН СССР 51, Москва, Изд-во АН СССР, 1958, 5—143.

[4] Томан, Э.: Геометрическое строение случайных булевых функций, Проблемы кибернетика, вып. 35, Москва, Наука, 1979, 111—132.

[5] Шковиера, М.: Оценки сложности дизъюнктивных нормальных форм случайных булевых функций, настоящий сборник.

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

Поступило: 8. 2. 1984

SÚHRN

EFEKTÍVNOSŤ NIEKTORÝCH LOKÁLNYCH ALGORITMOV ZJEDNODUŠENIA NÁHODNÝCH BOOLEOVSKÝCH FUNKCIÍ

Eduard Toman, Bratislava

V práci je určená efektívnosť dvoch lokálnych algoritmov zjednodušenia náhodných booleovských funkcií v triede disjunktívnych normálnych foriem.

SUMMARY

THE EFFECTIVITY OF SOME LOCAL ALGORITHMS FOR SIMPLIFYING THE RANDOM BOOLEAN FUNCTIONS

Eduard Toman, Bratislava

The effectivity of two local algorithms for simplifying the random boolean functions in the disjunctive normal forms class is specified.