Math-Net.Ru

Общероссийский математический портал

Ф. Ю. Воробьев, О нижней оценке порога 4-выполнимости, *Дискрет. матем.*, 2007, том 19, выпуск 2, 101–108

DOI: <https://doi.org/10.4213/dm25>

Использование Общероссийского математического портала Math-Net.Ru подразумевает, что вы прочитали и согласны с пользовательским соглашением

<http://www.mathnet.ru/rus/agreement>

Параметры загрузки:

IP: 54.89.56.158

26 апреля 2023 г., 17:01:41

О нижней оценке порога 4-выполнимости

© 2007 г. Ф. Ю. Воробьев

Пусть $F_k(n, m)$ — случайная k -конъюнктивная нормальная форма, полученная путем равновероятного и независимого выбора m скобок из числа всех k -буквенных скобок над множеством из n переменных. Доказывается, что если $F_4(n, rn)$ невыполнима с вероятностью, стремящейся к 1 при $n \rightarrow \infty$, то $r \geq 8,09$. Тем самым улучшена известная нижняя оценка $r \geq 7,91$.

Работа выполнена при поддержке Российского фонда фундаментальных исследований, проект 04-01-00359.

1. Введение

Пусть $x_1, \dots, x_n$ — множество из n булевых переменных. Назовем k -буквенной скобкой дизъюнкцию вида $(x_{i_1}^{\sigma_1} \vee x_{i_2}^{\sigma_2} \vee \dots \vee x_{i_k}^{\sigma_k})$. При этом одна переменная может встречаться в скобке несколько раз (такую скобку будем называть неправильной). Построим случайную k -конъюнктивную нормальную форму (k -КНФ) путем случайного равновероятного и независимого выбора m скобок из числа $(2n)^k$ всех скобок. При этом вероятность того, что некоторая скобка неправильная, меньше k^2/n . С высокой вероятностью ($P \rightarrow 1$) число неправильных скобок в формуле есть $o(n)$. Следовательно, если для некоторого r формула над n переменными с $m = rn$ скобками выполнима с высокой вероятностью, то это же верно при $m = rn - \varepsilon(n)$ для модели, $\varepsilon(n)$ неотрицательно и стремится к нулю при $n \rightarrow \infty$, и выбираются только правильные скобки. Пусть $S_k(n, r)$ — вероятность того, что $F_k(n, nr)$ выполнима. Пусть

$$r_k = \sup\{r: \lim_{n \rightarrow \infty} S_k(n, r) = 1\},$$
$$r_k^* = \inf\{r: \lim_{n \rightarrow \infty} S_k(n, r) = 0\},$$

то есть r_k — точная верхняя грань таких r , что вероятность выполнимости формулы все еще стремится к единице, r_k^* — точная нижняя грань таких r , что вероятность выполнимости формулы стремится к нулю. Ясно, что $r_k \leq r_k^*$. Существует предположение, что $r_k = r_k^*$, то есть при увеличении r в определенный момент происходит скачок предела вероятности выполнимости от единицы к нулю. Такое число r_k называется порогом выполнимости.

Существование порога не доказано, но известно следующее утверждение.

Теорема 1 ([2]). Для любого $k \geq 2$ существует такая последовательность $r_k(n)$, что

для любого $\varepsilon > 0$

$$\begin{aligned}\lim_{n \rightarrow \infty} S_k(n, (1 - \varepsilon)r_k(n)) &= 1, \\ \lim_{n \rightarrow \infty} S_k(n, (1 + \varepsilon)r_k(n)) &= 0.\end{aligned}$$

Следствие 1. Если $F_k(n, rn)$ выполнима при фиксированном значении $k \geq 2$ с вероятностью $P_n > C > 0$, то $r_k > r$.

Мы докажем, что $r_4 \geq 8,09$ и тем самым улучшим нижнюю оценку $r_4 \geq 7,91$, полученную в [1].

2. Метод вторых моментов

Мы будем применять метод вторых моментов в следующем виде.

Лемма 1. Для любой неотрицательной случайной величины X , для которой существует второй момент,

$$\mathbf{P}(X > 0) \geq \frac{(\mathbf{M}X)^2}{\mathbf{M}X^2}.$$

В работе [1] исследовалась применимость метода вторых моментов к различным случайным величинам, зависящим от случайных k -КНФ. В частности, если X — это число выполняющих наборов случайной формулы $F_k(n, rn)$, то можно получить нижнюю оценку вероятности выполнимости, применив лемму 1 к X . Действительно, по следствию 1, если $\mathbf{P}(X > 0) > 1/C$ для некоторой константы $C > 0$, то $r_k \geq r$.

Следовательно, если $\mathbf{M}X^2 = O(\mathbf{M}X)^2$, для некоторого r , то $r_k > r$. Но в [1] было продемонстрировано, что для любого положительного r существует константа $\beta = \beta(r) > 0$ такая, что $\mathbf{M}X^2 > (1 + \beta)^n (\mathbf{M}X)^2$.

Итак, требуется выбрать такую случайную величину X , что из неравенства $X > 0$ следует выполнимость формулы и к X применим метод вторых моментов. В [1] был найден целый класс случайных величин, удовлетворяющих этим свойствам.

3. Выбор случайной величины

Пусть W — множество действительных функций вида $w(\sigma, c)$, где $\sigma \in \{0, 1\}^n$, а c — некоторая скобка. Рассмотрим класс случайных величин

$$X = \sum_{\sigma} \prod_c w(\sigma, c),$$

где сумма берется по всем $\sigma \in \{0, 1\}^n$, а произведение — по всем скобкам случайной формулы, и $w(\sigma, c) \in W$. Прежде всего, выясним, какие условия следует наложить на $w(\sigma, c)$ для применимости метода вторых моментов, а также для упрощения вычислений. Так как переменные, входящие в формулу, выбираются равновероятно, естественно рассматривать функции вида $w(\sigma, c) = w(v) = w(|v|)$, где $v = (v_1, \dots, v_k)$ и $v_i = 1$, если i -я переменная скобки c обращается в 1 на σ , и $v_i = -1$ в противном случае, а $|v|$ равняется числу 1 в v . Таким образом, выбор функции w сводится к выбору $k + 1$ значения $w(0) = w_0, w(1) = w_1, \dots, w(k) = w_k$. Это существенно упрощает вычисления. Метод

вторых моментов применим, если из невыполнимости формулы следует равенство $X = 0$. Это возможно только при $w_0 = 0$. Нетрудно видеть, что

$$\begin{aligned}\mathbf{M}X &= 2^n (\mathbf{M}w(\sigma, c))^m, \\ \mathbf{M}X^2 &= \sum_{\sigma, \tau} (\mathbf{M}w(\sigma, c)w(\tau, c))^m.\end{aligned}$$

Пусть $A = \{-1, 1\}^k$. Тогда

$$\mathbf{M}w(\sigma, c) = \sum_{v \in A} w(v)2^{-k}.$$

Для пары наборов σ, τ , совпадающих по $z = \alpha n$ элементам, справедливо равенство

$$\mathbf{M}w(\sigma, c)w(\tau, c) = f_w(\alpha) = \sum_{u, v \in A} w(u)w(v)2^{-k} \prod_{i=1}^k (\alpha^{1_{u_i=v_i}} (1-\alpha)^{1_{u_i \neq v_i}}), \quad (1)$$

где 1_A — индикатор события A . Заметим, что $\mathbf{M}(w(\sigma, c))^2 = f_w(1/2)$. Подставив (1) в уравнение для $\mathbf{M}X^2$, получим, что

$$\mathbf{M}X^2 = 2^n \sum_{z=0}^n \binom{n}{z} f_w^m(z/n). \quad (2)$$

Нам понадобится следующее утверждение из [3].

Лемма 2. Пусть φ — действительная, положительная, дважды дифференцируемая функция на $[0, 1]$ и

$$S_n = \sum_{z=0}^n \binom{n}{z} \varphi^n(z/n).$$

Полагая $0^0 = 1$, определим g на $[0, 1]$ как

$$g(\alpha) = \frac{\varphi(\alpha)}{\alpha^\alpha (1-\alpha)^{1-\alpha}}.$$

Если существует $\alpha_{\max} \in (0, 1)$ такое, что $g(\alpha_{\max}) = g_{\max} > g(\alpha)$ для всех $\alpha \neq \alpha_{\max}$, и $g''(\alpha_{\max}) < 0$, то существуют константы $B, C > 0$ такие, что для всех достаточно больших n

$$Bg_{\max}^n \leq S_n \leq Cg_{\max}^n.$$

Следовательно, если функция

$$g_r(\alpha) = \frac{f_w(\alpha)^r}{\alpha^\alpha (1-\alpha)^{1-\alpha}}$$

имеет единственный глобальный максимум в $\alpha = 1/2$, а $g_r''(1/2) < 0$, то из (2) следует, что

$$\mathbf{M}X^2 = O(2^n (\max_{0 \leq \alpha \leq 1} g_r(\alpha))^n) = O((4f_w(1/2)^r)^n).$$

Но $(4f_w(1/2)^r)^n = (4\mathbf{M}(w(\sigma, c))^{2r})^n = (2^n(\mathbf{M}w(\sigma, c))^m)^2 = \mathbf{M}X^2$. Следовательно, $\mathbf{M}X^2/(\mathbf{M}X)^2 = O(1)$, и применяя метод вторых моментов, по следствию 1 получим, что $r_k > r$.

Необходимым условием достижения глобального максимума $g_r(\alpha)$ в $1/2$ является равенство $g'_r(1/2) = 0$. Это равносильно тому, что $f'_w(1/2) = 0$. Найдем производную $f_w(\alpha)$. Введем вспомогательную функцию

$$\varphi_{u,v}(\alpha) = \frac{1}{2^k} \prod_{i=1}^k (\alpha^{1_{u_i=v_i}} (1-\alpha)^{1_{u_i \neq v_i}}).$$

Тогда из (1) получим равенства

$$\begin{aligned} f'_w(\alpha) &= \sum_{u,v \in A} w(u)w(v)\varphi_{u,v}(\alpha)(\ln \varphi_{u,v}(\alpha))' \\ &= \sum_{u,v \in A} w(u)w(v)\varphi_{u,v}(\alpha) \sum_{i=1}^k \left(\frac{1_{u_i=v_i}}{\alpha} - \frac{1_{u_i \neq v_i}}{1-\alpha} \right). \end{aligned}$$

Будем обозначать скалярное произведение векторов u и v как $u \cdot v$. Тогда

$$f'_w(1/2) = 2^{1-2k} \sum_{u,v \in A} w(u)w(v)u \cdot v = 2^{1-2k} \left(\sum_{u \in A} w(u)u \right) \cdot \left(\sum_{v \in A} w(v)v \right).$$

Следовательно, для любой функции w условия $f'_w(1/2) = 0$ и $\sum_{v \in A} w(v)v = 0$ равносильны. Добавим условие нормировки $\sum_v w(v) = 1$. Если для функции $w^*(v)$ это условие не выполняется, то разделим ее на $\sum_v w^*(v)$.

Напомним, что выбор $w(v)$ сводится к выбору $k+1$ значения $w_0, w_1, \dots, w_k$. Кроме того, выполняются условия

$$w_0 = 0, \quad \sum_{v \in A} w(v)v = 0, \quad \sum_{v \in A} w(v) = 1.$$

Это позволяет свести выбор функции $w(v)$ к выбору $k-2$ параметров. В случае $k=4$ нам остается выбрать всего два параметра, что существенно упрощает вычисления.

4. Улучшенный метод

В работе [1] среди всех членов класса случайных величин X была выбрана одна случайная величина, которая, по словам авторов, позволяла получить наилучшие для данного класса нижние оценки порога выполнимости, хотя строго это не доказывалось. Оказалось, что это неверно, и в этом классе существуют другие случайные величины, позволяющие получить более высокие нижние оценки.

Для того чтобы получить более точную нижнюю оценку порога 4-выполнимости, можно следующим образом обобщить метод из [1].

Пусть $\sigma \in \{0, 1\}^n$, и пусть $H(\sigma, F)$ обозначает число букв формулы F , обращающихся в единицу на σ , минус число букв, обращающихся в ноль. Пусть

$$S^+ = \{\sigma \in \{0, 1\}^n : H(\sigma, F) \geq 0\}$$

— множество наборов, на которых не менее половины букв формулы F обращаются в единицу.

В [1] было показано, что основной вклад в $\mathbf{M}X^2$ дают наборы, на которых в единицу обращается меньше половины букв формулы. Поэтому имеет смысл рассмотреть случайную величину

$$X_+ = \sum_{\sigma \in S^+} \prod_c w(\sigma, c), \quad \mathbf{M}X_+ = \sum_{\sigma \in S^+} \mathbf{M} \prod_c w(\sigma, c).$$

При этом математическое ожидание произведения нельзя заменить на произведение математических ожиданий. Аналогичные трудности возникают при вычислении $\mathbf{M}X_+^2$. Тем не менее, оказывается, что к X_+ можно применить метод вторых моментов.

Лемма 3. Если $n \rightarrow \infty$, то $\mathbf{M}X_+/\mathbf{M}X \rightarrow 1/2$.

Доказательство. Заметим, что для любого σ

$$\mathbf{M}X_+ = 2^n \mathbf{M} \left(1_{\sigma \in S^+(F)} \prod_c w(\sigma, c) \right), \quad \mathbf{M}X = 2^n \mathbf{M} \left(\prod_c w(\sigma, c) \right),$$

и утверждение леммы эквивалентно утверждению, что при $n \rightarrow \infty$

$$\frac{\mathbf{M}(1_{\sigma \in S^+(F)} \prod_c w(\sigma, c))}{\mathbf{M}(\prod_c w(\sigma, c))} \rightarrow \frac{1}{2}.$$

Здесь σ меняется с ростом n , но числитель и знаменатель зависят только от длины набора.

Рассмотрим вспомогательное распределение $\mathbf{P}_1$ на множестве k -буквенных скобок,

$$\mathbf{P}_1(c) = \frac{\mathbf{P}(c)w(\sigma, c)}{N_1},$$

где $N_1 = \mathbf{M}(w(\sigma, c))$,

$$\mathbf{P}_1(F) = \frac{\mathbf{P}(F) \prod_c w(\sigma, c)}{N_1^m}.$$

Докажем, что $\mathbf{M}_1(H(\sigma, c)) = 0$. Действительно,

$$\begin{aligned} \mathbf{M}_1(H(\sigma, c)) &= \sum_c \mathbf{P}_1(c) H(\sigma, c) = \sum_{v \neq (-1, \dots, -1)} \mathbf{P}_1(v) (2|v| - k) \\ &= \sum_{v \neq (-1, \dots, -1)} \frac{\mathbf{P}(v)w(v)}{N_1} (2|v| - k) = \frac{\mathbf{P}(v)}{N_1} \sum_{v \neq (-1, \dots, -1)} w(v) (2|v| - k) = 0, \\ H(\sigma, F) &= \sum_c H(\sigma, c). \end{aligned}$$

Заметим, что $\sum_c H(\sigma, c)$ — сумма независимых одинаково распределенных случайных величин с конечной дисперсией. По центральной предельной теореме,

$$\mathbf{P}_1 \left(\frac{H(\sigma, F) - m\mathbf{M}_1(H(\sigma, c))}{\sqrt{mD_1(H(\sigma, c))}} \geq 0 \right) \rightarrow \frac{1}{\sqrt{2\pi}} \int_0^\infty e^{-t^2/2} dt,$$

то есть

$$\mathbf{P}_1(H(\sigma, F) \geq 0) \rightarrow \frac{1}{2}.$$

Заметим, что

$$\begin{aligned} \mathbf{M}\left(1_{\sigma \in S^+(F)} \prod_c w(\sigma, c)\right) &= \sum_F \mathbf{P}(F) \prod_c w(\sigma, c) 1_{\sigma \in S^+(F)} = N_1^m \sum_F \mathbf{P}_1(F) 1_{\sigma \in S^+(F)} \\ &= N_1^m \mathbf{P}_1(\sigma \in S^+(F)) = N_1^m \mathbf{P}_1(H(\sigma, F) \geq 0), \end{aligned}$$

и

$$\mathbf{M}\left(\prod_c w(\sigma, c)\right) = \sum_F \mathbf{P}(F) \prod_c w(\sigma, c) = N_1^m \sum_F \mathbf{P}_1(F) = N_1^m.$$

Отсюда следует, что

$$\frac{\mathbf{M}(1_{\sigma \in S^+(F)} \prod_c w(\sigma, c))}{\mathbf{M}(\prod_c w(\sigma, c))} = \mathbf{P}_1(H(\sigma, F) \geq 0) \rightarrow \frac{1}{2}.$$

Для пары наборов σ, τ , совпадающих по $z = \alpha n$ координатам, обозначим $\mathbf{M}(1_{\sigma, \tau \in S^+(F)} \prod_c w(\sigma, c) w(\tau, c))$ через $f_w^+(\alpha)$.
Ясно, что

$$\begin{aligned} X_+^2 &= \left(\sum_{\sigma \in S^+} \prod_c w(\sigma, c)\right) \left(\sum_{\tau \in S^+} \prod_c w(\tau, c)\right) \\ &= \left(\sum_{\sigma} 1_{\sigma \in S^+(F)} \prod_c w(\sigma, c)\right) \left(\sum_{\tau} 1_{\tau \in S^+(F)} \prod_c w(\tau, c)\right) \\ &= \sum_{\sigma, \tau} 1_{\sigma, \tau \in S^+(F)} \prod_c w(\sigma, c) w(\tau, c), \end{aligned}$$

и

$$\mathbf{M}(X_+^2) = 2^n \mathbf{M}\left(\sum_{\tau} 1_{\sigma, \tau \in S^+(F)} \prod_c w(\sigma, c) w(\tau, c)\right) = 2^n \sum_{z=0}^n \binom{n}{z} f_w^+(\alpha). \quad (3)$$

Для любого $\beta \geq 1$ из включений $\sigma, \tau \in S^+(F)$ следует, что $\prod_c \beta^{H(\sigma, c) + H(\tau, c)} \geq 1$, а значит,

$$\begin{aligned} f_w^+(\alpha) &= \mathbf{M}\left(1_{\sigma, \tau \in S^+(F)} \prod_c w(\sigma, c) w(\tau, c)\right) \\ &\leq \mathbf{M}\left(1_{\sigma, \tau \in S^+(F)} \prod_c \beta^{H(\sigma, c) + H(\tau, c)} \prod_c w(\sigma, c) w(\tau, c)\right) \\ &= \mathbf{M}\left(1_{\sigma, \tau \in S^+(F)} \prod_c w(\sigma, c) \beta^{H(\sigma, c)} w(\tau, c) \beta^{H(\tau, c)}\right) \\ &\leq \mathbf{M}\left(\prod_c w(\sigma, c) \beta^{H(\sigma, c)} w(\tau, c) \beta^{H(\tau, c)}\right) = (\mathbf{M}(w(\sigma, c) \beta^{H(\sigma, c)} w(\tau, c) \beta^{H(\tau, c)}))^m. \end{aligned}$$

Нетрудно видеть, что

$$\begin{aligned} \mathbf{M}(w(\sigma, c)\beta^{H(\sigma, c)}w(\tau, c)\beta^{H(\tau, c)}) \\ = \sum_{u, v \in A} w(u)\beta^{2|u|-k}w(v)\beta^{2|v|-k}2^{-k} \prod_{i=1}^k (\alpha^{1_{u_i=v_i}}(1-\alpha)^{1_{u_i \neq v_i}}) = f_w(\alpha, \beta). \end{aligned}$$

Итак,

$$f_w^+(\alpha) \leq (\inf_{\beta \geq 1} f_w(\alpha, \beta))^m,$$

из (3) получаем, что

$$\mathbf{M}(X_+^2) \leq 2^n \sum_{z=0}^n \binom{n}{z} (\inf_{\beta \geq 1} f_w(\alpha, \beta)^r)^n. \quad (4)$$

Введем обозначение

$$g_r(\alpha, \beta) = \frac{f_w(\alpha, \beta)^r}{\alpha^\alpha(1-\alpha)^{1-\alpha}}.$$

Заметим, что $f_w(\alpha, 1) = f_w(\alpha)$, и $g_r(\alpha, 1) = g_r(\alpha)$. Из леммы 3 следует, что существует константа C_1 такая, что

$$C_1 \mathbf{M}(X_+)^2 > \mathbf{M}(X)^2 = 2^n g_r(1/2, 1)^n.$$

Применим лемму 2 к (4). Для этого определим вспомогательную кусочно-постоянную функцию $b(\alpha) \geq 1$ такую, что для некоторого значения r выполняется неравенство $g_r(1/2, 1) > g_r(\alpha, b(\alpha))$ для всех $\alpha \neq 1/2$. Тогда

$$\sum_{z=0}^n \binom{n}{z} (\inf_{\beta \geq 1} f_w(\alpha, \beta)^r)^n \leq \sum_{z=0}^n \binom{n}{z} (f_w(\alpha, b(\alpha)))^m.$$

Пусть у $b(\alpha)$ всего T промежутков постоянства на $[0, 1]$. Рассмотрим функции $f_1(\alpha), \dots, f_T(\alpha)$, полученные следующим образом: $f_i(\alpha) = f_w(\alpha, b(\alpha))^r$ на i -м промежутке постоянства, а вне этого промежутка продолжена так, чтобы выполнялись условия леммы 2 (действительная, положительная, дважды дифференцируемая функция такая, что $f_i(1/2) = f_w(1/2, 1)^r$ и

$$g_i(\alpha) = \frac{f_i(\alpha)}{\alpha^\alpha(1-\alpha)^{1-\alpha}}$$

имеет единственный глобальный максимум в точке $\alpha = 1/2$ и $g_i''(1/2) < 0$). Применяя лемму 2 к $f_i(\alpha)$, получим, что

$$\sum_{z=0}^n \binom{n}{z} f_i^n(\alpha) \leq C_i g_{i \max}^n = C_i f_w^m(1/2, 1).$$

Тогда

$$\sum_{z=0}^n \binom{n}{z} f_w(z/n, b^{rn}(z/n)) \leq \sum_{i=1}^T \sum_{z=0}^n \binom{n}{z} f_i^n(z/n) \leq C_{\max} T g_r^n(1/2, 1),$$

где $C_{\max} = \max(C_1, \dots, C_T)$. Таким образом,

$$\mathbf{M}(X_+^2) \leq 2^n \sum_{z=0}^n \binom{n}{z} f_w^m(\alpha, b(\alpha)) \leq C_1 2^n g_r^n(1/2, 1) \leq C_2 (\mathbf{M}X_+)^2,$$

где C_1 и C_2 — константы. Из леммы 1 следует, что $r_k \geq r$.

5. Применение метода

Применим метод для случая $k = 4$. Для этого надо продемонстрировать значения $w(0), \dots, w(4)$, r и кусочно-постоянную функцию $b(\alpha) \geq 1$ такие, что для всех $\alpha \neq 1/2$ выполняется неравенство $g_r(1/2, 1) > g_r(\alpha, b(\alpha))$.

Приведем конкретные значения

$$\begin{aligned} w(0) = 0, \quad w(1) = 0,08265, \quad w(2) = 0,06485, \quad w(3) = 0,0575, \quad w(4) = 0,0503, \\ r = 8,09, \quad b(\alpha) = 1, \quad \alpha \in [0, 0,7], \quad b(\alpha) = 1,0285, \quad \alpha \in (0,7, 1]. \end{aligned}$$

Список литературы

1. Achlioptas D. Peres Y., The threshold for random k -SAT is $2^k \ln 2 - O(k)$. *STOC* (2003) 223–231.
2. Friedgut E., Necessary and sufficient conditions for sharp thresholds of graph properties, and the k -SAT problem. *J. Amer. Math. Soc.* (1999) **12**, 1017–1054.
3. de Bruijn N. G., *Asymptotic methods in analysis*. Dover, New York, 1981.

Статья поступила 15.06.2005.