Санкт–Петербургский государственный университет
Факультет математики и компьютерных наук

Эмдин Григорий Дмитриевич

Выпускная квалификационная работа

КНФ-кодировки функции четности

Уровень образования: бакалавриат
Направление 01.03.02 «Прикладная математика и информатика»
Основная образовательная программа СВ.5005.2018 «Прикладная математика, фундаментальная информатика и программирование»
Профиль «Современное программирование»

Научный руководитель:
профессор СПбГУ, д.ф.-м.н., А. С. Куликов

Рецензент:
доцент Джорджтаунского университета, PhD, А. Г. Головнев

Санкт-Петербург
2022 г.

Содержание

Введение

Многие годы ученые в области компьютерных наук придумывают алгоритмы для ускорения решения различных задач. В теории сложности существует иерархия классов, основными представителями которой являются классы P и NP. Класс P — класс языков (задач), разрешимых на детерминированной машине Тьюринга за полиномиальное время. Класс NP — класс языков (задач), ответ на который можно проверить за полиномиальное время. Вопрос о равенстве классов P и NP — это одна из центральных открытых проблем теории алгоритмов [2]. Каноническим представителем класса NP является задача выполнимости булевой формулы в конъюктивно-нормальной форме (КНФ). Несмотря на теоретическую сложность этой задачи, современные солверы работают очень быстро. К задаче выполнимости на практике сводятся огромное количество других задач. При этом сведении размер задачи может экспоненциально увеличиться. В связи с этим, возникает вопрос минимизации количества клозов при кодировки функций в виде КНФ.

Постановка задачи

Основной целью работы является изучение соотношений между количеством дополнительных переменных, числом клозов и максимальной шириной клозов при КНФ-кодировки функции четности. Должна быть доказана нижняя оценка на число клозов при фиксированном количестве дополнительных переменных, нижняя оценка на число клозов при произвольном количестве дополнительных переменных и нижняя оценка на ширину клозов при фиксированном количестве дополнительных переменных.

1. Обзорный раздел

1.1. Мотивация

На практике популярным подходом для решения трудных комбинаторных задач является кодирование этой задачи в КНФ и запуск солвера для задачи выполнимости (SAT-солвер). Есть две основные причины, почему такой подход хорошо справляется со многими сложными задачами: современные SAT-солверы чрезвычайно эффективны и многие комбинаторные задачи естественно записываются в КНФ. В тоже время, КНФ-кодировка не уникальна, и, обычно, ее выбирают эмпирически. Кроме того, не существует такого понятия, как наилучшая кодировка, так как это также зависит от выбранного SAT-солвера. Прествич [11] делает обзор различных способов перевода задач в КНФ и обсуждает их желательные свойства, как с теоретической точки зрения, так и с практической.

Уже для такой простой функции, как четность $x_1 \oplus x_2 \oplus \cdots \oplus x_n$, в действительности, не ясно, как кодировать ее в КНФ (чтобы SAT-солверу было проще работать). Функция четности часто возникает в криптографии (хэш - функция, потоковые шифры, и т.д.). Известно, что минимальное число клозов в КНФ, вычисляющей функцию четности — это 2^{n-1}. С ростом n это число становится неприменимо на практике. Стандартный способ уменьшить размер кодировки — это использовать дополнительные переменные. Давайте введем s дополнительны переменных $y_1, \ldots, y_s$, и разобьем множество входных переменных на $s+1$ блок размера не больше $\lceil n/(s+1) \rceil$: $\{x_1, x_2, \ldots, x_n\} = X_1 \sqcup X_2 \sqcup \cdots \sqcup X_{s+1}$, тогда функцию четности можно закодировать следующим способом:

$$\left(y_1 = \bigoplus_{x \in X_1} x\right), \left(y_2 = y_1 \oplus \bigoplus_{x \in X_2} x\right), \ldots, \left(y_s = y_{s-1} \oplus \bigoplus_{x \in X_s} x\right), \left(1 = y_s \oplus \bigoplus_{x \in X_{s+1}} x\right). \quad (1)$$

Значение для параметра s обычно определяется экспериментально. Например, Престич [11] пишет, что значение $s = 10$ дает наилучшие результаты при решении задачи "The Minimal Disagreement Parity Problem" [3], используя SAT-солвер, основанный на локальном поиске.

Простая конструкция, приведенная выше, влечет несколько верхних оценок на число клозов m, количество дополнительных переменных s и ширину клозов k:

Ограниченное количество дополнительных переменных: Используя s дополнительных переменных можно закодировать функцию четности либо как КНФ с не более чем

$$m \leq (s+1)2^{\lceil n/(s+1)\rceil+2-1} \leq 4(s+1)2^{n/(s+1)}$$

клозами, либо как k-КНФ, где

$$k = 2 + \lceil n/(s+1)\rceil \leq 3 + n/(s+1)\,.$$

Неограниченное количество дополнительных переменных: можно закодировать функцию четности в виде КНФ, использую не более чем $4n$ клозов (для этого надо взять $s = n-1$ дополнительных переменных; тогда каждую из n функций в (1) можно записать в КНФ, используя не больше 4 клозов).

1.2. Результаты

В этой работе показывается, что верхние оценки, упомянутые выше, являются практически оптимальными.

Теорема 1. *Пусть F — КНФ, кодирующая функцию PAR_n с помощью m клозов, s дополнительных переменных, и максимальной длиной клозов равной k.*

1. *Параметры s и m не могут быть слишком маленькие одновременно:*

$$m \geq \Omega\left(\frac{s+1}{n} \cdot 2^{n/(s+1)}\right)\,. \tag{2}$$

2. *Параметры s и k не могут быть слишком маленькие одновременно:*

$$k \geq n/(s+1)\,. \tag{3}$$

3. *Параметр m не может быть слишком маленький:*

$$m \geq 3n - 9\,. \tag{4}$$

1.3. Методы

Нижняя оценка $m \geq \Omega((s+1)2^{n/(s+1)}/n)$ получена из Satisfiability Coding Lemma авторов Патури, Пудлак и Зейн [10]. Эта лемма позволяет доказать $2^{\sqrt{n}}$ нижнюю оценку на размер схемы глубины 3, вычисляющую функцию четности. Отметим, что нижняя оценка $m \geq \Omega((s+1)2^{n/(s+1)}/n)$ влечет нижнюю $2^{\Omega(\sqrt{n})}$ практически сразу, при этом в обратную сторону такое следствие не ясно.

Для доказательства нижней оценки $m \geq 3n - 9$, в этой работе была тщательно проанализирована структура КНФ кодировки.

1.4. Ранние работы

Голдсмит, Леви и Манденк [4] показали много результатов для различных вычислительных моделей с дополнительными переменными. Обзор известных подходов для КНФ кодировок представлены у Прествича [11]. Два недавних результата, близких к результатам этой работы следующие. Моридзуми [9] доказал, что дополнительны входные переменные не помогают в модели булевых схем над базисом U_2 (множество всех бинарных функций, кроме эквивалентности и исключающего или) для вычисления функции четности: с и без дополнительных переменных минимальный размер схемы, вычисляющей функцию четности, равен $3(n-1)$. Киосера, Савицкий, Ворель [7] продемонстрировали практически совпадающие нижнюю и верхнюю границу на размер КНФ кодировки булевой функции at-most-one ($[x_1 + \cdots + x_n \leq 1]$). Синз [12] получил линейную нижнюю оценку на КНФ кодировку булевой функции at-most-k.

2. Основные понятие

2.1. Вычисление булевой функции с помощью КНФ

Рассмотрим булеву функцию $f(x_1, \ldots, x_n)\colon \{0,1\}^n \to \{0,1\}$. Будем говорить, что КНФ $F(x_1, \ldots, x_n)$ *вычисляет* f, если $f \equiv F$, то есть, для всех $x_1, \ldots, x_n \in \{0,1\}$, $f(x_1, \ldots, x_n) = F(x_1, \ldots, x_n)$. Будем представлять КНФ как множество клозов, и под размером КНФ будем подразумевать количество клозов. Известно, что для любой функции f существует КНФ, вычисляющая ее. Один из способов построить такую КНФ следующий: для каждого входа $x \in \{0,1\}^n$, такого что $f(x) = 0$ добавим в КНФ клоз длины n, который опровергает x.

Этот метод не гарантирует, что полученная КНФ будет иметь минимальное число клозов: было бы слишком хорошо, будь это иначе, ведь задача поиска КНФ минимального размера для данной булевой функции f (заданной с помощью таблицы истинности) является NP-трудной, как доказал Масек [8] (смотри также [1] и ссылки там). Например, для функции $f(x_1, x_2) = x_1$ этот метод создает КНФ $(\overline{x_1} \vee x_2) \wedge (\overline{x_1} \vee \overline{x_2})$, хотя функция x_1 уже представлена в виде КНФ.

2.2. Функция четности

Известно, что для многих функций минимальный размер КНФ, вычисляющей их, экспоненциальный. Каноническим примером такой функции является четность: $\mathrm{PAR}_n(x_1, \ldots, x_n) = x_1 \oplus \cdots \oplus x_n$. Основное свойство этой функции, из - за которого она не может быть посчитана короткой КНФ, — это высокая *чувствительность*: если в любом входе поменять значение любого бита на противоположенный, то значение всей функции изменится на противоположенное.

Лемма 1. *Минимальный размер КНФ, вычисляющей* PAR_n *имеет размер* 2^{n-1}

Доказательство. Верхняя границы следует из метода, описанного выше и того факта, что $|\mathrm{PAR}_n^{-1}(0)| = 2^{n-1}$.

Нижняя оценка основана на том, что любой клоз в КНФ f, вычисляющей PAR_n должен содержать все переменные $x_1, \ldots, x_n$ или их отрицания. Предположим, что это не так. Пусть есть клоз $C \in F$, который не зависит от x_i (то есть $x_i \notin C$ и $\overline{x_i} \notin C$). Рассмотрим вход $x \in \{0,1\}^n$, который не удовлетворяет C, тогда $F(x) = \mathrm{PAR}_n(x) = 0$. Но если в этом входе поменять значение x_i на противоположенное, то клоз C будет все еще не удовлетворен. Противоречие с высокой чувствительностью функции четности. Таким образом, все клозы F имеют ровно n переменных (или их отрицаний), а значит каждый клоз может опровергнуть ровно одно значение $x \in \{0,1\}^n$. Но опровергающих значений у PAR_n 2^{n-1}, значит должно быть хотя бы 2^{n-1} клозов.

□

2.3. Кодировка булевой функции с помощью КНФ

Будем говорить, что КНФ F *кодирует* булеву функцию $f(x_1, \ldots, x_n)$, если выполняются следующие два условия:

1. В дополнение ко входным битам $x_1, \ldots, x_n$, F также зависит от s битов $y_1, \ldots, y_s$, называемые *дополнительным* или *недетерминированным входом*.

2. Для любых $x \in \{0,1\}^n$, $f(x) = 1$ если и только если существует $y \in \{0,1\}^s$ такой, что $F(x,y) = 1$. Другими словами, для всех $x \in \{0,1\}^n$,

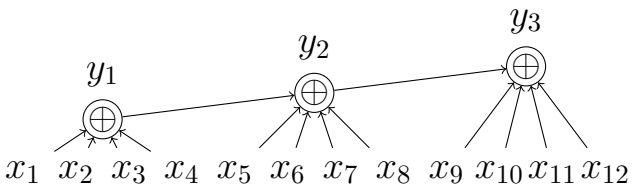
$$f(x) = \bigvee_{y \in \{0,1\}^s} F(x,y)\,. \tag{5}$$

Такое представление булевой функции широко используется на практике при переводе задач на язык КНФ. Например, так выглядит одна из КНФ-кодировок функции PAR_4:

$$(x_1 \vee x_2 \vee \overline{y_1}) \wedge (x_1 \vee \overline{x_2} \vee y_1) \wedge (\overline{x_1} \vee x_2 \vee y_1) \wedge (\overline{x_1} \vee \overline{x_2} \vee \overline{y_1}) \wedge (y_1 \vee x_3 \vee \overline{y_2}) \wedge$$
$$(y_1 \vee \overline{x_3} \vee y_2) \wedge (\overline{y_1} \vee x_3 \vee y_2) \wedge (\overline{y_1} \vee \overline{x_3} \vee \overline{y_2}) \wedge (\overline{x_4} \vee y_2) \wedge (x_4 \vee \overline{y_2})\,. \tag{6}$$

2.4. Булева схема и преобразование Цейтина

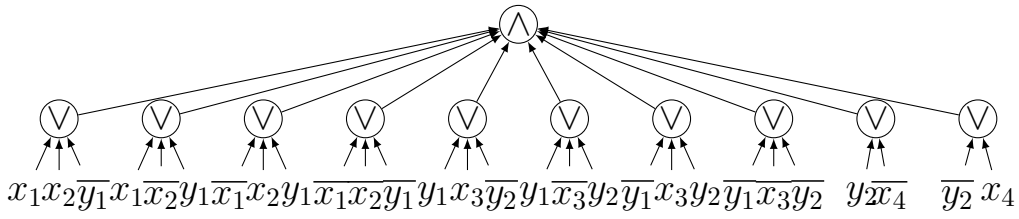
Одним из естественных способом получения КНФ-кодировки булевой функции f является преобразование Цейтина [13]. А именно, надо взять булеву схему, вычисляющую f, и применим к ней преобразование Цейтина. Наглядно продемонстрируем это на игрушечном примере. Рассмотрим схему, вычисляющую функцию PAR_{12}, которая приведена ниже. Она имеет 12 входов, 3 гейта (один из которых выходной) и ее глубина равна трем.



$$y_1 = x_1 \oplus x_2 \oplus x_3 \oplus x_4$$
$$y_2 = y_1 \oplus x_5 \oplus x_6 \oplus x_7 \oplus x_8$$
$$y_3 = y_2 \oplus x_9 \oplus x_{10} \oplus x_{11} \oplus x_{12}$$

Справа от схемы приведены функции, вычисляемые каждым гейтом. Преобразуем каждое равенство в КНФ, соберем все КНФ в одну и добавим в нее клоз (y_3). Полученная КНФ кодирует функцию, которую вычисляет схема. Отметим, что КНФ (1) получена таким же способом (после распространения значения выходного гейта).

КНФ может быть представлена в виде схемы глубины 2, в которой выходной гейт будет вычислять AND, все остальные гейты — OR, и входы — это переменные или их отрицания. Например, следующая схема соответствует КНФ (6). Такие схемы глубины 2 также обозначаются, как $\mathrm{AND} \circ \mathrm{OR}$ схемы.



2.5. Схемы глубины 3

Естественным обобщением конъюнктивной нормальной формы являются схемы глубины 3: Σ_3-*схема* — это OR нескольких КНФ. В схеме клозы

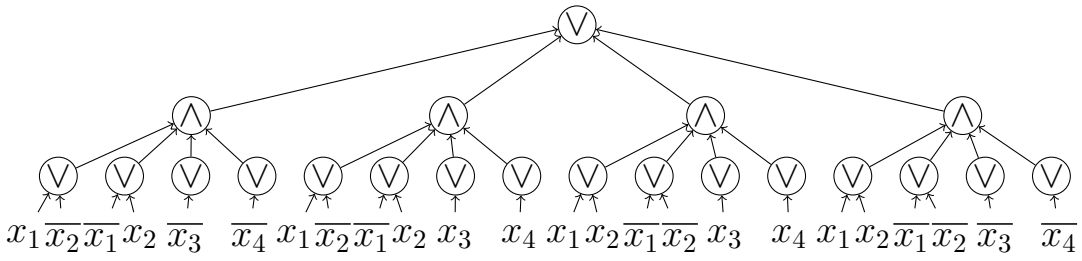
могут быть общие у разных КНФ. Σ_3-*формула* — это Σ_3-схема, КНФы которой не имеют общих клозов (другими словами, это схема, у которой выходная степень каждого гейта не больше 1).

С одной стороны, это вычислительная модель все еще достаточно простая. С другой стороны, доказать нижние оценки в такой модель оказывается трудно: получить нижнюю оценку $2^{\omega(n)}$ на размер явной функции (скажем, из NP или E^{NP}) это серьезная задача. Получение нижней оценки $2^{\omega(n/\log\log n)}$ разрешит еще один открытый вопрос за счет уменьшения глубины Вейлинта [14]: доказательство суперлинейной нижней оценки на размер схем логарифмической глубины. Подробнее об известные результатах со схемами глубины 3 есть в книге Юкны [6, Chapter 11]. Для функции четности лучшая известная нижняя оценка на схему глубины 3 — это $\Omega(2^{\sqrt{n}})$ [10], на формулу глубины 3 — это $\Omega(2^{2\sqrt{n}})$ [5]. Обе нижние оценки оптимальны с точностью до полиномиального фактора.

Равенство (5) показывает тесную связь между КНФ-кодировками и схемами глубины 3 типа $\mathrm{OR} \circ \mathrm{AND} \circ \mathrm{OR}$. В самом деле, пусть $F(x_1, \ldots, x_n, y_1, \ldots, y_s) = \{C_1, \ldots, C_m\}$ — это КНФ-кодировка булевой функции $f\colon \{0,1\}^n \to \{0,1\}$. Тогда $f(x) = \vee_{y\in\{0,1\}^s} F(x,y)$. Перебрав все возможные 2^n означиваний для y-ов, можно получить Σ_3 формулу, вычисляющую f:

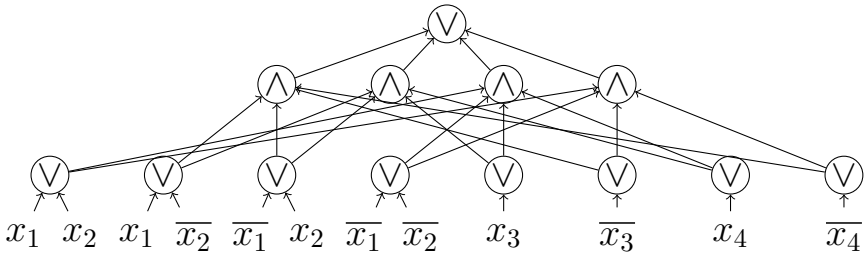
$$f(x) = \bigvee_{j\in[2^s]} F_j(x)\,,$$

где каждая F_j является КНФ. Будем называть это *расширением* F. Например, расширение КНФ (6) выглядит следующим образом. Это OR четырех КНФ.



Расширение — это формула, это OR нескольких КНФ, каждый гейт имеет выходную степень не больше 1. Аналогичном способом можно получить *расширение схемы*: в этом случае гейтам разрешено иметь выходную степень

больше 1, то есть КНФы могут иметь общие клозы. Например, это расширение схемы все того же примера (6).



Ниже будет показано, что КНФ-кодировка и схема глубины 3 могут быть легко преобразованы друг в друга. Для удобства, определим размер схемы как число гейтов *исключая* выходной. В таком случае, размер КНФ формулы равен числу клозов (КНФ — это схема глубины 2). Под $\Sigma_3(t, r)$-схемой будем обозначать Σ_3-схему имеющую не более t AND-ов на втором слое и не более r OR-ов на третьем слое (то есть ее размер не больше $t + r$).

Лемма 2. *Пусть $F(x_1, \ldots, x_n, y_1, \ldots, y_s)$ — это КНФ-кодировка размера m функции $f\colon \{0,1\}^n \to \{0,1\}$. Тогда, f может быть посчитана с помощью $\Sigma_3(2^s, m \cdot 2^s)$-формулы и с помощью $\Sigma_3(2^s, m)$-схемы.*

Доказательство. Пусть $F = \{C_1, \ldots, C_m\}$. Чтобы расширить F как $\bigvee_{j\in[2^s]} F_j$, мы переберем все 2^s означивание дополнительных переменных $y_1, \ldots, y_s$. В каждом таком означивании каждый клоз C_i либо становится выполненным, либо превращается в клоз $C'_i \subseteq C_i$ (C'_i — это клоз C_i, в котором удалили все дополнительные переменные). Таким образом, для каждого $j \in [2^s]$, $F_j \subseteq \{C'_1, \ldots, C'_m\}$. Соответствующая Σ_3-формула содержит не более $2^s + m2^s$ гейтов: есть 2^s гейтов для F_j, каждая F_j содержит не более, чем m клозов. Соответствующая Σ_3-схема содержит не более, чем $2^s + m$ гейтов: есть 2^s гейтов для F_j и m гейтов для $C'_1, \ldots, C'_m$ (каждая F_j выбирает какие из этих m клозов содержать). □

Стоит отметить, что нижняя граница на схемы глубины 3, полученная с помощью такого преобразования не может быть существенно улучшена. Действительно, взяв КНФ-кодировку функции PAR_n с $s = \sqrt{n}$ и $m = O(\sqrt{n}2^{\sqrt{n}})$

(как в (1)), можно получить Σ_3-формулу и Σ_3-схему размера $2^{2\sqrt{n}}$ и $2^{\sqrt{n}}$ соответственно, с точностью до полиномиального фактора. Как уже было сказано выше, известно, что эти оценки оптимальны (с обеих сторон).

Ниже мы покажем обратное преобразование.

Лемма 3. *Пусть C — это $\Sigma_3(t,r)$-формула (схема), вычисляющая булеву функцию $f\colon \{0,1\}^n \to \{0,1\}$. Тогда можно получить КНФ-кодировку f с $\lceil \log t \rceil$ дополнительными переменными и размера r ($2rt$, соответственно).*

Доказательство. Пусть $C = F_1 \vee \cdots \vee F_t$ - это Σ_3-формула (тогда, $r = \mathrm{size}(F_1) + \cdots + \mathrm{size}(F_t)$). Введем $s = \lceil \log t \rceil$ дополнительных переменных $y_1, \ldots, y_s$. Теперь для каждого означивания $y_1, \ldots, y_s$, возьмем соответствующую КНФ F_i ($1 \leq i \leq 2^s$ - однозначное целочисленное соответствие этому означиванию) и добавим y_i с соответствующим знаком в каждый клоз F_i. Назовем получившуюся КНФ F_i'. Тогда, $F = F_1' \wedge \cdots \wedge F_{2^s}'$ кодирует f и F имеет не больше r клозов.

Если C это Σ_3-схема, то создадим отдельные копии каждого гейта, соответствующего клозам каждой из 2^s КНФ. Таким образом, размер получившейся КНФ-кодировки не больше, чем $r2^s \leq 2rt$. □

В заключение, покажем, что доказать сильные нижние оценки на размер КНФ-кодировки - не проще, чем доказать сильные нижние оценки на размер формул глубины 3. Пусть C — это $\Sigma_3(t,r)$-формула, вычисляющая PAR_n. Лемма 3 гарантирует, что PAR_n может быть закодирована как КНФ размера r с $\lceil \log t \rceil$ дополнительными переменными. Тогда, согласно неравенству(2),

$$\mathrm{size}(C) = t + r \geq t + \Omega\left(\frac{1}{n} \cdot 2^{\frac{n}{\log t + 2}}\right) \geq \frac{1}{n}\left(t + \Omega\left(2^{\frac{n}{\log t+2}}\right)\right) \geq \Omega\left(\frac{2^{\sqrt{n}}}{n}\right).$$

Аналогично, если C — это $\Sigma_3(t,r)$-схема. Лемма 3 гарантирует, что PAR_n может быть закодирована как КНФ размера $2rt$ с $\lceil \log t \rceil$ дополнительными переменными. Тогда,

$$\mathrm{size}(C) = t + r \geq t + \Omega\left(\frac{1}{2tn} \cdot 2^{\frac{n}{\log t + 2}}\right) \geq \Omega\left(\frac{2^{\sqrt{n/2}}}{n}\right).$$

3. Нижние оценки на КНФ-кодировки функции четности

В этой главе будет приведено доказательство Теоремы 1. Главное свойство функции четности, которым мы будем пользоваться — это высокая чувствительность (каждое выполняющее означивание изолированно): для всех $i \in [n]$ и всех $x, x' \in \{0,1\}^n$, которые отличаются только в i-ой позиции, $\mathrm{PAR}(x) \neq \mathrm{PAR}(x')$. Это обозначает, что если КНФ F вычисляет PAR и $F(x) = 1$, то F обязана содержать клоз, который выполняется только переменной x_i. Как и в [10], назовем такой клоз *критическим* по отношению к (x, i). Эта обозначение естественно расширяется для КНФ-кодировки. Пусть $F(x, y)$ - это КНФ-кодировка функции четности. Тогда для всех (x, y) таких, что $F(x, y) = 1$, и всех $i \in [n]$ верно следующее: F содержит клоз, который перестанет быть выполненным, если поменять значение бита x_i. Будем называть его критическим клозом по отношению к (x, y, i).

3.1. Ограниченное количество дополнительных переменных

Для доказательства нижней оценки $m \geq \Omega((s+1)2^{n/(s+1)}/n)$, адаптируем доказательство нижней оценки $\Omega(n^{1/4}2^{\sqrt{n}})$ на схему глубины 3, вычисляющую PAR_n от Патури, Пудлак и Зейн [10]. Рассмотрим КНФ $F(x_1, \ldots, x_n)$. Для каждого изолированного выполняющего означивания $x \in \{0,1\}^n$ функции F и каждого $i \in [n]$ зафиксируем самый короткий клоз по отношению к (x, i) и обозначим его $C_{F,x,i}$. Теперь для изолированного выполняющего означивания x определим его вес по отношению к F, как

$$w_F(x) = \sum_{i=1}^{n} \frac{1}{|C_{F,x,i}|}\,.$$

Лемма 4 (Лемма 5 из [10])**.** *Для всех μ у F может быть не более $2^{n-\mu}$ изолированных выполняющих означиваний веса хотя бы μ.*

Доказательство (2), $m \geq \Omega\left(\frac{s+1}{n} \cdot 2^{n/(s+1)}\right)$. Пусть $F(x_1, \ldots, x_n, y_1, \ldots, y_s)$ -

это КНФ-кодировка размера m функции PAR_n. Рассмотрим ее расширение:

$$\mathrm{PAR}_n(x) = \bigvee_{j \in [2^s]} F_j(x)\,.$$

Обобщим определение $C_{F,x,i}$ и $w(x)$ для КНФ с дополнительными переменными следующим образом. Пусть $x \in \mathrm{PAR}_n^{-1}(1)$ и пусть $j \in [2^s]$ - самый маленький индекс такой, что $F_j(x) = 1$. Для $i \in [n]$, положим $C'_{F,x,i} = C_{F_j,x,i}$ (то есть мы просто берем первую F_j, для которой x — это выполняющий набор, и рассматриваем ее критический клоз по отношению к (x, i)). Тогда вес $w'_F(x)$ у x по отношению к F определяется как $w_{F_j}(x)$. Ясно, что

$$w'_F(x) = \sum_{i \in [n]} \frac{1}{|C'_{(F,x,i)}|}\,.$$

Для $l \in [n]$, определим также $N_{l,F}(x) = |\{i \in [n] \colon |C'_{F,x,i}| = l\}|$ — число критических клозов (по отношению к x) длины l. Отметим, что

$$w'_F(x) = \sum_{l \in [n]} \frac{N_{l,F}(x)}{l}\,. \tag{7}$$

Для некоторого параметра $0 < \varepsilon < 1$, который выберем позже, поделим $\mathrm{PAR}_n^{-1}(1)$ на легкие и тяжелые части:

$$H = \{x \in \mathrm{PAR}_n^{-1}(1) \colon w'_F(x) \geq s + 1 + \varepsilon\}\,,$$
$$L = \{x \in \mathrm{PAR}_n^{-1}(1) \colon w'_F(x) < s + 1 + \varepsilon\}\,.$$

Утверждается следующий факт:

$$|H| \leq 2^s \cdot 2^{n-s-1-\varepsilon}\,.$$

Проверим его. Для каждого $x \in H$, $w'_F(x) = w_{F_j}(x)$ для некоторого $j \in [2^s]$, и по Лемме 4, у F_j не может быть больше, чем $2^{n-s-1-\varepsilon}$ изолированных вы-

полняющих означиваний веса хотя бы $s + 1 + \varepsilon$. То есть

$$\frac{|H|}{2^{n-s-1-\varepsilon}} \leq 2^s \,.$$

Что мы и хотели получить.
С учетом того факта, что $|H| + |L| = |\operatorname{PAR}_n^{-1}(1)| = 2^{n-1}$, имеем

$$|L| = 2^{n-1} - |H| \geq (1 - 2^{-\varepsilon})2^{n-1} \,. \tag{8}$$

Пусть $F = \{C_1, \ldots, C_m\}$. Для каждого $k \in [m]$, определим $C'_k \subseteq C_k$, как клоз C_k с удаленными дополнительными переменными. Тогда для всех $j \in [2^s]$, $F_j \subseteq \{C'_1, \ldots, C'_m\}$. Для $l \in [n]$, определим $m_l = |\{k \in [m] \colon |C'_k| = l\}|$, как число таких клозов длины l. Рассмотрим клоз C'_k и пусть $l = |C'_k|$. Тогда есть не больше $l2^{n-l}$ пар (x, i), где $x \in \operatorname{PAR}^{-1}(1)$ и $i \in [n]$ таких, что $C'_{F,x,i} = C'_k$: есть не больше l способов для выбора i, дальше выбрав i, фиксируем значение все l литералов в C'_k (всех эти литералы делаем равными 0, кроме i-ого, который приравниваем к 1), и теперь есть не больше 2^{n-l} опций для выбора остальных битов в x. Вспомнив, что $N_{l,F}(x)$ - это число критических клозов по отношению к x длины l, получаем:

$$m_l \cdot l \cdot 2^{n-l} \geq \sum_{x \in \operatorname{PAR}^{-1}(1)} N_{F,l}(x) \geq \sum_{x \in L} N_{F,l}(x) \,.$$

Тогда

$$m = \sum_{l \in [n]} m_l \geq \sum_{l \in [n]} \frac{\sum_{x \in L} N_{F,l}(x)}{l2^{n-l}} = \sum_{x \in L} \sum_{l \in [n]} \frac{N_{F,l}(x)}{l2^{n-l}} = \sum_{x \in L} n2^{-n} \sum_{l \in [n]} \frac{N_{F,l}(x)}{n} \cdot \frac{2^l}{l} \,. \tag{9}$$

Для оценки последней суммы заведем следующую функцию:

$$T(x) = \sum_{l \in [n]} \frac{N_{F,l}(x)}{n} \cdot \frac{2^l}{l} = \sum_{l \in [n]} \frac{N_{F,l}(x)}{n} \cdot g(l) \,,$$

где $g(l) = \frac{2^l}{l}$. Так как $g(l)$ — выпуклая (для $l > 0$) и $\sum_{l \in [n]} \frac{N_{F,l}(x)}{n} = 1$, то

по неравенству Йенсена получаем

$$T(x) \geq g\left(\sum_{l\in[n]} \frac{N_{F,l}(x)}{n} \cdot l\right) . \tag{10}$$

Теперь применяя неравенство Седракяна[1] (учитывая(7) и $\sum_{l\in[n]} N_{F,l}(x) = n$), имеем

$$\sum_{l\in[n]} lN_{F,l}(x) = \sum_{l\in[n]} \frac{N_{F,l}^2(x)}{N_{F,l}(x)/l} \geq \frac{(\sum_{l\in[n]} N_{F,l}(x))^2}{\sum_{l\in[n]} N_{F,l}(x)/l} = \frac{n^2}{w'_F(x)} . \tag{11}$$

Так как $g(l)$ монотонно возрастает при $l \geq 1/\ln 2$ и $w'_F(x) < s + 1 + \varepsilon$ для всех $x \in L$, комбинируя с (10) и (11), получаем

$$T(x) \geq g\left(\frac{n}{w'_F(x)}\right) \geq g\left(\frac{n}{s+1+\varepsilon}\right) , \tag{12}$$

для $s \leq n\ln 2 - 1 - \varepsilon$. (Если $s > n\ln 2 - 1 - \varepsilon$, то нижняя оценка $m \geq \Omega(2^{n/(s+1)}/n)$ тривиальна.)
Таким образом,

$$\begin{aligned}
m &\geq \sum_{x\in L} n2^{-n}T(x) \geq && \text{(9 и 12)}\\
&\geq \sum_{x\in L} n2^{-n} g\left(\frac{n}{s+1+\varepsilon}\right) = && \text{(определение } g\text{)}\\
&= |L|2^{-n}2^{\frac{n}{s+1+\varepsilon}}(s+1+\varepsilon) \geq && \text{(8)}\\
&\geq \left(\frac{1}{2} - \frac{1}{2^{\varepsilon+1}}\right)(s+1+\varepsilon)2^{\frac{n}{s+1+\varepsilon}} = && \text{(переписывание)}\\
&= \left(\frac{1}{2} - \frac{1}{2^{\varepsilon+1}}\right)(s+1+\varepsilon)2^{\frac{n}{s+1}}2^{\frac{-n\varepsilon}{(s+1)(s+1+\varepsilon)}} .
\end{aligned}$$

[1]Неравенство Седракяна - это частный случай неравенства Коши-Буняковского-Шварца: для всех $a_1, \ldots, a_n \in \mathbb{R}$ и $b_1, \ldots, b_n \in \mathbb{R}_{>0}$, $\sum_{i=1}^n a_i^2/b_i \geq \left(\sum_{i=1}^n a_i\right)^2 / \sum_{i=1}^n b_i$.

Возьмем $\varepsilon = 1/n$. Тогда,

$$\left(\frac{1}{2} - \frac{1}{2^{\frac{1}{n}+1}}\right) = \Theta\left(\frac{1}{n}\right).$$

Также верно, что

$$\frac{1}{2} \leq 2^{\frac{-1}{(s+1)(s+1+1/n)}} \leq 1\,,$$

так как $2^{-1/x}$ возрастает для $x > 0$. В итоге получаем нижнюю оценку

$$m \geq \Omega\left(\frac{s+1}{n} \cdot 2^{\frac{n}{s+1}}\right).$$

□

3.2. Ширина дизъюнктов

Для доказательства нижней оценки $k \geq n/(s+1)$ воспользуемся следующим следствием Satisfiability Coding Lemma.

Лемма 5 (Лемма 2 из [10])**.** *У любой k-КНФ $F(x_1, \ldots, x_n)$ может быть не больше $2^{n-n/k}$ изолированных выполняющих означиваний.*

Доказательство (3)*,* $k \geq n/(s+1)$. Рассмотрим k-КНФ $F(x_1, \ldots, x_n, y_1, \ldots, y_s)$, которая кодирует PAR_n. Возьмем ее расширение до OR от 2^s k-КНФ:

$$\mathrm{PAR}_n(x) = \bigvee_{j \in [2^s]} F_j(x)\,.$$

По Лемме 5 у каждой F_j не больше $2^{n-n/k}$ принимающих изолированных решений. Следовательно

$$2^s \geq \frac{2^{n-1}}{2^{n-n/k}} = 2^{n/k-1}$$

и, таким образом, $k \geq n/(s+1)$. □

3.3. Неограниченное количество дополнительных переменных

В этом разделе будет доказана нижняя оценка $m \geq 3n - 9$.

Доказательство (4), $m \geq 3n - 9$. Доказательство будем проводить, используя индукцию по n. База: $n \leq 3$ - очевидно. Индукционный переход: $n > 3$. Рассмотрим КНФ-кодировку $F(x_1, \ldots, x_n, y_1, \ldots, y_s)$ функции PAR_n с минимальным числом клозов. Ниже будет показано, что можно найти k детерминированных переменных (то есть обычных, не дополнительных) так, что после подстановки в эти переменные некоторые константы, число клозов уменьшится хотя бы на $3k$ (во всех случаях k будет равно 1 или 2) . Полученная функция будет вычислять PAR_{n-k} или ее отрицание. Не трудно показать, что минимальное число клозов в кодировке функции четности и в кодировки отрицания функции четности одинаково. Для этого изменим знаки всех детерминированных переменных в КНФ-кодировки (из PAR получится $\neg\,\mathrm{PAR}$ и наоборот). Таким образом, по индукционному предположению F содержит хотя бы $3(n-k) - 9 + 3k = 3n - 9$ клозов.

Чтобы найти требуемые k детерминированные переменные, мы разберем ряд случаев. В анализе, представленном ниже, под d-литералом будет подразумеваться литерал, который встречается ровно d раз в F, под d^+ — литерал, который встречается хотя бы d раз. (d_1, d_2)-литерал — тот, который встречается ровно d_1 раз положительно и d_2 раза отрицательно. Остальные типа литералов определяются аналогично. Будем рассматривать клоз, как множество литералов (которое не содержит вместе литерал и его отрицание), КНФ-формулу — как множество клозов.

Заметим, что для всех $i \in [s]$, y_i должен быть $(2^+, 2^+)$-литералом. Действительно, если y_i (или $\overline{y_i}$) — это 0-литерал, то можно сделать подстановку $y_i \leftarrow 0$ ($y_1 \leftarrow 1$, соответственно). Не трудно видеть, что получившиеся формула все еще кодирует функцию PAR. Если y_i - это $(1, t)$-литерал, то можно удалить его, используя резолюцию: для всех пар клозов $C_0, C_1 \in F$ таких, что $\overline{y_i} \in C_0$ и $y_i \in C_1$, добавим клоз $C_0 \cup C_1 \setminus \{y_i, \overline{y_i}\}$ (если этот клоз содержит пару дополняющих литералов, то пропускаем его); затем удалим все клозы, содержащие y_i или $\overline{y_i}$. Результирующая формула все еще кодирует PAR_n, но имеет меньший размер, чем F (мы удалили $1 + t$ клоз и добавили не больше t клозов).

В случаях, разобранных дальше, мы обозначили в качестве l_i — литерал, соответствующий детерминированный переменной x_i или ее отрицанию $\overline{x_i}$.

1. *F содержит 3^+-литерал l_i.* Подстановка $l_i \leftarrow 1$ элиминирует хотя бы три клоза в F.

2. *F содержит 1-литерал l_i.* Пусть $l_i \in C \in F$. C не может содержать другие детерминированные переменные: если $l_i, l_j \in C$ (для $i \neq j \in [n]$), рассмотрим $x \in \{0,1\}^n$ такой, что $\mathrm{PAR}_n(x) = 1$ и $l_i = l_j = 1$ (такой x существует начиная с $n > 3$), и его расширение $y \in \{0,1\}^s$ такое, что $F(x,y) = 1$; тогда, F не содержит критического клоза по отношению к (x,y,i). Понятно, что C не может содержать только одну переменную. C может содержать недетерминированную переменную y_j. Рассмотрим $x \in \{0,1\}^n$ такой, что $\mathrm{PAR}_n(x) = 1$ и $l_i = 1$, и его расширение $y \in \{0,1\}^s$ такое, что $F(x,y) = 1$. Если $y_j = 1$, то F не содержит критического клоза по отношению к (x,y,i). Тогда для любых $(x,y) \in \{0,1\}^{n+s}$ таких, что $F(x,y) = 1$ и $l_i = 1$, будет следовать, что $y_j = 0$. Это наблюдение позволяет нам поступить следующим образом: сначала сделаем подстановку $l_i \leftarrow 1$, затем $y_j \leftarrow 0$. Первая подстановка выполнит клоз C, вторая выполнит все клозы, содержащие $\overline{y_j}$. Учитывая тот факт, что y_i — $(2^+, 2^+)$-литерал, мы удалили хотя бы 3 клоза.

3. *Для всех $i \in [n]$, x_i — это $(2,2)$-литерал.* Если в F не найдется клоза, содержащего хотя бы 2 детерминированные переменные, то F содержит хотя бы $4n$ клозов, и, в таком случае, все доказано. Рассмотрим клоз, содержащий две детерминированные переменные: пусть $l_i, l_j \in C_1 \in F$, где $i \neq j$. И пусть C_2 и C_3 — это клозы, которые содержат другие вхождения l_i и l_j: $l_i \in C_2 \in F$ и $l_j \in C_3 \in F$ ($C_1 \neq C_2$ и $C_1 \neq C_3$, но может быть, что $C_2 = C_3$).

   Предположим, что C_2 содержит другую детерминированную переменную: $l_k \in C_2$, где $k \neq i, j$. Рассмотрим $x \in \{0,1\}^n$ такой, что $\mathrm{PAR}_n(x) = 1$ и $l_i = l_j = l_k = 1$ (такой x существует, начиная с $n > 3$), и его расширение $y \in \{0,1\}^s$ такое, что $F(x,y) = 1$. Тогда F не содержит критического клоза по отношению к (x,y,i): l_j выполняет C_1, l_k выполняет C_2. По похожим причинам C_2 не может содержать литерал l_j. Аналогично, C_3 не может содержать другие детерминированные пере-

менные и литерал l_i. (В тоже время, не исключено, что $\overline{l_j} \in C_2$ или $\overline{l_i} \in C_3$.) Теперь мы понимаем, что $C_2 \neq C_3$. Отметим, что и C_2 и C_3 обязаны содержать хотя бы одну дополнительную переменную: иначе, можно было бы сделать подстановку только для l_i и l_j, получив, что F ложна.

(a) *Хотя бы один из клозов C_2 или C_3 содержит одну дополнительную переменную.* Предположим, что это C_2:

$$\{l_i, y_1\} \subseteq C_2 \subseteq \{l_i, \overline{l_j}, y_1\}\,.$$

Сделаем подстановку $l_j \leftarrow 1$. Это удалит два клоза: C_1 и C_3. Также после этой подстановки C_2 будет иметь вид $\{l_i, y_1\}$ и l_i станет 1-литералом. Давайте проверим, что во всех означиваниях, выполняющих формулу F' верно, что $l_i = \overline{y_1}$. В самом деле, если (x, y) является выполняющим набором F' и $l_i = y_1$, тогда $l_i = y_1 = 1$ (иначе C_2 не выполнен). Но тогда не будет критического клоза в F' по отношению (x, y, i). Таким образом во всех выполняющих наборах F': $l_i = \overline{y_1}$. Тогда мы можем заменить каждый встречающийся литерал y_1 ($\overline{y_1}$) на $\overline{l_i}$ (y_1, соответственно). Это, в частности, выполнит клоз C_2.

(b) *И C_2 и C_3 содержат хотя бы две дополнительные переменные:*

$$\{l_i,\ l_j\} \subseteq C_1, \quad \{l_i,\ y_1,\ y_2\} \subseteq C_2, \quad \{l_j,\ y_3,\ y_4\} \subseteq C_3\,.$$

Здесь y_1 и y_2 — разные переменные, y_3 и y_4 — тоже разные, при этом, не исключено, что некоторые из y_1 и y_2 совпадают с некоторыми из y_3 и y_4. Рассмотрим все дополнительные переменные, встречающиеся в C_2 или C_3: $Y \subseteq \{y_1, \ldots, y_s\}$.

Напомним, что для всех $(x, y) \in \{0, 1\}^{n+s}$ таких, что $F(x, y) = 1$ и $l_i = l_j = 1$, следует, что $y = 0$ для всех $y \in Y$. Это значит, что, если переменная $y \in Y$ встречается в обоих клозах C_2 и C_3, то она там встречается с одинаковым знаком. Рассмотрим два подслучая:

i. $Y = \{y_1, y_2\}$:

$$\{l_i,\ l_j\} \subseteq C_1, \quad \{l_i,\ y_1,\ y_2\} \subseteq C_2, \quad \{l_j,\ y_1,\ y_2\} \subseteq C_3\,.$$

Предположим, что $\overline{y_1} \notin C_1$. Сделаем подстановку $l_i \leftarrow 1$, $l_j \leftarrow 1$. Тогда подстановка $y_1 \leftarrow 0$ элиминирует хотя бы два клоза. Покажем, что остались клозы, содержащие $\overline{y_2}$. Предположим, это не так. Рассмотрим $x \in \mathrm{PAR}_n^{-1}(1)$ такой, что $l_i = l_j = 1$, и его расширение $y \in \{0,1\}^s$ такое, что $F(x,y) = 1$. Мы знаем, что y_1 и y_2 обязаны быть равны 0. Однако, если поменять значение y_2 с 0 на 1, то формула будет все еще выполнена. А такого не может быть, значит остался хотя бы один клоз, содержащий $\overline{y_2}$. И, сделав подстановку $y_2 \leftarrow 0$, мы удалим еще один клоз. Аналогично, если $\overline{y_2} \notin C_1$. Теперь осталось проанализировать следующий случай:

$$\{l_i,\ l_j, \overline{y_1}, \overline{y_2}\} \subseteq C_1, \quad \{l_i,\ y_1,\ y_2\} \subseteq C_2, \quad \{l_j,\ y_1,\ y_2\} \subseteq C_3\,.$$

Предположим, что $\overline{l_j} \notin C_2$ и $\overline{l_i} \notin C_1$. Сделаем подстановку $l_i \leftarrow 1$, и затем подстановку $y_1 \leftarrow 0$ и $y_2 \leftarrow 0$. После этого C_3 примет вид $\{l_j\}$ (напомним, что C_3 не содержит другие детерминированные переменные, смотри случай 3). Это значит, что $l_j = 1$ во всех выполняющих означиваниях результирующей КНФ формулах, чего не может быть для КНФ-кодировки функции четности. Таким образом, мы можем предположить, что либо $\overline{l_j} \in C_2$ либо $\overline{l_i} \in C_1$. Не умаляя общности, предположим, что $\overline{l_j} \in C_2$.

Давайте покажем, что для всех $(x,y) \in \{0,1\}^{n+s}$ таких, что $F(x,y) = 1$ и $l_i = 1$ следует, что $l_j \neq y_1$ и $l_j \neq y_2$. В самом деле, если есть $(x,y) \in \{0,1\}^{n+s}$ такой, что $F(x,y) = 1$ и $l_i = l_j = 1$, тогда y_1 и y_2 должны быть равны 0. Если есть $(x,y) \in \{0,1\}^{n+s}$ такой, что $F(x,y) = 1, l_i = 1, l_j = 0$, тогда y_1 и y_2 должны быть равны 0, иначе F не содержит критического

клоза по отношению к (x, y, i). Таким образом, подстановка $l_i \leftarrow 1$ удаляет два клоза (C_1 и C_2). Затем мы можем заменить y_1 и y_2 на $\overline{l_j}$ и удалить клоз C_3.

ii. $|Y| \geq 3, \{y_1, y_2, y_3\} \subseteq Y$:

$$\{l_i,\ l_j\} \subseteq C_1, \quad \{l_i,\ y_1,\ y_2\} \subseteq C_2, \quad \{l_j,\ y_1,\ y_3\} \subseteq C_3\,.$$

Сделаем подстановку $l_i \leftarrow 1, l_j \leftarrow 1$. Она удалит C_1, C_2, C_3. Подстановка $y_1 \leftarrow 0$ удалит еще хотя бы один клоз (y_1 встречается положительно хотя бы два раза, но один из этих двух раз может быть в C_1). После этого должен остаться клоз, содержащий $\overline{y_2}$ (иначе мы могли бы сделать подстановку $y_2 \leftarrow 1$). Подстановка $y_2 \leftarrow 0$ удалит еще хотя бы один клоз. Аналогично, подстановка $y_3 \leftarrow 1$ удалит еще один (новый) клоз. Итого, мы удалили хотя бы 6 клозов.

□

Заключение

Минимальное число клозов в КНФ представлении функции четности $x_1 \oplus x_2 \oplus \cdots \oplus x_n$ - это 2^{n-1}. Можно получить более компактную КНФ-кодировку, используя дополнительные переменные. В этой работе доказаны следующие нижние оценки, которые почти совпадают с известными верхними, на число m клозов и максимальную ширину k клозов: 1) если есть не больше s дополнительны переменных, то $m \geq \Omega\left(2^{n/(s+1)}/n\right)$ и $k \geq n/(s+1)$; 2) минимальное число клозов - хотя бы $3n$.

Список литературы

[1] Eric Allender, Lisa Hellerstein, Paul McCabe, Toniann Pitassi, and Michael E. Saks. Minimizing disjunctive normal form formulas and AC^0 circuits given a truth table. *SIAM J. Comput.*, 38(1):63–84, 2008. doi:10.1137/060664537.

[2] Stephen Cook. The p versus np problem. *Clay Mathematics Institute*, 2, 2000.

[3] James M. Crawford, Michael Kearns, and Robert E. Schapire. The minimal disagreement parity problem as a hard satisfiability problem. *Technical report, Computational Intelligence Research Laboratory and ATT Bell Labs*, 1995.

[4] Judy Goldsmith, Matthew A. Levy, and Martin Mundhenk. Limited nondeterminism. *SIGACT News*, 27(2):20–29, 1996. doi:10.1145/235767.235769.

[5] Shuichi Hirahara. A duality between depth-three formulas and approximation by depth-two. *Electron. Colloquium Comput. Complex.*, page 92, 2017. URL: https://eccc.weizmann.ac.il/report/2017/092.

[6] Stasys Jukna. *Boolean Function Complexity - Advances and Frontiers*, volume 27 of *Algorithms and combinatorics*. Springer, 2012. doi:10.1007/978-3-642-24508-4.

[7] Petr Kucera, Petr Savický, and Vojtech Vorel. A lower bound on CNF encodings of the at-most-one constraint. *Theor. Comput. Sci.*, 762:51–73, 2019. doi:10.1016/j.tcs.2018.09.003.

[8] William J. Masek. Some NP-complete set covering problems. Unpublished Manuscript, 1979.

[9] Hiroki Morizumi. Lower bounds for the size of nondeterministic circuits. In Dachuan Xu, Donglei Du, and Ding-Zhu Du, editors, *Computing and Combinatorics - 21st International Conference, COCOON 2015, Beijing, China, August 4-6, 2015, Proceedings*, volume 9198 of *Lecture Notes in*

Computer Science, pages 289–296. Springer, 2015. doi:10.1007/978-3-319-21398-9_23.

[10] Ramamohan Paturi, Pavel Pudlák, and Francis Zane. Satisfiability coding lemma. *Chic. J. Theor. Comput. Sci.*, 1999, 1999. URL: http://cjtcs.cs.uchicago.edu/articles/1999/11/contents.html.

[11] Steven David Prestwich. CNF encodings. In Armin Biere, Marijn Heule, Hans van Maaren, and Toby Walsh, editors, *Handbook of Satisfiability*, volume 185 of *Frontiers in Artificial Intelligence and Applications*, pages 75–97. IOS Press, 2009. doi:10.3233/978-1-58603-929-5-75.

[12] Carsten Sinz. Towards an optimal CNF encoding of boolean cardinality constraints. In Peter van Beek, editor, *Principles and Practice of Constraint Programming - CP 2005, 11th International Conference, CP 2005, Sitges, Spain, October 1-5, 2005, Proceedings*, volume 3709 of *Lecture Notes in Computer Science*, pages 827–831. Springer, 2005. doi:10.1007/11564751_73.

[13] G. S. Tsejtin. On the complexity of derivation in propositional calculus. Semin. Math., V. A. Steklov Math. Inst., Leningrad 8, 115-125 (1970); translation from Zap. Nauchn. Semin. Leningr. Otd. Mat. Inst. Steklova 8, 234-259 (1968)., 1968.

[14] Leslie G. Valiant. Graph-theoretic arguments in low-level complexity. In Jozef Gruska, editor, *Mathematical Foundations of Computer Science 1977, 6th Symposium, Tatranska Lomnica, Czechoslovakia, September 5-9, 1977, Proceedings*, volume 53 of *Lecture Notes in Computer Science*, pages 162–176. Springer, 1977. doi:10.1007/3-540-08353-7_135.