ПРИКЛАДНАЯ ТЕОРИЯ КОДИРОВАНИЯ

УДК 510.52 DOI 10.17223/20710410/70/1

О ПРОБЛЕМЕ ДЕКОДИРОВАНИЯ ПО ПРИНЦИПУ МАКСИМАЛЬНОГО ПРАВДОПОДОБИЯ

В. Ю. Попов

Уральский федеральный университет имени первого Президента России Б. Н. Ельцина, г. Екатеринбург, Россия

E-mail: popovvvv@gmail.com

Рассмотрен количественный аналог проблемы декодирования по принципу максимального правдоподобия. Установлена экономная сводимость от проблемы совершенного паросочетания и слабо экономная сводимость от проблемы максимального разреза. Показана полнота в классах **WPP**, $\mathbf{C}_{=}\mathbf{P}$ и **PP** для некоторых количественных вариантов проблемы декодирования по принципу максимального правдоподобия.

Ключевые слова: *вычислительная сложность, проблема декодирования по принципу максимального правдоподобия, проблема совершенного паросочетания, проблема максимального разреза.*

ON THE MAXIMUM-LIKELIHOOD DECODING PROBLEM

V. Yu. Popov

Ural Federal University named after the first President of Russia B. N. Yeltsin, Ekaterinburg, Russia

Maximum likelihood decoding is an extensively used technique for digital communication systems. The hardness of the maximum likelihood decoding problem is the fundamental basis of the security justification for code-based cryptography. The study of code-based cryptography algorithms is considered as one of the main directions in the development of post-quantum cryptography. Nevertheless, it is known relatively little about the hardness of the maximum likelihood decoding problem. In this paper, we present an alternative proof of the **NP**-completeness of the maximum likelihood decoding problem that provides additional evidence for the security of cryptographic algorithms based on Classic McEliece. Also, we consider the counting variant of the maximum likelihood decoding problem, an important tool for finding collisions. We obtain a parsimonious reduction from the perfect matching problem and a weakly parsimonious reduction from the simple Max Cut problem. As a consequence, we obtain the #**P**-completeness of the counting variant of the maximum likelihood decoding problem. Also, we consider some counting variants of the maximum likelihood decoding problem for classes of computational complexity that are of interest from the point of view of quantum computing and post-quantum cryptography. In particular, we obtain completeness results for classes **WPP**, $\mathbf{C}_{=}\mathbf{P}$, and **PP**.

Keywords: *computational complexity, maximum likelihood decoding problem, perfect matching problem, Max Cut problem.*

Введение

Проблема декодирования по принципу максимального правдоподобия является одной из ключевых алгоритмических проблем теории кодирования. От качества её решения зависит эффективность применения кодов. Однако, как показано в работе [1], эта проблема является вычислительно трудной даже для двоичных линейных кодов. С другой стороны, трудность этой проблемы стала обоснованием криптографической стойкости алгоритма шифрования, предложенного в [2]. Схема алгоритма [2] оказалась весьма популярной и продуктивной. Она получила существенное дальнейшее развитие (см., например, [3–5]). В частности, в конкурсе NIST (National Institute of Standards and Technology) [6] в качестве кандидатов на постквантовый криптографический стандарт участвовали алгоритмы Classic McEliece и NTS-KEM [7, 8]. Алгоритм Classic McEliece, по сути дела, отражает изначально предложенную в работе [2] идею. Алгоритм NTS-KEM является существенной переработкой алгоритмов [2, 9] на основе преобразования, подобного преобразованиям [10, 11]. Однако его криптографическая стойкость во многом опирается на тот же фундамент, что и у Classic McEliece. Существенное внимание исследователи проявляют и к разработке для алгоритма [2] квантовых аналогов (см., например, [12, 13]).

Развитие квантовых технологий в последние годы значительно усилило интерес к проблеме декодирования с различных точек зрения. Существующие и перспективные технологии квантовых вычислений критически зависят от методов кодирования и эффективности исправления ошибок. Этим обусловлены интенсивное развитие квантовой теории кодирования и разработка новых квантовых кодов [14–16]. Возможная стойкость Classic McEliece относительно квантовых атак обусловила ряд исследований по криптоанализу [17–19]. С другой стороны, для нахождения более надёжного алгоритма существенное внимание уделяется адаптации Classic McEliece к новым кодам [20–22]. Исходя из этого, возросла важность дополнительного исследования вычислительной сложности проблемы декодирования как в классическом, так и в квантовом случае. Для квантовой проблемы декодирования рассмотрен ряд формулировок, для которых получены результаты не только по **NP**-трудности [23–25], но и по #**P**-трудности [26, 27]. Значительный интерес проявляется к поиску эффективных методов решения проблемы декодирования. Рассматриваются различные подходы к решению проблемы декодирования не только для классических кодов, но и для квантовых [28–30]. Среди используемых методов можно выделить обучение с подкреплением [31, 32], глубокое обучение [33] и различные типы нейронных сетей [34, 35]. В частности, можно отметить активное применение свёрточных сетей [36, 37]. Следует отметить, что гипотеза о трудности решения проблемы декодирования, так же как и проблемы обучения с ошибками (LWE), используемой для обоснования надёжности криптографических алгоритмов на решётках, является некоторым противопоставлением гипотезе об эффективности машинного обучения [38]. Многочисленные попытки применения методов машинного обучения для решения задач, связанных с декодированием, в значительной мере обусловлены уверенностью в недостаточной обоснованности трудности проблемы декодирования с практической точки зрения, что неоднократно отмечалось исследователями [39–41].

На практике как в теории кодирования, так и в криптографии обычно предполагается, что ошибка должна быть сравнительно мала. Желательно, чтобы она была

меньше минимального расстояния кода. Для исправления w ошибок необходимо минимальное расстояние $2w+1$. Для проблемы декодирования **NP**-трудность возможности декодирования доказана лишь для очень больших значений ошибки, которые наверняка не встретятся на практике.

Вопрос о количестве вариантов декодирования является принципиально важным для практического применения. От его решения зависит качество декодирования получателем информации. Кроме того, задача выяснения количества вариантов декодирования возникает при поиске возможных коллизий, что делает её важной с криптографической точки зрения. Однако количественные варианты проблемы декодирования даже не рассматривались. В частности, в отличие от квантовых кодов, #**P**-трудность для классических двоичных кодов не доказана. Следует отметить, что трудность количественных версий не следует автоматически из **NP**-трудности проблемы. Интересным примером является проблема NAESAT [42, п. 9.2]. Эта проблема является **NP**-полной [42, теорема 9.3]. Вариант NAESAT, требующий выяснить единственность решения, разрешим за полиномиальное время [43], а вариант NAESAT, требующий найти количество решений, является #**P**-полной проблемой [44].

В данной работе доказана вычислительная трудность вопроса о количестве вариантов декодирования.

1. Основные определения

Двухэлементное поле будем обозначать через $\mathbb{Z}_2$; вес Хэмминга $\mathrm{wt}(x)$ вектора $x \in \mathbb{Z}_2^n$ — количество его ненулевых координат. Рассмотрим формальное определение проблемы декодирования по принципу максимального правдоподобия.

Maximum Likelihood Decoding (MLD)

Дано: Двоичная $(m \times n)$-матрица $H \in \mathbb{Z}_2^{m \times n}$, вектор $s \in \mathbb{Z}_2^m$, число $k \in \mathbb{N}$.

Вопрос: Существует ли вектор $x \in \mathbb{Z}_2^n$, такой, что $Hx = s$ и $\mathrm{wt}(x) \leqslant k$?

Следуя [45], подсчитывающей машиной Тьюринга будем называть стандартную недетерминированную машину Тьюринга с дополнительной лентой, предназначенной для печати в двоичном виде количества допустимых вычислений этой машины для данного входа. Пусть максимальное время допустимого вычисления на входах, размер которых не превосходит n, равно $t(n)$. Предполагается, что подсчитывающая машина Тьюринга в худшем случае имеет сложность по времени $t(n)$. Таким образом, трудоёмкость генерации количества допустимых вычислений на дополнительной ленте не учитывается.

Класс #**P** состоит из всех функций, которые могут быть вычислены подсчитывающей машиной Тьюринга за полиномиальное время [45]. Количественная версия проблемы MLD может быть сформулирована следующим образом:

#MLD

Дано: Двоичная $(m \times n)$-матрица $H \in \mathbb{Z}_2^{m \times n}$, вектор $s \in \mathbb{Z}_2^m$, число $k \in \mathbb{N}$.

Найти: Количество попарно различных векторов $x \in \mathbb{Z}_2^n$, таких, что $Hx = s$ и $\mathrm{wt}(x) \leqslant k$.

Стандартный подход к доказательству #**P**-трудности некоторой алгоритмической проблемы A заключается в сведении к ней некоторой #**P**-полной проблемы B. Однако в отличие от **NP**-трудности, кроме полиномиальности сводимости должно выполняться требование сохранения количества решений [42]. В некоторых случаях необходимо более точное определение условия, накладываемого на полиномиальную сводимость. Для произвольных исходных данных I алгоритмической проблемы Π обозначим че-

рез $\#I$ количество решений проблемы Π на входе I. Следуя [46], полиномиальную сводимость R проблемы Π_1 к проблеме Π_2 будем называть слабо экономной, если существует полиномиально вычислимая функция f_R, такая, что для любых входов $I_1 \in \Pi_1$ и $I_2 \in \Pi_2$, таких, что $R(I_1) = I_2$, имеет место равенство $\#I_1 = f_R(I_1)\#I_2$. Полиномиальная сводимость R проблемы Π_1 к проблеме Π_2 называется экономной, если для любых входов $I_1 \in \Pi_1$ и $I_2 \in \Pi_2$, таких, что $R(I_1) = I_2$, имеет место равенство $\#I_1 = \#I_2$.

2. Анализ полиномиальных сводимостей для проблемы декодирования

Многие известные полиномиальные сведения сохраняют количество решений. В этих случаях доказательство **NP**-трудности является и доказательством #**P**-трудности [42]. Поэтому имеет смысл проанализировать известные полиномиальные сводимости для проблемы MLD.

Доказательство **NP**-трудности проблемы MLD, предложенное в работе [1], основано на полиномиальном сведении проблемы существования трёхмерного сочетания, **NP**-трудность которой доказана в [47]. Проблема существования трёхмерного сочетания может быть сформулирована следующим образом.

3-Dimensional Matching (3DM)

Дано: Натуральное число $n \in \mathbb{N}$, множество T, такое, что $|T| = n$, семейство трёхэлементных множеств $U \subseteq T \times T \times T$.

Вопрос: Существует ли $W \subseteq U$, такое, что $|W| = n$ и никакие два элемента W не имеют общих компонент?

Предположим, что $T = \{1, 2, \ldots, n\}$, $U = \{S_1, S_2, \ldots, S_m\}$. Полиномиальное сведение проблемы 3DM к MLD определяет матрица H размера $m \times 3n$, такая, что $S_i = (a, b, c)$ тогда и только тогда, когда в i-й строке матрицы H ровно три единицы и эти единицы располагаются в столбцах с номерами a, $b + n$, $c + 2n$. Следуя рассуждениям [1], легко проверить, что сумма менее чем n строк не даёт вектор, состоящий из одних единиц, а сумма n строк, дающая вектор, состоящий из одних единиц, находится во взаимно однозначном соответствии с некоторым решением проблемы 3DM. Таким образом, полиномиальное сведение проблемы 3DM к проблеме MLD сохраняет количество решений. Рассмотрим теперь полиномиальные сведения к проблеме 3DM.

В работе [47] доказательство **NP**-трудности проблемы 3DM проведено последовательным полиномиальным сведением от проблемы выполнимости через проблемы 3-выполнимости, хроматического числа и точного покрытия. Появление проблемы хроматического числа в последовательности полиномиальных сведений очевидным образом делает эту последовательность сведением, не сохраняющим количество решений, поскольку вместе с каждой допустимой раскраской решением будет и любая взаимно однозначная перестановка цветов. Однако гипотетически это можно обойти аналогично тому, как это сделано для проблемы вычисления перманента [42, теорема 18.3], устанавливая соответствие между количеством решений t проблемы 3-выполнимости и количеством решений $c!d$ проблемы хроматического числа, где c обозначает количество цветов. Поэтому мы остановимся на полиномиальном сведении 3-выполнимости к проблеме хроматического числа более подробно. Рассмотрим проблемы 3-выполнимости и хроматического числа в формулировках, соответствующих работе [47].

SATisfiability with at most 3 literals per clause ($\leqslant$3SAT)

Дано: Булева функция $f(x_1, x_2, \ldots, x_m) = \bigwedge\limits_{i=1}^{r} D_i$, где для любого $1 \leqslant i \leqslant r$ функция D_i является дизъюнкцией не более трёх литералов из множества переменных и их отрицаний $\{x_1, x_2, \ldots, x_m, \neg x_1, \neg x_2, \ldots, \neg x_m\}$.

Вопрос: Существует ли набор значений переменных $x_j \in \{0, 1\}$, $1 \leqslant j \leqslant m$, такой, что выполняется равенство $f(x_1, x_2, \ldots, x_m) = 1$?

Chromatic Number (CN)

Дано: Граф $G = (V, E)$, заданный множеством вершин V и множеством рёбер E, натуральное число $k \in \mathbb{N}$.

Вопрос: Существует ли функция $\phi : \mathbb{N} \to \{1, 2, \ldots, k\}$, такая, что $\phi(u) \neq \phi(v)$ для любого ребра $(u, v) \in E$?

В предположении $m \geqslant 4$ в работе [47] полиномиальное сведение проблемы $\leqslant$3SAT к проблеме CN задаётся следующими соотношениями:

$$V = \{x_1, x_2, \ldots, x_m, \} \cup \{\neg x_1, \neg x_2, \ldots, \neg x_m\} \cup \{v_1, v_2, \ldots, v_m\} \cup \{D_1, D_2, \ldots, D_r\},$$
$$E = \{(x_i, \neg x_i) : 1 \leqslant i \leqslant m\} \cup$$
$$\cup \{(v_i, v_j) : 1 \leqslant i \leqslant m,\ 1 \leqslant j \leqslant m,\ i \neq j\} \cup$$
$$\cup \{(v_i, x_j) : 1 \leqslant i \leqslant m,\ 1 \leqslant j \leqslant m,\ i \neq j\} \cup$$
$$\cup \{(v_i, \neg x_j) : 1 \leqslant i \leqslant m,\ 1 \leqslant j \leqslant m, i \neq j\} \cup$$
$$\cup \{(x_i, D_j) : 1 \leqslant i \leqslant m,\ 1 \leqslant j \leqslant r,\ x_i \notin D_j\} \cup$$
$$\cup \{(\neg x_i, D_j) : 1 \leqslant i \leqslant m,\ 1 \leqslant j \leqslant r,\ \neg x_i \notin D_j\},$$
$$k = m + 1.$$

Включение $\{(v_i, v_j) : 1 \leqslant i \leqslant m,\ 1 \leqslant j \leqslant m,\ i \neq j\} \subset E$ гарантирует, что $\phi(v_i) \neq \phi(v_j)$ для всех $1 \leqslant i \leqslant m$, $1 \leqslant j \leqslant m$, $i \neq j$. Так как значения функции ϕ для всех вершин из множества $\{v_1, v_2, \ldots, v_m\}$ попарно различны и $k = m+1$, имеется лишь одно значение функции ϕ, такое, что оно не является элементом множества $\{\phi(v_1), \phi(v_2), \ldots, \phi(v_m)\}$. Обозначим это значение через a. Включение

$$\{(v_i, x_j) : 1 \leqslant i \leqslant m,\ 1 \leqslant j \leqslant m,\ i \neq j\} \cup \{(v_i, \neg x_j) : 1 \leqslant i \leqslant m,\ 1 \leqslant j \leqslant m,\ i \neq j\} \subset E$$

гарантирует, что для всех $1 \leqslant i \leqslant m$, $1 \leqslant j \leqslant m$, $i \neq j$ выполняется $\phi(v_i) \neq \phi(x_j)$ и $\phi(v_i) \neq \phi(\neg x_j)$. Поэтому $\phi(x_j) \in \{\phi(v_j), a\}$ и $\phi(\neg x_j) \in \{\phi(v_j), a\}$ для всех $1 \leqslant j \leqslant m$.

Из включения $\{(x_i, \neg x_i) : 1 \leqslant i \leqslant m\} \subset E$ получаем $\{\phi(x_j), \phi(\neg x_j)\} = \{\phi(v_j), a\}$ для всех $1 \leqslant j \leqslant m$. Поскольку $m \geqslant 4$ и дизъюнкции содержат не более трёх литералов, для любого i найдётся такое j, что $x_j \notin D_i$ и $\neg x_j \notin D_i$. Тогда из условия

$$\{(x_i, D_j) : 1 \leqslant i \leqslant m, 1 \leqslant j \leqslant r, x_i \notin D_j\} \cup \{(\neg x_i, D_j) : 1 \leqslant i \leqslant m, 1 \leqslant j \leqslant r, \neg x_i \notin D_j\} \subset E$$

получим, что $\phi(D_i) \neq a$ для всех $1 \leqslant i \leqslant r$. Кроме того, отсюда же следует, что

$$\phi(D_i) \in \{\phi(v_j) : x_j \in D_i,\ 1 \leqslant j \leqslant m\} \cup \{\phi(v_j) : \neg x_j \in D_i,\ 1 \leqslant j \leqslant m\}$$

для всех $1 \leqslant i \leqslant r$. Таким образом, функция $\phi : \mathbb{N} \to \{1, 2, \ldots, k\}$, такая, что $\phi(u) \neq \phi(v)$ для любого ребра $(u, v) \in E$, существует тогда и только тогда, когда для любой дизъюнкции найдётся литерал w с условием $\phi(w) \neq a$. Мы можем интерпретировать a как 0, рассматривая все элементы множества $\{\phi(v_1), \phi(v_2), \ldots, \phi(v_m)\}$ как 1.

Это позволяет убедиться в том, что данное полиномиальное сведение не сохраняет количество решений. В частности, значение $\phi(D_i)$ может совпадать со значением ϕ для любого истинного литерала из дизъюнкции D_i.

Кроме доказательства **NP**-трудности проблемы 3DM, предложенного в работе [47], имеется доказательство, приведённое в [42, 48], через полиномиальное сведение стандартной версии проблемы 3-выполнимости, предполагающей наличие ровно трёх литералов в каждой дизъюнкции. Однако это полиномиальное сведение тоже не сохраняет количество решений. В частности, в обозначениях [48, теорема 3.2] каждой дизъюнкции c_j соответствует множество

$$C_j = \{(u_i[j], s_1[j], s_2[j]) : u_i \in c_j\} \cup \{(\overline{u}_i[j], s_1[j], s_2[j]) : (\overline{u}_i \in c_j\}.$$

Из этого множества в трёхмерное сочетание M' можно выбрать любой элемент, соответствующий истинному литералу, что позволяет по одному решению проблемы 3-выполнимости построить несколько различных трёхмерных сочетаний.

Мы убедились в том, что имеющиеся для проблемы 3DM сводимости не подходят для доказательства #**P**-трудности проблемы #MLD. Однако сводимость, построенную в работе [1], несложно адаптировать для проблемы совершенного паросочетания для двудольного графа. Рассмотрим несколько более общий подход, установив сводимость для произвольного графа.

Perfect Matching (PM)

Дано: Граф $G = (V, E)$, заданный множеством вершин V и множеством рёбер E.

Вопрос: Существует ли $M \subseteq E$, такое, что каждая вершина графа G инцидентна ровно одному ребру из множества M?

Теорема 1. Существует экономная сводимость проблемы PM к проблеме MLD.

Доказательство. Без ограничения общности можем полагать, что граф имеет чётное количество вершин. Рассмотрим граф $G = (V, E)$, заданный множеством вершин $V = \{v_1, v_2, \ldots, v_n\}$ и множеством рёбер $E = \{e_1, e_2, \ldots, e_m\}$. Для графа G рассмотрим двоичную матрицу H размера $m \times n$, такую, что её элемент $h_{i,j}$ равен единице тогда и только тогда, когда вершина v_j инцидентна ребру e_i. Пусть $k = n/2$. Будем полагать, что вектор s состоит из одних единиц. Легко понять, что вектор $x \in \mathbb{Z}_2^n$, такой, что $Hx = s$ и $\mathrm{wt}(x) \leqslant k$, существует тогда и только тогда, когда в графе G существует совершенное паросочетание, т. е. такое подмножество $M \subseteq E$, что каждая вершина графа G инцидентна ровно одному ребру из множества M. Более того, рёбра множества M и единицы вектора x находятся во взаимно однозначном соответствии. ■

В работе [45] доказано, что проблема вычисления перманента двоичной матрицы является #**P**-полной относительно полиномиальной сводимости. Поскольку значение перманента двоичной матрицы равно количеству совершенных паросочетаний в двудольном графе, заданном этой матрицей, из теоремы 1 и результата [45] вытекает

Следствие 1. Проблема #MLD является #**P**-полной относительно полиномиальной сводимости.

Кроме полиномиального сведения, предложенного в [1], существует ещё один подход к обоснованию **NP**-трудности проблемы MLD. Он основан на использовании **NP**-трудности проблемы существования максимального разреза, которая может быть сформулирована следующим образом [39, 42].

Simple Max Cut (SMC)

Дано: Натуральное число $n \in \mathbb{N}$, граф $G = (V, E)$.

Вопрос: Существует ли такое множество вершин $W \subseteq V$, что $|F| \geqslant n$, где $F = \{(u, v) : u \in W,\ v \in V \setminus W\}$?

NP-полнота проблемы SMC доказана в работе [49] (см. также [42, теорема 9.5]). В [50] предложен подход к построению кодов по графам. В [39] указано, что проблема MLD является **NP**-полной, и это можно доказать, используя матрицу смежности графа и вектор, состоящий из одних единиц [39, предложение 1]. Идея [39] получила поддержку исследователей (см., например, [51]). Кроме того, на основе **NP**-полноты проблемы SMC предложен ряд подходов к получению альтернативных доказательств **NP**-трудности проблемы MLD через промежуточные сведения [52, 53]. Однако подход, предложенный в [39], без некоторой доработки использовать нельзя. Например, можно рассмотреть полный трёхвершинный граф K_3. Очевидно, что для K_3 максимальный разрез равен 2. В то же время граф K_3 можно представить в виде

$$K_3 = (V, E), \quad V = \{a_1, a_2, a_3\}, \quad E = \{b_1, b_2, b_3\},$$
$$b_1 = (a_1, a_2), \quad b_2 = (a_1, a_3), \quad b_3 = (a_2, a_3).$$

В этом случае строки матрицы H имеют вид $(1, 1, 0)$, $(1, 0, 1)$, $(0, 1, 1)$. Матричное уравнение $Hx = s$ для вектора s, состоящего из одних единиц, равносильно системе уравнений

$$\begin{cases} x_1 + x_2 = 1, \\ x_1 + x_3 = 1, \\ x_2 + x_3 = 1, \end{cases}$$

которая, очевидно, не имеет решений. Аналогичная ситуация имеет место для любого графа, не являющегося двудольным, а для двудольных графов максимальный разрез всегда равен количеству рёбер графа, что тривиально влечёт разрешимость проблемы SMC для двудольных графов за линейное время.

Непосредственное применение подхода из [39] позволяет получить альтернативное доказательство **NP**-трудности известной проблемы существования ближайшего кодового слова, которую можно сформулировать следующим образом [54, 55].

Nearest codeword (NC)

Дано: Двоичная матрица $H \in \mathbb{Z}_2^{m \times n}$, вектор $s \in \mathbb{Z}_2^m$, число $k \in \mathbb{N}$.

Вопрос: Существует ли вектор такой $x \in \mathbb{Z}_2^n$, что $\mathrm{wt}(Hx + s) \leqslant k$?

3. Полиномиальная сводимость для проблемы максимального разреза

Проблема MLD активно используется в криптографических целях. В частности, большое количество криптографических алгоритмов построено на основе схемы [2]. Однако полиномиальная сводимость, установленная в [1], гарантирует трудность проблемы MLD лишь для исходных данных, которые не могут быть использованы на практике. Поэтому представляет значительный практический интерес нахождение альтернативных доказательств **NP**-трудности проблемы MLD. Учитывая существенное внимание к использованию проблемы SMC для обоснования трудности проблемы MLD, установим корректность полиномиальной сводимости проблемы SMC к проблеме MLD.

Для произвольного алфавита Σ обозначим через Σ^n, где $n \in \mathbb{N}$, множество всевозможных слов длины n в алфавите Σ. Обозначим через 0^n и 1^n, где $n \in \mathbb{N}$, единственные элементы множеств $\{0\}^n$ и $\{1\}^n$ соответственно.

Рассмотрим граф $G = (V, E)$ без петель и кратных рёбер, заданный множеством вершин $V = \{v_1, v_2, \ldots, v_p\}$ и множеством рёбер $E = \{e_1, e_2, \ldots, e_q\}$. Каждой вершине v_i поставим в соответствие слово $h_i \in \{0,1\}^{(p+1)q}$. Пусть для любого $1 \leqslant i \leqslant p$ слово h_i имеет вид $h_i = a_{i,1}a_{i,2}\ldots a_{i,q}$, где $a_{i,j} = 1^{p+1}$, если $e_j = (v_i, v_k)$ для некоторого $k \in \in \{1, \ldots, p\}$, и $a_{i,j} = 0^{p+1}$, если $e_j \neq (v_i, v_k)$ для любого $k \in \{1, \ldots, p\}$. Определим слово

$$h_i = h_{i,1}h_{i,2}\ldots h_{i,(p+1)q} \in \{0,1\}^{(p+1)q}$$

для любого $p+1 \leqslant i \leqslant p+(p+1)q$, полагая

$$h_{i,j} = \begin{cases} 1, & j = i-p,\ 1 \leqslant j \leqslant (p+1)q, \\ 0, & j \neq i-p,\ 1 \leqslant j \leqslant (p+1)q. \end{cases} \tag{1}$$

Пусть вектор s состоит из одних единиц, $m = p+(p+1)q$, $n = (p+1)q$. С помощью слов h_i, $1 \leqslant i \leqslant m$, определим матрицу H размера $m \times n$, где i-я строка матрицы H равна слову h_i для любого $1 \leqslant i \leqslant m$. Заметим, что подматрица размера $n \times n$ матрицы H, состоящая из строк h_l, где $p+1 \leqslant l \leqslant m$, в силу соотношения (1) является единичной.

Покажем, что максимальный разрез графа G не меньше r тогда и только тогда, когда существует такой вектор $x \in \mathbb{Z}_2^n$, что $Hx = s$ и $\mathrm{wt}(x) \leqslant k$, где $k = p+(q-r)(p+1)$.

Допустим, что максимальный разрез графа G равен r. Без ограничения общности можно считать, что $r > 0$. Тогда существует разбиение $V = V_1 \cup V_2$ на непустые подмножества V_1 и V_2, такие, что

$$|\{(u,v) : u \in V_1,\ v \in V_2,\ (u,v) \in E\}| \geqslant r. \tag{2}$$

Каждому ребру $e_t = (v_i, v_j) \in E$, $1 \leqslant t \leqslant q$, поставим в соответствие набор столбцов матрицы H с номерами от $(t-1)(p+1)+1$ до $(t-1)(p+1)+p+1$. В каждом из этих столбцов ровно три единицы: две единицы в первых p строках столбца (по одной на каждую вершину ребра e_t), что следует из определения слов h_l при $1 \leqslant l \leqslant p$, и одна единица в последних n строках в силу единичности подматрицы, состоящей из строк h_l, где $p+1 \leqslant l \leqslant m$. Эти единицы расположены в строках с номерами i, j, $l+p$, где l — номер столбца. Поэтому в i-й строке, соответствующей вершине v_i, для каждого инцидентного вершине $v_i \in V_1$ ребра e_t имеется группа из $p+1$ единиц в таких столбцах, что все остальные строки, соответствующие вершинам из V_1, имеют в этих столбцах нули. Отсюда и из неравенства (2) получаем соотношение

$$\mathrm{wt}\left(\sum_{v_i \in V_1} h_i\right) \geqslant r(p+1). \tag{3}$$

Из неравенства (3) очевидным образом следует, что вектор

$$\sum_{v_i \in V_1} h_i \tag{4}$$

имеет не более $n-r(p+1)$ нулевых координат. Обозначим через N множество нулевых координат вектора (4). По определению вектора s из (1) получаем равенство

$$\sum_{v_i \in V_1} h_i + \sum_{j-p \in N} h_j = s. \tag{5}$$

Рассмотрим вектор

$$x = (x_1, x_2, \ldots, x_n)^{\mathrm{T}}, \tag{6}$$

такой, что для любого i, $1 \leqslant i \leqslant n$, равенство $x_i = 1$ выполняется тогда и только тогда, когда $v_i \in V_1$ или $i - p \in N$. Заметим, что соотношение $i - p \in N$ гипотетически может выполняться лишь при $i \geqslant p + 1$. По определению матрицы H получаем равенство

$$Hx = \sum_{v_i \in V_1} h_i + \sum_{j-p \in N} h_j. \tag{7}$$

Из (5) и (7) получаем равенство $Hx = s$. По определению вектора x имеет место

$$\mathrm{wt}(x) = |V_1| + |N|. \tag{8}$$

Поскольку вектор (4) имеет не более $n - r(p+1)$ нулевых координат, по определению множества N должно выполняться неравенство

$$|N| \leqslant n - r(p+1). \tag{9}$$

Мощность множества V_1 не превосходит мощности множества всех вершин графа G. Поэтому из соотношений (8) и (9) следует неравенство $\mathrm{wt}(x) \leqslant p + n - r(p+1)$. Так как $n = (p+1)q$, $\mathrm{wt}(x) \leqslant p + (p+1)q - r(p+1) = p + (q-r)(p+1)$, что и требовалось.

Предположим теперь, что существует вектор (6), такой, что $Hx = s$ и

$$\mathrm{wt}(x) \leqslant p + (q-r)(p+1). \tag{10}$$

Пусть

$$P = \{i : x_i = 1,\ i \leqslant p\}, \quad Q = \{i : x_i = 1,\ i > p\}. \tag{11}$$

Из (11) по определению матрицы H получаем равенство

$$Hx = \sum_{i \in P} h_i + \sum_{j \in Q} h_j.$$

По предположению $Hx = s$, поэтому $s = \sum\limits_{i \in P} h_i + \sum\limits_{j \in Q} h_j$. Отсюда по определению вектора s получаем соотношение

$$\mathrm{wt}\left(\sum_{i \in P} h_i + \sum_{j \in Q} h_j\right) = (p+1)q. \tag{12}$$

По определению расстояния Хэмминга выполняется неравенство

$$\mathrm{wt}\left(\sum_{i \in P} h_i + \sum_{j \in Q} h_j\right) \leqslant \mathrm{wt}\left(\sum_{i \in P} h_i\right) + \mathrm{wt}\left(\sum_{j \in Q} h_j\right). \tag{13}$$

По определению матрицы H из (11) получаем

$$\mathrm{wt}\left(\sum_{j \in Q} h_j\right) = |Q|. \tag{14}$$

Из соотношений (6), (11) и (14) следует, что $\mathrm{wt}\Big(\sum\limits_{j \in Q} h_j\Big) \leqslant \mathrm{wt}(x)$. Отсюда по предположению (10) получаем

$$\mathrm{wt}\left(\sum_{j \in Q} h_j\right) \leqslant p + (q-r)(p+1). \tag{15}$$

Из соотношений (12) и (13) очевидным образом следует, что

$$(p+1)q \leqslant \mathrm{wt}\left(\sum_{i\in P} h_i\right) + \mathrm{wt}\left(\sum_{j\in Q} h_j\right). \tag{16}$$

Из (15) и (16) можно получить неравенство

$$(p+1)q \leqslant \mathrm{wt}\left(\sum_{i\in P} h_i\right) + p + (q-r)(p+1). \tag{17}$$

Соотношение (17) равносильно неравенству

$$(r-1)(p+1)+1 \leqslant \mathrm{wt}\left(\sum_{i\in P} h_i\right). \tag{18}$$

Множество P задает множество вершин $V(P) = \{v_i : i \in P\}$, которое определяет некоторый разрез $E' \subseteq E$ графа G. Пусть $\sum\limits_{i\in P} h_i = (a_1, a_2, \ldots, a_{(p+1)q})$. Легко понять, что для произвольного t, $1 \leqslant t \leqslant q$, выполнимость равенства $a_j = 1$ для какого-либо j, удовлетворяющего условию

$$(t-1)(p+1)+1 \leqslant j \leqslant (t-1)(p+1)+p+1,$$

равносильна тому, что выполняется соотношение $e_t \in E'$ и равенство $a_i = 1$ имеет место для всех i, для которых справедливо

$$(t-1)(p+1)+1 \leqslant i \leqslant (t-1)(p+1)+p+1,$$

т. е. в векторе $(a_1, a_2, \ldots, a_{(p+1)q})$ все единичные координаты разбиваются на непересекающиеся группы, каждая из которых состоит из $p+1$ единиц и соответствует некоторому ребру e_t из множества E'. Следовательно, $\mathrm{wt}\left(\sum\limits_{i\in P} h_i\right) = (p+1)|E'|$. Поэтому из неравенства (18) следует требуемое соотношение $|E'| \geqslant r$.

Таким образом, мы установили полиномиальную сводимость проблемы SMC к проблеме MLD. Однако полученное сведение не сохраняет количество решений, поскольку для фиксированного разреза каждое разбиение $V = V_1 \cup V_2$ определяет два вектора x, а количество таких разбиений существенно зависит от свойств разреза. Более того, ясно, что никакая полиномиальная сводимость, развивающая предложенную в [39] идею кодирования векторов вершинами графа, не будет сохранять количество решений.

4. Количественная версия проблемы максимального разреза

Для количественного варианта проблемы SMC, пожалуй, наиболее естественно рассматривать требование нахождения количества разрезов. Однако нас интересует другая версия проблемы.

#SMC

Дано: Натуральное число $n \in \mathbb{N}$, граф $G = (V, E)$.

Найти: Количество множеств вершин $W \subseteq V$, таких, что выполняется неравенство $|F| \geqslant n$, где $F = \{(u, v) : (u, v) \in E, u \in W, v \in V \setminus W\}$.

Нетрудно убедиться, что полиномиальная сводимость проблемы NAESAT к проблеме SMC [42, теорема 9.5] является слабо экономной сводимостью проблемы

#NAESAT к проблеме #SMC. В частности, для любого решения проблемы #NAESAT мы получаем ровно два решения проблемы #SMC: W и $V \setminus W$. С учётом тривиальной принадлежности проблемы #SMC классу **#P** отсюда и из **#P**-полноты проблемы #NAESAT относительно слабо экономной сводимости [44] вытекает **#P**-полнота проблемы #SMC относительно слабо экономной сводимости.

Легко проверить, что полиномиальная сводимость проблемы SMC к проблеме MLD, рассмотренная в п. 3, является экономной сводимостью проблемы #SMC к проблеме #MLD: каждому множеству вершин W, задающему разрез, соответствует единственный вектор x, и наоборот. Поскольку принадлежность проблемы #MLD классу **#P** очевидна, отсюда и из **#P**-полноты проблемы #SMC вытекает

Теорема 2. Проблема #MLD является **#P**-полной относительно слабо экономной сводимости.

5. Полные проблемы для различных классов количественных проблем

Современная теория квантовых вычислений ассоциирует эффективную вычислимость с квантовой машиной Тьюринга и рассматривает класс **BQP** как класс эффективно решаемых задач [56, 57]. Точное соотношение класса **BQP** с классическими классами **P**, **NP** и **PSPACE** пока не выяснено. Однако господствует мнение, что $\mathbf{NP} \not\subseteq \mathbf{BQP}$. Это позволяет разрабатывать постквантовые криптографические алгоритмы, основываясь на трудности **NP**-полных проблем [57]. В то же время ведутся активные исследования в области специализированных квантовых вычислителей. В частности, архитектура D-Wave ориентирована на эффективное решение широкого класса **NP**-полных проблем [58–60]. Поэтому для важных криптографических моделей представляет значительный интерес исследование вычислительной сложности проблем за пределами класса **NP** [61, 62].

Для произвольной квантовой машины Тьюринга T обозначим через $P_{\mathrm{acc}}(x)$ вероятность того, что на входе x машина T переходит в допустимое состояние. Соответственно через $P_{\mathrm{rej}}(x)$ обозначим вероятность того, что машина T отвергает вход x. Следуя [63] (см. также [64, 65]), будем полагать, что

- **EQP** — класс языков $L \subseteq \Sigma^*$, для которых существует полиномиальная квантовая машина Тьюринга T, такая, что $x \in L \Rightarrow P_{\mathrm{acc}}(x) = 1$ и $x \notin L \Rightarrow P_{\mathrm{rej}}(x) = 1$ для любого $x \in \Sigma^*$;
- **BQP** — класс языков $L \subseteq \Sigma^*$, для которых существует полиномиальная квантовая машина Тьюринга T, такая, что $x \in L \Rightarrow P_{\mathrm{acc}}(x) > 2/3$ и $x \notin L \Rightarrow P_{\mathrm{rej}}(x) > 2/3$ для любого $x \in \Sigma^*$;
- **NQP** — класс языков $L \subseteq \Sigma^*$, для которых существует полиномиальная квантовая машина Тьюринга T, такая, что $x \in L \Rightarrow P_{\mathrm{acc}}(x) > 0$ и $x \notin L \Rightarrow P_{\mathrm{acc}}(x) = 0$ для любого $x \in \Sigma^*$.

Для классов **EQP**, **BQP** и **NQP** имеют место следующие очевидные включения:

$$\mathbf{EQP} \subseteq \mathbf{BQP} \subseteq \mathbf{NQP}.$$

Классы **EQP**, **BQP** и **NQP** обычно рассматриваются как квантовые аналоги классических классов **P**, **BPP** и **NP** соответственно [63]). Следует отметить, что алгоритмы Шора позволяют решать задачи факторизации и дискретного логарифма в классе **BQP** [66]. Обычно именно класс **BQP** рассматривается как класс алгоритмических проблем, которые могут быть эффективно решены на квантовой машине Тьюринга. Соответственно класс **NQP** следует рассматривать в рамках теоретически допустимой перспективы.

В работе [67] предложен модифицированный вариант квантовой машины Тьюринга, допускающий возможность измерения вероятности бита после завершения шага вычисления. Для этого варианта квантовой машины Тьюринга в [67] определён класс **PostBQP**, являющийся аналогом **BQP**. Хотя возможность практической реализации варианта машины, предложенного в [67], с точки зрения физики не считается реалистичной, сам класс **PostBQP** при определённых условиях может быть реализован на стандартных квантовых машинах. Поэтому класс **PostBQP**, как и класс **NQP**, следует учитывать в перспективных возможностях.

Определение класса **NP** и его криптографического подкласса **UP** через класс **#P** позволяет легко увидеть естественные аналоги **NP** и **UP**, расположенные выше в иерархии классов вычислительной сложности. Обозначим через **FP** класс разрешимых за полиномиальное время функциональных проблем. Для произвольной недетерминированной машины Тьюринга T обозначим через $\#\mathrm{acc}_T(x)$ и $\#\mathrm{rej}_T(x)$ количество допускающих и отвергающих вход x вычислений соответственно. Обозначим через **GapP** класс всех функций f, для которых существует недетерминированная машина Тьюринга T, такая, что $f(x) = \#\mathrm{acc}_T(x) - \#\mathrm{rej}_T(x)$ для всех x. Следуя [63, 68], дадим определение ряда классов вычислительной сложности как классов распознаваемых языков:

— **NP** — класс языков $L \subseteq \Sigma^*$, для которых существует функция $f \in \#\mathbf{P}$, такая, что $x \in L \Leftrightarrow f(x) > 0$ для любого $x \in \Sigma^*$;
— **UP** — класс языков $L \subseteq \Sigma^*$, для которых существует функция $f \in \#\mathbf{P}$, такая, что $x \in L \Rightarrow f(x) = 1$ и $x \notin L \Rightarrow f(x) = 0$ для любого $x \in \Sigma^*$;
— **PP** — класс языков $L \subseteq \Sigma^*$, для которых существует функция $f \in \mathbf{GapP}$, такая, что $x \in L \Leftrightarrow f(x) > 0$ для любого $x \in \Sigma^*$;
— **SPP** — класс языков $L \subseteq \Sigma^*$, для которых существует функция $f \in \mathbf{GapP}$, такая, что $x \in L \Rightarrow f(x) = 1$ и $x \notin L \Rightarrow f(x) = 0$ для любого $x \in \Sigma^*$;
— $\mathbf{C_=P}$ — класс языков $L \subseteq \Sigma^*$, для которых существует функция $f \in \mathbf{GapP}$, такая, что $x \in L \Leftrightarrow f(x) = 0$ для любого $x \in \Sigma^*$;
— **WPP** — класс языков $L \subseteq \Sigma^*$, для которых существуют функции $f \in \mathbf{GapP}$ и $g \in \mathbf{FP}$, такие, что для любого $x \in \Sigma^*$ значение функции $g(x)$ отлично от нуля и $x \in L \Rightarrow f(x) = g(x)$ и $x \notin L \Rightarrow f(x) = 0$.

Для этих классов справедливы следующие важные соотношения [63]:

$$\mathbf{P} \subseteq \mathbf{UP} \subseteq \mathbf{SPP} \subseteq \mathbf{WPP} \subseteq \mathbf{C_=P} \subseteq \mathbf{PP},$$
$$\mathbf{co-NP} \subseteq \mathbf{C_=P},$$
$$\mathbf{NP} \subseteq \mathbf{co-C_=P} = \mathbf{NQP},$$
$$\mathbf{P} \subseteq \mathbf{EQP} \subseteq \mathbf{BQP} \subseteq \mathbf{WPP} \subseteq \mathbf{co-C_=P}.$$

Кроме того, в работе [67] доказано, что $\mathbf{PP} = \mathbf{PostBQP}$.

Исходя из определений, очевидными аналогами классов **NP** и **UP** представляются классы **PP** и **SPP** соответственно. При этом классы **PP** и $\mathbf{C_=P}$ размещают в иерархии классических классов вычислительной сложности на верхней границе квантовых вычислений, а класс **WPP** на сегодняшний день определяет безопасную границу для криптографии. Соответственно класс **SPP** является «плохим» аналогом для **UP**: перспективные криптографические алгоритмы желательно строить на базе **WPP** или даже $\mathbf{C_=P}$.

Следует отметить, что с теоретической точки зрения нет фундаментальных препятствий для построения криптографических алгоритмов на базе столь сложных клас-

сов, какими являются классы **WPP** и $\mathbf{C}_{=}\mathbf{P}$. Рассмотрим эквивалентное определение класса **PP**, не использующее класс **GapP**: **PP** — класс языков $L \subseteq \Sigma^*$, для которых существуют функции $f \in \#\mathbf{P}$ и $g \in \mathbf{FP}$, такие, что $x \in L \Leftrightarrow f(x) > g(x)$ для любого $x \in \Sigma^*$ [68]. Классические криптографические схемы предполагают, что легальные участники передачи информации A и B, зная некоторую секретную информацию K, могут легко решить задачу $f(x) > 0$, а для злоумышленника C, не имеющего доступа к информации K, решение задачи $f(x) > 0$ является трудным. В случае класса **PP** участники A и B могут выбирать функции $g \in \mathbf{FP} \subseteq \#\mathbf{P}$, удобные для отображения $f(x) - g(x) \to f'(x) \in \#\mathbf{P}$. В результате, зная некоторую секретную информацию K и функцию $g(x)$, A и B могут решить задачу $f'(x) > 0$, сложность которой сравнима со сложностью задачи $f(x) > 0$, т. е. находится на уровне **NP**. Злоумышленник C, не имеющий доступа к информации K, должен решать задачу $f(x) > g(x)$, сложность которой находится на уровне **PP**, или суметь демаскировать $f'(x)$ по $f(x)$ и $g(x)$. Таким образом, мы имеем ситуацию, которая с точки зрения вычислительной сложности совершенно аналогична схеме, предложенной в [2] и предполагающей, что злоумышленник либо должен решать **NP**-трудную задачу декодирования, либо демаскировать исходную матрицу G по матрице $G' = SGP$.

Естественно, между отсутствием фундаментальных препятствий и практической реализацией всегда имеется значительный разрыв, требующий построения соответствующей теории. Однако некоторую перспективу для разработки практического подхода для построения криптографических алгоритмов на базе класса **PP** можно проиллюстрировать на основе известных результатов для следующей проблемы.

Majority satisfiability (MajSAT)

Дано: Булева функция $f(x_1, x_2, \ldots, x_m)$.

Вопрос: Верно ли, что не менее половины наборов значений $x_j \in \{0, 1\}$, $1 \leqslant j \leqslant m$, позволяют получить $f(x_1, x_2, \ldots, x_m) = 1$?

В общем случае проблема MajSAT является **PP**-полной [69]. Если вместо произвольной булевой функции $f(x_1, x_2, \ldots, x_m)$ рассматривать 3-КНФ, то проблема MajSAT разрешима за полиномиальное время [70]. Кроме того, известны варианты MajSAT, которые являются **PP**-полными при ограничении функции $f(x_1, x_2, \ldots, x_m)$ на случай 3-КНФ, но требуют другой доли в общем количестве решений [71]. Таким образом, легальные участники передачи информации A и B могут представлять открытый текст в виде исходных данных проблемы MajSAT для 3-КНФ. Шифрование будет заключаться в преобразовании 3-КНФ в булеву функцию произвольного вида или другую 3-КНФ с другой долей решений. Хороший фундамент для маскировки булевых функций может предоставить шифрование логики [72–74], а преобразования, позволяющие изменять или сохранять долю решений, найти не представляет труда. Например, для произвольной булевой функции $f(x_1, x_2, \ldots, x_m)$ булева функция

$$(f(x_1, x_2, \ldots, x_m) \wedge x_{m+1}) \vee (f(x_1, x_2, \ldots, x_m) \wedge \neg x_{m+1})$$

имеет ровно в 2 раза больше решений, чем исходная.

Рассмотрим ряд непосредственных следствий из теоремы 1, позволяющих установить некоторые аналоги проблемы MLD для классов вычислительной сложности за пределами класса **NP** и представляющих интерес с точки зрения постквантовой криптографии. Сформулируем следующие проблемы.

DiffPM$_{=0}$

Дано: Графы $G_1 = (V_1, E_1)$, $G_2 = (V_2, E_2)$.

Вопрос: Верно ли, что количество множеств $M_1 \subseteq E_1$, таких, что каждая вершина графа G_1 инцидентна ровно одному ребру из множества M_1, равно количеству множеств $M_2 \subseteq E_2$, таких, что каждая вершина графа G_2 инцидентна ровно одному ребру из множества M_2?

DiffPM$_{>0}$

Дано: Графы $G_1 = (V_1, E_1)$, $G_2 = (V_2, E_2)$.

Вопрос: Верно ли, что количество множеств $M_1 \subseteq E_1$, таких, что каждая вершина графа G_1 инцидентна ровно одному ребру из множества M_1, больше количества множеств $M_2 \subseteq E_2$, таких, что каждая вершина графа G_2 инцидентна ровно одному ребру из множества M_2?

DiffPM$_{=g}$

Дано: Графы $G_1 = (V_1, E_1)$, $G_2 = (V_2, E_2)$, натуральное число k.

Обещание: Пусть X — количество множеств $M_1 \subseteq E_1$, таких, что каждая вершина графа G_1 инцидентна ровно одному ребру из множества M_1, Y — количество множеств $M_2 \subseteq E_2$, таких, что каждая вершина графа G_2 инцидентна ровно одному ребру из множества M_2. Известно, что $X = Y$ или $X = Y + k$.

Вопрос: Верно ли, что $X = Y + k$?

DiffMLD$_{=0}$

Дано: Двоичные матрицы $H_1 \in \mathbb{Z}_2^{m_1 \times n_1}$, $H_2 \in \mathbb{Z}_2^{m_1 \times n_1}$, векторы $s_1 \in \mathbb{Z}_2^{m_1}$, $s_2 \in \mathbb{Z}_2^{m_2}$, натуральные числа k_1 и k_2.

Вопрос: Верно ли, что количество попарно различных векторов $x \in \mathbb{Z}_2^{n_1}$, таких, что $H_1 x = s_1$ и $\mathrm{wt}(x) \leqslant k_1$, равно количеству попарно различных векторов $y \in \mathbb{Z}_2^{n_2}$, таких, что $H_2 y = s_2$ и $\mathrm{wt}(y)) \leqslant k_2$?

DiffMLD$_{>0}$

Дано: Двоичные матрицы $H_1 \in \mathbb{Z}_2^{m_1 \times n_1}$, $H_2 \in \mathbb{Z}_2^{m_1 \times n_1}$, векторы $s_1 \in \mathbb{Z}_2^{m_1}$, $s_2 \in \mathbb{Z}_2^{m_2}$, натуральные числа k_1 и k_2.

Вопрос: Верно ли, что количество попарно различных векторов $x \in \mathbb{Z}_2^{n_1}$, таких, что $H_1 x = s_1$ и $\mathrm{wt}(x) \leqslant k_1$, больше количества попарно различных векторов $y \in \mathbb{Z}_2^{n_2}$, таких, что $H_2 y = s_2$ и $\mathrm{wt}(y) \leqslant k_2$?

DiffMLD$_{=g}$

Дано: Двоичные матрицы $H_1 \in \mathbb{Z}_2^{m_1 \times n_1}$, $H_2 \in \mathbb{Z}_2^{m_1 \times n_1}$, векторы $s_1 \in \mathbb{Z}_2^{m_1}$, $s_2 \in \mathbb{Z}_2^{m_2}$, натуральные числа k_1, k_2, k.

Обещание: Пусть X — количество попарно различных векторов $x \in \mathbb{Z}_2^{n_1}$, таких, что $H_1 x = s_1$ и $\mathrm{wt}(x) \leqslant k_1$, Y — количество попарно различных векторов $y \in \mathbb{Z}_2^{n_2}$, таких, что $H_2 y = s_2$ и $\mathrm{wt}(y) \leqslant k_2$. Известно, что $X = Y$ или $X = Y + k$.

Вопрос: Верно ли, что $X = Y + k$?

Заметим, что в отличие от большинства классов вычислительной сложности, для определения которых достаточно использования одной функции f, определение класса **WPP** содержит функции f и g, что затрудняет формулировку естественных проблем для класса **WPP** при помощи традиционного определения того, что дано, и вопроса. Обычно формулировка проблемы для класса **WPP** включает не только исходные данные и вопрос, но и некоторое обещание выполнимости какого-то условия. Предполагается, что алгоритм, решающий проблему, получает на вход исходные данные. Алгоритм не знает, выполняется ли условие, содержащееся в обещании, для этих исходных данных, и не проверяет его выполнимость. Алгоритм, решающий проблему,

должен гарантировать правильность ответа, если условие выполняется. Если условие не выполняется, то алгоритм может выдать ошибочный ответ. В частности, алгоритм, решающий проблему DIFFMLD$_{=g}$, должен ориентироваться на обещание того, что $X = Y$ или $X = Y + k$, и ответить на вопрос о том, верно ли, что $X = Y + k$. Получив на вход исходные данные, алгоритм должен выдать ответ «Да», если $X = Y + k$; ответ «Нет», если $X = Y$; если ни одно из равенств $X = Y$ и $X = Y + k$ не выполняется, то алгоритм может выдать любой из ответов «Да» и «Нет» или вообще не выдать ответа, продолжая работать вечно.

В [75] доказано, что проблема DIFFPM$_{=0}$ является $\mathbf{C}_{=}\mathbf{P}$-полной. В работе [76] для проблем DIFFPM$_{>0}$ и DIFFPM$_{=g}$ показана полнота в классах **PP** и **WPP** соответственно. Из этих результатов и теоремы 1 непосредственно вытекает

Следствие 2. Проблемы DIFFMLD$_{=g}$, DIFFMLD$_{=0}$ и DIFFMLD$_{>0}$ являются полными в классах **WPP**, $\mathbf{C}_{=}\mathbf{P}$ и **PP** соответственно.

Заключение

В работе рассмотрен количественный аналог #MLD проблемы декодирования по принципу максимального правдоподобия MLD. Для проблемы MLD установлена экономная сводимость от проблемы совершенного паросочетания и слабо экономная сводимость от проблемы максимального разреза. Как следствие, мы получили #**P**-полноту проблемы #MLD. Кроме того, это позволило сформулировать вычислительно трудные аналоги проблемы декодирования по принципу максимального правдоподобия для классов вычислительной сложности, представляющих интерес с точки зрения постквантовой криптографии. В частности, доказана полнота проблем DIFFMLD$_{=g}$, DIFFMLD$_{=0}$ и DIFFMLD$_{>0}$ в классах **WPP**, $\mathbf{C}_{=}\mathbf{P}$ и **PP** соответственно. Кроме того, получено альтернативное доказательство **NP**-полноты проблемы MLD, что является дополнительным обоснованием надежности криптографических алгоритмов на основе Classic McEliece.

ЛИТЕРАТУРА

1. *Berlekamp E., McEliece R., and van Tilborg H.* On the inherent intractability of certain coding problems (Corresp.) // IEEE Trans. Inform. Theory. 1978. V. 24. No. 3. P. 384–386.
2. *McEliece R. J.* A public-key cryptosystem based on algebraic coding theory // Deep Space Network Progress Report. 1978. V. 42. No. 44. P. 114–116.
3. *Kichna A. and Farchane A.* A survey on various decoding algorithms for McEliece cryptosystem based on QC-MDPC codes // Proc. IRASET. Mohammedia, Morocco, 2023. P. 1–7.
4. *Liu J., Tong X., Wang Z., et al.* An improved McEliece cryptosystem based on QC-MDPC code with compact key size // Telecommun. Syst. 2022. V. 80. P. 17–32.
5. *Lau T. and Tan C.* On the design and security of Lee metric McEliece cryptosystems // Des. Codes Cryptogr. 2022. V. 90. No. 3. P. 695–717.
6. `https://www.nist.gov/programs-projects/post-quantum-cryptography`. 2024.
7. `https://classic.mceliece.org/`. 2024.
8. `https://web.archive.org/web/20171229103229/https://nts-kem.io/`. 2024.
9. *Niederreiter H.* Knapsack-type cryptosystems and algebraic coding theory // Problems Control Inform. Theory. 1986. V. 15. No. 2. P. 159–166.
10. *Dent A. W.* A designer's guide to KEMs // LNCS. 2003. V. 2898. P. 133–151.
11. *Fujisaki E. and Okamoto T.* Secure integration of asymmetric and symmetric encryption schemes // J. Cryptology. 2013. V. 26. No. 1. P. 80–101.

12. *Fujita H.* Quantum McEliece public-key cryptosystem // Quantum Inform. & Comput. 2012. V. 12. No. 3–4. P. 181–202.
13. *Oh Y., Jang K., Lim S., et al.* Quantum implementation of core operations in classic McEliece // Proc. PlatCon. Busan, Korea, 2023. P. 67–72.
14. *Fuentes P., Martinez J. E., Crespo P. M., and Garcia-Frias J.* Degeneracy and its impact on the decoding of sparse quantum codes // IEEE Access. 2021. V. 9. P. 89093–89119.
15. *Kubica A. and Vasmer M.* Single-shot quantum error correction with the three-dimensional subsystem toric code // Nat. Commun. 2022. V. 13. Article No. 6272.
16. *Kuo K.-Y. and Lai C.-Y.* Exploiting degeneracy in belief propagation decoding of quantum codes // npj Quantum Inform. 2022. V. 8. Article No. 111.
17. *Elbro F. and Majenz C.* An algebraic attack against McEliece-like cryptosystems based on BCH codes // Proc. ITW. Saint-Malo, France, 2023. P. 70–75.
18. *Gray H., Battarbee C., Shahandashti S. F., and Kahrobaei D.* A novel attack on McEliece's cryptosystem // Intern. J. Computer Math.: Computer Systems Theory. 2023. V. 8. No. 3. P. 178–191.
19. *Kirshanova E. and May A.* Breaking Goppa-based McEliece with hints // Inform. Comput. 2023. V. 293. Article No. 105045.
20. *Baldi M., Bianchi M., and Chiaraluce F.* Security and complexity of the McEliece cryptosystem based on quasi-cyclic low-density parity-check codes // IET Inform. Security. 2013. V. 7. No. 3. P. 212–220.
21. *Freudenberger J. and Thiers J. P.* A new class of Q-ary codes for the McEliece cryptosystem // Cryptography. 2021. V. 5. No. 1. Article No. 11.
22. *Mariot L., Picek S., and Yorgova R.* On McEliece-type cryptosystems using self-dual codes with large minimum weight // IEEE Access. 2023. V. 11. P. 43511–43519.
23. *Hsieh M.-H. and Le Gall F.* NP-hardness of decoding quantum error-correction codes // Phys. Rev. A. 2011. V. 83. Article No. 052331.
24. *Kuo K.-Y. and Lu C.-C.* On the hardness of decoding quantum stabilizer codes under the depolarizing channel // Intern. Symp. Inform. Theory and its Appl. Honolulu, USA, 2012. P. 208–211.
25. *Kuo K.-Y. and Lu C.-C.* On the hardnesses of several quantum decoding problems // Quantum Inf. Process. 2020. V. 19. Article No. 123.
26. *Iyer P. and Poulin D.* Hardness of decoding quantum stabilizer codes // IEEE Trans. Inform. Theory. 2015. V. 61. No. 9. P. 5209–5223.
27. *Kuo K.-Y. and Lai C.-Y.* The encoding and decoding complexities of entanglement-assisted quantum stabilizer codes // Proc ISIT. Paris, France, 2019. P. 2893–2897
28. *Chamberland C., Goncalves L., Sivarajah P., et al.* Techniques for combining fast local decoders with global decoders under circuit-level noise // Quantum Sci. Technology. 2023. V. 8. Article No. 045011.
29. *Hammar K., Orekhov A., Hybelius P. W., et al.* Error-rate-agnostic decoding of topological stabilizer codes // Phys. Rev. A. 2022. V. 105. Article No. 042616.
30. *Théveniaut H. and van Nieuwenburg E.* A NEAT quantum error decoder // SciPost Physics. 2021. V. 11. Article No. 005.
31. *Colomer L. D., Skotiniotis M., and Muñoz-Tapia R.* Reinforcement learning for optimal error correction of toric codes // Phys. Let. A. 2020. V. 384. No. 17. Article 126353.
32. *Sweke R., Kesselring M. S., van Nieuwenburg E. P. L., and Eisert J.* Reinforcement learning decoders for fault-tolerant quantum computation // Mach. Learn.: Sci. Technol. 2021. V. 2. Article No. 025005.

33. *Krastanov S. and Jiang L.* Deep neural network probabilistic decoder for stabilizer codes // Sci. Rep. 2017. V. 7. Article No. 11003.
34. *Baireuther P., Caio M. D., Criger B., et al.* Neural network decoder for topological color codes with circuit level noise // New J. Physics. 2019. V. 21. Article No. 013003.
35. *Gicev S., Hollenberg L. C. L., and Usman M.* A scalable and fast artificial neural network syndrome decoder for surface codes // Quantum. 2023. V. 7. Article No. 1058.
36. *Bordoni S. and Giagu S.* Convolutional neural network based decoders for surface codes // Quantum Inf. Process. 2023. V. 22. Article No. 151.
37. *Li A., Li F., Gan Q., and Ma H.* Convolutional-Neural-Network-Based hexagonal quantum error correction decoder // Appl. Sci. 2023. V. 13. No. 17. Article 9689.
38. *Wenger E., Chen M., Charton F., and Lauter K.* SALSA: Attacking Lattice Cryptography with Transformers. Cryptology ePrint Archive. 2022. Paper 2022/935. `https://eprint.iacr.org/2022/935`.
39. *Bruck J. and Naor M.* The hardness of decoding linear codes with preprocessing // IEEE Trans. Inform. Theory. 1990. V. 36. No. 2. P. 381–385.
40. *Dumer I., Micciancio D., and Sudan M.* Hardness of approximating the minimum distance of a linear code // IEEE Trans. Inform. Theory. 2003. V. 49. No. 1. P. 22–37.
41. *Vardy A.* The intractability of computing the minimum distance of a code // IEEE Trans. Inform. Theory. 1997. V. 43. No. 6. P. 1757–1766.
42. *Papadimitriou C. H.* Computational Complexity. Reading, Addison-Wesley, 1994. 523 p.
43. *Juban L.* Dichotomy theorem for the generalized unique satisfiability problem // LNCS. 1999. V. 1684. P. 327–337.
44. *Creignou N. and Hermann M.* Complexity of generalized satisfiability counting problems // Inform. Comput. 1996. V. 125. No. 1. P. 1–12.
45. *Valiant L. G.* The complexity of computing the permanent // Theoretical Computer Sci. 1979. V. 8. No. 2. P. 189–201.
46. *Barbanchon R.* On unique graph 3-colorability and parsimonious reductions in the plane // Theoretical Computer Sci. 2004. V. 319. No. 1–3. P. 455–482.
47. *Karp R. M.* Reducibility among combinatorial problems // R. E. Miller, J. W. Thatcher, and J. D. Bohlinger (eds.). Complexity of Computer Computations. The IBM Research Symposia Series. Boston: Springer, 1972. P. 85–103.
48. *Garey M. R. and Johnson D. S.* Computers and Intractability: A Guide to the Theory of NP-Completeness. San Francisco: Freeman, 1979. 338 p.
49. *Garey M. R., Johnson D. S., and Stockmeyer L.* Some simplified NP-complete graph problems // Theoretical Computer Sci. 1976. V. 1. No. 3. P. 237–267.
50. *Bruck J. and Blaum M.* Neural networks, error-correcting codes, and polynomials over the binary n-cube // IEEE Trans. Inform. Theory. 1989. V. 35. No. 5. P. 976–987.
51. *Барг С.* Некоторые новые NP-полные задачи кодирования // Проблемы передачи информации. 1994. Т. 30. № 3. С. 23–28.
52. *Jelínková E., Suchý O., Hliněný P., and Kratochvíl J.* Parameterized problems related to Seidel's switching // Discrete Math. Theoretical Computer Sci. 2011. V. 13. No. 2. P. 19–42.
53. *Tanatmis A.* Mathematical Programming Approaches for Decoding of Binary Linear Codes. Vom Fachbereich Mathematik der Technischen Universität Kaiserslautern zur Erlangung des akademischen Grades Doktor der Naturwissenschaften (Doctor rerum naturalium, Dr. rer. nat.) genehmigte Dissertation, 2011.
54. *Arora S., Babai L., Stern J., and Sweedyk Z.* The hardness of approximate optima in lattices, codes, and systems of linear equations // J. Computer System Sci. 1997. V. 54. No. 2. P. 317–331.

55. *Lindell Y.* Introduction to Coding Theory. `https://yehudalindell.com/teaching/introduction-to-coding-theory/`. 2024.
56. *Kaye P., Laflamme R., and Mosca M.* An Introduction to Quantum Computing. N.Y.: Oxford University Press, 2007. 274 p.
57. *Nielsen M. A. and Chuang I. L.* Quantum Computation and Quantum Information. Cambridge: Cambridge University Press, 2010. 676 p.
58. *Ceselli A. and Premoli M.* On good encodings for quantum annealer and digital optimization solvers // Sci. Rep. 2023. V. 13. Article No. 5628.
59. *Koch D., Cutugno M., Patel S., et al.* Variational amplitude amplification for solving QUBO problems // Quantum Rep. 2023. V. 5. No. 4. P. 625–658.
60. *Pokharel B., Izquierdo Z. G., Lott P. A., et al.* Inter-generational comparison of quantum annealers in solving hard scheduling problems // Quantum Inf. Process. 2023. V. 22. Article No. 364.
61. *Aggarwal D., Bennett H., Brakerski Z., et al.* Lattice problems beyond polynomial time // Proc. STOC'2023. Orlando, FL, USA, 2023. P. 1516–1526.
62. *Pass R., Tseng W. L. D., and Venkitasubramaniam M.* Towards non-black-box lower bounds in cryptography // LNCS. 2011. V. 6597. P. 579–596.
63. *Spakowski H., Thakur M., and Tripathi R.* Quantum and classical complexity classes: Separations, collapses, and closure properties // Inform. Comput. 2005. V. 200. No. 1. P. 1–34.
64. *Adleman L., DeMarrais J., and Huang M.* Quantum computability // SIAM J. Computing. 1997. V. 26. No. 5. P. 1524–1540.
65. *Bernstein E. and Vazirani U.* Quantum complexity theory // SIAM J. Computing. 1997. V. 26. No. 5. P. 1411–1473.
66. *Shor P. W.* Algorithms for quantum computation: discrete logarithms and factoring // Proc. 35th Ann. Symp. FOCS. Santa Fe, USA, 1994. P. 124–134.
67. *Aaronson S.* Quantum computing, postselection, and probabilistic polynomial-time // Proc. R. Soc. A. 2005. V. 461. P. 3473–3482.
68. *Ogiwara M. and Hemachandra L. A.* A complexity theory for feasible closure properties // J. Computer System Sci. 1993. V. 46. No. 3. P. 295–325.
69. *Gill J.* Computational complexity of probabilistic Turing machines // SIAM J. Computing. 1977. V. 6. No. 4. P. 675–695.
70. *Akmal S. and Williams R.* MAJORITY-3SAT (and related problems) in polynomial time // Proc. 62nd Ann. Symp. FOCS. Denver, USA, 2022. P. 1033–1043.
71. *Bailey D. D., Dalmau V., and Kolaitis P. G.* Phase transitions of PP-complete satisfiability problems // Discrete Appl. Math. 2007. V. 155. No. 12. P. 1627–1639.
72. *Chandra S. S., Kannan R. J., Balaji B. S., et al.* Efficient design and analysis of secure CMOS logic through logic encryption // Sci. Rep. 2023. V. 13. Article No. 1145.
73. *Liang J., Wang K., Xi W., et al.* SILL: Preventing structural attack for logic locking // IEICE Electronics Express. 2023. V. 20. No. 2. P. 1–6.
74. *Rajendran J. and Garg S.* Logic encryption // Forte D., Bhunia S., and Tehranipoor M. M. (eds.). Hardware Protection through Obfuscation. Cham: Springer, 2017. P. 71–88.
75. *Curticapean R.* The simple, little and slow things count: On parameterized counting complexity. Dissertation for Obtaining the Title of Doctor rerum naturalium (Dr. rer. nat) of the Faculties of Natural Sciences and Technology of Saarland University, Saarbrücken, 2015.
76. *Bakali E., Chalki A., Kanellopoulos S., et al.* On the Power of Counting the Total Number of Computation Paths of NPTMs. `https://arxiv.org/abs/2306.11614`. 2024.

REFERENCES

1. *Berlekamp E., McEliece R., and van Tilborg H.* On the inherent intractability of certain coding problems (Corresp.). IEEE Trans. Inform. Theory, 1978, vol. 24, no. 3, pp. 384–386.
2. *McEliece R. J.* A public-key cryptosystem based on algebraic coding theory. Deep Space Network Progress Report, 1978, vol. 42, no. 44, pp. 114–116.
3. *Kichna A. and Farchane A.* A survey on various decoding algorithms for McEliece cryptosystem based on QC-MDPC codes. Proc. IRASET, Mohammedia, Morocco, 2023, pp. 1–7.
4. *Liu J., Tong X., Wang Z., et al.* An improved McEliece cryptosystem based on QC-MDPC code with compact key size. Telecommun. Syst., 2022, vol. 80, pp. 17–32.
5. *Lau T. and Tan C.* On the design and security of Lee metric McEliece cryptosystems. Des. Codes Cryptogr., 2022, vol. 90, no. 3, pp. 695–717.
6. `https://www.nist.gov/programs-projects/post-quantum-cryptography`. 2024.
7. `https://classic.mceliece.org/`. 2024.
8. `https://web.archive.org/web/20171229103229/https://nts-kem.io/`. 2024.
9. *Niederreiter H.* Knapsack-type cryptosystems and algebraic coding theory. Problems Control Inform. Theory, 1986, vol. 15, no. 2, pp. 159–166.
10. *Dent A. W.* A designer's guide to KEMs. LNCS, 2003, vol. 2898, pp. 133–151.
11. *Fujisaki E. and Okamoto T.* Secure integration of asymmetric and symmetric encryption schemes. J. Cryptology, 2013, vol. 26, no. 1, pp. 80–101.
12. *Fujita H.* Quantum McEliece public-key cryptosystem. Quantum Inform. & Comput., 2012, vol. 12, no. 3–4, pp. 181–202.
13. *Oh Y., Jang K., Lim S., et al.* Quantum implementation of core operations in classic McEliece. Proc. PlatCon, Busan, Korea, 2023, pp. 67–72.
14. *Fuentes P., Martinez J. E., Crespo P. M., and Garcia-Frias J.* Degeneracy and its impact on the decoding of sparse quantum codes. IEEE Access, 2021, vol. 9, pp. 89093–89119.
15. *Kubica A. and Vasmer M.* Single-shot quantum error correction with the three-dimensional subsystem toric code. Nat. Commun., 2022, vol. 13, article no. 6272.
16. *Kuo K.-Y. and Lai C.-Y.* Exploiting degeneracy in belief propagation decoding of quantum codes. npj Quantum Inform., 2022, vol. 8, article no. 111.
17. *Elbro F. and Majenz C.* An algebraic attack against McEliece-like cryptosystems based on BCH codes. Proc. ITW, Saint-Malo, France, 2023, pp. 70–75.
18. *Gray H., Battarbee C., Shahandashti S. F., and Kahrobaei D.* A novel attack on McEliece's cryptosystem. Intern. J. Computer Math.: Computer Systems Theory, 2023, vol. 8, no. 3, pp. 178–191.
19. *Kirshanova E. and May A.* Breaking Goppa-based McEliece with hints. Inform. Comput., 2023, vol. 293, article no. 105045.
20. *Baldi M., Bianchi M., and Chiaraluce F.* Security and complexity of the McEliece cryptosystem based on quasi-cyclic low-density parity-check codes. IET Inform. Security, 2013, vol. 7, no. 3, pp. 212–220.
21. *Freudenberger J. and Thiers J. P.* A new class of Q-ary codes for the McEliece cryptosystem. Cryptography, 2021, vol. 5, no. 1, article no. 11.
22. *Mariot L., Picek S., and Yorgova R.* On McEliece-type cryptosystems using self-dual codes with large minimum weight. IEEE Access, 2023, vol. 11, pp. 43511–43519.
23. *Hsieh M.-H. and Le Gall F.* NP-hardness of decoding quantum error-correction codes. Phys. Rev. A, 2011, vol. 83, article no. 052331.

24. *Kuo K.-Y. and Lu C.-C.* On the hardness of decoding quantum stabilizer codes under the depolarizing channel. Intern. Symp. Inform. Theory and its Appl., Honolulu, USA, 2012, pp. 208–211.
25. *Kuo K.-Y. and Lu C.-C.* On the hardnesses of several quantum decoding problems. Quantum Inf. Process., 2020, vol. 19, article no. 123.
26. *Iyer P. and Poulin D.* Hardness of decoding quantum stabilizer codes. IEEE Trans. Inform. Theory, 2015, vol. 61, no. 9, pp. 5209–5223.
27. *Kuo K.-Y. and Lai C.-Y.* The encoding and decoding complexities of entanglement-assisted quantum stabilizer codes. Proc ISIT, Paris, France, 2019, pp. 2893–2897
28. *Chamberland C., Goncalves L., Sivarajah P., et al.* Techniques for combining fast local decoders with global decoders under circuit-level noise. Quantum Sci. Technology, 2023, vol. 8, article no. 045011.
29. *Hammar K., Orekhov A., Hybelius P. W., et al.* Error-rate-agnostic decoding of topological stabilizer codes. Phys. Rev. A, 2022, vol. 105, article no. 042616.
30. *Théveniaut H. and van Nieuwenburg E.* A NEAT quantum error decoder. SciPost Physics, 2021, vol. 11, article no. 005.
31. *Colomer L. D., Skotiniotis M., and Muñoz-Tapia R.* Reinforcement learning for optimal error correction of toric codes. Phys. Let. A, 2020, vol. 384, no. 17. Article 126353.
32. *Sweke R., Kesselring M. S., van Nieuwenburg E. P. L., and Eisert J.* Reinforcement learning decoders for fault-tolerant quantum computation. Mach. Learn.: Sci. Technol, 2021, vol. 2, article no. 025005.
33. *Krastanov S. and Jiang L.* Deep neural network probabilistic decoder for stabilizer codes. Sci. Rep., 2017, vol. 7, article no. 11003.
34. *Baireuther P., Caio M. D., Criger B., et al.* Neural network decoder for topological color codes with circuit level noise. New J. Physics, 2019, vol. 21, article no. 013003.
35. *Gicev S., Hollenberg L. C. L., and Usman M.* A scalable and fast artificial neural network syndrome decoder for surface codes. Quantum, 2023, vol. 7, article no. 1058.
36. *Bordoni S. and Giagu S.* Convolutional neural network based decoders for surface codes. Quantum Inf. Process., 2023, vol. 22, article no. 151.
37. *Li A., Li F., Gan Q., and Ma H.* Convolutional-Neural-Network-Based hexagonal quantum error correction decoder. Appl. Sci., 2023, vol. 13, no. 17, article 9689.
38. *Wenger E., Chen M., Charton F., and Lauter K.* SALSA: Attacking Lattice Cryptography with Transformers. Cryptology ePrint Archive, 2022, paper 2022/935, `https://eprint.iacr.org/2022/935`.
39. *Bruck J. and Naor M.* The hardness of decoding linear codes with preprocessing. IEEE Trans. Inform. Theory. 1990, vol. 36, no. 2, pp. 381–385.
40. *Dumer I., Micciancio D., and Sudan M.* Hardness of approximating the minimum distance of a linear code. IEEE Trans. Inform. Theory, 2003, vol. 49, no. 1, pp. 22–37.
41. *Vardy A.* The intractability of computing the minimum distance of a code. IEEE Trans. Inform. Theory, 1997, vol. 43, no. 6, pp. 1757–1766.
42. *Papadimitriou C. H.* Computational Complexity. Reading, Addison-Wesley, 1994. 523 p.
43. *Juban L.* Dichotomy theorem for the generalized unique satisfiability problem. LNCS, 1999, vol. 1684, pp. 327–337.
44. *Creignou N. and Hermann M.* Complexity of generalized satisfiability counting problems. Inform. Comput., 1996, vol. 125, no. 1, pp. 1–12.
45. *Valiant L. G.* The complexity of computing the permanent. Theoretical Computer Sci., 1979, vol. 8, no. 2, pp. 189–201.

46. *Barbanchon R.* On unique graph 3-colorability and parsimonious reductions in the plane. Theoretical Computer Sci., 2004, vol. 319, no. 1–3, pp. 455–482.
47. *Karp R. M.* Reducibility among combinatorial problems. R. E. Miller, J. W. Thatcher, and J. D. Bohlinger (eds.). Complexity of Computer Computations. The IBM Research Symposia Series, Boston, Springer, 1972, pp. 85–103.
48. *Garey M. R. and Johnson D. S.* Computers and Intractability: A Guide to the Theory of NP-Completeness. San Francisco, Freeman, 1979, 338 p.
49. *Garey M. R., Johnson D. S., and Stockmeyer L.* Some simplified NP-complete graph problems. Theoretical Computer Sci., 1976, vol. 1, no. 3, pp. 237–267.
50. *Bruck J. and Blaum M.* Neural networks, error-correcting codes, and polynomials over the binary n-cube. IEEE Trans. Inform. Theory, 1989, vol. 35, no. 5, pp. 976–987.
51. *Barg S.* Nekotorye novye NP-polnye zadachi kodirovaniya [Some new NP-complete coding problems]. Problemy Peredachi Informatsii, 1994, vol. 30, no. 3, pp. 23–28. (in Russian)
52. *Jelínková E., Suchý O., Hliněný P., and Kratochvíl J.* Parameterized problems related to Seidel's switching. Discrete Math. Theoretical Computer Sci., 2011, vol. 13, no. 2, pp. 19–42.
53. *Tanatmis A.* Mathematical Programming Approaches for Decoding of Binary Linear Codes. Vom Fachbereich Mathematik der Technischen Universität Kaiserslautern zur Erlangung des akademischen Grades Doktor der Naturwissenschaften (Doctor rerum naturalium, Dr. rer. nat.) genehmigte Dissertation, 2011.
54. *Arora S., Babai L., Stern J., and Sweedyk Z.* The hardness of approximate optima in lattices, codes, and systems of linear equations. J. Computer System Sci., 1997, vol. 54, no. 2, pp. 317–331.
55. *Lindell Y.* Introduction to Coding Theory. `https://yehudalindell.com/teaching/introduction-to-coding-theory/`, 2024.
56. *Kaye P., Laflamme R., and Mosca M.* An Introduction to Quantum Computing. N.Y., Oxford University Press, 2007, 274 p.
57. *Nielsen M. A. and Chuang I. L.* Quantum Computation and Quantum Information. Cambridge, Cambridge University Press, 2010, 676 p.
58. *Ceselli A. and Premoli M.* On good encodings for quantum annealer and digital optimization solvers. Sci. Rep., 2023, vol. 13, article no. 5628.
59. *Koch D., Cutugno M., Patel S., et al.* Variational amplitude amplification for solving QUBO problems. Quantum Rep., 2023, vol. 5, no. 4, pp. 625–658.
60. *Pokharel B., Izquierdo Z. G., Lott P. A., et al.* Inter-generational comparison of quantum annealers in solving hard scheduling problems. Quantum Inf. Process., 2023, vol. 22, article no. 364.
61. *Aggarwal D., Bennett H., Brakerski Z., et al.* Lattice problems beyond polynomial time. Proc. STOC'2023, Orlando, FL, USA, 2023, pp. 1516–1526.
62. *Pass R., Tseng W. L. D., and Venkitasubramaniam M.* Towards non-black-box lower bounds in cryptography. LNCS, 2011, vol. 6597, pp. 579–596.
63. *Spakowski H., Thakur M., and Tripathi R.* Quantum and classical complexity classes: Separations, collapses, and closure properties. Inform. Comput., 2005, vol. 200, no. 1, pp. 1–34.
64. *Adleman L., DeMarrais J., and Huang M.* Quantum computability. SIAM J. Computing, 1997, vol. 26, no. 5, pp. 1524–1540.
65. *Bernstein E. and Vazirani U.* Quantum complexity theory. SIAM J. Computing, 1997, vol. 26, no. 5, pp. 1411–1473.
66. *Shor P. W.* Algorithms for quantum computation: discrete logarithms and factoring. Proc. 35th Ann. Symp. FOCS, Santa Fe, USA, 1994, pp. 124–134.

67. *Aaronson S.* Quantum computing, postselection, and probabilistic polynomial-time. Proc. R. Soc. A, 2005, vol. 461, pp. 3473–3482.
68. *Ogiwara M. and Hemachandra L. A.* A complexity theory for feasible closure properties. J. Computer System Sci., 1993, vol. 46, no. 3, pp. 295–325.
69. *Gill J.* Computational complexity of probabilistic Turing machines. SIAM J. Computing. 1977, vol. 6, no. 4, pp. 675–695.
70. *Akmal S. and Williams R.* MAJORITY-3SAT (and related problems) in polynomial time. Proc. 62nd Ann. Symp. FOCS, Denver, USA, 2022, pp. 1033–1043.
71. *Bailey D. D., Dalmau V., and Kolaitis P. G.* Phase transitions of PP-complete satisfiability problems. Discrete Appl. Math., 2007, vol. 155, no. 12, pp. 1627–1639.
72. *Chandra S. S., Kannan R. J., Balaji B. S., et al.* Efficient design and analysis of secure CMOS logic through logic encryption. Sci. Rep., 2023, vol. 13, article no. 1145.
73. *Liang J., Wang K., Xi W., et al.* SILL: Preventing structural attack for logic locking. IEICE Electronics Express, 2023, vol. 20, no. 2, pp. 1–6.
74. *Rajendran J. and Garg S.* Logic encryption. Forte D., Bhunia S., and Tehranipoor M. M. (eds.). Hardware Protection through Obfuscation. Cham, Springer, 2017, pp. 71–88.
75. *Curticapean R.* The simple, little and slow things count: On parameterized counting complexity. Dissertation for Obtaining the Title of Doctor rerum naturalium (Dr. rer. nat) of the Faculties of Natural Sciences and Technology of Saarland University, Saarbrücken, 2015.
76. *Bakali E., Chalki A., Kanellopoulos S., et al.* On the Power of Counting the Total Number of Computation Paths of NPTMs. `https://arxiv.org/abs/2306.11614`. 2024.