Министерство науки и высшего образования Российской Федерации ФГАОУ ВО «Балтийский федеральный университет имени Иммануила Канта»

УТВЕРЖДАЮ
ректор БФУ им. И. Канта
_____ А.А. Фёдоров
«__»_____ 2022 года

Отчет
о научно-исследовательской работе _____ этап
“Алгоритмы нахождения короткого вектора в алгебраических решетках”
(договор на выполнение НИР № 2165 от 8 октября 2021 года)

Исполнитель _____

Согласовано:
Проректор по научной работе
_____ М.В. Дёмин

Руководитель проекта
_____ Е.А. Киршанова

Калининград
2021

Оптимизации алгоритмов, связанных с редукцией решёток.

А.С. Каренин

9 марта 2022 г.

1 Введение

В настоящее время в целях практического криптоанализа криптосистем за звание наиболее эффективного алгоритма борются BKZ алгоритм [CN11] и алгоритм просеивания [ADH+19]. Алгоритм просеивания использует оракул SVP, дающий доступ к кратчайшему вектору в подрешётке. Этот оракул может быть либо уже упомянутым BKZ (или его HKZ вариантом), либо алгоритмом перечисления.

Оба подхода к нахождению коротких векторов могут быть оптимизированы. В данном отчёте рассматривается возможность оптимизации BKZ редукции при помощи спуска при помощи отображения нормы [KF17] [DMHS20] и оптимизация процесса Грама - Шмидта в случае циркулянтных решёток (решёток с базисом, задаваемых антициркулянтной матрицей). Также в библиотеке G6K для вызова алгоритма просеивания используется подход dimensions for free, суть которого заключается в том, что если мы нашли кратчайший вектор в подрешётки размерности $n/\log(n)$, то при помощи Babai Nearest Plane алгоритма мы можем подняться в исходную решётку размерности n и получить достаточно короткий вектор. Поэтому в данном отчёте также рассматривается и этот алгоритм.

2 Спуск при помощи нормы

Пусть $d = 2^n \in \mathbb{N}$, $d'|d$, а $L = \frac{\mathbb{Q}[x]}{\left(x^d-1\right)}, K = \frac{\mathbb{Q}[x]}{\left(x^{d'}-1\right)}$ два циклотомических числовых поля, причём K является подполем в L. Обозначим за $Gal_{L/K}$ группу Галуа поля L над K. Тогда её мощность будет равна d/d'. Согласно свойствам расширений Галуа для некоторого $a \in K$ справедливо, что произведение всех значений автоморфизмов из $Gal_{L/K}$ от элемента a лежит в подполе K:

$$\prod_{\sigma \in Gal_{L/K}} \sigma(a) \in K.$$

С другой стороны, NTRU решётки могут быть представлены как свободный модуль $h \cdot \mathcal{O}_L + q \cdot \mathcal{O}_L \bigoplus \mathcal{O}_L$, где $h \in L$, q - простое число, а $\mathcal{O}_L$ - кольцо целых числового поля L. Естественным образом возникает вопрос: возможно ли перейти при помощи отображения нормы в модуль $\left(N_{L/K}(h) \cdot \mathcal{O}_L + q \cdot \mathcal{O}_K\right) \bigoplus \mathcal{O}_K$? Действительно, отображение нормы переводит кольцо целых $\mathcal{O}_L$ поля L в кольцо целых $\mathcal{O}_K$ подполя K. На $q \in \mathbb{N}$ отображение нормы действует как тождественное отображение. Норма является мультипликативным отображением: $N_{L/K}(a \cdot b) = N_{L/K}(a) \cdot N_{L/K}(b)$, а на элементы свободного модуля действует покомпонентно, поэтому имеем:

$$N_{L/K}\left((h \cdot \mathcal{O}_L + q \cdot \mathcal{O}_L) \bigoplus \mathcal{O}_L\right) \subset N_{L/K}(h \cdot \mathcal{O}_K + q \cdot \mathcal{O}_K) \bigoplus \mathcal{O}_K. \quad (1)$$

Несложно проверить, обнулив h или q до выноса кольца целых за скобки, что модуль $(N_{L/K}(h)+q)\cdot\mathcal{O}_K \bigoplus \mathcal{O}_K$ является его подмодулем. Таким образом, если мы найдём короткие векторы в последнем, мы получим короткие векторы из предыдущего.

Группа Галуа $Gal_{L/K}$ для числовых полей L, K, имеющих индексом над $\mathbb{Q}$ степени двойки состоит из автоморфизмов:

$$Gal_{L/K} = \left\{ \sigma_s : L \to L : \sum_{0\leqslant i<2^n} a^i \cdot x^i \mapsto \sum_{0\leqslant i<2^n} a^i \cdot x^{i\cdot s} \mid s \equiv 0 \pmod{2^{d'}} \right\} \tag{2}$$

Вспомним, что NTRU решётка с вектор строками имеет вид:

$$\begin{pmatrix} q\boldsymbol{I}_{2^n} & \boldsymbol{0}_{2^n} \\ \mathrm{rot}(\boldsymbol{h}) & \boldsymbol{I}_{2^n} \end{pmatrix}$$

Тогда решётка, соответствующая подмодулю $(N_{L/K}(h)+q)\cdot\mathcal{O}_K \bigoplus \mathcal{O}_K$ модуля (1) имеет следующий вид:

$$\begin{pmatrix} q\boldsymbol{I}_{2^{n-1}} & \boldsymbol{0}_{2^{n-1}} \\ \mathrm{rot}(N_{L/K}(\boldsymbol{h})) & \boldsymbol{I}_{2^{n-1}} \end{pmatrix}.$$

В рамках данного исследования был раеализованы алгоритмы, находящие относительную группу Галуа $Gal_{L/K}$ для циклотомических полей со степенью, равной степени 2, применяющие её элементы к некоторому $a \in L$ и перемножающие результат, что на выходе возвращает $N_{L/K}(a)$. Реализация алгоритмов на языке python доступна по запросу на почту ASKarenin@stud.kantiana.ru.

3 Процесс Грама-Шмидта при помощи быстрого преобразования Фурье

Для достижения ускорения редукции решётки можно воспользоваться альтернативным подходом: редукции при помощи просеивания. Благодаря существованию алгебраической структуры (геометрически выражающейся в том, что базис решётки представляет собой антициркулянтную матрицу) мы можем перейти в домен Фурье при помощи быстрого преобразования Фурье (или FFT).

3.1 GSO и LDR* декомпозиции

Пусть $\boldsymbol{B}$ - матрица размера $2d \times 2d$, состоящая из вектор строк базиса решётки $\mathcal{L}$. Из этого сразу же следует её невырожденность, поэтому мы можем рассмотреть GSO декомпозицию:

$$\boldsymbol{B} = \boldsymbol{L} \cdot \widetilde{\boldsymbol{B}}, \tag{3}$$

где $\boldsymbol{L}$ - единично-нижнетреугольная (нижнетреугольная матрица с единицами по диагонали), а $\widetilde{\boldsymbol{B}}$ - ортогональная матрица. Необходимым условием существования[1] такого разложения является положительная определённость $\boldsymbol{B}$. Дадим более формальное объяснения понятия "положительная определённость".

Пусть $h(x) \in \mathbb{Q}(x)$ - унитарный многочлен с различными комплексными корнями. Введём понятие эрмитова сопряжения элемента $a \in L = \frac{\mathbb{Q}[x]}{\left(x^d-1\right)}$. Эрмитовым сопряжением элемента a называется элемент $b \in L$, такой, что для любого корня ζ многочлена $h(x)$ верно: $a^*(\zeta) = \overline{a(\zeta)}$, где $\overline{a}$ - комплексно сопряжённый к a элемент. Сопряжение матрицы положим равным транспонированию матрицы из сопряжённых элементов.

[1] Наверное, корректности

Назовём матрицу $\boldsymbol{G}$ называется матрицей Грама, если она невырождена и существует некоторое разложение $\boldsymbol{B} \cdot \boldsymbol{B}^*$. Матрицы, обладающие этим свойством, расширяют понятие положительной определённости.

LDL* декомпозиция записывает положительно определённую матрицу как произведение $\boldsymbol{B} = \boldsymbol{L}\boldsymbol{D}\boldsymbol{L}^*$, где L - единично-нижнетреугольная, а D - диагональная. Можно доказать, что $\widetilde{\boldsymbol{B}}$ является GSO разложением матрицы $\boldsymbol{B}$ тогда и только тогда $\boldsymbol{L} \cdot (\boldsymbol{B}\boldsymbol{B}^*)\, \boldsymbol{L}^*$ - её LDL* разложение.

3.2 Операторы линеаризации и их построение

Суть операторов линеаризации заключается в представлении умножения элементов числового поля при помощи умножения векторов и матриц. В этом пункте рассматривается построение оператора векторизации $V_{d/d'}$ и матрификации $M_{d/d'}$.

Для числовых полей $L/K : [L : K] = k$ мы можем рассмотреть L как K-модуль ранга k.

Определение: пусть натуральное d раскладывается в произведение h необязательно различных простых множителей. Тогда обозначим $d_h := d$ для $1 \leqslant i < h$ и положим $d_i := \mathrm{gpd}(d_i)$, где $\mathrm{gpd}(d)$ - наибольший собственный делитель d.

Таким образом при помощи предыдущего определения мы ввели понятие башни делителей числа d.

Определение: Пусть $d, d' \in \mathbb{N}$ такие, что d' принадлежит башне делителей числа d. Положим $k := d/d'$. Обозначим за x неизвестную многочлена из $R_d = \frac{\mathbb{Q}[x]}{\left(x^d-1\right)}$, а за $y = x^k$ - переменную многочлена из $R_d = \frac{\mathbb{Q}[x]}{\left(x^{d'}-1\right)}$. Определим частичную линеаризацию $V_{d/d'} : R_d^m \to R_{d'}^{km}$.

- Для $d = d' = 1$ оператор $V_{d/d'}$ - тождественное отображение.
- Для $d = gpd(d)$ и элемента $a \in R_d$ положим $a = \sum_{i \in \mathbb{Z}_k} x^i a_i(y)$. Тогда $V_{d/d'}(a) := (a_0, \ldots, a_{k-1})$.
- Для векторов из свободных модулей применение оператора - покомпонентное.
- Для $d''|d'|d$ определим оператор рекурсивно: $V_{d/d''} = V_{d/d'} \circ V_{d'/d''}$.

Такой подход к определению оператора линеаризации продиктован необходимостью обобщения Radix-2 порядка используемого в алгоритме FFT.

Также, в статье [DP15] описан алгоритм построения оператора матрификации. Имея доступ к нему, мы можем провести LDL* декомпозицию базиса в FFT виде.

3.3 Сравнение скорости работы Babai Nearest Plane с реализацией в библиотеке fplll

В статье [DP15] описан подход к нахождению LDL* декомпозиции в домене Фурье. Выходом этого алгоритма является дерево, проиндексированное нижнетреугольными матрицами L_{d_i}, на основе которого можно эффективно переходить между базисом B исходной решётки и базисом $\widetilde{B}$ - ортогональным, полученным в рамках процесса Грама - Шмидта, что даёт возможность ускорения алгоритма Babai Nearest Plane.

Ниже приведена таблица, сравнивающая скорость выполнения 1000 вызовов алгоритма на решётке, заданой над кольцом конволюции $R_d = \mathbb{Q}[x]/(x^d - 1)$, где размерность d решётки была выбрана равной 512. В первом эксперименте алгоритм запускался на случайном базисе над R_d. Во втором эксперименте брался вектор $f \in \mathbb{Q}[x]/(x^{d/2} + 1)$ и вкладывался в R_d при помощи канонического вложения. При этом эффективная размерность вектора f равна половине размерности d, а именно 256 для данного эксперимента.

Базовое кольцо	fpylll, с.	Ducas & Prest, с.
$\mathbb{Q}[x]/(x^d - 1)$	180.80	16.46
$\mathbb{Q}[x]/(x^{d/2} + 1)$	73.91	17.28

Таблица 1: Сравнение скорости работы алгоритма Babai Nearest Plane в реализации в библиотеке fplll с вариантом реализации [DP15].

Код, реализующий эксперимент на языке python, доступен по запросу на почту ASKarenin@stud.kantiana.ru.

3.4 Ускорение нахождения длины проекции ротации на вектор Грама-Шмидта

Для нужд алгоритмов просеивания полезно уметь быстро вычислять норму векторов [2]. Наивно это делается при помощи перемножения канонических координат вектора с матрицей, задающей базис решётки, после чего подсчитывается длина результирующего вектора. Однако, в NTRU решётках мы знаем, что вместе с вектором v там содержатся также и n его ротаций $x^i v, 0 \leqslant i < n$. Естественным образом возникает вопрос: можно ли эффективно посчитать нормы проекций всех его ротаций?

Сделать это можно за $O(n^2 \log n)$, просто перемножив в FFT формате блочно-диагональную матрицу из n блоков-ротаций вектора v на вектор столбец b^* ортогонализированного базиса Грама Шмидта, таким образом получив числитель в выражении:

$$w_{i,j} = \frac{< x^j \cdot v, b_i^* >}{||b_i^*||^2} \tag{4}$$

Формально, для нахождения всех длин проекций ротаций вектора v на векторы b_i^* Грама - Шмидта достаточно умножить блочно диагональную матрицу и вектор следующих видов:

$$\begin{pmatrix} \mathrm{rot}(v) & 0 & \dots & 0 \\ 0 & \mathrm{rot}(v) & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & \mathrm{rot}(v) \end{pmatrix} \cdot \begin{pmatrix} b_0^* \\ b_1^* \\ \vdots \\ b_n^* \end{pmatrix}$$

Благодаря циркулянтной структуре блоков на диагонали матрицы, а также её разрежённости, благодаря FFT мы можем эффективно найти это произведение.

4 Заключение

По результатам работы был проверен и большей частью реализован самостоятельно подход Л. Дюки и Т. Преста к ускорению алгоритма Babai Nearest Plane. Полученные теоретические результаты в возможности быстрого доступа к векторам Грама -

[2] корректнее сказать их проекцций на ГШ базис?

Шмидта и матрице L в LDL* декомпозиции потенциально могут вести к возможности ускорения LLL - алгоритма с использованием FFT.

Другим направлением оптимизации является ускорение нахождения длин ротаций векторов в алгоритмах просеивания: на данный момент в реализации просеивания в библиотеке G6K для определения длины проекций векторов кандидатов на базис Грама - Шмидта используется алгоритм ортогонализации, имеющий вычислительную сложность $O(n^3)$, где n - размерность решётки. Описанный в данном отчёте подход может ускорить асимптотику до $O(n^2 \log(n))$.

Главным препятствием для реализации LLL алгоритма в домене Фурье является необходимость положительной определённости матрицы G, подаваемой на вход LLL алгоритма. Чтобы это свойство выполнялось, мы находим G как $B \cdot B^*$, где * означает Эрмитово сопряжение и последующее транспонирование матрицы. Само это умножение должно быть эффективно реализовано для удержания асимптотики в рамках требуемых $O(n^2 \log(n))$ операций.

Также перспективным направлением оптимизации LLL алгоритма и просеивания является возможность обновление LDL* дерева без необходимости его полного пересчёта. При построении этого дерева используется стратегия “разделяй и влавствуй”, поэтому при изменении вершины дерева затрагиваются только её вершины потомки.

Данные результаты по завершению реализации быстрой ортогонализации Грама - Шмидта и её встраиванию в библиотеке G6K составляют практический интерес и могут быть поданы в рамках соответствующей научной статьи.

Список литературы

[ADH+19] Martin R. Albrecht, Léo Ducas, Gottfried Herold, Elena Kirshanova, Eamonn W. Postlethwaite, and Marc Stevens. The general sieve kernel and new records in lattice reduction. Cryptology ePrint Archive, Report 2019/089, 2019. `https://ia.cr/2019/089`.

[CN11] Yuanmi Chen and Phong Nguyen. Bkz 2.0: Better lattice security estimates. volume 7073, pages 1–20, 12 2011.

[DMHS20] Gabrielle De Micheli, Nadia Heninger, and Barak Shani. Characterizing overstretched ntru attacks. *Journal of Mathematical Cryptology*, 14(1):110–119, 2020.

[DP15] Léo Ducas and Thomas Prest. Fast fourier orthogonalization. Cryptology ePrint Archive, Report 2015/1014, 2015. `https://ia.cr/2015/1014`.

[KF17] Paul Kirchner and Pierre-Alain Fouque. Revisiting lattice attacks on overstretched ntru parameters. In *Advances in Cryptology – EUROCRYPT 2017*, pages 3–26, 2017.