О сложности двумерной задачи дискретного логарифмирования в группе точек эллиптической кривой с эффективным автоморфизмом порядка 6

Николаев Максим Владимирович
Научный руководитель: к.ф.-м.н. Матюхин Дмитрий Викторович

28 марта, 2013

Определения

- *Определение 1. Задача Дискретного логарифмирования.*
  Дано: группа $G = \langle P \rangle$, $\mathrm{ord}(P) = r$, $Q \in G$.
  Найти: $n \in \{0, ..., r-1\}$ *такое, что* $Q = nP$.

Определения

- *Определение 1. Задача Дискретного логарифмирования.*
  Дано: группа $G = \langle P \rangle$, $\mathrm{ord}(P) = r$, $Q \in G$.
  Найти: $n \in \{0, ..., r-1\}$ *такое, что* $Q = nP$.
- *Определение 2. Двумерная Задача Дискретного логарифмирования.*
  Дано: группа G; $P_1, P_2, Q \in G$, $N_1, N_2 \in \mathbb{N}$, $Q = n_1 P_1 + n_2 P_2$ *для некоторых (неизвестных)* $n_1 \in \{-N_1, \ldots, N_1\}$, $n_2 \in \{-N_2, \ldots, N_2\}$.
  Найти: n_1, n_2 *такие, что* $Q = n_1 P_1 + n_2 P_2$.

Алгоритм решения двумерной задачи дискретного логарифмирования (Gaudry, Schost, 2004)

- Построение Дикого и Домашнего множеств

$$T = \{-N_1, \ldots, N_1\} \times \{-N_2, \ldots, N_2\},$$

$$W = \{-N_1 + n_1, \ldots, N_1 + n_1\} \times \{-N_2 + n_2, \ldots, N_2 + n_2\}.$$

Алгоритм решения двумерной задачи дискретного логарифмирования (Gaudry, Schost, 2004)

- Построение Дикого и Домашнего множеств

$$T = \{-N_1, \ldots, N_1\} \times \{-N_2, \ldots, N_2\},$$

$$W = \{-N_1 + n_1, \ldots, N_1 + n_1\} \times \{-N_2 + n_2, \ldots, N_2 + n_2\}.$$

- Генерация последовательностей

$$x_i P_1 + y_i P_2, (x_i, y_i) \in T, i = 1, 2, \ldots, \quad (1)$$

$$Q + z_j P_1 + w_j P_2, (z_j, w_j) \in T, j = 1, 2, \ldots \quad (2)$$

Алгоритм решения двумерной задачи дискретного логарифмирования (Gaudry, Schost, 2004)

- Построение Дикого и Домашнего множеств

$$T = \{-N_1, \ldots, N_1\} \times \{-N_2, \ldots, N_2\},$$

$$W = \{-N_1 + n_1, \ldots, N_1 + n_1\} \times \{-N_2 + n_2, \ldots, N_2 + n_2\}.$$

- Генерация последовательностей

$$x_i P_1 + y_i P_2, (x_i, y_i) \in T, i = 1, 2, \ldots, \quad (1)$$

$$Q + z_j P_1 + w_j P_2, (z_j, w_j) \in T, j = 1, 2, \ldots \quad (2)$$

- Получение решения задачи

$$x_k P_1 + y_k P_2 = Q + z_l P_1 + w_l P_2, \quad (3)$$

Алгоритм решения двумерной задачи дискретного логарифмирования (Gaudry, Schost, 2004)

- Построение Дикого и Домашнего множеств

$$T = \{-N_1, \ldots, N_1\} \times \{-N_2, \ldots, N_2\},$$

$$W = \{-N_1 + n_1, \ldots, N_1 + n_1\} \times \{-N_2 + n_2, \ldots, N_2 + n_2\}.$$

- Генерация последовательностей

$$x_i P_1 + y_i P_2, (x_i, y_i) \in T, i = 1, 2, \ldots, \quad (1)$$

$$Q + z_j P_1 + w_j P_2, (z_j, w_j) \in T, j = 1, 2, \ldots \quad (2)$$

- Получение решения задачи

$$x_k P_1 + y_k P_2 = Q + z_l P_1 + w_l P_2, \quad (3)$$

- Оценка средней трудоемкости
$\Omega = 2.36\sqrt{N}$, где $N = (2N_1 + 1)(2N_2 + 1)$ [Galbraith, Ruprai, 2009]

Эффективно вычисляемый гомоморфизм и задача дискретного логарифмирования

- Эффективно вычисляемый гомоморфизм

$$\varphi : \ \varphi(g) = \lambda g, \ \forall g \in G$$

Группа G распадается на классы эквивалентности

$$\{g, \varphi(g), ..., \varphi^k(g)\}$$

Эффективно вычисляемый гомоморфизм и задача дискретного логарифмирования

- Эффективно вычисляемый гомоморфизм

$$\varphi : \ \varphi(g) = \lambda g, \ \forall g \in G$$

Группа G распадается на классы эквивалентности

$$\{g, \varphi(g), ..., \varphi^k(g)\}$$

- $\#\langle\varphi\rangle = 2$
  $\Omega = 1.45\sqrt{N}$ [Liu, 2010]

Эффективно вычисляемый гомоморфизм и задача дискретного логарифмирования

- Эффективно вычисляемый гомоморфизм

$$\varphi : \ \varphi(g) = \lambda g, \ \forall g \in G$$

Группа G распадается на классы эквивалентности

$$\{g, \varphi(g), ..., \varphi^k(g)\}$$

- $\#\langle\varphi\rangle = 2$
  $\Omega = 1.45\sqrt{N}$ [Liu, 2010]
- $\#\langle\varphi\rangle = 4$
  $\Omega = 1.0255\sqrt{N}$ [Liu, 2010]

Случай $\#\langle\varphi\rangle = 6$

- Кривая E задана уравнением $y^2 = x^3 + b$ над полем F_p, $p \equiv 1 \pmod 3$. Тогда эндоморфизм $\varphi(x, y) = (\beta x, -y)$, $\mathrm{ord}(\beta) = 3$ равносилен умножению на $\lambda : \lambda^2 - \lambda + 1 \equiv 0 \pmod n$, т.е. $\varphi(x, y) = \lambda(x, y)$ и при этом имеет порядок 6. Если $Q = n_1 P + n_2(\lambda P)$, то

$$\varphi(Q) = \varphi(n_1 P + n_2(\lambda P)) = n_1(\lambda P) + n_2(\lambda - 1)P = -n_2 P + (n_1 + n_2)(\lambda P)$$

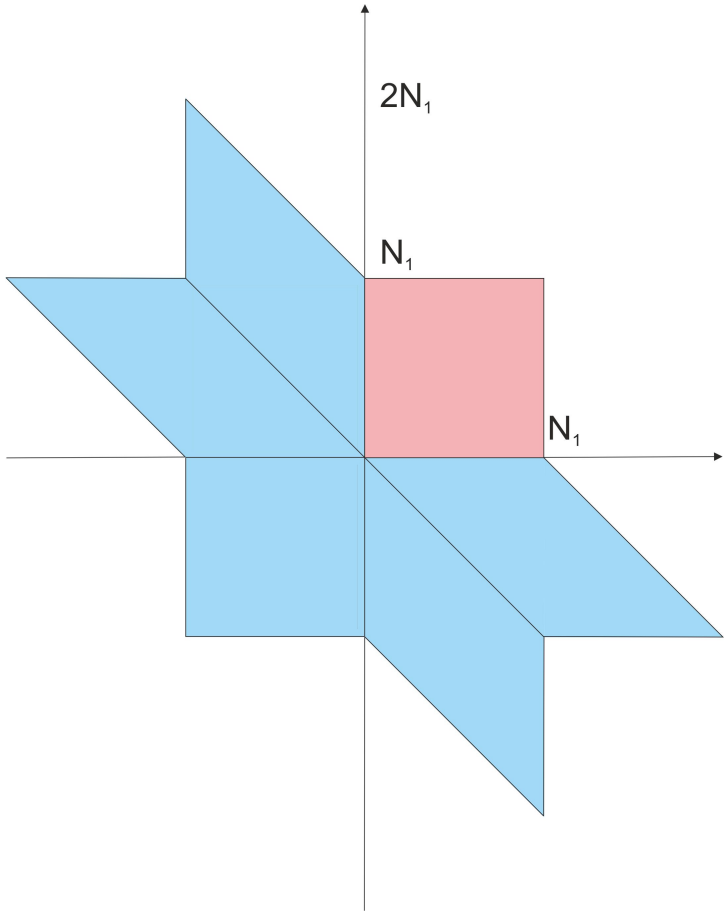
$$\varphi(Q_2) = -(n_1 + n_2)P + n_1(\lambda P) = Q_3$$

$$\varphi(Q_3) = -n_1 P - n_2(\lambda P) = Q_4$$

$$\varphi(Q_4) = n_2 P - (n_1 + n_2)(\lambda P) = Q_5$$

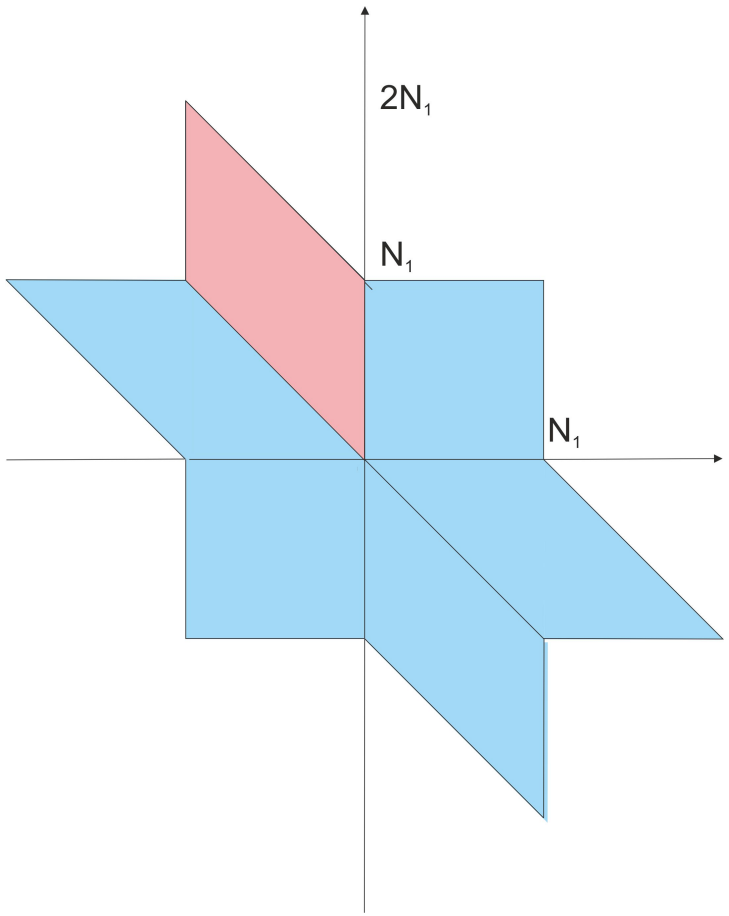
$$\varphi(Q_5) = (n_1 + n_2)P - n_1(\lambda P) = Q_6$$

Случай $\#\langle\varphi\rangle = 6$



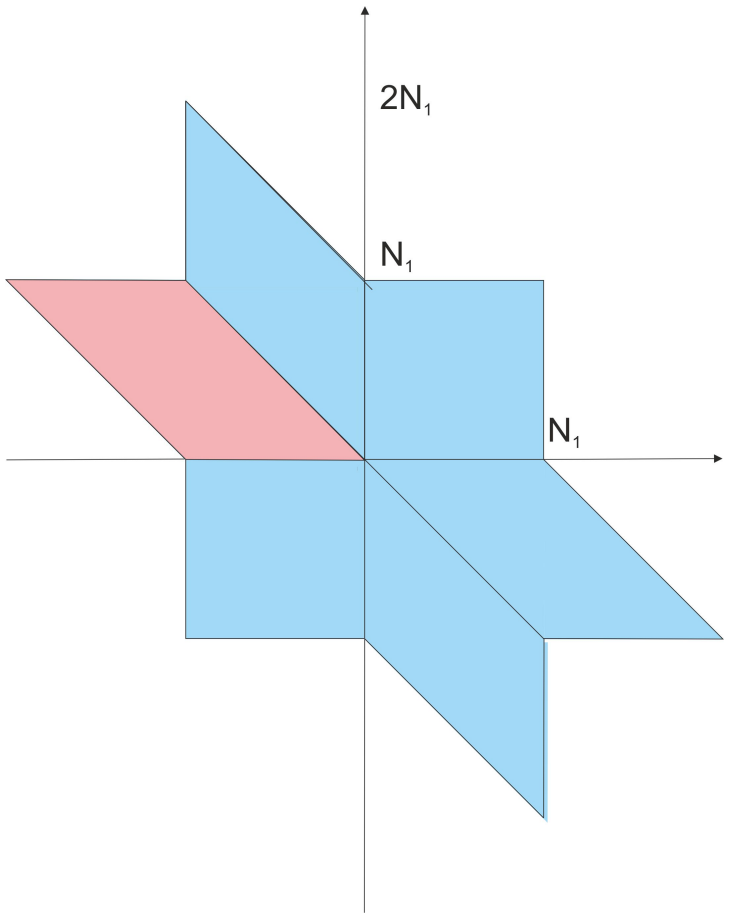
Случай $\#\langle\varphi\rangle = 6$

$$\varphi(Q) = -n_2 P + (n_1 + n_2)(\lambda P) = Q_2$$



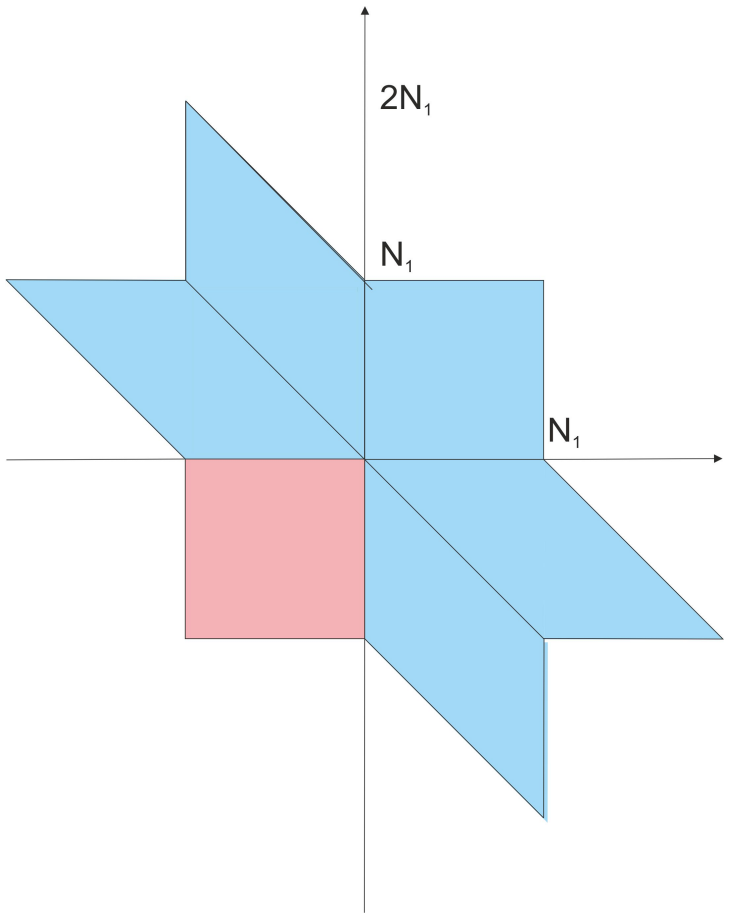
Случай $\#\langle\varphi\rangle = 6$

$$\varphi(Q_2) = -(n_1 + n_2)P + n_1(\lambda P) = Q_3$$



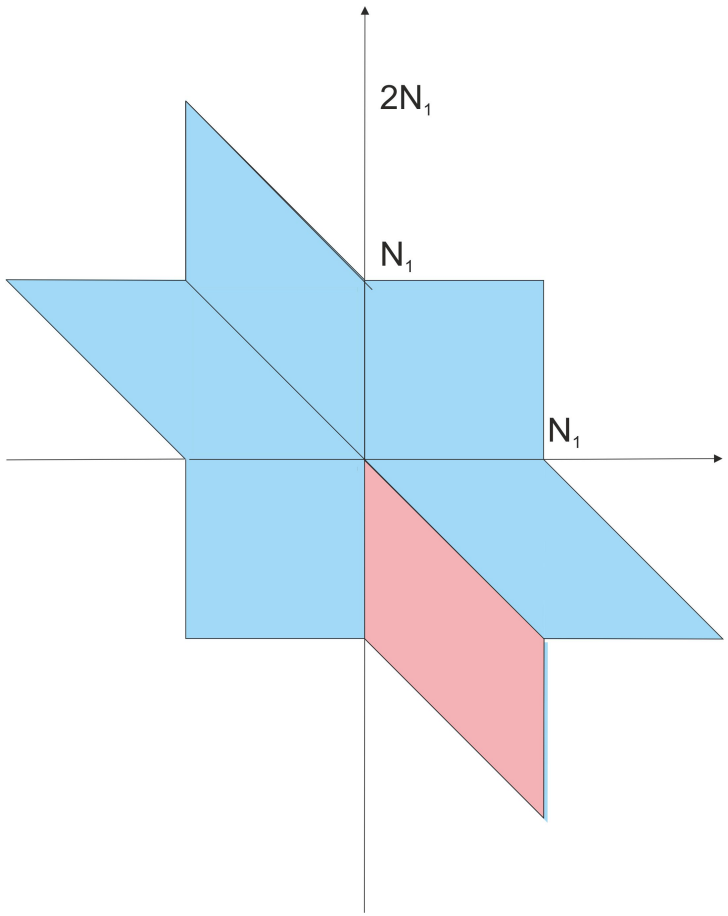
Случай $\#\langle\varphi\rangle = 6$

$$\varphi(Q_3) = -n_1 P - n_2(\lambda P) = Q_4$$



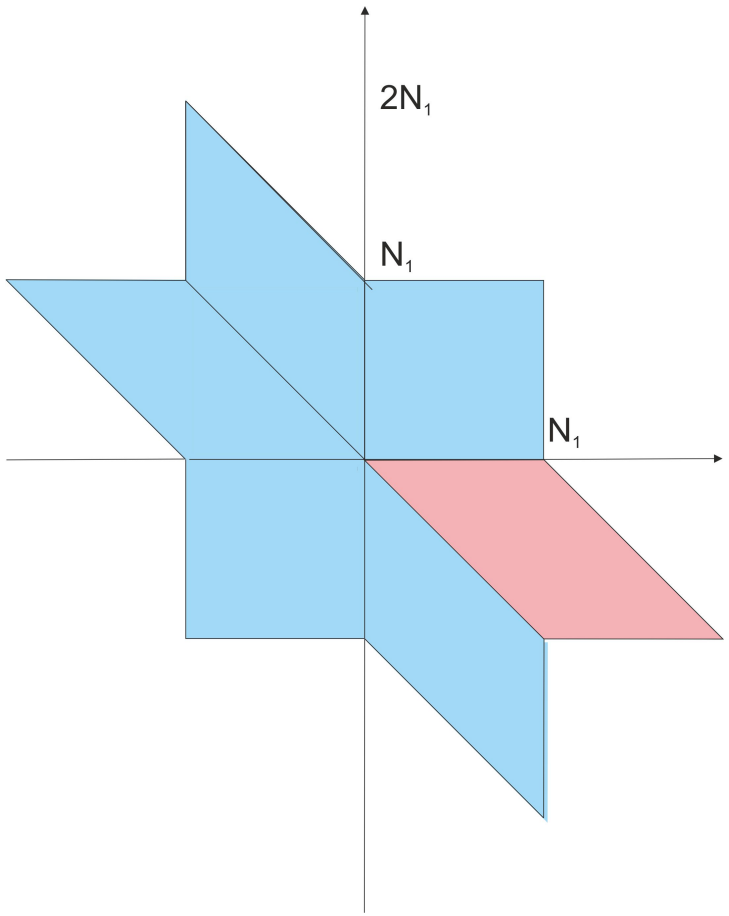
Случай $\#\langle\varphi\rangle = 6$

$$\varphi(Q_4) = n_2 P - (n_1 + n_2)(\lambda P) = Q_5$$



Случай $\#\langle\varphi\rangle = 6$

$$\varphi(Q_5) = (n_1 + n_2)P - n_1(\lambda P) = Q_6$$



Случай $\#\langle\varphi\rangle = 6$

- $$C(a,b) =$$
$$= \{(a,b),(-b,a+b),(-(a+b),a),(-a,-b),(b,-(a+b)),(a+b,-a)\}$$

Случай $\#\langle\varphi\rangle = 6$

- $$C(a,b) =$$

$$= \{(a,b),(-b,a+b),(-(a+b),a),(-a,-b),(b,-(a+b)),(a+b,-a)\}$$

- $$T = \{C(a,b) : -N_1 \leq a \leq N_1, -N_2 \leq b \leq N_2\}$$

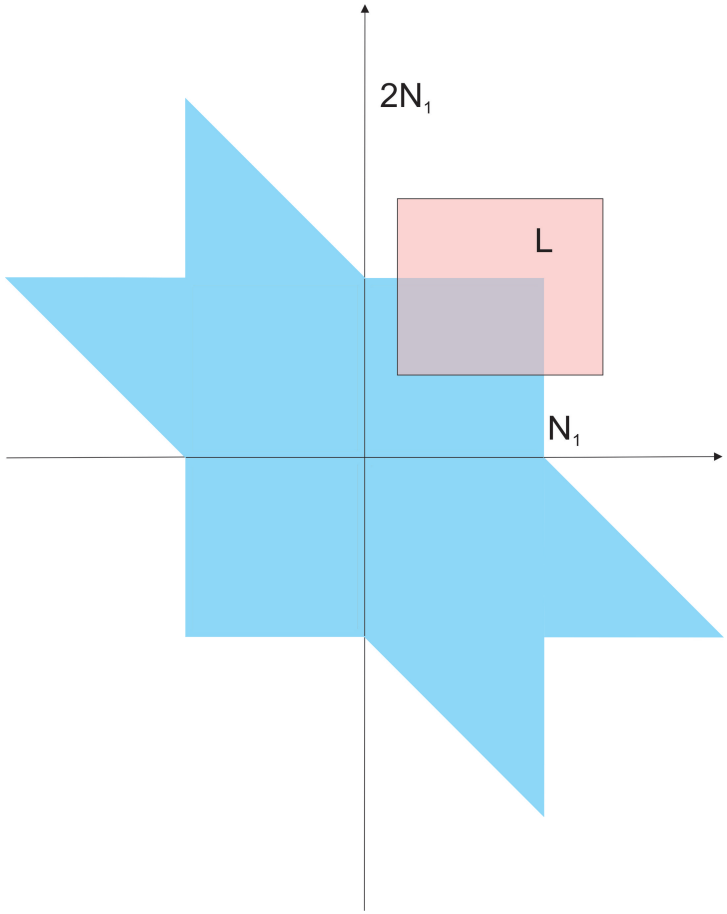
Случай $\#\langle\varphi\rangle = 6$

- $$C(a,b) =$$
$$= \{(a,b),(-b,a+b),(-(a+b),a),(-a,-b),(b,-(a+b)),(a+b,-a)\}$$

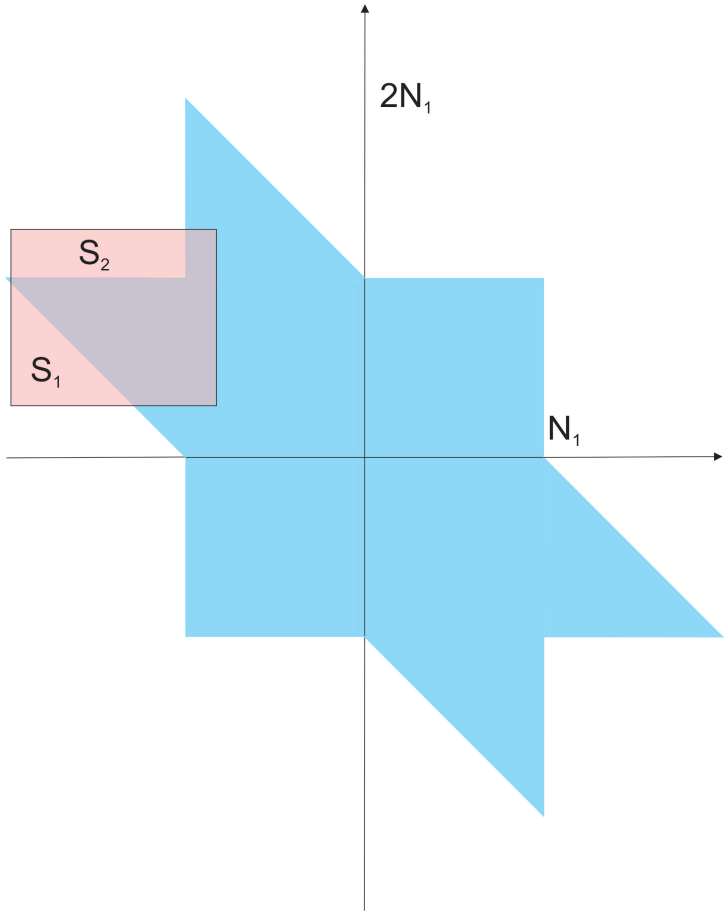
- $$T = \{C(a,b) : -N_1 \leq a \leq N_1, -N_2 \leq b \leq N_2\}$$

- $$W = \{C(n_1+a, n_2+b) : -\frac{N_1}{2} \leq a \leq \frac{N_1}{2}, -\frac{N_2}{2} \leq b \leq \frac{N_2}{2}\}$$

Случай $\#\langle\varphi\rangle = 6$



Случай $\#\langle\varphi\rangle = 6$



Оценка средней трудоемкости

[Galbraith, Holmes, 2010] Теорема

Пусть есть неограниченное количество шаров (отличающихся только в цвете) и N урн. Мы выбираем шары и перекрашиваем их в красный или синий цвета с вероятностями $q_c (c = 1, 2)$ *и бросаем их в урны. Вероятность попадания в урну a равна* $q_{c,a}$ *и* $q_{c',a}$ *для красных и синих шаров соответственно. Ожидаемое количество шаров, которые необходимо выбрать для того, чтобы получить разноцветные шары в одной урне, равно*

$$\sqrt{\frac{\pi}{2A_N}} + O(N^{1/4})$$

где $A_N = \sum_{c=1}^{2} q_c (\sum_{c'=1, c \neq c'}^{2} q_{c'} (\sum_{a=1}^{R} q_{c,a} q_{c',a}))$

Результаты

Теорема

Двумерная задача дискретного логарифмирования в группе точек эллиптической кривой E может быть решена со средней трудоемкостью $\Omega = (0.97811 + o(1))\sqrt{N}$ групповых операций.

GLV

$$Q = (k_1 + k_2\lambda)P = k_1P + k_2\lambda P$$

$$k_1, k_2 \leq c\sqrt{n}$$