行政院國家科學委員會專題研究計畫成果報告

不變量、演算數論與密碼學
Invariants、algorithmic number theory and cryptography

計畫類別：個別型計畫

計畫編號：NSC88-2115-M-002-002

執行期間：87 年 8 月 1 日至 88 年 7 月 31 日

計畫主持人：朱　樺 教授

壹年後可對外提供參考

執行單位：國立台灣大學理學院數學系

中華民國八十八年十二月三十日

中 文 摘 要

關鍵詞：不變量、單項式自同構、Weyl 體、離散對數、橢圓曲線。

這份報告包含兩部份：

第一部份，我們考慮 Weyl 體上的不變量理論。若 G 是 Weyl 體 $C(x, y)$上的有限單項式作用群，我們曾經証明其不變子體與 $C(x, y)$同構。現在我們想進一步考慮 $C(x_1, y_1, x_2, y_2)$的不變子體，首先在這篇報告中，我們先刻劃了上面的所有有限單項式作用群。

第二部份，我們討論 lifting 橢圓曲線的問題。我們分別用 index calculus 及 xedni calculus 方法來解橢圓曲線上的離散對數問題。

Abstract

Keywords : invariant subfield, monomial antomorphism, Weyl field, discrete logarithm, elliptic curve.

This report consists of two parts. In part I, we consider the invariant theory of Weyl field. Let G be a finite monomial antomorphism group on the Weyl field $C(x,y)$, we have proved that the invariant subfield is isomorphic to $C(x,y)$. Now we try to consider the invariant subfield of $C(x_1,y_1,x_2,y_2)$, we first characterize all the finite monomial amtomorphism groups in this note.

In part II, we analyze the problem of lifting elliptic curves with a finite set of points and draw several conclusions on the index calculus and the xedni calculus methods for solving the elliptic curve discrete logarithm problem over F_p.

Monomial automorphism groups on Weyl fields

by

Huah Chu

For a finite group G, any representation of G on a finite dimensional vector space V induces a G-action on fucnction field $\mathbb{C}(V)$. Noether asked whether the invariant subfield $\mathbb{C}(V)^G$ is rational (=purely transcendental) over $\mathbb{C}$. The answer is positive for dim $V \leq 3$ or G is an abelian group.

It is natural to consider the meta-abelian groups. Assume that G has a normal abelian group N for which $H = G/N$ is abelian. Using Fisher's method, we construct a base of $L = \mathbb{C}(V)^N$ on which H acts monomially. Thus our problem reduces to whether the abelian group H of monomial automorphism has a rational fixed field. Hajja[4] proved that if G is meta-abelian, then $\mathbb{C}(V)^G$ is rational for dim $V \leq 4$. Hajja and Kang[5] proved that the invariant subfield of $F(x_1, x_2, x_3)$ under any purely monomial gruop action is rational except for one case.

An analogue question raise for Weyl fields $D_n(\mathbb{C})$ which is the quotient field of the Weyl algebra $A_n(\mathbb{C})$. Let G be a finite linear automorphism group on $D_n(\mathbb{C})$, whether the invariant subfield $D_n(\mathbb{C})^G$ is isomorphic to $D_n(\mathbb{C})$. The answer is positive for the linear group on $A_1(\mathbb{C})$ and abelian groups on $A_n(\mathbb{C})$ [1, 2].

The Weyl algebra $A_n(\mathbb{C})$ in the "polynomial" $\mathbb{C}[x_1, y_1, \cdots, x_n, y_n]$ satisfying $x_iy_i - y_ix_i = 1$, $x_iy_j = y_jx_i$, $x_ix_j = x_jx_i$, $y_iy_j = y_jy_i$. The Weyl field $D_n(\mathbb{C})$=$\mathbb{C}(x_1, y_1, \cdots, x_n, y_n)$ satisfying the same relations. A monomial in $D_n(\mathbb{C})$ is an element of the form

$$u = ax_1^{\alpha_1}y_1^{\beta_1}\cdots x_1^{\alpha_l}y_1^{\beta_l}\cdots x_n^{\gamma_1}y_m^{\delta_1}\cdots x_n^{\gamma_m}y_n^{\delta_m}\cdots \ , \ a \in \mathbb{C}^* \ , \ \alpha_i, \beta_j, \gamma_l, \delta_k \in \mathbf{Z}.$$

A monomial automorphism on $D_n(\mathbb{C})$ is an automorphism with the form

$$x_i \mapsto u_i \ , \ y_i \mapsto v_i \ .$$

where u_i and v_i are all monomials. A monomial automorphism group is a group such that all of its elements are monomial automorphisms. In [3], we show that for any finite monomial automorphism group G on $D_1(\mathbb{C})$, $D_1(\mathbb{C})^G \cong D_1(\mathbb{C})$. In this paper,we first characterize, the monomial automorphism must have the form

$$\theta_k : x \mapsto \zeta_k x$$
$$y \mapsto \zeta_k^{-1} y$$

or

$$\rho_{alg} : x \mapsto \frac{a(w-l)}{g(w-1)} y$$
$$y \mapsto -\frac{1}{a} g(w) y^{-1}$$

when $l \in \mathbf{Z}$, $a \in \mathbb{C}^*$. $\deg\, g(w) = 1 - \alpha$ and g statisfies

$$g(-w+l) = (-1)^{\alpha+1} g(w-1) \ .$$

Then we also characterize the finite monomial automorphism groups are

$$G = \langle \theta_k \rangle \ , \ G = \langle \rho_{alg} \rangle \text{ or } G = \langle \rho_{alg}, \theta_k \rangle \ .$$

At last we show that $D_1(\mathbb{C})^G \cong D_1(\mathbb{C})$.

To treat the problems in $D_2(\mathbb{C})$, we first characterize the monomial automorphisms and the group. In this note, we settle these characterizations.

§1. Characterization of exponent matrices

Let $K = \mathbb{C}(x_1, y_1, x_2, y_2), x_1 y_1 - y_1 x_1 = 1, x_2 y_2 - y_2 x_2 = 1$, be the Weyl field with 4 variables. For any monomial u, we may write

$$u = ax_1^{\alpha_1} y_1^{\beta_1} \cdots x_1^{\alpha_n} y_1^{\beta_n} x_2^{\gamma_1} y_2^{\delta_1} \cdots x_2^{\gamma_m} y_2^{\delta_m}$$
$$= a(x_1^{\alpha_1+\cdots+\alpha_n} y_1^{\beta_1+\cdots+\beta_n} + bx_1^{\alpha_1+\cdots+\alpha_n-1} y_1^{\beta_1+\cdots+\beta_n-1} + ...)$$
$$(x_2^{\gamma_1+\cdots+\gamma_m} y_2^{\delta_1+\cdots+\delta_m} + cx_2^{\gamma_1+\cdots+\gamma_m-1} y_2^{\delta_1+\cdots+\delta_m-1} + \cdots)$$

Hence we may write any monomial as

$$u = a(x_1^{\alpha_1} y_1^{\beta_1} + cx_1^{\alpha_1-1} y_1^{\beta_1-1} + \cdots)(x_2^{\alpha_2} y_2^{\beta_2} + dx_2^{\alpha_2-1} y_2^{\beta_2-1} + \cdots)$$

$$v = b(x_1^{\gamma_1} y_1^{\delta_1} + cx_1^{\gamma_1-1} y_1^{\delta_1-1} + \cdots)(x_2^{\gamma_2} y_2^{\delta_2} + dx_2^{\gamma_2-1} y_2^{\delta_2-1} + \cdots)$$

Lemma 1. Let $[u, v] = uv - vu$. Then

$$[u, v] = ab\{(\alpha_1\delta_1)x_1^{\alpha_1+\gamma_1-1} y_1^{\beta_1+\delta_1-1} x_2^{\alpha_2+\delta_2-1} + (\text{terms with lower degree})\}$$

Proof. $[u, v]$

$$= ab\{(x_1^{\alpha_1} y_1^{\beta_1} x_1^{\gamma_1} y_1^{\delta_1} x_2^{\alpha_2} y_2^{\beta_2} x_2^{\gamma_2} y_2^{\delta_2} - x_1^{\gamma_1} y_1^{\delta_1} x_1^{\alpha_1} y_1^{\beta_1} x_2^{\gamma_2} y_2^{\delta_2} x_2^{\alpha_2} y_2^{\beta_2})$$
$$+c(x_1^{\alpha_1-1} y_1^{\beta_1-1} x_1^{\gamma_1} y_1^{\delta_1} x_2^{\alpha_2} y_2^{\beta_2} x_2^{\gamma_2} y_2^{\delta_2} - x_1^{\gamma_1} y_1^{\delta_1} x_1^{\alpha_1-1} y_1^{\beta_1-1} x_2^{\gamma_2} y_2^{\delta_2} x_2^{\alpha_2} y_2^{\beta_2})$$
$$+d(x_1^{\alpha_1} y_1^{\beta_1} x_1^{\gamma_1} y_1^{\delta_1} x_2^{\alpha_2-1} y_2^{\beta_2-1} x_2^{\gamma_2} y_2^{\delta_2} - x_1^{\gamma_1} y_1^{\delta_1} x_1^{\alpha_1} y_1^{\beta_1} x_2^{\gamma_2} y_2^{\delta_2} x_2^{\alpha_2-1} y_2^{\beta_2-1})$$
$$+e(x_1^{\alpha_1} y_1^{\beta_1} x_1^{\gamma_1-1} y_1^{\delta_1-1} x_2^{\alpha_2} y_2^{\beta_2} x_2^{\gamma_2} y_2^{\delta_2} - x_1^{\gamma_1-1} y_1^{\delta_1-1} x_1^{\alpha_1} y_1^{\beta_1} x_2^{\gamma_2} y_2^{\delta_2} x_2^{\alpha_2} y_2^{\beta_2})$$
$$+f(x_1^{\alpha_1} y_1^{\beta_1} x_1^{\gamma_1} y_1^{\delta_1} x_2^{\alpha_2} y_2^{\beta_2} x_2^{\gamma_2-1} y_2^{\delta_2-1} - x_1^{\gamma_1} y_1^{\delta_1} x_1^{\alpha_1} y_1^{\beta_1} x_2^{\gamma_2-1} y_2^{\delta_2-1} x_2^{\alpha_2} y_2^{\beta_2}) + \cdots\}$$
$$= ab\{(x_1^{\alpha_1+\gamma_1} y_1^{\beta_1+\delta_1} - \beta_1\gamma_1 x_1^{\alpha_1+\gamma_1-1} y_1^{\beta_1+\delta_1-1} + \cdots)$$
$$(x_2^{\alpha_2+\gamma_2} y_2^{\beta_2+\delta_2} - \beta_2\gamma_2 x_2^{\alpha_2+\gamma_2-1} y_1^{\beta_2+\delta_2-1} + \cdots)$$
$$-(x_1^{\alpha_1+\gamma_1} y_1^{\beta_1+\delta_1} - \alpha_1\delta_1 x_1^{\alpha_1+\gamma_1-1} y_1^{\beta_1+\delta_1-1} + \cdots)$$
$$(x_2^{\alpha_2+\gamma_2} y_2^{\beta_2+\delta_2} - \alpha_2\delta_2 x_2^{\alpha_2+\gamma_2-1} y_2^{\beta_2+\delta_2-1} + \cdots) + \cdots\}$$
$$= ab\{(\alpha_1\delta_1 - \beta_1\gamma_1)x_1^{\alpha_1+\gamma_1-1} y_1^{\beta_1+\delta_1-1} x_2^{\alpha_2+\gamma_2} y_2^{\beta_2+\delta_2}$$

$$+(\alpha_2\delta_2-\beta_2\gamma_2)x_1^{\alpha_1+\gamma_1}y_1^{\beta_1+\gamma_1}x_2^{\alpha_2+\gamma_2-1}y_2^{\beta_2+\delta_2-1}+\cdots\} \qquad \square$$

Now let φ be a monomial automorphism on K and

$$x_1 \mapsto u_1 = a(x_1^{\alpha_{11}}y_1^{\beta_{11}}x_2^{\alpha_{21}}y_2^{\beta_{21}}+\cdots)$$

$$y_1 \mapsto v_1 = b(x_1^{\gamma_{11}}y_1^{\delta_{11}}x_2^{\gamma_{21}}y_2^{\delta_{21}}+\cdots)$$

$$x_2 \mapsto u_2 = c(x_1^{\alpha_{12}}y_1^{\beta_{12}}x_2^{\alpha_{22}}y_2^{\beta_{22}}+\cdots)$$

$$y_2 \mapsto v_2 = d(x_1^{\gamma_{12}}y_1^{\delta_{12}}x_2^{\gamma_{22}}y_2^{\delta_{22}}+\cdots)$$

We write the exponents as a exponent matrix

$$E=\begin{bmatrix}\alpha_{11} & \gamma_{11} & \alpha_{12} & \gamma_{12}\\ \beta_{11} & \delta_{11} & \beta_{12} & \delta_{12}\\ \alpha_{21} & \gamma_{21} & \alpha_{22} & \gamma_{22}\\ \beta_{21} & \delta_{21} & \beta_{22} & \delta_{22}\end{bmatrix} \in GL_4(\mathbf{Z})$$

Lemma 2. The exponent matrix of a monomial automorphism has the following forms

$$\text{(I)}\quad E=\begin{bmatrix}0 & 0 & \alpha_{12} & \gamma_{12}\\ 0 & 0 & \beta_{12} & \delta_{12}\\ \alpha_{21} & \gamma_{21} & 0 & 0\\ \beta_{21} & \delta_{21} & 0 & 0\end{bmatrix} \text{ or } \quad \text{(II)}\quad E=\begin{bmatrix}\alpha_{11} & \gamma_{11} & 0 & 0\\ \beta_{11} & \delta_{11} & 0 & 0\\ 0 & 0 & \alpha_{22} & \gamma_{22}\\ 0 & 0 & \beta_{22} & \delta_{22}\end{bmatrix}.$$

Proof. From relations $[x_1,x_2]=[x_1,y_2]=[x_2,y_2]=[y_1,y_2]=0$, we have $[u_1,u_2]=[u_1,v_2]=[u_2,v_1]=[v_1,v_2]=0$, From Lemma 1, these conditions are

$$\begin{cases}\alpha_{11}\beta_{12}-\beta_{11}\alpha_{12}=0\\ \alpha_{21}\beta_{22}-\beta_{21}\alpha_{22}=0\end{cases}, \quad \begin{cases}\alpha_{11}\delta_{12}-\beta_{11}\gamma_{12}=0\\ \alpha_{21}\delta_{22}-\beta_{21}\gamma_{22}=0\end{cases},$$

$$\begin{cases}\gamma_{11}\beta_{12}-\alpha_{12}\delta_{11}=0\\ \gamma_{21}\beta_{22}-\alpha_{22}\delta_{21}=0\end{cases}, \quad \begin{cases}\gamma_{11}\delta_{12}-\delta_{11}\gamma_{12}=0\\ \gamma_{21}\delta_{22}-\delta_{21}\gamma_{22}=0\end{cases}.$$

We write the exponent matrix as

$$E=\begin{bmatrix}A_{11} & B_{11} & A_{12} & B_{12}\\ A_{21} & B_{21} & A_{22} & B_{22}\end{bmatrix},$$

then the above conditions are

(1) $\{A_{11}, A_{12}\}, \{A_{11}, B_{12}\}, \{B_{11}, B_{12}\}, \{B_{11}, A_{12}\}$ are linearly dependent

and

(2) $\{A_{21}, A_{22}\}, \{A_{21}, B_{22}\}, \{B_{21}, B_{22}\}, \{B_{21}, A_{22}\}$ are linearly dependent

If $A_{11} \neq 0$, then $A_{12} = \alpha A_{11}$ for some α. Assume that $A_{12} \neq 0$, then $B_{11} = \beta A_{12} = \alpha\beta A_{11}$. Thus the matrix

$$[A_{11}, B_{11}, A_{12}, B_{12}] = [A_{11}, \alpha\beta A_{11}, \alpha A_{11}, \gamma A_{11}]$$

has rank ≤ 1, contradicting to the asumption $A \in GL_4(\mathbf{Z})$. Thus we have $A_{12} = 0$. Similarly we have $B_{12} = 0$. If $B_{11} = 0$, similarly we have $A_{12} = B_{12} = 0$. By the same argument, we have

$$[A_{11}, B_{11}, A_{12}, B_{12}] = [A_{11}, B_{11}, 0, 0] \text{ or } [0, 0, A_{12}, B_{12}].$$

Applying the same arguments to (2), we have the same conclusion for $[A_{21}, B_{21}, A_{22}, B_{22}]$. The Lemma follows. □

We denote the matrices

$$A_\alpha := \begin{bmatrix} \alpha & 1-\alpha \\ \alpha+1 & -\alpha \end{bmatrix},$$

$$B_\alpha := \begin{bmatrix} \alpha & 1-\alpha \\ \alpha-1 & 2-\alpha \end{bmatrix}.$$

Note that $\det A_\alpha = -1$ and $A_\alpha^2 = I$, $\det B_\alpha = 1$ and ord $B_\alpha = \infty$, except that $B = I$. It's easy to verify that

Lemma 3.

(1) $B_\beta^{-1} = B_{2-\beta}$,

(2) $A_\alpha A_\beta = B_{\beta-\alpha+1}$, $A_\alpha B_\beta = A_{\alpha+\beta-1}$,

$$B_\alpha B_\beta = B_{\alpha+\beta-1} \quad , B_\alpha A_\beta = A_{\beta-\alpha+1}.$$

Lemma 4. We write the exponent matrix as

$$E = \begin{bmatrix} 0 & E_2 \\ E_1 & 0 \end{bmatrix} \quad , \text{ or } \quad \begin{bmatrix} E_1 & 0 \\ 0 & E_2 \end{bmatrix}$$

Then $E_1 = A_\alpha, ab = 1$ or $E_1 = B_\alpha, ab = -1$

Proof. Let $E = \begin{bmatrix} 0 & E_2 \\ E_1 & 0 \end{bmatrix}$. From $[x_1, y_1] = 1$. We have $[w_1, w_2] = 1$, so we have

$$ab(\alpha_{21}\delta_{21} - \beta_{21}\gamma_{21}) = 1$$

and

$$\alpha_{21} + \gamma_{21} = \beta_{21} + \delta_{21} = 1.$$

From $A \in GL_2(\mathbf{Z})$, we have $\det E_1 = \pm 1$. If

$$\det E_1 = \det \begin{bmatrix} \alpha_{21} & \gamma_{21} \\ \beta_{21} & \delta_{21} \end{bmatrix} = 1 \ ,$$

Then it is easy to see that $E = B_\alpha$. And if $\det E_1 = -1$ then $E_1 = A_\alpha$. □

Let φ be a monomial automorphism of finite order, since the exponent matrix satisfies

$$E_\varphi E_\psi = E_{\varphi\psi} \ .$$

so the exponent matrix is also of finite order. We have the following

Lemma 5. The exponent matrix of finite order has the following types

(1) $\begin{pmatrix} I & 0 \\ 0 & I \end{pmatrix}$,order $= 1$;

(2) $\begin{pmatrix} A_\alpha & 0 \\ 0 & I \end{pmatrix}$,order $= 2$;

(3) $\begin{pmatrix} I & 0 \\ 0 & A_\alpha \end{pmatrix}$, order $= 2$;

(4) $\begin{pmatrix} A_\alpha & 0 \\ 0 & A_\beta \end{pmatrix}$, order $= 2$;

(5) $\begin{pmatrix} 0 & A_\alpha \\ A_\alpha & 0 \end{pmatrix}$, order $= 2$;

(6) $\begin{pmatrix} 0 & B_\alpha \\ B_{2-\alpha} & 0 \end{pmatrix}$, order $= 2$;

(7) $\begin{pmatrix} 0 & A_\alpha \\ B_\beta & 0 \end{pmatrix}$, order $= 4$ and $\begin{pmatrix} 0 & A_\alpha \\ B_\beta & 0 \end{pmatrix}^2 = \begin{pmatrix} A_{\alpha+\beta-1} & 0 \\ 0 & A_{\alpha-\beta+1} \end{pmatrix}$;

(8) $\begin{pmatrix} 0 & B_\beta \\ A_\alpha & 0 \end{pmatrix}$, order $= 4$ and $\begin{pmatrix} 0 & B_\beta \\ A_\alpha & 0 \end{pmatrix}^2 = \begin{pmatrix} A_{\alpha-\beta+1} & 0 \\ 0 & A_{\alpha+\beta-1} \end{pmatrix}$.

Proof. If $E = \begin{pmatrix} E_1 & 0 \\ 0 & E_2 \end{pmatrix}$, all results are clear. If $E = \begin{pmatrix} 0 & A_\alpha \\ A_\beta & 0 \end{pmatrix}$, the $E^2 = \begin{pmatrix} B_{\beta-\alpha+1} & 0 \\ 0 & B_{\beta-\alpha+1} \end{pmatrix}$. It has finite order if and only if $\alpha = \beta$. If $\begin{pmatrix} 0 & A_\alpha \\ B_\beta & 0 \end{pmatrix}$, then $E^2 = \begin{pmatrix} B_{\alpha+\beta-1} & 0 \\ 0 & B_{\alpha+\beta-1} \end{pmatrix}$. It has finite order in and only if $\alpha+\beta-1 = 1$ and $\beta = 2-\alpha$. If $E = \begin{pmatrix} 0 & A_\alpha \\ B_\beta & 0 \end{pmatrix}$ or $\begin{pmatrix} 0 & B_\beta \\ A_\alpha & 0 \end{pmatrix}$, it is easy to check that $E^4 = 1$. □

§2. Characterization of exponent groups

Let G be a finite group of monomial automorphisms, then the exponent of $\varphi \in G$ also form a finite subgruop, we shall characterize the exponent group G_E.

Proposition 6. The exponent group G_E of monomial automorphisms has the following types:

(1) $G_{E_1} = \{1\}$

(2) $G_{E_2} = \langle \begin{pmatrix} A_\alpha & 0 \\ 0 & I \end{pmatrix} \rangle$ or $\langle \begin{pmatrix} I & 0 \\ 0 & A_\alpha \end{pmatrix} \rangle$

(3) $G_{E_3} = \langle \begin{pmatrix} A_\alpha & 0 \\ 0 & A_\beta \end{pmatrix} \rangle$

(4) $G_{E_4} = \langle \begin{pmatrix} 0 & A_\alpha \\ A_\alpha & 0 \end{pmatrix} \rangle$

(5) $G_{E_5} = \langle \begin{pmatrix} 0 & B_\alpha \\ B_{2-\alpha} & 0 \end{pmatrix} \rangle$

(6) $G_{E_6} = \langle \begin{pmatrix} 0 & A_\alpha \\ B_\beta & 0 \end{pmatrix} \rangle$ or $\langle \begin{pmatrix} 0 & B_\beta \\ A_\alpha & 0 \end{pmatrix} \rangle$

(7) $G_{E_7} = \langle \begin{pmatrix} A_\alpha & 0 \\ 0 & I \end{pmatrix}, \begin{pmatrix} I & 0 \\ 0 & A_\beta \end{pmatrix} \rangle$

(8) $G_{E_8} = \langle \begin{pmatrix} A_\alpha & 0 \\ 0 & A_{2\beta-\alpha} \end{pmatrix}, \begin{pmatrix} 0 & A_\beta \\ A_\beta & 0 \end{pmatrix} \rangle$

(9) $G_{E_9} = \langle \begin{pmatrix} 0 & A_\alpha \\ B_\beta & 0 \end{pmatrix}, \begin{pmatrix} A_{\alpha+\beta-1} & 0 \\ 0 & I \end{pmatrix} \rangle$

where (2)~(5) are cyclic of order 2, (6) is cyclic of order 4, (7),(8) are Klein 4-group and (9) is the dihedral group D_4.

Proof. Consider the short exact sequence

$$1 \to H \to G_E \xrightarrow{\varphi} \mathbf{Z}_2 \times \mathbf{Z}_2 \to 1$$

where the map φ is defined as follows: if $E = \begin{pmatrix} E_1 & 0 \\ 0 & E_2 \end{pmatrix}$. Then $\varphi(E) = (\det E, 1)$ and if $E = \begin{pmatrix} 0 & E_1 \\ E_2 & 0 \end{pmatrix}$, $\varphi(E) = (\det E, -1)$. Thus if $E \in H$, then $\varphi(E) = (1,1)$ and $E = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ or $\begin{pmatrix} A_\alpha & 0 \\ 0 & A_\beta \end{pmatrix}$. If $G_E/H = \langle (1,-1) \rangle$, then G_E is (6). If $G_E/H = \langle (1,-1) \rangle$. Then G_E is (2) or (7). If $G_E/H = \langle (-1,-1) \rangle G_E$. (4),(5) or (8), if $G_E/H = \langle (1,-1), (-1.1) \rangle$. Then G_E is (9). □

§3. Characterization of monomial automorphism

Lemma 7. If $E_\varphi = \begin{bmatrix} E_1 & 0 \\ 0 & E_2 \end{bmatrix}$, then

$$\varphi : x_1 \mapsto a f_1(w_1) y_1^{e_1} \ , \ x_2 \mapsto c f_4(w_2) y_2^{e_2}$$

$$y_1 \mapsto b g_1(w_1) y_1^{\delta_1} \ , \ y_2 \mapsto d g_4(w_2) y_2^{\delta_2} \ .$$

If $E_\varphi = \begin{bmatrix} 0 & E_1 \\ E_2 & 0 \end{bmatrix}$, then

$$\varphi : x_1 \mapsto af_2(w_2)y_2^{\varepsilon_2} \ , \ x_2 \mapsto cf_3(w_1)y_1^{\varepsilon_1}$$

$$y_1 \mapsto bg_2(w_2)y_2^{\delta_2} \ , \ y_2 \mapsto dg_3(w_1)y_1^{\delta_1}$$

Proof. First note that, if a monomial $\mathbf{m}(x_1, y_1)$ has degree (α, β), then

$$\mathbf{m} = af(w_1)y_1^\gamma$$

where $w_1 = x_1y_1$, $\deg f = \alpha$ and $\gamma = \beta - \alpha$. So for the case of $A_\alpha = \begin{pmatrix} \alpha & 1-\alpha \\ \alpha+1 & -\alpha \end{pmatrix}$, we have

$$\varphi : \begin{cases} x_1 \mapsto af(w_1)y \\ y_1 \mapsto -\frac{1}{a}g(w_1)y^{-1} \end{cases},$$

$\deg f = \alpha$ and $\deg g = 1 - \alpha$. For the case $B_\alpha = \begin{bmatrix} \alpha & 1-\alpha \\ \alpha-1 & 2-\alpha \end{bmatrix}$,

$$\varphi : \begin{cases} x_1 \mapsto af(w_1)y^{-1} \\ y_1 \mapsto \frac{1}{a}g(w_1)y \end{cases}$$

$\deg f = \alpha$ and $\deg g = 1 - \alpha$. Now if

$$E_\varphi = \begin{bmatrix} E_1 & 0 \\ 0 & E_2 \end{bmatrix},$$

then we have

$$\varphi : x_1 \mapsto af_1(w_1)y_1^{\varepsilon_1}f_2(w_2)$$

$$x_2 \mapsto bf_4(w_2)y_2^{\varepsilon_2}f_3(w_1)$$

$\varepsilon_i = \pm 1$, $f_2 \in \mathbb{Q}(w)$, $\deg f_2 = \deg f_3 = 0$. From $[\varphi(x_1), \varphi(x_2)] = 0$, we have

$$abf_1(w_1)y_1^{\varepsilon_1}f_2(w_2)f_3(w_1)f_4(w_2)y_2^{\varepsilon_2} = abf_3(w_1)f_4(w_2)y_2^{\varepsilon_2}f_1(w_1)y_1^{\varepsilon_1}f_2(w_2)$$

$$f_1(w_1)y_1^{\varepsilon_1} = cf_3(w_1)f_1(w_1)y_1^{\varepsilon_1}$$

$$f_2(w_2)y_4(w_2)y_2^{\varepsilon_1} = \frac{1}{c}f_4(w_2)y_2^{\varepsilon_2}f_2(w_2)$$

for some $c \in \mathbb{C}^{\times}$. It follows that

$$y_1^{\varepsilon_1} f_3(w_2) = e f_3(w_1) y_1^{\varepsilon_1}$$

$$y_3(w_1 - \varepsilon_1) = e f_3(w_1)$$

Similarly, $f_2(w_2 - \varepsilon_2) = e f_2(w_2)$. Thus f_2 and f_3 are constant. Since they are momc, so, $f_2 = f_3 = 1$. The same result holds for $\varphi(y_1)$ and $\varphi(y_2)$. Similar arguments holds for the case $E_\varphi = \begin{bmatrix} 0 & E_1 \\ E_2 & 0 \end{bmatrix}$. □

Lemma 8. If $E_\varphi = I$, then we may write φ as

$$\theta_{kl} : \begin{array}{ll} x_1 \mapsto \zeta_k x_1 & x_2 \mapsto \zeta_l x_2 \\ y_1 \mapsto \zeta_k^{-1} y_1 & y_2 \mapsto \zeta_l^{-1} y_2 \end{array}$$

where ζ_j is a primitive jth root of unity. Moreover,

$$\theta_{kl} : w_1 \mapsto w_1, w_2 \mapsto w_2, \mathrm{ord}\theta_{kl} = [k, l] .$$

Proof. In this case, we have

$$\varphi : \begin{array}{lll} x_1 \mapsto a f_1(w_1) y_1^{-1} & , x_2 \mapsto b f_4(w_2) y_2^{-1}, \\ y_1 \mapsto \dfrac{1}{a} g_1(w_1) y_1 & , y_2 \mapsto \dfrac{1}{b} g_4(w_2) y_2, \end{array}$$

$\deg f_1 = \deg f_4 = 1$, $\deg g_1 = \deg g_4 = 0$. Moreover $w_1 \mapsto f_1(w_1) g_1(w_1 + 1)$, $w_2 \mapsto f_4(w_2) g_4(w_2 + 1)$, $\deg f_1(w_1) g_1(w_1 + 1) = 1$. Since $\varphi \mid_{K(w_1)}$ is an automorphism, so

$$f_1(w_1) g_1(w_1 + 1) = w_1 + l.$$

But φ is of finite order, $\varphi(w_1) = w_1$. Thus, $\varphi : y_1 \mapsto \frac{1}{a} g_1(w_1) y_1$.

Now suppose $\varphi^n = 1$, then $(\frac{1}{a} g_1(w_1))^n = 1$. and $g(w_1) = 1$, $\frac{1}{a} \zeta_k^{-1}$ for some ζ_k. Thus $f_1(w_1) = w_1$, $a f_1(w_1) y_1^{-1} = \zeta_k x$. In conclusion, we have

$$\varphi : \begin{array}{l} x_1 \mapsto \zeta_k x_1, \\ y_1 \mapsto \zeta_k^{-1} y_1 \ . \end{array}$$ □

Lemma 9. If $E_\varphi = \begin{bmatrix} A_\alpha & 0 \\ 0 & I \end{bmatrix}$, then we can write φ as

$$\chi_{alkg} : \begin{cases} x_1 \mapsto a \frac{w_1 - l}{g(w_1 - 1)} y_1 \\ y_1 \mapsto -\frac{1}{a} g(w_1) y_1^{-1} \\ x_2 \mapsto \zeta_k x_2 \\ y_2 \mapsto \zeta_k^{-1} y_2 \ . \end{cases}$$

where $w_1 \mapsto -w_1 + l$ and $w_2 \mapsto w_2$. $\deg g = 1 - \alpha$ and g satisfies

$$g(-w + l) = (-1)^{\alpha+1} g(w - 1)$$

ord $\chi_{alkg} = [2, k]$ if α is odd; $= [4, k]$ if α is even.

Proof. This result follows from two variables case, we have

$$\varphi : \begin{cases} x_1 \mapsto a \frac{w - l}{g(w-1)} y \\ y_1 \mapsto -\frac{1}{a} g(w) y^{-1} \end{cases}$$

where $\deg g = 1 - \alpha$, g satisfies $g(-w + l) = (-1)^{\alpha+1} g(w - 1)$ and we have $w \mapsto -w + l$. If α is even, $\mathrm{ord}\varphi = 4$; α is odd, $\mathrm{ord}\varphi = 2$. □

If $E_\varphi = \begin{pmatrix} I & 0 \\ 0 & A_\alpha \end{pmatrix}$, we can define the automorphism χ'_{algk} as above. By the similar arguments, we have the following

Lemma 10. If $E_\varphi = \begin{bmatrix} A_\alpha & 0 \\ 0 & A_\beta \end{bmatrix}$ then it has the form

$$\eta_{a_1 a_2 l_1 l_2 g_1 g_2} : \begin{cases} x_1 \mapsto a_1 \frac{w_1 - l_1}{g_1(w_1 - 1)} y_1 \\ y_1 \mapsto -\frac{1}{a_1} g_1(w_1) y_1^{-1} \\ x_2 \mapsto a_2 \frac{w_2 - l_2}{g_2(w_2 - 1)} y_2 \\ y_2 \mapsto -\frac{1}{a_2} g_2(w_2) y_2^{-1} \end{cases}$$

where $\deg g_1 = 1-\alpha$, $\deg g_2 = 1-\beta$, $w_1 \mapsto -w_1 + l_1$, $w_2 \mapsto -w_2 + l_2$. ord $\eta = 2$ if α and β are odd; ord $\eta = 4$ if α or β is even.

Lemma 11. If $E_\varphi = \begin{pmatrix} 0 & A_\alpha \\ A_\alpha & 0 \end{pmatrix}$, then φ can be written as

$$\varphi_{algk} : \begin{cases} x_1 \mapsto a\frac{w_2-l}{g(w_2-1)}y_2 \\ y_1 \mapsto -\frac{1}{a}g(w_2)y_2^{-1} \\ x_2 \mapsto \frac{a}{\zeta_k}\frac{w_1-l}{g(-w_1+l)}y_1 \\ y_2 \mapsto -\frac{\zeta_k}{a}g(-w_1+l-1)y_1^{-1} \end{cases}$$

where $\deg g = 1-\alpha$, $w_1 \mapsto -w_2 + l$, $w_2 \mapsto -w_1 + l$ and ord $\varphi_{algk} = 4k$.

Proof. We can write φ as

$$x_1 \mapsto af_2(w_2)y_2$$

$$y_1 \mapsto -\tfrac{1}{a}g_2(w_2)y_2^{-1}$$

$$x_2 \mapsto bf_3(w_1)y_1$$

$$y_2 \mapsto -\tfrac{1}{b}g_3(w_1)y_1^{-1} \quad ,$$

$\deg f_2 = \deg f_3 = \alpha$, $\deg g_2 = \deg g_3 = 1-\alpha$, $w_1 \mapsto -f_2(w_2)g_2(w_2-1)$, $w_2 \mapsto -f_3(w_1)g_3(w_1-1)$. Since the image of w_1, w_2 must generate $k(x_1, x_2)$ so it must have the form $\frac{aw+b}{cw+b}$. Thus

$$w_1 \mapsto -f_2(w_2)g_2(w_2-1) = -w_2 + l_2$$

$$w_2 \mapsto -f_3(w_2)g_3(w_1-1) = -w_1 + l_1 \quad .$$

$\varphi^2 : w_1 \mapsto w_1 + (l_2 - l_1)$ and $w_2 \mapsto w_2 + (l_1 - l_2)$. Since ord φ^2 is finite, $l_1 = l_2$. Moreover, the exponent matrix of φ^2 is I. So

$$\varphi^2 : y_1 \mapsto \frac{b}{a}\frac{g_2(-w_1+l)}{g_3(w_1-l)}y_1 = \zeta_k^{-1}y_1$$
$$y_2 \mapsto \frac{a}{b}\frac{g_3(-w_2+l)}{g_2(w_2-l)}y_2 = \zeta_l^{-1}y_2 \quad .$$

Note that $\varphi^2 : x_1 \mapsto \frac{a}{b}\frac{g_3(w_1)}{g_2(-w_1+l-1)}y_1 = \zeta_k^{-1}y$, since $\frac{g_2(-w+l)}{g_3(w-1)} = \zeta_k\frac{a}{a}$ is a constant. Moreover, setting $w = -w_2 + 1 + l$ in the this constant, we have

$$\frac{g_2(w_2-1)}{g_3(-w_2+l)} = \zeta_k^{-1}\frac{a}{b} .$$

$$\zeta_l^{-1} = \frac{a}{b}\frac{g_3(-w_2+l)}{g_2(w_1-1)} = \frac{a}{b}(\zeta_k\frac{b}{a}) = \zeta_k . \qquad \square$$

Lemma 12. If $E_\varphi = \begin{bmatrix} 0 & B_\alpha \\ B_{2-\alpha} & 0 \end{bmatrix}$ then φ has the form

$$\rho_{algk} : \begin{cases} x_1 \mapsto a\frac{w_2+l}{g(w_2+1)}y_2^{-1} \\ y_1 \mapsto \frac{1}{a}g(w_2)y_2 \\ x_2 \mapsto \frac{\zeta_k}{a}(w_1-l)g(w_1+1-l)y_1^{-1} \\ y_2 \mapsto \frac{a}{\zeta_k}\frac{1}{g(w_1-l)}y_1 \end{cases}$$

where deg g_2=$\alpha - 1$. ord $\rho_{algk} = 2k$.

Proof. We may write

$$x_1 \mapsto af_2(w_2)y_2^{-1}$$

$$y_1 \mapsto \tfrac{1}{a}g_2(w_2)y_2$$

$$x_2 \mapsto bf_3(w_1)y_1^{-1}$$

$$y_2 \mapsto \tfrac{1}{b}g_3(w_1)y_1$$

where deg $f_2 = 2-\alpha$, deg $g_2 = \alpha - 1$, deg $f_3 = \alpha$, deg $g_3 = 1-\alpha$, $w_1 \mapsto f_2(w_2)g_2(w_2+1) = w_2 + l_2$, $w_2 \mapsto f_3(w_1)g_3(w_1+1) = w_1 + l_1$. Since $\varphi^2 : w_1 \mapsto w_1 + (l_1 + l_2)$, it has finite order, so $l_2 = -l_1$.

Now

$$\varphi^2 : y_1 \mapsto \frac{1}{ab}g_2(w_1-l)g_3(w_1)y_1 = \zeta_k^{-1}y_1$$
$$y_2 \mapsto \frac{1}{ab}g_3(w_2+l)g_2(w_2)y_2 = \zeta_l^{-1}y_2 .$$

Since $g_2(w_1 - l)g_3(w_1)$ is a constant, and it is equal to $g_3(w_2 + l)g_2(w_2)$, so $\zeta_k = \zeta_l$, and

$$g_3(w_1) = \frac{ab}{\zeta_k} \frac{1}{g_2(w_1 - l)} \; . \qquad \square$$

Lemma 13. If $E_\varphi = \begin{bmatrix} 0 & A_\alpha \\ B_\beta & 0 \end{bmatrix}$ then φ has the form

$$\pi_{a_1 a_2 l_1 l_2 g_1 g_2} : \begin{cases} x_1 \mapsto a_1 \frac{w_2 + l_1}{g_1(w_2+1)} y_2^{-1} \\ y_1 \mapsto \frac{1}{a_1} g_1(w_2) y_2 \\ x_2 \mapsto b_1 \frac{(w_1 + l_2)}{g_2(w_1 - 1)} y_1 \\ y_2 \mapsto \frac{1}{b_1} g_2(w_1) y_1^{-1} \end{cases}$$

where $w_1 \mapsto w_2 + l_1$ and $w_2 \mapsto -w_1 + l_2$ and g_1, g_2 satisfy

$$\frac{g_1(T)}{g_1(-T - l_1 + l_2 + 1)} = (-1)^{\alpha+\beta} \frac{g_2(T + l_1 - 1)}{g_2(-T + l_2)} \; ,$$

ord $\pi = 4$ if $\alpha + \beta$ is even and ord $\pi = 8$ if $\alpha + \beta$ is odd.

Proof. We may write φ as

$$x_1 \mapsto a_1 f_2(w_2) f_2^{-1}$$

$$y_1 \mapsto \tfrac{1}{a_1} g_2(w_2) y_2$$

$$x_2 \mapsto a_2 f_3(w_1) y_1$$

$$y_2 \mapsto -\tfrac{1}{a_2} g_3(w_1) y_1^{-1}$$

where $\deg f_2 = \beta$, $\deg g_2 = 1 - \beta$, $\deg f_3 = \alpha$, $\deg g_3 = 1 - \alpha$. Let $w_1 \mapsto f_2(w_2)g_2(w_2 + 1) = w_2 + l_1$, $w_2 \mapsto -f_3(w_1)g_3(w_-1) = -w_1 + l_2$. Then

$$\begin{aligned} y_1 \mapsto \frac{1}{a_1} g_2(w_2) y_2 &\mapsto \frac{-1}{a_1 a_2} g_2(-w_1 + l_2) g_3(w_1) y_1^{-1} \\ &\mapsto -\frac{1}{a_2} \frac{g_2(-w_2 - l_1 + l_2) g_3(w_2 + l_1)}{g_2(w_2 + 1)} y_2^{-1} \\ &\mapsto \frac{g_2(w_1 - l_1) g_3(-w_1 + l_1 + l_2)}{g_2(-w_1 + l_2 + 1) g_3(w_1 - 1)} y_1 := (-1)^{\alpha+\beta} y_1 \end{aligned}$$

$$y_2 \mapsto -\frac{1}{a_2} g_3(w_1) y_1^{-1} \mapsto -\frac{a_1}{a_2} \frac{g_3(w_2+l_1)}{g_2(w_2+1)} y_2^{-1}$$
$$\mapsto a_1 \frac{g_3(-w_1+l_1+l_2)}{g_3(w_1-1)g_2(-w_1+l_2+1)} y_1$$
$$\mapsto \frac{g_3(-w_2+l_2)g_2(w_2)}{g_3(w_2+l_1-1)g_2(-w_2-l_1+l_2+1)} y_2 := (-1)^{\alpha+\beta} y_2 .$$

So we have

$$\frac{g_2(w_1-l_1)g_3(-w_1+l_2-l_1)}{g_2(-w_1+l_2+1)g_3(w_1-1)} = \frac{g_3(-w_2+l_2)g_2(w_2)}{g_3(w_2+l_1-1)g_2(-w_2-l_1+l_2+1)} = (-1)^{\alpha+\beta} . \quad \square$$

§4. Characterization of monomial automorphism groups

Except the cyclic groups, we have the other groups list in the following.

Lemma 14. If $G_E = \langle \begin{pmatrix} A_\alpha & 0 \\ 0 & I \end{pmatrix} , \begin{pmatrix} I & 0 \\ 0 & A_\beta \end{pmatrix} \rangle$, then G is an abelian group generated by χ'_{bmlg_2}.

Proof. It follows from

$$\chi_{alkg_1} \chi'_{bmlg_2} = \eta_{(a\zeta_l^{-1})(b\zeta_k^{-1})lmg_1g_2} .$$

Lemma 15. If $G_E = \langle \begin{pmatrix} A_\alpha & 0 \\ 0 & A_{2\beta-\alpha} \end{pmatrix} , \begin{pmatrix} 0 & A_\beta \\ A_\beta & 0 \end{pmatrix} \rangle$, then G is a group generated by $\eta_{a_1a_2l_1l_2g_1g_2}$, φ_{mgk} and $\rho_{(a_1b^{-1})(m-l_1)(hg^{-1})k}$.

Lemma 16. If $G_E = \langle \begin{pmatrix} 0 & A_\alpha \\ B_\beta & 0 \end{pmatrix} , \begin{pmatrix} A_{\alpha+\beta-1} & 0 \\ 0 & I \end{pmatrix} \rangle$, then G is a group generated by $\pi_{a_1a_2l_1l_2g_1g_2}$ and χ_{bmkh}.

References

[1] J. Alev and F. Dumas. invariants du corps de Weyl sous l'action de groupes finis, Comm. in Alg., 25(1997), 1655-1672.

[2] J. Alev and F. Dumas, Sur les invariants des algebres Weyl et de leurs corps de fractions, preprint.

[3] H. Chu and C. C. Hsu, the invariants of monomial actions on Weyl fields, preprint.

[4] M. Hajja, Rational invariants of meta-abelian groups of linear automorphisms J. of Alg. 80 (1983), 295-305.

[5] M. Hajja and M. C. Kang, Three-dimensional purely monomial group actions, J. of Alg., 170 (1994) 805-860.

Lifting Elliptic Curves and Solving Elliptic Curve Discrete Logarithm Problem

Ming-Deh A. Huang* Ka Lam Kueh† Ki-Seng Tan‡

June 26, 1999

1 Introduction

The problem of lifting an elliptic curve over a finite field together with a finite set of points on the curve arises in extending the index calculus method for discrete logarithms over finite fields to work for the elliptic curve discrete logarithms problem. The first extension of the index calculus method as described by Miller in [5] involves lifting the elliptic curve E of interest to an elliptic curve $\mathcal{E}$ over the rationals, then lifting randomly chosen points from $E(\mathbb{F}_p)$ to $\mathcal{E}(\mathbb{Q})$. The difficulties of this approach were pointed out by Miller in [5] and more carefully analyzed by Silverman and Suzuki in [8]. Silverman [7] proposed an alternative extension - the xedni calculus, which involves first lifting a bounded number (nine) of points then finding a lift of the curve to fit the lifted points.

In this paper we analyze the problem of lifting elliptic curves with a finite set of points and draw several conclusions on the index calculus and the xedni calculus methods for solving the elliptic curve discrete logarithm problem over $\mathbb{F}_p$. More precisely, we derive necessary conditions for these

*Department of Computer Science, University of Southern California, Los Angeles, CA 90089-0781 (huang@pollux.usc.edu).

†Institute of Mathematics, Acedemia Sinica, Taipei, Taiwan (maklk@ccvax.sinica.edu.tw).

‡Department of Mathematics, National Taiwan University, Taipei, Taiwan (tan@math.ntu.edu.tw).

methods to possibly achieve asymptotic $O(\exp(c(\log p)^{1/2}(\log\log p)^{1/2})$ time complexity.

Concerning the index calculus method we show that, regardless of how a set of random points may be lifted from an elliptic curve E over a finite field $\mathbb{F}_p$ to an elliptic curve $\mathcal{E}$ over the rationals, the index calculus method will not give an asymptotic subexponential algorithm, unless the rank of $\mathcal{E}$ can grow at least as fast as $(\log p)^{1/4}$ as p grows.

Concerning the xedni calculus method we show that, regardless of how a curve $\mathcal{E}$ is constructed to fit the lifted points, the xedni calculus method will not give an asymptotic subexponential algorithm, unless the number of (randomly chosen) lifted points can grow at least as fast as $(\log p)^{1/4}$ as p grows. In particular, the xedni calculus method as described in [7] cannot work as a subexponential algorithm asymptotically speaking.

Our analysis depends on a conjecture of Lang [3] that the canonical height of any nonzero rational point on an elliptic curve $\mathcal{E}$ over $\mathbb{Q}$ is bounded from below by $c\log|\Delta(\mathcal{E})|$ where c is a universal constant independent of $\mathcal{E}$ and $\Delta(\mathcal{E})$ is the discriminant of $\mathcal{E}$. Assuming this conjecture one can show that if an elliptic curve over $\mathbb{Q}$ has rank less than r, then any set of r rational points on $\mathcal{E}$ has an integral relation whose coefficients can be bounded in terms of the heights of those points and r. (See Proposition 2.1.) This observation is the center piece of our analysis. A similar result has independently been obtained by Jacobson et al in [1], where the rank of the elliptic curve over $\mathbb{Q}$ is assumed to be bounded. It is also shown in [1] that with the xedni algorithm in [7] (where the number of lifted points is bounded), the probability of success in finding a discrete logarithm on an elliptic curve over a finite field is negligible asymptotically speaking.

Lang's conjecture is the only unproven assumption needed throughout this paper. Our analysis suggests that any extension of the index calculus method for solving the elliptic curve discrete logarithm problem is likely to encounter the following difficulty if it involves lifting an elliptic curve and points on the curve from a finite field $\mathbb{F}_p$: either the rank of the lifting curve or the number of random points to be lifted with the curve needs to grow as p grows. Our analysis also leads to an interesting connection between lifting many points with an elliptic curve over a finite field and constructing an elliptic curve of large rank over $\mathbb{Q}$.

2 The lifting problem and the elliptic curve discrete logarithm problem

Let E be an elliptic curve over a finite field $\mathbb{F}_p$ and $\lambda = (P_1, ..., P_m)$ with $P_i \in E(\mathbb{F}_p)$. Let $\mathcal{E}$ be an elliptic curve over $\mathbb{Q}$ and $\Lambda = (\mathcal{P}_1, ..., \mathcal{P}_m)$ with $\mathcal{P}_i \in \mathcal{E}(\mathbb{Q})$. We say that (E, λ) is lifted to $(\mathcal{E}, \Lambda)$ if E can be obtaineded as the reduction of $\mathcal{E}$ modulo p with P_i as the reduction of $\mathcal{P}_i$ modulo p for $i = 1, ..., m$. We say that λ is lifted with E with canonical height bounded by h if the canonical height of $\mathcal{P}_i$ is bounded by h for $i = 1, ..., m$.

Let $\hat{h}(\mathcal{P})$ denote the canonical height of $\mathcal{P}$ for $\mathcal{P} \in \mathcal{E}(\mathbb{Q})$ [6]. Let

$$N(\mathcal{E}, b) = \#\{\mathcal{P} \in \mathcal{E}(\mathbb{Q}) : \hat{h}(\mathcal{P}) \leq b\}.$$

Let $r = r(\mathcal{E})$ be the rank of $\mathcal{E}(\mathbb{Q})$, T be the number of torsion points in $\mathcal{E}(\mathbb{Q})$, and R be the regulator of $\mathcal{E}$ over $\mathbb{Q}$. Then it is known [3] that

$$N(\mathcal{E}, b) \approx T\alpha_r \left(\frac{b}{R^{1/r}}\right)^{r/2}.$$

Following the analysis in [8], we assume Lang's conjecture [3] that

$$\hat{h}(\mathcal{P}) \geq c \log |\Delta(\mathcal{E})|$$

for some constant c independent of $\mathcal{E}$, where $\Delta(\mathcal{E})$ denotes the discriminant of $\mathcal{E}$. Then from

$$R^{1/r} \geq \left(\frac{\sqrt{3}}{2}\right)^{r-1} \min \hat{h}(\mathcal{P})$$

where the minimum is over all nonzero $\mathcal{P} \in \mathcal{E}(\mathbb{Q})$ [3], and

$$\alpha_r \approx \frac{1}{\sqrt{\pi r}} \left(\frac{2\pi e}{r}\right)^{r/2},$$

and that $T \leq 16$ [4], it follws that for $r \geq 1$

$$N(\mathcal{E}, b) \leq 2^{c_1 r^2} \left(\frac{b}{\log |\Delta|}\right)^{r/2} \tag{1}$$

for some positive constant c_1 independent of $\mathcal{E}$.

Proposition 2.1 *There exists a positive constant c such that for all elliptuc curves $\mathcal{E}$ defined over $\mathbb{Q}$, if the rank of $\mathcal{E}(\mathbb{Q})$ is no greater than r, then for any $\mathcal{P}_0$, ..., $\mathcal{P}_r$ in $\mathcal{E}(\mathbb{Q})$ with $\hat{h}(\mathcal{P}_i) \leq h$, there exist integers c_i with $|c_i| \leq 2^{cr^2}(\frac{h}{\log|\Delta|})^{r/2}$ such that $\sum_i c_i\mathcal{P}_i = 0$, where Δ is the discriminant of $\mathcal{E}$.*

Proof For $\mathcal{P} \in \mathcal{E}(\mathbb{Q})$, let $||\mathcal{P}|| = \sqrt{\hat{h}(\mathcal{P})}$. For $a_i \in \{0, ..., m-1\}$,

$$||\sum_{i=0}^{r} a_i\mathcal{P}_i|| \leq \sum_{i=0}^{r} |a_i|||\mathcal{P}_i|| \leq \sqrt{h}\sum_{i=0}^{r} |a_i| \leq m(r+1)\sqrt{h}.$$

So

$$\hat{h}(\sum_{i=0}^{r} a_i\mathcal{P}_i) \leq m^2(r+1)^2h.$$

Since the number of $(a_0, ..., a_r)$ with $a_i \in \{0, ..., m-1\}$ is m^{r+1}, if

$$N(\mathcal{E}, m^2(r+1)^2h) < m^{r+1}, \tag{2}$$

then there must exist two distinct $(a_0, ..., a_r)$ and $(b_0, ..., b_r)$ with $a_i, b_i \in \{0, ..., m-1\}$ such that $\sum_i a_i\mathcal{P}_i = \sum_i b_i\mathcal{P}_i$, and hence $\sum_i c_i\mathcal{P}_i = 0$ with $c_i = a_i - b_i$, so $|c_i| < m$. From Eq. (1),

$$N(\mathcal{E}, m^2(r+1)^2h) < 2^{c_1r^2}\left(\frac{m^2(r+1)^2h}{\log|\Delta|}\right)^{r/2}$$

for some constant c_1 independent of $\mathcal{E}$. It follows that (2) holds if $m > 2^{cr^2}(h/\log|\Delta|)^{r/2}$ where c is a constant independent of $\mathcal{E}$. □

We now explore an immediate implication of the proposition on the index calculus method. In the elliptic curve discrete logarithm problem we are given an elliptic curve E over a finite field $\mathbb{F}_p$, and two points $S, T \in E(\mathbb{F}_p)$, and the problem is to find an integer m (if it exists) so that $mS = T$.

In the index calculus method outlined in [5], we first find an elliptic curve $\mathcal{E}$ defined over $\mathbb{Q}$ whose reduction mod p is E. Suppose $\mathcal{E}(\mathbb{Q})$ has rank r with generators $\mathcal{P}_i$, $i = 1$, ..., r, and suppose $P_i \in E(\mathbb{F}_p)$ is the reduction of $\mathcal{P}_i$ mod p. In the base building stage we seek to solve the discrete logarithms of P_i by choosing random j, lifting jS to some $S' \in \mathcal{E}(\mathbb{Q})$, and writing S'

in terms of $\mathcal{P}_i$ up to a torsion point. Each S' yields a linear relation on the discrete logarithms of P_i. With r many linearly independent relations we can solve for the discrete logarithms of all P_i.

Let h be an upper bound on $\hat{h}(\mathcal{P}_i)$ and $\hat{h}(S')$. Then from Proposition 2.1 it follows that there exist integers c_i with absolute values bounded by $2^{cr^2}(h/\log|\Delta|)^{r/2}$ such that

$$c_0 S' + c_1\mathcal{P}_1 + ... + c_r\mathcal{P}_r = 0$$

so

$$c_0(jS) + c_1 P_1 + ... + c_r P_r = 0.$$

The number of $P \in E(\mathbb{F}_p)$ satisfying

$$c_0 P + c_1 P_1 + ... + c_r P_r = 0$$

with $|c_i| \leq 2^{cr^2}(h/\log|\Delta|)^{r/2}$ is bounded by $2^{O(r^3)}h^{O(r^2)}$. It follows that the probability that a random jS can be lifted to some S' with height bounded by h is no greater than $\frac{2^{O(r^3)}h^{O(r^2)}}{p}$. For the probability to be at least $1/exp[(\log p)^{1/2}(\log\log p)^{1/2}]$, say, it is necessary that $r^2\log h > c'\log p$ for some constant c'. Even if we allow the points to be lifted to subexponential canonical height so that h is about $exp[(\log p)^{1/2}(\log\log p)^{1/2}]$, the rank r of $\mathcal{E}$ still needs to be at least in the order of $(\log p)^{1/4}$.

Note that the observation above holds regardless of the method used to lift a point from E to $\mathcal{E}$. The fact that the rank of $\mathcal{E}$ needs to grow at least as fast as $(\log p)^{1/4}$ as p grows already poses a significant difficulty for the index calculus method to work.

Next we turn our attention to the xedni calculus method for the elliptic curve discrete logarithm problem.

Proposition 2.2 *Let E be an elliptic curve over a finite field $\mathbb{F}_p$. For $r \in \mathbb{Z}_{>0}$ and $h \in \mathbb{R}_{>0}$, let $n_E(r,h)$ denote the number of $\lambda = (P_0, ..., P_r)$ with P_i in some cyclic subgroup of $E(\mathbb{F}_p)$ so that (E,λ) can be lifted to some $(\mathcal{E}_\lambda, \Lambda)$ over $\mathbb{Q}$ with the canonical heights of the points in Λ bounded by h and the rank of $\mathcal{E}(\mathbb{Q})$ bounded by r. Then $n_E(r,h)$ is bounded by $2^{O(r^3)}(h/\log|\Delta|)^{O(r^2)}N^r$ where $N = |E(\mathbb{F}_p)|$.*

Proof Let $\lambda = (P_0, ..., P_r)$ with P_i in some cyclic subgroup of $E(\mathbb{F}_p)$ with a generator S. Suppose (E, λ) is lifted to some $(\mathcal{E}, \Lambda)$ with canonical height bounded by h. Suppose $\Lambda = (\mathcal{P}_0, ..., \mathcal{P}_r)$. If the rank of $\mathcal{E}(\mathbb{Q})$ is bounded by r, then from Proposition 2.1 it follows that there exist integers c_i such that

$$\sum_i c_i \mathcal{P}_i = 0,$$

where

$$|c_i| \leq 2^{cr^2} \left(\frac{h}{\log |\Delta|} \right)^{r/2}$$

and Δ is the discriminant of $\mathcal{E}$.

Suppose $P_i = m_i S$. Then

$$0 = \sum_i c_i P_i = (\sum_i c_i m_i) S.$$

So

$$\sum_i c_i m_i \equiv 0 \pmod{N}$$

where N is the order of S. Now $n_E(r, h)$ is bounded by the number of $(m_0, ..., m_r)$ such that $\sum_i c_i m_i \equiv 0 \pmod{N}$ and $|c_i|$ is bounded by

$$M = 2^{cr^2} \left(\frac{h}{\log |\Delta|} \right)^{r/2}.$$

For each $c = (c_0, .., c_r)$, let n_c denote the the number of $(m_0, ..., m_r) \bmod N$ such that

$$c_0 m_0 + ... + c_r m_r \equiv 0 \pmod{N}.$$

Suppose the g.c.d. of c_0, ..., c_r is g, then

$$n_c \leq g N^r \leq M N^r.$$

So

$$n_E(r, h) \leq (2M + 1)^{r+1} M N^r = 2^{O(r^3)} (h / \log |\Delta|)^{O(r^2)} N^r.$$

□

In the xedni calculus method, instead of lifting the curve E, we first generate random P_0, ..., P_r with $P_i = a_i S + b_i T$ where a_i, b_i are random integers. We lift P_i to some $\mathcal{P}_i$ over $\mathbb{Q}$, then construct an elliptic curve $\mathcal{E}$ over $\mathbb{Q}$ so that the pair $\mathcal{E}$ and $(\mathcal{P}_0, ..., \mathcal{P}_r)$ is a lift of E and $(P_0, ..., P_r)$. If the rank of $\mathcal{E}(\mathbb{Q})$ is no greater than r, then $\mathcal{P}_0$, ..., $\mathcal{P}_r$ are integrally dependent, so that

$$\sum_i c_i \mathcal{P}_i = 0$$

for some integers c_i, then upon reduction mod p we have

$$0 = \sum_i c_i(a_i S + b_i T) = (\sum_i c_i a_i)S + (\sum_i c_i b_i)T.$$

From this the discrete logarithm of T in terms of S can be obtained with high probability, since a_i and b_i are randomly chosen.

Let h be an upper bound on $\hat{h}(\mathcal{P}_i)$. The number of random $\lambda = (P_0, ..., P_r)$ is bounded by N^{r+1}. Such a λ will lead to a success in finding the discrete logarithm only if (E, λ) can be lifted to some $(\mathcal{E}_\lambda, \Lambda)$ over $\mathbb{Q}$ with the canonical heights of the points in Λ bounded by h and the rank of $\mathcal{E}(\mathbb{Q})$ bounded by r. The number of such $(r+1)$-tuples is bounded by $n_E(r, h)$, which by Proposition 2.2 is bounded by $2^{O(r^3)}(h/\log|\Delta|)^{O(r^2)}N^r$. Hence the success probablity is bounded by $\frac{2^{O(r^3)}(h/\log|\Delta|)^{O(r^2)}}{N}$. Since N can be in the order of p, for the success probability to be at least $1/exp[(\log p)^{1/2}(\log\log p)^{1/2}]$, say, it is necessary that $r^2 \log h > c' \log p$ for some constant c'. Even if we allow the points to be lifted to subexponential canonical height so that h is about $exp[(\log p)^{1/2}(\log\log p)^{1/2}]$, the number of lifted points $r+1$ needs to be at least in the order of $(\log p)^{1/4}$ as p grows. This is true regardless of how the curve $\mathcal{E}$ is constructed for each $(r+1)$-tuple of points in $E(\mathbb{F}_p)$. In particular, for bounded r (such as the case with the xedni method in [7]), the probability of success tends to zero as p grows. Hence the xedni calculus method as described in [7] cannot work as a subexponential algorithm asymptotically. To extend the scope of applicability of the xedni calculus idea, we need to increase the number of points on an elliptic curve over a finite field that can be lifted with the curve with reasonably bounedd canonical height. The xedni calculus method in [8] sets the number of lifted points for nine, but it is not clear whether this number is maximum possible.

It is perhaps interesting to point out that a larger bound would also imply the existence of elliptic curves of large rank. Suppose it is possible to lift a fraction of all r-tuples of points on an elliptic curve over $\mathbb{F}_p$ with canonical height bounded by h, where $\log h / \log p$ tends to 0 as p tends to infinity. Then Proposition 2.2 implies that for sufficiently large p, some elliptic curve over $\mathbb{Q}$ lifting some elliptic curve over $\mathbb{F}_p$ and some r-tuple of points must have rank at least r.

3 Acknowledgement

We would like to thank Yen-Mei Chen for informing us of the result independently obtained by Jacobson et al in [1].

References

[1] M.J. Jacobson, N. Koblitz, J.H. Silverman, A. Stein, and E. Teske, Analysis of the Xedni Calculus Attack, Preprint.

[2] N. Koblitz, Elliptic curve cryptosystems, *Math. Comp.*, 48, pp. 203-209, 1987.

[3] S. Lang, *Fundamental of Diophantine Geometry*, Springer-Verlag, 1983.

[4] B. Mazur, Modular curves and Eisenstein ideal, *I.H.E.S. Publ. Math.* 47 (1977), 33-186.

[5] V. Miller, The use of elliptic curves in cryptography. *Advances in Cryptography*, Ed. H.C. Williams, Springer-Verlag, 1986, 417-426.

[6] J.H. Silverman, *The Arithmetic of Elliptic Curves*, Springer-Verlag, 1986.

[7] J.H. Silverman, The xedni calculus and the elliptic curve discrete logarithm problem, preprint.

[8] J.H. Silverman and J. Suzuki, Elliptic curve discrete logarithms and the index calculus, *Advances in Cryptology -Asiacrypt '98*, Springer-Verlag, 1998, 110-125.