効率的なCGLハッシュ関数の構成について.（橋本 侑知 / 東京電機大） 1-⑥

・ハッシュ関数 $H : \{0,1\}^* \longrightarrow \{0,1\}^n$ は任意長のbit列から固定長のbit列に圧縮する効率的に計算可能な関数

（多項式時間で）

（何かしらの情報を保存する）

・ハッシュ関数の安全性（collision - resistance）

$H(x_1) = H(x_2)$ となる $x_1 \neq x_2$ を見つけるのが困難である.

・2-同種写像グラフ.

頂点 ： 楕円曲線（の同型類）/ $\mathbb{F}_q$ （$q = p^2$, pは奇素数）

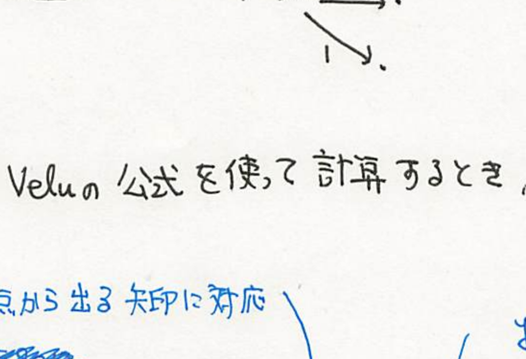
辺 ： 2-同種写像

次数は常に3.

となるようなグラフ.

・CGLハッシュ関数

- input： 2-同種写像グラフの walk data $w \in \{0,1\}^m$
  （と始点となる楕円曲線）
- output： j-invariant（始点からwalk wを辿った先の）
  完全不変量
- 安全性： $H(w) = H(w')$ となる $w \neq w'$ を計算することが困難.



・2-同種写像をVeluの公式を使って計算するとき，2-torsion point が必要となる.

これを見つけるのが困難

（α, β, γ が頂点から出る矢印に対応していて，~~[illegible]~~

の形）

→ （$y^2 = x^3 + ax + b$

$= (x-\alpha)(x-\beta)(x-\gamma)$

のとき，α, β, γ が 2-torsion pt.）

$$\begin{aligned} y^2 &= x^3 - ax + b \\ &= (x-\alpha_i)(x-\beta_i)(x-\gamma_i) \end{aligned}$$

i番目の楕円曲線の2-torsion pt.

i+1番目の ——

となっているとき, $y^2 = (x-\alpha_{i+1})(x-\beta_{i+1})(x-\gamma_{i+1})$ に効率的に計算する方法が Yoshida-Takashimaの方法.

$$\rightsquigarrow \begin{cases} \beta_{i+1} = -2\alpha_i \\ \alpha_{i+1}, \gamma_{i+1} = \alpha_i \pm 2\sqrt{(\beta_i-\alpha_i)(\gamma_i-\alpha_i)} \end{cases}$$ (ただし, β_i, β_{i+1} はバックトラック)

・Hashimoto-Nuida法

予備知識 : Legendre 曲線 $E_\lambda : y^2 = x(x-1)(x-\lambda)$ (λ は Legendre parameter)

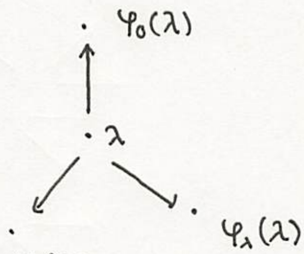
$p=2$ 以外の楕円曲線は E_λ へ変換可能

<u>大雑破な方針</u>

$E_\lambda \longrightarrow E_{\lambda'} \longrightarrow E_{\lambda''}$ のとき, λ と λ'' の関係式をみつける.

$E_\lambda, E_{\lambda'}$ をそれぞれ i, $i+1$番目の Legendre 曲線とする.
このとき, i番目の Legendre パラメータ λ を入力として, $i+1$番目の Legendre パラメータ λ' を出力するような関数 (fundamental Legendre map) と呼ぶ.
これを φ とおく:

$$\varphi_\bullet(\lambda) := \lambda'. \quad \bullet = 0, 1, \lambda$$



$$\rightsquigarrow \varphi_0(\lambda) = \left(\frac{\sqrt{\lambda}+1}{\sqrt{\lambda}-1}\right)^2$$

$$\varphi_1(\lambda) = \left(\frac{\sqrt{1-\lambda}+1}{\sqrt{1-\lambda}-1}\right)^2$$

$$\varphi_\lambda(\lambda) = \left(\frac{\sqrt{\lambda-1}+\sqrt{\lambda}}{\sqrt{\lambda-1}-\sqrt{\lambda}}\right)^2$$

Fact

$\varphi_0 \circ \varphi_0$, $\varphi_0 \circ \varphi_1$, $\varphi_0 \circ \varphi_\lambda$ はいずれも back-track する.

Theorem

k を $0, 1, \lambda$ のいずれかの値とする.

このとき, $1-\varphi_0(1-\varphi_k(\lambda))$ は non-backtrak な Legendre パラメータとなる.