Rational Points of Weighted Hypersurfaces over $\mathbb{F}_q$

An application to cryptography

Tanush Shaska

Oakland University, Rochester, Michigan

5th Pythagorean Conference,
Kalamata, Greece, June 1–6, 2025

shaska@oakland.edu

GENUS 2 CURVES I

Every genus 2 curve C over a field k of characteristic in $\mathrm{char}\, k \neq 2$ has affine equation

$$Y^2 = a_6X^6 + a_5X^5Z + \cdots + a_1X + a_0$$

Its invariants are:

$$\begin{aligned}
J_2 :=& -240a_0a_6 + 40a_1a_5 - 16a_2a_4 + 6a_3^2\\
J_4 :=& 48a_0a_4^3 + 48a_2^3a_6 + 4a_2^2a_4^2 + 1620a_0^2a_6^2 + 36a_1a_3^2a_5 - 12a_1a_3a_4^2 - 12a_2^2a_3a_5 + 300a_1^2a_4a_6 + 300a_0a_5^2a_2\\
&+ 324a_0a_6a_3^2 - 504a_0a_4a_2a_6 - 180a_0a_4a_3a_5 - 180a_1a_3a_2a_6 + 4a_1a_4a_2a_5 - 540a_0a_5a_1a_6 - 80a_1^2a_5^2\\
J_6 :=& -a_5^2a_4^2a_2^2 + 1600a_1^3a_5a_4a_6 + 1600a_1a_5^3a_0a_2 - 2240a_1^2a_5^2a_0a_6 + 20664a_0^2a_4a_6^2a_2 - 640a_0a_4a_2^2a_5^2 - 18600a_0a_4a_1^2a_6^2 + 76a_1a_3a_2a_4^3 - 198a_1a_3^3a_2a_6\\
&+ 26a_1a_3a_2^2a_5^2 + 616a_2^3a_5a_1a_6 + 28a_1a_4^2a_2^2a_5 - 640a_1^2a_4^2a_2a_6 + 26a_1^2a_4^2a_3a_5 + 616a_1a_4^3a_0a_5 + 59940a_0^2a_5a_6^2a_1 + 330a_0a_5^2a_2^2a_3 + 8a_2^2a_3^2a_4^2 - 24a_2^2a_3^2a_5\\
&+ 60a_2^3a_3^2a_6 + 60a_0a_4^3a_3^2 - 192a_2^3a_0a_6^2 - 320a_2^4a_4a_6 + 176a_1^2a_5^2a_3^2 + 2250a_1^3a_3a_6^2 - 900a_2^2a_1^2a_6^2 - 900a_0^2a_5^2a_4^2 - 10044a_0^2a_6^2a_3^2 + 162a_0a_6a_3^4 - 36a_2^4a_5^2\\
&- 36a_1^2a_4^4 + 76a_2^3a_2 - 320a_1^3a_5^3 + 484a + 492a_0a_4^2a_2a_3a_5 + 492a_0a_4^2a_2a_3a_5 + 3060a_0^2a_4a_6a_3a_5 - 468a_0a_4a_5^2a_2a_6 + 3472a_0a_4a_2a_5a_1a_6 + 492a_1a_3a_2^2a_4a_6\\
&- 238a_1a_5^2a_2a_4a_5 + 1818a_1a_5^2a_0a_6a_5 - 876a_2^2a_0a_6a_3a_5 - 3a_5 - 198a_0a_4a_3^2a_5 + 330a_1^2a_5^2a_6a_4 + 72a_1a_5^3a_5 - 24a_1a_3^3a_4^2 + 2250a_0^2a_5^3a_3 - 1860a_1a_4a_0a_5^2a_3\\
&+ 3060a_1a_3a_0a_6^2a_2 - 876a_0a_4^2a_1a_6a_3 - 1860a_1^2a_3a_2a_5a_6 - 18600a_0^2a_5^2a_6a_2 - 24a_2^3a_4^3 - 119880a_0^3a_6^3
\end{aligned}$$

$$J_{10} := a_6^{-1}\, Res_X\left(f, \frac{\partial f}{\partial X}\right)$$

Two genus 2 curves $\mathcal{X}$ and $\mathcal{X}'$ are isomorphic over k if and only if exists $\lambda \in k^\star$ such that

$$J_{2i}(\mathcal{X}) = \lambda^{2i} J_{2i}(\mathcal{X}').$$

Let the space of all tuples (J_2, J_4, J_6, J_{10}) be S. Define the following relation in S as follows. Two tuples

$$(J_2, J_4, J_6, J_{10}) \sim (J_2', J_4', J_6', J_{10}') \iff \exists \lambda \in k^\star,\ (J_2, J_4, J_6, J_{10}) = \left(\lambda^2 J_2', \lambda^4 J_4', \lambda^6 J_6', \lambda^{10} J_{10}'\right)$$

The set of equivalence classes is called a weighted projective space denoted by $\mathbb{WP}_{(2,4,6,10),k}$.

It can be mapped to the projective space $\mathbb{P}^3$ via the Veronese map

$$\mathbb{WP}_{(2,4,6,10),k} \to \mathbb{P}^3_k, \quad \text{via}$$
$$[J_2 : J_4 : J_6 : J_{10}] \longrightarrow \left[J_2^{30} : J_4^{15} : J_6^{10} : J_{10}^6\right].$$

Since J_{10} is the discriminant then $J_{10} \neq 0$ and we can get "affine" invariants as

$$\left[J_2^{30} : J_4^{15} : J_6^{10} : J_{10}^6\right] = \left[\frac{J_2^{30}}{J_{10}^6} : \frac{J_4^{15}}{J_{10}^6} : \frac{J_6^{10}}{J_{10}^6} : 1\right]$$

Thus, two genus curves are isomorphic if and only if they have the same invariants

$$i_1 := \frac{J_2^{30}}{J_{10}^6}, \quad i_2 := \frac{J_4^{15}}{J_{10}^6}, \quad i_3 := \frac{J_6^{10}}{J_{10}^6}$$

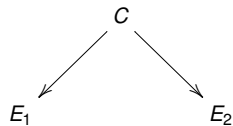
Such invariants i_1, i_2, i_3 are $GL_2(k)$-invariants and sometimes are called absolute invariants.

(N, N)-SPLIT JACOBIANS I

Let C genus 2 curve, E elliptic curve and $\psi_1 : C \to E_1$ be a degree n map(covering). I is called a maximal covering or optimal covering if it does not factor through a nontrivial isogeny.
Let $\psi_1 : C \longrightarrow E_1$ be maximal.

Then there exists an injective map ${\psi^*}_1 : E_1 \to J_C$. Let $E_2 := J_C/E_1$. Hence, E_2 is an elliptic curve. From the natural projection

$$J_C \to E_2, \quad \text{we obtain} \quad \psi_2 : C \to E_2$$



We say that J_C is (n, n)-split. The set of all curves with (n,n)-split Jacobians is an irreducible, 2-dimensional locus in the moduli space $\mathcal{M}_2$, denoted by $\mathcal{L}_n$.

The locus $\mathcal{L}_2$ is a closed subvariety of $\mathcal{M}_2$ with equation

$$\begin{aligned}
&-J_2^7J_4^4 + 8748J_{10}J_2^4J_6^2 507384000J_{10}^2J_4^2J_2 - 19245600J_{10}^2J_4J_2^3 - 592272J_{10}J_4^4J_2^2 + 77436J_{10}J_4^3J_2^4 - 78J_2^5J_4^5 - 81J_2^3J_6^4\\
&-3499200J_{10}J_2J_6^3 + 4743360J_{10}J_4^3J_2J_6 - 870912J_{10}J_4^2J_2^3J_6 + 3090960J_{10}J_4J_2^2J_6^2 - 5832J_{10}J_2^5J_4J_6 + 1332J_2^4J_4^4J_6 - 125971200000J_{10}^3\\
&+384J_4^6J_6 + 41472J_{10}J_4^5 - 236196J_{10}^2J_2^5 - 54J_2^5J_4^2J_6^2 - 47952J_2J_4J_6^4 + 104976000J_{10}^2J_2^2J_6 - 1728J_4^5J_2^2J_6 + 6048J_4^4J_2J_6^2 - 9331200J_{10}J_4^2J_6^2\\
&+108J_2^4J_4J_6^3 + 12J_2^6J_4^3J_6 + 29376J_2^2J_4^2J_6^3 - 8910J_2^3J_4^3J_6^2 - 2099520000J_{10}^2J_4J_6 + 31104J_6^5 - 6912J_4^3J_6^34 + 972J_{10}J_2^6J_4^2 - 80J_4^7J_2 + 159J_4^6J_2^3 =0
\end{aligned}$$

Notice the weighted degree is 30

(N, N)-SPLIT JACOBIANS II

The equation of $\mathcal{L}_3$ is:

$$C_8 J_{10}^8 + C_7 J_{10}^7 + \cdots + C_1 J_{10} + C_0 = 0, \text{ where } C_0, \ldots, C_8 \text{ are:}$$

$$C_8 = 2^4 \cdot 3^{31} \cdot 5^5 \cdot 19^{10} \cdot 29^5$$

$$C_7 = 2^4 \cdot 3^{27} \cdot 19^5 \left(-1948946400295111 J_2^5 - 55588661819356000 J_4^2 J_2 - 12239149540657725 J_2^3 J_4 + 223103526505680000 J_4 J_6 + 40811702108053500 J_2^2 J_6\right)$$

$$C_6 = 2^2 \cdot 3^{21}(-358022844687577658584 32 J_4^5 - 17562703991065877030391 J_4^2 J_2^6 - 28638991859523006654 J_4 J_2^8 - 84091225203760159441286 J_4^3 J_2^4$$
$$+ 400895959391006935610 32 J_4^4 J_2^2 - 617736857389994 43 J_2^{10} - 367320139607225960375616 0 J_4^3 J_2 J_6 + 787949175521826498438720 0 J_4^2 J_6^2$$
$$+ 152514473556086586299 52 J_2^5 J_4 J_6 + 117990300838484406625027 2 J_2^3 J_4^2 J_6 - 556667239858980988965876 0 J_2^2 J_4 J_6^2 + 112024289372554183680 J_7^2 J_6$$
$$- 321167694097227161828 88 J_2^4 J_6^2 + 851217187775496224915520 0 J_2 J_6^3)$$

$$C_5 = 2^2 \cdot 3^{19}(-126300043826954626 53 J_4^4 J_2^7 + 320839252764287362560 J_4^7 J_2 - 187606927239713688644 88 J_4^6 J_2^3 + 606742866220456356580 J_4^5 J_2^5 - 124173485719052715 J_4^3 J_2^9$$
$$+ 222410345121014389440000 J_4^5 J_2^2 J_6 - 885467367039388263045 12 J_4^4 J_2 J_6^2 - 107120789264207534499 84 J_2^4 J_4^4 J_6 + 689046353233036645 11264 J_2^3 J_4^3 J_6^2$$
$$- 192353895694677164016384 J_2^2 J_4^2 J_6^3 + 197449733923926905783808 J_2 J_4 J_6^4 - 191617304737164522393 6 J_6^6 J_6 + 116211018774997425051648 J_4^3 J_6^3$$
$$- 132143597697786172416 J_6^5 + 136140354245728 8 J_2^{10} J_4 J_6 - 500576511874049265 6 J_2^7 J_4 J_6^2 + 232819061639483430720 J_2^6 J_4^3 J_6 - 157631989469458517845 2 J_2^5 J_4^2 J_6^2$$
$$+ 465523945920876455308 8 J_2^4 J_4 J_6^3 - 226900590409548 J_2^{11} J_4^2 - 204210531368593 2 J_2^9 J_6^2 + 626163275596787280 0 J_2^6 J_6^3 - 506573479647827557617 6 J_2^3 J_6^4 + 135231810935082$$

$$C_4 = 3^{15}(14178253171532773 12 J_4^9 J_2^2 + 2391308818408811717 J_4^6 J_2^8 + 718590303030600 J_2^{10} J_4^5 - 638760745337170544640 J_4 J_6^6 + 440759275303802880 J_4^{10}$$
$$- 811871728077168654019 2 J_4^5 J_2^4 J_6^2 + 426684349068633980190 72 J_4^2 J_2 J_6^5 - 570546648140206405743 36 J_4^3 J_2^2 J_6^4 + 305467747401585816760 32 J_4^4 J_2^3 J_6^3$$
$$+ 860181421512383127590 4 J_4^6 J_2^2 J_6^2 - 144956270068219591680 0 J_4^7 J_2^3 J_6 + 106792835412424930310 4 J_4^6 J_2^5 J_6 - 104438962630243163013 12 J_2^3 J_4 J_6^5$$
$$+ 724797031515043028112 J_2^2 J_4^2 J_6^4 - 217692411767517366190 08 J_4^5 J_2 J_6^3 - 264020191999154595648 J_2^5 J_4^3 J_6^3 - 558935624244452613 12 J_2^7 J_4^2 J_6$$
$$+ 531409635241191119304 J_2^6 J_4^4 J_6^2 - 10126142051335 20 J_2^8 J_4^3 J_6^2 - 245485501532619955 2 J_2^5 J_6^5 - 125014099399 20 J_2^{12} J_4^4 - 675076136755680 J_2^{10} J_4^2 J_6^2$$
$$- 333905186668284 00 J_2^9 J_4^4 J_6 + 318836356802749843 2 J_2^6 J_4^4 J_6^3 - 156900149854740230 4 J_2^7 J_2^2 J_6^3 - 275375222428239820800 J_2^7 J_6^5 + 198098490955180503306 24 J_4^4 J_6^4$$

(N, N)-split Jacobians III

$$C_3 = 2^4 \cdot 3^{12}(-19225816442103600J_4^{10}J_2^5 + 643395269039414 4J_2^4J_6^7 - 2917203075615J_2^{11}J_4^7 + 629516056136 40J_2^{10}J_6^4J_6 + 7900854051362368J_4^{11}J_2^3 - 873165475591982J_2^9J_6^8$$
$$+ 4077902864550187008J_4^5J_6^5 + 7506792545698293J_4^9J_2^7 - 55019014994202624J_4^{11}J_6 - 3415519987075510272J_2^4J_6^7 - 9326051372726231 04J_4^8J_6^3 - 6607177263254292480J_2$$
$$- 2582935938 00J_2^{11}J_4^4J_6^2 - 19762995976163015 04J_4^8J_2^3J_6^2 + 13375981920858041744J_4^7J_2^5J_6^2 - 2324642344200J_2^9J_4^2J_6^4 + 2789570813040J_2^8J_4J_6^5 - 243015467955111198J_2^7J_4^3$$
$$- 155463896437263612J_4^8J_2^5J_6 + 161010337961830043 52J_4^5J_2^3J_6^4 + 1636729863179645030 4J_4^3J_2J_6^5 + 8433152J_4^7J_2^2J_6^3 - 825496517802146918 4J_6^4J_2J_6^4 + 34439145840J_2^{12}J_4^5J$$
$$- 8749875412454175J_2^7J_4^3J_6^4 + 156375115922003 40J_6^2J_4^2J_6^5 - 127105068829245696J_4^{10}J_2^2J_6 + 614908581517421568J_4^9J_2J_6^2 - 2337441943136020761 6J_4^4J_2^2J_6^5 + 1508868948 6$$
$$+ 140949838965116301 12J_2^4J_4^3J_6^5 + 10331743752002 0J_2^{10}J_4^3J_6^3 + 3140697982040647 2J_4^9J_2^4J_6 - 61501104J_6^4J_2^5J_6^3 - 2119416308022025024J_2^3J_2^2J_6^6 + 1800240211976332544J$$
$$C_2 = 2^5 \cdot 3^8(-159732958548480J_4^{13}J_2J_6 - 279451929685939 20J_2J_4J_6^9 + 2385961241500 86J_4^{10}J_2^7J_6 + 3224288J_2^3J_6^9 - 3631113621524 4J_2^9J_4^3J_6 - 996173640J_2^{12}J_6^4J_6^2 + 59770$$
$$+ 142103120496971 49J_2^5J_6^6J_6^4 + 8635491888558076 8J_2^4J_4^4J_6^6 - 111444977082978432J_2^3J_4^7J_6^7 + 279088939778 56J_4^{14}J_2^2 + 837681410382515 2J_2^6J_2^4J_6^8 - 4294298096876548 8J_2^5$$
$$+ 410958880454688J_4^{12}J_2^3J_6 - 140592520576604 16J_4^3J_6^8 - 164365980986649 6J_4^{11}J_2^2J_6^2 + 441832778741790J_2^8J_4^2J_6^2 - 3128599551108636J_2^7J_4^7J_6^3 + 2815950495430656J_4^{10}J_2$$
$$- 2286353789913249J_4^9J_2^8J_6^2 - 403004765256293 52J_4^7J_2^4J_6^4 + 817070437989290 88J_6^6J_2^3J_6^5 - 2593609227 0J_2^8J_6^8 - 9825776527448908 8J_4^5J_2^2J_6^6 + 3318887207480832J_4^{10}J_2^4J_6^2$$
$$- 121532536493026 56J_4^9J_2^3J_6^3 + 2475797570016537 6J_4^8J_2^2J_6^4 - 265709024579819 52J_4^7J_2J_6^5 - 67550650890 24J_4^{15} + 10883911680J_6^{10} + 5379337656 0J_2^9J_4^3J_6^5 - 8069006484 0J$$
$$+ 227109129291J_2^{10}J_4^7J_6^2 - 628213747356J_2^9J_6^6J_6^3 - 1389130574661J_2^8J_4^5J_6^4 + 164657939888 70J_2^7J_4^4J_6^5 - 5679419194 4715J_2^6J_4^3J_6^6 + 102713329135 52J_2^5J_2^4J_6^7 - 985297464 5$$
$$- 1716480768J_4^9J_6^4 + 117180539541900 40J_6^6J_6^6 + 220752428322816J_4^{12}J_6^2 + 1322792799725J_2^{10}J_4^{10} - 3953070J_2^{14}J_6^8)$$
$$C_1 = -2^8 \cdot 3^5(61736960J_6^8J_2 - 182135808J_4^7J_6 + 16021872J_4^7J_2^3 - 211022400J_6^4J_2^2J_6 - 26594919J_6^4J_2^5 + 899159040J_4^5J_2J_6^2 + 330458928J_6^5J_4^2J_6 - 215198J_2^7J_5^5 - 12274053$$
$$+ 2930532J_4^4J_2^5J_6 - 363J_2^9J_4^4 + 3162070656J_4^3J_2^2J_6^3 - 16471998J_4^3J_2^5J_6^2 + 4356J_4^3J_2^8J_6 - 19602J_4^2J_2^7J_6^2 - 2433162240J_4^2J_2J_6^4 + 47961936J_4^2J_2^4J_6^3 + 39204J_4J_2^6J_6^3 - 72369$$
$$+ 45116352J_2^2J_6^5)(J_4^3 - J_2^2J_4^2 + 6J_2J_6J_4 - 9J_6^2)^3$$
$$C_0 = 2^8(768J_4^2 - 416J_4J_2^2 - J_4^2 + 1536J_2J_6)(J_4^3 - J_2^2J_4^2 + 6J_2J_6J_4 - 9J_6^2)^6$$

(N,N)-SPLIT JACOBIANS AND ISOGENY BASED CRYPTOGRAPHY

Isogeny based cryptography: Analogous to the Diffie–Hellman key exchange, but based on walks in a supersingular isogeny graph and was designed to resist cryptanalytic attack by an adversary in possession of a quantum computer.

Supersingular Isogeny Diffie–Hellman key exchange (SIDH or SIKE)
1997 Couveignes introduces the Hard Homogeneous Spaces framework. (unpublished for 10 years.)
2006 Rostovtsev & Stolbunov suggest isogeny-based Diffie–Hellman as a quantum-resistant primitive.
2011-2012 De Feo, Jao & Plut introduce SIDH, an efficient post–quantum key exchange
2017 SIDH is submitted to the NIST competition (with the name SIKE, only isogeny-based candidate).
2022 SIDH is broken by Castryck, Decru.

Isogeny-based cryptography based on (n,n)-split Jacobians: Now the isogenies are $(n, n,)$-isogenies between Jacobian surfaces (Jacobians of genus 2 curves).

Such curves are exactly curves with (n, n)-split Jacobians, parameterized by the loci $\mathcal{L}_n$, $(n = 2, 3, 5)$, as their splitting property enables the construction of isogenies with kernel $(\mathbb{Z}/n\mathbb{Z})^2$.

Advanced Research Workshop : Isogeny based post-quantum cryptography,
Hebrew University of Jerusalem, July 29-31, 2024.

Next we outline a method to compute such (n, n)-isogenies over a finite field $\mathbb{F}_q$, utilizing the structure of $\mathcal{L}_n$.

Computing (n, n)-Isogenies I

To compute an (n, n)-isogeny $\phi : J(C) \to E_1 \times E_2$ for a genus 2 curve C over $\mathbb{F}_q$ with $J(C)$ (n, n)-split, we utilize the locus $\mathcal{L}_n$ in $\mathbb{P}_{\mathbf{w}} = \mathbb{P}(2, 4, 6, 10)$, defined by $F_n(J_2, J_4, J_6, J_{10}) = 0$. The process is outlined as follows.

- Pick a rational point $\mathfrak{p} \in \mathcal{L}_n$ over $\mathbb{F}_q$

$$\mathfrak{p} = [J_2 : J_4 : J_6 : J_{10}] \in \mathcal{L}_n(\mathbb{F}_q),$$

- Construct the genus two curve C: $y^2 = f(x)$ using (Malmendier and Shaska, 2017).
- Compute the Jacobian $J(C)$ as the group of degree-0 divisor classes on C, represented via Mumford's coordinates (pairs $(u(x), v(x))$).
- Determine the n-torsion subgroup $J(C)[n]$: The n-torsion subgroup $J(C)[n]$ over an algebraic closure is isomorphic to $(\mathbb{Z}/n\mathbb{Z})^4$, though its size over $\mathbb{F}_q$ depends on the Frobenius polynomial

$$P(T) = T^4 - s_1 T^3 + s_2 T^2 - q s_1 T + q^2.$$

  For $P \in J(C)[n]$, $[n]P = 0$, and $|J(C)(\mathbb{F}_q)| = P(1)$.
- Pick a subgroup $K \subset J(C)[n]$ of order n^2 isotropic under the Weil pairing

$$e_n : J(C)[n] \times J(C)[n] \to \mu_n,$$

  where $e_n(P, Q) = 1$ for all $P, Q \in K$. This involves:
  1. Generating a basis for $J(C)[n]$ over $\mathbb{F}_q$ (or an extension if needed), computing points $P_i = (u_i(x), v_i(x)) - \infty$ such that $nP_i = 0$ using Cantor's addition algorithm over $\mathbb{F}_{q^d}$ (where $n \mid q^d - 1$),

Computing (n, n)-Isogenies II

2. Selecting a subgroup K of order n^2 via linear algebra over $\mathbb{Z}/n\mathbb{Z}$, e.g., $K = \langle P_1, P_2 \rangle$ with P_1, P_2 linearly independent, forming $K = \{aP_1 + bP_2 \mid a, b = 0, \ldots, n-1\}$,
3. Verifying isotropy by computing the Weil pairing on K's generators, $e_n(P_i, P_j) = (-1)^{\langle P_i, P_j \rangle_n}$, where $\langle P_i, P_j \rangle_n$ is the intersection number modulo n. Adjust if $e_n(P_1, P_2) \neq 1$. Since $C \in \mathcal{L}_n(\mathbb{F}_q)$, $K \cong (\mathbb{Z}/n\mathbb{Z})^2$ exists.

- Compute the quotient $J(C)/K$
  The quotient $J(C)/K$ is expected to be isomorphic to $E_1 \times E_2$. For n odd, use Vélu-type formulas adapted for genus 2, generalizing Richelot isogenies for $n = 2$, by:
  - Representing divisors in $J(C)$ using Mumford coordinates, e.g.,

$$D = (u(x), v(x)) - 2\infty,$$

  - Applying K's action to form equivalence classes, $D \sim D + P$ for $P \in K$, via addition laws (e.g., for $P = (x_1, y_1) - \infty$, $D + P = (u'(x), v'(x)) - \infty$),
  - Constructing the codomain $J(C)/K$ as a product of elliptic curves via explicit equations or theta functions. For $n = 3$, if $K = \langle P_1, P_2 \rangle$, $J(C)/K$ yields $E_1 : y^2 = x^3 + a_1 x + b_1$, $E_2 : y^2 = x^3 + a_2 x + b_2$, derived from K's orbit.
- Verify the isogeny One can verify the isogeny

$$\phi : J(C) \to J(C)/K \cong E_1 \times E_2$$

  by computing the j-invariants of E_1 and E_2 or testing $\phi(nP) = 0$ for sample $P \in J(C)$, confirming $\ker(\phi) = K$.
  This method applies uniformly to $n = 2, 3, 5$, with $|\mathcal{L}_n(\mathbb{F}_q)|$ determining the availability of suitable curves, a key factor in cryptographic design. For $n = 2$, this is well known by Richelot isogenies; see (?2021-1, Prop. 2.1) for a detailed discussion.

Weighted Projective Spaces and Varieties I

Main Problem: Find rational points on weighted varieties over $\mathbb{F}_q$.

Let $\mathbb{F}$ be a field and $\mathbf{w} = (w_0, w_1, \ldots, w_n)$ a tuple of positive integers, called weights. The weighted projective space $\mathbb{P}_{\mathbf{w}}(\mathbb{F})$ is the quotient space $\mathbb{A}^{n+1}(\mathbb{F}) \setminus \{0\}/\sim$, where

$$(\alpha_0, \alpha_1, \ldots, \alpha_n) \sim (\beta_0, \beta_1, \ldots, \beta_n) \quad \text{if there is } \lambda \in \mathbb{F}^* \text{ s.t. } \alpha_i = \lambda^{w_i}\beta_i,\ i = 0, 1, \ldots, n.$$

We denote the equivalence class by $[\alpha_0 : \alpha_1 : \cdots : \alpha_n]_{\mathbf{w}}$.
Consider the graded polynomial ring $\mathbb{F}[x_0, \ldots, x_n]_{\mathbf{w}}$, where variable x_i has degree w_i. A polynomial $f(x_0, \ldots, x_n)$ is **weighted homogeneous** of degree d if every monomial $x_0^{a_0} \cdots x_n^{a_n}$ satisfies $\sum_{i=0}^{n} a_i w_i = d$ or equivalently:

$$f(\lambda^{w_0}x_0, \lambda^{w_1}x_1, \ldots, \lambda^{w_n}x_n) = \lambda^d f(x_0, x_1, \ldots, x_n) \quad \text{for all } \lambda \in \mathbb{F}^*.$$

A **weighted variety** is a subvariety of $\mathbb{P}_{\mathbf{w}}$ defined by weighted homogeneous polynomials. A **weighted hypersurface** $X \subset \mathbb{P}_{\mathbf{w}}$ is the zero set of a weighted homogeneous polynomial f:

$$X = \{[\alpha_0 : \alpha_1 : \cdots : \alpha_n]_{\mathbf{w}} \in \mathbb{P}_{\mathbf{w}} \mid f(\alpha_0, \alpha_1, \ldots, \alpha_n) = 0\}.$$

The $\mathbb{F}_q$-**rational points**, denoted $X(\mathbb{F}_q)$, are equivalence classes $[x_0 : \cdots : x_n]_{\mathbf{w}}$ with $x_i \in \mathbb{F}_q$, not all zero, satisfying X's defining equations.

Lang-Weil Estimate: For a geometrically irreducible variety $X \subset \mathbb{P}^n$ of dimension d from (Lang and Weil, 1954)

$$|X(\mathbb{F}_q)| \approx q^d + O(q^{d-1/2})$$

Weighted Projective Spaces and Varieties II

Weil Conjectures: For a smooth projective variety, the zeta function is rational, with roots tied to Betti numbers (Deligne, 1974).

$$Z(X,t) = \exp\left(\sum_{d=1}^{\infty} |X(\mathbb{F}_{q^d})| \frac{t^d}{d}\right)$$

Serre's Inequality: For a hypersurface in $\mathbb{P}^n$ with degree $d < n+1$, or adjusted for weights in $\mathbb{P}_{\mathbf{w}}$, (Li, 2019)

$$|X(\mathbb{F}_q)| \equiv 1 \pmod{p}, \quad \text{where} \quad p = \mathrm{char}(\mathbb{F}_q)$$

Point Count Bounds: For a hypersurface in $\mathbb{P}^n$, refined by degree and singularities (Aubry et al., 2017).

$$|X(\mathbb{F}_q)| \leq \frac{q^n - 1}{q - 1},$$

The $\mathbb{F}_q^*$-Action and Orbit Sizes

The weighted projective space $\mathbb{P}_{\mathbf{w}}(\mathbb{F}_q)$ is defined by the $\mathbb{F}_q^*$-action on $\mathbb{A}^{n+1}(\mathbb{F}_q) \setminus \{0\}$, where for $\lambda \in \mathbb{F}_q^*$ and point $\mathbf{x} = (\alpha_0, \ldots, \alpha_n)$:

$$\lambda \cdot \mathbf{x} = (\lambda^{w_0}\alpha_0, \lambda^{w_1}\alpha_1, \ldots, \lambda^{w_n}\alpha_n).$$

Points $[\alpha_0 : \cdots : \alpha_n]_{\mathbf{w}}$ are orbits under this action. For a point $\mathbf{x}$ with support set $S = \{i \mid \alpha_i \neq 0\} \subseteq \{0, \ldots, n\}$, the stabilizer is:

$$\mathrm{Stab}(\mathbf{x}) = \{\lambda \in \mathbb{F}_q^* \mid \lambda^{k_S} = 1\},$$

Weighted Projective Spaces and Varieties III

where $k_S = \gcd(\{w_i \mid i \in S\})$. Since $\mathbb{F}_q^*$ is cyclic of order $q-1$, $|\mathrm{Stab}(\mathbf{x})| = \gcd(k_S, q-1)$. By the orbit-stabilizer theorem, the orbit size is:

$$|\mathrm{Orb}(\mathbf{x})| = \frac{|\mathbb{F}_q^*|}{|\mathrm{Stab}(\mathbf{x})|} = \frac{q-1}{\gcd(k_S, q-1)}.$$

Challenges in Weighted Projective Spaces

Non-Uniform Orbits. The $\mathbb{F}_q^*$-action on points in $\mathbb{P}_{\mathbf{w}}(\mathbb{F}_q)$ yields orbit sizes $(q-1)/\gcd(k_S, q-1)$, where $k_S = \gcd(\{w_i \mid i \in S\})$ for support set $S \subseteq \{0, \ldots, n\}$. This non-uniformity, unlike in standard projective spaces, complicates the enumeration of rational points.

Singularity Analysis. Weighted hypersurfaces exhibit quotient singularities, such as at $[1 : 0 : \cdots : 0]$, requiring adjusted tangent spaces to analyze their local geometry (Reid, 1987). These singularities affect point counts and demand specialized techniques.

Bound Adaptation. The orbifold structure of $\mathbb{P}_{\mathbf{w}}$ limits the effectiveness of classical bounds like Lang-Weil. Aubry et al. propose

$$|X(\mathbb{F}_q)| \leq \min\left\{\frac{q^{m+1}-1}{q-1}, \frac{d}{w_0}q^{m-1} + \frac{q^{m-1}-1}{q-1}\right\}$$

for hypersurfaces of degree d and minimal weight w_0 (Aubry et al., 2017).

Computational Complexity. Enumerating rational points requires stratifying by support sets $S \subseteq \{0, \ldots, n\}$, with computational complexity increasing due to the diversity of weights w_i. This stratification poses significant computational challenges.

Counting Points on Weighted Projective Spaces

To compute $|\mathbb{P}_{\mathbf{w}}(\mathbb{F}_q)|$, stratify points by support sets $S \subseteq \{0, \ldots, n\}$, where $x_i \neq 0$ for $i \in S$, $x_i = 0$ otherwise.
Define

$$N_S = |\{(x_0, \ldots, x_n) \in (\mathbb{F}_q^*)^{|S|} \times \{0\}^{n+1-|S|} \mid x_i \neq 0 \text{ for } i \in S\}| = (q-1)^{|S|}.$$

The stabilizer under $\mathbb{F}_q^*$ consists of $\lambda \in \mathbb{F}_q^*$ with $\lambda^{w_i} = 1$ for $i \in S$, giving order $\gcd(k_S, q-1)$, where $k_S = \gcd(\{w_i \mid i \in S\})$.
By the orbit-stabilizer theorem, the orbit size is $\frac{q-1}{\gcd(k_S, q-1)}$. The number of orbits for support S is:

$$\frac{N_S}{\frac{q-1}{\gcd(k_S, q-1)}} = (q-1)^{|S|-1} \gcd(k_S, q-1).$$

Thus:

$$|\mathbb{P}_{\mathbf{w}}(\mathbb{F}_q)| = \sum_{S \neq \emptyset} (q-1)^{|S|-1} \gcd(k_S, q-1).$$

For $w_i = 1$, $k_S = 1$, so $|\mathbb{P}^n(\mathbb{F}_q)| = \frac{q^{n+1}-1}{q-1}$.
This stratification underpins hypersurface counts.

Conjectures on Rational Points

1. Serre's Inequality (Serre, 1991)**:** For a hypersurface $X \subset \mathbb{P}(w_0, \ldots, w_n)$ of degree $d < n+1$, adjusted for weights (e.g., $d < \sum w_i$), the number of rational points satisfies:

$$|X(\mathbb{F}_q)| \equiv 1 \pmod{p}, \quad p = \text{char}(\mathbb{F}_q).$$

This extends Chevalley-Warning to weighted spaces. The affine solutions $N(f) = |\{(x_0, \ldots, x_n) \in \mathbb{F}_q^{n+1} \mid f = 0\}|$ are divisible by p if $d < n+1$, projecting to $\mathbb{P}_{\mathbf{w}}$ with congruence adjusted for the origin (Li, 2019). For $d \geq n+1$, alternative constraints are needed.

2. Aubry et al.'s Conjecture (Aubry et al., 2017)**:** If a hyperplane $H \subset \mathbb{P}_{\mathbf{w}}$ exists with $X \cap H = \emptyset$, then:

$$|X(\mathbb{F}_q)| \leq \min\left\{p_m, \frac{d}{w_0} q^{m-1} + p_{m-2}\right\},$$

where $m = n$, $p_m = \frac{q^{m+1}-1}{q-1}$, $p_{m-2} = \frac{q^{m-1}-1}{q-1}$, and $w_0 = \min\{w_i\}$. This adapts classical bounds, with $\frac{d}{w_0} q^{m-1} + p_{m-2}$ scaling by degree and minimal weight. Proven for $\mathbb{P}(1, 1, w_2, \ldots, w_n)$, with equality conjectured for $d \leq w_0(q+1)$ (Aubry et al., 2017).

Implications: These guide our orbit-stabilizer algorithm, refining estimates like Lang-Weil's for weighted contexts.

Zeta Functions

The **zeta function** of a variety X over $\mathbb{F}_q$ encodes point counts over extensions, revealing arithmetic properties. For $X \subset \mathbb{P}^n$:

$$Z(X,t) = \exp\left(\sum_{d=1}^{\infty} |X(\mathbb{F}_{q^d})| \frac{t^d}{d}\right).$$

Properties for Projective Varieties (Deligne, 1974)**:**

1. **Rationality**: $Z(X,t) = \frac{P(t)}{Q(t)}$, with $P(t), Q(t) \in \mathbb{Z}[t]$. For a smooth variety of dimension m:

$$Z(X,t) = \frac{\prod_{i=1,\text{odd}}^{2m} P_i(t)}{\prod_{i=0,\text{even}}^{2m} P_i(t)},$$

   where $P_i(t) = \prod_j (1 - \alpha_{i,j} t)$, $\alpha_{i,j}$ tied to Betti numbers.

2. **Functional Equation**: For smooth X, $Z(X, 1/(q^m t)) = \pm q^{m\chi/2} t^{\chi} Z(X,t)$, where χ is the Euler characteristic.

3. **Riemann Hypothesis**: Roots $\alpha_{i,j}$ satisfy $|\alpha_{i,j}| = q^{i/2}$.

For a hypersurface of dimension $m = n - 1$, $|X(\mathbb{F}_q)| \approx q^{n-1} + O(q^{n-3/2})$ (Lang and Weil, 1954).

Zeta Functions for Weighted Projective Varieties

For $X \subset \mathbb{P}_{\mathbf{w}}$, the zeta function is:

$$Z(X,t) = \exp\left(\sum_{d=1}^{\infty} |X(\mathbb{F}_{q^d})| \frac{t^d}{d}\right).$$

Properties and Challenges:

1. **Rationality**: $Z(X,t) = \frac{P(t)}{Q(t)}$, with polynomials reflecting the orbifold structure. For a hypersurface of dimension $m-1$, the denominator often includes $(1-t)(1-qt)\cdots(1-q^{m-1}t)$, adjusted for weights (Aubry et al., 2017).
2. **Singularity Effects**: Quotient singularities (e.g., $[1:0:\cdots:0]$) alter pole structures, deviating from Betti number patterns (Reid, 1987).
3. **Weight-Dependent Counts**: The weighted $\mathbb{F}_q^*$-action complicates $|X(\mathbb{F}_{q^d})|$, requiring stratification by support sets.
4. **Functional Equation**: Holds under smoothness, but χ accounts for weighted singularities.

Implications: Links counts to cohomology, guiding bounds and computations.

Algorithm for Counting Rational Points

For a hypersurface $X = V(f) \subset \mathbb{P}_{\mathbf{w}}$ over $\mathbb{F}_q$, with $f \in \mathbb{F}_q[x_0, \ldots, x_n]$ of degree d, compute $|X(\mathbb{F}_q)|$. The **orbit-stabilizer algorithm** uses the $\mathbb{F}_q^*$-action.

Algorithm Steps:

1. **Compute N_S for each $S \subseteq \{0, \ldots, n\}, S \neq \emptyset$:**

$$N_S = \left| \left\{ (x_0, \ldots, x_n) \in \mathbb{F}_q^{n+1} \mid f = 0, x_i \neq 0 \text{ for } i \in S, x_i = 0 \text{ for } i \notin S \right\} \right|.$$

   Evaluate f on $(\mathbb{F}_q^*)^{|S|} \times \{0\}^{n+1-|S|}$, leveraging $f(\lambda^{w_0} x_0, \ldots, \lambda^{w_n} x_n) = \lambda^d f$.

2. **Compute k_S:** The stabilizer consists of $\lambda \in \mathbb{F}_q^*$ with $\lambda^{w_i} = 1$ for $i \in S$, order $\gcd(k_S, q-1)$, where $k_S = \gcd(\{w_i \mid i \in S\})$.

3. **Sum contributions:** Orbit size is $\frac{q-1}{\gcd(k_S, q-1)}$, so:

$$|X(\mathbb{F}_q)| = \sum_{S \neq \emptyset} \frac{N_S \cdot \gcd(k_S, q-1)}{q-1}.$$

Application to $\mathcal{L}_n$: I

We present point counts $|\mathcal{L}_n(\mathbb{F}_q)|$ for $n = 2, 3$, zeta functions as in (Mello et al., 2025).

- Apply the algorithm to compute $|\mathcal{L}_n(\mathbb{F}_q)|$.
- Derive $Z(\mathcal{L}_n, t)$ to analyze point growth.

using the above

$$|\mathcal{L}_n(\mathbb{F}_q)| = \sum_{S \neq \emptyset} \frac{N_S \cdot \gcd(k_S, q-1)}{q-1},$$

where $N_S = |\{(x_0, \ldots, x_3) \in \mathbb{F}_q^4 \mid F_n = 0, x_i \neq 0 \text{ for } i \in S, x_i = 0 \text{ else}\}|$, $k_S = \gcd(\{w_i \mid i \in S\})$, $\mathbf{w} = (2, 4, 6, 10)$,

Results for for $n = 2, p = 5$:

- $\mathbb{F}_5$: 64 points ($S = \{0\}, \{1\}, \{0, 1, 2, 3\}$; 20% singular).
- $\mathbb{F}_{25}$: 1304 points ($S = \{0\}, \{0, 1, 2\}, \{0, 1, 2, 3\}$; 40% singular).
- $\mathbb{F}_{125}$: 31504 points ($S = \{0\}, \{0, 1, 2\}, \{0, 1, 2, 3\}$; 40% singular).

Results for $n = 2, p = 3$: Degeneration to a curve:

- $\mathbb{F}_3$: 62 points (70% singular).
- $\mathbb{F}_9$: 508 points (68% singular).
- $\mathbb{F}_{27}$: 4430 points.
- $\mathbb{F}_{81}$: 39540 points (68% singular).

Application to $\mathcal{L}_n$: II

Results for $n = 3, p = 5$:

- $\mathbb{F}_5$: 74 points ($S = \{0\}, \{0, 1, 2\}, \{0, 1, 2, 3\}$; 66% singular).
- $\mathbb{F}_{25}$: 1294 points ($S = \{0\}, \{0, 1, 2\}, \{0, 1, 2, 3\}$; 68% singular).

Results for $n = 3, p = 3$: Identical to $\mathcal{L}_2$, e.g., 62 ($\mathbb{F}_3$), 508 ($\mathbb{F}_9$).

Note: Degeneration in $p = 3$ shows algorithm's adaptability to reduced dimensions.

Zeta Functions: For $\mathcal{L}_2, p = 5$: $Z(\mathcal{L}_2, t) \approx \frac{1+38t}{(1-t)(1-25t)}$, matching 64, 652 (Mello et al., 2025). For $p = 3$:

$$Z(\mathcal{L}_2, t; p = 3) = \frac{1 + 49t - 747t^2}{(1 - t)(1 - 3t)(1 - 9t)},$$

same for $\mathcal{L}_3$. For $\mathcal{L}_3, p = 5$: $Z(\mathcal{L}_3, t) \approx \frac{1+48t}{(1-t)(1-25t)}$, matching 74, 647.

Bounds: (Aubry et al., 2017)

- $\mathcal{L}_2$: $|\mathcal{L}_2(\mathbb{F}_q)| \leq 15q^2 + q + 1$, e.g., 381 ¿ 64 ($\mathbb{F}_5$).
- $\mathcal{L}_3$: $|\mathcal{L}_3(\mathbb{F}_q)| \leq 40q^2 + q + 1$, e.g., 1006 ¿ 74 ($\mathbb{F}_5$).

FUTURE WORK

- Develop a theory of rational points of weighted projective varieties over $\mathbb{F}_q$.
- Given a weighted projective curve $\mathcal{X}_{\mathbf{w}}$ and $\mathcal{X}$ its image under the Veronese map

$$\mathcal{X}_{\mathbf{w}} \to \mathcal{X}$$

  Determine the relation between the number of rational points of $\mathcal{X}_{\mathbf{w}}$ and the number of rational points of $\mathcal{X}$.

Here are some of our latest papers/preprints that lead to this problem or trying to address this problem :

- S. Salami, T. Shaska, Vojta's conjecture on weighted projective varieties, European Journal of Mathematics, 11, 12 (2025).
- E. Shaska, T. Shaska, Machine learning for moduli space of genus two curves and an application to isogeny based cryptography, Journal of Algebr Comb 61, 23 (2025).
- A. Clingher, A. Malmendier, T. Shaska, Isogenies, Kummer surfaces, and theta functions, NATO Sci. Peace Secur. Ser. D Inf. Commun. Secur.
- J. Mello, S. Salami, E. Shaska, T. Shaska, Rational Points and Zeta Functions of Humbert Surfaces with Square Determinant over F_q, NATO Sci. Peace Secur. Ser. D Inf. Commun. Secur.
- J. Mello, T. Shaska, Counting of Rational Points on Weighted Projective Spaces

Hopefully more exciting results to be announced soon

References, I

Anni, Samuele, Gaetan Bisson, Annamaria Iezzi, Elisa Lorenzo Garcia, and Benjamin Wesolowski. 2025. *On the computation of endomorphism rings of abelian surfaces over finite fields*, Preprint. Submitted work, referenced as primary source for this section.

Aubry, Yves, Wouter Castryck, Sudhir R. Ghorpade, Gilles Lachaud, Michael E. O'Sullivan, and Samrith Ram. 2017. *Hypersurfaces in weighted projective spaces over finite fields with applications to coding theory*, Algebraic geometry for coding theory and cryptography, pp. 25–61.

Bisson, Gaetan. 2015. *Computing endomorphism rings of abelian varieties of dimension two*, Mathematics of Computation **84**, no. 294, 1977–1989. MR3356035

Deligne, P. 1974. *La conjecture de weil. I*, Publications Mathématiques de l'IHÉS **43**, 273–307.

Lang, S. and A. Weil. 1954. *Number of points of varieties in finite fields*, American Journal of Mathematics **76**, no. 4, 819–827.

Li, Rupert. 2019. $\mathbb{F}_q$*-rational points of hypersurfaces in weighted projective spaces over finite fields*, Graduate Dissertation, MIT.

Malmendier, Andreas and Tony Shaska. 2017. *A universal genus-two curve from siegel modular forms*, SIGMA Symmetry Integrability Geom. Methods Appl. **13**, Paper No. 089, 17.

Mello, J., S. Salami, E. Shaska, and T. Shaska. 2025. *Rational points and zeta functions of humbert surfaces with square discriminant*, Preprint.

Page, Aurel and Benjamin Wesolowski. 2024. *The supersingular endomorphism ring and one endomorphism problems are equivalent*, Advances in Cryptology – EUROCRYPT 2024, 388–417.

Reid, Miles. 1987. *Young person's guide to canonical singularities*, Algebraic geometry, bowdoin 1985, pp. 345–414.

Robert, Damien. 2022. *Some applications of higher dimensional isogenies to elliptic curves*. Report 2022/1704.

Serre, Jean-Pierre. 1991. *Lettre à M. Tsfasman*, Astérisque **198-200**, 351–353. Journées Arithmétiques, 1989 (Luminy, 1989).

Shaska, Elira and Tanush Shaska. 2025. *Machine learning for moduli space of genus two curves and an application to isogeny-based cryptography*, J. Algebraic Combin. **61**, no. 2, 23. MR4870337

Shaska, Tanush. 2001. *Curves of genus two covering elliptic curves*, Ph.D. Thesis. Thesis (Ph.D.)–University of Florida. MR2701993

Shaska, Tony. 2004. *Genus 2 fields with degree 3 elliptic subfields*, Forum Mathematicum **16**, no. 2, 263–280. MR2039100

_____. 2025. *Quantum Gröbner: Taming Weighted Varieties*. preprint.