THORSTEN KLEINJUNG*

BENJAMIN WESOLOWSKI*

A NEW PERSPECTIVE ON THE POWERS OF TWO DESCENT
for discrete logarithms in finite fields

PRESENTED AT ANTS-XIII, MADISON, WI, USA, ON THE 20/07/2018 BY BENJAMIN WESOLOWSKI

*EPFL, LAUSANNE, SWITZERLAND

1

A ZIGZAG DESCENT

HEURISTIC AND RIGOROUS ALGORITHMS FOR DLP

Discrete logarithm problem (DLP) in finite fields of fixed characteristic ($\mathbb{F}_{p^n}$ with p fixed and $n \to \infty$... think $\mathbb{F}_{2^n}$):

- Given a generator g of $\mathbb{F}_{p^n}^{\times}$ and an arbitrary element h, find an integer m such that $h = g^m$

HEURISTIC AND RIGOROUS ALGORITHMS FOR DLP

Discrete logarithm problem (DLP) in finite fields of fixed characteristic ($\mathbb{F}_{p^n}$ with p fixed and $n \to \infty$... think $\mathbb{F}_{2^n}$):

- Given a generator g of $\mathbb{F}_{p^n}^\times$ and an arbitrary element h, find an integer m such that $h = g^m$

This DLP is in an uncomfortable position: huge gap between

HEURISTIC AND RIGOROUS ALGORITHMS FOR DLP

Discrete logarithm problem (DLP) in finite fields of fixed characteristic ($\mathbb{F}_{p^n}$ with p fixed and $n \to \infty$… think $\mathbb{F}_{2^n}$):

- Given a generator g of $\mathbb{F}_{p^n}^{\times}$ and an arbitrary element h, find an integer m such that $h = g^m$

This DLP is in an uncomfortable position: huge gap between

- The best known **rigorous** algorithm: Pomerance's variant of Hellman-Reyneri's of complexity $L(1/2)$ [Pom87, HR82]

HEURISTIC AND RIGOROUS ALGORITHMS FOR DLP

Discrete logarithm problem (DLP) in finite fields of fixed characteristic ($\mathbb{F}_{p^n}$ with p fixed and $n \to \infty$… think $\mathbb{F}_{2^n}$):

- Given a generator g of $\mathbb{F}_{p^n}^\times$ and an arbitrary element h, find an integer m such that $h = g^m$

This DLP is in an uncomfortable position: huge gap between

- The best known **rigorous** algorithm: Pomerance's variant of Hellman-Reyneri's of complexity $L(1/2)$ [Pom87, HR82]
- The best known **heuristic** algorithms: in quasi-polynomial time [BGJT14, GKZ18]

HEURISTIC AND RIGOROUS ALGORITHMS FOR DLP

Discrete logarithm problem (DLP) in finite fields of fixed characteristic ($\mathbb{F}_{p^n}$ with p fixed and $n \to \infty$... think $\mathbb{F}_{2^n}$):

- Given a generator g of $\mathbb{F}_{p^n}^{\times}$ and an arbitrary element h, find an integer m such that $h = g^m$

This DLP is in an uncomfortable position: huge gap between

- The best known **rigorous** algorithm: Pomerance's variant of Hellman-Reyneri's of complexity $L(1/2)$ [Pom87, HR82]
- The best known **heuristic** algorithms: in quasi-polynomial time [BGJT14, GKZ18]

they need to be understood better

QUASI-POLYNOMIAL ALGORITHMS FOR DLP

- First heuristic quasi-poly. algorithm discovered by Barbulescu, Gaudry, Joux, Thomé [BGJT14]

[BGJT14] R. Barbulescu, P. Gaudry, A. Joux, and E. Thomé. *A heuristic quasi-polynomial algorithm for discrete logarithm in finite fields of small characteristic*, EUROCRYPT 2014.

- Soon after, Granger, Kleinjung, Zumbrägel [GKZ18] proposed another one, with a promise: **getting closer to a rigorous algorithm**

[GKZ18] R. Granger, T. Kleinjung, and J. Zumbrägel. *On the discrete logarithm problem in finite fields of fixed characteristic*, Transactions of the American Mathematical Society, 2018.

QUASI-POLYNOMIAL ALGORITHMS FOR DLP

Main theorem of [GKZ18]: the DLP in fixed characteristic can be solved in expected quasi-poly. time in fields that admit a suitable representation.

QUASI-POLYNOMIAL ALGORITHMS FOR DLP

Main theorem of [GKZ18]: the DLP in fixed characteristic can be solved in expected quasi-poly. time in fields that admit a suitable representation.

- Suitable representation? Field $\mathbb{F}_{q^d}[x]/(J)$ where J is an irreducible polynomial in $\mathbb{F}_{q^d}[x]$ such that

$$x^q \equiv h_0/h_1 \bmod J$$

with h_0 and h_1 polynomials in $\mathbb{F}_{q^d}[x]$ of degree at most 2

- Expected time $q^{\log_2(\deg(J)) + O(d)}$

A DESCENT IS SUFFICIENT

First idea of the proof: **a descent algorithm is sufficient**

A DESCENT IS SUFFICIENT

First idea of the proof: **a descent algorithm is sufficient**

- Fix the factor base $\mathfrak{F} = \{$ linear polynomials in $\mathbb{F}_{q^d}[x]$ $\}$

A DESCENT IS SUFFICIENT

First idea of the proof: **a descent algorithm is sufficient**

- Fix the factor base $\mathfrak{F}$ = { linear polynomials in $\mathbb{F}_{q^d}[x]$ }
- **Descent:** Given any polynomial Q in $\mathbb{F}_{q^d}[x]$ find integers e_f, for f in $\mathfrak{F}$, such that

$$Q \equiv \prod_{f \in \mathfrak{F}} f^{e_f} \mod J.$$

A DESCENT IS SUFFICIENT

First idea of the proof: **a descent algorithm is sufficient**

- Fix the factor base $\mathfrak{F}$ = { linear polynomials in $\mathbb{F}_{q^d}[x]$ }
- **Descent:** Given any polynomial Q in $\mathbb{F}_{q^d}[x]$ find integers e_f, for f in $\mathfrak{F}$, such that

$$Q \equiv \prod_{f \in \mathfrak{F}} f^{e_f} \mod J.$$

- To solve the DLP, it is sufficient to have an efficient descent

DEGREE TWO ELIMINATION

Main ingredient of the descent, the **degree two elimination**:

DEGREE TWO ELIMINATION

Main ingredient of the descent, the **degree two elimination**:

- Given an extension k of $\mathbb{F}_{q^d}$ and an irreducible **quadratic** polynomial Q in $k[x]$,

DEGREE TWO ELIMINATION

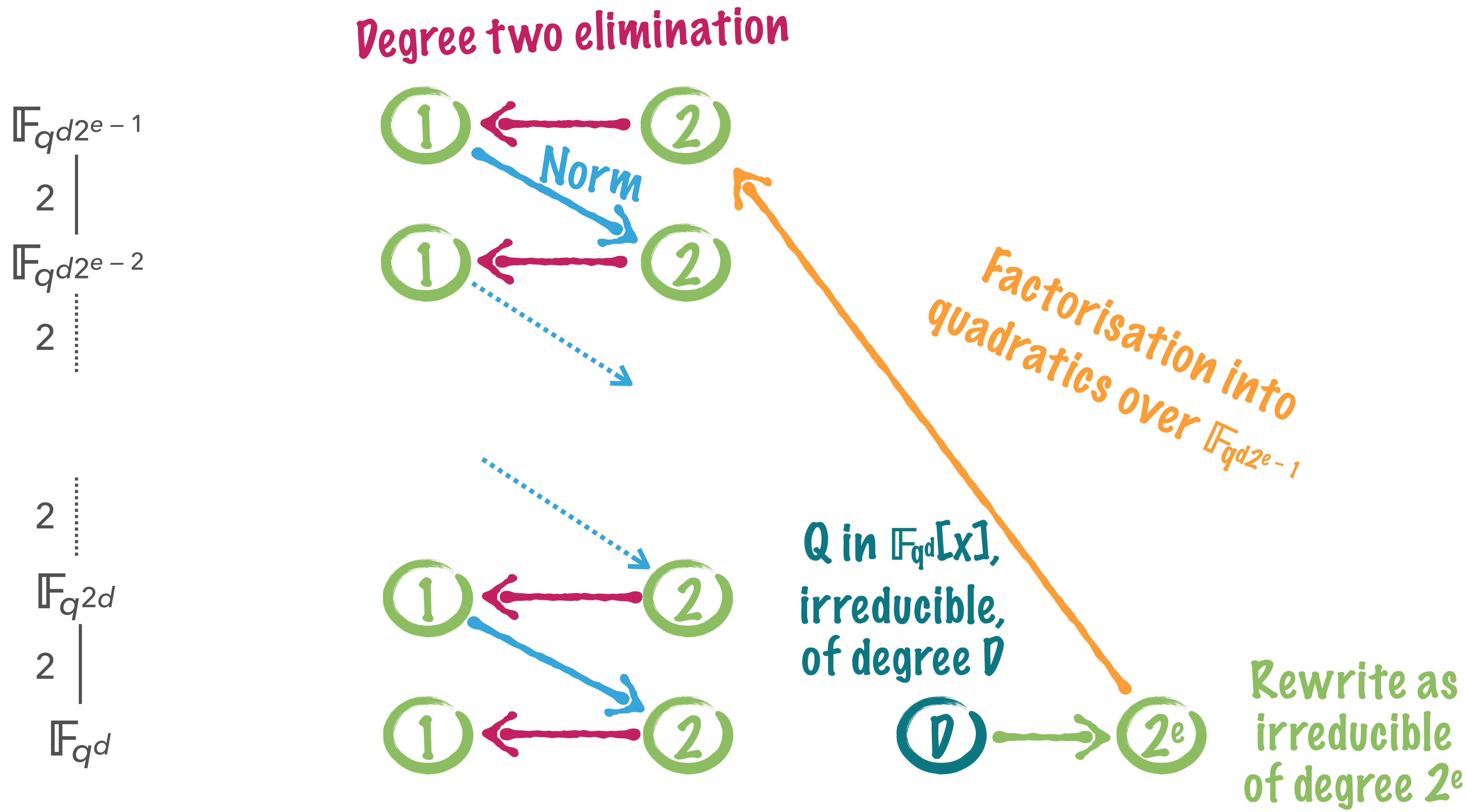
Main ingredient of the descent, the **degree two elimination**:

- Given an extension k of $\mathbb{F}_{q^d}$ and an irreducible **quadratic** polynomial Q in $k[x]$,
- Find **linear** polynomials $L_1, L_2, \ldots, L_m$ in $k[x]$ such that

$$Q \equiv \prod_{i=1}^{m} L_i \mod J.$$

ZIGZAG DESCENT

The **zigzag descent**: transform the degree two elimination into a **full descent algorithm**



SUMMARY

Degree two elimination

SUMMARY

Degree two elimination

↓

Descent algorithm

SUMMARY

Degree two elimination

↓

Descent algorithm

↓

An algorithm for computing logarithms

SUMMARY

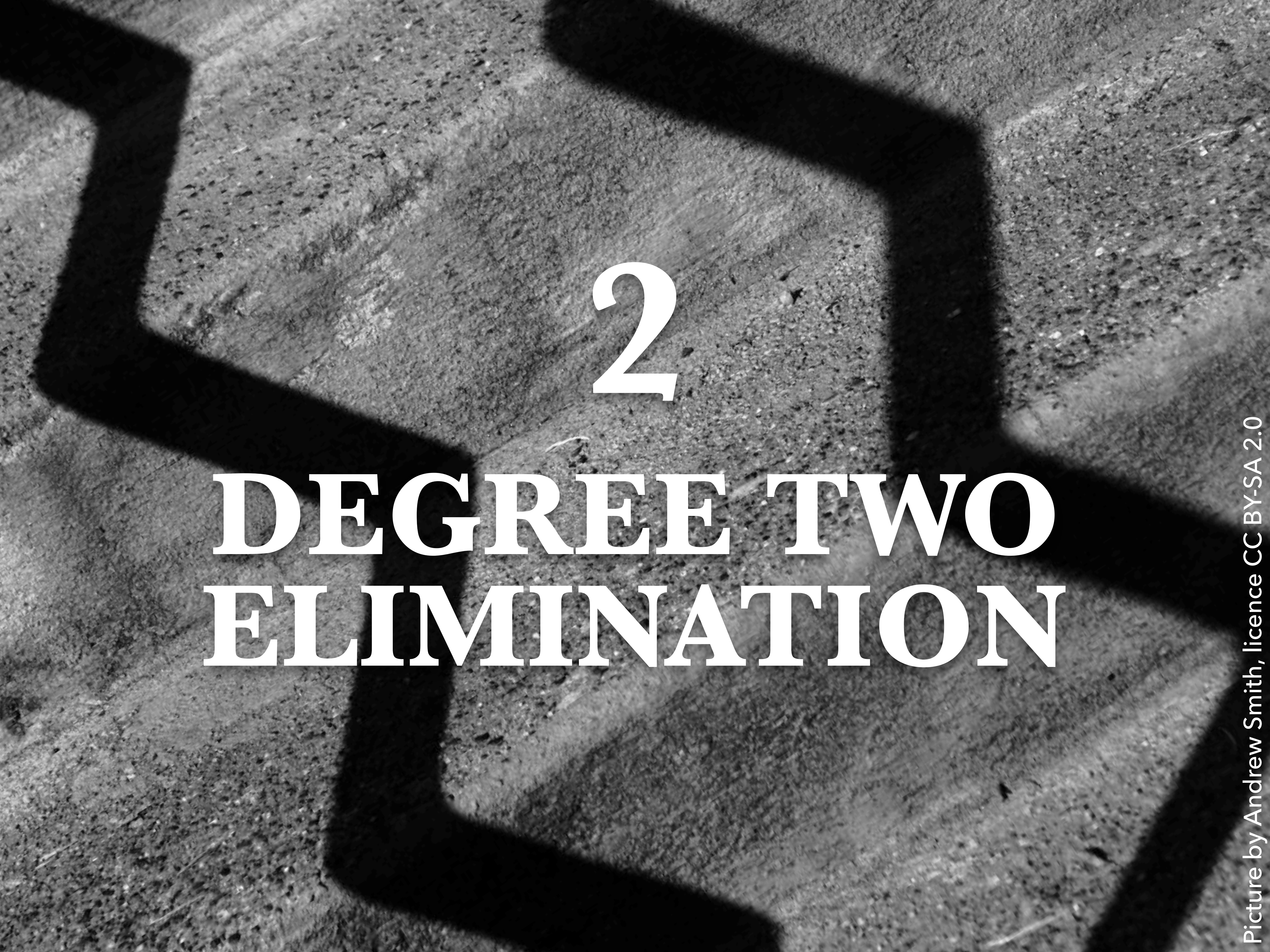
Degree two elimination ?

↓

Descent algorithm

↓

An algorithm for
computing logarithms


2
DEGREE TWO
ELIMINATION
Picture by Andrew Smith, licence CC BY-SA 2.0

POLYNOMIALS WITH HIGHER SPLITTING PROBABILITY

Fix an extension k of $\mathbb{F}_{q^d}$, and let Q an irred. quadratic in $k[x]$

POLYNOMIALS WITH HIGHER SPLITTING PROBABILITY

Fix an extension k of $\mathbb{F}_{q^d}$, and let Q an irred. quadratic in $k[x]$

- Key idea (from [GGMZ13]): polynomials of the form

$$\alpha x^{q+1} + \beta x^q + \gamma x + \delta \qquad \text{in } k[x]$$

  have a high probability to split over k (around q^{-3})

[GGMZ13] F. Göloğlu, R. Granger, G. McGuire, and J. Zumbrägel. *On the function field sieve and the impact of higher splitting probabilities*. CRYPTO 2013.

POLYNOMIALS WITH HIGHER SPLITTING PROBABILITY

Fix an extension k of $\mathbb{F}_{q^d}$, and let Q an irred. quadratic in $k[x]$

- Key idea (from [GGMZ13]): polynomials of the form

$$\alpha x^{q+1} + \beta x^q + \gamma x + \delta \qquad \text{in } k[x]$$

  have a high probability to split over k (around q^{-3})

- Let V be the vector space of dimension 4 of these polynomials, i.e., $V = \mathrm{span}(x^{q+1}, x^q, x, 1) \subset k[x]$

[GGMZ13] F. Göloğlu, R. Granger, G. McGuire, and J. Zumbrägel. *On the function field sieve and the impact of higher splitting probabilities*. CRYPTO 2013.

SMOOTH RELATIONS

- $V = \text{span}(x^{q+1}, x^q, x, 1) \subset k[x]$

SMOOTH RELATIONS

- $V = \text{span}(x^{q+1}, x^q, x, 1) \subset k[x]$
- We have $x^q \equiv h_0/h_1 \bmod J$, so

$$ax^{q+1} + \beta x^q + \gamma x + \delta \equiv \frac{axh_0 + \beta h_0 + \gamma x h_1 + \delta h_1}{h_1} \bmod J$$

SMOOTH RELATIONS

- $V = \text{span}(x^{q+1}, x^q, x, 1) \subset k[x]$
- We have $x^q \equiv h_0/h_1 \bmod J$, so

$$\alpha x^{q+1} + \beta x^q + \gamma x + \delta \equiv \frac{\alpha x h_0 + \beta h_0 + \gamma x h_1 + \delta h_1}{h_1} \bmod J$$

Splits with high probability

SMOOTH RELATIONS

- $V = \mathrm{span}(x^{q+1}, x^q, x, 1) \subset k[x]$
- We have $x^q \equiv h_0/h_1 \bmod J$, so

$$\alpha x^{q+1} + \beta x^q + \gamma x + \delta \equiv \frac{\alpha x h_0 + \beta h_0 + \gamma x h_1 + \delta h_1}{h_1} \bmod J$$

Splits with high probability

numerator of degree 3

SMOOTH RELATIONS

- $V = \mathrm{span}(x^{q+1}, x^q, x, 1) \subset k[x]$

- We have $x^q \equiv h_0/h_1 \bmod J$, so

$$\alpha x^{q+1} + \beta x^q + \gamma x + \delta \equiv \frac{\alpha x h_0 + \beta h_0 + \gamma x h_1 + \delta h_1}{h_1} \bmod J$$

Splits with high probability

numerator of degree 3

- Consider the vector subspace V_Q of dimension 2 in V, where Q divides the right-hand side:

$$V_Q = \{\alpha x^{q+1} + \beta x^q + \gamma x + \delta \mid \alpha x h_0 + \beta h_0 + \gamma x h_1 + \delta h_1 \equiv 0 \bmod Q\}$$

THE DEGREE TWO ELIMINATION

- For any $f = ax^{q+1} + \beta x^q + \gamma x + \delta$ in V_Q,

$$h_1 f \equiv axh_0 + \beta h_0 + \gamma x h_1 + \delta h_1 \bmod J$$

THE DEGREE TWO ELIMINATION

- For any $f = \alpha x^{q+1} + \beta x^q + \gamma x + \delta$ in V_Q,

$$h_1 f \equiv \alpha x h_0 + \beta h_0 + \gamma x h_1 + \delta h_1 \bmod J$$

- The quotient $L_0 = (\alpha x h_0 + \beta h_0 + \gamma x h_1 + \delta h_1)/Q$ is linear

$$h_1 f \equiv L_0 Q \bmod J$$

THE DEGREE TWO ELIMINATION

- For any $f = \alpha x^{q+1} + \beta x^q + \gamma x + \delta$ in V_Q,

$$h_1 f \equiv \alpha x h_0 + \beta h_0 + \gamma x h_1 + \delta h_1 \bmod J$$

- The quotient $L_0 = (\alpha x h_0 + \beta h_0 + \gamma x h_1 + \delta h_1)/Q$ is linear

$$h_1 f \equiv L_0 Q \bmod J$$

- If f splits into linears $L_1, \ldots, L_{q+1}$ in $k[x]$, then

$$Q \equiv h_1 L_0^{-1} L_1 \ldots L_{q+1} \bmod J$$

THE DEGREE TWO ELIMINATION

- For any $f = \alpha x^{q+1} + \beta x^q + \gamma x + \delta$ in V_Q,

$$h_1 f \equiv \alpha x h_0 + \beta h_0 + \gamma x h_1 + \delta h_1 \bmod J$$

- The quotient $L_0 = (\alpha x h_0 + \beta h_0 + \gamma x h_1 + \delta h_1)/Q$ is linear

$$h_1 f \equiv L_0 Q \bmod J$$

- If f splits into linears $L_1,\ldots,L_{q+1}$ in $k[x]$, then

$$Q \equiv h_1 L_0^{-1} L_1 \ldots L_{q+1} \bmod J$$

- **Algorithm**: choose random polynomials f in V_Q until it splits over k. Equivalently, sample f from the projective line $\mathbb{P}(V_Q)$.

STRATEGY

How many polynomials on the curve $\mathbb{P}(V_Q)$ split over k? Here is the new approach:

STRATEGY

How many polynomials on the curve $\mathbb{P}(V_Q)$ split over k? Here is the new approach:

- Construct a curve C defined over k, and a surjective morphism $\theta : C \longrightarrow \mathbb{P}(V_Q)$ such that

STRATEGY

How many polynomials on the curve $\mathbb{P}(V_Q)$ split over k? Here is the new approach:

- Construct a curve C defined over k, and a surjective morphism $\theta : C \longrightarrow \mathbb{P}(V_Q)$ such that

➡ C is absolutely irreducible

STRATEGY

How many polynomials on the curve $\mathbb{P}(V_Q)$ split over k? Here is the new approach:

- Construct a curve C defined over k, and a surjective morphism $\theta : C \to \mathbb{P}(V_Q)$ such that

➡ C is absolutely irreducible

➡ For any rational point P in $C(k)$, the polynomial $\theta(P)$ splits over k

STRATEGY

How many polynomials on the curve $\mathbb{P}(V_Q)$ split over k? Here is the new approach:

- Construct a curve C defined over k, and a surjective morphism $\theta : C \to \mathbb{P}(V_Q)$ such that

➡ C is absolutely irreducible

➡ For any rational point P in $C(k)$, the polynomial $\theta(P)$ splits over k

- Then, by the absolute irreducibility, $C(k)$ has a lot of points, therefore a lot of polynomials in $\mathbb{P}(V_Q)$ split over k

3

THE ACTION OF PGL_2 ON $X^q - X$

THE ACTION OF PGL_2

Given $f \in k[x]$ and a matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ in GL_2, we define

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} * f(x) = (cx + d)^{\deg f} f\left(\frac{ax + b}{cx + d}\right)$$

THE ACTION OF PGL_2 ON $X^q - X$

$V = span(x^{q+1}, x^q, x, 1)$

- For any m in PGL_2, $m * (x^q - x)$ is in $\mathbb{P}(V)$

THE ACTION OF PGL_2 ON $X^q - X$

$V = \mathrm{span}(x^{q+1}, x^q, x, 1)$

- For any m in PGL_2, $m * (x^q - x)$ is in $\mathbb{P}(V)$
- The $(q + 1)$ distinct roots of $m * (x^q - x)$ are $m^{-1}\mathbb{P}^1(\mathbb{F}_q)$

THE ACTION OF PGL_2 ON $X^q - X$

$V = \text{span}(x^{q+1}, x^q, x, 1)$

- For any m in PGL_2, $m * (x^q - x)$ is in $\mathbb{P}(V)$
- The $(q + 1)$ distinct roots of $m * (x^q - x)$ are $m^{-1}\mathbb{P}^1(\mathbb{F}_q)$
- Is there anything in $\mathbb{P}(V)$ that is not of this form $m * (x^q - x)$?

THE ACTION OF PGL_2 ON $X^q - X$

$V = \mathrm{span}(x^{q+1}, x^q, x, 1)$

- For any m in PGL_2, $m * (x^q - x)$ is in $\mathbb{P}(V)$
- The $(q + 1)$ distinct roots of $m * (x^q - x)$ are $m^{-1}\mathbb{P}^1(\mathbb{F}_q)$
- Is there anything in $\mathbb{P}(V)$ that is not of this form $m * (x^q - x)$?

➡ Yes, for instance $(x - a)^q(x - b)$… These polynomials form a quadratic surface S in $\mathbb{P}(V)$

THE ACTION OF PGL_2 ON $X^q - X$

$V = \text{span}(x^{q+1}, x^q, x, 1)$

- For any m in PGL_2, $m * (x^q - x)$ is in $\mathbb{P}(V)$
- The $(q + 1)$ distinct roots of $m * (x^q - x)$ are $m^{-1}\mathbb{P}^1(\mathbb{F}_q)$
- Is there anything in $\mathbb{P}(V)$ that is not of this form $m * (x^q - x)$?

➡ Yes, for instance $(x - a)^q(x - b)$… These polynomials form a quadratic surface S in $\mathbb{P}(V)$

Lemma: $\mathbb{P}(V) \setminus S = PGL_2 * (x^q - x)$.

4
IRREDUCIBLE COVERS

IRREDUCIBLE COVER

Recall that we want to construct a curve C defined over k, and a surjective morphism $\theta : C \to \mathbb{P}(V_Q)$ such that

- C is absolutely irreducible
- For any rational point P in $C(k)$, the polynomial $\theta(P)$ splits over k

IRREDUCIBLE COVER

$$C = \{(u, r_1, r_2, r_3) \mid r_1, r_2, r_3 \text{ are three dist. roots of } u\}$$

$$\subset \mathbb{P}(V_Q) \times \mathbb{P}^1 \times \mathbb{P}^1 \times \mathbb{P}^1$$

IRREDUCIBLE COVER

$$C = \{(u, r_1, r_2, r_3) \mid r_1, r_2, r_3 \text{ are three dist. roots of } u\}$$
$$\subset \mathbb{P}(V_Q) \times \mathbb{P}^1 \times \mathbb{P}^1 \times \mathbb{P}^1$$

Proposition: If $(u, r_1, r_2, r_3) \in C(k)$ then u splits over k.

IRREDUCIBLE COVER

$$C = \{(u, r_1, r_2, r_3) \mid r_1, r_2, r_3 \text{ are three dist. roots of } u\}$$
$$\subset \mathbb{P}(V_Q) \times \mathbb{P}^1 \times \mathbb{P}^1 \times \mathbb{P}^1$$

Proposition: If $(u, r_1, r_2, r_3) \in C(k)$ then u splits over k.

Proof: Recall the lemma $\mathbb{P}(V) \setminus S = \mathrm{PGL}_2 * (x^q - x)$.

IRREDUCIBLE COVER

$$C = \{(u, r_1, r_2, r_3) \mid r_1, r_2, r_3 \text{ are three dist. roots of } u\}$$
$$\subset \mathbb{P}(V_Q) \times \mathbb{P}^1 \times \mathbb{P}^1 \times \mathbb{P}^1$$

Proposition: If $(u, r_1, r_2, r_3) \in C(k)$ then u splits over k.

Proof: Recall the lemma $\mathbb{P}(V) \setminus S = \mathrm{PGL}_2 * (x^q - x)$.

- u has three distinct roots r_1, r_2, r_3, so it is not in S

IRREDUCIBLE COVER

$$C = \{(u, r_1, r_2, r_3) \mid r_1, r_2, r_3 \text{ are three dist. roots of } u\}$$
$$\subset \mathbb{P}(V_Q) \times \mathbb{P}^1 \times \mathbb{P}^1 \times \mathbb{P}^1$$

Proposition: If $(u, r_1, r_2, r_3) \in C(k)$ then u splits over k.

Proof: Recall the lemma $\mathbb{P}(V) \setminus S = \mathrm{PGL}_2 * (x^q - x)$.

- u has three distinct roots r_1, r_2, r_3, so it is not in S
- $u = m * (x^q - x)$ where $m \in \mathrm{PGL}_2$ is the automorphism of $\mathbb{P}^1$ sending the three points r_1, r_2, r_3 to the points $0, 1, \infty$

IRREDUCIBLE COVER

$$C = \{(u, r_1, r_2, r_3) \mid r_1, r_2, r_3 \text{ are three dist. roots of } u\}$$
$$\subset \mathbb{P}(V_Q) \times \mathbb{P}^1 \times \mathbb{P}^1 \times \mathbb{P}^1$$

Proposition: If $(u, r_1, r_2, r_3) \in C(k)$ then u splits over k.

Proof: Recall the lemma $\mathbb{P}(V) \setminus S = \mathrm{PGL}_2 * (x^q - x)$.

- u has three distinct roots r_1, r_2, r_3, so it is not in S
- $u = m * (x^q - x)$ where $m \in \mathrm{PGL}_2$ is the automorphism of $\mathbb{P}^1$ sending the three points r_1, r_2, r_3 to the points $0, 1, \infty$
- m is defined over k, so all the roots $m^{-1}\mathbb{P}^1(\mathbb{F}_q)$ are over k

IRREDUCIBLE COVERS

$$C = \{(u, r_1, r_2, r_3) \mid r_1, r_2, r_3 \text{ are three dist. roots of } u\}$$

$$\subset \mathbb{P}(V_Q) \times \mathbb{P}^1 \times \mathbb{P}^1 \times \mathbb{P}^1$$

- Is C absolutely irreducible? Consider a chain of covers

IRREDUCIBLE COVERS

$$C = \{(u, r_1, r_2, r_3) \mid r_1, r_2, r_3 \text{ are three dist. roots of } u\}$$
$$\subset \mathbb{P}(V_Q) \times \mathbb{P}^1 \times \mathbb{P}^1 \times \mathbb{P}^1$$

- Is C absolutely irreducible? Consider a chain of covers

$$\begin{array}{lll} X_3 = C = \{(u, r_1, r_2, r_3)\} & \subset \mathbb{P}(V_Q) \times \mathbb{P}^1 \times \mathbb{P}^1 \times \mathbb{P}^1 \\ \theta_3 \downarrow & \\ X_2 = \{(u, r_1, r_2)\} & \subset \mathbb{P}(V_Q) \times \mathbb{P}^1 \times \mathbb{P}^1 \\ \theta_2 \downarrow & \\ X_1 = \{(u, r_1)\} & \subset \mathbb{P}(V_Q) \times \mathbb{P}^1 \\ \theta_1 \downarrow & \\ X_0 = \{(u)\} & = \mathbb{P}(V_Q) \end{array}$$

IRREDUCIBLE COVERS

$$C = \{(u, r_1, r_2, r_3) \mid r_1, r_2, r_3 \text{ are three dist. roots of } u\}$$
$$\subset \mathbb{P}(V_Q) \times \mathbb{P}^1 \times \mathbb{P}^1 \times \mathbb{P}^1$$

- Is C absolutely irreducible? Consider a chain of covers

$$\begin{array}{ll} X_3 = C = \{(u, r_1, r_2, r_3)\} & \subset \mathbb{P}(V_Q) \times \mathbb{P}^1 \times \mathbb{P}^1 \times \mathbb{P}^1 \\ \theta_3 \downarrow & \\ X_2 = \{(u, r_1, r_2)\} & \subset \mathbb{P}(V_Q) \times \mathbb{P}^1 \times \mathbb{P}^1 \\ \theta_2 \downarrow & \\ X_1 = \{(u, r_1)\} & \subset \mathbb{P}(V_Q) \times \mathbb{P}^1 \\ \theta_1 \downarrow & \\ X_0 = \{(u)\} & = \mathbb{P}(V_Q) \end{array}$$

Irreducible?

IRREDUCIBLE COVERS

$$C = \{(u, r_1, r_2, r_3) \mid r_1, r_2, r_3 \text{ are three dist. roots of } u\}$$
$$\subset \mathbb{P}(V_Q) \times \mathbb{P}^1 \times \mathbb{P}^1 \times \mathbb{P}^1$$

- Is C absolutely irreducible? Consider a chain of covers

$$\begin{array}{lll} X_3 = C = \{(u, r_1, r_2, r_3)\} & \subset \mathbb{P}(V_Q) \times \mathbb{P}^1 \times \mathbb{P}^1 \times \mathbb{P}^1 & \text{Irreducible?} \\ \theta_3 \downarrow & & \\ X_2 = \{(u, r_1, r_2)\} & \subset \mathbb{P}(V_Q) \times \mathbb{P}^1 \times \mathbb{P}^1 & \\ \theta_2 \downarrow & & \\ X_1 = \{(u, r_1)\} & \subset \mathbb{P}(V_Q) \times \mathbb{P}^1 & \\ \theta_1 \downarrow & & \\ X_0 = \{(u)\} & = \mathbb{P}(V_Q) & \text{Irreducible: isomorphic to } \mathbb{P}^1 \end{array}$$

IRREDUCIBLE COVERS

$$C = \{(u, r_1, r_2, r_3) \mid r_1, r_2, r_3 \text{ are three dist. roots of } u\}$$
$$\subset \mathbb{P}(V_Q) \times \mathbb{P}^1 \times \mathbb{P}^1 \times \mathbb{P}^1$$

- Is C absolutely irreducible? Consider a chain of covers

$$\begin{array}{lll} X_3 = C = \{(u, r_1, r_2, r_3)\} & \subset \mathbb{P}(V_Q) \times \mathbb{P}^1 \times \mathbb{P}^1 \times \mathbb{P}^1 & \text{Irreducible?} \\ \quad \downarrow \theta_3 & & \\ X_2 = \{(u, r_1, r_2)\} & \subset \mathbb{P}(V_Q) \times \mathbb{P}^1 \times \mathbb{P}^1 & \\ \quad \downarrow \theta_2 & & \\ X_1 = \{(u, r_1)\} & \subset \mathbb{P}(V_Q) \times \mathbb{P}^1 & \text{Irreducible: also isomorphic to } \mathbb{P}^1 \\ \quad \downarrow \theta_1 & & \\ X_0 = \{(u)\} & = \mathbb{P}(V_Q) & \text{Irreducible: isomorphic to } \mathbb{P}^1 \end{array}$$

IRREDUCIBLE COVERS

$$C = \{(u, r_1, r_2, r_3) \mid r_1, r_2, r_3 \text{ are three dist. roots of } u\}$$
$$\subset \mathbb{P}(V_Q) \times \mathbb{P}^1 \times \mathbb{P}^1 \times \mathbb{P}^1$$

- Is C absolutely irreducible? Consider a chain of covers

$$X_3 = C = \{(u, r_1, r_2, r_3)\} \subset \mathbb{P}(V_Q) \times \mathbb{P}^1 \times \mathbb{P}^1 \times \mathbb{P}^1$$ Irreducible?

$$\downarrow \theta_3$$

$$X_2 = \{(u, r_1, r_2)\} \subset \mathbb{P}(V_Q) \times \mathbb{P}^1 \times \mathbb{P}^1$$ Irreducible?

$$\downarrow \theta_2$$

$$X_1 = \{(u, r_1)\} \subset \mathbb{P}(V_Q) \times \mathbb{P}^1$$ Irreducible: also isomorphic to $\mathbb{P}^1$

$$\downarrow \theta_1$$

$$X_0 = \{(u)\} = \mathbb{P}(V_Q)$$ Irreducible: isomorphic to $\mathbb{P}^1$

IRREDUCIBLE COVERS

$$
\begin{array}{lll}
X_3 = C = \{(u, r_1, r_2, r_3)\} & \subset \mathbb{P}(V_Q) \times \mathbb{P}^1 \times \mathbb{P}^1 \times \mathbb{P}^1 & \text{Irreducible?} \\
\theta_3 \downarrow & & \\
X_2 = \{(u, r_1, r_2)\} & \subset \mathbb{P}(V_Q) \times \mathbb{P}^1 \times \mathbb{P}^1 & \text{Irreducible?} \\
\theta_2 \downarrow & & \\
X_1 = \{(u, r_1)\} \cong \mathbb{P}^1 & \subset \mathbb{P}(V_Q) \times \mathbb{P}^1 & \\
\theta_1 \downarrow & & \\
X_0 = \{(u)\} \cong \mathbb{P}^1 & = \mathbb{P}(V_Q) &
\end{array}
$$

IRREDUCIBLE COVERS

$$\begin{array}{lll}
X_3 = C = \{(u, r_1, r_2, r_3)\} & \subset \mathbb{P}(V_Q) \times \mathbb{P}^1 \times \mathbb{P}^1 \times \mathbb{P}^1 & \text{Irreducible?} \\
\theta_3 \big\downarrow & & \\
X_2 = \{(u, r_1, r_2)\} & \subset \mathbb{P}(V_Q) \times \mathbb{P}^1 \times \mathbb{P}^1 & \text{Irreducible?} \\
\theta_2 \big\downarrow & & \\
X_1 = \{(u, r_1)\} \cong \mathbb{P}^1 & \subset \mathbb{P}(V_Q) \times \mathbb{P}^1 & \\
\theta_1 \big\downarrow & & \\
X_0 = \{(u)\} \cong \mathbb{P}^1 & = \mathbb{P}(V_Q) &
\end{array}$$

- For the irreducibility of X_2: observe that $X_2 = X_1 \times_{X_0} X_1 \setminus \Delta$, and deduce the irreducibility from the ramification properties of $\theta_1 : X_1 \to X_0$

IRREDUCIBLE COVERS

$$\begin{array}{lll}
X_3 = C = \{(u, r_1, r_2, r_3)\} & \subset \mathbb{P}(V_Q) \times \mathbb{P}^1 \times \mathbb{P}^1 \times \mathbb{P}^1 & \text{Irreducible?} \\
\theta_3 \downarrow & & \\
X_2 = \{(u, r_1, r_2)\} & \subset \mathbb{P}(V_Q) \times \mathbb{P}^1 \times \mathbb{P}^1 & \text{Irreducible?} \\
\theta_2 \downarrow & & \\
X_1 = \{(u, r_1)\} \cong \mathbb{P}^1 & \subset \mathbb{P}(V_Q) \times \mathbb{P}^1 & \\
\theta_1 \downarrow & & \\
X_0 = \{(u)\} \cong \mathbb{P}^1 & = \mathbb{P}(V_Q) &
\end{array}$$

Fibre product

- For the irreducibility of X_2: observe that $X_2 = X_1 \times_{X_0} X_1 \setminus \Delta$, and deduce the irreducibility from the ramification properties of $\theta_1 : X_1 \to X_0$

IRREDUCIBLE COVERS

$$\begin{array}{lll} X_3 = C = \{(u, r_1, r_2, r_3)\} & \subset \mathbb{P}(V_Q) \times \mathbb{P}^1 \times \mathbb{P}^1 \times \mathbb{P}^1 & \text{Irreducible?} \\ \theta_3 \downarrow & & \\ X_2 = \{(u, r_1, r_2)\} & \subset \mathbb{P}(V_Q) \times \mathbb{P}^1 \times \mathbb{P}^1 & \text{Irreducible?} \\ \theta_2 \downarrow & & \\ X_1 = \{(u, r_1)\} \cong \mathbb{P}^1 & \subset \mathbb{P}(V_Q) \times \mathbb{P}^1 & \\ \theta_1 \downarrow & & \\ X_0 = \{(u)\} \cong \mathbb{P}^1 & = \mathbb{P}(V_Q) & \end{array}$$

Fibre product

Diagonal

- For the irreducibility of X_2: observe that $X_2 = X_1 \times_{X_0} X_1 \setminus \Delta$, and deduce the irreducibility from the ramification properties of $\theta_1 : X_1 \to X_0$

IRREDUCIBLE COVERS

$$
\begin{array}{lll}
X_3 = C = \{(u, r_1, r_2, r_3)\} & \subset \mathbb{P}(V_Q) \times \mathbb{P}^1 \times \mathbb{P}^1 \times \mathbb{P}^1 & \text{Irreducible?} \\
\theta_3 \downarrow & & \\
X_2 = \{(u, r_1, r_2)\} & \subset \mathbb{P}(V_Q) \times \mathbb{P}^1 \times \mathbb{P}^1 & \text{Irreducible?} \\
\theta_2 \downarrow & & \\
X_1 = \{(u, r_1)\} \cong \mathbb{P}^1 & \subset \mathbb{P}(V_Q) \times \mathbb{P}^1 & \\
\theta_1 \downarrow & & \\
X_0 = \{(u)\} \cong \mathbb{P}^1 & = \mathbb{P}(V_Q) &
\end{array}
$$

Fibre product → $\times_{X_0}$; Diagonal → Δ

- For the irreducibility of X_2: observe that $X_2 = X_1 \times_{X_0} X_1 \setminus \Delta$, and deduce the irreducibility from the ramification properties of $\theta_1 : X_1 \to X_0$
- For X_3, same idea with $X_3 = X_2 \times_{X_1} X_2 \setminus \Delta$

THORSTEN KLEINJUNG*

BENJAMIN WESOLOWSKI*

A NEW PERSPECTIVE ON THE POWERS OF TWO DESCENT

for discrete logarithms in finite fields

PRESENTED AT ANTS-XIII, MADISON, WI, USA, ON THE 20/07/2018 BY BENJAMIN WESOLOWSKI

*EPFL, LAUSANNE, SWITZERLAND

COUNTING SPLIT POLYNOMIALS

- We have a cover $\theta : C \to \mathbb{P}(V_Q)$ defined over k such that

➡ C is absolutely irreducible

➡ For any P in $C(k)$, the poly. $\theta(P)$ splits completely over k

COUNTING SPLIT POLYNOMIALS

- We have a cover $\theta : C \to \mathbb{P}(V_Q)$ defined over k such that
- ➡ C is absolutely irreducible
- ➡ For any P in $C(k)$, the poly. $\theta(P)$ splits completely over k
- We want to show that $\theta(C(k))$ is a large part of $\mathbb{P}(V_Q)(k)$

COUNTING SPLIT POLYNOMIALS

- We have a cover $\theta : C \to \mathbb{P}(V_Q)$ defined over k such that

➡ C is absolutely irreducible

➡ For any P in $C(k)$, the poly. $\theta(P)$ splits completely over k

- We want to show that $\theta(C(k))$ is a large part of $\mathbb{P}(V_Q)(k)$

➡ C is of small degree, and absolutely irreducible, so

$$|C(k)| \approx |k|$$

COUNTING SPLIT POLYNOMIALS

- We have a cover $\theta : C \to \mathbb{P}(V_Q)$ defined over k such that
  - ➡ C is absolutely irreducible
  - ➡ For any P in $C(k)$, the poly. $\theta(P)$ splits completely over k
- We want to show that $\theta(C(k))$ is a large part of $\mathbb{P}(V_Q)(k)$
  - ➡ C is of small degree, and absolutely irreducible, so
$$|C(k)| \approx |k|$$
  - ➡ θ is "$(q^3 - q)$-to-one", therefore
$$|\theta(C(k))| \approx |k|/q^3 \approx |\mathbb{P}(V_Q)(k)|/q^3$$