Smooth models for Suzuki and Ree Curves

Abdulla Eid

RICAM Workshop
Algebraic curves over finite fields
Linz, Austria, November 11-15, 2013

Introduction

Three important examples of algebraic curves over finite fields:

- The Hermitian curve
- The Suzuki curve
- The Ree curve

Common properties

- Many rational points for given genus.
- Optimal w.r.t. Serre's explicit formula method.
- Large automorphism group
- Of Deligne-Lusztig type
- Ray class field over the projective line

Goal

For each of the curves, we want

- Function Field description.
- Very ample linear series.
- Smooth model in projective space.
- Weierstrass non-gaps semigroup at a rational point.
- Weierstrass non-gaps semigroup at a pair of rational points.

Known results

	Hermitian	Suzuki	Ree
Function field	✓	✓	✓
Very ample series	✓	✓	-
Smooth model	✓	-	-
non-gaps (1-point)	✓	✓	-
non-gaps (2-points)	✓	✓	-

Table : Known results about the three families of curves.

Deligne-Lusztig Theory

Deligne-Lusztig theory constructs linear representations for finite groups of Lie type (DL 1976).

It provides constructions for all representations of all finite simple groups of Lie type (L 1984).

Let G be a reductive algebraic group defined over a finite field with Frobenius F.

For a fixed $w \in W$, W the Weyl group of G, the DL variety $X(w)$ has as points those Borel subgroups B such that $F(B)$ is conjugate to B by an element bw, for some $b \in B$.

For a projective model of $X(w)$ we need to interpret B as a point (as the stabilizer of a point) in projective space.

DL curves

Let G be a connected reductive algebraic group over a finite field and let $G^\sigma := \{g \in G \mid \sigma(g) = g\}$, where σ^2 equals the Frobenius morphism. Associated to G^σ is a DL variety with automorphism group G^σ.

The points of a DL variety are Borel subgroups of the group G.

If G^σ is a simple group then G^σ = ${}^2A_2$, ${}^2B_2$, or ${}^2G_2$. For these groups the associated DL varieties are:

- Hermitian curve associated to ${}^2A_2 = \mathrm{PGU}(3, q)$.
- Suzuki curve associated to ${}^2B_2 = \mathrm{Sz}(q)$.
- Ree curve associated to ${}^2G_2 = R(q)$.

Projective model

(Tits 1962, Giulietti-Korchmáros-Torres 2006, D 2010, Kane 2011, Eid 2012)

The interpretation of the borel subgroup $B \in X(w)$ as a point in projecitve space will be as (stabilizer of) a line through a suitable point P and its Frobenius image $F(P)$ in a suitably chosen projective space.

- Hermitian curve : $P, F(P) \in \mathbb{P}^2$, smooth model in $\mathbb{P}^2$.
- Suzuki curve: $P, F(P) \in \mathbb{P}^3$, smooth model in $\mathbb{P}^4$.
- Ree curve $P, F(P) \in \mathbb{P}^6$, smooth model in $\mathbb{P}^{13}$.

Hermitian 2-pt codes

Reed-Solomon codes over $\mathbb{F}_q = \{0, a_1, \ldots, a_n\}$, defined with functions f such that $-\operatorname{ord}_\infty f \leq m_\infty$ and $\operatorname{ord}_0 f \geq m_0$,

$$C = \langle (f(a_1), \ldots, f(a_n)) : f = x^i, m_0 \leq i \leq m_\infty \rangle$$

Hermitian codes over $\mathbb{F}_q$, $q = q_0^2$, defined with the curve $y^{q_0} + y = x^{q_0+1}$, set of finite rational points $\mathcal{P} = \{O, P_1, \ldots, P_n\}$

$$\begin{aligned} C = \langle (f(P_1), \ldots, f(P_n)) : f = x^i y^j, & \\ -\operatorname{ord}_\infty f = q_0 i + (q_0+1) j \leq m_\infty, & \\ \operatorname{ord}_O f = i + (q_0+1) j \geq m_0 \rangle & \end{aligned}$$

Actual minimum distances are known:
(1-pt codes) Kumar-Yang, Kirfel-Pellikaan
(2-pt codes) Homma-Kim; Beelen, Park

Suzuki and Ree 2-pt codes

Suzuki codes over $\mathbb{F}_q$, $q = 2q_0^2$, defined with the *singular* curve $y^q + y = x^{q_0}(x^q + x)$.

Construction of Suzuki codes:
(1-pt codes) Hansen-Stichtenoth
(2-pt codes) Matthews, D-Park
Actual minimum distances unknown.

Ree codes over $\mathbb{F}_q$, $q = 3q_0^2$, defined with the *singular* curve $y^q - y = x^{q_0}(x^q - x)$, $z^q - z = x^{2q_0}(x^q - x)$.

Progress towards 1-pt codes: Hansen-Pedersen, Pedersen
Actual minimum distances unknown.

Suzuki curve

Deligne-Lusztig: Existence of Suzuki curve
Henn: The equation $y^q + y = x^{q_0}(x^q + x)$

Hansen-Stichtenoth:

(1) 1-pt codes can be defined using monomials in x, y, z, w, where

$$z = x^{2q_0+1} + y^{2q_0}, w = xy^{2q_0} + z^{2q_0}$$

(2) To prove irreducibility of the Suzuki curve, the following equations are used

$$z^q + z = x^{2q_0}(x^q + x), z^{q_0} = y + x^{q_0+1}, w^{q_0} = z + yx^{q_0}$$

Suzuki cont

Giulietti-Korchmáros-Torres:

(3) The divisor $D = (q + 2q_0 + 1)P_\infty$ is very ample. A basis for the vector space of functions with poles only at P_∞ and of order at most $q + 2q_0 + 1$ is given by the functions $1, x, y, z, w$. In other words: The morphism $(1 : x : y : z : w)$ that maps the Suzuki curve into projective space $\mathbb{P}^4$ has as image a smooth model for the Suzuki curve.

(4) $y = x^{q_0+1} + z^{q_0}$, $w = x^{2q_0+2} + xz + z^{2q_0}$.

Thus: $w = y^2 + xz$.

Smooth model

What are the equations for the smooth model of the Suzuki curve?

(Step 1) We identify the 5$-$tuple $(t : x : y : z : w)$ with the 2×4 matrix

$$\begin{pmatrix} 0 & t & x & y \\ y & z & w & 0 \end{pmatrix}$$

The equation $y^2 = xz + tw$ shows that two of the minors have the same determinant.

Upto multiplication by y the six minors have determinants t, x, y, y, z, w. And the coordinates $(t : x : y : z : w)$ are the Plücker coordinates for the matrix (after removing one of the two ys). They describe a line in $\mathbb{P}^3$.

Smooth model cont

(Step 2) As equations for the Suzuki curve we use the incidence of the line in $\mathbb{P}^3$ with the point $(w^{q_0} : z^{q_0} : x^{q_0} : t^{q_0})$.

(D 2010) The equations $y^2 + xz + tw = 0$ and

$$\begin{bmatrix} 0 & t & x & y \\ t & 0 & y & z \\ x & y & 0 & w \\ y & z & w & 0 \end{bmatrix} \begin{bmatrix} w^{q_0} \\ z^{q_0} \\ x^{q_0} \\ t^{q_0} \end{bmatrix} = 0.$$

define a smooth model for the Suzuki curve.

Suzuki 2-pt codes

For the given model, what are the functions that define 1-pt codes and 2-pt codes?

(D-Park 2008, 2012) The set M of $q + 2q_0 + 1$ monomials in x, y, z,

$$M = \{x^i z^j, 0 \leq i, j \leq q_0\} \cup \{yx^i z^j, 0 \leq i, j \leq q_0 - 1\}$$

gives a basis for the function field as an extension of $k(w)$.

Each 1-pt or 2-pt Suzuki code is an evaluation code for a uniquely defined subset of the functions $\{fw^i : f \in M, i \in \mathbb{Z}\}$.

Results for the Ree curve

(Abdulla Eid, Thesis 2013)

- The linear series $\left|(q^2 + 3q_0q + 2q + 3q_0 + 1)P_\infty\right|$ is very ample.
- Equations for the corresponding smooth model.
- Weierstrass non-gaps semigroup over $\mathbb{F}_{27}$ (1pt and 2-pt).

Henceforth $m = q^2 + 3q_0q + 2q + 3q_0 + 1$.

The Ree function field

(Pedersen, AGCT-3, 1991)

The Ree curve corresponds to the Ree function field $k(x, y_1, y_2)$ defined by the two equations

$$\begin{aligned} y_1^q - y_1 &= x^{q_0}(x^q - x), \\ y_2^q - y_2 &= x^{q_0}(y_1^q - y_1), \end{aligned}$$

where $q := 3q_0^2$, $q_0 := 3^s$, $s \geq 1$.

Construction of thirteen rational functions $x, y_1, y_2, w_1, \ldots, w_{10}$ with *independent* pole orders. The pole orders do not generate the full semigroup of Weierstrass nongaps.

The groups G_2 and ${}^2G_2$

- (Cartan 1896) G_2 is the automorphism group of the Octonion algebra.
- (Dickson 1905) $G_2(q)$ is the automorphism group of a variety in $\mathbb{P}^6$.
- (Ree 1961) After the work of Chevalley, ${}^2G_2$ is defined as the twisted subgroup of $G_2(q)$ using the Steinberg automorphism with $\sigma^2 = \mathrm{Fr}_q$, i.e., ${}^2G_2 = \{g \in G_2(q) \mid \sigma(g) = g\}$
- (Tits 1962) ${}^2G_2$ is defined as the group of automorphisms that are fixed under a polarity map
- (Pedersen 1992) ${}^2G_2$ is the automorphism group of the Ree function field.
- (Wilson 2010) Elementary construction without the use of Lie algebra.

1- Very Ample Linear Series

- For a divisor D of a function field $F/\mathbb{F}_q$, let

$$\begin{aligned} |D| :=& \{E \in \mathrm{Div}(F) \mid E \geq 0, E \sim D\} \\ =& \{D + (f) \mid f \in \mathcal{L}(D)\} \end{aligned}$$

- If $\mathcal{D}$ is a very ample linear series, then the morphism

$$\phi_{\mathcal{D}} : X \to \mathbb{P}^k$$

  associated with $\mathcal{D}$ is a smooth embedding, i.e., $\phi_{\mathcal{D}}(X)$ is isomorphic to X and is a smooth curve.

Theorem

For the Ree curve:

(1) *The space* $\mathcal{L}(mP_\infty)$ *is generated by* $1, x, y_1, y_2, w_1, \dots, w_{10}$ *over* $\mathbb{F}_q$ *and hence it is of dimension 14.*

(2) $\mathcal{D} = |mP_\infty|$ *is a very ample linear series.*

Outline of the proof:

- Since $h(\tilde{\Phi}) = 0$, where $\tilde{\Phi} : \mathcal{J}_\mathrm{R} \ni [P] \mapsto [P - P_\infty] \in \mathcal{J}_\mathrm{R}$, we have $q^2P + 3q_0q\Phi(P) + 2q\Phi^2(P) + 3q_0\Phi^3(P) + \Phi^4(P) \sim mP_\infty$
- We show that $\pi := (1 : x : y_1 : y_2 : w_1 : \cdots : w_{10})$ is injective using the equivalence above. So $\mathcal{D}$ separates points.
- We show that $j_1(P) = 1\ \forall P \in X_\mathrm{R}$, hence π separates tangent vectors.
- The maximal subgroup that fixes P_∞ acts linearly on $1, x, y_1, y_2, w_1, \dots, w_{10}$ and has a representation of dimension 14.

2 - Defining Equations

Hermitian curve

$F_{\mathrm{H}} := \mathbb{F}_q(x, y)$ defined by $y^{q_0+1} + x^{q_0+1} + 1 = 0$. ($q = q_0^2$).

Consider the matrix

$$H = \begin{pmatrix} 1 & : x & : y \\ 1 & : x^q & : y^q \end{pmatrix}.$$

and let $H_{i,j}$ be the Plücker coordinate of columns i, j.

Then

$$\begin{pmatrix} y^{q_0} & x^{q_0} & 1^{q_0} \end{pmatrix} \begin{pmatrix} y & y^q \\ x & x^q \\ 1 & 1^q \end{pmatrix} = 0$$

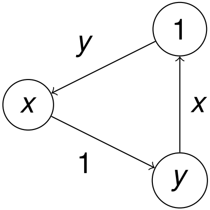
and

$$\begin{pmatrix} H_{1,2} & H_{3,1} & H_{2,3} \end{pmatrix} \begin{pmatrix} y & y^q \\ x & x^q \\ 1 & 1^q \end{pmatrix} = 0.$$

Both equations define the unique line between a point $P := (1, x, y)$ and its Frobenius image $P^{(q)} := (1, x^q, y^q)$.
So that y^{q_0} is proportional to $H_{1,2}$, x^{q_0} is proportional to $H_{3,1}$, and 1^{q_0} is proportional to $H_{2,3}$.

$$f = \begin{matrix} 1 \\ x \\ y \end{matrix} \qquad f^{q_0} \sim \begin{matrix} H_{2,3} \\ H_{3,1} \\ H_{1,2} \end{matrix}$$

We can read the defining equation of the Hermitian curve from a complete graph with three vertices (and edges labeled by Plücker coordinates) as follows:



We raise the vertices to the power of q_0 and we multiply them by the opposite edge and we sum the result to get $1 + x^{q_0+1} + y^{q_0+1} = 0$.

Suzuki curve

We apply the same idea of Plücker coordinates and the fact that the line between a point and its Frobenius image is unique.

Function field $F_S := \mathbb{F}_q(x, y)$ defined by $y^q - y = x^{q_0}(x^q - x)$
Define $z := x^{2q_0+1} - y^{2q_0}$ and $w := xy^{2q_0} - z^{2q_0}$.

Lemma

The Suzuki curve has a smooth model in $\mathbb{P}^4$ defined by the five equations $y^2 + xz + tw = 0$ and

$$\begin{bmatrix} 0 & t & x & y \\ t & 0 & y & z \\ x & y & 0 & w \\ y & z & w & 0 \end{bmatrix} \begin{bmatrix} w^{q_0} \\ z^{q_0} \\ x^{q_0} \\ t^{q_0} \end{bmatrix} = 0.$$

Consider the following matrix S

$$S = \begin{pmatrix} t & : x & : z & : w \\ t^q & : x^q & : z^q & : w^q \end{pmatrix}.$$

Then,

$$\begin{pmatrix} 0 & t^{2q_0} & x^{2q_0} & y^{2q_0} \\ t^{2q_0} & 0 & y^{2q_0} & z^{2q_0} \\ x^{2q_0} & y^{2q_0} & 0 & w^{2q_0} \\ y^{2q_0} & z^{2q_0} & w^{2q_0} & 0 \end{pmatrix} \begin{pmatrix} w & w^q \\ z & z^q \\ x & z^q \\ t & t^q \end{pmatrix} = 0$$

and

$$\begin{pmatrix} 0 & S_{1,2} & S_{1,3} & S_{3,2} \\ S_{1,2} & 0 & S_{1,4} & S_{4,2} \\ S_{1,3} & S_{1,4} & 0 & S_{4,3} \\ S_{3,2} & S_{4,2} & S_{4,3} & 0 \end{pmatrix} \begin{pmatrix} w & w^q \\ z & z^q \\ x & x^q \\ t & t^q \end{pmatrix} = 0.$$

We find

$$
\begin{array}{llll}
f = & 1 & f^{2q_0} \sim & S_{1,2} \\
 & x & & S_{1,3} \\
 & y & & S_{1,4} = S_{3,2} \\
 & z & & S_{4,2} \\
 & w & & S_{4,3}
\end{array}
$$

The five equations can be read from a complete graph with four vertices labeled by t, x, z, w.

$$
\begin{tikzcd}
t \arrow[r, "t"] \arrow[d, "x"'] \arrow[dr, "y"] & x \\
z \arrow[ur, "y"] & w \arrow[u, "z"'] \arrow[l, "w"]
\end{tikzcd}
$$

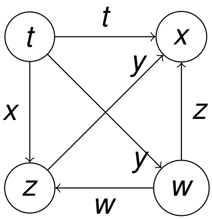
One plus four equations

The complete graph on four vertices gives rise to five equations:

A Plücker type relation for the six edges

and

Four more equations, one for each triangle in the graph.



Ree Curve

We apply the same techniques of the previous two curves to the Ree curve.

The Ree function field is defined by the two equations

$$y_1^q - y_1 = x^{q_0}(x^q - x), y_2^q - y_2 = x^{q_0}(y_1^q - y_1).$$

Pedersen defined ten rational functions $w_1, \ldots, w_{10}$ as polynomials in x, y_1, y_2.

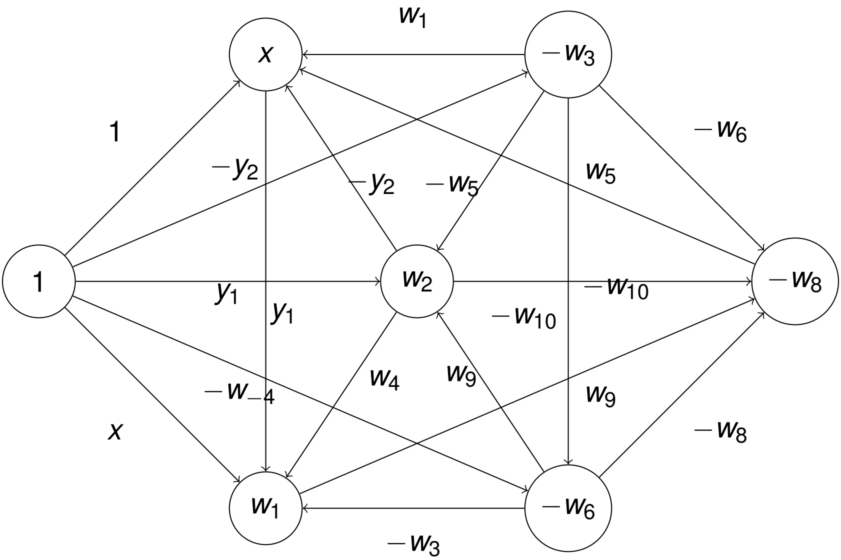
- Consider the following matrix R

$$R = \begin{pmatrix} t & : & x & : & w_1 & : & w_2 & : & w_3 & : & w_6 & : & w_8 \\ t^q & : & x^q & : & w_1^q & : & w_2^q & : & w_3^q & : & w_6^q & : & w_8^q \end{pmatrix}.$$

- Using the same techniques and ideas for the Hermitian and Suzuki curves we find that the Plücker coordinates correspond to the following functions

$$\begin{array}{llllll}
f = & t & f^{3q_0} \sim & R_{1,2} & y_1 & R_{2,3} = R_{1,4} \\
 & x & & R_{1,3} & y_2 & R_{1,5} = R_{2,4} \\
 & w_1 & & R_{2,5} & w_4 & R_{1,6} = R_{4,3} \\
 & w_3 & & R_{6,3} & w_5 & R_{7,2} = R_{5,4} \\
 & w_6 & & R_{7,5} & w_9 & R_{7,3} = R_{4,6} \\
 & w_8 & & R_{7,6} & w_{10} & R_{6,5} = R_{4,7} \\
 & & & & & \\
 & v_1 & & R_{5,3} & & \\
 & v_1 + w_2 & & R_{1,7} & & \\
 & v_1 - w_2 & & R_{6,2} & &
\end{array}$$

The Graph



Smooth model

From the complete graph we obtain 105 equations that define a smooth model for the Ree curve in $\mathbb{P}^{13}$.

$35 = \binom{7}{4}$ quadratic equations.

$35 = \binom{7}{3}$ equations of total degree $q_0 + 1$ of the form

$$aA^{q_0} + bB^{q_0} + cC^{q_0} = 0.$$

$35 = \binom{7}{3}$ equations of total degree $3q_0 + 1$ of the form

$$a^{3q_0}A + b^{3q_0}B + c^{3q_0}C = 0.$$

Relation to the previous embeddings of the Deligne-Lusztig Curves

- Kane independently gave smooth embeddings for the Deligne-Lusztig curves (arXiv 2011).
- Kane used the abstract definition of the DL curves as a set of Borel subgroups.
- For the Ree curve we can show that the set of $\mathbb{F}_q$-rational points is the same in our embedding and in Kane's embedding.
- The two approaches are similar if we associate to a line through a point and its Frobenius its stabilizer, which turns out to be a Borel subgroup and thus a rational point in the original definition as Deligne-Lusztig curve

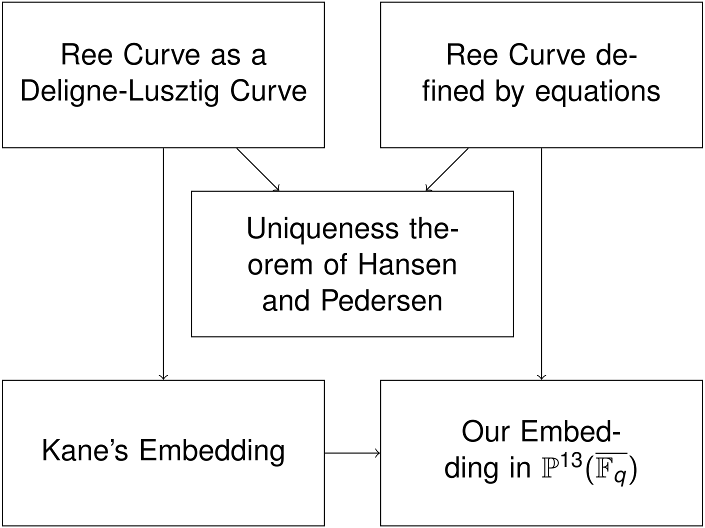


Figure : The relation between the two embeddings.

f	$\nu_0(f)$	$\nu_\infty(f)$
x	1	$-(q^2)$
y_1	q_0+1	$-(q^2+q_0q)$
y_2	$2q_0+1$	$-(q^2+2q_0q)$
w_1	$3q_0+1$	$-(q^2+3q_0q)$
w_2	$q+3q_0+1$	$-(q^2+3q_0q+q)$
w_3	$2q+3q_0+1$	$-(q^2+3q_0q+2q)$
w_4	$q+2q_0+1$	$-(q^2+2q_0q+q)$
v	$2q+3q_0+1$	$-(q^2+3q_0q+q)$
w_5	$q_0q+q+3q_0+1$	$-(q^2+3q_0q+q+q_0)$
w_6	$3q_0q+2q+3q_0+1$	$-(q^2+3q_0q+2q+3q_0)$
w_7	$q_0q+q+2q_0+1$	$-(q^2+2q_0q+q+q_0)$
w_8	$q^2+3q_0q+2q+3q_0+1$	$-(q^2+3q_0q+2q+3q_0+1)$
w_9	$q_0q+2q+3q_0+1$	$-(q^2+3q_0q+2q+q_0)$
w_{10}	$2q_0q+2q+3q_0+1$	$-(q^2+3q_0q+2q+2q_0)$

729	810	891	918	921	972	999	1002	1026	1029	1032
1866	2520	2547	2601	2604	2628	2631	2658	2706	2709	2712
3250	3277	3285	3286	3287	3312	3313	3314	3331	3358	3366
3393	3394	3395	3396	3444	3447	3471	3474	3477	3498	3501
3557	3558	3584	3585	3592	3612	3619	3638	3665	3673	3700
3751	3754	3777	3778	3781	3784	3804	3805	3808	3811	3814
3865	3889	3890	3892	3899	3919	3926	3943	3944	3946	3947
3973	3974	3980	4000	4001	4007	4010	4047	4048	4049	4051
4055	4057	4058	4061	4081	4082	4084	4085	4088	4091	4111
4118	4121	4174	4201	4228	4237	4238	4240	4241	4481	4484
4535	4538									

Non-gaps

Using the smooth model we computed the Weierstrass non-gaps semigroup at a rational point P for the Ree curve over $\mathbb{F}_{27}$
(of genus $g = 3627$).

(Computations in Magma/Macaulay2 using the singular model are not feasible)

THANK YOU