Good towers of function fields

Peter Beelen

RICAM Workshop on Algebraic Curves Over Finite Fields

12th of November 2013

joint with Alp Bassa and Nhut Nguyen
Recursive towers

- Explicit recursive towers have given rise to good lower bounds on $A(q)$. 

- Garcia & Stichtenoth introduced an explicit tower with the equation
  
  \[ (x^{i+1}x^i)^q + x^{i+1}x^i = x^{q+1} \text{ over } F_{q^2} \]
  
  This tower is optimal: $\lambda(F) = q^2 - 1$. 

Recursive towers

- Explicit recursive towers have given rise to good lower bounds on $A(q)$.
- A recursive towers is obtained by an equation $0 = \varphi(X, Y) \in \mathbb{F}_q[X, Y]$ such that
  - $F_0 = \mathbb{F}_q(x_0)$,
  - $F_{i+1} = F_i(x_{i+1})$ with $\varphi(x_{i+1}, x_i) = 0$ for $i \geq 0$.
Recursive towers

- Explicit recursive towers have given rise to good lower bounds on $A(q)$.
- A recursive tower is obtained by an equation $0 = \varphi(X, Y) \in \mathbb{F}_q[X, Y]$ such that
  - $F_0 = \mathbb{F}_q(x_0)$,
  - $F_{i+1} = F_i(x_{i+1})$ with $\varphi(x_{i+1}, x_i) = 0$ for $i \geq 0$.
- Garcia & Stichtenoth introduced an explicit tower with the equation
  \[
  (x_{i+1}x_i)^q + x_{i+1}x_i = x_i^{q+1} \quad \text{over } \mathbb{F}_{q^2}.
  \]

This tower is optimal: $\lambda(\mathcal{F}) = q - 1$. 
Recursive towers

- Explicit recursive towers have given rise to good lower bounds on $A(q)$.

- A recursive towers is obtained by an equation $0 = \varphi(X, Y) \in \mathbb{F}_q[X, Y]$ such that

  - $F_0 = \mathbb{F}_q(x_0)$,
  - $F_{i+1} = F_i(x_{i+1})$ with $\varphi(x_{i+1}, x_i) = 0$ for $i \geq 0$.

- Garcia & Stichtenoth introduced an explicit tower with the equation

  $$(x_{i+1}x_i)^q + x_{i+1}x_i = x_i^{q+1} \text{ over } \mathbb{F}_q^2.$$ 

This tower is optimal: $\lambda(\mathcal{F}) = q - 1$. 
Optimal towers and modular theory

- Elkies gave a modular interpretation of this Garcia–Stichtenoth tower using Drinfeld modular curves.
- Recipe to construct optimal towers using modular curves.
- All (?) currently known optimal towers can be (re)produced using modular theory.
Elkies gave a modular interpretation of this Garcia–Stichtenoth tower using Drinfeld modular curves.

Recipe to construct optimal towers using modular curves.

All (?) currently known optimal towers can be (re)produced using modular theory.

Not always directly clear! An example.
An example of a good tower

An example of a good tower

An example of a good tower

- After a change of variables, it is defined recursively by

$$ w^5 = v \frac{v^4 - 3v^3 + 4v^2 - 2v + 1}{v^4 + 2v^3 + 4v^2 + 3v + 1} $$
An example of a good tower


- After a change of variables, it is defined recursively by

$$w^5 = \nu \frac{\nu^4 - 3\nu^3 + 4\nu^2 - 2\nu + 1}{\nu^4 + 2\nu^3 + 4\nu^2 + 3\nu + 1}$$

- Tower by Elkies $X_0(5^n)_{n \geq 2}$ given by

$$y^5 + 5y^3 + 5y - 11 = \frac{(x - 1)^5}{x^4 + x^3 + 6x^2 + 6x + 11}.$$
An example of a good tower


- After a change of variables, it is defined recursively by

$$w^5 = v \frac{v^4 - 3v^3 + 4v^2 - 2v + 1}{v^4 + 2v^3 + 4v^2 + 3v + 1}$$

- Tower by Elkies $X_0(5^n)_{n \geq 2}$ given by

$$y^5 + 5y^3 + 5y - 11 = \frac{(x - 1)^5}{x^4 + x^3 + 6x^2 + 6x + 11}.$$  

- Relation turns out to be $1/v - v = x$ and $1/w - w = y$.  

An example of a good tower


After a change of variables, it is defined recursively by

$$w^5 = v \frac{v^4 - 3v^3 + 4v^2 - 2v + 1}{v^4 + 2v^3 + 4v^2 + 3v + 1}$$

Tower by Elkies $X_0(5^n)_{n\geq 2}$ given by

$$y^5 + 5y^3 + 5y - 11 = \frac{(x - 1)^5}{x^4 + x^3 + 6x^2 + 6x + 11}.$$  

Relation turns out to be $1/v - v = x$ and $1/w - w = y$. 

An example of a good tower (continued)

- Turns out that the equation

\[ w^5 = \nu \frac{\nu^4 - 3\nu^3 + 4\nu^2 - 2\nu + 1}{\nu^4 + 2\nu^3 + 4\nu^2 + 3\nu + 1} \]

occurred 100 years ago in the first letter of Ramanujan to Hardy.
An example of a good tower (continued)

- Turns out that the equation

\[ w^5 = v \frac{v^4 - 3v^3 + 4v^2 - 2v + 1}{v^4 + 2v^3 + 4v^2 + 3v + 1} \]

occurred 100 years ago in the first letter of Ramanujan to Hardy.

- The equation relates two values of the Roger–Ramanujan continued fraction, which can be used to parameterize \( X(5) \).
An example of a good tower (continued)

- Turns out that the equation

\[ w^5 = v \frac{v^4 - 3v^3 + 4v^2 - 2v + 1}{v^4 + 2v^3 + 4v^2 + 3v + 1} \]

occurred 100 years ago in the first letter of Ramanujan to Hardy.

- The equation relates two values of the Roger–Ramanujan continued fraction, which can be used to parameterize \( X(5) \).

- Obtain an optimal tower over \( \mathbb{F}_{p^2} \) if \( p \equiv \pm 1 \, (\text{mod} \, 5) \) and a good tower over \( \mathbb{F}_{p^4} \) if \( p \equiv \pm 2 \, (\text{mod} \, 5) \).
An example of a good tower (continued)

- Turns out that the equation

\[ w^5 = v \frac{v^4 - 3v^3 + 4v^2 - 2v + 1}{v^4 + 2v^3 + 4v^2 + 3v + 1} \]

occurred 100 years ago in the first letter of Ramanujan to Hardy.

- The equation relates two values of the Roger–Ramanujan continued fraction, which can be used to parameterize $X(5)$.

- Obtain an optimal tower over $\mathbb{F}_{p^2}$ if $p \equiv \pm 1 \pmod{5}$ and a good tower over $\mathbb{F}_{p^4}$ if $p \equiv \pm 2 \pmod{5}$. For the splitting one needs that $\zeta_5$ is in the constant field.
Drinfeld modules over an elliptic curve

- \( A := \mathbb{F}_q[T, S]/(f(T, S)) \) is the coordinate ring of an elliptic curve \( E \) defined over \( \mathbb{F}_q \) by a Weierstrass equation \( f(T, S) = 0 \) with

\[
f(T, S) = S^2 + a_1 TS + a_3 S - T^3 - a_2 T^2 - a_4 T - a_6, \quad a_i \in \mathbb{F}_q.
\]

(1)
Drinfeld modules over an elliptic curve

- $A := \mathbb{F}_q[T, S]/(f(T, S))$ is the coordinate ring of an elliptic curve $E$ defined over $\mathbb{F}_q$ by a Weierstrass equation $f(T, S) = 0$ with

$$f(T, S) = S^2 + a_1 TS + a_3 S - T^3 - a_2 T^2 - a_4 T - a_6, a_i \in \mathbb{F}_q.$$  \hspace{1em} (1)

- We write $A = \mathbb{F}_q[E]$.
- $P = (T_P, S_P) \in \mathbb{F}_q \times \mathbb{F}_q$ is a rational point of $E$.
- We set the ideal $\langle T - T_P, S - S_P \rangle$ as the characteristic of $F$ (the field $F$ is yet to be determined).
Drinfeld modules over an elliptic curve

- $A := \mathbb{F}_q[T, S]/(f(T, S))$ is the coordinate ring of an elliptic curve $E$ defined over $\mathbb{F}_q$ by a Weierstrass equation $f(T, S) = 0$ with

$$f(T, S) = S^2 + a_1TS + a_3S - T^3 - a_2T^2 - a_4T - a_6, a_i \in \mathbb{F}_q.$$  

(1)

- We write $A = \mathbb{F}_q[E]$.
- $P = (T_P, S_P) \in \mathbb{F}_q \times \mathbb{F}_q$ is a rational point of $E$.
- We set the ideal $\langle T - T_P, S - S_P \rangle$ as the characteristic of $F$ (the field $F$ is yet to be determined).
- We consider rank 2 Drinfeld modules $\phi$ specified by the following polynomials

$$\begin{cases} 
\phi_T := \tau^4 + g_1\tau^3 + g_2\tau^2 + g_3\tau + T_P, \\
\phi_S := \tau^6 + h_1\tau^5 + h_2\tau^4 + h_3\tau^3 + h_4\tau^2 + h_5\tau + S_P.
\end{cases}$$

(2)
Relations between the variables

\[
\begin{cases}
\phi_T := \tau^4 + g_1 \tau^3 + g_2 \tau^2 + g_3 \tau + T_P, \\
\phi_S := \tau^6 + h_1 \tau^5 + h_2 \tau^4 + h_3 \tau^3 + h_4 \tau^2 + h_5 \tau + S_P.
\end{cases}
\]

$\triangleright$ $S, T$ satisfy $f(T, S) = 0$ and (clearly) $ST = TS$, implying $\phi_S \phi_T = \phi_T \phi_S$.

$\triangleright$ Since $f(T, S) = 0$, we have $\phi_f(T, S) = 0$.
Relations between the variables

\[
\begin{aligned}
\phi_T &:= \tau^4 + g_1\tau^3 + g_2\tau^2 + g_3\tau + T_P, \\
\phi_S &:= \tau^6 + h_1\tau^5 + h_2\tau^4 + h_3\tau^3 + h_4\tau^2 + h_5\tau + S_P.
\end{aligned}
\]

- $S, T$ satisfy $f(T, S) = 0$ and (clearly) $ST = TS$, implying $\phi_S \phi_T = \phi_T \phi_S$.
- Since $f(T, S) = 0$, we have $\phi_{f(T,S)} = 0$.
- $\phi$ is a Drinfeld module if and only if it satisfies $\phi_{f(T,S)} = 0$ and $\phi_T \phi_S = \phi_S \phi_T$. 

Writing down a Drinfeld module amounts to solving a system of polynomial equations over $F$. 
Relations between the variables

\[
\begin{align*}
\phi_T &:= \tau^4 + g_1 \tau^3 + g_2 \tau^2 + g_3 \tau + T_P, \\
\phi_S &:= \tau^6 + h_1 \tau^5 + h_2 \tau^4 + h_3 \tau^3 + h_4 \tau^2 + h_5 \tau + S_P.
\end{align*}
\]

▶ \(S, T\) satisfy \(f(T, S) = 0\) and (clearly) \(ST = TS\), implying \(\phi_S \phi_T = \phi_T \phi_S\).

▶ Since \(f(T, S) = 0\), we have \(\phi_{f(T, S)} = 0\).

▶ \(\phi\) is a Drinfeld module if and only if it satisfies \(\phi_{f(T, S)} = 0\) and \(\phi_T \phi_S = \phi_S \phi_T\).

▶ In general characteristic \(\phi_{f(T, S)} = 0\) is implied by \(\phi_T \phi_S = \phi_S \phi_T\).
Relations between the variables

\[
\begin{align*}
\phi_T &:= \tau^4 + g_1 \tau^3 + g_2 \tau^2 + g_3 \tau + T_P, \\
\phi_S &:= \tau^6 + h_1 \tau^5 + h_2 \tau^4 + h_3 \tau^3 + h_4 \tau^2 + h_5 \tau + S_P.
\end{align*}
\]

- \(S, T\) satisfy \(f(T, S) = 0\) and (clearly) \(ST = TS\), implying \(\phi_S \phi_T = \phi_T \phi_S\).
- Since \(f(T, S) = 0\), we have \(\phi_{f(T,S)} = 0\).
- \(\phi\) is a Drinfeld module if and only if it satisfies \(\phi_{f(T,S)} = 0\) and \(\phi_T \phi_S = \phi_S \phi_T\).
- In general characteristic \(\phi_{f(T,S)} = 0\) is implied by \(\phi_T \phi_S = \phi_S \phi_T\).
- Writing down a Drinfeld module amounts to solving a system of polynomial equations over \(F\).
Gekeler’s description

Theorem (Gekeler)

The algebraic set describing isomorphism classes of normalized rank 2 Drinfeld modules over $A = \mathbb{F}_q[E]$ consists of $h_E$ rational curves.
Gekeler’s description

Theorem (Gekeler)

The algebraic set describing isomorphism classes of normalized rank 2 Drinfeld modules over $A = \mathbb{F}_q[E]$ consists of $h_E$ rational curves.

- This means that there exist one-parameter families of isomorphism classes of normalized rank 2 Drinfeld modules (described by a parameter we denote by $u$).
Gekeler’s description

Theorem (Gekeler)

The algebraic set describing isomorphism classes of normalized rank 2 Drinfeld modules over $A = \mathbb{F}_q[E]$ consists of $h_E$ rational curves.

- This means that there exist one-parameter families of isomorphism classes of normalized rank 2 Drinfeld modules (described by a parameter we denote by $u$).
- If $c \in F^*$ satisfies $c\phi = \psi c$, then $c \in \mathbb{F}_{q^2}$. 

Gekeler’s description

Theorem (Gekeler)

The algebraic set describing isomorphism classes of normalized rank 2 Drinfeld modules over $A = \mathbb{F}_q[E]$ consists of $h_E$ rational curves.

- This means that there exist one-parameter families of isomorphism classes of normalized rank 2 Drinfeld modules (described by a parameter we denote by $u$).
- If $c \in F^*$ satisfies $c\phi = \psi c$, then $c \in \mathbb{F}_{q^2}$.
- The quantities $g_1^{q+1}, g_2, g_3^{q+1}, h_1^{q+1}, h_2, h_3^{q+1}, h_4, h_5^{q+1}$ are invariant under isomorphism (and hence expressible in $u$).
Theorem (Gekeler)

The algebraic set describing isomorphism classes of normalized rank 2 Drinfeld modules over $A = \mathbb{F}_q[E]$ consists of $h_E$ rational curves.

- This means that there exist one-parameter families of isomorphism classes of normalized rank 2 Drinfeld modules (described by a parameter we denote by $u$).
- If $c \in F^*$ satisfies $c\phi = \psi c$, then $c \in \mathbb{F}_{q^2}$.
- The quantities $g_1^{q+1}, g_2, g_3^{q+1}, h_1^{q+1}, h_2, h_3^{q+1}, h_4, h_5^{q+1}$ are invariant under isomorphism (and hence expressible in $u$).
- Furthermore Gekeler showed that supersingular Drinfeld modules in characteristic $P$ are defined over $\mathbb{F}_{q^e}$, with $e = 2 \operatorname{ord}(P) \deg(P)$.
Example

- Let \( A = \mathbb{F}_{2}[T, S]/(f(T, S)) \) with
  \[
f(T, S) := S^2 + S + T^3 + T^2,
  \]
  \( (3) \)

- Choose \( T_P = S_P = 0 \), condition \( \phi_{f(T, S)} = 0 \) gives us

\[
\begin{align*}
h_5 &= 0, h_4 + h_5^3 + g_3^3 = 0, h_3 + h_4 h_5 + h_4 h_5^4 + g_2 g_3 + g_2 g_3^4 + g_3^7 = 0, \\
h_2 &= h_3^2 h_5 + h_3 h_5^8 + h_4^5 + g_1 g_3 + g_1 g_3^8 + g_3^5 + g_2^3 + g_2^9 + g_2 g_3^{12} = 0, \\
h_1 &= h_2^2 h_5 + h_2 h_5^{16} + h_3 h_4 + h_3 h_4^8 + g_4 g_2 + g_4^3 g_3 + g_1^2 g_3 + g_1 g_3^8 + g_1 g_3^{24} + g_2^{10} g_3 \\
&\quad+ g_2^9 g_3 + g_2 g_3^{16} + g_3^{16} + g_3 = 0, \\
h_1^2 h_5 + h_1 h_5^{32} + h_2 h_4 + h_2 h_4^{16} + h_3 + g_1^9 + g_1 g_2 g_3 + g_1 g_2 g_3^4 + g_1 g_2 g_3^{32} + g_1 g_2^{16} g_3 \\
&\quad+ g_1 g_2^{16} g_3 + g_1 g_2 g_3^{32} + g_2^{21} + g_2^{16} + g_2 + g_3^{48} + g_3^{33} + g_3^3 + 1 = 0, \\
h_1^4 h_4 + h_1 h_4^{32} + h_2 h_3 + h_2 h_3^{16} + h_5 + g_1^{18} g_3 + g_1^{17} g_3 + g_1^{16} g_3 + g_1^{16} g_3 + g_1^{9} g_3 \\
&\quad+ g_1^{4} g_2^{33} + g_1 g_2^{40} + g_1 + g_1^{32} g_3 + g_1^{32} g_3 + g_2^{16} g_3 + g_2^{64} + g_2 g_3 + g_2 g_3^{16} + g_2 g_3^{64} + g_2 g_3^{4} = 0, \\
h_8 h_3 + h_1 h_3^{2} + h_2^{17} + h_4^4 + h_4^4 + g_1^{36} g_2 + g_1^{33} g_2 + g_1^{32} g_3 + g_1^{32} g_3 + g_1^{16} g_3 + g_1^{12} g_2 \\
&\quad+ g_1^{2} g_3 + g_1 g_3^{128} + g_1 g_3^8 + g_2^{80} + g_2^{65} + g_2^5 + 1 = 0, \\
h_1^{16} h_2 + h_1 h_2^{32} + h_3^4 + h_3 + g_1^{73} + g_1^{64} g_2 + g_1^{64} g_2 + g_1^{16} g_2 + g_1^{12} g_2 + g_1^{4} g_2 + g_1 g_2^{128} + g_1 g_2^{8} \\
&\quad+ g_3^{256} + g_3^{16} + g_3 = 0, \\
h_1^{33} + h_2^{64} + h_2 + g_1^{144} + g_1^{129} + g_1^9 + g_2^{256} + g_2^{16} + g_2 = 0, \\
h_1^{64} + h_1 + g_1^{256} + g_1^{16} + g_1 = 0.
\]
Example

The condition $\phi_T \phi_S = \phi_S \phi_T$ gives us

\[
\begin{align*}
    h_5^2 g_3 + h_5 g_3^2 &= 0, \\
    h_4^2 g_3 + h_4 g_3^4 + h_5^4 g_2 + h_5 g_2^2 &= 0, \\
    h_3^2 g_3 + h_3 g_3^8 + h_4^4 g_2 + h_4 g_2^4 + h_5^8 g_1 + h_5 g_1^2 &= 0, \\
    h_2^2 g_3 + h_2 g_3^{16} + h_3^4 g_2 + h_3 g_2^8 + h_4^8 g_1 + h_4 g_1^4 + h_5^{16} + h_5 &= 0, \\
    h_1^2 g_3 + h_1 g_3^{32} + h_2^4 g_2 + h_2 g_2^{16} + h_3^8 g_1 + h_3 g_1^8 + h_4^{16} + h_4 &= 0, \\
    h_1^4 g_2 + h_1 g_2^{32} + h_2 g_1^{16} + h_3^{16} + h_3 + g_3^{64} + g_3 &= 0, \\
    h_1^8 g_1 + h_1 g_1^{32} + h_2^{16} + h_2 + g_2^{64} + g_2 &= 0, \\
    h_1^{16} + h_1 + g_1^{64} + g_1 &= 0.
\end{align*}
\]
Example

- The condition $\phi_T \phi_S = \phi_S \phi_T$ gives us

\[
\begin{align*}
 h_5^2 g_3 + h_5 g_3^2 &= 0, \\
 h_4^2 g_3 + h_4 g_3^4 + h_4^4 g_2 + h_5 g_2^2 &= 0, \\
 h_3^2 g_3 + h_3 g_3^8 + h_4^4 g_2 + h_4^4 g_2 + h_5^8 g_1 + h_5 g_1^2 &= 0, \\
 h_2^2 g_3 + h_2 g_3^{16} + h_3 g_2 + h_3 g_2 + h_4^8 g_1 + h_4 g_1^4 + h_5^{16} + h_5 &= 0, \\
 h_1^2 g_3 + h_1 g_3^{32} + h_2^4 g_2 + h_2 g_2^{16} + h_3^8 g_1 + h_3 g_1^8 + h_4^{16} + h_4 &= 0, \\
 h_1^4 g_2 + h_1 g_2^{32} + h_2 g_1 + h_2 g_1^{16} + h_3^{16} + h_3 + g_3^{64} + g_3 &= 0, \\
 h_1^8 g_1 + h_1 g_1^{32} + h_2^{16} + h_2 + g_2^{64} + g_2 &= 0, \\
 h_1^{16} + h_1 + g_1^{64} + g_1 &= 0.
\end{align*}
\]

Groebner basis

- Variable elimination, some simplifications and a Groebner basis computation on a computer give a complete description of all rank 2 normalized Drinfeld modules.
Computational results (an example)

Let $\alpha^5 + \alpha^2 + 1 = 0$. The quantities $g_1^3, g_2, g_3^3, h_1^3, h_2, h_3^3, h_4, h_5^3$ can all be expressed in a parameter $u$. 
Let $\alpha^5 + \alpha^2 + 1 = 0$. The quantities $g_1^3, g_2, g_3^3, h_1^3, h_2, h_3^3, h_4, h_5^3$ can all be expressed in a parameter $u$.

- The parameter $u$ itself is first expressed in terms of $g_1^3, \ldots, h_5^3$. 
Computational results (an example)

Let $\alpha^5 + \alpha^2 + 1 = 0$. The quantities $g_1^3, g_2, g_3^3, h_1^3, h_2, h_3^3, h_4, h_5^3$ can all be expressed in a parameter $u$.

- The parameter $u$ itself is first expressed in terms of $g_1^3, \ldots, h_5^3$.
- Afterwards, all variables are expressed in terms of $u$. 
Computational results (an example)

Let $\alpha^5 + \alpha^2 + 1 = 0$. The quantities $g_3^3, g_2, g_3, h_1^3, h_2, h_3^3, h_4, h_5^3$ can all be expressed in a parameter $u$.

- The parameter $u$ itself is first expressed in terms of $g_3^3, \ldots, h_5^3$.
- Afterwards, all variables are expressed in terms of $u$.

For example

$$g_3^3 = \alpha \frac{(u + \alpha^5)^3(u + \alpha^{26})(u + \alpha^{27})^3(u^2 + \alpha^{20}u + \alpha^{27})^3}{(u + \alpha^6)^2(u + \alpha^{10})^2(u + \alpha^{16})^2(u + \alpha^{19})^2(u + \alpha^{28})^5}$$
Isogenies

Definition
Let $\phi$ and $\psi$ be two Drinfeld modules. We say $\phi$ and $\psi$ are isogenous if there exists $\lambda \in F\{\tau\}$ such that for all $a \in A$,

$$\lambda \phi_a = \psi_a \lambda.$$ 

Such $\lambda$ is called an isogeny.
Isogenies

Definition
Let \( \phi \) and \( \psi \) be two Drinfeld modules. We say \( \phi \) and \( \psi \) are isogenous if there exists \( \lambda \in F\{\tau\} \) such that for all \( a \in A \),

\[
\lambda \phi_a = \psi_a \lambda.
\]

Such \( \lambda \) is called an isogeny.

- Isogenies exist only between modules of the same rank.
Isogenies

Definition
Let $\phi$ and $\psi$ be two Drinfeld modules. We say $\phi$ and $\psi$ are isogenous if there exists $\lambda \in F\{\tau\}$ such that for all $a \in A$,

$$\lambda \phi_a = \psi_a \lambda.$$ 

Such $\lambda$ is called an isogeny.

- Isogenies exists only between modules of the same rank.

Example (continue)
Let $\lambda = \tau - a \in F\{\tau\}$ and $\psi$ is another Drinfeld $A$-module defined by

$$\begin{cases} 
\psi_T := \tau^4 + l_1 \tau^3 + l_2 \tau^2 + l_3 \tau + T_P, \\
\psi_S := \tau^6 + t_1 \tau^5 + t_2 \tau^4 + t_3 \tau^3 + t_4 \tau^2 + t_5 \tau + S_P.
\end{cases}$$
Isogenies

- $\lambda = \tau - a \in F\{\tau\}$ is an isogeny from $\phi$ to $\psi$ if and only if
  \[ \lambda \phi_T = \psi_T \lambda \]  
  \[ \lambda \phi_S = \psi_S \lambda. \]
Isogenies

- $\lambda = \tau - a \in F\{\tau\}$ is an isogeny from $\phi$ to $\psi$ if and only if
  \[ \lambda \phi_T = \psi_T \lambda \]  
  \[ \lambda \phi_S = \psi_S \lambda. \]  

- Solving (5) gives us
  \[ a^{q^3+q^2+q+1} + g_1 a^{q^2+q+1} + g_2 a^{q+1} + g_3 a = \gamma \in F_q. \]  

- Solving (6) gives us
  \[ a^{q^5+q^4+q^3+q^2+q+1} + h_1 a^{q^4+q^3+q^2+q+1} + h_2 a^{q^3+q^2+q+1} + h_3 a^{q^2+q+1} + h_4 a^{q+1} + h_5 a = \beta \in F_q. \]
Idea to get a tower equation

- Connect two one parameter families (using variables \( u_0 \) and \( u_1 \)) with an isogeny of the form \( \tau - a_0 \). We can use the resulting algebraic relations to construct two inclusions.
- We have \( \mathbb{F}_q(u_0) \subset \mathbb{F}_q(a_0, u_0, u_1) \supset \mathbb{F}_q(u_1) \).
- Relating the variables \( u_0 \) and \( u_1 \) gives a polynomial equation \( \phi(u_1, u_0) = 0 \).
Towers from isogenous Drinfeld modules

Idea to get a tower equation

- Connect two one parameter families (using variables $u_0$ and $u_1$) with an isogeny of the form $\tau - a_0$. We can use the resulting algebraic relations to construct two inclusions
- We have $\mathbb{F}_q(u_0) \subset \mathbb{F}_q(a_0, u_0, u_1) \supset \mathbb{F}_q(u_1)$.
- Relating the variables $u_0$ and $u_1$ gives a polynomial equation $\varphi(u_1, u_0) = 0$.
- Iterating this gives a tower recursively defined by

$$\varphi(x_{i+1}, x_i) = 0$$
Example (continued)

- Relating the variables is easy and we find:

\[
\phi_i(x_{i+1}, x_i) = 0:
\]

\[
0 = x_{3i+1} + (\alpha_{17i} x_{3i} + \alpha_{29i} x_{2i} + x_i + \alpha_{30i}) (x_{3i} + \alpha_{24i} x_{2i} + \alpha_{4i} x_i + \alpha_{9i}) x_{2i+1} + (\alpha_{30i} x_{3i} + \alpha_{12i} x_{2i} + \alpha_{30i} x_i + \alpha_{17i}) (x_{3i} + \alpha_{24i} x_{2i} + \alpha_{4i} x_i + \alpha_{9i}) x_i + (\alpha_{4i} x_{3i} + \alpha_{14i} x_{2i} + \alpha_{19i}) (x_{3i} + \alpha_{24i} x_{2i} + \alpha_{4i} x_i + \alpha_{9i}).
\]

The resulting tower \( F = (F_1, F_2, \ldots) \) is defined by \( F_1 = F_2^{10}(x_1) \).

\( F_i+1 = F_i(x_{i+1}) \) with \( \phi_i(x_{i+1}, x_i) = 0. \)

Limit of the resulting tower is at least 1.
Example (continued)

- Relating the variables is easy and we find:
- The tower equation $\varphi_i(x_{i+1}, x_i) = 0$:

$$0 = x_{i+1}^3 + \frac{(\alpha_i^{17} x_i^3 + \alpha_i^{29} x_i^2 + x_i + \alpha_i^{30})}{(x_i^3 + \alpha_i^{24} x_i^2 + \alpha_i^{4} x_i + \alpha_i^{9})} x_{i+1}^2 + \frac{(\alpha_i^{30} x_i^3 + \alpha_i^{12} x_i^2 + \alpha_i^{30} x_i + \alpha_i^{17})}{(x_i^3 + \alpha_i^{24} x_i^2 + \alpha_i^{4} x_i + \alpha_i^{9})} x_{i+1}^3 + \frac{(\alpha_i^{4} x_i^3 + \alpha_i^{14} x_i^2 + \alpha_i^{19})}{(x_i^3 + \alpha_i^{24} x_i^2 + \alpha_i^{4} x_i + \alpha_i^{9})}. $$

- Here $\alpha_i = \alpha^{8^i}$
Relating the variables is easy and we find:

The tower equation $\varphi_i(x_{i+1}, x_i) = 0$:

$$0 = x_{i+1}^3 + \frac{(\alpha_i^{17} x_i^3 + \alpha_i^{29} x_i^2 + x_i + \alpha_i^{30})}{(x_i^3 + \alpha_i^{24} x_i^2 + \alpha_i^4 x_i + \alpha_i^9)} x_{i+1}^2 +$$

$$\frac{(\alpha_i^{30} x_i^3 + \alpha_i^{12} x_i^2 + \alpha_i^{30} x_i + \alpha_i^{17})}{(x_i^3 + \alpha_i^{24} x_i^2 + \alpha_i^4 x_i + \alpha_i^9)} x_{i+1} + \frac{(\alpha_i^4 x_i^3 + \alpha_i^{14} x_i^2 + \alpha_i^{19})}{(x_i^3 + \alpha_i^{24} x_i^2 + \alpha_i^4 x_i + \alpha_i^9)} x_{i+1}.$$

Here $\alpha_i = \alpha^{8_i}$

The resulting tower $\mathcal{F} = (F_1, F_2, \ldots)$ is defined by

- $F_1 = \mathbb{F}_{2^{10}}(x_1)$.
- $F_{i+1} = F_i(x_{i+1})$ with $\varphi_i(x_{i+1}, x_i) = 0$.

Limit of the resulting tower is at least 1.
Thank you for your attention!