A problem of Beelen, Garcia and Stichtenoth on an Artin-Schreier tower

Horacio Navarro

IMAL-CONICET

XXI Coloquio Latinoamericano de Álgebra

Buenos Aires

July 29, 2016

Joint work with María Chara and Ricardo Toledano

Is the tower recursively defined by the equation

$$y^2 + y = \frac{x}{x^2 + x + 1}$$

asymptotically good over $\mathbb{F}_{2^s}$ for some $s \geq 1$?

Is the tower recursively defined by the equation

$$y^2 + y = \frac{x}{x^2 + x + 1}$$

asymptotically good over $\mathbb{F}_{2^s}$ for some $s \geq 1$?

In this talk we show that the answer for this problem is negative for any s odd, i.e. the tower $\mathcal{H}$ is asymptotically bad over $\mathbb{F}_{2^s}$ for any s odd.

Is the tower recursively defined by the equation

$$y^2 + y = \frac{x}{x^2 + x + 1}$$

asymptotically good over $\mathbb{F}_{2^s}$ for some $s \geq 1$?

In this talk we show that the answer for this problem is negative for any s odd, i.e. the tower $\mathcal{H}$ is asymptotically bad over $\mathbb{F}_{2^s}$ for any s odd.

A motivation to study towers of function fields comes from coding theory.

Algebraic function fields

A field extension F/K is an *algebraic function field* if there exists an element $x \in F$ trascendental over K such that $F/K(x)$ is a finite extension.

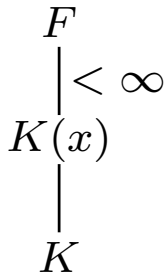
Algebraic function fields

A field extension F/K is an *algebraic function field* if there exists an element $x \in F$ trascendental over K such that $F/K(x)$ is a finite extension.

Invariants of F/K: genus $g(F)$, number of rational places $N(F)$.

Algebraic function fields

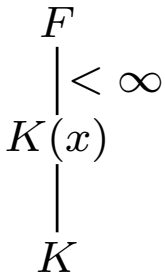
A field extension F/K is an *algebraic function field* if there exists an element $x \in F$ trascendental over K such that $F/K(x)$ is a finite extension.



Invariants of F/K: genus $g(F)$, number of rational places $N(F)$.

Algebraic function fields

A field extension F/K is an *algebraic function field* if there exists an element $x \in F$ trascendental over K such that $F/K(x)$ is a finite extension.



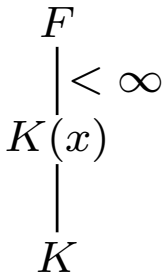
Invariants of F/K: genus $g(F)$, number of rational places $N(F)$.

Examples:

i) The rational function field $F := \mathbb{F}_q(x)$ has $g(F) = 0$ and $N(F) = q + 1$.

Algebraic function fields

A field extension F/K is an *algebraic function field* if there exists an element $x \in F$ trascendental over K such that $F/K(x)$ is a finite extension.



Invariants of F/K: genus $g(F)$, number of rational places $N(F)$.

Examples:

i) The rational function field $F := \mathbb{F}_q(x)$ has $g(F) = 0$ and $N(F) = q + 1$.

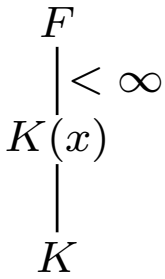
ii) The algebraic function field $F := \mathbb{F}_8(x, y)$ defined by the equation

$$y^2 + y = \frac{x}{x^2 + x + 1}$$

has $g(F) = 1$ and $N(F) = 4$.

Algebraic function fields

A field extension F/K is an *algebraic function field* if there exists an element $x \in F$ trascendental over K such that $F/K(x)$ is a finite extension.



Invariants of F/K: genus $g(F)$, number of rational places $N(F)$.

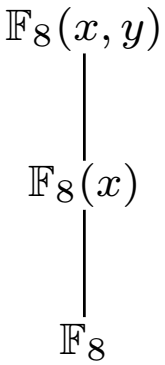
Examples:

i) The rational function field $F := \mathbb{F}_q(x)$ has $g(F) = 0$ and $N(F) = q + 1$.

ii) The algebraic function field $F := \mathbb{F}_8(x, y)$ defined by the equation

$$y^2 + y = \frac{x}{x^2 + x + 1}$$

has $g(F) = 1$ and $N(F) = 4$.



Towers of function fields

A *tower of function fields* over $\mathbb{F}_q$ is a sequence of algebraic function fields $\mathcal{F} = \{F_i\}_{i=0}^{\infty}$ such that

i) $F_i \subsetneq F_{i+1}$ for all $i \geq 0$,

ii) F_{i+1}/F_i is a separable finite extension for all $i \geq 0$,

iii) $\mathbb{F}_q$ is algebraically closed in F_i for all $i \geq 0$, and

iv) there exists F_j with genus greater than one.

Towers of function fields

A *tower of function fields* over $\mathbb{F}_q$ is a sequence of algebraic function fields $\mathcal{F} = \{F_i\}_{i=0}^{\infty}$ such that

i) $F_i \subsetneq F_{i+1}$ for all $i \geq 0$,

ii) F_{i+1}/F_i is a separable finite extension for all $i \geq 0$,

iii) $\mathbb{F}_q$ is algebraically closed in F_i for all $i \geq 0$, and

iv) there exists F_j with genus greater than one.

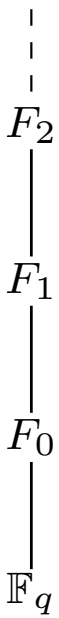


Figure : Sequence of function fields

A tower $\mathcal{F} = \{F_i\}_{i=0}^{\infty}$ over $\mathbb{F}_q$ is called *recursive* if there exist a sequence of transcendental elements $\{x_i\}_{i=0}^{\infty}$ over $\mathbb{F}_q$ and a bivariate polynomial $H(X, Y) \in \mathbb{F}_q[X, Y]$ such that $F_0 = \mathbb{F}_q(x_0)$ and

$$F_{i+1} = F_i(x_{i+1}), \quad \text{where } H(x_i, x_{i+1}) = 0,$$

for all $i \geq 0$.

A tower $\mathcal{F} = \{F_i\}_{i=0}^{\infty}$ over $\mathbb{F}_q$ is called *recursive* if there exist a sequence of transcendental elements $\{x_i\}_{i=0}^{\infty}$ over $\mathbb{F}_q$ and a bivariate polynomial $H(X, Y) \in \mathbb{F}_q[X, Y]$ such that $F_0 = \mathbb{F}_q(x_0)$ and

$$F_{i+1} = F_i(x_{i+1}), \quad \text{where } H(x_i, x_{i+1}) = 0,$$

for all $i \geq 0$.

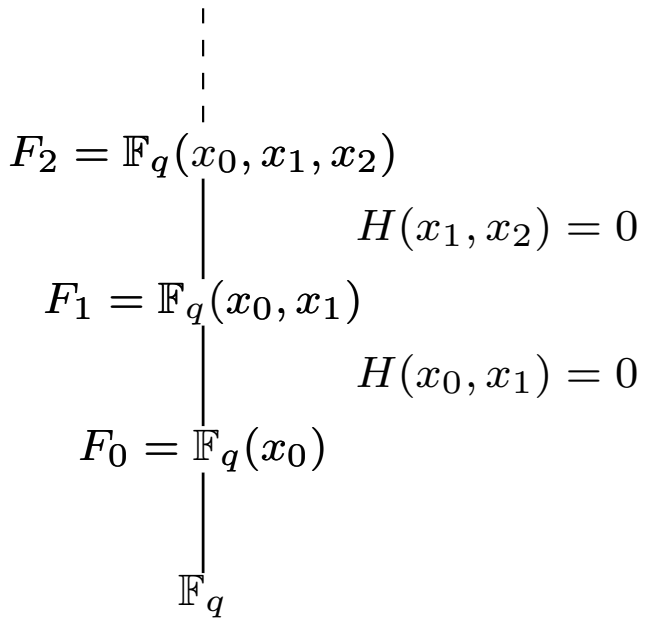


Figure : Recursive tower of function fields

The genus of $\mathcal{F} = \{F_i\}_{i \geq 0}$ over F_0 is defined as

$$\gamma(\mathcal{F}/F_0) := \lim_{i \to \infty} \frac{g(F_i)}{[F_i : F_0]},$$

where $g(F_i)$ is the genus of F_i.

The genus of $\mathcal{F} = \{F_i\}_{i \geq 0}$ over F_0 is defined as

$$\gamma(\mathcal{F}/F_0) := \lim_{i \to \infty} \frac{g(F_i)}{[F_i : F_0]},$$

where $g(F_i)$ is the genus of F_i.

The splitting rate of $\mathcal{F} = \{F_i\}_{i=0}^{\infty}$ over F_0 is defined as

$$\nu(\mathcal{F}/F_0) := \lim_{i \to \infty} \frac{N(F_i)}{[F_i : F_0]},$$

where $N(F_i)$ is the number of rational places of F_i.

The genus of $\mathcal{F} = \{F_i\}_{i \geq 0}$ over F_0 is defined as

$$\gamma(\mathcal{F}/F_0) := \lim_{i \to \infty} \frac{g(F_i)}{[F_i : F_0]},$$

where $g(F_i)$ is the genus of F_i.

The splitting rate of $\mathcal{F} = \{F_i\}_{i=0}^{\infty}$ over F_0 is defined as

$$\nu(\mathcal{F}/F_0) := \lim_{i \to \infty} \frac{N(F_i)}{[F_i : F_0]},$$

where $N(F_i)$ is the number of rational places of F_i.

The limit of $\mathcal{F} = \{F_i\}_{i=0}^{\infty}$ is defined as

$$\lambda(\mathcal{F}) := \lim_{i \to \infty} \frac{N(F_i)}{g(F_i)} = \frac{\nu(\mathcal{F})}{\gamma(F)}$$

The genus of $\mathcal{F} = \{F_i\}_{i \geq 0}$ over F_0 is defined as

$$\gamma(\mathcal{F}/F_0) := \lim_{i \to \infty} \frac{g(F_i)}{[F_i : F_0]},$$

where $g(F_i)$ is the genus of F_i.

The splitting rate of $\mathcal{F} = \{F_i\}_{i=0}^{\infty}$ over F_0 is defined as

$$\nu(\mathcal{F}/F_0) := \lim_{i \to \infty} \frac{N(F_i)}{[F_i : F_0]},$$

where $N(F_i)$ is the number of rational places of F_i.

The limit of $\mathcal{F} = \{F_i\}_{i=0}^{\infty}$ is defined as

$$\lambda(\mathcal{F}) := \lim_{i \to \infty} \frac{N(F_i)}{g(F_i)} = \frac{\nu(\mathcal{F})}{\gamma(F)}$$

$\mathcal{F}$ is *asymptotically good* if $\lambda(\mathcal{F}) > 0$ (equiv. $\nu(\mathcal{F}) > 0$ and $\gamma(\mathcal{F}) < \infty$)

Theorem (Beleen-García-Stichtenoth).

Let $p = char(\mathbb{F}_q)$ and let $\mathcal{F}$ be a tower over $\mathbb{F}_q$ which can be described recursively by the equation $f(y) = g(x)$, with rational functions $f(t), g(t) \in \mathbb{F}_q(t)$ and $\deg(f(t)) = \deg(g(t)) = p$. Let $0 \neq e \in \mathbb{F}_q$ and

$$\mathrm{P}(t) := t^p - e^{p-1}t \in \mathbb{F}_q[t].$$

Suppose that $\mathbb{F}_q(x,y)/\mathbb{F}_q(x)$ and $\mathbb{F}_q(x,y)/\mathbb{F}_q(y)$ are Galois extensions. Then $\mathcal{F}$ can be described by one of the following equations:

$$\mathrm{P}(y) = \begin{cases} \frac{a}{\mathrm{P}(\alpha x)+b} + c & \text{(case 1)} \\ a\,\mathrm{P}(\alpha x) + b & \text{(case 2)} \\ \frac{a}{\mathrm{P}(\alpha/x)+b} + c & \text{(case 3)} \end{cases}$$

with $a, \alpha \in \mathbb{F}_q^*$, $b, c \in \mathbb{F}_q$. In case 1 $\alpha \notin \mathbb{F}_p$ and $a \notin \mathbb{F}_p$ in case 2.

Remark.

Let $\mathcal{F}$ be a tower over $\mathbb{F}_2$ which can be described recursively by the equation

$$f(y) = g(x),$$

where $f(t), g(t) \in \mathbb{F}_2(t)$ are rational functions such that $\deg(f(t)) = \deg(g(t)) = 2$. Then $\mathcal{F}$ can be described by

$$y^2 + y = \frac{1}{(1/x)^2 + (1/x) + b} + c$$

with $b, c \in \mathbb{F}_2$.

b	c	equation	asymptotically
0	0	$y^2+y=\dfrac{x^2}{x+1}$	good over $\mathbb{F}_4$
0	1	$y^2+y=\dfrac{x^2+x+1}{x+1}$	good over $\mathbb{F}_8$
1	0	$y^2+y=\dfrac{x^2}{x^2+x+1}$	good over $\mathbb{F}_8$
1	1	$y^2+y=\dfrac{x+1}{x^2+x+1}$	?

The genus of the tower

Theorem.

Let s be a positive integer. The tower $\mathcal{H} = \{F_i\}_{i=0}^{\infty}$ recursively defined over $\mathbb{F}_{2^s}$ by the equation

$$y^2 + y = \frac{x}{x^2 + x + 1} \tag{1}$$

has finite genus, more precisely

$$\gamma(\mathcal{H}) = \lim_{i \to \infty} \frac{g(F_i)}{2^i} \leq 4$$

The splitting rate of the tower

Theorem.

Consider the tower $\mathcal{H} = \{F_i\}_{i=0}^{\infty}$ over $\mathbb{F}_{2^s}$ with s odd. Then the number of rational places of F_i is $2(|S|+1)$ for all $i \geq 1$ where

$$S = \left\{ \alpha \in \mathbb{F}_{2^s} : \mathrm{Tr}\left(\frac{\alpha}{\alpha^2 + \alpha + 1} \right) = 0 \right\}.$$

The splitting rate of the tower

Theorem.

Consider the tower $\mathcal{H} = \{F_i\}_{i=0}^{\infty}$ over $\mathbb{F}_{2^s}$ with s odd. Then the number of rational places of F_i is $2(|S|+1)$ for all $i \geq 1$ where

$$S = \left\{ \alpha \in \mathbb{F}_{2^s} : \mathrm{Tr}\left(\frac{\alpha}{\alpha^2 + \alpha + 1} \right) = 0 \right\}.$$

Theorem.

The tower $\mathcal{H} = \{F_i\}_{i=0}^{\infty}$ over $\mathbb{F}_{2^s}$, with s odd, has splitting rate zero, i.e.

$$\nu(\mathcal{H}) = \lim_{i \to \infty} \frac{N(F_i)}{2^i} = 0.$$

Lemma (The key lemma)**.**

Let $\theta, \beta \in \mathbb{F}_{2^s}$ with s odd, such that $\theta^2 + \theta = \frac{\beta}{\beta^2+\beta+1}$. Then

$$\mathrm{Tr}\left(\frac{\theta}{\theta^2+\theta+1}\right) \neq \mathrm{Tr}\left(\frac{\theta+1}{\theta^2+\theta+1}\right).$$

Proof.

Suppose that

$$\mathrm{Tr}\left(\frac{\theta}{\theta^2+\theta+1}\right) = \mathrm{Tr}\left(\frac{\theta+1}{\theta^2+\theta+1}\right) \text{ then } \mathrm{Tr}\left(\frac{1}{\theta^2+\theta+1}\right) = 0.$$

Proof.

Suppose that

$$\mathrm{Tr}\left(\frac{\theta}{\theta^2+\theta+1}\right) = \mathrm{Tr}\left(\frac{\theta+1}{\theta^2+\theta+1}\right) \text{ then } \mathrm{Tr}\left(\frac{1}{\theta^2+\theta+1}\right) = 0.$$

On the other hand, by hypothesis $\theta^2+\theta = \frac{\beta}{\beta^2+\beta+1}$ then

$$\frac{1}{\theta^2+\theta+1} = \frac{\beta^2+\beta+1}{\beta^2+1} = 1 + \frac{\beta}{\beta+1} + \left(\frac{\beta}{\beta+1}\right)^2.$$

Proof.

Suppose that

$$\mathrm{Tr}\left(\frac{\theta}{\theta^2+\theta+1}\right) = \mathrm{Tr}\left(\frac{\theta+1}{\theta^2+\theta+1}\right) \text{ then } \mathrm{Tr}\left(\frac{1}{\theta^2+\theta+1}\right) = 0.$$

On the other hand, by hypothesis $\theta^2+\theta = \frac{\beta}{\beta^2+\beta+1}$ then

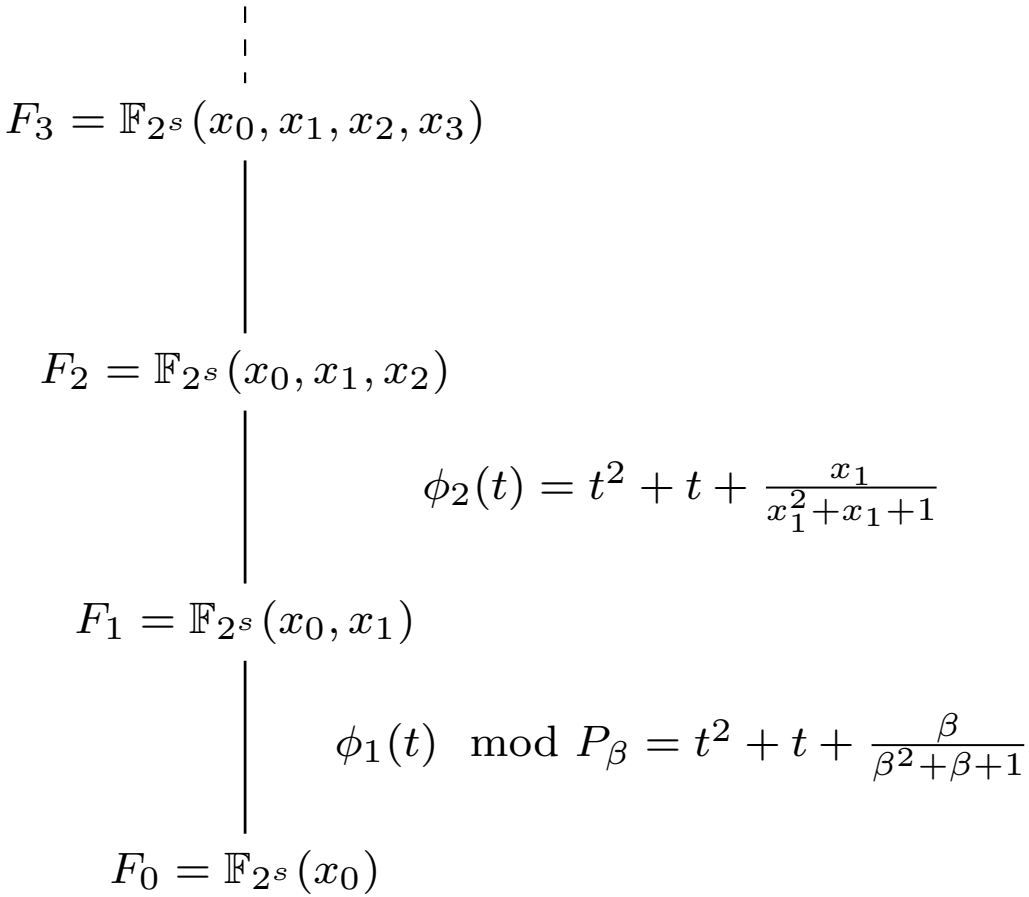
$$\frac{1}{\theta^2+\theta+1} = \frac{\beta^2+\beta+1}{\beta^2+1} = 1 + \frac{\beta}{\beta+1} + \left(\frac{\beta}{\beta+1}\right)^2.$$

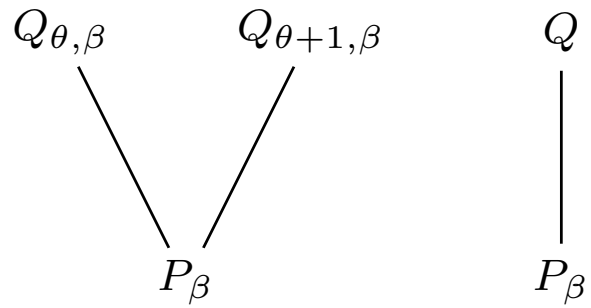
Finally, since $\mathrm{Tr}(1) = 1$ and $\mathrm{Tr}(\alpha) = \mathrm{Tr}(\alpha^2)$ for all $\alpha \in \mathbb{F}_{2^s}$, we have

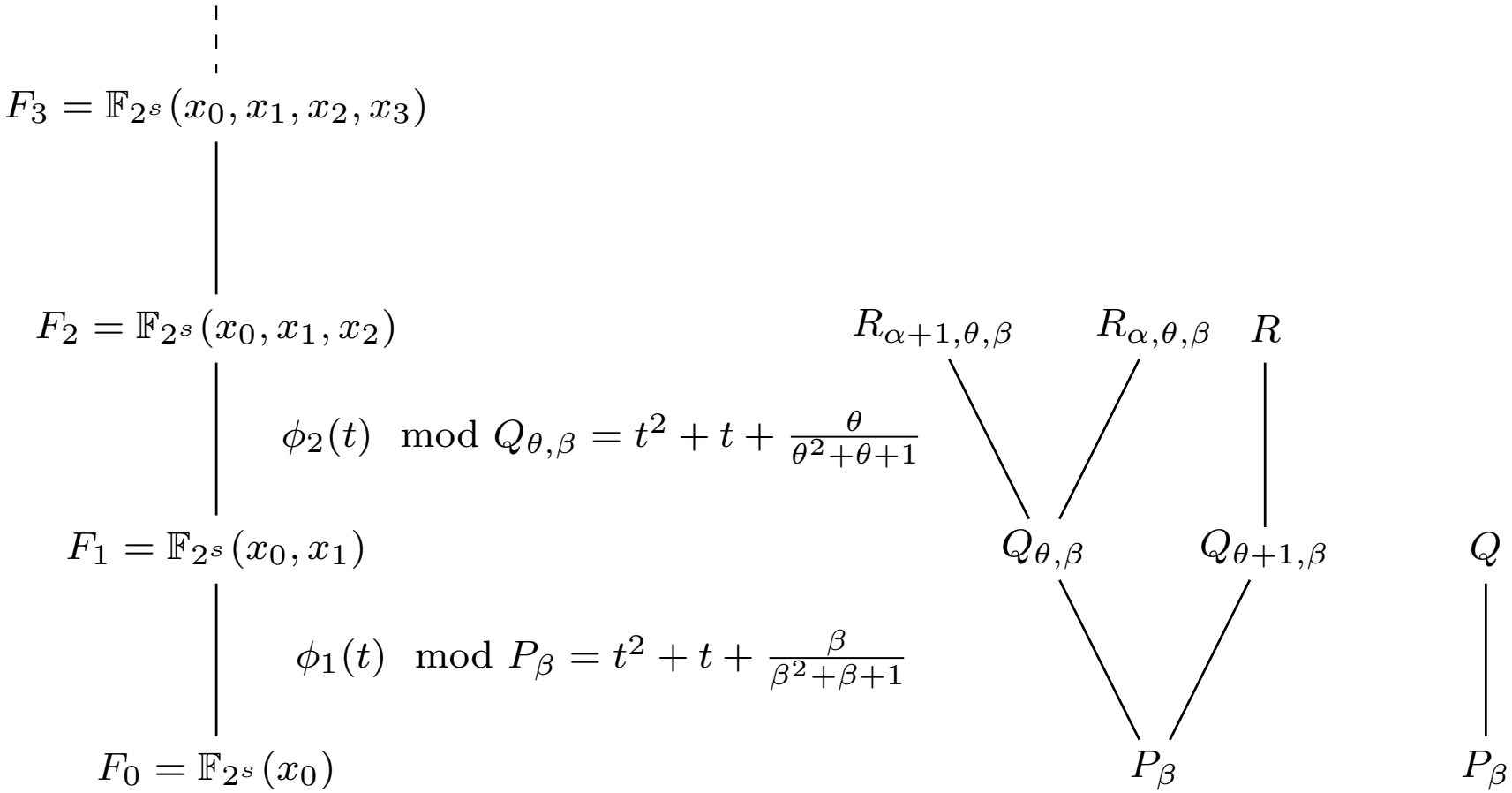
$$\mathrm{Tr}\left(\frac{1}{\theta^2+\theta+1}\right) = \mathrm{Tr}(1) + \mathrm{Tr}\left(\frac{\beta}{\beta+1}\right) + \mathrm{Tr}\left(\left(\frac{\beta}{\beta+1}\right)^2\right) = 1,$$

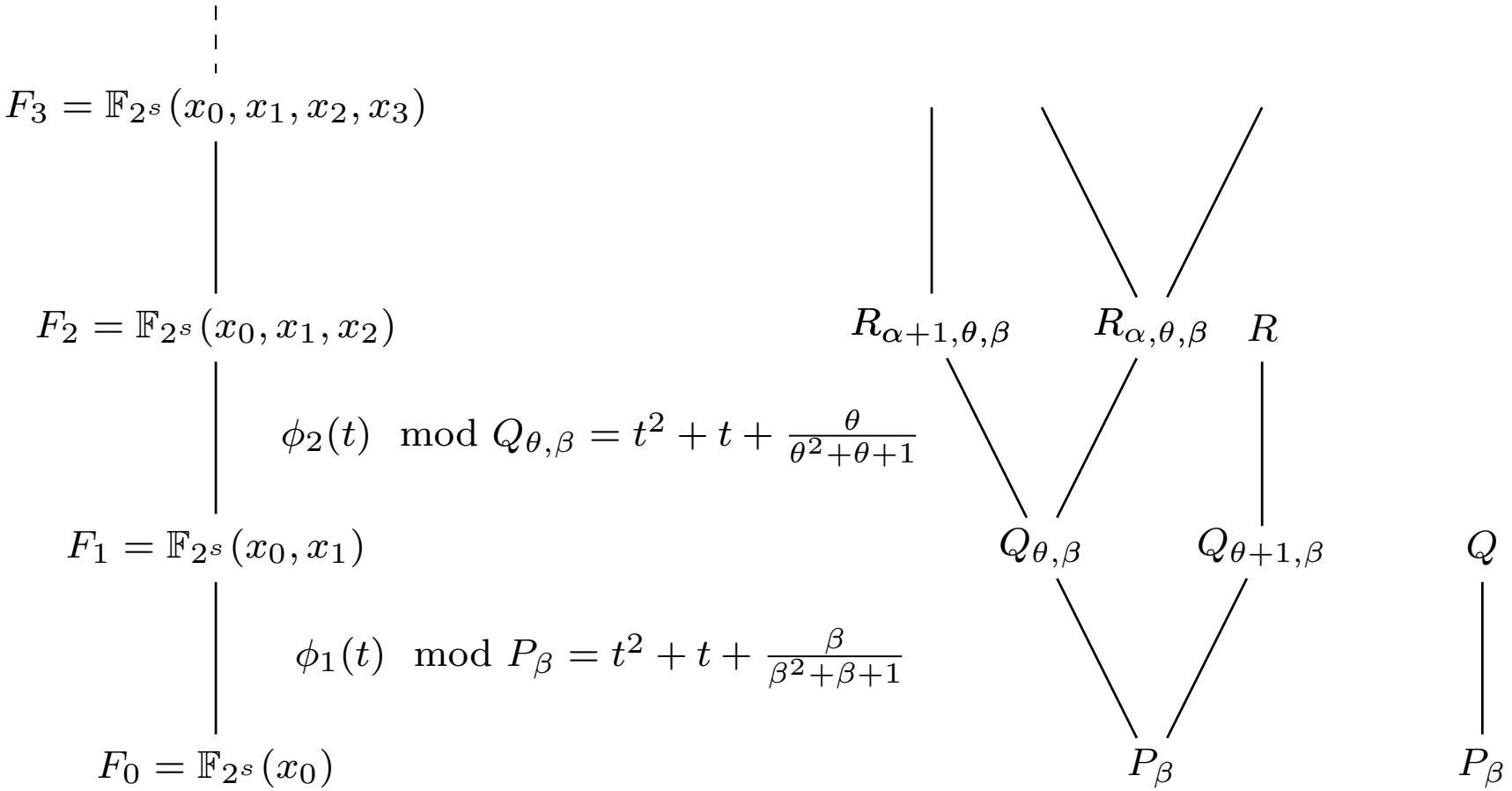
a contradiction.

$$
\begin{array}{l}
\vdots \\
F_3 = \mathbb{F}_{2^s}(x_0, x_1, x_2, x_3) \\
\Big| \\
F_2 = \mathbb{F}_{2^s}(x_0, x_1, x_2) \qquad \phi_2(t) = t^2 + t + \frac{x_1}{x_1^2 + x_1 + 1} \\
\Big| \\
F_1 = \mathbb{F}_{2^s}(x_0, x_1) \qquad \phi_1(t) = t^2 + t + \frac{x_0}{x_0^2 + x_0 + 1} \\
\Big| \\
F_0 = \mathbb{F}_{2^s}(x_0)
\end{array}
$$


$F_3 = \mathbb{F}_{2^s}(x_0, x_1, x_2, x_3)$
$F_2 = \mathbb{F}_{2^s}(x_0, x_1, x_2)$
$\phi_2(t) = t^2 + t + \frac{x_1}{x_1^2+x_1+1}$
$F_1 = \mathbb{F}_{2^s}(x_0, x_1)$
$\phi_1(t) \mod P_\beta = t^2 + t + \frac{\beta}{\beta^2+\beta+1}$
$F_0 = \mathbb{F}_{2^s}(x_0)$


$Q_{\theta,\beta}$
$Q_{\theta+1,\beta}$
P_β
Q
P_β


$F_3 = \mathbb{F}_{2^s}(x_0, x_1, x_2, x_3)$
$F_2 = \mathbb{F}_{2^s}(x_0, x_1, x_2)$
$\phi_2(t) \mod Q_{\theta,\beta} = t^2 + t + \frac{\theta}{\theta^2+\theta+1}$
$F_1 = \mathbb{F}_{2^s}(x_0, x_1)$
$\phi_1(t) \mod P_\beta = t^2 + t + \frac{\beta}{\beta^2+\beta+1}$
$F_0 = \mathbb{F}_{2^s}(x_0)$
$R_{\alpha+1,\theta,\beta}$
$R_{\alpha,\theta,\beta}$
R
$Q_{\theta,\beta}$
$Q_{\theta+1,\beta}$
Q
P_β
P_β


$F_3 = \mathbb{F}_{2^s}(x_0, x_1, x_2, x_3)$
$F_2 = \mathbb{F}_{2^s}(x_0, x_1, x_2)$
$\phi_2(t) \mod Q_{\theta,\beta} = t^2 + t + \frac{\theta}{\theta^2+\theta+1}$
$F_1 = \mathbb{F}_{2^s}(x_0, x_1)$
$\phi_1(t) \mod P_\beta = t^2 + t + \frac{\beta}{\beta^2+\beta+1}$
$F_0 = \mathbb{F}_{2^s}(x_0)$
$R_{\alpha+1,\theta,\beta}$
$R_{\alpha,\theta,\beta}$
R
$Q_{\theta,\beta}$
$Q_{\theta+1,\beta}$
Q
P_β
P_β


M. Chara, H. Navarro and R. Toledano.
A problem of Beelen, Garcia and Stichtenoth on an Artin-Schreier tower in characteristic 2.
Preprint.


P. Beelen, A. Garcia and H. Stichtenoth.
Towards a classification of recursive towers of function fields over finite fields.
Finite Fields Appl, 12(1):56–77, 2006.


H. Stichtenoth.
Algebraic function fields and codes, volume 254 of *Graduate Texts in Mathematics*.
Springer-Verlag, Berlin, second edition, 2009.


G. van der Geer and M. van der Vlugt.
An asymptotically good tower of curves over the field with eight elements.
Bull. London Math. Soc., 34(3):291–300, 2002.