A Graph Aided Strategy to Produce Good Recursive Towers over Finite Fields

Emmanuel Hallouin, Marc Perret

A Graph Aided Strategy to Produce Good Recursive Towers over Finite Fields

Emmanuel Hallouin & Marc Perret*

March 23, 2015

Abstract

We propose a systematic method to produce potentially good recursive towers over finite fields. The graph point of view, so as some `magma` and `sage` computations are used in this process. We also establish some theoretical functional criterion ensuring the existence of many rational points on a recursive tower. Both points are illustrated on an example, from the production process, to the theoretical study, using this functional criterion, of the parameters of the obtained potentially good tower.

Contents

Introduction

The search of *explicit* examples of sequences of algebraic curves over a given finite field, of genus growing to infinity and having as much as possible rational points with regard to their genera became more and more important not only for its own, but also for several uses such as coding theory and cryptography (Garcia and Stichtenoth [GS07]) or for multiplication algorithms over

*Institut de Mathématiques de Toulouse, UMR 5219

finite fields (Ballet [Bal03]). For quite a long time, only modular examples were known for square size of the finite field (Tsfasmann-Vladut-Zink [TVZ82] and Ihara [Iha81, "The general case", p. 723]), and only examples coming from class field theory were known for non square size. Unfortunately, these examples were not explicit.

In 1995 appeared the important Garcia-Stichtenoth's paper [GS95] in which the very first explicit example was given. The explicitness comes from the recursive definition of each floor of the tower; such towers are now called *recursive towers*. Since then, several authors gave many examples of recursive towers (see Garcia and Stichtenoth's survey [GS07] or Li's one [Li10]). Two features appear at a look at the literature. First, the authors never explain how they where able to guess their examples. Second, once the explicit tower is given, there is always some difficulty in its study. Either the genus sequence is hard to compute (usually in the wildly ramified case), either the existence of many rational points is hard to prove (usually in the moderately ramified case). For instance, in the particularly interesting example of Garcia-Sitchtenoth moderately ramified tower recursively defined by the equation $y^2 = \frac{x^2+1}{2x}$, the proof of the splitting behavior is quite mysteriously related to some functional equation satisfied by the well known Deuring polynomial[1].

Apart from our previous article [HP14], the present work joins in the continuation of Lenstra's and Beelen's one [Len02, Bee04]. A kind of non-existence result is proved by Lenstra [Len02] over prime finite fields for a very particular type of recursive towers. The proof is technical and quite intricate, at least for the authors of the present paper. A somehow understandable point is that it relies upon some *functional equation* labeled as (5) therein and whose meaning is explained in a concluding remark. Beelen proved soon after that the characteristic function of a totally splitting set has to fulfill some functional equation in case of separable variable correspondances on the projective line [Bee04, Theorem 3.2]. Beelen also proves, in a second part of his paper, that such a functional equation can have at most one solution for a special type of recursive tower, he called *of type A*. This second part has already been generalized by the authors [HP14].

In Section 1, we recall some backgrounds about recursive towers. Geometrically, the definition only requires a base curve X and a correspondence $\Gamma \subset X \times X$. In this article we focus on the special case of recursive towers with *separable variables*[2], where the correspondence is given by two morphisms $f, g : X \to X_0$. One of the main tool for the study of a recursive tower is an associated graph $\mathcal{G}_\infty(X, \Gamma)$. This graph has already been introduced by Beelen [Bee04] with a slightly different definition, and has been extensively used by the authors [HP14]. Many features of the tower can be directly read on the graph. In particular, the existence of some kind of finite component, the *d-regular* ones, is related to the existence of sets of points of the base curve splitting totally in the tower. Following Beelen (loc. cit.), this leads to introduce the weaker notion of *completeness* for subset of $X(\overline{\mathbb{F}_q})$. The importance of completeness comes from Proposition 6, that the search for a splitting set in a tower is carried out if one knows the ramification loci of f and g, an easy task, and if one can find complete sets, an harder task.

In section 2, we push further the understanding of the functional equation and its connection with the existence of many rational points in the tower. Theorem 9 asserts essentially that a finite set of points of the base curve splits totally in the tower if and only if the characteristic function of its support satisfies some functional equation. Beyond the fact that we do not need to assume the base curve to be the projective line, the contribution of Section 2 compared to Beelen's one is at first that while he proved that the functional equation is a *necessary* condition for *completeness*, we prove here that it is in fact a necessary and *sufficient* conditions for *regularness*. Next, that

[1] This is the characteristic polynomial of supersingular invariants in characteristic p.

[2] In a forthcoming paper, we intend to prove that one can always reduce the study of a general recursive tower to the study of a recursive tower with separable variables.

the precise form of the functional equation can be easily read from the singular graph of the tower. The sufficiency is of great importance for the applications given in the following of the present article.

We think that Theorem 9 is interesting in both theoretical and algorithmic study of recursive towers. In section 3, we give several applications that may convince the reader.

On the theoretical side, we deduce Theorem 10 from Theorem 9, extending one of the two main results in [HP14].

On the explicit side, we give two applications of the functional equation. Both use also the graph theoretic approach of recursive towers. In Section 3.2, we explain how the mysterious functional equation needed in [GSR03] to prove the splitting behavior of some base points can in fact been deduced from the initial data $y^2 = \frac{x^2+1}{2x}$.

Then, in Section 3.3, we describe our main application of the functional equation. It consists in a systematic method to produce some potentially good recursive towers (Section 3.3.1) and in original methods to compute the asymptotic parameters of the tower. These methods use jointly the graph approach, some `magma` and `sage` computations, and Theorem 9 (Sections 3.3.2 & 3.3.3). All these ideas are illustrated on a concrete example. An interesting feature of this example is the following. The reader will be convinced that no modular tool is used in its production. However, the tower turns to be modular (Proposition 18). This can be seen as another experimental evidence toward Elkies' modularity conjecture[3] that any tame good recursive tower over a square finite field should be modular!

1 Preliminary notations and background

We recall the definition of a recursive tower and of its principal parameters, and we associate a graph to a recursive tower, as in our previous work [HP14]. Some of the results of this article are also included.

1.1 Recursive towers

Let X be a smooth projective absolutely irreducible curve defined over the finite field $\mathbb{F}_q$ and let $\Gamma \subset X \times X$ be an irreducible correspondence, without no vertical nor horizontal component. The *singular recursive tower* $\mathcal{T}(X,\Gamma) = (X_n)_{n\geq 1}$ is defined, for $n \geq 1$, by

$$X_n = \{(P_1, P_2, \cdots, P_n) \in X^n \mid (P_i, P_{i+1}) \in \Gamma \text{ for each } i = 1, 2, \ldots, n-1\}.$$

In this article, we restrict ourselves to correspondences with **separable variables**, that is of the form

$$\Gamma = \Gamma_{f,g} = \{(P,Q) \in X \times X; f(P) = g(Q)\}, \tag{1}$$

where $f, g : X \to X_0$ are two degree d maps from X to a given smooth base curve X_0.

The curves X_n may be singular and by desingularization process, we obtain the *smooth recursive tower* $\widetilde{\mathcal{T}}(X,\Gamma) = (\widetilde{X}_n)_{n\geq 1}$. The interesting parameters of the towers are:

- the *arithmetic genus* of X_n, $\gamma_n = \gamma(X_n)$;
- the *geometric genus* of X_n, i.e. the *genus* of $\widetilde{X}_n$, $g_n = g(X_n) = g(\widetilde{X}_n)$;
- the number of rational points over $\mathbb{F}_{q^r}$ for $r \geq 1$, $N_r(\widetilde{X}_n) = \sharp \widetilde{X}_n(\mathbb{F}_{q^r})$;

[3] Or Elkies' fantasia, as Elkies himself stated it in [Elk01].

- last, the limit

$$\lambda_r(\mathcal{T}) = \lim_{n\to+\infty} \frac{N_r(\widetilde{X}_n)}{g_n}.$$

For a recursive tower, this limit always exists and is thus a non negative number. The tower is said to be *asymptotically good* if it is non-zero for some $r \geq 1$. This happens (see Lemma 1 in [HP14] for instance) if and only if there exist some $c, c' > 0$ such that

$$g_n = c \times d^n + o(d^n) \qquad \text{and} \qquad N_r(\widetilde{X}_n) = c' \times d^n + o(d^n). \tag{2}$$

1.2 Graphs and Recursive towers

To each recursive tower, one can associate a directed graph.

Definition 1. *Let $\mathcal{T}(X,\Gamma)$ be a recursive tower, where Γ is associated, via (1), to the functions $f, g : X \to X_0$.*

*(i) The **geometric graph** $\mathcal{G}_\infty(X,\Gamma)$ is the graph whose vertices are the geometric points of X, and for which there is an oriented edge from $P \in X(\overline{\mathbb{F}_q})$ to $Q \in X(\overline{\mathbb{F}_q})$ if $(P,Q) \in \Gamma(\overline{\mathbb{F}_q})$, that is if $f(P) = g(Q)$.*

(ii) For $S \subset X(\overline{\mathbb{F}_q})$, the S-graph $\mathcal{G}_S(X,\Gamma)$ is the subgraph of $\mathcal{G}_\infty(X,\Gamma)$ whose vertices are the points of S.

*(iii) The r-th **arithmetic graph** $\mathcal{G}_r(X,\Gamma)$ is the $X(\mathbb{F}_{q^r})$-graph.*

*(iv) The **singular graph** is the union of the weakly connected components containing a (directed) path joining a ramified point of f to a ramified point of g.*

The adjectives geometric, arithmetic, or singular, qualifying the different graphs come from the following correspondence between the points of tower and the paths in the graphs (see [HP14, Section 3.2]).

Proposition 2. *Let $\mathcal{T}(X,\Gamma)$ be a recursive tower, where Γ is associated, via (1), to the functions $f, g : X \to X_0$. There is a one-to-one correspondence between*

$$\{\text{paths of } \mathcal{G}_\infty(X,\Gamma) \text{ of length } n-1\} \longleftrightarrow X_n(\overline{\mathbb{F}_q}).$$

This correspondence:

(i) restricts to a one-to-one correspondence between $X_n(\mathbb{F}_{q^r})$ and the set of paths of length $(n-1)$ of the r-th arithmetic graph $\mathcal{G}_r(X,\Gamma)$;

(ii) is such that a path corresponds to a singular point of X_n if and only if it joins a ramified point of f to a ramified point of g.

At any point outside the ramification loci of f and g, the in and out degrees in the geometric graph are equal to the common degree d of both morphisms f, g, and only points that are ramified by f or g have in or out degrees less than d. The following definition is of importance in this article because of the following alternative which follows from (2) and [HP14, Proposition 21].

Definition 3. *A finite subset $S \subset X(\overline{\mathbb{F}_q})$ is said to be d-**regular** if the S-graph $\mathcal{G}_S(X,\Gamma)$ is a d-regular graph that is if any vertex has in and out degrees equal to d.*

Proposition 4. *Let $\mathcal{T}(X,\Gamma)$ be a recursive tower, where Γ is associated, via (1), to the functions $f,g : X \to X_0$ of degree d. Then the tower $\mathcal{T}(X,\Gamma)$ is asymptotically good over $\mathbb{F}_{q^r}$ if and only if there exists some $c>0$, such that $g_n = c\times d^n + o(d^n)$, and*

(i) either the number of points of $\widetilde{X}_n$, defined over $\mathbb{F}_{q^r}$, coming from the desingularization of the singular component of $\mathcal{G}_r(X,\Gamma)$ has asymptotic behaviour of the form to $c'\times d^n + o(d^n)$ for some $c'>0$;

(ii) or there exists a finite d-regular set inside the r-th arithmetic graph $\mathcal{G}_r(X,\Gamma)$.

See loc. cit. for details, but notice that if there exists a d-regular finite subset $S \subset X(\mathbb{F}_{q^r})$ for some $r \geq 1$, then the number of paths of length $(n-1)$ of this component is clearly $\sharp S \times d^n$. By Proposition 2, these paths are in one-to-one correspondence with smooth points of X_n defined over $\mathbb{F}_{q^r}$. Therefore the number of points of $\widetilde{X}_n$ satisfies the last condition in Proposition 4 and the tower is asymptotically good, provided that the genus sequence do not grows too fast as required also as a first condition in Proposition 4. Note that geometrically, the vertices/points of S are nothing else than the totally split points in the tower.

One of the main result of our previous work [HP14] says that there exists at most one finite d-regular set. But there may exist other interesting finite subsets satisfying a weaker property than regularness which turns to be useful to give characterizations of d-regular set.

Definition 5. *Let X and X_0 be two smooth, projective, absolutely irreducible curves over $\mathbb{F}_q$ and let $f : X \to X_0$, $g : X \to X_0$ be two morphisms of degree d. A subset S of $X(\overline{\mathbb{F}_q})$ is said to be:*

*(i) **forward complete** if $g^{-1}(f(S)) \subset S$;*

*(ii) **backward complete** if $f^{-1}(g(S)) \subset S$;*

*(iii) **complete** if it is both backward and forward complete.*

For $S \subset X(\overline{\mathbb{F}_q})$ a finite subset, if the graph $\mathcal{G}_S(X,\Gamma)$ is d-regular, then S is complete. The converse is false, but one easily see that the following Proposition holds.

Proposition 6. *Let $\mathcal{T}(X,\Gamma)$ be a recursive tower, where Γ is associated, via (1), to the morphisms $f,g : X \to X_0$ and let S be a subset of $X(\overline{\mathbb{F}_q})$. Then S is d-regular if and only if S is complete and outside the ramification loci of f and g. If this is the case, then any point of S splits totally in the tower.*

2 Completeness and regularness criteria

We build successively in this section three characterizations of complete and of regular sets. The first one is a basic set theoretic criterion for completeness, the second one is a divisorial criterion for completeness, and the last one is a functional equation characterizing, once a first *complete* finite set is known, if another given finite set is *d-regular*.

2.1 A divisorial criterion for completeness

Lemma 7 (Set theoretical completeness criterion)**.** *A subset $S \subset X(\overline{\mathbb{F}_q})$ is complete if and only if there exists $S_0 \subset X_0(\overline{\mathbb{F}_q})$ such that $S = f^{-1}(S_0) = g^{-1}(S_0)$.*

Proof — Suppose that S is complete. First we prove that $f(S) = g(S)$. Let $P \in S$. There exists some $Q \in X(\overline{\mathbb{F}_q})$ such that $f(P) = g(Q)$. By forward completeness, one has $Q \in S$. This leads to $f(S) \subset g(S)$, and the reverse inclusion is proved the same way using backward completeness. Put $S_0 = f(S) = g(S)$ and let us prove that $S = f^{-1}(S_0) = g^{-1}(S_0)$. Of course $S \subset f^{-1}(S_0) = f^{-1}(f(S))$. Conversely, if $P \in f^{-1}(S_0)$ then $f(P) \in S_0 = g(S)$, that is $f(P) = g(Q)$ for some $Q \in S$. By backward completeness, we deduce that $P \in S$ and that $f^{-1}(S_0) \subset S$. The proof of the converse works also in the same way. □

For the remaining characterizations, we need to introduce the following notations.

- For $S \subset X(\overline{\mathbb{F}_q})$, we put $\operatorname{div}(S) = \sum_{P \in S} P$ and for $\varphi \in \mathbb{F}_q(X)$, we denote by $\operatorname{div}(\varphi)$ the associated divisor.
- For $P \in X(\overline{\mathbb{F}_q})$ we denote by $e_f(P)$ the **ramification index** of P by f.
- For $S_0 \subset X_0(\overline{\mathbb{F}_q})$, let
$$\mathfrak{D}_f(S_0) = \sum_{P \in f^{-1}(S_0)} (e_f(P) - 1)\, P$$
be the **restricted different** divisor of f.

Under these notations, if S_0 is a subset of $X_0(\overline{\mathbb{F}_q})$, one can point out the useful divisorial equalities

$$f^* \operatorname{div}(S_0) = \mathfrak{D}_f(S_0) + \operatorname{div}\left(f^{-1}(S_0)\right) \qquad \text{and} \qquad g^* \operatorname{div}(S_0) = \mathfrak{D}_g(S_0) + \operatorname{div}\left(g^{-1}(S_0)\right). \tag{3}$$

We can then state the following, a generalization of Lenstra's identity.

Proposition 8 (Divisorial completeness criterion)**.** *Let S_0 be a finite subset of $X_0(\overline{\mathbb{F}_q})$. The following assertions are equivalent.*

(i) *The set $f^{-1}(S_0)$ is complete.*

(ii) *The set $g^{-1}(S_0)$ is complete.*

(iii) $f^* \operatorname{div}(S_0) - g^* \operatorname{div}(S_0) = \mathfrak{D}_f(S_0) - \mathfrak{D}_g(S_0)$.

Proof — This is a direct consequence of (3) together with the set theoretical completeness criterion (Lemma 7). □

2.2 A functional criterion for regularness

From this section, and for the rest of this article, given a curve X defined over $\mathbb{F}_q$ and $f, g \in \mathbb{F}_q(X)$, we write $f \sim g$ if $\operatorname{div}(f) = \operatorname{div}(g)$ in $\operatorname{div}(X)$, that is if there exists a constant $c \in \mathbb{F}_q^*$ such that $f = cg$.

The characterizations of completeness given in Lemma 7 and Proposition 8 are not always sufficiently effective in practice. The most fruitful characterization is the following functional regularness characterization.

Theorem 9 (functional regularness criterion)**.** *Let Γ be a correspondence induced by $f, g : X \to X_0$ as in (1). Let $S = f^{-1}(S_0) = g^{-1}(S_0)$ be a complete subset of $X(\overline{\mathbb{F}_q})$. Let b be the order of the degree zero divisor $\mathfrak{D}_f(S_0) - \mathfrak{D}_g(S_0)$ in the jacobian $\operatorname{Jac}(X)$, and let $\rho \in \mathbb{F}_q(X)$ be a function such that $\operatorname{div}(\rho) = b(\mathfrak{D}_f(S_0) - \mathfrak{D}_g(S_0))$. Let T_0 be a finite subset of $X_0(\overline{\mathbb{F}_q})$, disjoint from the ramification locus of g. Let $s, t \in \mathbb{N}^*$ be such that $t \sharp S_0 = s \sharp T_0$, let a be the order of*

the degree zero divisor $s\operatorname{div}(T_0) - t\operatorname{div}(S_0)$ *in* $\mathrm{Jac}(X_0)$*, and let* $\varphi \in \mathbb{F}_q(X_0)$ *be a function such that* $\operatorname{div}(\varphi) = a\,(s\operatorname{div}(T_0) - t\operatorname{div}(S_0))$.

Then the functional equation

$$\rho^{ta} \times (\varphi \circ f)^b \sim (\varphi \circ g)^b \tag{4}$$

holds in $\mathbb{F}_q(X_0)$ *if and only if* $f^{-1}(T_0)$ *is* d*-regular.*

> **Remark** – In most instances[4], the singular graph turns to be finite and complete. It is then fruitful to choose S to be this singular graph, see Sections 3.2 and 3.3.3.

Proof — The divisors of the functions $\varphi \circ f$ and $\varphi \circ g$ on X are

$$\operatorname{div}(\varphi \circ f) = a\,(sf^*\operatorname{div}(T_0) - tf^*\operatorname{div}(S_0)) \qquad \text{and} \qquad \operatorname{div}(\varphi \circ g) = a\,(sg^*\operatorname{div}(T_0) - tg^*\operatorname{div}(S_0))\,,$$

so that by difference

$$\operatorname{div}(\varphi \circ f) - \operatorname{div}(\varphi \circ g) = as\,(f^*\operatorname{div}(T_0) - g^*\operatorname{div}(T_0)) - at\,(f^*\operatorname{div}(S_0) - g^*\operatorname{div}(S_0))\,. \tag{5}$$

Since S is complete, it follows by the divisorial completeness criterion (Proposition 8) that $f^*\operatorname{div}(S_0) - g^*\operatorname{div}(S_0) = \mathfrak{D}_f(S_0) - \mathfrak{D}_g(S_0)$. Since none of the points of T_0 are ramified by g, we have $\mathfrak{D}_g(T_0) = 0$, hence (3) reduces to $f^*\operatorname{div}(T_0) - g^*\operatorname{div}(T_0) = \operatorname{div}\left(f^{-1}(T_0)\right) + \mathfrak{D}_f(T_0) - \operatorname{div}\left(g^{-1}(T_0)\right)$. Multiplying by b and taking $\operatorname{div}(\rho^{ta})$ into account, equation (5) becomes

$$b\,[\operatorname{div}(\varphi \circ f) - \operatorname{div}(\varphi \circ g)] + ta\operatorname{div}(\rho) = abs\left[\operatorname{div}\left(f^{-1}(T_0)\right) + \mathfrak{D}_f(T_0) - \operatorname{div}\left(g^{-1}(T_0)\right)\right].$$

It follows that the functional equation (4) holds if and only if

$$\operatorname{div}\left(f^{-1}(T_0)\right) + \mathfrak{D}_f(T_0) = \operatorname{div}\left(g^{-1}(T_0)\right). \tag{6}$$

Suppose that the functional equation (4), or equivalently that (6) do holds. Since the effective divisor $\operatorname{div}\left(g^{-1}(T_0)\right)$ is reduced, the effective divisor $\operatorname{div}\left(f^{-1}(T_0)\right) + \mathfrak{D}_f(T_0)$ is also reduced. Moreover, the support of the divisor $\mathfrak{D}_f(T_0)$ is contained in the support of $\operatorname{div}\left(f^{-1}(T_0)\right)$, hence we can deduce that $\mathfrak{D}_f(T_0) = 0$, that is T_0 is outside the ramification locus of f. Furthermore, (6) becomes

$$\operatorname{div}\left(f^{-1}(T_0)\right) = \operatorname{div}\left(g^{-1}(T_0)\right),$$

meaning that $f^{-1}(T_0)$ is complete by the set theoretical completeness criterion Lemma 7. It follows that $f^{-1}(T_0)$ is d-regular by Proposition 6. Conversely, suppose that that $f^{-1}(T_0)$ is d-regular, so that T_0 is disjoint from the ramification locus of f and $f^{-1}(T_0)$ is complete by Proposition 6. Then $\mathfrak{D}_f(T_0) = 0$, and by the set theoretical completeness criterion, we have $\operatorname{div}\left(f^{-1}(T_0)\right) = \operatorname{div}\left(g^{-1}(T_0)\right)$, so that (6), hence the functional equation (4), holds true. □

3 Applications

3.1 Non existence of totally splitting sets for some recursive towers

We deduce from the functional regularness criterion the following Theorem, extending the main result of [HP14].

[4] We will prove in a forthcoming paper that the singular graph is *not* finite for the recursive tower $X_0(\mathcal{P}_2^n)$ over $\mathbb{Q}(\sqrt{3})$, whose explicit recursive equation is given in [Elk01, equations (47) and (48)].

Theorem 10. *Let $\mathcal{T}(X,\Gamma)$ be a recursive tower, where Γ is associated, via (1), to the morphisms $f,g : X \to X_0$ of degree d. Suppose that the tower is irreducible, and that there exists a complete set S such that $\mathfrak{D}_f(S_0) = \mathfrak{D}_g(S_0)$ for $S_0 = f(S) = g(S)$. Then the graph do not contains any non-empty finite d-regular component T disjoint to S.*

> **Remark** – A d-regular set S satisfies $\mathfrak{D}_f(S_0) = \sum_{P\in S} P = \mathfrak{D}_g(S_0)$, so that this statement contains Theorem 19 of [HP14] in case of correspondences with separable variables. This Theorem also contains the case of a complete loop at a point P (for instance for type A towers in Bellen's [Bee04] and in [Len02]), in which case we have $S = \{P\}$, $S_0 = \{f(P_0)\}$ and $\mathfrak{D}_f(S_0) = (d-1)P = \mathfrak{D}_g(S_0)$.

Proof — Suppose by contradiction that there do exist a finite d-regular component T and let $T_0 = f(T) = g(T)$. Since $\mathcal{G}_T(X,\Gamma)$ is assumed to be d-regular, each vertex of T is unramified by f and g. One can apply the functional regularness criterion (Theorem 9) to S_0 and T_0. Since by assumption $\mathfrak{D}_f(S_0) - \mathfrak{D}_g(S_0) = 0$, we have $b = 1$ and one can choose $\rho = 1$. We denote by a the order, in $\mathrm{Jac}(X_0)$, of the zero degree divisor $\sharp S_0 \operatorname{div}(T_0) - \sharp T_0 \operatorname{div}(S_0)$, and we consider $\varphi \in \mathbb{F}_q(X_0)$ such that $\operatorname{div}(\varphi) = a(\sharp S_0 \operatorname{div}(T_0) - \sharp T_0 \operatorname{div}(S_0))$. By the functional regularness criterion (Theorem 9), there exists some $c \in \overline{\mathbb{F}_q}^*$ such that

$$\varphi \circ g = c \times \varphi \circ f.$$

For any $Q, R \in X(\overline{\mathbb{F}_q})$ such that $f(Q) = g(R)$, we deduce that

$$\varphi \circ f(Q) = \varphi \circ g(R) = c \times \varphi \circ f(R).$$

Therefore, if Q is any vertex of $\mathcal{G}_\infty(X,\Gamma)$, then $\varphi \circ f$ takes values in $c^{\mathbb{Z}} \times \varphi \circ f(Q)$ on the vertices in the connected component of Q. But this set of values is finite since $c \in \overline{\mathbb{F}_q}^*$. Hence, the function $\varphi \circ f$ takes only finitely many values on each given connected component. Since $\varphi \circ f$ is a finite morphism, every connected components is thus finite. Now, the graph $\mathcal{G}_\infty(X,\Gamma)$ being infinite and since since there are only finitely many ramified points by f or g, it must have infinitely many finite d-regular components by Proposition 6, a contradiction with Theorem 19 in [HP14] that under the irreducibility assumption, the graph contains at most one d-regular component. □

3.2 Understanding the splitting set of the optimal tower $y^2 = \frac{x^2+1}{2x}$

For some known Garcia-Stichtenoth recursive towers, especially for the tame one, it is quite difficult to prove that some set of places splits totally in the tower. Suppose that the base curve is $\mathbb{P}^1$ (which is the case for all known explicit examples) whose Jacobian is trivial. Once the characteristic function of the involved points on $\mathbb{P}^1$ is guessed (we explain in Subsection 3.3 how it can be guessed on an example), the functional regularness criterion Theorem 9 is the good tool to prove that they do split in the tower. Let us illustrate this on the example of the moderate tower $\mathcal{T}\left(\mathbb{P}^1, y^2 = \frac{x^2+1}{2x}\right)$, studied for instance in [GSR03] and well known to be optimal. The genus computation being not difficult in this case, the hard point is the existence of some totally splitting locus. Let H be the Deuring polynomial over $\mathbb{F}_p$, whose simple roots are supersingular j-invariants in characteristic p. The splitting behaviour of some set closely related to the zero set of H is easily deduced by Garcia and Stichtenoth from the functional equation

$$H(x^4) = x^{p-1} H\left(\left(\frac{x^2+1}{2x}\right)^2\right), \tag{7}$$

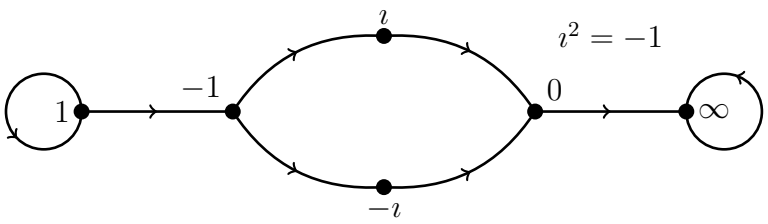


Figure 1: The singular component of $\mathcal{T}\left(\mathbb{P}^1, \frac{x^2+1}{2x} = y^2\right)$ over $\mathbb{F}_{p^2}$

which seems to be pulled out of the hat! We explain in this subsection that taking into account the singular part of the graph, this is nothing but the functional equation (4) requested in the functional regularness criterion (Theorem 9) for the characteristic function of some splitting set!

Let $h(x) = \prod_{P\in T_0}(x - x(P)) \in \mathbb{F}_q[x]$ be the characteristic polynomial of any finite set $T_0 \subset \mathbb{P}^1 \setminus \{\infty\}$ outside the ramification locus $\{0, \infty\}$ of $g(y) = y^2$.

The singular graph is drawn in figure 1. For general $p \geq 3$, the involved points of $X = \mathbb{P}^1$ are $S = \{1, -1, \imath, -\imath, 0, \infty\}$ where $\imath$ is a square root of -1 in $\overline{\mathbb{F}_p}$. Applying $f(x) = \frac{1+x^2}{2x}$ (or $g(y) = y^2$), we have $S_0 = \{1, -1, 0, \infty\}$. Moreover, $\mathfrak{D}_f(S_0) = (2-1)[1]+(2-1)[-1]$ and $\mathfrak{D}_g(S_0) = (2-1)[0] + (2-1)[\infty]$, hence the condition $\operatorname{div}(\rho) = \mathfrak{D}_f(S_0) - \mathfrak{D}_g(S_0) = [1] + [-1] - [0] - [\infty]$ is fulfilled by the function

$$\rho(x) = \frac{(x-1)(x+1)}{x} \in \mathbb{F}_p(\mathbb{P}^1).$$

Some `magma` experiments, for few small values of p, show that there do exist such a set with $\sharp T_0 = p - 1$. Since $\sharp S_0 = 4$ and p is odd, one can try $t = \frac{p-1}{2}$ and $s = 2$. The functional regularness criterion also requires a function $\varphi \in \mathbb{F}_p(X_0)$ such that $\operatorname{div}(\varphi) = 2\operatorname{div}(T_0) - \frac{p-1}{2}\operatorname{div}(S_0)$. Up to a constant,

$$\varphi(x) = \frac{h(x)^2}{[(x-1)(x+1)x]^{\frac{p-1}{2}}}$$

works. Hence, Theorem 9 asserts that the set $f^{-1}(T_0)$ is complete if and only if $h(0) \neq 0$ and

$$\rho(x)^{\frac{p-1}{2}}\varphi\left(\frac{x^2+1}{2x}\right) \sim \varphi(x^2).$$

This functional equation can be written

$$\left[\frac{(x-1)(x+1)}{x}\right]^{\frac{p-1}{2}} \times \frac{h\left(\frac{x^2+1}{2x}\right)^2}{\left[\left(\frac{x^2+1}{2x}-1\right)\left(\frac{x^2+1}{2x}+1\right)\left(\frac{x^2+1}{2x}\right)\right]^{\frac{p-1}{2}}} \sim \frac{h(x^2)^2}{[(x^2-1)(x^2+1)x^2]^{\frac{p-1}{2}}}.$$

After simplification by powers of x, $x-1$ and $x+1$, this is equivalent to

$$\left[x^{p-1}h\left(\frac{x^2+1}{2x}\right)\right]^2 \sim \left[h(x^2)\right]^2,$$

that is to

$$x^{p-1}h\left(\frac{x^2+1}{2x}\right) \sim h(x^2),$$

which is neither than (7) with $h(x) = H(x^2)$.

Of course, proving that this functional equation do have a solution H is another task. On this example, the solution H have been already guessed by Garcia and Stichtenoth. To ovoid cheating, we explain in the following section how this task can be achieved on another example, chosen in such a way that the solution is *a priori* unknown.

3.3 Graph based strategy to produce and to study asymptotically good recursive towers

The goal of this section is to show how a good recursive tower can be studied, from its production process in Section 3.3.1, to the computation of its parameters in Sections 3.3.2 and 3.3.3.

3.3.1 Producing a potentially good recursive tower using graphs and computer help

The strategy to produce such a candidate is the following. For algorithmic purpose, we fix a base curve X and a "kind" of correspondence $\Gamma \subset X \times X$, that is a set of correspondences parametrized by some quasi-projective variety V. In order to obtain recursive towers having potentially low genus sequence as required by Proposition 4, we also fix a specific finite singular graph. Now, any edge of the graph $\mathcal{G}_\infty(X, \Gamma)$ corresponds to a relation on the parameters of the correspondence Γ viewed as a points of V. Hence, correspondences Γ on X of the given kind such that $\mathcal{G}_\infty(X, \Gamma)$ contains the fixed finite graph as a subgraph are parametrized by a subvariety W of V. Then, a `magma` program returns, for a given prime p, all $\mathbb{F}_p$-rational points of W.

After very few trials of specific singular graphs[5], we obtain for few values of p some explicit equations. The associated graph having, as checked using a `sage` program, some d-regular component, these equations define *potentially good* recursive towers. Indeed, they experimentally possess some d-regular set ensuring that the number of points is large enough, and their singular graph have a certain imposed shape, making it possible that the genus sequence is low enough as required in Proposition 4.

Here is how all this works on an example. We choose:

- the base curve X to be $\mathbb{P}^1$;
- correspondences Γ of bi-degree $(2, 2)$ and with separable variables, that is of type $\Gamma_{f,g}$ where f and g are two functions from $\mathbb{P}^1$ to $\mathbb{P}^1$ of degree 2;
- a singular graph of the form

  where R_1, R_2 are the ramified points of f and S_1, S_2 those of g. In particular, in view of the specific shape of the singular graph, these four ramification points should be distinct.

  Remark – This kind of singular graph is not chosen at random. In order to minimize the genus sequence, the curves X_n must be singular as pointed out in [HP14]. This means by Proposition 2 that there must exist some paths from ramification points of f to ramification points of g. We also have noted that in most known examples of good recursive tower, there are loops at some of these ramification points. The chosen graph is one of the most simple that takes into account these constraints.

Note that there are 6 parameters in such a singular graph, namely the 6 points P_i, R_i, S_i, for $i = 1, 2$. We use the automorphisms group $\mathrm{Aut}(\mathbb{P}^1)$ to fix some of them as follows. For any $\sigma, \tau \in \mathrm{Aut}(\mathbb{P}^1)$, the map

$$(P_1, \ldots, P_n) \mapsto (\tau^{-1}(P_1), \ldots, \tau^{-1}(P_n))$$

[5] Trying with the singular graph in figure 1 gives as an unique solution (up to $\mathrm{Aut}(\mathbb{P}^1)$) the Garcia-Stichtenoth tower $y^2 = \frac{x^2+1}{2x}$!

defines an isomorphism from the tower $\mathcal{T}(\mathbb{P}^1, \Gamma_{f,g})$ to the tower $\mathcal{T}(\mathbb{P}^1, \Gamma_{\sigma\circ f\circ\tau, \sigma\circ g\circ\tau})$. Therefore, using the simply 3-transitivity of $\mathrm{Aut}(\mathbb{P}^1)$ on $\mathbb{P}^1$, one can suppose that $R_1 = 1$, $S_1 = 0$ and $S_2 = \infty$. In the same way, one can suppose that $g(S_1) = 0$, $g(S_2) = \infty$ and $g(1) = 1$. These normalizations lead to $g(y) = y^2$, so that we are reduced to look for a rational function

$$f(x) = \frac{a_2x^2 + a_1x + a_0}{b_2x^2 + b_1x + b_0}$$

where the parameter $(a_2 : a_1 : a_0 : b_2 : b_1 : b_0)$ lives in $\mathbb{P}^5$. Since f have to be of degree $\deg f = \deg g = 2$, this point in $\mathbb{P}^5$ must lie in the complementary V of the sets of constant functions and of degree one functions. The constant functions is the zero set of the 2-by-2 minors of $\left(\begin{smallmatrix} a_2 & a_1 & a_0 \\ b_2 & b_1 & b_0 \end{smallmatrix}\right)$, and the degree one functions is the zero set of the resultant of $a_2x^2 + a_1x + a_0$ and $b_2x^2 + b_1x + b_0$.

For such a $f \in V$, the equation of the correspondence $\Gamma_{f,g}$ in $\mathbb{P}^1 \times \mathbb{P}^1 = \mathrm{Proj}(\mathbb{F}_q[X_1, Y_1]) \times \mathrm{Proj}(\mathbb{F}_q[X_2, Y_2])$ is

$$E(X_1, Y_1, X_2, Y_2) = Y_2^2(a_2X_1^2 + a_1X_1Y_1 + a_0Y_1^2) - X_2^2(b_2X_1^2 + b_1X_1Y_1 + b_0Y_1^2) = 0.$$

Let us now traduce as equations on the parameter $(a_2 : a_1 : a_0 : b_2 : b_1 : b_0)$ the requested shape for the singular graph. The fact that the point $(1 : 1)$ is ramified by f gives as a first constraint the vanishing at $x = 1$ of the derivative of $f(x)$, a quadratic equation in the parameters. Note for later use that the second ramified point by f is $(a_1b_0 - a_0b_1 : a_2b_1 - a_1b_2)$. Each loop, so as each horizontal path of length 2, gives rise to linear algebraic constraints on the parameters as follows. The four loops lead to the equations

$$E(1,1,1,1) = E(0,1,0,1) = E(1,0,1,0) = E(a_1b_0 - a_0b_1, a_2b_1 - a_1b_2, a_1b_0 - a_0b_1, a_2b_1 - a_1b_2) = 0.$$

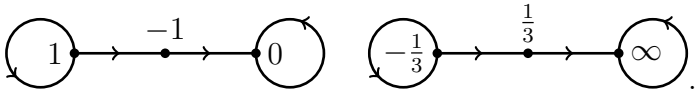
The existence of a path of length 2 from R_i to S_i is equivalent to the vanishing of a resultant, since this is the request of the existence of some common zero P_i of $f(R_i) - g(P)$ and of $f(P) - g(S_i)$. Finally these $1 + 4 + 2 = 7$ equations define a quasi-projective curve W in $\mathbb{P}^5$.

For the small values of the prime $p \in \{5, 7, 11, 13, 17\}$, we find using `magma` the unique solution whose equation $f(x) = \frac{x^2+x}{3x-1}$ doesn't depend on p.

To conclude, this graph aided strategy suggests to study the recursive tower defined by $X = \mathbb{P}^1$ for $p \geq 5$, and

$$\Gamma_{f,g} = \left\{ ((x_1 : y_1), (x_2 : y_2)) \in \mathbb{P}^1 \times \mathbb{P}^1 \mid \frac{x_1^2 + x_1y_1}{3x_1y_1 - y_1^2} = \frac{x_2^2}{y_2^2} \right\}.$$

The ramification points of the function $f(x) = \frac{x^2+x}{3x-1}$ are 1 and $-\frac{1}{3} \in \mathbb{F}_p$, those of the function $g(y) = y^2$ are 0 and ∞, and the singular complete subgraph is the following



The remaining of this section is devoted to the proof of the following result stating that this *potentially good* tower is actually *asymptotically good*.

Theorem 11. *The recursive tower* $\mathcal{T}\left(\mathbb{P}^1, y^2 = \frac{x^2+x}{3x-1}\right)$ *is asymptotically good.*

Proof — The proof is divided in two steps. In Propositions 12, the genus sequence is computed and we observe that it has the good shape requested in Proposition 4. Then, we prove Proposition 14 that the number of points sequence also have the good shape. □

3.3.2 Genus sequence computation

In this section we establish a closed formula for the genus sequence of the tower. One can distinguish at least two strategies to compute the genus sequence of such a recursive tower. The first one, used by Garcia and Stichtenoth in their articles in this area, consists in applying the Riemann-Hurwitz genus formula to the function field extensions $\mathbb{F}_p(X_n)/\mathbb{F}_p(X_1)$ after having computed the different divisor of these extensions. The second one, used in our previous work on recursive towers [HP14], consists in computing the geometric genus of the curves X_n from their arithmetic one by subtracting the sum of the measures of singularity of the points. This last point of view takes better into account the geometry of the data. Furthermore, as will be seen by the reader in the proof of Lemma 12 below, this method is a guide for the choice of a fixed singular graph as was done in Subsection 3.3.1. This is the first time that we illustrate our method on a simple, though non-trivial, example of recursive tower.

Proposition 12. *The genus sequence $(g_n)_{n\geq 1}$ of the tower $\mathcal{T}\left(\mathbb{P}^1, y^2 = \frac{x^2+x}{3x-1}\right)$ is given by*

$$g_n = 2^n - (2 + n \bmod 2) \times 2^{\lfloor \frac{n}{2} \rfloor} + 1, \qquad \forall n \geq 1.$$

Proof — Let $n \geq 1$. We denote by ν_n the desingularization morphism $\nu_n : \widetilde{X}_n \to X_n$ and by $X_n^\sharp$ the pullback of the embedding $X_n \hookrightarrow X_{n-1} \times X$ along $\nu_{n-1} \times \mathrm{Id} : \widetilde{X}_{n-1} \times X \to X_{n-1} \times X$. We have the cartesian diagram

$$\begin{array}{ccc} X_n^\sharp & \hookrightarrow & \widetilde{X}_{n-1} \times X \\ \downarrow & & \downarrow{\scriptstyle \nu_{n-1} \times \mathrm{Id}} \\ X_n & \hookrightarrow & X_{n-1} \times X \end{array}$$

The curves $X_n, X_n^\sharp$ and $\widetilde{X}_n$ are birational and the two first one are singular for $n \geq 3$. We thus introduce the *measure of singularity* of the curve $X_n^\sharp$ defined, as usual, by

$$\Delta_n = \sum_{P \in X_n^\sharp(\overline{\mathbb{F}_p})} \dim_{\overline{\mathbb{F}_p}} \widetilde{\mathcal{O}}_P / \mathcal{O}_P,$$

where $\mathcal{O}_P$ and $\widetilde{\mathcal{O}}_P$ denote the local ring at P of $X_n^\sharp$ and of its integral closure. Then, using Proposition 4 in [HP14] specialized to the case where $d = 2$, $g_1 = 0$ and $\gamma_2 = 1$, we obtain:

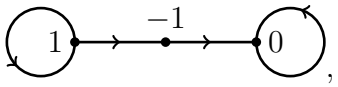
$$g_n = 1 + (n-2)2^{n-1} - \sum_{i=2}^{n} 2^{n-i} \Delta_i.$$

From the following Lemma 13, we have $\Delta_i = 2^{i-1} - 2^{\lfloor \frac{i}{2} \rfloor}$. Proposition 12 follows from an easy summation exercise. □

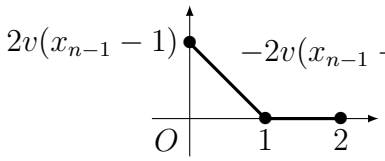
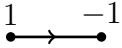
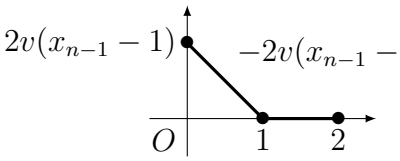
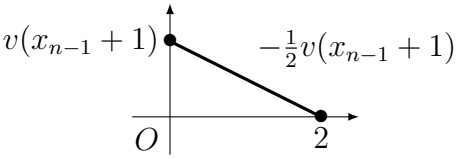
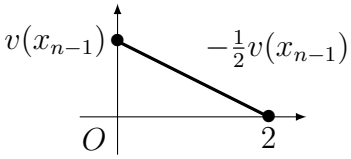
Lemma 13. *Let $n \geq 1$. The singular points of the curve $X_n^\sharp$ are above the points $(1^r, -1, 0^s)$ and $\left(-\frac{1}{3}^r, \frac{1}{3}, \infty^s\right)$ of X_n, for $r + s + 1 = n$ and $r \geq s \geq 1$. For such r, s, there are exactly 2^{s-1} points on $X_n^\sharp$, all of them giving rise to two points on $\widetilde{X}_n$, and having a measure of singularity equal to 2^{r-s}. The global measure of singularity of the curve $X_n^\sharp$ is $\Delta_n = 2^{n-1} - 2^{\lfloor \frac{n}{2} \rfloor}$.*

Remark – The curves X_1 and X_2 are smooth and thus so are $X_1^\sharp$ and $X_2^\sharp$.

Proof — The singular points of X_n correspond by Proposition 2 to the paths of the graph $\mathcal{G}_\infty$ joining a ramified point of f to a ramified point of g. In view of the chosen singular graph, they are the points $(1^r, -1, 0^s)$ and $\left(-\frac{1}{3}^r, \frac{1}{3}, \infty^s\right)$ for $r, s \geq 1$ and $r+s+1 = n$. The second one going the same way, let us concentrate on the first type of points. For each edge of the corresponding singular component of the singular graph



one can associate an appropriate recursive algebraic relation and the corresponding Newton polygon in the following way:

	$(x_n-1)^2 - 2(x_n-1) - \frac{(x_{n-1}-1)^2}{3x_{n-1}-1}$ 		$(x_n+1)^2 - 2(x_n+1) - \frac{(x_{n-1}-1)^2}{3x_{n-1}-1}$ 
	$x_n^2 - \frac{x_{n-1}(x_{n-1}+1)}{3x_{n-1}-1}$ 		$x_n^2 - \frac{x_{n-1}(x_{n-1}+1)}{3x_{n-1}-1}$ 

In this tabular, v respectively denotes a valuation of the field $\mathbb{F}_p(X_{n-1})$ satisfying $v(x_{n-1}-1) > 0$, $v(x_{n-1}-1) > 0$, $v(x_{n-1}+1) > 0$ and $v(x_{n-1}) > 0$. In the remaining of this section, for $r, s \geq 1$, we denote by $v_{(1^r,-1,0^s)}$ any valuation of the field $\mathbb{F}_p(X_{r+s+1})$ satisfying $v_{(1^r,-1,0^s)}(x_i - 1) > 0$ for $1 \leq i \leq r$, $v_{(1^r,-1,0^s)}(x_{r+1}+1) > 0$, $v_{(1^r,-1,0^s)}(x_j) > 0$ for $1 \leq j \leq s$ and $v_{(1^r,-1,0^s)}(x_1 - 1) = 1$ (we normalize this way in order to have formulas (8)). We do the same for $v_{(1^r)}$ and $v_{(1^r,-1)}$. With these notations, the Newton polygons of the preceding tabular permit to prove that every loop at 1 and the path form 1 to -1 multiply the valuations by 2, while the path from -1 to 0 and the loop at 0 divides the valuations by 2. More precisely, we have

$$v_{(1^r)}(x_r - 1) = 2^{r-1}, \qquad v_{(1^r,-1)}(x_{r+1}+1) = 2^r, \qquad v_{(1^r,-1,0^s)}(x_{r+s+1}) = 2^{r-s}. \tag{8}$$

Let us start with the point $Q = (1^{n-2}, -1, 0)$, that is with $r = n-2$ and $s = 1$. The point $P = (1^{n-2}, -1) \in X_{n-1}$ is smooth and thus corresponds to a unique point of $\widetilde{X}_{n-1}$, and the function x_1 is an uniformizing parameter at P. Let $\mathcal{O}_P$ be the local ring at P. There is a unique singular point $Q^\sharp \in X_n^\sharp$ above $P \in X_{n-1}$, and above $Q \in X_n$. The local ring at $Q^\sharp$ is $\mathcal{O}_{Q^\sharp} = \mathcal{O}_P[x_n]$. Since $v_P(x_{n-1}+1) = 2^{n-2}$, one has

$$\left(\frac{x_n}{x_1^{2^{n-3}}}\right)^2 - \underbrace{\frac{x_{n-1}}{3x_{n-1}-1} \times \frac{x_{n-1}+1}{x_1^{2^{n-2}}}}_{\text{non zero at } P} = 0.$$

The non-vanishing of the constant function shows that this equation is smooth. This proves that $\widetilde{\mathcal{O}_P[x_n]} = \mathcal{O}_P\left[\frac{x_n}{x_1^{2^{n-3}}}\right]$. Thus there are two points in $\widetilde{X_n}$ above $Q^\sharp \in X_n^\sharp$, or above $(1^{n-2}, -1, 0) \in X_n$ and moreover $\delta_{P^\sharp} = 2^{n-3}$.

We proceed by induction on s for the study of the singularity above the general singular point $P = (1^r, -1, 0^s) \in X_n$ for $r + s + 1 = n$. We need to distinguish two cases.

If $r \geq s \geq 1$, then by induction, there are exactly 2^{s-1} points of $\widetilde{X}_{n-1}$ above $(1^r, -1, 0^{s-1})$. Let P one of them and let $\mathcal{O}_P$ be the local ring at P. The function x_1 is still an uniformizing parameter at P and above P there is only one point $Q^\sharp \in X_n^\sharp$, whose local ring is $\mathcal{O}_{Q^\sharp} = \mathcal{O}_P[x_n]$. Then $v_P(x_{n-1}) = 2^{r-s+1}$, and the equation

$$\left(\frac{x_n}{x_1^{2^{r-s}}}\right)^2 - \underbrace{\frac{x_{n-1}}{3x_{n-1}-1} \times \frac{x_{n-1}+1}{x_1^{2^{r-s+1}}}}_{\text{non zero at } P} = 0$$

is smooth. This proves that there are two points of $\widetilde{X_n}$ above $Q^\sharp \in X_n^\sharp$, that is above $(1^r, -1, 0^s) \in X_n$, and that $\delta_{P^\sharp} = 2^{r-s}$.

In the other case, that is if $s > r \geq 1$, then x_{n-1} turns to be an uniformizing element for all the points of $\widetilde{X}_{n-1}$ above $P = (1^r, -1, 0^{s-1})$, and the corresponding points $P^\sharp$ on $X_n^\sharp$ are smooth (and ramified over $\widetilde{X}_{n-1}$).

In conclusion, we get by summation

$$\Delta_n = 2 \times \sum_{s=1}^{\lfloor \frac{n-1}{2} \rfloor} 2^{s-1} \times 2^{r-s} = \sum_{s=1}^{\lfloor \frac{n-1}{2} \rfloor} 2^{n-s-1},$$

where the first factor 2 comes from the other component of the singular graph. The remaining of the computation is left to the reader. □

3.3.3 Lower bound for the number of points sequence

The last step is to prove that the tower has a large enough number of rational points sequence over some $\mathbb{F}_{p^r}$, that is of size $\sharp\widetilde{X}_n(\mathbb{F}_{p^r}) = c \times 2^n + o(2^n)$ for some non-zero constant c as requested in Proposition 4. To this end, we prove the following result.

Proposition 14. *Let $p \geq 5$ be a prime. There exists $r \geq 1$, and a finite set $T \subset \mathbb{P}^1(\mathbb{F}_{p^r})$ with $2(p-1)$ elements, such that the graph $\mathcal{G}_T(X, \Gamma)$ is 2-regular and the number of points sequence of the tower $\mathcal{T}\left(\mathbb{P}^1_{\mathbb{F}_p}, y^2 = \frac{x^2+x}{3x-1}\right)$ satisfies*

$$\sharp X_n(\mathbb{F}_q^r) \geq (p-1) \times 2^n.$$

By the correspondence recalled in Proposition 2, if such a finite set T exists, then the curve X_n contains at least $2^n(p-1)$ points over $\mathbb{F}_{p^2}$. The rest of this section is devoted to the proof of the existence of this finite set T, stated in Lemma 15. It is divided in few steps.

First, we experimentally compute this finite set and its characteristic polynomial for few small primes p. Second, we observe that these polynomials for these small values of p do lift to $\mathbb{Z}$, that is are reduction modulo p of some truncation of some integer coefficients series. We enter this experimental integer sequence of first coefficients in the database OEIS, which luckily returns a whole infinite integer sequence. Finally, we prove that the reduction modulo p of some truncation of the generating series of this infinite integer sequence do fulfill the functional equation required in Theorem 9. This implies the regularness of the reciprocal image by f of the zeroes of the truncations. The fact that the power series is closely related to a Gaussian hypergeometric function, hence satisfies some second order linear differential equation, turns to be a crucial point here.

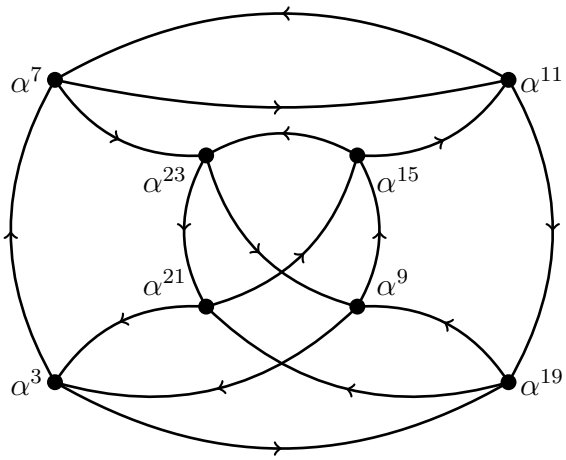


Figure 2: The 2 regular complete component of $\mathcal{G}_\infty$ for $p = 5$

Experimental observation for few small primes p. — It is an experimental observation, using `magma` and `sage`, that for small values of the prime p, the geometric graph $\mathcal{G}_\infty(\mathbb{P}^1_{\mathbb{F}_p}, y^2 = \frac{x^2+x}{3x-1})$ contains a finite 2-regular component with $2(p-1)$ vertices. In figure 2, we represent this component for $p = 5$.

Looking for a potentially splitting set for any prime p. — Suppose that there exists, for any prime $p \geq 5$, some non-empty finite 2-regular set $T = T_p$ in the geometric graph $\mathcal{G}_\infty(\mathbb{P}^1_{\mathbb{F}_p}, y^2 = \frac{x^2+x}{3x-1})$. Note that in this case, this set is unique thanks to [HP14, Theorem 19]. Let $\chi_p(x) \in \mathbb{F}_p[x]$ be the characteristic polynomial of the set of values of f (or g) at the vertices of T_p

$$\chi_p(x) = \prod_{P \in T_p} \left(x - x\left(f(P)\right)\right).$$

It is an easy task using `magma` to compute $\chi_p(x)$ for small primes p. Here is the table for $p \in \{5, 7, 11, 13, 17, 23\}$:

p	$\chi_p(x)$
5	$-1 + 2x + 2x^3 + x^4$
7	$1 + 3x + x^2 + 2x^3 + 2x^4 - 2x^5 + x^6$
11	$-1 - 3x - 4x^2 - 5x^3 - x^4 - 2x^6 - 2x^7 + x^8 + 4x^9 + x^{10}$
13	$1 + 3x + 2x^2 + 2x^3 + 2x^4 - x^5 + 4x^6 + 4x^7 + 6x^8 + 2x^9 + 5x^{10} - 4x^{11} + x^{12}$
17	$-1 - 3x + 2x^2 - 8x^3 + 7x^4 + 5x^5 + 4x^6 - 2x^7 + x^9 - x^{10} - 7x^{11} + 7x^{12} - 4x^{13}$ $-8x^{14} + 6x^{15} + x^{16}$
19	$1 + 3x - 4x^2 - 2x^3 - 7x^4 - 2x^5 - 5x^7 + 5x^8 + 7x^9 + 7x^{10} - 6x^{11} + 7x^{13} + 2x^{14}$ $-3x^{15} + 3x^{16} - 6x^{17} + x^{18}$
23	$-1 - 3x + 8x^2 - x^3 + 5x^4 - 7x^5 - 2x^6 - 9x^7 + 9x^8 - 9x^9 + 4x^{10} + 10x^{12} - 7x^{13}$ $-6x^{14} + 8x^{15} - 7x^{16} - 2x^{17} + 3x^{18} - 10x^{19} + 7x^{20} + 8x^{21} + x^{22}$

We observe that the constant term is nothing but the Legendre symbol $\left(\frac{-3}{p}\right)$. So all the polynomials $\left(\frac{-3}{p}\right)\chi_p(x)$ have unitary constant coefficient.

These polynomials can be seen as the analogue for this tower, of the Deuring polynomials for the tame optimal tower already touched on in Subsection 3.2. However, in contrast with this Subsection, we *a priori* do not know here any theoretical polynomial which could play the part of the Deuring polynomials therein. Fortunately, the Deuring polynomials turn to be the modulo p truncations at degree $(p-1)$ of a power series in $\mathbb{Z}[[x]]$. One can expect that

the same holds in our example. More precisely, we want to prove that there exists a power series $H(x) = \sum_{n\geq 0} a_n x^n \in \mathbb{Z}[[x]]$, such that for all primes $p \geq 5$, one has

$$\left(\frac{-3}{p}\right)\chi_p(x) = \sum_{n=0}^{p-1} a_n x^n \bmod p.$$

In other terms, we want to lift to $\mathbb{Z}[[x]]$ the polynomials $\left(\frac{-3}{p}\right)\chi_p(x) \in \mathbb{F}_p[x]$. Thanks to the Chinese Remainder Theorem and using more and more primes, one can lift the experimentally known polynomials $\left(\frac{-3}{p}\right)\chi_p(x)$ for small p modulo increasing integers. For example using primes of the preceding tabular, one obtains

$$\begin{aligned} H(x) = 1 &+ 3x + 15x^2 + 93x^3 + 639x^4 + 4653x^5 + 35169x^6 + 272835x^7 + 33065x^8 \\ &+ 322285x^9 + 438261x^{10} + 43884x^{11} + 40470x^{12} + 1755x^{13} - 2202x^{14} \\ &+ 130x^{15} - 1327x^{16} - 44x^{17} + 20x^{18} + 10x^{19} - 7x^{20} - 8x^{21} - x^{22} + \cdots, \end{aligned}$$

each coefficient being respectively known modulo

37182145, 37182145, 37182145, 37182145, 37182145, 7436429, 7436429, 1062347, 1062347, 1062347, 1062347, 96577, 96577, 7429, 7429,
7429, 7429, 437, 437, 23, 23, 23, 23.

Requesting for the integer sequence $1, 3, 15, 93, 639, 4\,653, 35\,169$ on the *Online Encyclopedia of Integer Sequences* [OEI], we fortunately learn that these are the first terms of the sequence

$$a_n = \sum_{k=0}^{n} \binom{n}{k}^2 \binom{2k}{k}.$$

The associated generating power series $H(x)$ is moreover related to a Gaussian hypergeometric function by

$$H(x) = \sum_{k=0}^{\infty} \underbrace{\left(\sum_{k=0}^{n} \binom{n}{k}^2 \binom{2k}{k}\right)}_{a_n} x^n = \frac{1}{1-3x} F\left(\begin{matrix}1/3,\ 2/3 \\ 1\end{matrix}\middle|\ \frac{27x^2(1-x)}{(1-3x)^3}\right), \tag{9}$$

where the Gaussian hypergeometric part (see for instance [GKP89, Chap. 5] for hypergeometric series) is

$$F\left(\begin{matrix}1/3,\ 2/3 \\ 1\end{matrix}\middle|\ z\right) = \sum_{n=0}^{\infty} \frac{\left(\frac{1}{3}\right)_n \left(\frac{2}{3}\right)_n}{(1)_n\, n!} z^n, \qquad \text{so that} \qquad F\left(\begin{matrix}1/3,\ 2/3 \\ 1\end{matrix}\middle|\ 27z\right) = \sum_{n=0}^{\infty} \frac{(3n)!}{(n!)^3} z^n.$$

Here, we denote as usual $(a)_n \overset{\text{def}}{=} a(a+1)\cdots(a+n-1)$. We denote by $H_p(x) \in \mathbb{F}_p[x]$ the modulo p truncation in degree $(p-1)$ of H:

$$H_p(x) = \sum_{n=0}^{p-1} a_n x^n \bmod p. \tag{10}$$

Proof of the splitting behavior. — We have now reached the point where we do have, for any prime $p \geq 5$, a candidate for a 2-regular set, namely the set of roots of the explicit polynomial $H_p(x)$ defined in (10). The encouraging point is that it is easily checked using `magma` and `sage` that for any tested value of p, this set do corresponds to a 2-regular component of the geometric graph.

Lemma 15. *Let $p \geq 5$ be a prime and let T_0 (depending on p) be the set of roots of the polynomial $H_p(x) \in \mathbb{F}_p[x]$ defined in (10). Then $f^{-1}(T_0)$ is 2-regular.*

Proof — In order to apply the functional regularness criterion Theorem 9 of which we keep notations, we choose as finite complete set S the support of the singular graph

$$S = \left\{0, \pm 1, \pm\tfrac{1}{3}, \infty\right\}, \qquad \text{so that} \qquad S_0 = \left\{0, 1, \tfrac{1}{9}, \infty\right\}.$$

The different divisors are

$$\mathfrak{D}_f(S_0) = \left[-\tfrac{1}{3}\right] + [1] \qquad \text{and} \qquad \mathfrak{D}_g(S_0) = [0] + [\infty],$$

hence one can choose the function ρ to be

$$\rho(x) = \frac{(x-1)\left(x+\frac{1}{3}\right)}{x} \in \mathbb{F}_q(\mathbb{P}^1).$$

Since $H_p(0) \equiv H_p(0) \equiv 1 \neq 0 \pmod{p}$, the set T_0 of roots of $H_p(x)$ in $\overline{\mathbb{F}_p}$ is disjoint from the ramification locus $\{0, \infty\}$ of g. Since $\sharp T_0 = \deg(H_p) = (p-1)$, we can try $t = 2$ and $s = \frac{p-1}{2}$. We put

$$\varphi(x) = \frac{H_p(x)}{x(x-1)\left(x-\frac{1}{9}\right)}.$$

After some easy computation similar to those in Subsection 3.2, we see that the functional regularness criterion specializes as follows in this example. For the set $f^{-1}(T_0)$ to be 2-regular, it suffices that the functional equation

$$\frac{1}{(3x-1)^{1-p}} H_p\left(\frac{x^2+x}{3x-1}\right) \sim H_p\left(x^2\right) \tag{11}$$

holds, which follows from Lemma 17 below. □

Lemma 16. *Let $n = \sum_{i=0}^{r} n_i p^i$ be the decomposition of n in basis p. Then we have*

$$a_n \equiv \prod_{i=1}^{r} a_{n_i} \pmod{p}.$$

Proof — We recall Lucas formula [Dic66, p. 271] for binomial coefficients modulo a prime p. If $n = n_0 + n_1 p + \cdots + n_r p^r$ and $k = k_0 + k_1 p + \cdots + k_r p^r$ with $p_i \in \{0, \ldots, p-1\}$, then

$$\binom{n}{k} \equiv \prod_{i=0}^{r} \binom{n_i}{k_i} \pmod{p}.$$

From both computations

$$\begin{aligned} a_n &= \sum_{k=\sum_{i=0}^{r} k_i p^i = 0}^{n=\sum_{i=0}^{r} n_i p^i} \binom{\sum_{i=0}^{r} n_i p^i}{\sum_{i=0}^{r} k_i p^i}^2 \binom{2k}{k} \\ &\equiv \sum_{i=0}^{r} \sum_{k_i=0}^{p-1} \prod_{i=0}^{r} \binom{n_i}{k_i}^2 \binom{2k}{k} \pmod{p} \qquad \text{(by Lucas formula)} \end{aligned}$$

and

$$\prod_{i=1}^{r} a_{n_i} \equiv \sum_{i=0}^{r} \sum_{k_i=0}^{p-1} \prod_{i=0}^{r} \binom{n_i}{k_i}^2 \prod_{i=0}^{r} \binom{2k_i}{k_i} \pmod{p}$$

which takes into account that $\binom{n_r}{k_r} = 0$ if $k_r > n_r$, we have only to prove that for any $k = \sum_{i=0}^{r} k_i p^i$ with $0 \leq k_i \leq p-1$, equality

$$\binom{2k}{k} \equiv \prod_{i=0}^{r} \binom{2k_i}{k_i} \pmod{p} \tag{12}$$

holds. Suppose first that for any $i = 0, \ldots, r$, we have $0 \leq k_i \leq \frac{p-1}{2}$. Then $2k = \sum_{i=0}^{r} 2k_i p^i$ is the decomposition of $2k$ in basis p, and (12) follows from Lucas formula. Suppose now that for at least one $i \in \{0, 1, \ldots, r\}$, we have $\frac{p-1}{2} < k_i \leq p-1$. Then $k_i \leq p-1 < p \leq 2k_i$, hence as is well known $\binom{2k_i}{k_i} \equiv 0 \pmod{p}$. We now prove that in this case, $\binom{2k}{k} \equiv 0 \pmod{p}$, so that both sides in (12) vanish. We use Legendre Theorem [Dic66, p. 263] that the p-adic valuation of the factorial $n!$ of an integer n, written in basis p as $n = \sum_{i=0}^{r} n_i p^i$, is given by

$$v_p(n!) = \frac{n - S_p(n)}{p-1}, \tag{13}$$

where $S_p(n) := \sum_{i=0}^{r} n_i$. The vanishing of $\binom{2k}{k} = \frac{(2k)!}{(k!)^2}$ modulo p is equivalent to $v_p((2k)!) > 2v_p(k)$, hence by (13), is equivalent to $S_p(2k) < 2S_p(k)$. We observe that :

- for $i \in \{0, 1, \ldots, r\}$ such that $0 \leq k_i \leq \frac{p-1}{2}$, then $0 \leq 2k_i \leq p-1$;
- for $i \in \{0, 1, \ldots, r\}$ such that $k_i = \frac{p-1}{2} + \ell_i$, with $1 \leq \ell_i \leq \frac{p-1}{2}$, then $2k_i = (2\ell_i - 1) + p$, with $0 \leq 2\ell_i - 1 \leq p-1$.

Denote by $[N]_i$ the i-th digit of a composite integer N in basis p, so that

$$2S_p(k) - S_p(2k) = \sum_{i=0}^{r} 2k_i - [2k]_i. \tag{14}$$

We deduce the following tabular, where contrib. means "contribution to":

$k_i \in$	k_i	$2k_i$	contrib. $[2k]_i$	contrib. $[2k]_{i+1}$	contrib. to (14)
$\{0, \ldots, \frac{p-1}{2}\}$	k_i	$2k_i$	$+2k_i$	$+0$	$+0$
$\{\frac{p-1}{2}+1, \ldots, p-1\}$	$\frac{p-1}{2} + \ell_i$	$(2\ell_i - 1) + p$	$+(2\ell_i - 1)$	$+1$	$+p-1 > 0$

from which it follows that $v_p(\binom{2k}{k}) = 0$ if, and only if, there exists some $0 \leq i \leq r$ such that $\frac{p-1}{2} < k_i$. The proof of Lemma 16 is complete. □

We are now able to prove that the functional equation (11) holds. We use a Li's trick [Li10, §7.2], which relies this truncated series modulo p to the initial series, and on the fact that hypergeometric functions are solutions of some second order linear differential equations.

Lemma 17. *Let $H(x) \in \mathbb{Z}[[x]]$ be the series defined in (9) and for every prime p, let $H_p(x) \in \mathbb{F}_p[x]$ be the degree $(p-1)-th$ truncation of $H(x)$ modulo p defined in (10).*

(i) The series H and its truncation H_p modulo p are related by the relation

$$H(x)^{1-p} \equiv H_p(x) \pmod{p}.$$

(ii) The series H and its truncation H_p satisfy the functional equations

$$\frac{1}{1-3x}H\left(\frac{x^2+x}{3x-1}\right) = H(x^2) \qquad \text{and} \qquad \frac{1}{(1-3x)^{1-p}}H_p\left(\frac{x^2+x}{3x-1}\right) = H_p(x^2).$$

Proof — Point *(i)*. We have the following congruences modulo p:

$$\begin{aligned} H_p(x) \times H_p(x)^p \times H_p(x)^{p^2} \times \ldots &\equiv H_p(x) \times H_p(x^p) \times H_p(x^{p^2}) \times \ldots \\ &\equiv \prod_{i=0}^{\infty}\left(\sum_{n_i=0}^{p-1} a_{n_i}x^{n_i p^i}\right) \\ &\equiv \sum_{r\in\mathbb{N};0\le n_0,\ldots,n_r\le p-1} \prod_{i=1}^{r} a_{n_i}x^{n_0+pn_1+\cdots+n_rp^r} \\ &\equiv \sum_{n\in\mathbb{N}} a_n x^n \qquad \text{(by Lemma 16)} \\ &\equiv H(x), \end{aligned}$$

where the first product converges to an invertible function in $\mathbb{Z}_p[[x]]$. It follows that

$$H(x)^{1-p} = \frac{H(x)}{H(x)^p} \equiv H_p(x) \pmod{p},$$

which proves *(i)*. Now, Gaussian hypergeometric functions are known to be solution of some second order linear differential equation. As for the hypergeometric geometric function $F(x) = F\left(\left.\begin{smallmatrix}1/3, 2/3\\ 1\end{smallmatrix}\right| x\right)$, it satisfies the equation

$$x(1-x)F''(x) + (1-2x)F'(x) - \frac{2}{9}F(x) = 0$$

(see [GKP89, Ex. 5.108 p. 221]). We then deduce (the details of the computations are left to the reader) two second order linear differential equations respectively satisfied by the functions $x \mapsto \frac{1}{1-3x}H\left(\frac{x^2+x}{3x-1}\right)$ and $x \mapsto H(x^2)$. These two equations turn to be proportional. Since the two preceding functions have same value and derivative at zero, they must be equal. This complete the proof of the first functional equation. To prove the second one, it suffices to raise the first one to the power $(p-1)$ and to use point *(i)*. This completes the proofs of *(ii)*. □

3.3.4 The last question

We have not yet answered the important question of the value of r, such that $\lambda_r\left(\mathcal{T}\left(\mathbb{P}^1, y^2 = \frac{x^2+x}{3x-1}\right)\right) > 0$. The `magma` experiments for small values of $p \ge 5$ show that, at least for these values of p, one has $r = 2$. Unfortunately, we were not able to prove this. But a close look at Elkies article [Elk01] leads to the following Proposition, showing that this tower is actually not new.

Proposition 18. *The recursive tower $\mathcal{T}\left(\mathbb{P}^1, y^2 = \frac{x^2+x}{3x-1}\right)$ is isomorphic to the modular tower $(X_0(3\cdot 2^n))_{n\ge 2}$ described by Elkies [Elk01]. This tower is asymptotically good, and even optimal, over $\mathbb{F}_{p^2}$ for every prime p outside $\{2,3\}$.*

Proof — The model of the tower $(X_0(3\cdot 2^n))_{n\ge 2}$ given by Elkies [Elk01, formula (45)] is the recursive tower with base curve $X = \mathbb{P}^1$ and correspondence Γ_{f_E,g_E} defined by the two functions $f_E(x) = x^2$ and $g_E(y) = \frac{y^2+3y}{y-1}$. One easily verifies that $f = \sigma \circ f_E \circ \tau$ and $g = \sigma \circ g_E \circ \tau$ for $\tau(x) = \frac{3x+1}{x-1}$ and $\sigma(x) = \frac{x-1}{x-9}$. □

References

[Bal03] Stéphane Ballet, *Low increasing tower of algebraic function fields and bilinear complexity of multiplication in any extension of* $\mathbb{F}_q$, Finite Fields Appl. **9** (2003), no. 4, 472–478. MR 2007465 (2004m:11191)

[Bee04] Peter Beelen, *Graphs and recursively defined towers of function fields*, J. Number Theory **108** (2004), no. 2, 217–240.

[Dic66] Leonard Eugene Dickson, *History of the theory of numbers. Vol. I: Divisibility and primality.*, Chelsea Publishing Co., New York, 1966. MR 0245499 (39 #6807a)

[Elk01] Noam D. Elkies, *Explicit towers of Drinfeld modular curves*, European Congress of Mathematics, Vol. II (Barcelona, 2000), Progr. Math., vol. 202, Birkhäuser, Basel, 2001, pp. 189–198.

[GKP89] Ronald L. Graham, Donald E. Knuth, and Oren Patashnik, *Concrete mathematics*, Addison-Wesley Publishing Company, Advanced Book Program, Reading, MA, 1989, A foundation for computer science. MR 1001562 (91f:00001)

[GS95] Arnaldo Garcia and Henning Stichtenoth, *A tower of Artin-Schreier extensions of function fields attaining the Drinfeld-Vladut bound*, Invent. Math. **121** (1995), 211–222.

[GS07] ———, *Explicit towers of function fields over finite fields*, Topics in geometry, coding theory and cryptography, Algebr. Appl., vol. 6, Springer, Dordrecht, 2007, pp. 1–58. MR 2278034 (2007m:11160)

[GSR03] Arnaldo Garcia, Henning Stichtenoth, and Hans-Georg Rück, *On tame towers over finite fields*, J. Reine Angew. Math. **557** (2003), 53–80.

[HP14] Emmanuel Hallouin and Marc Perret, *Recursive towers of curves over finite fields using graph theory*, Mosc. Math. J. **14** (2014), no. 4, 773–806, 828. MR 3292049

[Iha81] Yasutaka Ihara, *Some remarks on the number of rational points of algebraic curves over finite fields*, J. Fac. Sci. Univ. Tokyo Sect. IA Math. **28** (1981), no. 3, 721–724 (1982). MR 656048 (84c:14016)

[Len02] H. W. Jr. Lenstra, *On a problem of Garcia, Stichtenoth, and Thomas*, Finite Fields App. **8** (2002), 166–170.

[Li10] Wen-Ching W. Li, *Modular curves and coding theory: a survey*, Finite fields: theory and applications, Contemp. Math., vol. 518, Amer. Math. Soc., Providence, RI, 2010, pp. 301–314.

[OEI] OEIS, *The on-line encyclopedia of integer sequences*, https://oeis.org.

[TVZ82] M. A. Tsfasman, S. G. Vlăduţ, and Th. Zink, *Modular curves, shimura curves, and goppa codes, better than the varshamov-gilbert bound*, Math. Nachr. **109** (1982), 21–28.

Hallouin Emmanuel (`hallouin@univ-tlse2.fr`)
Perret Marc (`perret@univ-tlse2.fr`)

Université Toulouse Jean Jaurès
5, allées Antonio Machado
31058 Toulouse cedex
France