



ALGEBRAIC COMBINATORICS

Adler Marques, Erik Mendoza, Luciane Quoos & Guilherme Tizziotti

A closed formula for the Geil-Matsumoto bound on numerical semigroups via Apéry sets

Volume 9, issue 4 (2026), p. 1139-1155.

<https://doi.org/10.5802/alco.503>

© The author(s), 2026.

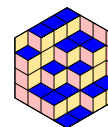


This article is licensed under the
CREATIVE COMMONS ATTRIBUTION (CC-BY) 4.0 LICENSE.
<http://creativecommons.org/licenses/by/4.0/>



Algebraic Combinatorics is published by The Combinatorics Consortium
and is a member of the Centre Mersenne for Open Scientific Publishing
www.tccpublishing.org www.centre-mersenne.org
e-ISSN: 2589-5486





A closed formula for the Geil-Matsumoto bound on numerical semigroups via Apéry sets

Adler Marques, Erik Mendoza, Luciane Quoos & Guilherme Tizziotti

ABSTRACT The Geil-Matsumoto bound (GM bound) constrains the number of rational points on a curve over a finite field in terms of the Weierstrass semigroup of any of the points on the curve. For general numerical semigroups, the GM bound lacks a simple closed-form expression, making its computation a challenging problem. A closed formula has been obtained for the case when the semigroup is generated by two co-prime integers. In this work, for any numerical semigroup, we provide a closed formula for the GM bound in terms of the Apéry set of a nonzero element of the semigroup. In the case where the numerical semigroup is generated by consecutive integers $n, n+1, \dots, n+t$ with $\lceil \frac{n-1}{2} \rceil \leq t \leq n-1$, we obtain a simple closed formula for the bound. We apply these results to obtain upper bounds on the number of rational points for algebraic curves over finite fields. In some cases, our bounds improve some well-known upper bounds on the number of rational points.

1. INTRODUCTION

Let $\mathbb{F}_q$ be the finite field with q elements of characteristic p , and $\mathbb{F}_q(\mathcal{X})$ be the function field of an absolutely irreducible, non-singular algebraic curve $\mathcal{X}$ defined over $\mathbb{F}_q$ of genus g . We denote by $N_q(\mathcal{X})$ the number of rational points over $\mathbb{F}_q$ (or rational places) on $\mathcal{X}$ (on $\mathbb{F}_q(\mathcal{X})$). The study of curves with many rational points is a classical problem that has regained prominence due to its numerous applications in mathematics, see [1, 25, 2, 12, 20, 30, 31], and coding theory, see [4, 7, 3] and references in there.

Several upper bounds for the number of rational points on algebraic curves are available in the literature. A fundamental upper bound is the Hasse-Weil bound, which states

$$N_q(\mathcal{X}) \leq q + 1 + 2g\sqrt{q},$$

see [26, Theorem V.2.3]. Serre remarked this bound could be improved in general to

$$(1) \quad N_q(\mathcal{X}) \leq q + 1 + g\lfloor 2\sqrt{q} \rfloor \quad \text{HWS-bound,}$$

Manuscript received 13th October 2025, revised 20th February 2026, accepted 30th March 2026.

KEYWORDS. Geil-Matsumoto bound, algebraic curves, rational points, Lewittes' bound.

ACKNOWLEDGEMENTS. The first three authors were partially financed by Coordenação de Aperfeiçoamento de Pessoal de Nível Superior (CAPES): Finance Code 001. The third author was also partially financed by Conselho Nacional de Desenvolvimento Científico e Tecnológico (CNPq): Project 307261/2023-9, and Fundação de Amparo a Pesquisa do Estado do Rio de Janeiro (FAPERJ): Project E-26/204.037/2024. The fourth author was partially financed by CNPq Project 306270/2023-4, and Fundação de Amparo à Pesquisa do Estado de Minas Gerais (FAPEMIG) Project APQ-01443-23.

see [26, Theorem V.3.1]. For curves of “large genus”, the bound established by Ihara [15] is better than the Hasse-Weil in many cases, and is given by

$$(2) \quad N_q(\mathcal{X}) \leq q + 1 + \frac{\sqrt{(8q+1)g^2 + 4(q^2 - q)g} - g}{2} \quad \text{Ihara-bound.}$$

Given a rational point Q on the curve $\mathcal{X}$ of genus g , the *Weierstrass semigroup* at Q is defined by

$$H(Q) = \{s \in \mathbb{N} : (z)_\infty = sQ \text{ for some } z \in \mathbb{F}_q(\mathcal{X})\},$$

where $(z)_\infty$ denotes the pole divisor of the function z . The complement set $G(Q) = \mathbb{N} \setminus H(Q)$ is the set of gaps at Q . The Weierstrass Gap Theorem states that if $g > 0$, then $\#G(Q) = g$, see [26, Theorem 1.6.8]. It is easy to show that for any $s_1, s_2 \in H(Q)$, their sum $s_1 + s_2$ remains in $H(Q)$. This closure property under addition shows that $H(Q)$ forms a numerical semigroup. By definition, a *numerical semigroup* is an additive submonoid $S \subseteq \mathbb{N}$ for which the complement $\mathbb{N} \setminus S$ is finite. The cardinality of this complement, $g = \#(\mathbb{N} \setminus S)$, is called the *genus* of the semigroup.

In 1990, Lewittes obtained a new upper bound for the number of rational points on a curve over $\mathbb{F}_q$ using a local information, the Weierstrass semigroup at one rational point Q on the curve. Let $m_{H(Q)}$ be the least positive element in $H(Q)$, the *Lewittes upper bound* $L_q(H(Q))$ is given by

$$(3) \quad N_q(\mathcal{X}) \leq L_q(H(Q)) := qm_{H(Q)} + 1,$$

see [18, Theorem 1]. For $q = 2, 3, 4$ and $g \geq 2$, this bound improves the Hasse-Weil bound. The Hermitian curve is a famous example of a curve attaining the Lewittes' bound considering the Weierstrass semigroup at the only point at infinity in the curve. In [19, Theorem 5.3], Mendoza characterized for the specific family of Kummer extensions with one point Q_∞ at infinity, the connections between being a Castle curve, attaining the Lewittes' bound for $H(Q_\infty)$, and the structure of the Weierstrass semigroup at Q_∞ .

In 2009, Geil and Matsumoto generalized Lewittes' upper bound by incorporating arithmetic information about all the generators of the Weierstrass semigroup. Specifically, suppose $\{h_1 < h_2 < \dots < h_m\}$ is a system of generators of the semigroup $H(Q)$, the *Geil-Matsumoto bound* $GM_q(H(Q))$ is given by

$$N_q(\mathcal{X}) \leq GM_q(H(Q)) := \#(H(Q) \setminus \bigcup_{i=1}^m (qh_i + H(Q))) + 1,$$

where $qh_i + H(Q) = \{qh_i + s : s \in H(Q)\}$ (see [12, Theorem 1]). In the same paper they also showed that the Lewittes' bound can be deduced from the Geil-Matsumoto bound, since

$$(4) \quad GM_q(H(Q)) \leq \#(H(Q) \setminus (qh_1 + H(Q))) + 1 = qh_1 + 1 = L_q(H(Q)).$$

An interesting example of a curve attaining the GM bound is the norm-trace curve over $\mathbb{F}_{q^r}$ with $2 \leq r$, introduced by Geil in [11]. This curve has $q^{2r-1} + 1$ rational points over $\mathbb{F}_{q^r}$ and the Weierstrass semigroup H at the only point at infinity on the curve is generated by two integers $H = \langle q^{r-1}, q^{r-1} + \dots + q + 1 \rangle$. The equality of the GM bound follows from [5, Theorem 3.2].

The Lewittes' bound is significantly simpler than the Geil-Matsumoto bound. In fact, the latter lacks a closed-form expression for a general semigroup. This computational difficulty has led to an interesting theoretical problem:

- deriving a closed-form expression for the Geil-Matsumoto bound for arbitrary numerical semigroups.

For a semigroup generated by two (co-prime) integers, Bras-Amorós and Vico-Oton [5] provided a closed formula for the Geil-Matsumoto bound. It is well known that given a semigroup generated by two elements, there exists a curve having a rational point whose Weierstrass semigroup is exactly this semigroup. These semigroups have also been related with Fermat and Mersenne numbers, see [10]. Semigroups generated by consecutive integers were studied by García-Sánchez and Rosales in [23] and [22], and also appear as Weierstrass semigroups in algebraic curves, see [6] and [11].

It is also interesting to mention that, despite their natural association with algebraic curves, not all numerical semigroups occur as the Weierstrass semigroup at a point on a projective nonsingular irreducible curve. In fact, let S denote a numerical semigroup with gap set $\mathbb{N} \setminus S = \{\ell_1, \dots, \ell_g\}$ and let S_m denote the set of all sums of m elements of S . If $\#S_m \geq (2m-1)(g-1)$ for some $m \geq 1$, then S cannot be the Weierstrass semigroup of a point on a projective nonsingular irreducible curve of genus g ; see [17]. Explicit examples of semigroups that are not realizable as Weierstrass semigroups can be found in [17, 21] and [27]. On the other hand, let m_S denote the smallest positive element in a semigroup S and let ℓ_g denote the largest gap of S . If $\ell_g < 2m_S$ and the weight of S is at most $g-2$, then Eisenbud and Harris showed that S does occur as the Weierstrass semigroup of a point on some curve; see [9]. Furthermore, in [16] Kaplan and Ye investigated the asymptotic proportion of numerical semigroups that are Weierstrass.

Motivated by these results, we investigated the Geil-Matsumoto bound and obtained two principal results, Theorems 3.3 and 4.4. In Theorem 3.3 we provide a closed expression for the Geil-Matsumoto bound in terms of the Apéry set of a nonzero element of the semigroup, and in Theorem 4.4 we give a simple closed formula for the GM bound for semigroups generated by consecutive integers $n, n+1, \dots, n+t$, where $\lceil \frac{n-1}{2} \rceil \leq t \leq n-1$. In Tables 1 and 2 we provide examples of algebraic curves where the GM bound on the number of rational points improves some well-known bounds.

The paper is organized as follows. In Section 2 we fix the notation that will be used throughout the paper and recall some basic facts about numerical semigroups and the Geil-Matsumoto bound. Section 3 is devoted to present a closed-form expression for the Geil-Matsumoto bound, while in Section 4 we study the Geil-Matsumoto bound for numerical semigroups generated by consecutive positive integers. Section 5 presents applications of the results established in previous sections to derive bounds for the number of rational points on certain Kummer extensions. Additionally, we provide comparisons with other known bounds.

2. PRELIMINARIES AND NOTATION

We start this section by establishing the notation that will be employed throughout this work.

At first we fix some arithmetical notation. For a and b integers, we denote by (a, b) the greatest common divisor of a and b . If $a \geq 1$ we let “ $b \bmod a$ ” stand for the remainder of the division of b by a . For $c \in \mathbb{R}$, we denote by $\lfloor c \rfloor$, $\lceil c \rceil$, and $\{c\}$ the floor, ceiling and fractional part functions of c , respectively. The set of nonnegative integers is denoted by $\mathbb{N}$. For $\alpha \in \mathbb{N}$ and a subset A of $\mathbb{N}$, we use the standard notation for the translation of A by α , that is, $A + \alpha := \{\beta + \alpha : \beta \in A\}$.

A *numerical semigroup* is an additive submonoid $S \subseteq \mathbb{N}$ such that its complement $G(S) := \mathbb{N} \setminus S$ is finite. The elements in $G(S)$ are called *gaps*, and $g := \#G(S)$ is the genus of the semigroup. The smallest nonzero element of S , denoted by m_S , is the *multiplicity* of the numerical semigroup S . It is well known that a numerical semigroup is finitely generated, that is, there exist $h_1, \dots, h_t \in S^* = S \setminus \{0\}$ coprimes

such that

$$S = \langle h_1, \dots, h_t \rangle := \left\{ \sum_{j=1}^t h_j n_j : n_j \in \mathbb{N} \text{ for } j = 1, \dots, t \right\}.$$

The set $\{h_1, \dots, h_t\}$ is called a *system of generators* for S . A distinguished family of generators for a semigroup arises from Apéry sets, a fundamental construction in semigroup theory. We now introduce this concept.

DEFINITION 2.1. *Let S be a numerical semigroup and n be a nonzero element of S . The Apéry set of n in S is defined by*

$$\text{Ap}(S, n) := \{s \in S : s - n \notin S\}.$$

García-Sánchez and Rosales proved a method for constructing the Apéry set.

LEMMA 2.2 ([24, Lemma 2.4, Lemma 2.6]). *Let S be a numerical semigroup and let n be a nonzero element of S . Then*

- (1) $\text{Ap}(S, n) = \{0 = w(0), w(1), \dots, w(n-1)\}$, where $w(i)$ is the least element of S congruent to i modulo n , for $i = 1, \dots, n$.
- (2) The set $\{n\} \cup (\text{Ap}(S, n) \setminus \{0\})$ is a system of generators for S .

In [23] and [22], the same authors investigated generators, and minimal generators sets of numerical semigroups. Of particular interest is their result concerning semigroups generated by consecutive integers.

LEMMA 2.3 ([23, Corollary 4]). *Let $S = \langle n, n+1, \dots, n+t \rangle$ be a numerical semigroup with $1 \leq t < n$. Then*

$$\text{Ap}(S, n) = \{\lambda n + (\lambda - 1)t + r : 1 \leq r \leq t, \lambda \in \mathbb{N}, \text{ and } 0 \leq (\lambda - 1)t + r < n\}.$$

Surprisingly, the theory of numerical semigroups has a deep connection with the theory of algebraic curves over finite fields through Weierstrass semigroups. This relation yields a particularly interesting result, the fact that the number of rational points on an algebraic curve over a finite field can be bounded using properties of the Weierstrass semigroup at one point of the curve [18]. We now introduce the relevant notation and recall several fundamental results connecting these theories.

An *algebraic curve* $\mathcal{X}$ over $\mathbb{F}_q$ is a projective, nonsingular, absolutely irreducible of genus g . Let $\mathbb{F}_q(\mathcal{X})$ be the function field of $\mathcal{X}$ and $\mathcal{P}_{\mathbb{F}_q(\mathcal{X})}$ denote the set of places of $\mathbb{F}_q(\mathcal{X})$. The number of rational places (degree one places) of $\mathbb{F}_q(\mathcal{X})$, or equivalently, the number of rational points on $\mathcal{X}$, is denoted by $N_q(\mathcal{X})$. The study of curves with many points and bounds (lower and upper) for $N_q(\mathcal{X})$ dates back to the work of Gauss and Fermat and has been extensively investigated, see [18, 15, 28] for results from eighties, and for more recent works on the subject see [12, 13, 2, 14, 29].

The Lewittes and the Geil-Matsumoto bounds can be studied in greater generality by extending the analysis to arbitrary numerical semigroups. Let q be a positive integer and S a numerical semigroup with multiplicity m_S . We define the Lewittes' bound of S as

$$(5) \quad L_q(S) := qm_S + 1 \quad \text{Lewittes' bound,}$$

and for $qS^* + S := \{qa + b : a \in S^* \text{ and } b \in S\}$ we denote the *Geil-Matsumoto bound* of S by

$$(6) \quad GM_q(S) := \#(S \setminus (qS^* + S)) + 1 \quad \text{GM bound.}$$

Given a numerical semigroup S , Equation (4) establishes that $GM_q(S) \leq L_q(S)$. Some authors have investigated conditions for equality in this bound. In [2, Proposition 9], Beelen and Ruano proved that for any semigroup S , the equality $GM_q(S) =$

$L_q(S)$ holds whenever $q \in S$. In particular,

$$(7) \quad \text{there exists } a \in S \text{ such that } a \text{ divides } q \Rightarrow GM_q(S) = L_q(S).$$

In 2014, Bras-Amorós and Vico-Oton provided a necessary and sufficient condition for the Geil-Matsumoto and Lewittes bounds to coincide. More specifically, they established the following result.

THEOREM 2.4 ([5, Theorem 4.1]). *Suppose that $S = \langle h_1, h_2, \dots, h_t \rangle$, where h_1 is the multiplicity of the semigroup S . Then*

$$GM_q(S) = L_q(S) \Leftrightarrow q(h_i - h_1) \in S \text{ for every } 2 \leq i \leq t.$$

In contrast with the Lewittes' bound simpler formulation, for an arbitrary numerical semigroup S the Geil-Matsumoto bound $GM_q(S)$ lacks a general closed-form expression and can be a challenging problem to obtain it. In [5], Bras-Amorós and Vico-Oton established an explicit closed-form expression for $GM_q(S)$ in the special case where S is a numerical semigroup generated by two integers.

THEOREM 2.5 ([5, Theorem 3.2]). *Let $a < b$ with $(a, b) = 1$, then*

$$GM_q(\langle a, b \rangle) = 1 + \sum_{k=0}^{a-1} \min \left\{ q, \left\lceil \frac{q-k}{a} \right\rceil b \right\}.$$

In the following sections, we present several results concerning the Geil-Matsumoto bound for numerical semigroups.

3. GEIL-MATSUMOTO BOUND FOR NUMERICAL SEMIGROUPS VIA APÉRY SETS

In this section, we first present a new simple condition on the semigroup S that guarantees the equality $GM_q(S) = L_q(S)$. We then derive a closed-form expression for the Geil-Matsumoto bound using the Apéry set of a nonzero element of the semigroup.

Let S be a numerical semigroup and $n \in S^*$. By Lemma 2.2,

$$\text{Ap}(S, n) = \{0 = w(0), w(1), \dots, w(n-1)\},$$

where $w(i)$ is the least element of S congruent with i modulo n . Furthermore, from the definition of $w(i)$ and writing $\gamma(i) := (w(i) - i)/n$ for $0 \leq i \leq n-1$, we can rewrite the semigroup S and as

$$(8) \quad S = \{jn + i : 0 \leq i \leq n-1, \gamma(i) \leq j\}.$$

Moreover, by Lemma 2.2, we have that

$$(9) \quad S = \langle n, w(1), w(2), \dots, w(n-1) \rangle.$$

Using Apéry sets, we can prove a similar result as in (7), that is, if the multiplicity m_S divides $q-1$, then the Lewittes' bound and the Geil-Matsumoto bound coincide.

PROPOSITION 3.1. *Let S be a numerical semigroup and m_S its multiplicity. If m_S divides $q-1$, then $GM_q(S) = L_q(S)$.*

Proof. Let $2 \leq n \in S$, and $S = \langle n, w(1), w(2), \dots, w(n-1) \rangle$ as in (9). Then,

$$s \in S \Leftrightarrow s \geq w(s \bmod n).$$

Thus, we have that for each $1 \leq i \leq m_S - 1$,

$$\begin{aligned} q(w(i) - m_S) \in S &\Leftrightarrow q(w(i) - m_S) \geq w((q(w(i) - m_S)) \bmod m_S) \\ &\Leftrightarrow q(w(i) - m_S) \geq w((q(\gamma(i)n + i - m_S)) \bmod m_S) \\ &\Leftrightarrow q(w(i) - m_S) \geq w((qi) \bmod m_S). \end{aligned}$$

Therefore, from Theorem 2.4, we conclude that

$$(10) \quad GM_q(S) = L_q(S) \Leftrightarrow q(w(i) - m_S) \geq w((qi) \bmod m_S) \text{ for every } 1 \leq i \leq m_S - 1.$$

Since m_S divides $q - 1$, then for every $1 \leq i \leq m_S - 1$,

$$w((qi) \bmod m_S) = w(((q - 1)i + i) \bmod m_S) = w(i).$$

This yields

$$q(w(i) - m_S) - w(i) = (q - 1)w(i) - qm_S \geq (m_S + 1)(q - 1) - qm_S = q - 1 - m_S \geq 0.$$

From (10) we conclude that $GM_q(S) = L_q(S)$. $\square$

From Proposition 3.1 one could wonder if in a semigroup S we also have the following similar result: if m_S is a divisor of $q + 1$, then $GM_q(S) = L_q(S)$. This is not true, since for $q = 11$ and $S = \langle 6, 7 \rangle$ we have $m_S = 6$ is a divisor of 12 but $GM_q(S) \neq L_q(S)$ from Theorem 2.4 (notice that $11 \notin S$).

In what follows, we present a closed formula for the Geil-Matsumoto bound $GM_q(S)$ for a numerical semigroup S using Apéry sets. First we need a technical lemma.

LEMMA 3.2. *If $S = \langle h_1, h_2, \dots, h_t \rangle$ is the semigroup generated by $h_1, h_2, \dots, h_t$, then*

$$GM_q(S) = \# \left\{ s \in S : \begin{array}{l} s - qh_1 \notin S \\ s - qh_2 \notin S \\ \vdots \\ s - qh_t \notin S \end{array} \right\} + 1.$$

Proof. We recall that $GM_q(S) := \#(S \setminus (qS^* + S)) + 1$. Let $s \in S \setminus (qS^* + S)$. Suppose that $s - qh_j \in S$ for some $j \in \{1, \dots, t\}$. We can write $s = qh_j + (s - qh_j)$ and so $s \in qS^* + S$, since $h_j \in S$, a contradiction. Conversely, let $s \in S$ such that $s - qh_j \notin S$ for all $j \in \{1, \dots, t\}$. If $s \in qS^* + S$, then $s = qs_1 + s_2$, for some $s_1 \in S^*$ and $s_2 \in S$. Since $S = \langle h_1, h_2, \dots, h_t \rangle$ and $h_i \in S^*$ for every $1 \leq i \leq t$, there exists $j \in \{1, \dots, t\}$ such that $s_1 = h_j + s_3$, with $s_3 \in S$. Then, we have $s = qh_j + qs_3 + s_2$ that implies $s - qh_j \in S$, a contradiction. $\square$

THEOREM 3.3. *Let S be a numerical semigroup, $n \in S^*$, and consider the Apéry set*

$$\text{Ap}(S, n) = \{0 = w(0), w(1), \dots, w(n - 1)\}.$$

Then $S = \langle n, w(1), w(2), \dots, w(n - 1) \rangle$, and for $k_i := (k - iq) \bmod n$ we have

$$GM_q(S) = 1 + \frac{1}{n} \sum_{k=0}^{n-1} \min_{1 \leq i \leq n-1} \{qn, qw(i) - w(k) + w(k_i)\}.$$

Proof. For each $0 \leq k \leq n - 1$, define the set

$$S_k := \{s \in S : s \equiv k \bmod n, s - qn \notin S, \text{ and } s - qw(i) \notin S \text{ for every } 1 \leq i \leq n - 1\}.$$

From Lemma 3.2, we have that $GM_q(S) = 1 + \sum_{k=0}^{n-1} \#S_k$. Now, we compute the cardinality of S_k for each k . Let $s \in S_k$. By the description of S given in (8), we have that $s = jn + k$, where $\gamma(k) \leq j$. Furthermore,

$$\begin{aligned} s - qn \notin S &\Leftrightarrow jn + k - qn \notin S \\ &\Leftrightarrow (j - q)n + k \notin S \\ &\Leftrightarrow j - q \leq \gamma(k) - 1 && \text{by Equation (8)} \\ &\Leftrightarrow j \leq q - 1 + \gamma(k) \end{aligned}$$

and, for $1 \leq i \leq n-1$, using that $w(i) = \gamma(i)n + i$, we get

$$\begin{aligned}
 s - qw(i) \notin S &\Leftrightarrow jn + k - q(\gamma(i)n + i) \notin S \\
 &\Leftrightarrow (j - q\gamma(i))n + k - iq \notin S \\
 &\Leftrightarrow \left(j - q\gamma(i) + \left\lfloor \frac{k - iq}{n} \right\rfloor \right)n + k_i \notin S \\
 &\Leftrightarrow j - q\gamma(i) + \left\lfloor \frac{k - iq}{n} \right\rfloor \leq \gamma(k_i) - 1 \\
 &\Leftrightarrow j \leq q\gamma(i) + \gamma(k_i) - \left\lfloor \frac{k - iq}{n} \right\rfloor - 1.
 \end{aligned}$$

Thus, $s = jn + k \in S_k$ if and only if

$$\gamma(k) \leq j \leq \min \left\{ q - 1 + \gamma(k), \min_{1 \leq i \leq n-1} \left\{ q\gamma(i) + \gamma(k_i) - \left\lfloor \frac{k - iq}{n} \right\rfloor - 1 \right\} \right\}.$$

Hence,

$$\#S_k = \max \left\{ 0, \min \left\{ q, \min_{1 \leq i \leq n-1} \left\{ q\gamma(i) - \gamma(k) + \gamma(k_i) - \left\lfloor \frac{k - iq}{n} \right\rfloor \right\} \right\} \right\}.$$

Note that, for $1 \leq i \leq n-1$,

$$\begin{aligned}
 q\gamma(i) - \gamma(k) + \gamma(k_i) - \left\lfloor \frac{k - iq}{n} \right\rfloor &= q\gamma(i) - \gamma(k) + \gamma(k_i) - \frac{k - iq - k_i}{n} \\
 &= \frac{q(n\gamma(i) + i) - (n\gamma(k) + k) + n\gamma(k_i) + k_i}{n} \\
 &= \frac{qw(i) - w(k) + w(k_i)}{n}.
 \end{aligned}$$

This implies that

$$\begin{aligned}
 \#S_k &= \max \left\{ 0, \min \left\{ q, \min_{1 \leq i \leq n-1} \left\{ q\gamma(i) - \gamma(k) + \gamma(k_i) - \left\lfloor \frac{k - iq}{n} \right\rfloor \right\} \right\} \right\} \\
 &= \max \left\{ 0, \min \left\{ q, \min_{1 \leq i \leq n-1} \left\{ \frac{qw(i) - w(k) + w(k_i)}{n} \right\} \right\} \right\} \\
 &= \frac{1}{n} \max \left\{ 0, \min \left\{ qn, \min_{1 \leq i \leq n-1} \{qw(i) - w(k) + w(k_i)\} \right\} \right\}.
 \end{aligned}$$

To finish the proof, we prove that $qw(i) - w(k) + w(k_i) \geq 0$ for every $1 \leq i \leq n-1$.

In fact, for $1 \leq i \leq n-1$, we can write

$$\begin{aligned}
 qw(i) + w(k_i) &= q(n\gamma(i) + i) + n\gamma(k_i) + k_i \\
 &= q(n\gamma(i) + i) + n\gamma(k_i) + k - iq - \left\lfloor \frac{k - iq}{n} \right\rfloor n \\
 &= \left(q\gamma(i) + \gamma(k_i) - \left\lfloor \frac{k - iq}{n} \right\rfloor \right)n + k.
 \end{aligned}$$

Since $w(i)$ and $w(k_i)$ are elements of the semigroup S , we have that $qw(i) + w(k_i)$ is an element of S congruent with k modulo n . Now, from the definition of $w(k)$,

$$qw(i) + w(k_i) \geq w(k).$$

Thus, we conclude that $qw(i) - w(k) + w(k_i) \geq 0$ for every $0 \leq i \leq n-1$. Consequently,

$$\#S_k = \frac{1}{n} \min_{1 \leq i \leq n-1} \{qn, qw(i) - w(k) + w(k_i)\},$$

and the proof is complete. $\square$

COROLLARY 3.4. *With notation as in Theorem 3.3, if $\{s_1, s_2, \dots, s_r\} \subseteq \{1, \dots, n-1\}$ is such that*

$$S = \langle n, w(s_1), w(s_2), \dots, w(s_r) \rangle,$$

then

$$GM_q(S) = 1 + \frac{1}{n} \sum_{k=0}^{n-1} \min_{i \in \{s_1, s_2, \dots, s_r\}} \{qn, qw(i) - w(k) + w(k_i)\}.$$

Proof. The proof follows straightforward from the proof of Theorem 3.3. $\square$

Now, we show that we can recover the closed-form expression for the Geil-Matsumoto bound $GM_q(S)$ given in Theorem 2.5 for $S = \langle a, b \rangle$ with $(a, b) = 1$. Note that we do not assume the condition $a < b$.

COROLLARY 3.5. *Let $S = \langle a, b \rangle$ be the semigroup generated by two elements with $(a, b) = 1$. Then*

$$GM_q(S) = 1 + \sum_{k=0}^{a-1} \min \left\{ q, \left\lceil \frac{q-k}{a} \right\rceil b \right\}.$$

Proof. It is well known that the Apéry set of a in S is given by

$$\text{Ap}(S, a) = \{0, b, 2b, \dots, (a-1)b\}.$$

Therefore $w(i) = b((ib') \bmod a)$ for $0 \leq i \leq a-1$, where $b' \in \{1, 2, \dots, a-1\}$ is such that $bb' \equiv 1 \bmod a$. Moreover, observe that $w(b \bmod a) = b$. Thus, from Corollary 3.4,

$$\begin{aligned} GM_q(S) &= 1 + \frac{1}{a} \sum_{k=0}^{a-1} \min_{i \in \{b \bmod a\}} \{qa, qw(i) - w(k) + w(k_i)\} \\ &= 1 + \frac{1}{a} \sum_{k=0}^{a-1} \min \{qa, qb - w(k) + w(k_{b \bmod a})\}. \end{aligned}$$

Now, note that

$$\begin{aligned} qb - w(k) + w(k_{b \bmod a}) &= qb - b((kb') \bmod a) + b((kb' - q) \bmod a) \\ &= qb - b \left(kb' - \left\lfloor \frac{kb'}{a} \right\rfloor a \right) + b \left(kb' - q - \left\lfloor \frac{kb' - q}{a} \right\rfloor a \right) \\ &= \left\lceil \frac{q}{a} - \left\lfloor \frac{kb'}{a} \right\rfloor \right\rceil ab. \end{aligned}$$

Since $(a, b') = 1$, we conclude that

$$\begin{aligned} GM_q(S) &= 1 + \frac{1}{a} \sum_{k=0}^{a-1} \min \left\{ qa, \left\lceil \frac{q}{a} - \left\lfloor \frac{kb'}{a} \right\rfloor \right\rceil ab \right\} \\ &= 1 + \sum_{k=0}^{a-1} \min \left\{ q, \left\lceil \frac{q}{a} - \left\lfloor \frac{kb'}{a} \right\rfloor \right\rceil b \right\} \\ &= 1 + \sum_{k=0}^{a-1} \min \left\{ q, \left\lceil \frac{q}{a} - \frac{k}{a} \right\rceil b \right\} \\ &= 1 + \sum_{k=0}^{a-1} \min \left\{ q, \left\lceil \frac{q-k}{a} \right\rceil b \right\}. \end{aligned}$$

$\square$

4. GM BOUND FOR SEMIGROUPS GENERATED BY INTERVALS

In this section, we study the Geil-Matsumoto bound for numerical semigroups generated by consecutive positive integers, that is, semigroups of the form $S = \langle n, n+1, \dots, n+t \rangle$ with $1 \leq t < n$. We begin by noting that if $S = \langle n, n+1, \dots, n+t \rangle$ with $1 \leq t < n$ then, by Theorem 2.4, the following equivalences hold:

$$(11) \quad GM_q(S) = L_q(S) \Leftrightarrow qi \in S \text{ for every } 1 \leq i \leq t \Leftrightarrow q \in S.$$

Moreover, from [23, Corollary 2], we have that $q \in S$ if and only if $(q \bmod n) \leq \lfloor \frac{q}{n} \rfloor t$. In particular, if $q < n$, we always have $GM_q(S) < L_q(S)$. Consequently, for this class of semigroups we have

$$GM_q(S) < L_q(S) \Leftrightarrow \left\lfloor \frac{q}{n} \right\rfloor t < (q \bmod n).$$

In the following theorem, we provide a formula for the Geil-Matsumoto bound for semigroups generated by consecutive integers.

THEOREM 4.1. *Let $S = \langle n, n+1, \dots, n+t \rangle$ with $1 \leq t < n$. Then*

$$(12) \quad GM_q(S) = 1 + \sum_{k=0}^{n-1} \min_{1 \leq i \leq t} \{q, C_{k,i}\},$$

where $k_i = (k - iq) \bmod n$ and $C_{k,i} := q - \left\lceil \frac{k}{t} \right\rceil + \left\lceil \frac{k_i}{t} \right\rceil + \left\lceil \frac{iq-k}{n} \right\rceil$.

Proof. Let $S = \langle n, n+1, \dots, n+t \rangle$ with $1 \leq t < n$. By Lemma 2.3, we obtain

$$\begin{aligned} \text{Ap}(S, n) &= \{\lambda n + (\lambda - 1)t + r : 1 \leq r \leq t, \lambda \in \mathbb{N}, \text{ and } 0 \leq (\lambda - 1)t + r < n\} \\ &= \{\lambda n + k : 1 \leq r \leq t, \lambda \in \mathbb{N}, 0 \leq k < n, \text{ and } k = (\lambda - 1)t + r\} \\ &= \{\lambda n + k : 1 \leq r \leq t, \lambda \in \mathbb{N}, 0 \leq k < n, \text{ and } \lambda = \left\lceil \frac{k}{t} \right\rceil\} \\ &= \left\{ \left\lceil \frac{k}{t} \right\rceil n + k : 0 \leq k < n \right\}. \end{aligned}$$

So, for every $0 \leq k \leq n-1$ we have $w(k) = \left\lceil \frac{k}{t} \right\rceil n + k$. Then, since

$$S = \langle n, w(1), w(2), \dots, w(t) \rangle,$$

Corollary 3.4 together with the following equality

$$k - iq - k_i = n \left\lfloor \frac{k - iq}{n} \right\rfloor = -n \left\lceil \frac{iq - k}{n} \right\rceil$$

yields

$$\begin{aligned} GM_q(S) &= 1 + \frac{1}{n} \sum_{k=0}^{n-1} \min_{1 \leq i \leq t} \left\{ qn, q \left\lceil \frac{i}{t} \right\rceil n + iq - \left\lceil \frac{k}{t} \right\rceil n - k + \left\lceil \frac{k_i}{t} \right\rceil n + k_i \right\} \\ &= 1 + \frac{1}{n} \sum_{k=0}^{n-1} \min_{1 \leq i \leq t} \left\{ qn, qn + iq - \left\lceil \frac{k}{t} \right\rceil n - k + \left\lceil \frac{k_i}{t} \right\rceil n + k_i \right\} \\ &= 1 + \frac{1}{n} \sum_{k=0}^{n-1} \min_{1 \leq i \leq t} \left\{ qn, qn - \left\lceil \frac{k}{t} \right\rceil n + \left\lceil \frac{k_i}{t} \right\rceil n + n \left\lceil \frac{iq - k}{n} \right\rceil \right\} \\ &= 1 + \sum_{k=0}^{n-1} \min_{1 \leq i \leq t} \left\{ q, q - \left\lceil \frac{k}{t} \right\rceil + \left\lceil \frac{k_i}{t} \right\rceil + \left\lceil \frac{iq - k}{n} \right\rceil \right\}. \quad \square \end{aligned}$$

In the follow, we aim to establish conditions under which the expression for $GM_q(S)$, given in the previous result, can be simplified. To achieve this, we analyze the possible values of

$$C_{k,i} := q - \left\lceil \frac{k}{t} \right\rceil + \left\lceil \frac{k_i}{t} \right\rceil + \left\lceil \frac{iq - k}{n} \right\rceil.$$

We begin by noting that $\left\lceil \frac{iq - k}{n} \right\rceil \geq 0$, since $0 \leq k \leq n - 1$ and $1 \leq i \leq t$. Therefore, in the case $k = 0$, we have

$$(13) \quad C_{0,i} = q + \left\lceil \frac{0_i}{t} \right\rceil + \left\lceil \frac{iq}{n} \right\rceil \geq q \quad \text{for every } 1 \leq i \leq t.$$

PROPOSITION 4.2. *Let $q \geq 2, n, t, k$ and i be integers such that $1 \leq t < n$, $1 \leq i \leq t$, and $1 \leq k \leq \min\{n - 1, 2t\}$. Let*

$$C_{k,i} := q - \left\lceil \frac{k}{t} \right\rceil + \left\lceil \frac{k_i}{t} \right\rceil + \left\lceil \frac{iq - k}{n} \right\rceil,$$

where $k_i = (k - iq) \bmod n$.

- If $1 \leq k \leq t$, then

$$(14) \quad \min_{1 \leq i \leq t} \{q, C_{k,i}\} = \begin{cases} q - 1, & \text{if } q \mid k, \\ q, & \text{otherwise.} \end{cases}$$

- If $t < k \leq \min\{n - 1, 2t\}$, then

$$(15) \quad \min_{1 \leq i \leq t} \{q, C_{k,i}\} = \begin{cases} q - 2, & \text{if } q \mid k, \\ q - 1, & \text{if } t \geq (k \bmod q) \text{ and } q \nmid k, \\ q - 1, & \text{if } q \mid (k + n), k \leq qt - n, \text{ and } q \nmid k, \\ q, & \text{otherwise.} \end{cases}$$

Proof. First, suppose that $1 \leq k \leq t$. Then, we have $C_{k,i} = q - 1 + \left\lceil \frac{k_i}{t} \right\rceil + \left\lceil \frac{iq - k}{n} \right\rceil \geq q - 1$. Thus,

$$\begin{aligned} C_{k,i} = q - 1 &\Leftrightarrow \left\lceil \frac{k_i}{t} \right\rceil + \left\lceil \frac{iq - k}{n} \right\rceil = 0 \\ &\Leftrightarrow \left\lceil \frac{k_i}{t} \right\rceil = 0 \text{ and } \left\lceil \frac{iq - k}{n} \right\rceil = 0 \\ &\Leftrightarrow k_i = 0 \text{ and } 0 \leq k - iq < n \\ &\Leftrightarrow k = iq. \end{aligned}$$

This implies that, for each $1 \leq k \leq t$ such that q divides k , we can choose $i = \frac{k}{q} \leq \frac{t}{q} \leq t$ to obtain $C_{k,i} = q - 1$, and (14) follows.

Now, for each $t < k \leq \min\{n - 1, 2t\}$, we have $C_{k,i} = q - 2 + \left\lceil \frac{k_i}{t} \right\rceil + \left\lceil \frac{iq - k}{n} \right\rceil \geq q - 2$. Hence, $C_{k,i} = q - 2$ if and only if $k = iq$. Thus, for each $t < k \leq \min\{n - 1, 2t\}$ such that q divides k , we can choose $i = \frac{k}{q} \leq \frac{2t}{q} \leq t$ to obtain $C_{k,i} = q - 2$. On the other hand, if q does not divide k then

$$\begin{aligned} C_{k,i} = q - 1 &\Leftrightarrow \left\lceil \frac{k_i}{t} \right\rceil + \left\lceil \frac{iq - k}{n} \right\rceil = 1 \\ &\Leftrightarrow \left(\left\lceil \frac{k_i}{t} \right\rceil = 1 \text{ and } \left\lceil \frac{iq - k}{n} \right\rceil = 0 \right) \text{ or } \left(\left\lceil \frac{k_i}{t} \right\rceil = 0 \text{ and } \left\lceil \frac{iq - k}{n} \right\rceil = 1 \right). \end{aligned}$$

For the first case, we have

$$\begin{aligned} \left\lceil \frac{k_i}{t} \right\rceil = 1 \text{ and } \left\lceil \frac{iq - k}{n} \right\rceil = 0 &\Leftrightarrow 0 < k_i \leq t \text{ and } 0 \leq k - iq < n \\ &\Leftrightarrow 0 < k - iq \leq t \\ &\Leftrightarrow \frac{k - t}{q} \leq i < \frac{k}{q} \\ &\Leftrightarrow \left\lceil \frac{k - t}{q} \right\rceil \leq i \leq \left\lceil \frac{k}{q} \right\rceil - 1. \end{aligned}$$

Since $\left\lceil \frac{k}{q} \right\rceil - \left\lceil \frac{k-t}{q} \right\rceil \geq 1$ if and only if $t \geq (k \bmod q)$, we have that, for each $t < k \leq \min\{n-1, 2t\}$ such that $q \nmid k$ and $t \geq (k \bmod q)$, we can choose any $\left\lceil \frac{k-t}{q} \right\rceil \leq i \leq \left\lceil \frac{k}{q} \right\rceil - 1$ to obtain $C_{k,i} = q - 1$.

For the second case,

$$\begin{aligned} \left\lceil \frac{k_i}{t} \right\rceil = 0 \text{ and } \left\lceil \frac{iq - k}{n} \right\rceil = 1 &\Leftrightarrow k_i = 0 \text{ and } -n \leq k - iq < 0 \\ &\Leftrightarrow k + n = iq. \end{aligned}$$

Now, since $1 \leq i \leq t$, we must have $\frac{k+n}{q} \leq t$, that is, $k \leq qt - n$. Thus we have that, for each $t < k \leq \min\{n-1, 2t\}$ such that $q \nmid k$, $q \mid (k+n)$, and $k \leq qt - n$, we can choose $i = \frac{k+n}{q}$ to obtain $C_{k,i} = q - 1$.

This implies that for each $t < k \leq \min\{n-1, 2t\}$,

$$\min_{1 \leq i \leq t} \{q, C_{k,i}\} = \begin{cases} q - 2, & \text{if } q \mid k, \\ q - 1, & \text{if } t \geq (k \bmod q) \text{ and } q \nmid k, \\ q - 1, & \text{if } q \mid (k+n), k \leq qt - n, \text{ and } q \nmid k, \\ q, & \text{otherwise.} \end{cases} \quad \square$$

Using the results in Proposition 4.2, we obtain the following corollary.

COROLLARY 4.3. *Let $S = \langle n, n+1, \dots, n+t \rangle$ with $\left\lceil \frac{n-1}{2} \right\rceil \leq t < n$. Then*

$$(16) \quad GM_q(S) = qn + \left\lfloor \frac{t}{q} \right\rfloor - 2 \left\lceil \frac{n}{q} \right\rceil - \#A + 3,$$

where

$$\begin{aligned} A = &\{t < k \leq n-1 : t \geq (k \bmod q), q \nmid k\} \\ &\cup \{t < k \leq n-1 : k \leq qt - n, q \mid (k+n), \text{ and } q \nmid k\}. \end{aligned}$$

Proof. We have $GM_q(S) = 1 + \sum_{k=0}^{n-1} \min_{1 \leq i \leq t} \{q, C_{k,i}\}$. From Equation (13), we obtain

$$\min_{1 \leq i \leq t} \{q, C_{0,i}\} = q,$$

while Equation (14) yields

$$\sum_{k=1}^t \min_{1 \leq i \leq t} \{q, C_{k,i}\} = (q-1) \left\lfloor \frac{t}{q} \right\rfloor + q \left(t - \left\lfloor \frac{t}{q} \right\rfloor \right).$$

So,

$$(17) \quad \sum_{k=0}^t \min_{1 \leq i \leq t} \{q, C_{k,i}\} = q(t+1) - \left\lfloor \frac{t}{q} \right\rfloor.$$

Furthermore, we have $n - 1 = \min\{n - 1, 2t\}$, and defining the set

$$A := \{t < k \leq n - 1 : t \geq (k \bmod q) \text{ and } q \nmid k\} \\ \cup \{t < k \leq n - 1 : k \leq qt - n, q \mid (k + n), \text{ and } q \nmid k\},$$

by Equation (15), we conclude that

$$(18) \quad \sum_{k=t+1}^{n-1} \min_{1 \leq i \leq t} \{q, C_{k,i}\} = (q - 2) \left(\left\lfloor \frac{n-1}{q} \right\rfloor - \left\lfloor \frac{t}{q} \right\rfloor \right) \\ + (q - 1) \#A + q \left(n - 1 - t - \left\lfloor \frac{n-1}{q} \right\rfloor + \left\lfloor \frac{t}{q} \right\rfloor - \#A \right).$$

The result follows from Equations (17) and (18). $\square$

Using the last previous results, we are able to obtain explicit expressions for the GM bound $GM_q(S)$ for $2 \leq q$, $S = \langle n, n + 1, \dots, n + t \rangle$ and $\lceil \frac{n-1}{2} \rceil \leq t \leq n - 1$. Firstly, we observe that, if S is an ordinary semigroup (i.e. $t = n - 1$), then $\#A = 0$. Therefore, by Equation (16),

$$GM_q(S) = 2 + qn - \left\lfloor \frac{n}{q} \right\rfloor.$$

This formula matches the one provided in [12, Example 3]. On the other hand, if $t = 1$ then $S = \langle n, n + 1 \rangle$ and consequently the formula for $GM_q(S)$ reduces to that given in Corollary 3.5. Henceforth, we may assume $t \neq 1$.

THEOREM 4.4. *Let $q \geq 2$, and $S = \langle n, n + 1, \dots, n + t \rangle$, where $\lceil \frac{n-1}{2} \rceil \leq t < n$ and $t \neq 1$.*

(1) *If $q \leq t + 1$, then*

$$GM_q(S) = 3 + (q - 1)n - \left\lfloor \frac{n}{q} \right\rfloor + t.$$

(2) *If $t + 2 \leq q \leq n - 1$, then*

$$GM_q(S) = 4 + (q - 1)n + q - 2 \left\lfloor \frac{n}{q} \right\rfloor + \left\lfloor \frac{t+n}{q} \right\rfloor - \max \left\{ \left\lfloor \frac{t+n}{q} \right\rfloor, \min \left\{ 1 + \left\lfloor \frac{n}{q} \right\rfloor, t \right\} \right\}.$$

(3) *If $n \leq q$, then*

$$GM_q(S) = 2 + qn - \left\lfloor \frac{2n}{q} \right\rfloor + \left\lfloor \frac{t+n}{q} \right\rfloor.$$

Proof. (1) If $q \leq t + 1$ then, for any $k \in \{t + 1, t + 2, \dots, n - 1\}$ we have $t \geq (k \bmod q)$, and therefore $A = \{t < k \leq n - 1 : q \nmid k\}$. Thus

$$\#A = n - t - \left\lfloor \frac{n}{q} \right\rfloor + \left\lfloor \frac{t}{q} \right\rfloor,$$

and the result follows from Equation (16).

(2) For $t + 2 \leq q \leq n - 1$ we have

$$\{t < k \leq n - 1 : t \geq k \bmod q, q \nmid k\} = \{q + 1, q + 2, \dots, n - 1\}.$$

On the other hand, if $q \mid (k + n)$, then $q \nmid k$ if and only if $q \nmid n$. Moreover, as $\lceil \frac{n-1}{2} \rceil \leq t$ and $t + 2 \leq q \leq n - 1$, we obtain $\frac{n}{2} < q \leq n - 1$ and therefore $q \nmid n$. Thus,

$$\{t < k \leq n - 1 : k \leq qt - n, q \mid (k + n) \text{ and } q \nmid k\} = \{t < k \leq \min\{n - 1, qt - n\} : q \mid (k + n)\}.$$

So,

$$\begin{aligned} A &= \{q+1, q+2, \dots, n-1\} \cup \{t < k \leq \min\{n-1, qt-n\} : q|(k+n)\} \\ &= \{q+1, q+2, \dots, n-1\} \dot{\cup} \{t < k \leq \min\{q, qt-n\} : q|(k+n)\} \end{aligned}$$

and therefore

$$\begin{aligned} \#A &= n-1-q + \max \left\{ 0, \min \left\{ 1 + \left\lfloor \frac{n}{q} \right\rfloor, t \right\} - \left\lfloor \frac{t+n}{q} \right\rfloor \right\} \\ &= n-1-q - \left\lfloor \frac{t+n}{q} \right\rfloor + \max \left\{ \left\lfloor \frac{t+n}{q} \right\rfloor, \min \left\{ 1 + \left\lfloor \frac{n}{q} \right\rfloor, t \right\} \right\}. \end{aligned}$$

(3) Suppose that $n \leq q$. Thus,

$$\{t < k \leq n-1 : t \geq (k \bmod q), q \nmid k\} = \{t < k \leq n-1 : t \geq k, q \nmid k\} = \emptyset.$$

In addition, since $t \neq 1$, we have $qt-n \geq nt-n \geq n > k$ and therefore

$$\{t < k \leq n-1 : k \leq qt-n, q \mid k+n, \text{ and } q \nmid k\} = \{t < k \leq n-1 : q|(k+n)\}.$$

Thus, $A = \{t < k \leq n-1 : q|(k+n)\}$ and

$$\#A = \left\lfloor \frac{2n-1}{q} \right\rfloor - \left\lfloor \frac{t+n}{q} \right\rfloor.$$

The result follows from Equation (16). $\square$

From the proof of Proposition 4.2, we observe that finding a simple closed formula for the Geil-Matsumoto bound becomes more challenging for the semigroup $S = \langle n, n+1, \dots, n+t \rangle$ when $t < \lceil \frac{n-1}{2} \rceil$, as the number of cases grows substantially. Notably, for smaller values of t , the Geil-Matsumoto bound yields more significant improvements over Lewittes' bound. This is exemplified in Figure 1, which compares the two bounds for $n = 15$, $1 \leq q \leq 75$, and $t = 3, 6, 9, 12$. For $t = 9, 12$, we use the formula from Theorem 4.4, whereas for $t = 3, 6$, we apply Theorem 4.1. As the figure shows, the most pronounced improvements arise when t is small.

5. GEIL-MATSUMOTO BOUND AND RATIONAL POINTS ON KUMMER EXTENSIONS

Let $\mathcal{X}$ be the algebraic curve defined over $\mathbb{F}_q$ and given by the affine equation

$$(19) \quad \mathcal{X} : y^m = f(x) = \prod_{k=1}^r (x - \alpha_k)^{\lambda_k}, \quad 1 \leq \lambda_k \leq m-1, \quad \lambda_k \in \mathbb{N},$$

where $m, r \geq 2$, $\text{char}(\mathbb{F}_q) \nmid m$, $f(x) \in \mathbb{F}_q[x]$ is not a d -th power (where d divides m) of an element in $\mathbb{F}_q(x)$, and $\alpha_1, \dots, \alpha_r \in \mathbb{F}_q$ are pairwise distinct elements. Let $\lambda_0 := -\sum_{k=1}^r \lambda_k$ and $\mathbb{F}_q(\mathcal{X}) := \mathbb{F}_q(x, y)$ be the function field of the curve. The field extension $\mathbb{F}_q(\mathcal{X})/\mathbb{F}_q(x)$ is called a Kummer extension. For each $j = 1, \dots, r$, let P_j and P_0 be the places in $\mathbb{F}_q(x)$ corresponding to the zero of $x - \alpha_j$ and the pole of x , respectively. For $0 \leq s \leq r$ such that $(m, \lambda_s) = 1$, let Q_s be the unique place in $\mathbb{F}_q(\mathcal{X})$ lying over P_s .

Regarding rational points on Kummer extensions, Yoo and Lee established an upper bound (the so called YL bound) for algebraic curves of Kummer type. In some of the cases they actually improved Hasse-Weil bound, see [30].

COROLLARY 5.1 ([30, Corollary 4.1]). *Consider a Kummer extension with affine defining equation given by $\mathcal{X} : y^m = f(x)$ as in (19). Then the following bound holds:*

$$|N_q(\mathcal{X}) - (q+1)| \leq \begin{cases} (q-r)(m-1), & \text{if } (m, \lambda_0) = 1, \\ (q+1-r)(m-1), & \text{if } (m, \lambda_0) \neq 1. \end{cases}$$

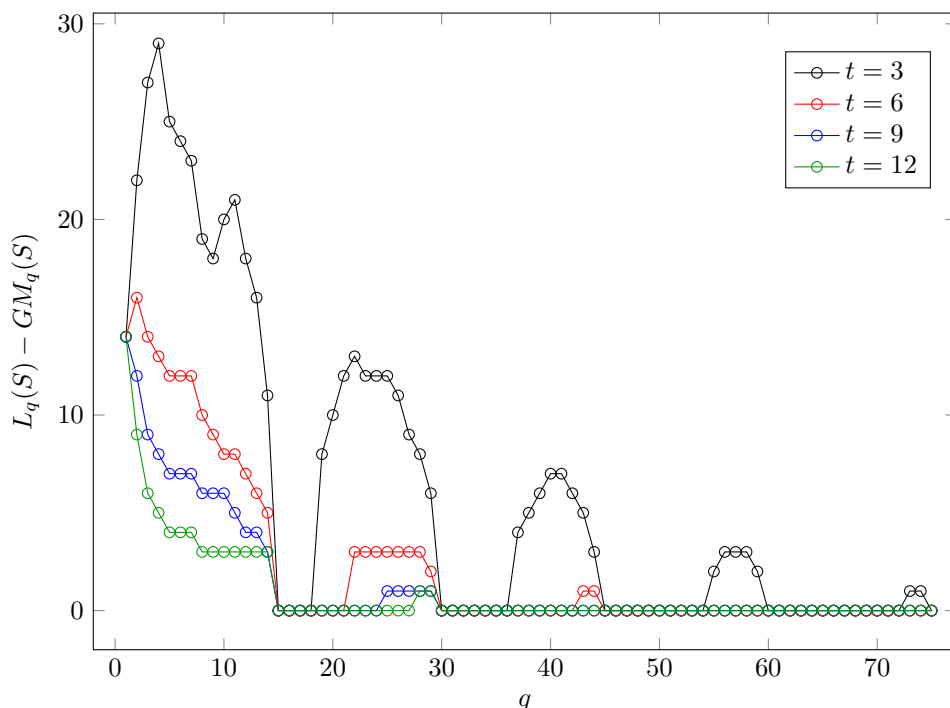


FIGURE 1. Analysis of the improvement of $GM_q(S)$ with respect to $L_q(S)$ for the semigroup $S = \langle n, n+1, \dots, n+t \rangle$, with $n = 15$ and $1 \leq q \leq 75$.

First we provide some examples of algebraic curves over $\mathbb{F}_q$ in which the GM bound given in Theorem 3.3 improves the Lewittes, HWS, YL, and Ihara bounds. To establish this, we require a description of the Apéry set of the Weierstrass semigroup in a point of the curve. For Kummer extensions as defined in (19), Cotterill, Mendoza, and Speziali [8] determined the Apéry set of m in $H(Q_s)$ and a system of generators for $H(Q_s)$ for any $0 \leq s \leq r$ such that $(m, \lambda_s) = 1$. More precisely, they proved the following result.

COROLLARY 5.2 ([8, Corollary 3.9]). *Let $0 \leq s \leq r$ be such that $(m, \lambda_s) = 1$. The Apéry set of m in the Weierstrass semigroup $H(Q_s)$ is given by*

$$\text{Ap}(H(Q_s), m) = \{0\} \cup \{m\beta(i) + t_s(i) : 1 \leq i \leq m-1\},$$

where $\beta(i) = \sum_{k=0}^r \left\lceil \frac{i\lambda_k}{m} \right\rceil - 1$ and $t_s(i) = (i\lambda_s) \bmod m$ for $1 \leq i \leq m-1$. In particular,

$$H(Q_s) = \langle m, m\beta(i) + t_s(i) : 1 \leq i \leq m-1 \rangle.$$

We use this last corollary to identify some cases where the Geil-Matsumoto and Lewittes bounds coincide for Kummer extensions as in (19). From Corollary 5.2, if $\beta(i) \geq 1$ for every $1 \leq i \leq m-1$ and m divides $q-1$, we have $m_{H(Q)} = m$ and, from Proposition 3.1 we conclude $GM_q(H(Q)) = L_q(H(Q))$ for any totally ramified place Q in the extension $\mathbb{F}_q(\mathcal{X})/\mathbb{F}_q(x)$.

Now, from Theorem 3.3 and Corollary 5.2, we construct families of algebraic curves where the Geil-Matsumoto bound outperforms known upper bounds for the number of rational places. Consider the curve over $\mathbb{F}_q$ defined by

$$y^m = (x - \alpha_1)(x - \alpha_2)^{\lambda_2}(x - \alpha_3)^{\lambda_3},$$

where $(m, q) = 1$ and $\alpha_1, \alpha_2, \alpha_3 \in \mathbb{F}_q$ are distinct, and let Q_1 be the rational place of $\mathbb{F}_q(x, y)$ corresponding to $x = \alpha_1$. In Table 1 we compare the GM bound for $H(Q_1)$ against the Lewittes, HWS, YL, and Ihara bounds for various $q, m, \lambda_2, \lambda_3$, demonstrating its improvement in these cases.

In an analogous way, considering a curve over $\mathbb{F}_q$ defined by

$$y^m = (x - \alpha_1)(x - \alpha_2)^{\lambda_2}(x - \alpha_3)^{\lambda_3}(x - \alpha_4)^{\lambda_4},$$

in Table 2 we compare the GM bound for $H(Q_1)$ against the Lewittes, HWS, YL, and Ihara bounds for various $q, m, \lambda_2, \lambda_3, \lambda_4$, demonstrating its improvement in these cases.

q	g	m	λ_2	λ_3	$S := H(Q_1)$	$GM_q(S)$	$L_q(S)$	HWS	YL	Ihara
37	24	27	3	3	$\langle 8, 9, 31 \rangle$	295	297	326	922	299
37	28	32	7	28	$\langle 8, 9 \rangle$	294	297	374	1123	333
37	33	34	3	3	$\langle 10, 11, 34, 39 \rangle$	366	371	434	1160	374
41	21	24	3	3	$\langle 7, 8 \rangle$	287	288	294	916	297
41	31	35	7	31	$\langle 9, 10, 35 \rangle$	367	370	414	1334	386
41	36	40	4	4	$\langle 9, 10 \rangle$	366	370	474	1524	430
79	45	50	9	45	$\langle 10, 11 \rangle$	789	791	845	3853	830

TABLE 1. Improvements with respect to the Lewittes bound (**L**), the HWS bound (**HWS**), the YL bound (**YL**), and the Ihara bound (**Ihara**).

q	g	m	λ_2	λ_3	λ_4	$S := H(Q_1)$	$GM_q(S)$	$L_q(S)$	HWS	YL	Ihara
13	10	10	5	8	8	$\langle 5, 6 \rangle$	64	66	84	104	73
13	15	11	3	6	6	$\langle 7, 9, 11 \rangle$	91	92	119	104	97

TABLE 2. Improvements with respect to the Lewittes bound (**L**), the HWS bound (**HWS**), the YL bound (**YL**), and the Ihara bound (**Ihara**).

We now provide some upper bounds on the number of rational points for curves admitting a rational point with Weierstrass semigroup generated by consecutive integers. In the next result from [6], the authors provided a family of algebraic curves satisfying this property. This family includes the famous Hermitian curve, and more generally curves of type norm-trace, see [11]. The upper bound for the number of rational points on this family of curves will follow straightforward from Theorem 4.4.

THEOREM 5.3 ([6, Theorem 3.4]). *Consider a Kummer extension defined by the algebraic curve $\mathcal{X} : y^m = f(x)$, where $f(x)$ is a separable polynomial of degree $r \geq 2$ and $m = rt + 1$ with $t \geq 1$. If $Q \neq Q_0$ is a totally ramified place of $\mathbb{F}_q(x, y)/\mathbb{F}_q(x)$, then*

$$H(Q) = \langle m - \lfloor m/r \rfloor, m - \lfloor m/r \rfloor + 1, \dots, m \rangle.$$

We establish an upper bound for the number of rational points over $\mathbb{F}_q$ on the curves from Theorem 5.3 by applying Theorem 4.4. The condition on the number of generators in Theorem 4.4 implies that

$$\left\lceil \frac{m - 1 - \lfloor m/r \rfloor}{2} \right\rceil \leq \left\lfloor \frac{m}{r} \right\rfloor \leq m - 1 - \left\lfloor \frac{m}{r} \right\rfloor,$$

which is equivalent to

$$2 \left\lfloor \frac{m}{r} \right\rfloor \leq m - 1 \leq 3 \left\lfloor \frac{m}{r} \right\rfloor.$$

This last inequality holds only for $r = 2$ or 3 . Thus, we can provided the following upper bound for the number of rational points.

PROPOSITION 5.4. *Let $\mathbb{F}_q(\mathcal{X})/\mathbb{F}_q$ be a Kummer extension defined by the algebraic curve $\mathcal{X} : y^m = f(x)$, where $2 \leq m = rt + 1 \leq q - 1$ and $f(x)$ is a separable polynomial of degree $r = 2$ or 3 . Then the number $N_q(\mathcal{X})$ of $\mathbb{F}_q$ -rational points of the curve $\mathcal{X}$ satisfies*

$$N_q(\mathcal{X}) \leq 2 + \frac{q(mr - m + 1)}{r} - \left\lceil \frac{2(mr - m + 1)}{qr} \right\rceil.$$

Proof. We apply Theorem 5.3, item (3) of Theorem 4.4, and the fact that $\left\lfloor \frac{m}{r} \right\rfloor = \frac{m-1}{r}$. $\square$

REFERENCES

- [1] Abdallah Assi, Marco D’Anna, and Pedro A. García-Sánchez, *Numerical semigroups and applications*, second ed., RSME Springer Series, vol. 3, Springer, Cham, [2020] ©2020.
- [2] Peter Beelen and Diego Ruano, *Bounding the number of points on a curve using a generalization of Weierstrass semigroups*, Des. Codes Cryptogr. **66** (2013), no. 1-3, 221–230.
- [3] Maria Bras-Amorós, *Acute semigroups, the order bound on the minimum distance, and the Feng-Rao improvements*, IEEE Trans. Inform. Theory **50** (2004), no. 6, 1282–1289.
- [4] Maria Bras-Amorós, Kwankyu Lee, and Albert Vico-Oton, *New lower bounds on the generalized Hamming weights of AG codes*, IEEE Trans. Inform. Theory **60** (2014), no. 10, 5930–5937.
- [5] Maria Bras-Amorós and Albert Vico-Oton, *On the Geil-Matsumoto bound and the length of AG codes*, Des. Codes Cryptogr. **70** (2014), no. 1-2, 117–125.
- [6] Alonso S. Castellanos, Ariane M. Masuda, and Luciane Quoos, *One- and two-point codes over Kummer extensions*, IEEE Trans. Inform. Theory **62** (2016), no. 9, 4867–4872.
- [7] Alonso S. Castellanos, Erik A. R. Mendoza, and Luciane Quoos, *Weierstrass semigroups, pure gaps and codes on function fields*, Des. Codes Cryptogr. **92** (2024), no. 5, 1219–1242.
- [8] Ethan Cotterill, Erik A. R. Mendoza, and Pietro Speziali, *On gap sets in arbitrary Kummer extensions of $K(x)$* , 2025, <https://arxiv.org/abs/2506.19169>.
- [9] David Eisenbud and Joe Harris, *Existence, decomposition, and limits of certain Weierstrass points*, Invent. Math. **87** (1987), no. 3, 495–515.
- [10] Shalom Eliahou and Jorge Ramírez Alfonsín, *Two-generator numerical semigroups and Fermat and Mersenne numbers*, SIAM J. Discrete Math. **25** (2011), no. 2, 622–630.
- [11] Olav Geil, *On codes from norm-trace curves*, Finite Fields Appl. **9** (2003), no. 3, 351–371.
- [12] Olav Geil and Ryutaroh Matsumoto, *Bounding the number of $\mathbb{F}_q$ -rational places in algebraic function fields using Weierstrass semigroups*, J. Pure Appl. Algebra **213** (2009), no. 6, 1152–1156.
- [13] Rohit Gupta, Erik A. R. Mendoza, and Luciane Quoos, *Reciprocal polynomials and curves with many points over a finite field*, Res. Number Theory **9** (2023), no. 3, article no. 60 (23 pages).
- [14] Emmanuel Hallouin, Philippe Moustrou, and Marc Perret, *Refinements on higher order Weil-Oesterlé bounds via a Serre type argument*, 2025, <https://arxiv.org/abs/2506.05212>.
- [15] 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.
- [16] Nathan Kaplan and Lynnelle Ye, *The proportion of Weierstrass semigroups*, J. Algebra **373** (2013), 377–391.
- [17] J. Komeda, *Non-Weierstrass numerical semigroups*, Semigroup Forum **57** (1998), no. 2, 157–185.
- [18] Joseph Lewittes, *Places of degree one in function fields over finite fields*, J. Pure Appl. Algebra **69** (1990), no. 2, 177–183.
- [19] Erik A. R. Mendoza, *On Kummer extensions with one place at infinity*, Finite Fields Appl. **89** (2023), article no. 102209 (24 pages).
- [20] Harald Niederreiter and Chaoping Xing, *Sequences with high nonlinear complexity*, IEEE Trans. Inform. Theory **60** (2014), no. 10, 6696–6701.
- [21] Gilvan Oliveira and Karl-Otto Stöhr, *Gorenstein curves with quasi-symmetric Weierstrass semigroups*, Geom. Dedicata **67** (1997), no. 1, 45–63.
- [22] J. C. Rosales, *Numerical semigroups with Apéry sets of unique expression*, J. Algebra **226** (2000), no. 1, 479–487.
- [23] J. C. Rosales and P. A. García-Sánchez, *Numerical semigroups generated by intervals*, Pacific J. Math. **191** (1999), no. 1, 75–83.

- [24] J. C. Rosales and P. A. García-Sánchez, *Numerical semigroups*, Developments in Mathematics, vol. 20, Springer, New York, 2009.
- [25] Igor E. Shparlinski, Michael A. Tsfasman, and Serge G. Vladut, *Curves with many points and multiplication in finite fields*, in Coding theory and algebraic geometry (Luminy, 1991), Lecture Notes in Math., vol. 1518, Springer, Berlin, 1992, pp. 145–169.
- [26] Henning Stichtenoth, *Algebraic function fields and codes*, second ed., Graduate Texts in Mathematics, vol. 254, Springer-Verlag, Berlin, 2009.
- [27] Fernando Torres, *On certain N -sheeted coverings of curves and numerical semigroups which cannot be realized as Weierstrass semigroups*, Comm. Algebra **23** (1995), no. 11, 4211–4228.
- [28] S. G. Vláduts and V. G. Drinfel'd, *The number of points of an algebraic curve*, Funktsional. Anal. i Prilozhen. **17** (1983), no. 1, 68–69.
- [29] Chaoping Xing and Sze Ling Yeo, *Algebraic curves with many points over the binary field*, J. Algebra **311** (2007), no. 2, 775–780.
- [30] Jinjoo Yoo and Yoonjin Lee, *Improvements of the Hasse-Weil-Serre bound over global function fields*, Finite Fields Appl. **101** (2025), article no. 102538 (26 pages).
- [31] Qin Yuan, Chunlei Li, Xiangyong Zeng, Tor Helleseeth, and Debiao He, *Further investigations on nonlinear complexity of periodic binary sequences*, IEEE Trans. Inform. Theory **70** (2024), no. 7, 5376–5391.

ADLER MARQUES, Universidade Federal do Rio de Janeiro, Instituto de Matemática, Cidade Universitária, CEP 21941-909, Rio de Janeiro, Brazil
E-mail : adler@im.ufrj.br

ERIK MENDOZA, Universidade Federal do Rio de Janeiro, Instituto de Matemática, Cidade Universitária, CEP 21941-909, Rio de Janeiro, Brazil
E-mail : erik@im.ufrj.br

LUCIANE QUOOS, Instituto de Matemática, Universidade Federal do Rio de Janeiro, Cidade Universitária, CEP 21941-909, Rio de Janeiro, Brazil
E-mail : luciane@im.ufrj.br

GUILHERME TIZZIOTTI, Instituto de Matemática e Estatística, Universidade Federal de Uberlândia, Campus Santa Mônica, CEP 38400-902, Uberlândia, Brazil
E-mail : guilhermect@ufu.br