Electronic Colloquium on Computational Complexity, Report No. 174 (2025)

Tracing AG Codes: Toward Meeting the Gilbert–Varshamov Bound

Gil Cohen* Dean Doron† Noam Goldgraber‡ Tomer Manket§

Abstract

One of the oldest problems in coding theory is to match the Gilbert–Varshamov bound with explicit binary codes. Over larger—yet still constant-sized—fields, algebraic-geometry codes are known to beat the GV bound. In this work, we leverage this phenomenon by taking traces of AG codes. Our hope is that the margin by which AG codes exceed the GV bound will withstand the parameter loss incurred by taking the trace from a constant field extension to the binary field. In contrast to concatenation, the usual alphabet-reduction method, our analysis of trace-of-AG (TAG) codes uses the AG codes' algebraic structure throughout – including in the alphabet-reduction step.

Our main technical contribution is a Hasse–Weil–type theorem that is well-suited for the analysis of TAG codes. The classical theorem (and its Grothendieck trace-formula extension) are inadequate in this setting. Although we do not obtain improved constructions, we show that a constant-factor strengthening of our bound would suffice. We also analyze the limitations of TAG codes under our bound and prove that, in the high-distance regime, they are inferior to code concatenation. Our Hasse–Weil–type theorem holds in far greater generality than is needed for analyzing TAG codes. In particular, we derive new estimates for exponential sums.

*Tel Aviv University. gil@tauex.tau.ac.il. Supported by ERC starting grant 949499 and by the Israel Science Foundation grant 2989/24.

†Ben Gurion University. deand@bgu.ac.il. Supported in part by NSF-BSF grant 2022644.

‡Ben Gurion University and Tel Aviv University. goldgrab@post.bgu.ac.il. Supported by NSF-BSF grant 2022644.

§Tel Aviv University. tomermanket@mail.tau.ac.il. Supported by ERC starting grant 949499.

ISSN 1433-8092

Contents

1 Introduction

The study of the tradeoff between rate and distance is as old as coding theory itself, dating back to the late 1940s and early 1950s. Gilbert [Gil52] proved the existence of codes with distance δ and rate $\rho \geq 1 - H_2(\delta)$, and Varshamov [Var57] subsequently proved that such codes can be taken to be linear. Naturally, the ultimate goal is to achieve *explicit* constructions, and indeed much effort has focused on obtaining efficiently encodable codes with a good rate-vs.-distance tradeoff.

For binary codes, notable early constructions include Justesen's code [Jus72], the first explicit construction to get constant rate and constant relative distance, and expander-based codes [Tan82, SS02], which further enjoy very efficient decoding. The large distance regime, $\delta = 1/2 - \varepsilon$, has been the subject of extensive and fruitful research over the past decades, in part due to its importance in complexity theory via its relation to small-bias sets. The GV bound guarantees the existence of codes with such δ and rate $\Omega(\varepsilon^2)$. Earlier explicit constructions achieved suboptimal rates [AGHP92, NN93, BT13], but a breakthrough construction of Ta-Shma attained nearly optimal rate $\varepsilon^{2+o(1)}$ via a sophisticated expander-based bias-reduction technique [Ta-17]. Progress toward the GV bound in the regime where δ is bounded away from $\frac{1}{2}$ has been comparatively limited.

Constructing codes over large alphabets has proved easier, particularly with respect to the rate–distance tradeoff. Reed–Solomon codes are the prototypical example: they attain the optimal tradeoff by meeting the Singleton bound with alphabet size equal to the block length. Consequently, a particularly useful tool for constructing codes over small alphabets is *code concatenation*, which reduces the alphabet size by combining large-alphabet outer codes with short, small-alphabet inner codes, yielding arbitrarily long codes over a small alphabet. Importantly, in the $\delta = 1/2 - \varepsilon$ regime, several constructions are concatenation-based (say, [AGHP92, BT13]), and in particular, one can show that concatenating optimal AG codes with the Hadamard code yield codes of rate $\Omega(\varepsilon^3)$.

Remarkably, the GV bound is suboptimal for sufficiently large constant alphabets. A major line of research, initiated by Goppa's 1981 introduction of algebraic-geometry (AG) codes [Gop81], constructs codes from algebraic curves over finite fields. This approach laid the foundation for the breakthrough of Tsfasman, Vlăduţ, and Zink [TVZ82], who proved that for sufficiently large fields (e.g., already over $\mathbb{F}_{49}$), AG codes can asymptotically achieve a rate–distance tradeoff exceeding the GV bound. Their result relies on families of curves with many rational points relative to their genus. Subsequently, Garcia and Stichtenoth [GS95, GS96] constructed explicit recursive towers of function fields attaining the Drinfel'd-Vlăduţ [VD83] upper bound on the number of rational points, thereby providing explicit families of AG codes that meet the Tsfasman–Vlăduţ-Zink bound in a

fully constructive way. Moreover, as the field size increases, the quantitative improvement becomes more pronounced, and the range of parameters for which the GV bound can be exceeded broadens accordingly.

1.1 Our Approach: Trace-Based Alphabet Reduction for AG Codes

Inspired by the work of Kopparty, Ta-Shma, and Yakirevitch [KTY24] and by a talk of Ta-Shma at the Simons Institute (Berkeley) [Ta-24], this paper studies a family of explicit constructions over constant-size fields that aim to meet—or even surpass—the GV bound, with a particular focus on binary codes. Our primary technical contribution is to develop tools for analyzing these candidate constructions and for understanding their limitations. The resulting statements are general and extend beyond the original motivation, with potential further applications.

Our idea is simple: we aim to leverage the underlying algebraic structure of AG codes—which enables them to beat the GV bound—in the alphabet-reduction step as well. The hope is that, by exploiting this structure, the reduction will not substantially compromise the excellent rate–distance tradeoff of the original AG code. In its most basic form, the alphabet-reduction method we propose applies the field trace to each coordinate of every codeword. While this is the variant we focus on in this work, we view it as a special case within a broader family of constructions whose common feature is the aforementioned strategy of leveraging structure for alphabet reduction.

This approach is, in a sense, an antithesis of the off-the-shelf technique of the black-box analysis of code concatenation. The latter ignores the code's internal structure: the rate and distance of the resulting code are simply the products of the corresponding parameters of the outer and inner codes (see Section 3). One can hope to get better guarantees by exploiting additional, more complicated, structure.[1]

Concatenation is reminiscent of other composition-type primitives, such as the zig–zag product in expander-graph constructions, where the roles of rate and distance are played by the graph's degree and spectral expansion. In contrast, exploiting more of the underlying structure—in the graph setting, the entire spectrum—yields stronger, and in fact optimal, analyses [CCM24].

Of course, this is not the first work to consider trace codes: they have been studied for decades, most notably since Delsarte [Del75], who established their connection to subfield

[1]We note that while our trace code approach is inherently "non black-box", there have been few attempts at exploiting structure in concatenation-based construction, most recently in [DMW24], with a similar goal of attaining the GV bound.

subcodes and, in particular, to dual BCH codes. Trace codes of AG codes have likewise been investigated since the 1990s (e.g., [vdV91, Sko91, LC16] and subsequent works). However, the aspects examined in that literature, largely motivated by the analysis of BCH and cyclic codes, are of limited relevance to our goals here. The papers by Kopparty, Ta-Shma, and Yakirevitch [KTY24, KTY25] as well as an earlier paper by Vlăduţ [Vla96] are the most relevant to our work. We discuss Vlăduţ's work in Section 2.2.

To clarify the challenges in analyzing trace codes of AG codes and to place our technical results in context, we must first turn to describe the simplest case: the trace of Reed–Solomon codes. This (by now standard) analysis exposes the intimate relationship between taking traces of codes and the geometry of algebraic curves. It also shows why existing techniques, while effective for Reed–Solomon codes, fall short for trace codes of general AG codes. With this perspective, we present our main result, which constitutes a first step toward overcoming these obstacles.

Concurrent work. In concurrent, independent work, Kopparty, Ta-Shma, and Yakirevitch [KTY25] also study trace codes of AG codes, focusing on the Hermitian function field; this extends their earlier paper [KTY24], which inspired the present work. We give a technical comparison with [KTY24, KTY25] after presenting our results (see Section 2.3).

1.2 Trace Codes of Reed–Solomon: Analysis via the Hasse–Weil Theorem

We recall that a Reed–Solomon (RS) code over $\mathbb{F}_q$ is defined by identifying messages with polynomials $f \in \mathbb{F}_q[x]$ of degree $< k$ and evaluating them at distinct field elements. Specifically, for evaluation points $\mathfrak{p}_1, \ldots, \mathfrak{p}_n \in \mathbb{F}_q$ (with $n \le q$), the codeword corresponding to f is $(f(\mathfrak{p}_1), \ldots, f(\mathfrak{p}_n))$. Let p denote the characteristic of $\mathbb{F}_q$, and write $q = p^m$. The trace code of the Reed–Solomon code is obtained by applying the (absolute) field trace Tr to each coordinate. Thus the encoder maps $\mathbb{F}_q^k \to \mathbb{F}_p^n$ via

$$f \longmapsto \big(\mathsf{Tr}(f(\mathfrak{p}_1)), \ldots, \mathsf{Tr}(f(\mathfrak{p}_n))\big), \tag{1.1}$$

where $\mathsf{Tr}(x) = x + x^p + \cdots + x^{p^{m-1}}$. Note that the resulted code is $\mathbb{F}_p$-linear. As it stands, as long as the encoder is injective, the rate of the code is

$$\rho = \frac{k \log q}{n \log p} = \frac{mk}{n}, \tag{1.2}$$

which is a factor-m improvement over the rate of the underlying RS code. We now turn to the distance analysis, which is more challenging.[2]

Fix a polynomial $f \in \mathbb{F}_q[x]$ of degree $t < k$. Using Hilbert's Theorem 90, it can be shown that the number of zeros z_f in the codeword corresponding to f in Equation (1.1) is related to the number of pairs $(x, y) \in \mathbb{F}_q^2$ satisfying

$$y^p - y = f(x), \tag{1.3}$$

that is, to the number of $\mathbb{F}_q$-rational points n_f on this curve. More precisely, we have that

$$z_f \leq \frac{n_f}{p}, \tag{1.4}$$

and equality holds when $n = q$. Therefore, analyzing the distance of the trace code is *equivalent* to counting points on curves, one curve for each message f.

Counting points on curves over finite fields is a difficult task. A deep and powerful result, the Hasse–Weil theorem (see [Sti09, Chapter 5]), provides a bound on the number of points. We will discuss the Hasse–Weil theorem in more depth later on; for now it suffices to note that in our current setting, where the curve has the form of Equation (1.3), the theorem implies that the number of $\mathbb{F}_q$-rational points n_f satisfies

$$|n_f - (q+1)| \leq (t-1)(p-1)\sqrt{q}. \text{ [3]} \tag{1.5}$$

Combining this with Inequality (1.4), we readily obtain a bound on the distance. Assuming, for simplicity, that we evaluate over all field elements (i.e., $n = q$), we get

$$\delta \geq 1 - \frac{1}{p} - \frac{1}{np} - \frac{p-1}{p} \cdot \frac{k-2}{\sqrt{n}} \geq 1 - \frac{1}{p} - \frac{k}{\sqrt{n}}.$$

Since one cannot expect a distance better than $1 - \frac{1}{p}$, we see that the "loss" term is $\frac{k}{\sqrt{n}}$. This, in particular, means that to obtain a nontrivial bound on the distance we must take $k = O(\sqrt{n})$, which forces the rate to vanish at an inverse–square-root rate, $\rho = O\left(\frac{1}{\sqrt{n}}\right)$.

The above construction extends naturally to trace codes of AG codes, and this is what we undertake in the following sections. However, the distance analysis based on the

[2] As it turns out, analyzing the distance will require a slight tweak to the construction, incurring a small loss in the rate computed in Equation (1.2).

[3] To be precise, for some polynomials f the Hasse–Weil theorem does not apply: If f can be written as $f(x) = g(x)^p - g(x)$ for some polynomial $g(x)$, then the number of solutions of Equation (1.3) is $q \cdot p$, yielding a trivial bound on the number of zeros. To circumvent this, we require the degree t of f to be coprime to p. This accounts for the rate loss mentioned above, namely a multiplicative $(1 - \frac{1}{p})$ factor relative to Equation (1.2).

Hasse–Weil bound does not carry over. This motivates our results, and in particular our main theorem: a Hasse–Weil–type bound suitable to the analysis of trace codes of AG codes, which yields a meaningful lower bound on their distance.

To keep this introductory section accessible, we continue to assume no prior knowledge of algebraic function fields. As a result, this section has an expository flavor, while the formal treatment appears later in the technical sections. In particular, in Section 1.3 we provide a brief, informal introduction to algebraic curves.

1.3 A Brief Introduction to Algebraic Curves

Informally, an algebraic curve over a finite field $\mathbb{F}_q$ is the set of points in $\mathbb{F}_q^m$ satisfying $m-1$ independent polynomial equations. A good example to have in mind is the Hermitian plane curve over a field of size $q = r^2$, consisting of all points $(x, y) \in \mathbb{F}_q^2$ satisfying $y^r + y = x^{r+1}$. It is not hard to show that this curve has $r^3 + 1 = q^{3/2} + 1$ points. In general, the number of points n on a curve is a key parameter; in the coding-theoretic context, it governs the block length of the associated code, as we shall see. Generally, these points are denoted by $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$.

AG codes are obtained by evaluating functions on a fixed curve. The notion of a function on a curve is somewhat delicate. For example, on the Hermitian curve the two polynomials y^r and $x^{r+1} - y$, although different as formal polynomials, are identical as functions, since they agree on all points of the curve. Nonetheless, there is a notion analogous to the *degree* of a function irrespective of its representation as a polynomial. As with polynomials, this notion of degree bounds the number of zeros a function may have on the curve. Moreover, the set of all functions of degree at most k forms an $\mathbb{F}_q$-vector space.

Given a curve, we associate the corresponding AG code in a manner analogous to the Reed–Solomon code. We fix a degree k and identify the messages with the subspace of functions of degree at most k. The codeword corresponding to such a function f is obtained by evaluating f at all points on the curve, $(f(\mathfrak{p}_1), \ldots, f(\mathfrak{p}_n)) \in \mathbb{F}_q^n$.

A second important parameter is the curve's *genus*. This natural number, denoted by g, is a measure of the curve's complexity. We will not give a formal definition of the genus here, but rather adopt the following operative perspective. The Hasse–Weil theorem mentioned above is fundamental in the study of algebraic curves over finite fields; it is, in fact, the proof of the Riemann Hypothesis over finite fields. We will discuss the theorem itself later; however, an important corollary—referred to here as the Hasse–Weil bound—

states that the number of points n on a curve of genus g satisfies

$$|n - (q+1)| \leq 2\sqrt{q} \cdot g.$$

From this result we deduced Inequality (1.5).[4] Thus, the smaller the genus, the better the bound on the number of points on the curve. That is, we view the genus as the parameter that controls $|n - (q+1)|$ (up to the factor $2\sqrt{q}$).

1.4 TAG Codes

With the concepts in Section 1.3 in place, we are ready to give an informal definition of trace codes of AG codes (TAG codes, for short). Fix an algebraic curve over a finite field $\mathbb{F}_q$ of characteristic p, choose n points $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$, and identify the message space with functions of degree less than k. As in (1.1), we map a message f by

$$f \longmapsto \big(\mathsf{Tr}(f(\mathfrak{p}_1)), \ldots, \mathsf{Tr}(f(\mathfrak{p}_n))\big) \in \mathbb{F}_p^n. \tag{1.6}$$

As in the analysis of the trace of RS codes in Section 1.2, here too there is a precise relation between the number of zeros z_f in the codeword corresponding to f and the number of points on a certain curve. This time, the latter curve depends on both the original curve and the function f. In particular, analogously to Equation (1.3), if the original curve lies in an ambient space of dimension m, then the new curve we consider lies in an ambient space of dimension $m+1$, and in addition to the $m-1$ polynomial relations among $x_1, \ldots, x_m$ dictated by the original curve, we have the relation

$$x_{m+1}^p - x_{m+1} = f(x_1, \ldots, x_m). \tag{1.7}$$

Analogously to Inequality (1.4), there is an exact relation between the number of points n_f on the new curve and n, the number of points on the original curve. It takes a slightly less simple form, which is quantitatively almost identical; for simplicity, in this informal section we will use the same relation as before, namely,

$$z_f = \frac{n_f}{p}. \tag{1.8}$$

Recall that, to analyze the distance of the trace of RS codes, we relied on the Hasse–Weil bound as stated in Inequality (1.5). Looking more closely at that equation, the term q counts the number of points on the base curve underlying the Reed–Solomon code, namely the line over $\mathbb{F}_q$. The Hasse–Weil bound controls the difference between the

[4] The reason it is $q+1$ rather than q is that, in this context, curves are taken to be projective rather than affine, so one additional "point at infinity" is included.

number of points on the base curve and the number of points on the new curve. The bound in Inequality (1.5) is in terms of the genus of the new curve. What should the bound be in the case of TAG codes? There are now two genera involved: the genus of the curve defining the code, denoted by g, and the genus of the new, extended curve, denoted by g_f. In the original case, since the genus of the line is 0, it made no appearance in the Hasse–Weil bound. There is a sense in which the $\sqrt{q}$ appearing in the Hasse–Weil bound provides the natural "units" for measuring the number of points, independent of whether we extend the line or another curve (see Section 2.2). Thus, it is conceivable that the difference of genera should be used in the bound. Indeed, the general result in this context is Grothendieck's trace formula [Gro77] which states exactly this; namely, it yields the bound

$$|n_f - n| \leq 2\sqrt{q} \cdot (g_f - g). \tag{1.9}$$

Unfortunately, this bound, which is tight in general, doesn't give any nontrivial bounds on the distance of TAG codes. To see why, we rely on two results from the theory of algebraic curves. First, there is a formula relating the genus g_f of the extended curve and the genus g of the base curve, known as the Hurwitz genus formula. For our introductory purposes it suffices to say that

$$g_f = pg + \Delta, \tag{1.10}$$

where $\Delta \geq 0$ is an integer. [5] Hence, the bound given by Inequality (1.9) is at least $2\sqrt{q}\,(p-1)g$.

The second result is the Drinfeld–Vlăduţ bound [VD83], which, informally, states that asymptotically, as the genus of the curve tends to infinity, we have

$$\frac{n}{g} \leq \sqrt{q} - 1. \tag{1.11}$$

Combining this with the calculation above shows that the bound in Inequality (1.9) is worse than $2(p-1)n$. Consequently, the resulting upper bound on n_f is no better than $(2p-1)n$. Together with Equation (1.8), this yields an upper bound of $\frac{(2p-1)n}{p}$ on the number of zeros in a codeword, which is trivial since this quantity exceeds n.[6]

As discussed above, a distance analysis for TAG codes demands estimates stronger than those yielded by Grothendieck's trace formula. This is the main technical contribution of the present work. In the next section we state our main result and its applications to the analysis of TAG codes, as well as its broader consequences.

[5] For readers familiar with algebraic function fields, Δ is the degree of the Different divisor of the corresponding function field extension.

[6] We remark that even a bound of the form $\sqrt{q}\,(g_f - g)$ in Inequality (1.9)—which may be obtainable asymptotically—still does not yield a nontrivial distance bound.

2 Our Results

As discussed in Section 1.4, the issue with Grothendieck's trace formula for analyzing the distance of TAG codes is that the upper bound it yields for $|n_f - n|$ depends too heavily on the genus g of the underlying curve. In other words, regardless of how simple the extension is (equivalently, regardless of the degree t of f), the bound is too loose when the underlying function field is of large genus. Indeed, the degree of f is encoded in Δ, and the previous section showed that even if the contribution of Δ to the bound is ignored, one still does not obtain a meaningful bound on the distance. Thus, we seek a bound that depends on the complexity of the *extension* as captured by Δ, rather than on how complex is the base curve, as encoded by the genus g. More precisely, one can show that $\Delta = \Theta(pt)$, and in particular it can be taken significantly smaller than the genus g.

A bound of the form

$$|n_f - n| \;=\; \Phi(\Delta)\,\sqrt{q}, \tag{2.1}$$

for some function Φ (e.g., linear in Δ) is most desirable, as it is completely independent of the genus g. Our main technical contribution is a step toward such a result, in which the bound we obtain is the *geometric mean* of Δ (the quantity we wish to appear in the bound) and the genus g, which by itself is too large.

For the analysis of TAG codes we only need to consider specific types of extensions, as in Equation (1.7). Such extensions are called Artin–Schreier extensions. Our result, however, holds in much greater generality. In this introductory section we choose to be somewhat informal and consider only the special case required for analyzing TAG codes.

Theorem 2.1 (main result; informal)**.** *Let $\mathbb{F}_q$ be a finite field of characteristic p. Let C be a "nice" curve over $\mathbb{F}_q$ with genus g and n points. Let f be a "nice" function on C of degree t, and define the curve C_f by the additional polynomial constraint $y^p - y = f$, where y is a new formal variable. Then the number of points n_f on the curve C_f satisfies*

$$|n_f - n| = O\big(p^2\sqrt{tg}\sqrt{q}\big)\,. \tag{2.2}$$

In fact, the result also extends to Kummer extensions and, more generally, to extensions of the form $\phi(y) = f$ for an arbitrary polynomial ϕ, as formalized in Proposition 5.3. The theorem further applies to even more general extensions under technical conditions—hidden in the two "nice" instances highlighted in the informal Theorem 2.1. For the complete, formal statement, see Theorem 5.6.

2.1 Implications for Error Correcting Codes

As discussed in Section 1.4, an upper bound on n_f directly translates into a lower bound on the weight of the codeword corresponds to f in the TAG construction. In this section, we examine the resulting codes parameters and highlight the limitations of this approach.

2.1.1 The Hermitian TAG code

In this section, we illustrate Theorem 2.1 by giving an explicit instantiation of TAG codes based on the Hermitian curve introduced in Section 1.3. Let $r = p^\ell$ be a power of a prime p, and let $q = r^2$. Let $A \subseteq \mathbb{F}_q \times \mathbb{F}_q$ be the set of roots of the polynomial $y^r + y - x^{r+1}$. For $T \geq 0$, let

$$\begin{aligned} B = \{(i,j) \in \mathbb{N} \times \mathbb{N} : & \; ir + j(r+1) \leq T, \\ & \; i \text{ is odd and } j \text{ is even}, \\ & \; j < r/6\}. \end{aligned} \tag{2.3}$$

The Hermitian TAG code is defined by

$$\mathcal{C} = \left\{ \left(\mathsf{Tr}\left(\sum_{(i,j)\in B} c_{i,j} \alpha^i \beta^j \right) \right)_{(\alpha,\beta)\in A} \; : \; c_{i,j} \in \mathbb{F}_q \right\}.$$

The following theorem specifies the parameters of this code; the formal statement appears in Theorem 7.2.

Theorem 2.2 (Hermitian TAG codes; informal)**.** *The Hermitian TAG code with message length k and relative distance $1/2 - \varepsilon$ has block length*

$$n = O\left(\frac{k}{\varepsilon^4}\right)^{3/2}.$$

In fact, the result shows that the Hermitian TAG code not only has relative distance $\frac{1}{2} - \varepsilon$ but is actually ε-*balanced*: every nonzero codeword has relative Hamming weight in $[\,\frac{1}{2} - \varepsilon, \frac{1}{2} + \varepsilon\,]$. In Section 7, we further instantiate our results for additional curves—specifically the Hermitian tower of function fields and the norm–trace function field—obtaining ε-balanced codes with varying parameter trade-offs.

2.1.2 The high distance regime: TAG codes vs. concatenation

As our case studies in Section 7 show, in the regime $\delta = \frac{1}{2} - \varepsilon$ all the TAG codes we consider are still far from the GV bound, requiring $n = \omega\left(\frac{k}{\varepsilon^2}\right)$. This prompts the question: does there exist a curve for which the corresponding TAG code matches the GV bound?

In Section 8 we present strong evidence for a negative answer. We show that, when analyzed using our bound from Theorem 2.1, in the high-distance regime $\delta = \frac{1}{2} - \varepsilon$, TAG codes instantiated from a given AG code are outperformed by concatenating the same AG code with Hadamard. This remains true even under a bound of the form Equation (2.1) with $\Phi(\Delta)$ that is linear in Δ. In particular, we establish the following.

Theorem 2.3. *Assume the bound given by Equation (2.1) is tight up to a constant. Then, any TAG code with rate k and relative distance $1/2 - \varepsilon$ has block length*

$$n = \Omega\left(\frac{k}{\varepsilon^3}\right).$$

Moreover, assuming the bound given in Theorem 2.1 is tight up to a constant, $n = \Omega(k/\varepsilon^6)$.

2.1.3 The constant distance regime

As implied by Section 2.1.2, under our analysis, attaining the GV bound requires operating in the regime where the distance δ is bounded away from $\frac{1}{2}$. To approach the GV bound in this regime, we must have a nonvanishing rate. In this short section, we examine the implications for the parameters of the underlying AG code.

For a curve C, let $\ell(T)$ denote the dimension of the vector space of functions on C of degree less than T. Assume that Theorem 2.1 applies to every function in this space, and let $\mathcal{C}$ be the resulting TAG code. By Equation (2.2) together with Equation (1.8), the encoding of a function f of degree t is nonzero provided the right-hand side is $< (p-1)\,n$.

For simplicity, assume the implicit constant hidden in the big-O of Equation (2.2) is 1, and that $n/g = \sqrt{q} - 1$ (the optimal AG-code guarantee). To obtain a nontrivial bound on the number of zeros of f, we require

$$p^2\sqrt{tg}\,\sqrt{q} < pn,$$

which is equivalent (since $n = g(\sqrt{q} - 1)$) to

$$t < \frac{g}{p^2}\left(1 - \frac{1}{\sqrt{q}}\right)^2.$$

Hence, to apply our result we must work in the regime $T < g/p^2$. The resulting TAG code $\mathcal{C}$ has rate

$$\rho \;=\; \frac{\ell(T)\,\log_p(q)}{n}.$$

Since $\ell(T) \le T \le g/p^2$ and $n = (\sqrt{q} - 1)g$, we obtain

$$\rho \;=\; \frac{\log_p(q)}{\sqrt{q} - 1} \cdot \frac{\ell(T)}{g} \;\le\; \frac{\log_p(q)}{(\sqrt{q} - 1)\,p^2}.$$

Thus, to obtain a family with constant rate, we must fix q and choose curves (and $T \leq g/p^2$) so that $\ell(T) = \Omega_q(g)$.

This is a somewhat nonstandard regime for AG codes. Typically one works with functions of degree at least $2g$, where Riemann–Roch guarantees linear growth of $\ell(T)$ (indeed, $\ell(T) = T + 1 - g$ for $T \geq 2g - 1$). In particular, among degrees up to $(1 + \alpha)g$ one obtains at least αg attainable degrees. By contrast, working below g is subtler: the attainable sub-g degrees—the *Weierstrass non-gaps*—depend on the curve. In our TAG setting, one must therefore understand this sub-g regime.

A property closely related to the latter was examined in [BT13, Section 4.1]. However, we are not aware of any optimal family of function fields exhibiting this behavior. For instance, in [YH19], the authors show that certain Riemann–Roch spaces on the Garcia–Stichtenoth tower do not satisfy this property. We formalize this as an open problem.

Open Problem 2.4. *Does there exist a prime power $q = p^\ell$ and a family of function fields $F_i/\mathbb{F}_q$ with $\frac{n_i}{g_i} = \Theta_q(1)$, such that each F_i of genus g_i contains a Riemann–Roch space $\mathcal{L}_i$ of degree $T_i \leq \frac{g_i}{p^2}$ satisfying $\ell_i(T_i) = \Omega_q(g_i)$?*

2.1.4 Limitations and consequences of improving the bound

In Section 2.1.3, we assumed that the constant appearing in the error term in Equation (2.2) is equal to 1. Suppose instead that we could obtain a small constant $0 < c < 1$ such that, for every "nice" function f of degree t, the bound

$$n_f \leq n + cp^2\sqrt{tg}\sqrt{q}$$

holds. If a β-fraction of all functions of degree up to T would be "nice", then the resulting TAG code would have rate and relative distance, correspondingly,

$$\rho = \beta \cdot \frac{\log_p q}{\sqrt{q} - 1} \cdot \frac{\ell(T)}{g},$$
$$\delta \geq 1 - \frac{1}{p} - c \cdot \frac{p\sqrt{gT}\sqrt{q}}{n}.$$

Taking $T = 2g$, the Riemann–Roch theorem gives $\ell(T) = g + 1$. We then have

$$\rho \geq \beta \cdot \frac{\log_p q}{\sqrt{q} - 1},$$
$$\delta \geq 1 - \frac{1}{p} - cp\frac{\sqrt{2q}}{\sqrt{q} - 1}.$$

From this we see that if our bound were sharpened by reducing the leading constant, TAG codes would work in the usual AG regime (e.g., for degrees $\geq 2g - 1$) and could lead

to better code parameters. Note that the constant c cannot be taken arbitrarily small; doing so would violate the MRRW linear-programming upper bounds [MRRW77]. This offers an unusual direction of inference: using coding-theoretic limits to deduce statements about algebraic curves.

2.2 Exponential Sums over Curves

Exponential sums over finite fields play a central role in number theory and algebraic geometry. A. Weil was the first to observe a deep connection between exponential sums of polynomials and Artin–Schreier covers. Specifically, for a polynomial $f(x)$ of degree d over $\mathbb{F}_q$ such that $f \neq u^p - u$ for all $u \in \overline{\mathbb{F}_q}(x)$, the exponential sum

$$S(f) = \sum_{\alpha \in \mathbb{F}_q} e^{\frac{2\pi i}{p} \mathsf{Tr}(f(\alpha))} \tag{2.4}$$

can be expressed as $S(f) = \omega_1 + \cdots + \omega_D$, where the ω_i are a subset of the reciprocals of the roots of the zeta function of the Artin–Schreier curve

$$y^p - y = f(x).$$

Weil also showed that if $\deg f$ is relatively prime to p, then $D = d - 1$. Combined with his proof of the Riemann Hypothesis for curves over finite fields, which asserts that each ω_i satisfies $|\omega_i| = \sqrt{q}$, this yields the bound

$$|S(f)| \leq (d-1)\sqrt{q}.$$

In 1966, Bombieri [Bom66, Theorem 5] extended Weil's results from polynomials to general rational functions defined over algebraic curves.

Theorem 2.5 ([Bom66], Theorem 5)**.** *Let C be a complete, irreducible, non-singular curve of genus g over $\mathbb{F}_q$, which contains n points. Let $f \in \mathbb{F}_q(C)$ be a function on C such that $f \neq u^p - u$ for all $u \in \overline{\mathbb{F}_q}(C)$. Let $\mathcal{P}$ be the set of poles of f. Then the exponential sum*

$$S(f) = \sum_{\mathfrak{p} \in C \setminus \mathcal{P}} e^{\frac{2\pi i}{p} \mathsf{Tr}(f(\mathfrak{p}))}, \tag{2.5}$$

can be expressed as

$$S(f) = \omega_1 + \cdots + \omega_D, \tag{2.6}$$

where $|\omega_i| = \sqrt{q}$ for all $1 \leq i \leq D$, and

$$D \leq 2g - 2 + |\mathcal{P}| + \deg(f).$$

Moreover, if f has a single pole of degree relatively prime to p, then $D = 2g - 1 + \deg(f)$.

Corollary 2.6 ([Bom66])**.** *In the setting of Theorem 2.5, we have*

$$|S(f)| \leq (2g - 1 + \deg(f))\sqrt{q}.$$

Note that a trivial bound $|S(f)| \leq n - |\mathcal{P}|$ follows directly from Equation (2.5). Hence, the bound in Corollary 2.6 is non-trivial only when

$$(2g - 1 + \deg(f))\sqrt{q} < n - |\mathcal{P}|. \tag{2.7}$$

Corollary 2.6 was used in [LC16] to compute the dimension of certain TAG codes defined over curves for which Inequality (2.7) holds.

There is a major limitation of Bombieri's bound in our setting: If the curve C satisfies $2g\sqrt{q} \geq n$, then the bound becomes trivial for any function on the curve. By the Drinfeld–Vlăduţ bound, Inequality (1.11), this inequality holds for all curves of sufficiently large genus. Since such curves are precisely those used in AG codes constructions, Bombieri's bound is not applicable in this regime.

In [Vla96], Vlăduţ proves nontrivial bounds for the case of Hermitian and Hansen–Stichtenoth curves, showing that for certain functions f of bounded degree one has $S(f) \leq cn$ for some constant $0 < c < 1$. Our results provide new bounds on exponential sums of functions over curves of large genus, yielding in particular that $S(f) = o(n)$ for functions f of degree $o(g)$.

Theorem 2.7 (exponential sums; informal)**.** *Let $\mathbb{F}_q$ be a finite field of characteristic p. Let C be a "nice" curve over $\mathbb{F}_q$ with genus g and n rational points, and let f be a "nice" function on C of degree t. Then,*

$$S(f) = O\left(p^3\sqrt{tg}\sqrt{q}\right).$$

The reader is referred to Theorem 6.4 for the formal statement. Interestingly, in conjunction with Theorem 2.5, this implies that the complex roots ω_i, each of absolute value $\sqrt{q}$, cannot be all in the same direction.

Note that this bound remains meaningful even for families of curves with $g \to \infty$. However, since $g\sqrt{q} = \Theta(n)$, as in Section 2.1.3, the function f must satisfy $t \ll g$ for the bound to be non-trivial.

2.3 Comparison with [KTY24, KTY25]

In this section, we compare our results with those obtained in an earlier work by Kopparty, Ta-Shma, and Yakirevitch [KTY24], and with a concurrent work by the same authors [KTY25]. These works focus primarily on the Hermitian function field. For a technical comparison, we instantiate Proposition 6.5 with this function field.

Theorem 2.8. *Let $d > 1$ be such that $d \mid q-1$. Let $f \in \mathcal{L}(q\mathfrak{P}_\infty)$ of degree $t = ir+j(r+1)$, such that $(d,t) = 1$, $(i+j,d) = 1$ and $j < \frac{r}{3d}$. Then,*

$$\frac{1}{N}\left|\left\{\mathfrak{q} \in \mathbb{P}_F^1 \setminus \{\mathfrak{p}\} : \exists\, y \in \mathbb{F}_q^\times,\ y^d = f(\mathfrak{q})\right\}\right| \leq \frac{1}{d} + O\left(p\sqrt{\frac{t}{q}} + pd\,\frac{t}{q}\right).$$

The corresponding theorem from [KTY24] goes as follows.

Theorem 2.9 ([KTY24])**.** *Assume that $r > 500$ is a prime number, $q = r^2$ and let d be a prime number that divides $q-1$. Let $f \in \mathcal{L}(q\mathfrak{P}_\infty)$ of degree $t = ir + j(r+1)$, such that $(d,t) = 1$, $(i+j,d) = 1$, and $d < O(\sqrt{t} + \frac{q^{3/2}}{t})$. Then,*

$$\frac{1}{N}\left|\left\{\mathfrak{q} \in \mathbb{P}_F^1 \setminus \{\mathfrak{p}\} : \exists\, y \in \mathbb{F}_q^\times,\ y^d = f(\mathfrak{q})\right\}\right| \leq \frac{1}{d} + O\left(\sqrt{\frac{t}{q}}\right).$$

There are several distinctions between these results. First, Theorem 2.9 is restricted to the case where r is a prime number, reflecting the limitations of the derivatives method as used in [KTY24]. In contrast, our result applies to general prime powers $r = p^e$; but the error term in our bound depends on p. For the purpose of TAG codes, one can take p to be a constant, particularly $p = 2$ (and we are free to vary r) so it has no effect on our bound. Importantly, our result is meaningful for all $e > 2$ whereas Theorem 2.9 requires $e = 1$.

In [KTY25], the authors extend the bound for the case $d = 2$ to all functions $f \in \mathcal{L}\left(q^{3/4}\mathfrak{P}_\infty\right)$ for which the polynomial $T^2 - f$ is absolutely irreducible, without imposing any restriction on $\deg(f)$. However, this comes at the cost of replacing the error term $O\left(\sqrt{\frac{t}{q}}\right)$ with $O\left(\frac{t}{q^{3/4}}\right)$. Moreover, in [KTY25], the authors provide a bound on the exponential sum Equation (2.5) in the setting of the Hermitian curve, when $p = 2$ and q is an arbitrary power of 2, for any function $f \in \mathcal{L}\left(q^{3/4}\mathfrak{P}_\infty\right)$ of odd degree; the resulting error term is $O\left(\frac{t}{q^{3/4}}\right)$, whereas our result Theorem 6.4 yields the sharper bound $O\left(\sqrt{\frac{t}{q}}\right)$ as $t = \Omega(\sqrt{q})$.

3 Preliminaries

We assume familiarity with basic background on algebraic function fields, such as places, valuations, extensions, decomposition and ramification of places, etc. A detailed exposition of the subject can be found in [Sti09]. In this section we recall some basic notions concerning algebraic function fields, the trace map over finite fields, ε-balanced codes, and code concatenation.

Algebraic function fields, valuations and places

Let $\mathbb{F}_q$ be the finite field with q elements. The *rational function field* $\mathbb{F}_q(x)$ is the field of rational functions in an indeterminate x with coefficients in $\mathbb{F}_q$. An *algebraic function field* $F/\mathbb{F}_q$ is a finite algebraic extension of $\mathbb{F}_q(x)$. Elements of F are called *functions*.

A *discrete valuation* on F is a map $v\colon F^\times \to \mathbb{Z}$ satisfying $v(fg) = v(f) + v(g)$, $v(f+g) \geq \min\{v(f), v(g)\}$, and it can be extended to F by setting $v(0) = \infty$. Associated to a discrete valuation v is its valuation ring $\mathcal{O}_v = \{f \in F : v(f) \geq 0\}$, a maximal ideal $\mathfrak{m}_v = \{f \in \mathcal{O}_v : v(f) > 0\}$ and the residue field $\mathbb{F}_v = \mathcal{O}_v/\mathfrak{m}_v$. A *place* $\mathfrak{p}$ of F is the maximal ideal $\mathfrak{m}_v$ of some valuation ring $\mathcal{O}_v$. We write $v_\mathfrak{p}$ for the valuation corresponding to $\mathfrak{p}$, $\mathcal{O}_\mathfrak{p}$ for its valuation ring and $\mathbb{F}_\mathfrak{p}$ for its residue field.

The *degree* of a place $\mathfrak{p}$ is $\deg \mathfrak{p} := [\mathbb{F}_\mathfrak{p} : \mathbb{F}_q]$. Places of degree 1 are called *rational places*. We denote the set of all places of F by $\mathbb{P}_F$, and the set of all rational places of F by $\mathbb{P}_F^1$.

Extensions of function fields and integral closures

Let $F/\mathbb{F}_q$ be an algebraic function field, and let L/F be a finite extension of function fields. For each place $\mathfrak{p} \in \mathbb{P}_F$, we consider the behavior of $\mathfrak{p}$ in the extension L/F. A place $\mathfrak{P} \in \mathbb{P}_L$ is said to *lie above* $\mathfrak{p}$, denoted $\mathfrak{P} \,|\, \mathfrak{p}$, if $\mathcal{O}_\mathfrak{p} \subseteq \mathcal{O}_\mathfrak{P}$, or equivalently, if $\mathfrak{P} \cap \mathcal{O}_\mathfrak{p} = \mathfrak{p}$. For a fixed place $\mathfrak{p}$ of F, there are finitely many places $\mathfrak{P}_1, \ldots, \mathfrak{P}_r$ of L lying above it. Associated with each $\mathfrak{P} \,|\, \mathfrak{p}$ are two important numerical invariants:

- The *ramification index* $e(\mathfrak{P}|\mathfrak{p})$, defined by $v_\mathfrak{P}(f) = e(\mathfrak{P}|\mathfrak{p})\, v_\mathfrak{p}(f)$ for all $f \in F$.
- The *inertia degree* $f(\mathfrak{P}|\mathfrak{p}) := [\mathbb{F}_\mathfrak{P} : \mathbb{F}_\mathfrak{p}]$.

These invariants satisfy the fundamental identity

$$\sum_{\mathfrak{P}|\mathfrak{p}} e(\mathfrak{P}|\mathfrak{p}) f(\mathfrak{P}|\mathfrak{p}) = [L : F].$$

The *integral closure* of $\mathcal{O}_\mathfrak{p}$ in L is defined as

$$\mathcal{O}'_\mathfrak{p} := \{\, f \in L : f \text{ is integral over } \mathcal{O}_\mathfrak{p} \,\}.$$

Equivalently, $\mathcal{O}'_\mathfrak{p}$ consists of all elements of L that satisfy a monic polynomial with coefficients in $\mathcal{O}_\mathfrak{p}$.

Divisors, principal and pole divisors

A *divisor* of F is a formal finite $\mathbb{Z}$-linear combination

$$G = \sum_{\mathfrak{p} \in \mathbb{P}_F} n_{\mathfrak{p}}\, \mathfrak{p}, \qquad n_{\mathfrak{p}} \in \mathbb{Z},$$

with finite support $\mathsf{supp}(G) = \{\mathfrak{p} \in \mathbb{P}_F : n_{\mathfrak{p}} \neq 0\}$. For two divisors G_1, G_2 we write $G_1 \geq G_2$ if $n_{\mathfrak{p}}(G_1) \geq n_{\mathfrak{p}}(G_2)$ for all $\mathfrak{p}$. The *degree* of G is $\deg(G) = \sum_{\mathfrak{p}} n_{\mathfrak{p}} \deg \mathfrak{p}$.

Every nonzero function $f \in F^\times$ determines the *principal divisor*

$$(f) = \sum_{\mathfrak{p} \in \mathbb{P}_F} v_{\mathfrak{p}}(f)\, \mathfrak{p}.$$

The *pole divisor* (or divisor of poles) of f is

$$(f)_\infty = \sum_{\mathfrak{p}\,:\, v_{\mathfrak{p}}(f) < 0} -v_{\mathfrak{p}}(f)\, \mathfrak{p}.$$

The *zero divisor* of f is defined analogously by

$$(f)_0 = \sum_{\mathfrak{p}\,:\, v_{\mathfrak{p}}(f) > 0} v_{\mathfrak{p}}(f) \mathfrak{p}.$$

An important connection between those divisors states that the number of zeros equals the number of poles. Moreover, if $f \in F \setminus \mathbb{F}_q$ then

$$\deg(f)_\infty = \deg(f)_0 = [F : \mathbb{F}_q(f)].$$

In particular, $(f) = (f)_0 - (f)_\infty$ has degree 0. The number

$$\gamma = \min\{[F : \mathbb{F}_q(f)] : f \in F \setminus \mathbb{F}_q\} = \min\{\deg(f)_\infty : f \in F \setminus \mathbb{F}_q\}$$

is called the *gonality* of $F/\mathbb{F}_q$. The following claim gives a lower bound on γ.

Claim 3.1 ([BT13], Lemma 4.2)**.** *Let $F/\mathbb{F}_q$ be a function field with N_F rational places. Then*

$$\gamma \geq \frac{N_F}{q+1}.$$

Riemann–Roch spaces and the genus

For a divisor G, define the *Riemann–Roch space*

$$\mathcal{L}(G) \;=\; \{\, f \in F^\times : (f) + G \geq 0 \,\} \cup \{0\}.$$

This is a finite-dimensional $\mathbb{F}_q$-vector space; denote $\ell(G) := \dim_{\mathbb{F}_q} \mathcal{L}(G)$. The function $\ell(\cdot)$ encodes the number of independent functions with poles bounded by a given divisor.

Claim 3.2. *Let G be a divisor of F with $\deg(G) \geq 0$. Then $\ell(G) \leq \deg(G) + 1$.*

The *genus* $g = g(F)$ is the nonnegative integer characterized as the unique constant for which $\ell(G) \geq \deg(G) - g + 1$ holds for every divisor G, and equality holds for all G of sufficiently large degree. The celebrated Riemann–Roch theorem gives the precise relation.

Theorem 3.3 (Riemann–Roch)**.** *If G is a divisor of F and K is a canonical divisor, then*

$$\ell(G) - \ell(K - G) \;=\; \deg(G) - g + 1.$$

In particular, if $\deg(G) \geq 2g - 1$ then $\ell(G) = \deg(G) - g + 1$.

Bounds on the number of rational places

Let N_F denote the number of rational places of a function field $F/\mathbb{F}_q$ of genus g. The classical Hasse–Weil bound states that

$$|N_F - (q+1)| \leq 2g\sqrt{q}. \tag{3.1}$$

Thus N_F grows at most linearly with g.

Considering the asymptotic regime, let

$$N_q(g) := \max\{N_F \;:\; F \text{ is a function field over } \mathbb{F}_q \text{ of genus } g\}.$$

Ihara's constant is defined by

$$A(q) := \limsup_{g\to\infty} \frac{N_q(g)}{g}.$$

Drinfeld and Vlăduţ proved the upper bound

$$A(q) \leq \sqrt{q} - 1.$$

Moreover, when q is a square, this bound is tight: explicit towers of function fields (notably those of Garcia–Stichtenoth) achieve $N_F/g_F \to \sqrt{q} - 1$. Such optimal towers are the key source of asymptotically good algebraic-geometric codes.

Trace map on finite fields

For an extension of finite fields $\mathbb{F}_{q^m}/\mathbb{F}_q$, the *trace* $\mathsf{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q} \colon \mathbb{F}_{q^m} \to \mathbb{F}_q$ is the $\mathbb{F}_q$-linear map

$$\mathsf{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(z) \;=\; z + z^q + z^{q^2} + \cdots + z^{q^{m-1}}, \qquad z \in \mathbb{F}_{q^m}.$$

The trace is surjective and every $a \in \mathbb{F}_q$ has inverse image $\mathsf{Tr}^{-1}(a)$ of size q^{m-1}.

Additional coding theory preliminaries

We say that C is an $[n, k, d]_q$ code if C is a linear subspace of $\mathbb{F}_q^n$ of dimension k, and the distance of C (i.e., the minimal Hamming distance between each two distinct codewords) is at least d. We will often choose to omit the distance parameter. We say that an $[n, k]_2$ code C is *ε-balanced* if for any nonzero $c \in C$, the relative Hamming weight of c lies in the range $[1/2 - \varepsilon, 1/2 + \varepsilon]$.[7]

We conclude this section by recalling the operation of code concatenation. Letting $C_{\text{out}} \subseteq \mathbb{F}_q^N$ be an "outer" $[N, K, D]_q$ code, and C_{in} be an "inner" $[n_{\text{in}}, \log q, d_{\text{in}}]_2$ code, the concatenated code $C_{\text{out}} \circ C_{\text{in}}$ is an $[N \cdot n, K \cdot \log_2 q, D \cdot d]$ such that for any $x \in \mathbb{F}_q^K \equiv \mathbb{F}_2^{K \cdot \log_2 q}$,

$$(C_{\text{out}} \circ C_{\text{in}})_{i,j} = C_{\text{in}}(C_{\mathsf{out}}(x)_i)_j$$

where $i \in [N]$ and $j \in [n]$. A particularly useful inner code is the *Hadamard code*. Given a message length m, set $q = 2^m$, and identify $\mathbb{F}_q$ with the vector space $\mathbb{F}_2^m$. For $u \in \mathbb{F}_2^m$, the (binary) Hadamard codeword $\mathrm{Had}(u)$ is the length-2^m vector indexed by $v \in \mathbb{F}_2^m$ with entries $\langle u, v \rangle$ (dot product modulo 2). The Hadamard code has relative distance $\frac{1}{2}$.

4 TAG Codes and Function Field Extensions

In this short section, we formally define the construction of the trace code associated with an algebraic geometric code. We then review the relation of its minimum distance to the number of rational points in a certain elementary abelian p-extension of the underlying function field. This connection is a known result, which we include here for completeness.

Let p be a prime number, and let $p \leq \ell \leq q$ be powers of p such that $\mathbb{F}_p \subseteq \mathbb{F}_\ell \subseteq \mathbb{F}_q$. Throughout, Tr is the trace function from $\mathbb{F}_q$ down to $\mathbb{F}_\ell$. Let $F/\mathbb{F}_q$ be a function field of genus g with $N = n + 1$ rational points, one of which is denoted by $\mathfrak{p}$, and the remaining by $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$. For an integer r, we denote the set of pole numbers up to r at $\mathfrak{p}$ by

$$\mathsf{WS}_r = \{i \in [r] : \mathcal{L}(i\mathfrak{p}) \neq \mathcal{L}((i-1)\mathfrak{p})\},$$

and for each $i \in \mathsf{WS}_r$, let $b_i \in \mathcal{L}(i\mathfrak{p}) \setminus \mathcal{L}((i-1)\mathfrak{p})$. We now focus on those functions whose pole order is coprime to the characteristic p: let $i_1 < i_2 < \cdots < i_k$ be the elements of WS_r such that $p \nmid i$, and define

$$B_r = \{b_i : i \in \mathsf{WS}_r \text{ such that } p \nmid i\}$$

[7] Linear ε-balanced codes are essentially equivalent to *ε-biased sets*, a primitive of great importance in pseudorandomness (see, e.g., [HH+24, Section 2.2]).

to be the corresponding set of functions.

With these notations, we define the $\mathbb{F}_\ell$-linear code $\mathsf{TC}\colon \mathbb{F}_q^k \to \mathbb{F}_\ell^n$ as follows. Given $m = (m_1, \ldots, m_k) \in \mathbb{F}_q^k$, define the function $f_m = \sum_{j=1}^k m_j b_{i_j}$. Then, set

$$\mathsf{TC}(m) = (\mathsf{Tr}(f_m(\mathfrak{p}_1)), \ldots, \mathsf{Tr}(f_m(\mathfrak{p}_n)))\,.$$

Put differently, we identify the domain of TC with $\mathsf{Span}_{\mathbb{F}_q}(B_r)$, and for a given input function $f \in \mathsf{Span}_{\mathbb{F}_q}(B_r)$, we evaluate it at the n rational points $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$, followed by applying the trace function from $\mathbb{F}_q$ to $\mathbb{F}_\ell$ coordinate-wise.

We now turn to analyze the distance of the code TC. As hinted above, the key fact used is that the distance is closely related to the number of rational points in a certain extension of the function field F. To make this connection precise, fix a function $0 \neq f \in \mathsf{Span}_{\mathbb{F}_q}(B_r)$ and consider the field extension $L = F(z)$ defined by the equation

$$z^\ell - z = f.$$

We first note that L/F is an elementary abelian p-extension, which is a generalization of Artin-Schreier extensions (which are the case $\ell = p$). Indeed, notice that the polynomial $a(T) = T^\ell - T$ is additive, and its set of roots is $\mathbb{F}_\ell \subseteq \mathbb{F}_q$. In addition, $v_\mathfrak{p}(f) < 0$ with $p \nmid v_\mathfrak{p}(f)$, and $v_\mathfrak{q}(f) \geq 0$ for all $\mathfrak{q} \in \mathbb{P}_F \setminus \{\mathfrak{p}\}$. Thus, all the conditions of [Sti09, Proposition 3.7.10] are satisfied, and the extension L/F is an elementary abelian p-extension of degree ℓ.

Claim 4.1. *For every $i \in [n]$, we have $\mathsf{Tr}(f(\mathfrak{p}_i)) = 0$ if and only if the place $\mathfrak{p}_i$ splits completely in the extension L/F.*

For the proof of Claim 4.1, we make use of Kummer's Theorem (see Theorem 3.3.7 in [Sti09]), which we cite here, with some modifications to suit our needs, for convenience.

Theorem 4.2 (Kummer's Theorem)**.** *Let L/F be a function field extension, and fix a place $\mathfrak{p}$ of F. Assume there exists an element $z \in L$ such that $L = F(z)$ and $z \in \mathcal{O}'_\mathfrak{p}$. Consider the minimal polynomial of z over F,*

$$\varphi(T) = \sum_{i=0}^{d} h_i T^i,$$

where we use the known fact that $h_i \in \mathcal{O}_\mathfrak{p}$ for all i. Define

$$\bar{\varphi}(T) = \sum_{i=0}^{d} h_i(\mathfrak{p}) T^i \in F_\mathfrak{p}[T],$$

where $F_{\mathfrak{p}}$ denotes the residue class field at $\mathfrak{p}$. Factor $\bar{\varphi}$ over $F_{\mathfrak{p}}$ as

$$\bar{\varphi}(T) = \prod_{j=1}^{r} \gamma_j(T)^{\varepsilon_j},$$

where $\gamma_1, \ldots, \gamma_r$ are distinct irreducible factors and ε_j denotes the multiplicity of γ_j in the factorization. Assuming that $\varepsilon_1 = \cdots = \varepsilon_r = 1$, there are exactly r distinct places $\mathfrak{P}_1, \ldots, \mathfrak{P}_r$ of L lying above $\mathfrak{p}$. Moreover, for each $i \in [r]$, we have $e(\mathfrak{P}_i|\mathfrak{p}) = 1$ and $f(\mathfrak{P}_i|\mathfrak{p}) = \deg \gamma_i$.

With this we are in position to prove Claim 4.1.

Proof of Claim 4.1. We recall Hilbert's Theorem 90, in its additive form, which asserts that for every $\alpha \in \mathbb{F}_q$

$$\mathsf{Tr}(\alpha) = 0 \quad \Longleftrightarrow \quad \exists \beta \in \mathbb{F}_q \;\; \alpha = \beta^{\ell} - \beta.$$

Fix $i \in [n]$ and assume that $\mathsf{Tr}(f(\mathfrak{p}_i)) = 0$. By Hilbert's Theorem 90,

$$\exists \beta \in \mathbb{F}_q \quad f(\mathfrak{p}_i) = \beta^{\ell} - \beta. \tag{4.1}$$

Observe that $z \in \mathcal{O}'_{\mathfrak{p}_i}$. Indeed, the minimal polynomial of z over F is

$$\varphi(T) = T^{\ell} - T - f \in \mathcal{O}_{\mathfrak{p}_i}[T],$$

where $f \in \mathcal{O}_{\mathfrak{p}_i}$ since the only pole of f is $\mathfrak{p}$. As we also have that $L = F(z)$, we are in a position to apply Kummer's Theorem. With the notations of Theorem 4.2, we get by Equation (4.1) that

$$\begin{aligned}
\bar{\varphi}(T) &= T^{\ell} - T - f(\mathfrak{p}_i) \\
&= T^{\ell} - T - (\beta^{\ell} - \beta) \\
&= (T - \beta)^{\ell} - (T - \beta) \\
&= \prod_{t \in \mathbb{F}_{\ell}} (T - \beta - t).
\end{aligned}$$

Hence, Kummer's Theorem implies that $\mathfrak{p}_i$ splits completely in the extension L/F.

On the other hand, if $\mathsf{Tr}(f(\mathfrak{p}_i)) \neq 0$, then Hilbert's Theorem 90 implies that the polynomial $\bar{\varphi}(T)$ has no roots in $\mathbb{F}_q$. Notice that $F_{\mathfrak{p}_i} = \mathbb{F}_q$, as $\mathfrak{p}_i$ is a rational place. Let

$$\bar{\varphi}(T) = \prod_{j=1}^{r} \gamma_j(T)^{\varepsilon_j}$$

be the factorization of $\bar{\varphi}(T)$ over $F_{\mathfrak{p}_i}$. Then it follows that $\deg \gamma_j > 1$ for all $j \in [r]$. In addition, since $\gcd(\bar{\varphi}(T), \bar{\varphi}'(T)) = 1$, the polynomial $\bar{\varphi}(T)$ is separable. Hence $\varepsilon_j = 1$ for all $j \in [r]$. Thus, by Kummer's Theorem, every place of L lying above $\mathfrak{p}_i$ must be of degree > 1, and the proof is completed. □

As a consequence of Claim 4.1, we obtain the following result. We denote by N_L the number of rational points of L.

Corollary 4.3. *The relative-distance of the code* TC *defined above is*

$$\delta = 1 - \frac{1}{\ell} \cdot \frac{N_L - 1}{n}.$$

Proof. Choose a codeword $(\mathsf{Tr}(f(\mathfrak{p}_1)), \ldots, \mathsf{Tr}(f(\mathfrak{p}_n)))$ of minimal weight, and let

$$Z = \{i \in [n] : \mathsf{Tr}(f(\mathfrak{p}_i)) = 0\}.$$

Then the relative distance of the code is given by $\delta = 1 - \frac{|Z|}{n}$.

By Claim 4.1, for every $i \in Z$ there are exactly ℓ rational places of L lying above $\mathfrak{p}_i$. Moreover, from the proof of the claim, for every $i \in [n] \setminus Z$, there are no rational places of L lying above $\mathfrak{p}_i$. As the remaining rational place $\mathfrak{p} \in \mathbb{P}_F$ is totally ramified in L/F, there is one more rational place of L lying above it. Altogether, we conclude that

$$N_L = |Z| \cdot \ell + 1,$$

hence $|Z| = \frac{N_L - 1}{\ell}$, and the proof follows. □

By Corollary 4.3, to lower bound the distance of TC, it suffices to upper bound the ratio $\frac{N_L-1}{n} = \frac{N_L-1}{N_F-1}$, or, essentially equivalently, the more natural ratio $\frac{N_L}{N_F}$. Note that the trivial upper bound $N_L \leq \ell n + 1$ yields only the trivial lower bound $\delta \geq 0$. Obtaining a nontrivial upper bound on N_L is the content of Section 5.

5 Our Bound on the Number of Rational Points

In this section, we prove the following fairly general—though somewhat technical to state—proposition, which serves as the foundation for our results on elementary abelian p-extensions and Kummer extensions. The statement of Proposition 5.1 is formulated in a broad setting and thus involves several unspecified parameters. In Corollary 5.2, we present new normalized parameters, and rewrite the bound with these notations. In Proposition 5.3 we instantiate these parameters, and obtain the main general result, although still quite technical. In Section 5.3 we show that a quite general family of extensions satisfy the conditions of Proposition 5.3, and conclude Theorem 5.6, which will be used in all our applications.

From here onwards, p is a prime number and $q = p^u$ for some integer $u \geq 1$. Moreover, $F/\mathbb{F}_q$ is a function field with N rational places and genus g. We focus on curves in the

regime $g = \Omega\left(\frac{N}{\sqrt{q}}\right)$. For the complementary regime, one can apply the Grothendieck's trace formula to bound the number of rational places over extensions of F; see the discussion in Section 1.4. Let $\mathfrak{p}$ be a rational place of F, and let $x \in \mathcal{L}(s\mathfrak{p}) \setminus \mathcal{L}((s-1)\mathfrak{p})$ for some integer $s > 1$. Hence $\deg(x)_\infty = s$. We consider field extensions of the form L/F where $L = F(z)$. We denote by

$$t \triangleq \deg(z)_\infty.$$

The reader may think of t as given as input, and the resulted bound depends on t. The parameter s on the other hand is "internal" to the proof and it will be beneficiary to choose it as small as possible.[8]

We will need to introduce a few more parameters. Let $1 \leq m \leq q$ be a power of p. Denote

$$A \triangleq \left\lfloor \frac{Nm}{2q} \right\rfloor$$

and let $B \in \mathbb{N}$ be a parameter.

Proposition 5.1. *Let L/F be a function field extension of the form $L = F(z)$, and let $d \triangleq [L : F]$. Assume that $\mathfrak{p}$ is totally ramified in L, and denote by $\mathfrak{P}$ the unique place of L lying above $\mathfrak{p}$. Let $\{b_i\}_{i\in\mathcal{I}}$ be a basis of $\mathcal{L}(A\mathfrak{P})$ such that $v_{\mathfrak{P}}(b_i) = -i$. Assume that the elements*

$$S = \left\{ b_i x^{jm} z^{km} : i \leq A,\ j \leq B,\ k < d \right\} \tag{5.1}$$

are linearly independent over $\mathbb{F}_q$. Further assume that

$$(A - g_L)Bd > \frac{N}{2} + dsB + (d-1)t, \tag{5.2}$$

where g_L denotes the genus of L. Then, the number of rational points N_L of L satisfies

$$N_L \leq \left(sdB + \frac{N}{2q} + td \right) m.$$

Proof of Proposition 5.1. First, notice that as $\mathfrak{p}$ is totally ramified, $\mathbb{F}_q$ is the full constant field of L. Let U be the $\mathbb{F}_q$ vector space spanned by S as given in Equation (5.1). Consider the $\mathbb{F}_p$ linear map $\Psi : U \to L$ defined by

$$\Psi\left(\sum_{\substack{i\leq A \\ j\leq B, k<d}} c_{i,j,k} b_i x^{jm} z^{km} \right) = \sum_{i,j,k} c_{i,j,k}^{q/m} b_i^{q/m} x^j z^k,$$

where $c_{i,j,k} \in \mathbb{F}_q$. Note that

$$\mathrm{Im}\Psi \subseteq \mathcal{L}\left((N/2 + dsB)\,\mathfrak{P} + (d-1)(z)_\infty \right),$$

[8] Note that by Claim 3.1, $s \geq \frac{N}{q+1}$.

where we used that $v_{\mathfrak{P}}(x) = e(\mathfrak{P}|\mathfrak{p})v_{\mathfrak{p}}(x) = ds$. This, together with Claim 3.2, shows that

$$\dim_{\mathbb{F}_p} \mathrm{Im}\Psi \leq (N/2 + dsB + (d-1)t + 1) \cdot [\mathbb{F}_q : \mathbb{F}_p].$$

Per our assumption on S, as an $\mathbb{F}_q$-vector space,

$$\dim_{\mathbb{F}_p} U = \dim_{\mathbb{F}_q} \mathcal{L}(A\mathfrak{P}) \cdot (B+1)\, d \cdot [\mathbb{F}_q : \mathbb{F}_p] \geq (A - g_L)\,(B+1)\, d \cdot [\mathbb{F}_q : \mathbb{F}_p],$$

where the last inequality follows by Riemann's Theorem.

Therefore our assumption Inequality (5.2) implies that $\dim_{\mathbb{F}_p} U > \dim_{\mathbb{F}_p} \mathrm{Im}\Psi$ and so there exists a nonzero element $h \in U$ such that $\Psi(h) = 0$. Indeed, this follows since Ψ is additive. Note however that for every degree-1 place $\mathfrak{Q} \neq \mathfrak{P}$ of L,

$$0 = \Psi(h)^m(\mathfrak{Q}) = h(\mathfrak{Q}).$$

That is, h vanishes on all rational places $\mathfrak{Q} \neq \mathfrak{P}$ of L, and so $N_L \leq \deg(h)_\infty + 1$. But

$$h \in U \subseteq \mathcal{L}\left((A + sdBm)\,\mathfrak{P} + (d-1)m(z)_\infty\right),$$

hence $\deg(h)_\infty \leq A + sdBm + t(d-1)m$, which concludes the proof. □

We define the parameters τ, β, γ, μ and σ which satisfies the following relations with regards to the previously defined parameters in this section so far:

$$\begin{aligned} t &= \tau \frac{N}{\sqrt{q}} \\ B &= \beta \frac{\sqrt{q}}{d} \\ g &= \gamma \frac{N}{\sqrt{q}} \\ m &= \mu\sqrt{q} \\ s &= \sigma \frac{N}{q} \end{aligned} \tag{5.3}$$

Note that we assume that $\gamma = \Omega(1)$.

With this we have the following corollary, retaining the notation from Proposition 5.1.

Corollary 5.2. *Assume that*

$$g_L \leq d(g+t) \tag{5.4}$$

and that

$$\beta\mu \geq 1 + 2(\tau+\gamma)\beta d + \frac{2}{\sqrt{q}}\left(\tau(d-1) + \sigma\beta\right) \tag{5.5}$$

hold. Assume further, as in Proposition 5.1, that the elements in S are linearly independent over $\mathbb{F}_q$. Then,

$$N_L \leq \mu N\left(\sigma\beta + \tau d + \frac{1}{2\sqrt{q}}\right). \tag{5.6}$$

Proof. Per our assumption, Inequality (5.4), and using the parameters defined in Equation (5.3), we have that the LHS of Inequality (5.2) can be bounded from below by

$$\begin{aligned}(A - g_L)Bd &\geq \left(\frac{Nm}{2q} - d(g+t)\right) Bd \\ &= (\mu/2 - (\tau+\gamma)d)\beta N,\end{aligned}$$

whereas the RHS of Inequality (5.2) can be rewritten as

$$\frac{N}{2} + dsB + (d-1)t = \left(\frac{1}{2} + \frac{1}{\sqrt{q}}\left(\tau(d-1) + \sigma\beta\right)\right) N.$$

Thus, Inequality (5.2) in Proposition 5.1 holds per our assumption, Inequality (5.5). Thus, we can invoke Proposition 5.1 to conclude that

$$\begin{aligned}N_L &\leq \left(sdB + \frac{N}{2q} + td\right) m \\ &= \mu N \left(\sigma\beta + \tau d + \frac{1}{2\sqrt{q}}\right).\end{aligned}$$

□

5.1 Before the Instantiation: A Parameter Walkthrough

Before proceeding to instantiate the parameters β, μ in Corollary 5.2, we provide the reader with some informal insight into the magnitudes of the various parameters. While this discussion is not rigorous, it is intended to offer intuition about the bounds one should expect.

The five parameters appearing in Equation (5.3) can be grouped into three distinct categories. As previously noted, the reader should view τ as the input parameter – the bound we derive for N_L depends on τ, and it is the nature of this dependence that we aim to understand. The parameters β and μ are under our control; by selecting them appropriately, we can optimize the resulting bound. In contrast, the parameters γ and σ are intrinsic to the function field under consideration, and for the purposes of this discussion, the reader may assume $\gamma = \sigma = 1$.

As a starting point, we ignore terms that vanish as $q \to \infty$. This simplification allows us to gain an initial understanding of how the bound depends on the dominant quantities, namely, p, d and τ. It also offers guidance on how to optimize the bound by appropriately choosing the parameters β and μ. The assumption in Inequality (5.5) then simplifies to

$$\beta\mu \geq 1 + 2(\tau+1)\beta d.$$

We take this to hold with equality, yielding the following relation between β and μ:

$$\mu = \frac{1}{\beta} + 2(\tau+1)d. \tag{5.7}$$

Now, the bound guaranteed by Corollary 5.2 simplifies, as discussed above, to

$$\frac{N_L}{N} \leq \mu\left(\beta + \tau d\right).$$

Plugging in the relation between μ and β, we obtain

$$\frac{N_L}{N} \leq \left(\frac{1}{\beta} + 2(1+\tau)d\right)\left(\beta + \tau d\right).$$

Generally, for $a, b > 0$, the minimum of the function $f(x) = (x+a)\left(\frac{1}{x}+b\right)$ in $(0,\infty)$ is $(1+\sqrt{ab})^2$, attained at $x = \sqrt{\frac{a}{b}}$. Applying this, we get that setting $\beta = \sqrt{\frac{\tau}{2(1+\tau)}}$ yields the bound

$$\frac{N_L}{N} \leq \left(1 + \sqrt{2\tau(1+\tau)}\, d\right)^2.$$

Analogously to the Hasse–Weil theorem, where the number of rational points on a curve lying over the projective line is expressed as $q + 1 + \mathrm{Err}$, the presence of the constant term 1 is natural and expected. The remaining contribution is the "error term". Note that a bound of d on the ratio is trivial, since L/F is an extension of degree d. Thus, the bound is meaningful only when $\tau \ll 1$, in which case we can simplify the informal (and inaccurate) bound to

$$\frac{N_L}{N} \leq \left(1 + \sqrt{2\tau}\, d\right)^2 = 1 + 2\sqrt{2\tau}\, d + 2\tau d^2.$$

Note that the contributions of the two summands on the right-hand side to the error term are incomparable; which one dominates depends on whether $2\tau < \frac{1}{d^2}$ or not.

The dependence on q. Of course, this bound is not accurate — in particular, it ignores the dependence on q, which is actually quite important in applications, as it determines how the alphabet reduction (i.e., the minimal value of q for which we start) affects the bound. Moreover, the parameter β should be chosen such that B is an integer, and μ should be chosen such that m is a power of p, which we will take care of later.

However, the above discussion provides useful insight into how to choose β and μ. In particular, we set $\beta = \sqrt{\frac{\tau}{2(1+\tau)}}$, which is well-approximated by $\sqrt{\tau/2}$ under the assumption that $\tau \ll 1$. Thus, we proceed with the choice $\beta = \sqrt{\tau/2}$. Substituting this into Equation (5.7), and using again that $\tau \ll 1$, a suitable choice for μ is

$$\mu = \frac{1}{\sqrt{\tau/2}} + 2d. \tag{5.8}$$

Plugging this into Inequality (5.6), we obtain

$$\frac{N_L}{N} \leq \left(1+\sqrt{2\tau}d\right)^2 + \frac{1}{\sqrt{q}}\left(d+\frac{1}{\sqrt{2\tau}}\right). \tag{5.9}$$

Notice that by Claim 3.1, we have $\tau = t\frac{\sqrt{q}}{N} \geq \frac{1}{\sqrt{q}} \cdot \frac{q}{q+1}$. Thus,

$$\frac{d}{\sqrt{q}} \leq \tau d \cdot \left(1+q^{-1}\right),$$
$$\frac{1}{\sqrt{2q\tau}} \leq \sqrt{\tau}.$$

Hence, the bound in Inequality (5.9) can be rewritten as

$$\frac{N_L}{N} \leq 1 + O(\sqrt{\tau}d + \tau d^2). \tag{5.10}$$

5.2 Instantiation of Parameters

In this subsection, we formalize the above discussion and establish the following general result.

Proposition 5.3. *Let L/F be a function field extension of the form $L = F(z)$, and let $d \triangleq [L:F]$. Assume that $\mathfrak{p}$ is totally ramified in L, and denote by $\mathfrak{P}$ the unique place of L lying above $\mathfrak{p}$. Let $\{b_i\}_{i\in\mathcal{I}}$ be a basis of $\mathcal{L}(A\mathfrak{P})$ such that $v_{\mathfrak{P}}(b_i) = -i$. Assume that the elements*

$$S = \left\{b_i x^{jm} z^{km} : i \leq A,\ j \leq B,\ k < d\right\} \tag{5.11}$$

are linearly independent over $\mathbb{F}_q$. Further, assume that $g_L \leq d(g+t)$. Then,

$$\frac{N_L}{N} \leq \sigma + O_\sigma\left(\sqrt{\tau}d\gamma p + \tau d^2\gamma p + \frac{d}{\sqrt{q}}\left(\frac{1}{\sqrt{\tau}}+d\right)\gamma p\right). \tag{5.12}$$

Remark 5.4. *If $\sigma \sim 1, \gamma \sim 1$ as in Section 5.1, this is the same error term as in Inequality (5.9) up to a factor of p.*

Proof. By Corollary 5.2, if

$$\beta\mu \geq 1 + 2(\tau+\gamma)\beta d + \frac{2}{\sqrt{q}}\left(\tau(d-1)+\sigma\beta\right), \tag{5.13}$$

then,

$$N_L \leq \mu N\left(\sigma\beta + \tau d + \frac{1}{2\sqrt{q}}\right). \tag{5.14}$$

We now choose values for the parameters β and μ. Similarly to Section 5.1, we want to take Inequality (5.13) with equality. But we have to make sure that $B = \beta\frac{\sqrt{q}}{d}$ is an integer. Isolating β in Inequality (5.13), as long as $\mu > 2d(\tau+\gamma) + \frac{2\sigma}{\sqrt{q}}$, we get

$$\beta \geq \frac{1 + \frac{2}{\sqrt{q}}\tau(d-1)}{\mu - 2d(\tau+\gamma) - \frac{2\sigma}{\sqrt{q}}}. \tag{5.15}$$

To ensure that B is an integer, we can choose

$$\beta = \frac{1 + \frac{2}{\sqrt{q}}\tau(d-1)}{\mu - 2d(\tau+\gamma) - \frac{2\sigma}{\sqrt{q}}} + O\left(\frac{d}{\sqrt{q}}\right).$$

Notice the inequality $\frac{1}{1-x} \leq 1 + 2x$ which holds for $0 \leq x \leq 0.5$. Under the assumption

$$\frac{d}{\mu}(\tau+\gamma) + \frac{\sigma}{\sqrt{q}\mu} \leq \frac{1}{4}, \tag{5.16}$$

we have

$$\beta \leq \frac{1}{\mu}\left(1 + \frac{2}{\sqrt{q}}\tau(d-1)\right)\left(1 + \frac{4d}{\mu}(\tau+\gamma) + \frac{4\sigma}{\mu\sqrt{q}}\right) + O\left(\frac{d}{\sqrt{q}}\right).$$

We want to choose μ similarly to Equation (5.8), but we have to make sure that m is a power of p, and that Inequality (5.16) is satisfied. Pick $0 \leq \alpha \leq 1$ and $C = C(\sigma)$ such that

$$\mu = \left(\frac{1}{\sqrt{\tau/2}} + 2d\right)\gamma C p^{\alpha}$$

satisfies Inequality (5.16), and such that m is a power of p. Instantiating those choices into Inequality (5.14), we obtain

$$\begin{aligned}
\frac{N_L}{N} &\leq \mu\beta\sigma + \mu\left(\tau d + \frac{1}{2\sqrt{q}}\right) \\
&\leq \sigma\left(1 + \frac{2}{\sqrt{q}}\tau(d-1)\right)\left(1 + \frac{4d}{\mu}(\tau+\gamma) + \frac{4\sigma}{\mu\sqrt{q}}\right) + O\left(\frac{\sigma\mu d}{\sqrt{q}}\right) \\
&\quad + \left(\tau d + \frac{1}{2\sqrt{q}}\right)\left(\frac{1}{\sqrt{\tau/2}} + 2d\right)\gamma C p^{\alpha}.
\end{aligned}$$

Expanding using Inequality (5.16), we have

$$\begin{aligned}
\frac{N_L}{N} &\leq \sigma\left(1 + \frac{4d}{\mu}(\tau+\gamma) + \frac{4\sigma}{\mu\sqrt{q}} + O\left(\frac{\mu d}{\sqrt{q}}\right)\right) \\
&\quad + C\sqrt{2\tau}d\gamma p^{\alpha} + C2\tau d^2\gamma p^{\alpha} + C\frac{\gamma p^{\alpha}}{\sqrt{2q\tau}} + C\frac{d\gamma p^{\alpha}}{\sqrt{q}}.
\end{aligned}$$

Now, notice that $\frac{1}{\mu} \leq \frac{\sqrt{\tau/2}}{C\gamma p^\alpha}$, and $p^\alpha \leq p$, hence

$$C\sqrt{2\tau}d\gamma p^\alpha + C2\tau d^2\gamma p^\alpha + C\frac{\gamma p^\alpha}{\sqrt{2q\tau}} + C\frac{d\gamma p^\alpha}{\sqrt{q}} \\ = O\left(\sqrt{\tau}d\gamma p + \tau d^2\gamma p + \frac{\mu d}{\sqrt{q}}\right).$$

If $\tau \geq 1$, the bound is trivial, therefore we can assume $\tau < 1$. As $\gamma = \Omega(1)$, we have $\tau + \gamma = O(\gamma)$, hence

$$\frac{4d}{\mu}(\tau + \gamma) + \frac{4\sigma}{\mu\sqrt{q}} = O_\sigma(d\sqrt{\tau}).$$

This implies

$$\frac{N_L}{N} \leq \sigma + O_\sigma\left(\sqrt{\tau}d\gamma p + \tau d^2\gamma p + \frac{\mu d}{\sqrt{q}}\right) \\ = \sigma + O_\sigma\left(\sqrt{\tau}d\gamma p + \tau d^2\gamma p + \frac{d}{\sqrt{q}}\left(\frac{1}{\sqrt{\tau}} + d\right)\gamma p\right).$$

□

5.3 Extensions that Satisfy the Conditions of Proposition 5.3

Proposition 5.5. *Let $\mathfrak{p} \in \mathbb{P}_F$ be a rational place, and let $f \in F$ have poles only at $\mathfrak{p}$. Let L/F be a function field extension defined by*

$$L = F(z) \quad \text{such that} \quad \phi(z) = f,$$

where $\phi(T) \in \mathbb{F}_q[T]$ is a polynomial of degree d. Assume that the polynomial $\phi(T) - f \in F[T]$ is irreducible. Assume that $\mathfrak{p}$ is totally ramified in L, and denote by $\mathfrak{P}$ the unique place of L lying above $\mathfrak{p}$. Let $\{b_i\}_{i\in\mathcal{I}}$ be a basis of $\mathcal{L}(A\mathfrak{P})$ such that $v_\mathfrak{P}(b_i) = -i$. Then,

1. *$t \triangleq \deg_L(z)_\infty = -v_\mathfrak{P}(z) = \deg_F(f)_\infty$.*
2. *If we can write $\deg_F(f)_\infty = t = \ell s + \varepsilon\frac{N}{q}$ for some ℓ relatively prime to d, and $|\varepsilon| < \frac{\sigma - 1/2}{d-1}$, then the set*

$$S = \left\{b_i x^{jm} z^{km} : i \leq A,\ j \leq B,\ k < d\right\} \tag{5.17}$$

is linearly independent over $\mathbb{F}_q$.

Proof. First, we prove that for every $h \in F$ we have $\deg_L(h)_\infty = d\deg_F(h)_\infty$. Indeed, since the place $\mathfrak{p}$ is totally ramified, $\mathbb{F}_q$ is the constant field of L and so by Proposition 3.1.9 and Corollary 3.1.14 in [Sti09]:

$$\deg_L(h)_\infty = \deg \mathrm{Con}_{L/F}(h)_\infty = [L : F]\deg_F(h)_\infty = d\deg_F(h)_\infty.$$

In particular, for $h = f$ we obtain

$$d \deg_F(f)_\infty = \deg_L(f)_\infty = \deg_L(\phi(z))_\infty = d \deg_L(z)_\infty.$$

We turn to prove the remaining equality appearing in Item 1, namely, $\deg_L(z)_\infty = -v_{\mathfrak{P}}(z)$. As $f \in \mathcal{L}(r\mathfrak{p})$ it has a pole only at $\mathfrak{p}$, and so $v_{\mathfrak{p}}(f) = -\deg_F(f)_\infty$. Consider now a pole $\mathfrak{Q}$ of z. Then, $v_{\mathfrak{Q}}(z) < 0$ and so by the strict triangle inequality $v_{\mathfrak{Q}}(\phi(z)) = dv_{\mathfrak{Q}}(z) < 0$. But $v_{\mathfrak{Q}}(\phi(z)) = v_{\mathfrak{Q}}(f)$, and so $\mathfrak{Q}$ lies over a pole of f. As the only pole of f is $\mathfrak{p}$ and since $\mathfrak{P}$ is the only place lying over $\mathfrak{p}$, we get that $\mathfrak{Q} = \mathfrak{P}$. Thus, $(z)_\infty = -v_{\mathfrak{P}}(z)\mathfrak{P}$, and so

$$\deg_L(z)_\infty = -v_{\mathfrak{P}}(z) \deg \mathfrak{P} = -v_{\mathfrak{P}}(z),$$

where the last equality follows since $\mathfrak{P} \mid \mathfrak{p}$ totally ramifies, hence $f(\mathfrak{P}|\mathfrak{p}) = 1$ and $\deg \mathfrak{P} = f(\mathfrak{P}|\mathfrak{p}) \deg \mathfrak{p} = 1$.

Next, we prove Item 2. Recall that $A = \lfloor \frac{Nm}{2q} \rfloor$. We claim that for $i, i' \leq A,\ j, j' \leq B$ and $k, k' < d$ we have $(i, j, k) = (i', j', k')$ if and only if $v_{\mathfrak{P}}(b_i x^{jm} z^{km}) = v_{\mathfrak{P}}(b_{i'} x^{j'm} z^{k'm})$. This will complete the proof.

Assume that $v_{\mathfrak{P}}(b_i x^{jm} z^{km}) = v_{\mathfrak{P}}(b_{i'} x^{j'm} z^{k'm})$. Denote $\Delta_i = i - i'$ and similarly for j, k. We have

$$0 = v_{\mathfrak{P}}(b_i x^{jm} z^{km}) - v_{\mathfrak{P}}(b_{i'} x^{j'm} z^{k'm}) = \Delta_i + \frac{mN}{q} \left(\sigma d \Delta_j + t \frac{q}{N} \Delta_k \right).$$

Since $t = \ell s + \varepsilon \frac{N}{q}$, we can write $t \frac{q}{N} = \ell\sigma + \varepsilon$, to get

$$\begin{aligned} 0 &= \Delta_i + \frac{mN}{q} (\sigma d \Delta_j + (\ell\sigma + \varepsilon)\Delta_k) \\ &= \Delta_i + \frac{mN}{q} (\sigma(d\Delta_j + \ell\Delta_k) + \varepsilon\Delta_k), \end{aligned}$$

which is equivalent to

$$-\Delta_i = \frac{mN}{q} \left(\sigma(d\Delta_j + \ell\Delta_k) + \varepsilon\Delta_k \right), \tag{5.18}$$

Since $\gcd(\ell, d) = 1$ and $|\Delta_k| < d$, we have either $\Delta_k = 0$ or $\ell\Delta_k \not\equiv 0 \mod d$. However, if $\ell\Delta_k \not\equiv 0 \mod d$, then

$$|\sigma(d\Delta_j + \ell\Delta_k) + \varepsilon\Delta_k| \geq \sigma - (d-1)\varepsilon > \frac{1}{2}.$$

Plugging this into Equation (5.18), we get

$$\frac{mN}{2q} < \left| \frac{mN}{q} \left(\sigma(d\Delta_j + \ell\Delta_k) + \varepsilon\Delta_k \right) \right| = |\Delta_i| \leq \frac{mN}{2q},$$

which is a contradiction. Thus, $\Delta_k = 0$. Now, if $\Delta_j \neq 0$, then by Equation (5.18) we have

$$\frac{mN}{q} < \left| \frac{mN}{q} \sigma d \Delta_j \right| = |\Delta_i| \leq \frac{mN}{2q},$$

which is again a contradiction. Thus $\Delta_j = \Delta_k = 0$, and hence $\Delta_i = 0$ which completes the proof. □

As a corollary, we state the main theorem which will be used in all our applications.

Theorem 5.6. *Let $\mathfrak{p} \in \mathbb{P}_F$ be a rational place, and let $f \in F$ have poles only at $\mathfrak{p}$. Assume that $\deg_F(f)_\infty$ is relatively prime to d, and that we can write $\deg_F(f)_\infty = \ell s + \varepsilon \frac{N}{q}$ for some ℓ relatively prime to d, and $0 \leq \varepsilon < \frac{\sigma - 1/2}{d-1}$. Let L/F be a function field extension defined by*

$$L = F(z) \quad \text{such that} \quad \phi(z) = f,$$

where $\phi(T) \in \mathbb{F}_q[T]$ is a polynomial of degree d. Assume that the polynomial $\phi(T) - f \in F[T]$ is irreducible. Assume that $\mathfrak{p}$ is totally ramified in L. Further, assume that $g_L \leq d(g+t)$. Then $\deg_F(f)_\infty = t$, and

$$\frac{N_L}{N} \leq \sigma + O_\sigma \left(\sqrt{\tau} d \gamma p + \tau d^2 \gamma p \right). \tag{5.19}$$

Proof. Let $\mathfrak{P} \in \mathbb{P}_L$ be a place lying above $\mathfrak{p}$. The equation $\phi(z) = f$ implies that

$$e(\mathfrak{P}|\mathfrak{p}) \cdot \deg_F(f)_\infty = \deg_L(f)_\infty = d \deg_L(z)_\infty = dt.$$

As $\deg_F(f)_\infty$ is relatively prime to d, we must have $\deg_F(f)_\infty = t$ and $e(\mathfrak{P}|\mathfrak{p}) = d$. Hence we are in a position to apply Proposition 5.3, to obtain

$$\frac{N_L}{N} \leq \sigma + O_\sigma \left(\sqrt{\tau} d \gamma p + \tau d^2 \gamma p + \frac{d}{\sqrt{q}} \left(\frac{1}{\sqrt{\tau}} + d \right) \gamma \right).$$

To complete the proof, we use Claim 3.1 to observe that

$$\tau = t \frac{\sqrt{q}}{N} = \deg_F(f)_\infty \cdot \frac{\sqrt{q}}{N} \geq \frac{1}{2\sqrt{q}}.$$

Hence

$$\frac{d^2}{\sqrt{q}} \leq 2\tau d^2,$$
$$\frac{d}{\sqrt{q\tau}} \leq 2\sqrt{\tau} d.$$

□

6 Abelian Extensions and Character Sums

In this section, we instantiate the bound from Theorem 5.6 for two families of abelian extensions. The first family consists of elementary abelian p-extensions of the form $L = F(z)$, where $z^\ell - z = f$ and d is a prime power. We apply the bound to this setting to derive a lower bound on the minimum distance of TAG codes, as discussed in Section 4. Moreover, in the Artin–Schreier case (i.e., when $\ell = p$ is prime), the bound yields an upper bound on exponential sums of functions over curves. The second family we consider is Kummer extensions, namely those of the form $L = F(z)$ with $z^d = f$, where d is not divisible by the characteristic p of F.

6.1 Elementary Abelian p-Extensions and Exponential Sums

In this subsection we consider elementary abelian p-extensions of the form $L = F(z)$, where $z^\ell - z = f$ and ℓ is a prime power. These extensions satisfy the conditions of Theorem 5.6. As discussed in Section 4, any non-trivial bound for the number of rational points on this type of extensions immediately yields a lower bound on the minimum distance of the corresponding TAG code. In Theorem 6.1, we use this connection to obtain a lower bound for the distance of TAG codes; in Corollary 6.3 we give an argument that also yields an *upper* bound. We use this in Theorem 6.4 to get an upper bound for exponential sums of function on curves.

Recall the setting of Section 5. Let $\ell > 1$ be a power of p. Let $\phi(T) = T^\ell - T$, let $f \in \mathcal{L}(r\mathfrak{p})$ and assume that $t = \deg(f)_\infty = -v_\mathfrak{p}(f)$ is not divisible by p. Let $L = F(z)$ with $\phi(z) = f$. By [Sti09, Theorem 3.7.10(a)], L/F is an elementary abelian extension of exponent p. By part (d) of this proposition, the prime $\mathfrak{p}$ is totally ramified in L, and moreover by part (e) we have

$$g_L = \ell g + \frac{\ell - 1}{2}(-2 + (t+1)) \leq \ell(g + t).$$

Thus we are in a position to apply Theorem 5.6 to L/F.

Proposition 6.1. *In the above setting, assume further that f satisfies the condition in Item 2 of Proposition 5.5. Then,*

$$\frac{N_L}{N} \leq \sigma + O_\sigma\left(\ell\sqrt{\tau}\gamma p + \ell^2\tau\gamma p\right). \tag{6.1}$$

Let Tr be the trace function from $\mathbb{F}_q$ to $\mathbb{F}_\ell$. Claim 4.1 relates splitting places in L/F to the vanishing of the trace of f at these places. We use this relation together with Theorem 6.1 to get an upper bound for the number of vanishing traces of evaluations of f.

Corollary 6.2. *For every function $f \in \mathcal{L}(r\mathfrak{p})$ such that $t = \deg(f)_\infty$ is not divisible by p, we have*

$$\left|\left\{\mathfrak{q} \in \mathbb{P}_F^1 \setminus \{\mathfrak{p}\} : \mathsf{Tr}(f(\mathfrak{q})) = 0\right\}\right| = \frac{N_L - 1}{\ell}.$$

If moreover f satisfies the condition in Item 2 of Proposition 5.5, then

$$\frac{1}{N-1}\left|\left\{\mathfrak{q} \in \mathbb{P}_F^1 \setminus \{\mathfrak{p}\} : \mathsf{Tr}(f(\mathfrak{q})) = 0\right\}\right| \leq \frac{\sigma}{\ell} + O_\sigma\left(p\sqrt{\tau}\gamma + p\ell\tau\gamma\right). \tag{6.2}$$

As we will see in Section 7, for all function fields in which we instantiate our results, it will be possible to choose $x \in F$ such that $\sigma \leq 1$. Moreover, Proposition 5.5 provides a condition for the set $S = S(f)$ to be linearly independent over $\mathbb{F}_q$, depending only on t. Consequently, if the result applies to f, it also applies to $f - \alpha$ for all $\alpha \in \mathbb{F}_q$.
In this case, we can also obtain a lower bound.

Corollary 6.3. *Assume that $\sigma \leq 1$. For every function $f \in \mathcal{L}(r\mathfrak{p})$ of degree not divisible by p, and that satisfies the condition in Item 2 of Proposition 5.5, we have*

$$\frac{1}{N-1}\left|\left\{\mathfrak{q} \in \mathbb{P}_F^1 \setminus \{\mathfrak{p}\} : \mathsf{Tr}(f(\mathfrak{q})) = \beta\right\}\right| = \frac{1}{\ell} + O\left(\ell\sqrt{\tau}\gamma p\right).$$

Proof. Let $\beta \in \mathbb{F}_\ell$. Since the map $\mathsf{Tr} : \mathbb{F}_q \to \mathbb{F}_\ell$ is onto, there exists some $\gamma \in \mathbb{F}_q$ such that $\mathsf{Tr}(\gamma) = \beta$. Applying Corollary 6.2 to $f - \gamma$, we obtain

$$\frac{1}{N-1}\left|\left\{\mathfrak{q} \in \mathbb{P}_F^1 \setminus \{\mathfrak{p}\} : \mathsf{Tr}(f(\mathfrak{q})) = \beta\right\}\right| \leq \frac{1}{\ell} + O\left(\sqrt{\tau}\gamma p + \ell\tau\gamma p\right).$$

For $\alpha \in \mathbb{F}_\ell$, let

$$\mathcal{S}_\alpha = \left|\left\{\mathfrak{q} \in \mathbb{P}_F^1 \setminus \{\mathfrak{p}\} : \mathsf{Tr}(f(\mathfrak{q})) = \alpha\right\}\right|.$$

Since

$$\sum_{\alpha \in \mathbb{F}_\ell} \mathcal{S}_\alpha = N - 1,$$

we get

$$1 - \frac{\mathcal{S}_\beta}{N-1} = \frac{1}{N-1}\sum_{\beta \neq \alpha \in \mathbb{F}_\ell} \mathcal{S}_\alpha \leq 1 - \frac{1}{\ell} + O\left(\ell\sqrt{\tau}\gamma p + \ell^2\tau\gamma p\right).$$

Thus,

$$\frac{1}{\ell} - O\left(\ell\sqrt{\tau}\gamma p + \ell^2\tau\gamma p\right) \leq \frac{\mathcal{S}_\beta}{N-1}.$$

To complete the proof, notice that if $\sqrt{\tau}\ell \geq 1$ the result is trivial, and otherwise $\tau\ell^2 < \sqrt{\tau}\ell < 1$. □

In Section 7 we use these results to construct and analyze TAG codes on some curves.

Lastly, from the special case of Artin-Schreier extensions, i.e. when $\ell = p$, we conclude an upper bound for the exponential sums arising from these functions.

Theorem 6.4. *Let $\ell = p$. Assume that $\sigma \leq 1$. For every function $f \in \mathcal{L}(r\mathfrak{p})$ of degree not divisible by p, and that satisfies the condition in Item 2 of Proposition 5.5, we have*

$$\frac{1}{N} \sum_{\mathfrak{q} \in \mathbb{P}_F^1 \setminus \{\mathfrak{p}\}} e^{\frac{2\pi i}{p} \mathsf{Tr}(f(\mathfrak{q}))} = O\left(\sqrt{\tau}\gamma p^3\right).$$

Proof. Applying Corollary 6.3 to the case $\ell = p$, we get

$$\begin{aligned}
\frac{1}{N} \sum_{\mathfrak{q} \in \mathbb{P}_F^1 \setminus \{\mathfrak{p}\}} e^{\mathsf{Tr}(f(\mathfrak{q}))} &= \frac{1}{N} \sum_{\beta=0}^{p-1} e^{\frac{2\pi i}{p}\beta} \left|\left\{\mathfrak{q} \in \mathbb{P}_F^1 \setminus \{\mathfrak{p}\} : \mathsf{Tr}(f(\mathfrak{q})) = \beta\right\}\right| \\
&= \sum_{\beta=0}^{p-1} e^{\frac{2\pi i}{p}\beta} \left(\frac{1}{p} + O\left(\sqrt{\tau}\gamma p^2\right)\right) \\
&= O\left(\sqrt{\tau}\gamma p^3\right),
\end{aligned}$$

which finishes the proof. □

6.2 Kummer Extensions and Multiplicative Character Sums

In this section, following a similar outline to Section 6.1, we instantiate the bound from Theorem 5.6 in the setting of Kummer extensions to get an upper bound on the number of rational place on such extensions. Similarly to Corollary 6.3, in Proposition 6.6 we give an argument that also yields a *lower* bound. We then apply this bound to derive upper bounds for multiplicative character sums of functions on curves, in direct analogy with the upper bounds for exponential sums obtained from the Artin–Schreier case.

Recall the setting of Section 5. Let $\phi(T) = T^d$ for $d > 1$ such that $d \mid q - 1$. Let $f \in \mathcal{L}(r\mathfrak{p})$ and assume that $t = \deg(f)_\infty = -v_\mathfrak{p}(f)$ is relatively prime to d. Let $L = F(z)$ with $\phi(z) = f$. Since $d \mid q - 1$, the field $\mathbb{F}_q$ contains a primitive d-th root of unity. By Corollary 3.7.4 in [Sti09], L/F is a cyclic Kummer extension of degree d, and hence $\phi(T) - f$ is irreducible. By Proposition 3.7.3(b) in [Sti09], the place $\mathfrak{p}$ is totally ramified in L, and moreover by Corollary 3.7.4 in [Sti09] we have

$$g_L = 1 + d(g-1) + \frac{1}{2} \sum_{\mathfrak{q} \in \mathbb{P}_F} (d - (d, v_\mathfrak{q}(f))) \deg \mathfrak{q}.$$

Note that for $\mathfrak{q} \in \mathbb{P}_F$, if $v_\mathfrak{q}(f) = 0$ then $d - (d, v_\mathfrak{q}(f)) = 0$. Otherwise, $d - (d, v_\mathfrak{q}(f)) \leq d$. Therefore,

$$\begin{aligned}
g_L &\leq 1 + d(g-1) + \frac{1}{2} \cdot \sum_{\mathfrak{q} \in \mathbb{P}_F \,:\, v_\mathfrak{q}(f) \neq 0} d \deg \mathfrak{q} \\
&\leq dg + \frac{d}{2} \left(\deg(f)_0 + \deg(f)_\infty\right) \leq d(g+t)
\end{aligned}$$

as $\deg(f)_0 = \deg(f)_\infty = t$. Thus we are in a position to apply Theorem 5.6 to L/F.

Proposition 6.5. *In the above setting, assume further that* $\deg_F(f)_\infty$ *is relatively prime to* d*, and satisfies the condition in Item 2 of Proposition 5.5. Then,*

$$\frac{N_L}{N} \leq \sigma + O_\sigma\left(\sqrt{\tau} d\gamma p + \tau d^2 \gamma p\right). \tag{6.3}$$

Similarly to Section 6.1, we can also achieve a lower bound under further assumptions.

Proposition 6.6. *Assume that* $\sigma \leq 1$*. For every function* $f \in \mathcal{L}(r\mathfrak{p})$ *such that* $\deg_F(f)_\infty$ *is relatively prime to* d*, and satisfies the condition in Item 2 of Proposition 5.5, we have*

$$\frac{N_L}{N} = 1 + O\left(\sqrt{\tau} d^2 \gamma p\right).$$

Furthermore, we have

$$\frac{1}{N}\left|\left\{\mathfrak{q} \in \mathbb{P}_F^1 \setminus \{\mathfrak{p}\} : \exists\, y \in \mathbb{F}_q^\times,\ y^d = f(\mathfrak{q})\right\}\right| = \frac{1}{d} + O\left(\sqrt{\tau} d\gamma p\right).$$

Proof. Fix representatives $\{\epsilon_1 = 1, \ldots, \epsilon_d\}$ of $\left(\mathbb{F}_q^\times / \mathbb{F}_q^{d\times}\right)$. For $i = 1, \ldots, d$, let

$$S_i = \left\{\mathfrak{q} \in \mathbb{P}_F^1 \setminus \{\mathfrak{p}\} : \exists\, y \in \mathbb{F}_q^\times,\ y^d = \epsilon_i f(\mathfrak{q})\right\}.$$

Note that the sets S_i form a partition of the set $\{\mathfrak{q} \in \mathbb{P}_F^1 \setminus \{\mathfrak{p}\} : f(\mathfrak{q}) \neq 0\}$. Denote $\mathcal{S}_i = |S_i|$ and let

$$L_i := F(z_i),\ z_i^d = \epsilon_i f.$$

Since L_i/F is Galois, every $\mathfrak{q} \in \mathbb{P}_F$ decomposes in L_i to places of the same degree with the same ramification index. Hence, rational places in L_i must lie above splitting rational places in F, or above ramified rational places. Let $\mathbb{P}_{L_i}^1$ be the set of rational place in L_i. We have,

$$\begin{aligned} N_{L_i} = &\left|\left\{\mathfrak{Q} \in \mathbb{P}_{L_i}^1 : \mathfrak{Q} \text{ lies above } \mathfrak{q} \text{ such that } f(\mathfrak{q}) \neq 0\right\}\right| \\ &+ \left|\left\{\mathfrak{Q} \in \mathbb{P}_{L_i}^1 : \mathfrak{Q} \text{ lies above } \mathfrak{q} \text{ such that } f(\mathfrak{q}) = 0\right\}\right| \\ &+ 1, \end{aligned}$$

where the last term corresponds to the totally ramified place lying above $\mathfrak{p}$. By Theorem 4.2, if $f(\mathfrak{q}) \neq 0$, then $\mathfrak{q} \in S_i$ if and only if $\mathfrak{q}$ splits completely into d rational places in L_i. Hence the first summand in the RHS is $d\mathcal{S}_i$. As for the second summand, note that the number of rational places $\mathfrak{q}$ in F with $f(\mathfrak{q}) = 0$ is at most $\tau\frac{N}{\sqrt{q}} = t = \deg(f)_0$, and there are at most d places in L_i lying above each. Thus,

$$0 \leq N_{L_i} - d\mathcal{S}_i = O\left(d\tau \frac{N}{\sqrt{q}}\right). \tag{6.4}$$

Thus, by applying Proposition 6.5 to L_i in the inequality above on the left, we obtain

$$\frac{\mathcal{S}_i}{N-1} \leq \frac{1}{d} + O\left(\sqrt{\tau}\gamma p + \tau d\gamma p\right). \tag{6.5}$$

On the other hand we have

$$\sum_{i=1}^{d} \mathcal{S}_i + \left|\left\{\mathfrak{q} \in \mathbb{P}^1_F \setminus \{\mathfrak{p}\} : f(\mathfrak{q}) = 0\right\}\right| = N - 1.$$

Thus,

$$\begin{aligned}\frac{N_L}{N-1} &\geq \frac{d}{N-1}\mathcal{S}_1 \\ &\geq d - \frac{d}{N-1}\left|\left\{\mathfrak{q} \in \mathbb{P}^1_F \setminus \{\mathfrak{p}\} : f(\mathfrak{q}) = 0\right\}\right| - \frac{d}{N-1}\sum_{i=2}^{d}\mathcal{S}_i.\end{aligned}$$

Notice that $\tau \leq 1$, and hence $\deg(f)_0 < \frac{N}{\sqrt{q}}$. Therefore,

$$\left|\left\{\mathfrak{q} \in \mathbb{P}^1_F \setminus \{\mathfrak{p}\} : f(\mathfrak{q}) = 0\right\}\right| = O\left(\frac{N}{\sqrt{q}}\right).$$

Combined with Inequality (6.5), we obtain

$$\frac{N_L}{N-1} \geq d - O\left(\frac{d}{\sqrt{q}}\right) - (d-1) - O\left(\sqrt{\tau}d^2\gamma p + \tau d^3\gamma p\right).$$

To complete the proof of the first part, notice that if $\sqrt{\tau}d \geq 1$ the result is trivial, and otherwise $\tau d^2 < \sqrt{\tau}d < 1$.
To conclude the second part, plug the first part into the right equality in (6.4). □

Lastly, we conclude the bound for multiplicative character sums arising from these functions.

Theorem 6.7. *For all multiplicative characters $\chi \in \widehat{\mathbb{F}_q^\times}$ of order d, and for all functions $f \in F$ which satisfy the conditions of Proposition 6.6, we have*

$$\frac{1}{N}\sum_{\mathfrak{q} \in \mathbb{P}^1_F \setminus \{\mathfrak{p}\}} \chi(f(\mathfrak{q})) = O\left(\sqrt{\tau}d^2\gamma p\right).$$

Proof. We use the notation of $\mathcal{S}_i$ and ϵ_i used in Proposition 6.6. Notice that,

$$\begin{aligned}\frac{1}{N}\sum_{\mathfrak{q} \in \mathbb{P}^1_F \setminus \{\mathfrak{p}\}} \chi(f(\mathfrak{q})) &= \frac{1}{N}\sum_{i=1}^{d}\chi(\epsilon_i)^{-1}\mathcal{S}_i \\ &= \left(\frac{1}{N}\sum_{i=1}^{d}\chi(\epsilon_i)^{-1}\frac{1}{d}\right) + O\left(\sqrt{\tau}d^2\gamma p\right) \\ &= O\left(\sqrt{\tau}d^2\gamma p\right),\end{aligned}$$

where we have used the second part of Proposition 6.6. □

7 TAG Codes Instantiations

In this section, we use the results obtained in the previous sections to construct and analyze TAG codes of specific function fields F. As discussed in Section 2.1.3, the functions captured by our result are roughly those of degree $t < \frac{g}{p^2}$. Therefore, in order to construct TAG codes with high rate, it is necessary to consider curves that admit a place for which the associated Riemann-Roch spaces of degree $< \frac{g}{p^2}$ have sufficiently large dimensions.

7.1 The Hermitian TAG Code

Let r be a power of a prime p, and let $q = r^2$. The Hermitian function field over $\mathbb{F}_q$ is defined by

$$F = \mathbb{F}_q(x, y), \qquad y^r + y = x^{r+1}. \tag{7.1}$$

It is an elementary abelian p-extension of $\mathbb{F}_q(x)$ of degree r. Consider the place $\mathfrak{p}_\infty \in \mathbb{P}_{\mathbb{F}_q(x)}$. Let $\mathfrak{P}$ be some place lying above it. Then

$$v_{\mathfrak{P}}(x^{r+1}) = e(\mathfrak{P}|\mathfrak{p}_\infty) \cdot v_{\mathfrak{p}_\infty}(x^{r+1}) = -(r+1) \cdot e(\mathfrak{P}|\mathfrak{p}_\infty) < 0,$$

hence by Equation (7.1),

$$v_{\mathfrak{P}}(y^r + y) = r \cdot v_{\mathfrak{P}}(y) = -(r+1) \cdot e(\mathfrak{P}|\mathfrak{p}_\infty).$$

Since r and $r+1$ are coprime, it follows that

$$\begin{aligned} e(\mathfrak{P}|\mathfrak{p}_\infty) &= r, \\ v_{\mathfrak{P}}(x) &= -r, \\ v_{\mathfrak{P}}(y) &= -(r+1). \end{aligned}$$

In particular, the place $\mathfrak{p}_\infty$ is totally ramified. Let $\mathfrak{P}_\infty$ be the only place lying above it.

This function field has $N = r^3 + 1$ rational places - $\mathfrak{P}_\infty$, and another place $\mathfrak{P}_{\alpha,\beta}$ for all $\alpha, \beta \in \mathbb{F}_q$ such that $\alpha^{r+1} = \beta^r + \beta$. Taking x as the element with $\deg(x)_\infty = s$, we have $s = r$ and $\sigma = s\frac{q}{N} = \frac{r^3}{r^3+1} \leq 1$. The genus of this curve is $g = \frac{r(r-1)}{2}$, and hence $\gamma = g\frac{\sqrt{q}}{N} = \frac{r^2(r-1)}{2(r^3+1)} = \Theta(1)$.
Fix an integer $r \leq T \leq g$. We have

$$\mathcal{L}(T\mathfrak{P}_\infty) = \mathsf{Span}_{\mathbb{F}_q}\left\{x^i y^j : i, j \geq 0,\ ir + j(r+1) \leq T\right\}.$$

To use Corollary 6.2, we seek a subspace of $\mathcal{L}(T\mathfrak{P}_\infty)$ consisting of functions whose degrees are not divisible by p, and that satisfy the condition in Item 2 of Proposition 5.5. Notice that $r = s$, and that

$$\deg(x^i y^j)_\infty = -v_{\mathfrak{P}_\infty}(x^i y^j) = ir + j(r+1) = (i+j)r + j.$$

Thus, if $p \nmid j$ then the degree of $x^i y^j$ is not divisible by p. Moreover, if $i+j$ is relatively prime to ℓ, and $j\frac{q}{N} < \frac{1}{3\ell}$, then the monomial $x^i y^j$ satisfies the condition of Item 2. Therefore we define $V \leq \mathcal{L}(T\mathfrak{P}_\infty)$ by

$$\begin{aligned} V = \mathsf{Span}_{\mathbb{F}_q}\{x^i y^j : & i,j \geq 0, \\ & ir + j(r+1) \leq T, \\ & j \not\equiv 0 \mod p, \\ & \gcd(i+j,\ell) = 1, \\ & j < r/(3\ell)\}. \end{aligned} \tag{7.2}$$

Every function $f \in V$ must satisfy the conditions of Corollary 6.2. We are in a position to obtain a code and calculate its dimension and distance.

Theorem 7.1. *Let T be an integer such that $r \leq T \leq g$, and let ℓ be a power of p such that $\mathbb{F}_p \subseteq \mathbb{F}_\ell \subseteq \mathbb{F}_q$. Let V be defined as in Equation (7.2). Let $\mathfrak{P}_1, \ldots, \mathfrak{P}_{N-1}$ be the set of all rational places of the Hermitian function field, except $\mathfrak{P}_\infty$. Let $\mathsf{TC} : V \to \mathbb{F}_\ell^{r^3}$ be the trace code of V to $\mathbb{F}_\ell$, defined by*

$$\mathsf{TC}(f) = \left(\mathsf{Tr}(f(\mathfrak{P}_1)), \ldots, \mathsf{Tr}(f(\mathfrak{P}_{N-1}))\right).$$

Then, this code has rate ρ and relative distance δ satisfying

$$\rho = \Omega\left(\frac{T^2 \log(q)}{\ell \log(\ell) q^{5/2}}\right), \tag{7.3}$$

$$\delta = 1 - \frac{1}{\ell} - O_p\left(\frac{\sqrt{T}}{\sqrt{q}} + \ell\frac{T}{q}\right). \tag{7.4}$$

Proof. Every function $f \in V$ satisfies the conditions of Corollary 6.2. Hence, the distance of the code is at least

$$\delta = 1 - \frac{1}{\ell} - O_p(\sqrt{\tau} + \ell\tau),$$

where $\tau\frac{N}{r} = T$. Using Equation (7.2), it is easy to verify that

$$\dim V = \Omega\left(\frac{1}{\ell}\left(\frac{T}{r}\right)^2\right).$$

Hence,

$$\rho = \frac{\dim V \cdot \log_\ell(q)}{r^3} = \Omega\left(\frac{T^2 \log(q)}{\ell \log(\ell) q^{5/2}}\right).$$

□

We instantiate Theorem 7.1 to the setting of ε-balanced codes to get an $\mathbb{F}_2$ linear code.

Theorem 7.2. *For every k and every $\varepsilon > 0$, there are choices for $T, r = 2^a$ such that the Hermitian trace code $\mathsf{TC}(V)$ from $\mathbb{F}_q$ to $\mathbb{F}_2$ is a $[n, \Omega(k)]_2$ linear code that is ε-balanced, with*

$$n = O\left(\frac{k}{\varepsilon^4}\right)^{3/2}.$$

Proof. Let $p = \ell = 2$. Pick r and T with $r \leq T \leq \frac{r(r-1)}{2}$, where r is a power of 2, and

$$T = \Theta\left(\frac{k}{\varepsilon^2}\right),$$
$$r = \Theta\left(\frac{\sqrt{k}}{\varepsilon^2}\right),$$

such that the O-term in Equation (7.4) is at most ε. Consider the construction of Theorem 7.1 over $\mathbb{F}_q$ with these choices of T, r, and $q = r^2$. It admits an ε-balanced codes over $\mathbb{F}_2$, with rate

$$\Omega\left(\frac{T^2 \log(q)}{r^2}\right) = \Omega(k \log(q)).$$

Since $n = r^3$, we have

$$n = r^3 = O\left(\frac{k^{3/2}}{\varepsilon^6}\right) = O\left(\frac{k}{\varepsilon^4}\right)^{3/2},$$

as claimed. □

7.2 The Norm-Trace TAG Code

Here we present some known facts that can be found in [MP12]. Let r be a prime power, let $e \geq 2$ be an integer and let $q = r^e$. The extended norm-trace function field is a function field over $\mathbb{F}_q$, with a parameter $u > 1$ such that $u \mid \frac{q-1}{r-1}$, and is defined by

$$F = \mathbb{F}_q(x, y), \qquad y^{r^{e-1}} + y^{r^{e-2}} + \cdots + y = x^u. \tag{7.5}$$

The extended norm-trace function field $F/\mathbb{F}_q$ has genus $g = \frac{(u-1)(r^{e-1}-1)}{2}$, and

$$N = r^{e-1}(u(r-1)+1) + 1$$

places of degree one. Hence,

$$g \approx \frac{ur^{e-1}}{2}, \qquad N \approx ur^e, \qquad \frac{N}{g} \approx 2r.$$

Thus we have

$$\gamma = g\frac{\sqrt{q}}{N} = \Theta\left(r^{e/2-1}\right). \tag{7.6}$$

Consider the place $\mathfrak{p}_\infty \in \mathbb{P}_{\mathbb{F}_q(x)}$. Let $\mathfrak{P}$ be some place lying above it. Then

$$v_{\mathfrak{P}}(x^u) = e(\mathfrak{P}|\mathfrak{p}_\infty) \cdot v_{\mathfrak{p}_\infty}(x^u) = -u \cdot e(\mathfrak{P}|\mathfrak{p}_\infty) < 0$$

and hence by Equation (7.5),

$$v_{\mathfrak{P}}(y^{r^{e-1}} + y^{r^{e-2}} + \ldots + y) = r^{e-1} \cdot v_{\mathfrak{P}}(y) = -u \cdot e(\mathfrak{P}|\mathfrak{p}_\infty).$$

Since $u \mid q-1$ we have $(u,p) = 1$, hence $r^{e-1} \mid e(\mathfrak{P}|\mathfrak{p}_\infty)$. As $e(\mathfrak{P}|\mathfrak{p}_\infty) \leq [F : \mathbb{F}_q(x)] = r^{e-1}$, we conclude that

$$\begin{aligned} e(\mathfrak{P}|\mathfrak{p}_\infty) &= r^{e-1}, \\ v_{\mathfrak{P}}(x) &= -r^{e-1}, \\ v_{\mathfrak{P}}(y) &= -u. \end{aligned}$$

In particular, the place $\mathfrak{p}_\infty$ is totally ramified. Let $\mathfrak{P}_\infty$ be the only place lying above it. From now on, assume that $u = \frac{q-1}{r-1} = \sum_{i=0}^{e-1} r^i = O(r^{e-1})$. We remark that in this case, Equation (7.5) may be written as

$$F = \mathbb{F}_q(x,y), \quad \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_r}(y) = N_{\mathbb{F}_q/\mathbb{F}_r}(x).$$

Taking x as the element with $\deg(x)_\infty = s$, we get that $s = r^{e-1}$ and

$$\sigma = s\frac{q}{N} = r^{e-1}\frac{r^e}{ur^e - ur^{e-1} + r^{e-1} + 1} = \frac{r^{e-1}}{u(1-1/r) + 1/r + 1/r^e}.$$

Since $u = \frac{q-1}{r-1}$, we have $u\left(1 - \frac{1}{r}\right) = r^{e-1} - \frac{1}{r}$. Thus we obtain

$$\sigma = \frac{r^{e-1}}{r^{e-1} + 1/r^e} \leq 1.$$

Fix an integer $r^{e-1} \leq T \leq g$. We have

$$\mathcal{L}(T\mathfrak{P}_\infty) = \mathsf{Span}_{\mathbb{F}_q}\left\{x^i y^j : i,j \geq 0,\ ir^{e-1} + ju \leq T\right\}.$$

To use Corollary 6.2, we seek a subspace of $\mathcal{L}(T\mathfrak{P}_\infty)$ consisting of functions whose degrees are not divisible by p, and that satisfy the condition in Item 2 of Proposition 5.5. Notice that

$$\deg(x^i y^j)_\infty = -v_{\mathfrak{P}_\infty}(x^i y^j) = ir^{e-1} + ju = (i+j)r^{e-1} + j\sum_{i=0}^{e-2} r^i.$$

Thus, if $p \nmid j$ then the degree of $x^i y^j$ is not divisible by p. Write $j = a(r-1)+b$ for some integers a, b such that $0 \le a < r^{e-2}$ and $0 \le b < r-1$. Then,

$$\begin{aligned} -v_{\mathfrak{P}_\infty}(x^i y^j) &= (i+j)r^{e-1} + (a(r-1)+b)\sum_{i=0}^{e-2} r^i \\ &= (i+j)r^{e-1} + a(r^{e-1}-1) + b\sum_{i=0}^{e-2} r^i \\ &= (i+j+a)r^{e-1} + b\sum_{i=0}^{e-2} r^i - a. \end{aligned}$$

Notice that $s = r^{e-1}$. If $\gcd(i+j+a,\, \ell) = 1$, and $\left(b\sum_{i=0}^{e-2} r^i - a\right)\frac{q}{N} = O\left(\frac{b}{r}\right) < \frac{1}{\ell}$, then the monomial $x^i y^j$ satisfies the condition of Item 2. Let $V \le \mathcal{L}(T\mathfrak{P}_\infty)$ be defined by

$$\begin{aligned} V = \mathsf{Span}_{\mathbb{F}_q}\{x^i y^j : & i, j \ge 0, \\ & ir^{e-1} + ju \le T, \\ & j \neq 0 \mod p \\ & \gcd(i+j+a, \ell) = 1, \\ & b < O\left(\frac{r}{\ell}\right)\}. \end{aligned} \tag{7.7}$$

Thus, every function $f \in V$ satisfies the conditions of Corollary 6.2.

Theorem 7.3. *Let T be an integer such that $r^{e-1} \le T \le g$, and let ℓ be a power of p such that $\mathbb{F}_p \subseteq \mathbb{F}_\ell \subseteq \mathbb{F}_q$. Let V be defined as in Equation (7.7). Let $\mathfrak{P}_1, \ldots, \mathfrak{P}_{N-1}$ be the set of all rational places in the norm-trace function field, except $\mathfrak{P}_\infty$. Let $\mathsf{TC} : V \to \mathbb{F}_\ell^{N-1}$ be the trace code to of V to $\mathbb{F}_\ell$, defined by*

$$\mathsf{TC}(f) = \left(\mathsf{Tr}(f(\mathfrak{P}_1)), \ldots, \mathsf{Tr}(f(\mathfrak{P}_{N-1}))\right).$$

Then,

$$\rho = \Omega\left(\frac{T^2 \log(q)}{\ell \log(\ell) r^{4e-3}}\right), \tag{7.8}$$

$$\delta = 1 - \frac{1}{\ell} - O_p\left(\sqrt{\frac{T}{r^{e/2+1}}} + \ell\frac{T}{r^e}\right). \tag{7.9}$$

Remark 7.4. *Since $r^{e-1} \le T$, Equation (7.9) is non-trivial only if $e < 4$.*

Proof. Every function $f \in V$ satisfies the conditions of Corollary 6.2. Hence, the distance of the code is at least

$$\delta = 1 - \frac{1}{\ell} - O_p(\sqrt{\tau}\gamma + \ell\tau\gamma),$$

where $\tau \frac{N}{r^{e/2}} = T$. We have,

$$\tau = \Theta\left(T \frac{r^{e/2}}{r^{2e-1}}\right) = \Theta\left(\frac{T}{r^{3e/2-1}}\right).$$

Together with Equation (7.6), we obtain Equation (7.9). To analyze the rate of the code, using Equation (7.7) it is easy to verify that

$$\dim V = \Omega\left(\frac{1}{\ell}\left(\frac{T}{r^{e-1}}\right)^2\right).$$

We output $N - 1 = \Theta\left(r^{2e-1}\right)$ elements in $\mathbb{F}_\ell$, hence

$$\rho = \frac{\dim V \cdot \log_\ell(q)}{N} = \Omega\left(\frac{T^2 \log(q)}{\ell \log(\ell) r^{4e-3}}\right).$$

□

We instantiate Theorem 7.3 with $e = 3$ in the setting of ε-balanced codes, thereby obtaining an $\mathbb{F}_2$-linear code. In this case, the resulting ε-balanced codes are significantly weaker than those in Theorem 7.2, primarily because γ is non-constant and appears in the error term of the relative distance.

Theorem 7.5. *For every k and every $\varepsilon > 0$, there are choices for $T, r = 2^a$ such that the trace code $\mathsf{TC}(V)$ of the norm-trace curve with $e = 3$ from $\mathbb{F}_q$ to $\mathbb{F}_2$ is a $[n, \Omega(k)]_2$ linear code that is ε-balanced, with*

$$n = O\left(\frac{k}{\varepsilon^4}\right)^5.$$

Proof. In the above setting, let $e = 3$, and let $p = \ell = 2$. Pick r, T such that $r^2 \leq T \leq g$ where r is a power of 2, and

$$T = \Theta\left(\frac{k^{5/2}}{\varepsilon^8}\right),$$
$$r = \Theta\left(\frac{k}{\varepsilon^4}\right),$$

such that the O-term in Equation (7.9) is at most ε. Consider the construction of Theorem 7.3 over $\mathbb{F}_q$ with these choices of $e = 3$, T, r, and $q = r^2$. It admits an ε-balanced codes over $\mathbb{F}_2$, with rate

$$\Omega\left(\frac{T^2 \log(q)}{r^4}\right) = \Omega(k \log(q)) = \Omega(k).$$

Since $n = O(r^5)$, we have

$$n = O(r^5) = O\left(\frac{k}{\varepsilon^4}\right)^5,$$

as claimed. □

7.3 The Hermitian Tower TAG Code

In this subsection we mainly follow [GX12, Section 3.1].

Let p be a prime number, and $r = p^\ell$ for some integer $\ell \geq 1$. Let $q = r^2$ and let $e \leq r/2$ be an integer. The Hermitian tower is defined by the following recursive equations

$$x_{i+1}^r + x_{i+1} = x_i^{r+1}, \qquad i = 1, 2, \ldots, e-1,$$

and $F_e = \mathbb{F}_q(x_1, x_2, \ldots, x_e)$. The place $\mathfrak{p}_\infty \in \mathbb{P}_{\mathbb{F}_q(x)}$ is totally ramified in F_e and let $\mathfrak{P}_\infty$ be the unique place lying above it. This is a rational place. There are exactly r^{e+1} more rational places in $\mathbb{P}_{F_e}$, coming from e-tuples $(\alpha_1, \ldots, \alpha_e) \in \mathbb{F}_q^e$ such that $\alpha_{i+1}^r + \alpha_{i+1} = \alpha_i^{r+1}$, $i = 1, 2, \ldots, e-1$. The genus of F_e is

$$g_e = \frac{1}{2}\left(\sum_{i=1}^{e-1} r^e \left(1 + \frac{1}{r}\right)^{i-1} - (r+1)^{e-1} + 1\right) \leq er^e.$$

Hence,

$$\gamma = g\frac{\sqrt{q}}{N} \leq er^e \frac{r}{r^{e+1}} = e. \tag{7.10}$$

Taking x as the element with $\deg(x)_\infty = s$, we have $s = -v_{\mathfrak{P}_\infty}(x) = e(\mathfrak{P}_\infty|\mathfrak{p}_\infty) = r^{e-1}$. Hence

$$\sigma = s\frac{q}{N} = r^{e-1}\frac{r^2}{r^{e+1}+1} \leq 1.$$

Moreover, for all $1 \leq i \leq e$, we have

$$v_{\mathfrak{P}_\infty}(x_i) = r^{e-i}(r+1)^{i-1}.$$

Next, fix an integer $r^{e-1} \leq T \leq g_e \leq er^e$. We have

$$\mathcal{L}(T\mathfrak{P}_\infty) = \mathsf{Span}_{\mathbb{F}_q}\left\{x_1^{j_1}\cdots x_e^{j_e} : (j_1, \ldots, j_e) \in \mathbb{Z}_{\geq 0}^e, \sum_{i=1}^e j_i r^{e-i}(r+1)^{i-1} \leq T\right\}.$$

To use Corollary 6.2, we seek a subspace of $\mathcal{L}(T\mathfrak{P}_\infty)$ consisting of functions whose degrees are not divisible by p, and that satisfy the condition in Item 2 of Proposition 5.5. Notice that $s = r^{e-1}$, and that

$$\begin{aligned} -v_{\mathfrak{P}_\infty}(x_1^{j_1}\cdots x_e^{j_e}) &= \sum_{i=1}^e j_i r^{e-i}(r+1)^{i-1} \\ &= j_1 r^{e-1} + \sum_{i=2}^e j_i(r^{e-1} + O_e(r^{e-2})). \end{aligned}$$

Hence, if j_e is not divisible by p, then $\deg(x_1^{j_1}\cdots x_e^{j_e})_\infty$ is not divisible by p. Moreover, if $j_i \le O_e(\frac{r}{\ell})$ for all $i \ge 2$, then this monomial satisfies the condition of Item 2. Let $V \le \mathcal{L}(T\mathfrak{P}_\infty)$ be defined by

$$\begin{aligned} V = \mathsf{Span}_{\mathbb{F}_q}\{x_1^{j_1}\cdots x_e^{j_e} \ : \ & j_i \ge 0, \\ & \sum_{i=1}^{e} j_i r^{e-i}(r+1)^{i-1} \le T, \\ & j_e \neq 0 \mod p, \\ & \gcd\left(\sum_{i=1}^{e} j_i,\ \ell\right) = 1, \\ & j_i \le O_e\left(\frac{r}{\ell}\right) \forall i \ge 2\}. \end{aligned} \tag{7.11}$$

Thus, every function $f \in V$ satisfies the conditions of Corollary 6.2.

Theorem 7.6. *Let T be an integer such that $r^{e-1} \le T \le g_e \le er^e$, and let ℓ be a power of p such that $\mathbb{F}_p \subseteq \mathbb{F}_\ell \subseteq \mathbb{F}_q$. Let V be defined as in Equation (7.11). Let $\mathfrak{P}_1, \ldots, \mathfrak{P}_{N-1}$ be the set of all rational places in F_e, except $\mathfrak{P}_\infty$. Let $\mathsf{TC} : V \to \mathbb{F}_\ell^{N-1}$ be the trace code to of V to $\mathbb{F}_\ell$, defined by*

$$\mathsf{TC}(f) = \left(\mathsf{Tr}(f(\mathfrak{P}_1)), \ldots, \mathsf{Tr}(f(\mathfrak{P}_{N-1}))\right).$$

Then,

$$\rho = \Theta_e\left(\frac{T^e \log(q)}{\ell^{e-1} r^{e(e-1)} \log(\ell)}\right), \tag{7.12}$$

$$\delta = 1 - \frac{1}{\ell} - O_{p,e}\left(\sqrt{\frac{T}{r^e}} + \ell\frac{T}{r^e}\right). \tag{7.13}$$

Proof. Every function $f \in V$ satisfies the conditions of Corollary 6.2. Hence, the relative distance of the code is at least

$$\delta = 1 - \frac{1}{\ell} - O_p(\sqrt{\tau}\gamma + \ell\tau\gamma),$$

where $\tau\frac{N}{r} = T$. We have,

$$\tau = \Theta\left(T\frac{r}{r^{e+1}}\right) = \Theta\left(\frac{T}{r^e}\right).$$

Together with Equation (7.10), we obtain Equation (7.13). Using Equation (7.11), it is easy to verify that

$$\dim V = \Omega_e\left(\frac{T}{r^{e-1}}\left(\frac{T}{\ell r^{e-1}}\right)^{e-1}\right)$$

Since we output $N - 1 = r^{e+1}$ elements in $\mathbb{F}_\ell$, we conclude

$$\rho = \frac{\dim V \cdot \log_\ell(q)}{N} = \Theta_e\left(\frac{T^e \log(q)}{\ell^{e-1} r^{e(e-1)} \log(\ell)}\right).$$

□

We instantiate Theorem 7.6 to the setting of ε-balanced codes to get an $\mathbb{F}_2$ linear code.

Theorem 7.7. *For every k, $\varepsilon > 0$ and $e \geq 2$, there are choices for $T, r = 2^a$ such that the trace code of the Hermitian tower of level e $\mathsf{TC}(V)$ from $\mathbb{F}_q$ to $\mathbb{F}_2$ is a $[n, \Omega_e(k)]_2$ linear code that is ε-balanced, with*

$$n = O_e\left(\frac{k}{\varepsilon^{2e}}\right)^{\frac{e+1}{e}}.$$

Proof. Let $p = \ell = 2$. Pick r, T such that $r^{e-1} \leq T \leq g_e \leq er^e$, where r is a power of 2, and

$$T = \Theta_e\left(\frac{k}{\varepsilon^{2(e-1)}}\right),$$
$$r = \Theta_e\left(\frac{k^{1/e}}{\varepsilon^2}\right),$$

such that the O-term in Equation (7.13) is at most ε. Consider the construction of Theorem 7.6 over $\mathbb{F}_q$ with these choices of T, r, and $q = r^2$. It admits an ε-balanced codes over $\mathbb{F}_2$, with rate

$$\Omega_e\left(\frac{T}{r^{e-1}}\right)^e = \Omega_e\left(\frac{k}{\varepsilon^{2(e-1)}} \frac{\varepsilon^{2(e-1)}}{k^{\frac{e-1}{e}}}\right)^e = \Omega_e(k).$$

Since $n = r^{e+1}$, we have

$$n = r^{e+1} = O_e\left(\frac{k^{\frac{e+1}{e}}}{\varepsilon^{2(e+1)}}\right) = O_e\left(\frac{k}{\varepsilon^{2e}}\right)^{\frac{e+1}{e}},$$

as claimed. □

8 TAG Codes vs. Concatenation in the High Distance Regime

In this section we compare binary TAG codes with the familiar approach of concatenating with the Hadamard code, thereby proving Theorem 2.3. We consider here the case where

the error term guaranteed in Corollary 6.2 is $O(\tau)$, which would lead to the $\Omega(\varepsilon^3)$ lower bound on the rate. The "Moreover" part of Theorem 2.3, corresponds to $O(\sqrt{\tau})$, is similar.

Let C be a one-point evaluation AG code, defined by an algebraic function field $F/\mathbb{F}_q$ with genus g, and a set of N rational places Y with respect to a divisor $G = T\mathfrak{P}$ such that $\mathfrak{P} \notin Y, T < g$. Assume that F contains an element $x \in F$ with $\frac{q}{N}\deg(x)_\infty = 1+O(q^{-1/2})$, and $N/g = \Omega(\sqrt{q})$. Let $\ell = \ell(T\mathfrak{P})$, the dimension of the corresponding Riemann-Roch space. This AG code has parameters $n_1 = N$, designated distance $d_1 = N - T$, and dimension ℓ, and it is defined over $\mathbb{F}_q$. We compare the parameters of the two methods described above:

1. **TAG codes.** Without loss of generality, assume that every function $f \in \mathcal{L}(T\mathfrak{P})$ satisfies the conditions of Corollary 6.2. The error term guaranteed in Corollary 6.2 is $O(\tau) = O\left(\frac{t\sqrt{q}}{N}\right)$. Then the resulting TAG code has parameters

$$\begin{aligned} n_T &= N, \\ k_T &= \ell \log(q), \\ \varepsilon_T &= \Omega\left(\frac{T\sqrt{q}}{N}\right). \end{aligned}$$

2. **Concatenation with Hadamard.** The resulting code has parameters

$$\begin{aligned} n_H &= Nq, \\ k_H &= \ell \log(q), \\ \varepsilon_H &\leq \frac{T}{N}. \end{aligned}$$

We let $k = k_H = k_T$. Ta-Shma and Ben-Aroya [BT13] proved that in the regime of $g = \Omega(\sqrt{q})$ we have

$$n_H = \Omega\left(\frac{k}{\varepsilon_H^{2.5}\log(k/\varepsilon_H)}\right). \tag{8.1}$$

Assume that $\alpha, \beta > 0$ are such that

$$n_H = \Omega\left(\frac{k^\alpha}{\varepsilon_H^\beta}\right), \tag{8.2}$$

and note that per Equation (8.1), $\beta \geq 2.5$. Observe that $\varepsilon_T = \Omega(\varepsilon_H\sqrt{q})$, $n_T = n_H/q$. Hence,

$$n_T = \frac{n_H}{q} = \Omega\left(\frac{k^\alpha \varepsilon_H^{-\beta}}{q}\right) = \Omega\left(k^\alpha \varepsilon_T^{-\beta} q^{\beta/2-1}\right).$$

Notice that by Claim 3.1, in order to have $\mathcal{L}(T\mathfrak{P}) \neq \mathbb{F}_q$, we must have $T \geq \frac{N}{q+1}$, hence as $\varepsilon_T = \Omega(\frac{T\sqrt{q}}{N})$ we have $\sqrt{q} = \Omega(\frac{1}{\varepsilon_T})$. Finally, we obtain

$$n_T = \Omega\left(k^\alpha \varepsilon_T^{-\beta-(\beta-2)}\right) = \Omega\left(\frac{k^\alpha}{\varepsilon_T^{2\beta-2}}\right).$$

Comparing this with Equation (8.2), recalling that $\beta \geq 2.5$, wee see that the exponent in the dependence in ε in the TAG code, $2\beta - 2$, is larger by at least 0.5 from the corresponding exponent for the concaentated code. Indeed, the difference is $(2\beta-2)-\beta = \beta - 2 \geq 0.5$.

Acknowledgment

We are grateful to Amnon Ta-Shma for illuminating discussions and for sharing his insights on trace codes of algebraic geometric codes.

References

[AGHP92] Noga Alon, Oded Goldreich, Johan Håstad, and René Peralta. Simple constructions of almost k-wise independent random variables. *Random Structures & Algorithms*, 3(3):289–304, 1992.

[Bom66] Enrico Bombieri. On exponential sums in finite fields. *American Journal of Mathematics*, 88(1):71–105, 1966.

[BT13] Avraham Ben-Aroya and Amnon Ta-Shma. Constructing small-bias sets from Algebraic-Geometric codes. *Theory of Computing*, 9(5):253–272, 2013.

[CCM24] Gil Cohen, Itay Cohen, and Gal Maor. Tight bounds for the zig-zag product. In *Annual Symposium on Foundations of Computer Science (FOCS)*, pages 1470–1499. IEEE, 2024.

[Del75] P. Delsarte. On subfield subcodes of modified Reed–Solomon codes. *IEEE Transactions on Information Theory*, 21(5):575–576, 1975.

[DMW24] Dean Doron, Jonathan Mosheiff, and Mary Wootters. When do low-rate concatenated codes approach the gilbert-varshamov bound? In *Approximation, Randomization, and Combinatorial Optimization. Algorithms and Techniques (APPROX/RANDOM)*, volume 317, pages 53:1–53:12. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2024.

[Gil52] Edgar N. Gilbert. A comparison of signalling alphabets. *Bell System Technical Journal*, 31(3):504–522, May 1952.

[Gop81] V. D. Goppa. Codes on algebraic curves. *Doklady Akademii Nauk SSSR*, 259(6):1289–1290, 1981.

[Gro77] Alexander Grothendieck. Formule de lefschetz. In *Cohomologie ℓ-adique et Fonctions L (SGA 5)*, volume 589 of *Lecture Notes in Mathematics*, pages 73–137. Springer, 1977.

[GS95] Arnaldo García and Henning Stichtenoth. A tower of Artin–Schreier extensions of function fields attaining the Drinfeld–Vlăduţ bound. *Inventiones mathematicae*, 121:211–222, 1995.

[GS96] Arnaldo García and Henning Stichtenoth. On the asymptotic behaviour of some towers of function fields over finite fields. *Journal of Number Theory*, 61(2):248–273, 1996.

[GX12] Venkatesan Guruswami and Chaoping Xing. Folded codes from function field towers and improved optimal rate list decoding. In *Annual Symposium on Theory of Computing (STOC)*, page 339–350. ACM, 2012.

[HH+24] Pooya Hatami, William Hoza, et al. Paradigms for unconditional pseudorandom generators. *Foundations and Trends® in Theoretical Computer Science*, 16(1-2):1–210, 2024.

[Jus72] J. Justesen. A class of constructive asymptotically good algebraic codes. *IEEE Transactions on Information Theory*, 18(5):652–656, 1972.

[KTY24] Swastik Kopparty, Amnon Ta-Shma, and Kedem Yakirevitch. Character sums over AG codes. *ECCC*, 2024. https://eccc.weizmann.ac.il/report/2024/069/ (manuscript).

[KTY25] Swastik Kopparty, Amnon Ta-Shma, and Kedem Yakirevitch. Trace Hermitian codes have vanishing bias. Personal communication, 2025.

[LC16] Phong Le and Sunil Chetty. On the dimension of AG trace codes. *arXiv*, 2016. https://arxiv.org/abs/0902.1729 (manuscript).

[MP12] Gretchen L. Matthews and Justin Peachey. Small-bias sets from extended norm-trace codes. *Proceedings of Fq10, Contemporary Mathematics*, 44, 2012.

[MRRW77] Robert McEliece, Eugene Rodemich, Howard Rumsey, and Lloyd Welch. New upper bounds on the rate of a code via the Delsarte–MacWilliams inequalities. *IEEE transactions on Information Theory*, 23(2):157–166, 1977.

[NN93] Joseph Naor and Moni Naor. Small-bias probability spaces: efficient constructions and applications. *SIAM Journal on Computing*, 22(4):838–856, 1993.

[Sko91] Alexei N. Skorobogatov. The parameters of subcodes of algebraic-geometric codes over prime subfields. *Discrete Applied Mathematics*, 33(1-3):205–214, 1991.

[SS02] Michael Sipser and Daniel A. Spielman. Expander codes. *IEEE Transactions on Information Theory*, 42(6):1710–1722, 2002.

[Sti09] Henning Stichtenoth. *Algebraic function fields and codes*, volume 254 of *Graduate Texts in Mathematics*. Springer-Verlag, Berlin, second edition, 2009.

[Ta-17] Amnon Ta-Shma. Explicit, almost optimal, epsilon-balanced codes. In *Annual Symposium on Theory of Computing (STOC)*, pages 238–251. ACM, 2017.

[Ta-24] Amnon Ta-Shma. The hermitian trace code. https://simons.berkeley.edu/talks/amnon-ta-shma-tel-aviv-university-2024-04-08, 2024. Invited talk.

[Tan82] R. Tanner. A recursive approach to low complexity codes. *IEEE Transactions on Information Theory*, 27:533–547, 1982.

[TVZ82] M. A. Tsfasman, S. G. Vlăduţ, and Th. Zink. Modular curves, Shimura curves, and Goppa codes, better than the Varshamov–Gilbert bound. *Mathematische Nachrichten*, 109(1):21–28, 1982.

[Var57] R. R. Varshamov. Estimate of the number of signals in error-correcting codes. *Doklady Akademii Nauk SSSR*, 117:739–741, 1957. English translation reprinted in I. F. Blake (ed.), *Algebraic Coding Theory: History and Development*, Dowden, Hutchinson & Ross, 1973, pp. 68–71.

[VD83] S. G. Vlăduţ and V. G. Drinfel'd. Number of points of an algebraic curve. *Functional Analysis and Its Applications*, 17(1):53–54, 1983.

[vdV91] Marcel van der Vlugt. On the dimension of trace codes. *IEEE Transactions on Information Theory*, 37(1):196–199, 1991.

[Vla96] S. G. Vladut. Two applications of Weil-Serre's explicit formula. *Applicable Algebra in Engineering, Communication and Computing*, 7(4):279–288, 1996.

[YH19] Shudi Yang and Chuangqiang Hu. Weierstrass semigroups from a tower of function fields attaining the Drinfeld-Vladut bound. *arXiv*, 2019. https://arxiv.org/abs/1911.04269 (manuscript).

ECCC ISSN 1433-8092

https://eccc.weizmann.ac.il