An Improvement of the Gilbert–Varshamov Bound over Non-prime Fields

Alp Bassa[*], Peter Beelen[†], Arnaldo Garcia[‡], and Henning Stichtenoth[§]

Abstract

The Gilbert–Varshamov bound guarantees the existence of families of codes over the finite field $\mathbb{F}_\ell$ with good asymptotic parameters. We show that this bound can be improved for all non-prime fields $\mathbb{F}_\ell$ with $\ell \geq 49$, except possibly $\ell = 125$. We observe that the same improvement even holds within the class of transitive codes and within the class of self-orthogonal codes.

The Gilbert–Varshamov bound guarantees the existence of families of codes over the finite field $\mathbb{F}_\ell$ with good asymptotic parameters (information rate and relative minimum distance). In case $\ell \geq 49$ is a square, the bound was improved by the famous Tsfasman–Vlăduţ–Zink bound [12], using Goppa's algebraic geometry codes and modular curves with many rational points over $\mathbb{F}_\ell$. Also, for $\ell = p^n$ with odd $n > 1$ and very large p (depending on n), there are improvements of the GV bound due to Niederreiter and Xing [9].

For a linear code C we denote by $n(C)$, $k(C)$ and $d(C)$ its length, dimension and minimum distance. By $R(C) = k(C)/n(C)$ and $\delta(C) = d(C)/n(C)$ we denote the information rate and the relative minimum distance of C, respectively.

Following Manin [8], we define the set $U_\ell \subseteq \mathbb{R}^2$ to be the set of all points (δ, R) such that there exists a family of codes $(C_i)_{i\geq 0}$ over $\mathbb{F}_\ell$ with $n(C_i) \to \infty$, $\delta(C_i) \to \delta$ and $R(C_i) \to R$, as $i \to \infty$. Manin proved that there exists a function $\alpha_\ell : [0, 1] \to [0, 1]$ such that

$$U_\ell = \{(\delta, R) \in \mathbb{R}^2 \mid 0 \leq \delta \leq 1,\ 0 \leq R \leq \alpha_\ell(\delta)\ \}.$$

This function $\alpha_\ell(\delta)$ is continuous and non-increasing, and one knows that $\alpha_\ell(0) = 1$ and $\alpha_\ell(\delta) = 0$ for $1 - \ell^{-1} \leq \delta \leq 1$. All other values of $\alpha_\ell(\delta)$ are unknown.

The explicit description of the function $\alpha_\ell(\delta)$ is considered to be one of the most important (and most difficult) problems in coding theory. Many *upper* bounds for $\alpha_\ell(\delta)$ are known, among them the (asymptotic) Plotkin bound and the linear programming bound, see [6] and [7]. One may argue that *lower* bounds are more important since every non-trivial lower bound for $\alpha_\ell(\delta)$ assures the existence of long codes over $\mathbb{F}_\ell$ having good parameters. The classical lower bound for $\alpha_\ell(\delta)$ is the Gilbert–Varshamov bound (GV bound) which states that

$$\alpha_\ell(\delta) \geq 1 - \delta \log_\ell(\ell - 1) + \delta \log_\ell(\delta) + (1 - \delta) \log_\ell(1 - \delta),\ \text{for all}\ \ \delta \in (0, 1 - \ell^{-1}). \qquad (1)$$

[*]Alp Bassa is supported by Tübitak Proj. No. 112T233
[†]Peter Beelen is supported by DNRF (Denmark) and NSFC (China), grant No.11061130539.
[‡]Arnaldo Garcia is supported by CNPq (Brazil) and Sabancı University (Turkey).
[§]Henning Stichtenoth is supported by Tübitak Proj. No. 111T234.

Using algebraic geometry codes (see [10, Proposition 8.4.6], [12]), Tsfasman, Vlăduţ and Zink proved another lower bound:

$$\alpha_\ell(\delta) \geq 1 - \delta - A(\ell)^{-1} \quad \text{for} \quad 0 \leq \delta \leq 1 - \ell^{-1}. \tag{2}$$

Here $A(\ell)$ is Ihara's constant. It is defined as follows:

$$A(\ell) = \limsup_{g\to\infty} N_\ell(g)/g,$$

where $N_\ell(g)$ is the maximum number of rational places that a function field over $\mathbb{F}_\ell$ of genus g can have. If ℓ is a square then

$$A(\ell) = \sqrt{\ell} - 1, \tag{3}$$

which was first shown by Ihara [5]. Tsfasman, Vlăduţ and Zink gave in [12] an independent proof of Equation (3) in the cases $\ell = p^2$ and $\ell = p^4$, with a prime number p. Actually, in [5] and [12] only the inequality $A(\ell) \geq \sqrt{\ell} - 1$ was shown. The opposite inequality was proved shortly after by Drinfeld and Vlăduţ [3]. Combining Equation (3) with Inequality (2), one obtains the bound

$$\alpha_\ell(\delta) \geq 1 - \delta - 1/(\sqrt{\ell} - 1) \quad \text{for square} \quad \ell, \tag{4}$$

which improves the Gilbert–Varshamov bound (1) on a non-empty interval $I_\ell \subseteq (0, 1 - \ell^{-1})$ for every square $\ell \geq 49$.

We point out that, while the proof of the GV bound (1) is simple, the proof of Equation (3) (and hence the proof of the bound (4)) is highly non-trivial. It requires tools from number theory and algebraic geometry. A more elementary proof was given by Garcia and Stichtenoth [4].

For certain non-prime values of ℓ, the class field tower method of Serre provides lower bounds for $A(\ell)$ which are sufficient for improving the GV bound over $\mathbb{F}_\ell$ in these cases, see [9, Theorem 6.2.8]. However, these values of ℓ are very large. The main result of our note is that Inequality (2), together with a new lower bound for Ihara's constant $A(\ell)$, improves the GV bound (1) for most non-prime fields $\mathbb{F}_\ell$.

The harmonic mean of two positive real numbers a, b is denoted by $H(a, b)$; i.e.

$$H(a, b) = 2ab/(a + b).$$

The floor and the ceiling of a are $\lfloor a \rfloor$ and $\lceil a \rceil$, respectively.

Main Theorem. *Let $\ell = p^n$ with p prime and $n \geq 2$. Then we have*

$$\alpha_\ell(\delta) \geq 1 - \delta - \frac{1}{H\big(p^{\lceil n/2 \rceil} - 1, p^{\lfloor n/2 \rfloor} - 1\big)} \quad \textit{for} \quad 0 \leq \delta \leq 1 - \ell^{-1}. \tag{5}$$

For all non-prime $\ell \geq 49$, except for $\ell = 125$, Inequality (5) *is better than the GV bound in a non-empty interval $I_\ell \subseteq (0, 1 - \ell^{-1})$.*

Proof. If $\ell = p^n$ with n even, then $H(p^{\lceil n/2 \rceil} - 1, p^{\lfloor n/2 \rfloor} - 1) = p^{n/2} - 1 = \sqrt{\ell} - 1$, hence Inequality (5) coincides with the Tsfasman–Vlăduţ–Zink bound (4). We can therefore assume that $\ell = p^n$ with $n = 2m + 1 \geq 3$. In [1] we have constructed a family of function fields $(F_i)_{i\geq 0}$ over $\mathbb{F}_\ell$ with the limit

$$\lim_{i\to\infty} \frac{\text{number of rational places of } F_i}{\text{genus of } F_i} \geq H(p^{\lceil n/2 \rceil} - 1, p^{\lfloor n/2 \rfloor} - 1). \tag{6}$$

Together with Inequality (2), this proves the first statement of the Main Theorem. It remains to show that the bound (5) improves the GV bound for $\ell > 125$. We have to compare the function

$$f(\delta) := 1 - \delta \log_\ell(\ell - 1) + \delta \log_\ell(\delta) + (1-\delta)\log_\ell(1-\delta)$$

with the linear function

$$h(\delta) := 1 - \delta - \frac{1}{H\big(p^{\lceil n/2\rceil} - 1, p^{\lfloor n/2\rfloor} - 1\big)}$$

on the interval $(0, 1-\ell^{-1})$. We follow the proof of [9, Theorem 6.2.7]. Note that $f(\delta)$ is a convex, monotonously decreasing function on the whole interval. Hence it is sufficient to compare the values $f(\delta_0)$ and $h(\delta_0)$ where δ_0 is determined by the condition $f'(\delta_0) = -1$. One checks easily that $\delta_0 = (\ell-1)/(2\ell-1)$. The desired inequality $h(\delta_0) > f(\delta_0)$ means therefore that

$$1 - \delta_0 - 1/H > 1 - \delta_0 \log_\ell(\ell-1) + \delta_0 \log_\ell(\delta_0) + (1-\delta_0)\log_\ell(1-\delta_0), \tag{7}$$

where we set $H := H(p^{m+1}-1, p^m-1) = 2(p^{m+1}-1)(p^m-1)/(p^{m+1}+p^m-2)$. A straightforward calculation shows that Inequality (7) is equivalent to the condition

$$\frac{(2m+1)\ln p}{H} < \ln 2 + \ln\Big(1 - \frac{1}{2\ell}\Big). \tag{8}$$

Observe that $H \geq p^m$ for $p^m \neq 2$, so the left hand side of (8) is less or equal to

$$\frac{(2m+1)\ln p}{p^m},$$

while the right hand side of (8) is bigger or equal to $(\ln 2 - 1/\ell)$. This follows from the Taylor series of $\ln(1-x)$. So it will be sufficient to prove the inequality

$$(2m+1)\ln p < p^m\big(\ln 2 - 1/\ell\big). \tag{9}$$

The validity of Inequality (9) is easily checked in the cases ($p = 2$ and $m \geq 3$), ($p = 3, 5$ or 7 and $m \geq 2$) and ($p \geq 11$ and $m \geq 1$). In the case ($p = 7$ and $m = 1$) one checks directly that Inequality (8) holds. In the case ($p = 5$ and $m = 1$, i.e., $\ell = 125$), Inequality (8) does not hold. This finishes the proof of the Main Theorem. ■

We recall that a code C is called *transitive* if its automorphism group acts transitively on the coordinates of the code. For instance, *cyclic* codes are transitive. A code C which is contained in its dual $C^\perp$, is called *self-orthogonal.* In [11] it was shown that the class of transitive codes and also the class of self-orthogonal codes attain the bound (4) if ℓ is a square. Analogous results hold for all non-prime ℓ:

Theorem 2. *Let $\ell = p^n$ with p prime and $n \geq 2$, and set $H := H\big(p^{\lceil n/2\rceil} - 1, p^{\lfloor n/2\rfloor} - 1\big)$. Let $R \geq 0, \delta \geq 0$ be real numbers with $R = 1 - \delta - H^{-1}$. Then there exists a family $(C_j)_{j\geq 0}$ of linear codes over $\mathbb{F}_\ell$ with parameters $[n_j, k_j, d_j]$ such that the following hold:*

(1) all C_j are transitive codes;

(2) $n_j \to \infty$ as $j \to \infty$;

(3) $\lim_{j\to\infty} k_j/n_j \geq R$ and $\lim_{j\to\infty} d_j/n_j \geq \delta$.

For all non-prime $\ell \geq 49$, except possibly for $\ell = 125$, these codes are better than the GV bound in a non-empty interval $I_\ell \subseteq (0, 1 - \ell^{-1})$.

Theorem 3. *Let $\ell = p^n$ with p prime and $n \geq 2$, and set $H := H\big(p^{\lceil n/2 \rceil} - 1, p^{\lfloor n/2 \rfloor} - 1\big)$. Let $0 \leq R \leq 1/2$ and $\delta \geq 0$ be real numbers with $R = 1 - \delta - H^{-1}$. Then there exists a family $(C_j)_{j \geq 0}$ of linear codes over $\mathbb{F}_\ell$ with parameters $[n_j, k_j, d_j]$ such that the following hold:*

(1) all C_j are self-orthogonal codes;

(2) $n_j \to \infty$ as $j \to \infty$;

(3) $\lim_{j\to\infty} k_j/n_j \geq R$ and $\lim_{j\to\infty} d_j/n_j \geq \delta$.

For all non-prime $\ell \geq 49$, except possibly for $\ell = 125$, these codes are better than the GV bound in a non-empty interval $J_\ell \subseteq (0, 1 - \ell^{-1})$.

The proofs of these theorems are analogous to the proofs of Theorems 1.5 and 1.6 in [11]. The main ingredient in [11] is a certain tower of function fields $\mathcal{E} = (E_0 \subseteq E_1 \subseteq \ldots)$ over $\mathbb{F}_\ell$ (ℓ being a square) where all extensions E_i/E_0 are Galois and its limit satisfies

$$\lim_{i\to\infty} \frac{\text{number of rational places of } E_i}{\text{genus of } E_i} \geq \sqrt{\ell} - 1. \tag{10}$$

In the case $\ell = p^n$ with $n \geq 3$ odd, we replace this tower $\mathcal{E}$ by a 'Galois' tower $\mathcal{N}$ over $\mathbb{F}_\ell$ whose limit satisfies Inequality (6), see [2, Theorem 1].

References

[1] A. Bassa, P. Beelen, A. Garcia and H. Stichtenoth, "Towers of function fields over non-prime finite fields", arXiv:1202.5922v2 [math.AG], 19 May 2013.

[2] A. Bassa, P. Beelen, A. Garcia and H. Stichtenoth, "Galois towers over non-prime finite fields", arXiv:1311.1779v1 [math.AG], 7 Nov 2013.

[3] V.G. Drinfeld and S.G. Vlăduţ, "The number of points of an algebraic curve", Funktsional Anal. i Prilozhen **17**, 68-69 (1983).

[4] A. Garcia and H. Stichtenoth, "A tower of Artin-Schreier extensions of function fields attaining the Drinfeld-Vlăduţ bound", Invent. Math. **121**, 211-22 (1995).

[5] Y. Ihara, "Congruence relations and Shimura curves", *Automorphic forms, representations and L-functions*, Sympos. Pure Math., Oregon State Univ. 1977, Proc. Sympos. Pure Math., XXXIII, Amer. Math. Soc., Providence, R.I., 291-311 (1979).

[6] J.H. van Lint, *Introduction to coding theory*, Springer Verlag, New York (1982).

[7] F.J. MacWilliams and N.J.A. Sloane, *The theory of error-correcting codes*, North Holland, Amsterdam (1977).

[8] Y.J. Manin, "What is the maximal number of points on a curve over $\mathbb{F}_2$?", J. Fac. Sci. Tokyo **28**, 715-720 (1981).

[9] H. Niederreiter and C.-P. Xing, *Rational points of curves over finite fields*, Cambridge University Press, Cambridge (2001).

[10] H. Stichtenoth, *Algebraic function fields and codes*, second ed., Graduate Texts in Mathematics, vol. **254**, Springer Verlag, Berlin-Heidelberg (2009).

[11] H. Stichtenoth, "Transitive and self-dual codes attaining the Tsfasman–Vlăduţ–Zink bound", IEEE Trans. Inf. Theory **52**, 2218-2224 (2006).

[12] M.A. Tsfasman, S.G. Vlăduţ and T. Zink, "Modular curves, Shimura curves and Goppa codes better than the Varshamov–Gilbert bound". Math. Nachr. **109**, 21-28 (1982).

Alp Bassa
Sabancı University, MDBF
34956 Tuzla, İstanbul, Turkey
bassa@sabanciuniv.edu

Peter Beelen
Technical University of Denmark, Department of Applied Mathematics and Computer Science
Matematiktorvet, Building 303B
DK-2800, Lyngby, Denmark
p.beelen@mat.dtu.dk

Arnaldo Garcia
Instituto Nacional de Matemática Pura e Aplicada, IMPA
Estrada Dona Castorina 110
22460-320, Rio de Janeiro, RJ, Brazil
garcia@impa.br

Henning Stichtenoth
Sabancı University, MDBF
34956 Tuzla, İstanbul, Turkey
henning@sabanciuniv.edu