Construction-D lattice from Garcia-Stichtenoth tower code

Elena Kirshanova[1,2*†] and Ekaterina Malygina[2†]

[1*]Technology Innovation Institute, Abu Dhabi, UAE.
[2]Immanuel Kant Baltic Federal University, Kaliningrad, Russia.

*Corresponding author(s). E-mail(s): elenakirshanova@gmail.com;
Contributing authors: emalygina@kantiana.ru;
[†]These authors contributed equally to this work.

Abstract

We show an explicit construction of an efficiently decodable family of n-dimensional lattices whose minimum distances achieve $\Omega(\sqrt{n}/(\log n)^{\varepsilon+o(1)})$ for $\varepsilon > 0$. It improves upon the state-of-the-art construction due to Mook-Peikert (IEEE Trans. Inf. Theory, no. 68(2), 2022) that provides lattices with minimum distances $\Omega(\sqrt{n/\log n})$. These lattices are construction-D lattices built from a sequence of BCH codes. We show that replacing BCH codes with subfield subcodes of Garcia-Stichtenoth tower codes leads to a better minimum distance. To argue on decodability of the construction, we adapt soft-decision decoding techniques of Koetter-Vardy (IEEE Trans. Inf. Theory, no. 49(11), 2003) to algebraic-geometric codes.

Keywords: construction-D lattice, algebraic-geometric code, Garcia-Stichtenoth tower

1 Introduction

A (full-rank) lattice $\Lambda \subset \mathbb{R}^n$ is a discrete additive subgroup whose linear span is $\mathbb{R}^n$. Its minimum distance $\lambda_1(\Lambda)$ is the minimum Euclidean norm of its nonzero vectors, and its determinant $\det(\Lambda) = \mathrm{vol}(\mathbb{R}^n/\Lambda)$ is the covolume of Λ.

Lattices can be used for error correction, where the main decoding 'quality' of the lattice is its normalized minimum distance $\sqrt{\gamma(\Lambda)} = \lambda_1(\Lambda)/\det(\Lambda)^{1/n}$. Minkowski's theorem bounds this quantity as $\sqrt{\gamma(\Lambda)} < \sqrt{n}$ for any n-dimensional lattice. The

main question that we address in this work is how to explicitly construct an efficiently decodable family of lattices with quality close to Minkowski's bound.

Prior work

Barnes-Wall lattices Λ_{BW} [1] with efficient decoding procedure given in [2] achieve moderately good quality $\sqrt{\gamma(\Lambda_{\mathrm{BW}})} = \mathcal{O}(n^{1/4})$. Another family of efficiently decodable lattices due to Ducas and Pierrot [3] is the discrete-logarithm lattices Λ_{DP} that achieve normalized distance $\sqrt{\gamma(\Lambda_{\mathrm{DP}})} = \Theta(\sqrt{n}/\log n)$. The work of Mook-Peikert [4] presents an efficient algorithm to decode the family of Barnes and Sloane [5] lattices Λ_{BS} with $\sqrt{\gamma(\Lambda_{\mathrm{BS}})} = \Omega(\sqrt{n/\log n})$. In the recent work, Bennet and Peikert [6] build another family of efficiently decodable lattices achieving the same normalized distance $\Omega(\sqrt{n/\log n})$. This line of works gets closer to the best asymptotically possible $\sqrt{\gamma(\Lambda)}$, with the resent results being only by a factor $\sqrt{\log n}$ away from Minkowski's bound.

This work

We give an explicit construction of n-dimensional family of lattices Λ that achieve $\sqrt{\gamma(\Lambda)} = \Omega(\sqrt{n}/(\log n)^{\varepsilon+o(1)})$ for a constant $\varepsilon > 0$. Since we allow ε to be *any* constant and, in particular, smaller than $1/2$, we improve upon the existing constructions.

Our lattices are the so-called construction-D lattices [5] applied to a certain tower of linear p-ary codes for a prime p. Different to the original work of Barnes and Sloane that builds a lattice from a tower of binary BCH codes, we use a more general construction of subfield subcodes. In particular, we build a tower of algebraic-geometry (AG) codes using the Garcia-Stichtenoth function field. These codes have good minimal distance and high rates. In particular, they were used in [7] to construct a sequence of lattices with exponentially large kissing numbers.

As AG codes are necessarily defined over a prime-field extension $\mathbb{F}_q = \mathbb{F}_{p^h}$ for some $h > 1$, they cannot be directly applied to lattice constructions. We show that restricting these codes to the subfield $\mathbb{F}_p$ gives a tower of p-ary codes. Such p-ary codes inherit good properties from AG-codes allowing us to argue on their dimensions and minimal distances. Applying construction-D to these codes gives a family of lattices that achieves the claimed quality. In particular, out result can be informally stated as

Theorem 1. *For $\varepsilon > 0$ and $\varepsilon' > 0$, there is a family of lattices $\Lambda \subset \mathbb{R}^n$ with normalized minimum distance $\lambda_1(\Lambda)/(\det(\Lambda)^{1/n}) = \Omega(\sqrt{n}/(\log n)^{\varepsilon+o(1)})$. These lattices are list decodable to within distance $\lambda_1(\Lambda)\sqrt{(1-\varepsilon')/2}$ in poly(n) time.*

The decodability of the constructed family is our second result. To instantiate an efficient decoder for our lattice, we build upon the following three results: first, we use the work of Guruswami-Sudan [8] that show how to list-decode any AG-code for which we known explicitly a basis for the Riemann-Roch space. For the AG-code associated to a Garcia-Stichtenoth tower it is indeed the case thanks to the work of Shum et al. [9, Theorem 7]. Second, we show how to adapt soft-decision decoder of Koetter-Vardy from [10] to AG-codes. Third, we use the ideas from Mook-Peikert [4] to adapt the soft-decision decoder in a way that allows to decode subfield subcodes of Garcia-Stichtenoth tower codes.

2

In Section 2 we give necessary background on AG-codes and construction-D lattices. In Section 3 we show how to efficiently construct a family of lattices that achieve the claimed normalized minimal distance. Finally, in Section 4 we show how to efficiently decode the constructed lattices.

2 Preliminaries

2.1 Subfield Subcodes

Let p be prime and for $h \geq 1$, let $q = p^h$ and $\mathbb{F}_q$ be a finite field with q elements. Then $\mathbb{F}_p$ is a subfield of $\mathbb{F}_q$. For a linear q-ary code C of dimension k and length n, its subfield subcode $C|_{\mathbb{F}_p}$ is defined by

$$C|_{\mathbb{F}_p} = C \cap \mathbb{F}_p^n.$$

We shall be interested in the parameters of $C|_{\mathbb{F}_p}$. The length of $C|_{\mathbb{F}_p}$ is n, and since $C|_{\mathbb{F}_p} \subseteq C$, the minimal distance of the subfield subcode, denoted $d(C|_{\mathbb{F}_p})$, is no smaller than $d(C)$, i.e.,

$$d(C|_{\mathbb{F}_p}) \geq d(C).$$

A bound on the dimension of $C|_{\mathbb{F}_p}$ follows from the relation between subfield subcodes and trace codes from [11]. We do not introduce trace codes here, so we give a weaker statement, which suffices for our result. A proof (of a stronger statement) can be found in [12, Corollary 9.1.5.]

Lemma 1 (Adapted from [12, Corollary 9.1.5.]). *Let C be a code of length n and dimension k defined over $\mathbb{F}_q = \mathbb{F}_{p^h}$ for $h \geq 1$. Then it holds that*

$$\dim_{\mathbb{F}_p}(C|_{\mathbb{F}_p}) \geq n - h(n - k).$$

2.2 Algebraic-Geometry codes

For a comprehensive study of Algebraic-Geometry (AG) codes we refer the reader to [12]. A more compact, but sufficient for our purposes, introduction to AG-codes is given in [13, Section 4].

Let $\mathbb{F}_q$ be a finite field and $F/\mathbb{F}_q$ be an algebraic function field. Elements of $F/\mathbb{F}_q$ are rational functions, i.e., fractions of polynomials with coefficients from $\mathbb{F}_q$.

Valuation

A *place* P of $F/\mathbb{F}_q$ is, by definition, the maximal ideal of some valuation ring O in $F/\mathbb{F}_q$. For every place P there exists a unique discrete valuation $\nu_P : F/\mathbb{F}_q \to \mathbb{Z} \cup \{\infty\}$. It is a surjective map that satisfies certain properties, see [12, Definition 1.1.9]. In particular, the valuation ν_P defines a valuation ring $O = \{f \in F/\mathbb{F}_q : \nu_P(f) \geq 0\}$ and P is its maximal ideal $P = \{f \in F/\mathbb{F}_q : \nu_P(f) > 0\}$. The extension degree $[O/P : \mathbb{F}_q]$, denoted $\deg P$, is called the degree of P. We shall consider only places of degree 1, called rational places. In this case there is a residue class map at P acting from F to

$O_P/P \cup \{\infty\}$ as $f \mapsto f(P)$ for $f \in O_P$. It is worth mentioning that O_P/P is isomorphic to $\mathbb{F}_q$ giving a way to evaluate functions at places.

As an example, consider $P = tO$ to be a principal ideal in O generated by t (in fact, O is a principal ideal domain [12, Theorem 1.1.6]). Then any $z \in F/\mathbb{F}_q$ can be written uniquely as $z = t^n u$ for $n \in \mathbb{Z}$ and $u \in O^\star$, where $O^\star$ is the group of units of O. Then ν_P, defined by $\nu_P(z) = n$ for $z \neq 0$ and $\nu_P(0) = \infty$, is a discrete valuation associated to P.

Divisors

Denote by $\mathbb{P}_F$ the set of all places of the function field $F/\mathbb{F}_q$. A divisor D is a formal sum $D = \sum_{P \in \mathbb{P}_F} n_P P$ for $n_P \in \mathbb{Z}$ and almost all $n_P = 0$. Often one writes $\nu_P(D)$ for the coefficient n_P, thus

$$D = \sum_{P \in \mathbb{P}_F} \nu_P(D) P.$$

The set $\mathrm{supp}(D) = \{P \in \mathbb{P}_F \mid n_P \neq 0\}$ is called the support of D and $\deg D = \sum_{P \in \mathrm{supp}(D)} n_P \cdot \deg P$ is called the degree of D. The set of divisors forms an additive Abelian group, where for $D = \sum_{P \in \mathbb{P}_F} n_P P$ and $D' = \sum_{P \in \mathbb{P}_F} n'_P P$, we have $D + D' = \sum_{P \in \mathbb{P}_F} (n_P + n'_P) P$, see [12, Definition 1.4.1].

Let P be a place of $F/\mathbb{F}_q$ and $f \in F/\mathbb{F}_q$ be non-zero element. The place P is called a *zero* of f if $\nu_P(f) > 0$ and a pole of f if $\nu_P(f) < 0$. The *zero divisor* of f is then defined as

$$(f)_0 = \sum_{P \text{ is a zero of } f} \nu_P(f) P,$$

and the *pole divisor* as

$$(f)_\infty = \sum_{P \text{ is a pole of } f} \nu_P(f) P.$$

Then the principal divisor of f, denoted $\mathsf{div}(f)$, is the following formal sum $\mathsf{div}(f) = (f)_0 - (f)_\infty$. All principal divisors have degree 0. For example, for $F = \mathbb{F}_q(x)$, i.e., x is transcendental over $\mathbb{F}_q$, the point at infinity, denoted P_∞, is the unique pole of the function x. It is a place of degree one, and hence, the divisor of the form $D = nP_\infty$ has degree n.

Riemann-Roch space

The concept of divisors gives rise to $\mathbb{F}_q$-linear spaces. Concretely, for a divisor G, the set

$$\mathcal{L}(G) = \{f \in F \setminus \{0\} : \mathsf{div}(f) + G \geq 0\} \cup \{0\}$$

is called the Riemann-Roch space associated to G. Let

$$G = \sum_{P_i} \nu_{P_i}(G) P_i - \sum_{Q_i} \nu_{Q_i}(G) Q_i,$$

where $\nu_{P_i}(G), \nu_{Q_i}(G) > 0$. Then $\mathcal{L}(G)$ consists of all $f \in F/\mathbb{F}_q$ such that (1) f has zeros of order $\nu_{Q_i}(f) \geq \nu_{Q_i}(G)$ for all Q_i, and (2) f may have poles only at the places P_i of orders bounded from above by $\nu_{P_i}(G)$. In other words, $f \in \mathcal{L}(G)$ if and only of $\nu_P(f) \geq -\nu_P(G)$ for all $P \in \mathbb{P}_F$.

4

Associated to a function field is the notion of genus. The genus $\mathfrak{g}$ of $F/\mathbb{F}_q$ is $\max\{\deg G - \dim \mathcal{L}(G) + 1\}$, where the maximum is taken over all divisors G.

A nice feature of $\mathcal{L}(G)$ is that it is a finite dimensional space over $\mathbb{F}_q$ of dimension $\dim \mathcal{L}(G) \geq \deg(G) + 1 - \mathfrak{g}$, and the equality holds if $\deg(G) \geq 2\mathfrak{g} - 1$ [12, Theorem 1.5.17].

In order to define an AG-code, fix $\mathcal{P} = \{P_1, \ldots, P_n\}$ – a set of n distinct rational places of a function field $F/\mathbb{F}_q$. Let further G be a divisor of F such that $\mathrm{supp}(G) \cap \mathcal{P} = \emptyset$. Then the set

$$C(\mathcal{P}, G) = \{f(P_1), \ldots, f(P_n) : f \in \mathcal{L}(G)\}. \tag{1}$$

defines an n-dimensional $\mathbb{F}_q$-linear code. There exist efficient algorithms to construct a basis of this code, for instance [9] describes an algorithm that outputs a basis in time $\mathcal{O}((n \log_q n)^3)$. The following lemma summarizes the parameters of $C(\mathcal{P}, G)$.

Lemma 2 ([12, Corollary 2.2.3]). *For a divisor G defined over a function field of genus $\mathfrak{g}$ such that $2\mathfrak{g} - 2 < \deg(G) < n$, the code $C(\mathcal{P}, G)$ defined above is a linear code over $\mathbb{F}_q$ of length n, dimension k and minimal Hamming distance d, where*

$$k = \dim(\mathcal{L}(G)) = \deg(G) - \mathfrak{g} + 1, \qquad d \geq n - \deg(G).$$

Garcia-Stichtenoth tower

A concrete example of a tower of function fields is given by Garcia-Stichtenoth in [14]. In particular, let h in $q = p^h$ be even, hence we can write $q = p^h = r^2$ for $r = p^{h/2}$. For an integer $e \geq 2$, define the following recursive relations

$$x_{i+1}^r + x_{i+1} = \frac{x_i^r}{x_i^{r-1} + 1}, \quad i = 1, \ldots, e - 1. \tag{2}$$

Then $K_e = \mathbb{F}_q(x_1, \ldots, x_e)$ is a function field, and the sequence $K_1, K_2, \ldots$ is known as the Garcia-Stichtenoth tower of function fields. An attractive feature of such function fields is that we know a lower bound on the number of their rational places (hence, the maximal possible length of AG codes constructed from them) and we known exactly the genus of K_e. We formulate these two facts in the following lemma. The lower bound on the number of rational places is given in [13, Paragraph 4.4.1] (the exact number of rational places can be found in [9, Section II], but a lower bound suffices for our purposes). The genus of K_e is computed in [14, Remark 3.8].

Lemma 3 ([13, Paragraph 4.4.1] and [14, Remark 3.8]]). *Let $K_e = \mathbb{F}_q(x_1, \ldots, x_e)$ be the Garcia-Stichtenoth function field defined by Equation (2) for $e \geq 2$ and $q = r^2$. Then K_e has at least $r^e(r - 1) + 1$ rational places and its genus $\mathfrak{g}$ satisfies*

$$\mathfrak{g} = \begin{cases} (r^{e/2} - 1)^2, & \text{if } e \text{ is even} \\ (r^{(e-1)/2} - 1)(r^{(e+1)/2} - 1), & \text{if } e \text{ is odd.} \end{cases}$$

What will turn out to be important for our construction is that the genus $\mathfrak{g}$ is below r^e, while the number of rational places, which will translate into the length of a code, is of order r^{e+1}.

From the lower bound on the number of rational places of K_e follows another useful property of Garcia-Stichtenoth function fields: they enable us to construct codes with many codewords by increasing e rather than increasing the base field, i.e., one obtains dense codes while keeping r relatively small.

2.3 Lattices

We give only necessary notions related to Euclidean lattices and refer the reader to [15] for a broader introduction to the topic.

An n-dimensional integral lattice Λ is a full-rank subgroup of $\mathbb{Z}^n$. A full-rank integral lattice is usually represented by the columns of a rank-n matrix $\mathbf{B} \in \mathbb{Z}^{n \times n}$. The two important invariants associated to a lattice are its determinant and the first minimum.

The *determinant* of Λ, $\det(\Lambda)$, is the absolute value of the determinant of $\mathbf{B}$:

$$\det(\Lambda) = |\det \mathbf{B}|.$$

The *first successive minimum* or the *minimum distance* of a lattice Λ, denoted $\lambda_1(\Lambda)$, is the Euclidean length of a shortest nonzero lattice vector:

$$\lambda_1(\Lambda) = \min_{\mathbf{v} \in \Lambda \setminus \{\mathbf{0}\}} \|\mathbf{v}\|.$$

2.4 Construction D lattices

Construction-D, introduced in [5], is a name of a method to construct lattices from codes. The original construction uses a nested family of binary codes of lengths n to construct a lattice in $\mathbb{Q}^n$. It is not difficult to generalize the construction to a nested family of p-ary linear codes. We follow the description of this method presented in [4] that scales the lattice such it becomes integral.

Definition 1. *For an integer $L \geq 0$, let $C_L \subseteq C_{L-1} \subseteq \ldots \subseteq C_1 \subseteq C_0 = \mathbb{F}_p^n$ be a tower of p-ary codes of length n, where C_i has dimension k_i. Let $\mathbf{b}_1, \ldots, \mathbf{b}_n$ be a basis of $\mathbb{F}_p^n$ such that*

1. $\mathbf{b}_1, \ldots, \mathbf{b}_{k_i}$ is a basis of C_i for all $i = 0, \ldots, L$, and

2. some permutation of the row vectors $\mathbf{b}_1, \ldots, \mathbf{b}_n$ forms an upper-triangular matrix. Define a set of distinguished $\mathbb{Z}^n$ representatives of C_i as follows: for any $\mathbf{c}_i \in C_i$ express it as $\mathbf{c}_i = \sum_{j=1}^{k_i} a_j \mathbf{b}_j$ for some unique $a_j \in \mathbb{F}_p$, and define its representative $\bar{\mathbf{c}}_i = \sum_{j=1}^{k_i} \bar{a}_j \bar{\mathbf{b}}_j \in \mathbb{Z}^n$, that is we consider the set of representatives $\{0, \ldots, p-1\}$ as elements from $\mathbb{Z}$.

Let $\Lambda_0 = \mathbb{Z}^n$, and for each $i = 1, \ldots, L$ define

$$\Lambda_i = \bar{C}_i + p\Lambda_{i-1},$$

where $\bar{C}_i = \{\bar{c}_i : c_i \in C_i\}$. The construction-D for the tower $\{C_i\}$ is $\Lambda = \Lambda_L$.

A basis $\mathbf{b}_1, \ldots, \mathbf{b}_n$ from Definition 1 can be efficiently constructed from the bases of C_i's, see [4, Footnote 4].

6

From the above definition, it follows that a vector in Λ is of the form

$$p^L \mathbf{z} + \sum_{i=1}^{L} \sum_{j=1}^{k_i} p^{L-i} \bar{a}_j^{(i)} \bar{\mathbf{b}}_j, \tag{3}$$

where $\mathbf{z} \in \mathbb{Z}^n$, $\bar{a}_j^{(i)} \in \mathbb{F}_p$.

The following lemma is borrowed from [4, Theorem 5.1], which is itself an adaptation of [5, Theorem 1]. The difference between prior work and this statement is the generalization from binary codes to p-ary for any prime p. For completeness, we give a proof.

Lemma 4. *Let $C_L \subseteq C_{L-1} \subseteq \ldots \subseteq C_1 \subseteq C_0 = \mathbb{F}_p^n$ be a tower of p-ary codes of length n, where C_i has dimension k_i and minimal Hamming distance $d(C_i)$ satisfying $d(C_i) \geq p^{2i}$ for $i = 0, \ldots, L$. The construction-D lattice $\Lambda = \Lambda_L$ for the tower $\{C_i\}$ has Euclidean minimum distance $\lambda_1(\Lambda) = p^L$ and determinant*

$$\det(\Lambda) \leq (p-1)^{n-k_L} p^{\sum_{i=1}^{L}(n-k_i)}. \tag{4}$$

Proof. We start with the statement on the minimum distance. From Equation (3), we can represent any Λ-vector as $\mathbf{b} = p^L \mathbf{z} + \sum_{i=1}^{L} p^{L-i} \bar{\mathbf{c}}_i \in \Lambda$, where $\bar{\mathbf{c}}_i \in \bar{C}_i$ and $\mathbf{z} \in \mathbb{Z}^n$. By the definition of construction-D, every $\bar{\mathbf{c}}_i = \sum_{j=1}^{k_i} \bar{a}_j \bar{\mathbf{b}}_j$, and, if we choose the representatives $\bar{\mathbf{b}}_j$ to have coordinates in $\mathbb{F}_p = \{0, \ldots, p-1\}$ (hence the coefficients satisfy $\bar{a}_j \geq 0$), then $\langle \bar{\mathbf{c}}_j, \bar{\mathbf{c}}_i \rangle \geq 0$ for all i, j.

Assume on the contrary that $\|\mathbf{b}\|^2 < p^{2L}$. Then we necessarily have $\mathbf{z} = \mathbf{0}$ in the representation of $\mathbf{b}$. Hence,

$$\|\mathbf{b}\|^2 = \sum_{i=1}^{L} p^{2L-2i} \|\bar{\mathbf{c}}_i\|^2 + 2 \sum_{i<j} \langle \bar{\mathbf{c}}_j, \bar{\mathbf{c}}_i \rangle \geq \sum_{i=1}^{L} p^{2L-2i} \|\bar{\mathbf{c}}_i\|^2.$$

From the lower bound on $d(C_i)$, we have $\|\mathbf{b}\|^2 \geq \max_i \{p^{2L-2i} d(C_i)\} = p^{2L}$. This contradicts the assumption on $\|\mathbf{b}\|$. Therefore, $\lambda_1(\Lambda) \geq p^L$. The equality (rather than the inequality) comes from the fact that Λ contains vectors $p^L \mathbb{I}$, where $\mathbb{I}$ is the identity-matrix.

From Definition 1, a basis of Λ forms an upper-triangular matrix whose first $k_0 - k_1$ rows are scaled by p^L, next $k_1 - k_2$ rows are scaled by p^{L-1}, next $k_2 - k_3$ rows are scaled by p^{L-2}, and so on, until the last k_L rows are scaled by 1. On the main diagonal we have integers bounded by p (again, choosing the representatives such that $\|\bar{\mathbf{b}}_i\|_\infty < p$). We thus have

$$\det(\Lambda) \leq \prod_{i=0}^{L} ((p-1) \cdot p^{L-i})^{k_i - k_{i+1}} = (p-1)^{n-k_L} \cdot p^{Ln - \sum_{i=1}^{L} k_i},$$

where we set $k_{L+1} = 0$. □ □

7

Remark 1. *For $p = 2$, Inequality 4 becomes the equality $\det(\Lambda) = 2^{\sum_{i=1}^{L}(n-k_i)}$ since the only option we have for the main diagonal elements of the upper-triangular basis matrix that we consider in the proof, are 2^L for the first $k_0 - k_1$ rows, 2^{L-1}, for the next $k_1 - k_2$ rows, etc.*

3 Construction

In this section we state our main result. To build a construction-D lattice, we need a tower of p-ary codes. The following theorem shows a specific construction of a tower of codes from AG-codes by fixing a function field $F/\mathbb{F}_q$ for $\mathbb{F}_q = \mathbb{F}_{p^h}$, the place at infinity P_∞, and considering q-ary codes associated to the divisors of the form $D_i = \ell_i P_\infty$ for $\ell_i \geq \ell_{i+1}$. Further, restricting these codes to $\mathbb{F}_p$ preserves the inclusion, and in Corollary 1 we state the properties of the resulting p-ary codes, which are subfield subcodes of Garcia-Stichtenoth tower codes. These properties then translate into the quality of the resulting conctruction-D lattice as we show in Theorem 3.

Theorem 2. *Fix an integer e, a function field K_e of genus $\mathfrak{g}$ defined by recursive relations from Equation (2). Let $\mathcal{P} = \{P_1, \ldots, P_n\}$ be n distinct rational places of K_e, all different from P_∞. Let $L \geq 1$ be an integer and $\{\ell_i\}_i$ be a sequence of positive integers satisfying $\ell_i \geq \ell_{i+1}$ for $i = 1, \ldots, L - 1$. Then the $\mathbb{F}_q$-linear codes $C_i = C(\mathcal{P}, \ell_i P_\infty)$ defined in Equation (1) build the tower of codes $C_L \subseteq C_{L-1} \subseteq \ldots \subseteq C_1 \subseteq C_0 = \mathbb{F}_q^n$.*

If, moreover, $\ell_L > 2\mathfrak{g}-2$, then $\dim(C_i) = \ell_i - \mathfrak{g}+1$ and $d(C_i) \geq n - \ell_i$ for $0 < i \leq L$.

Proof. The inclusion of $C_i = C(\mathcal{P}, \ell_i P_\infty)$'s immediately follows from the inclusion of the corresponding Riemann-Roch spaces $\mathcal{L}(\ell_i P_\infty)$, see Equation (1). Consider $f \in \mathcal{L}(\ell_{i+1}P_\infty)$ for any $i = 0, \ldots, L-1$. By definition of the Riemann-Roch space associated to $\ell_{i+1}P_\infty$, it follows that $f \in \mathcal{L}(\ell_{i+1}P_\infty) \iff \nu_{P_\infty}(f) \geq -\ell_{i+1}$. As $-\ell_{i+1} \geq -\ell_i$, we have $f \in \mathcal{L}(\ell_i P_\infty)$.

The second part of the statement follows immediately from Lemma 2. □ □

The following corollary follows by combining Theorem 2 with Lemma 1. As the result, we have an explicit construction of a tower of p-ary codes with known dimensions and minimal distances.

Corollary 1. *Consider the tower of codes $C_L \subseteq C_{L-1} \subseteq \ldots \subseteq C_1 \subseteq C_0 = \mathbb{F}_q^n$ defined as in Theorem 2 over a function field of genus $\mathfrak{g}$ with $q = p^h$ for a prime p using the divisors $\ell_i P_\infty$. Then $\widetilde{C}_i = C|_{\mathbb{F}_p} = C \cap \mathbb{F}_p^n$ is a p-ary code of length n, dimension $\tilde{k}_i \geq n - h(n - \ell_i + \mathfrak{g} - 1)$, and minimal Hamming distance $d(\widetilde{C}_i) \geq n - \ell_i$. Moreover, these p-ary codes construct the tower $\widetilde{C}_L \subseteq \widetilde{C}_{L-1} \subseteq \ldots \subseteq \widetilde{C}_1 \subseteq \widetilde{C}_0 = \mathbb{F}_p^n$.*

Proof. It is clear that the restriction of the tower of codes over $\mathbb{F}_q$ to $\mathbb{F}_p$ preserves the inclusion. It also preserves the length of the codes. Minimal distance does not decrease after the restriction, hence $d(\widetilde{C}_i) \geq d(C_i) \geq n - \ell_i$. Finally from Lemma 2 and Theorem 2, we have $\tilde{k}_i \geq n - h(n - \dim(C_i)) = n - h(n - \ell_i + \mathfrak{g} - 1)$. □ □

The next theorem formulates our main result. It shows that for certain choices of function fields, i.e., for some p, h, and e, and when the degree of the divisors $\ell_i P_\infty$ are

chosen to be $\ell_i = n - p^{2i}$, the tower of codes from Corollary 1 leads to a construction-D lattice $\Lambda \subset \mathbb{Z}^n$ that achieves $\lambda_1(\Lambda)/\det(\Lambda)^{1/n} = \Omega(\sqrt{n}/(\log\log n(\log n)^\varepsilon))$ for some constant $\varepsilon > 0$.

Theorem 3. *Fix a prime p. Let $\varepsilon > 0$ and κ be a sufficiently large parameter such that $\kappa > p^{p^{\frac{p}{\varepsilon}}}$. Let further c be a constant such that $c > \frac{2\log_p(\log_p \kappa)}{\varepsilon \log_p(\log_p \kappa) - 1}$ and $\lceil c\log_p \kappa \rceil$ is a power of p. Set $r = \lceil c\log_p \kappa \rceil$ and $e = \lceil \log_r \kappa \rceil - 1 \geq 2$ to be integers. Let $q = r^2 = p^h$ for $h = 2\log_p r$ and let $K_e = \mathbb{F}_q(x_1, \ldots, x_e)$ be the e-th function field in Garcia-Stichtenoth tower of function fields, of genus $\mathfrak{g}$.*

Let further $\widetilde{C}_L \subseteq \widetilde{C}_{L-1} \subseteq \ldots \subseteq \widetilde{C}_1 \subseteq \widetilde{C}_0 = \mathbb{F}_p^n$ be a tower of p-ary linear codes from Corollary 1 that are subfield subcodes of the tower $\{C_i\}_{0 \leq i \leq L}$ of q-ary linear n-dimensional AG-codes defined in Theorem 2, where $C_i = C(\mathcal{P}, \ell_i P_\infty)$ for $\ell_i = n - p^{2i}$, $0 < i \leq L$.

Then for $n = r^e(r-1)$ and $L = \lfloor \frac{1}{2}\log_p(n/h - \mathfrak{g}) \rfloor$, the construction-D lattice built upon $\{\widetilde{C}_i\}_{0 \leq i \leq L}$, yields an n-dimensional lattice Λ, such that

$$\lambda_1(\Lambda) = p^L = \Omega\left(\sqrt{\frac{n}{\log\log n}}\right),$$

and

$$\det(\Lambda)^{1/n} \leq p^{\varepsilon\log_p(\log_p n)} = (\log_p n)^\varepsilon.$$

Proof. First, note that choosing, for example, $c = p^u$ and $\kappa = p^{p^v}$ for some integers $u, v > 1$ makes the expression $c\log_p \kappa$ to be a power of p. Other choices of κ and c are, of course, also possible. Second, the lower bound on κ ensures that $c > 0$. Third, note that the choice of n in the theorem's statement is legitimate, since K_e has at least $r^e(r-1)$ rational places different from P_∞, see Lemma 3. Further, from the choices for r and e, we have $n = \frac{r^{\lceil\log_r \kappa\rceil}(r-1)}{r} \geq \frac{\kappa(r-1)}{r}$. On the other hand, it holds that $n \leq \frac{r^{\log_r \kappa + 1}(r-1)}{r} = \kappa(r-1)$. These two bounds relate n to κ and allow us to use the former in $\mathcal{O}$-notations.

The lower bound on $\lambda_1(\Lambda)$ follows from Lemma 4. Indeed, as $p^L > p^{\frac{1}{2}\log_p(\frac{n}{h} - \mathfrak{g}) - 1}$, we have $\lambda_1(\Lambda) > \frac{1}{p}\sqrt{n/h - \mathfrak{g}}$. Further, as $\mathfrak{g} < r^e = o(n/h)$, $h = \Theta(\log_p \log_p(n))$, and p is fixed, we have $p^L = \Omega(\sqrt{n/\log\log n})$.

Now let us obtain an upper bound on $\det(\Lambda)$. From our choice of $\ell_i = n - p^{2i}$ for $0 \leq i \leq L$, L, and $\mathfrak{g} < n - n/h$, we have that $\deg(\ell_i P_\infty) \geq \deg(\ell_L P_\infty) \geq n - n/h + \mathfrak{g} > 2\mathfrak{g}$ for all $0 \leq i \leq L$. Hence, by Theorem 2, $\dim(C_i) = \ell_i - \mathfrak{g} + 1$. From Corollary 1 we thus have that $\tilde{k}_i = \dim(\widetilde{C}_i) = \dim(C_i \cap \mathbb{F}_p^n) > n - hp^{2i} - h\mathfrak{g}$. Furthermore, our choice of L ensures that $\tilde{k}_L > 0$.

Consider now the right-hand side of Inequality 4:

$$\sum_{i=1}^{L}(n - \tilde{k}_i) < \sum_{i=1}^{L} h(p^{2i} + \mathfrak{g}) = \frac{hp^2(p^{2L} - 1)}{p^2 - 1} + h\mathfrak{g}L$$

$$< hp^{2L+1} + h\mathfrak{g}L < np + \frac{1}{2}h\mathfrak{g}\log_p(n/h).$$

9

Dividing the right-hand side of the above inequality by n and using the facts that $\mathfrak{g} < r^e$ and $n = r^e(r-1)$, we obtain

$$\frac{1}{n} \sum_{i=1}^{L} (n - k_i) < p + \frac{1}{2} \frac{h \log_p(n/h)}{r-1} < p + \frac{2 \log_p(r)}{c} < \varepsilon \log_p(\log_p \kappa) + O(1),$$

where for the second inequality we use the facts that $\sqrt{n/h} < \kappa$ and $r = \lceil c \log_p \kappa \rceil$. For the third inequality, we use the lower bound on c. $\qquad\square\qquad\square$

Comparison with [4].

Let us compare our construction with the one from [4] based on the sequence of BCH codes. The latter achieves $\lambda_1(\Lambda) > \sqrt{n/\log n}$ and $\det(\Lambda)^{1/n} = \Theta(1)$ using a sequence of codes of length $L = \frac{1}{2} \log_2(n/\log n)$. The choice of L determines the bound on $\lambda_1(\Lambda)$. In contrast, using AG-codes we are able to choose a longer sequence, e.g. $L \approx \frac{1}{2} \log_2(n/(\log n \log n))$, which makes our lower bound on $\lambda_1(\Lambda)$ larger: $\lambda_1(\Lambda) > \sqrt{n/(\log \log n)}$. However, we pay the price in the determinant: while in [4] it holds that $n - k_i \approx 4^i \log n \leq \mathcal{O}(n)$ (and hence, $\det(\Lambda)^{1/n} = \Theta(1)$), for us, $n - k_i \leq \mathcal{O}(n \cdot h)$ (e.g., the summond $\frac{1}{2} h \mathfrak{g} \log_p(n/h)$ dominates np in the computations from the proof), making $\det(\Lambda)^{1/n} = (\log_p n)^\varepsilon$.

4 Decoding Garcia-Stichtenoth subfield subcodes

In this section we present an algorithm to list decode subfield subcodes $\widetilde{C}_i$ of Garcia-Stichtenoth codes as defined in the previous section. Being able to efficiently decode a tower of codes $\widetilde{C}_L \subseteq \ldots \subseteq \widetilde{C}_0 = \mathbb{F}_p^n$ enables to decode the corresponding construction-D lattices. More specifically, Mook-Peikert show in [4] the following result.

Theorem 4 ([4, Theorem 4.6 and Theorem 4.7]). *Let $L \leq 0$ be an integer and let Λ_i be a sequence of lattices built from a tower $\widetilde{C}_L \subseteq \widetilde{C}_{L-1} \subseteq \ldots \subseteq \widetilde{C}_1 \subseteq \widetilde{C}_0 = \mathbb{F}_p^n$. Further, let $\mathcal{D}_i$ be a list decoder for $\widetilde{C}_i$ that decodes up to Euclidean distance $e_i = p^i e_0$ for some $0 < e_0 < p/2$ for all $0 \leq i \leq L$ in time less than $\mathcal{T}_i$ and returns a list of size less than $\mathcal{S}_i$. Then there exists an algorithm that given on input $\mathbf{y} \in \mathbb{R}^n$ and access to $\mathcal{D}_i$, outputs a list of vectors $\mathbf{v} \in \Lambda_i$ s.t. $\|\mathbf{y} - \mathbf{v}\| \leq e_i$ in time*

$$R < L \cdot (\mathcal{T} + \mathrm{poly}(n, \log p, \mathcal{S})) \cdot \mathcal{S}^L,$$

where $\mathcal{T} = \max_i \mathcal{T}_i$ and $\mathcal{S} = \max_i \mathcal{S}_i$.

In this section we give an efficient decoder for subfield subcodes $\widetilde{C}_i$'s. We start with a short description of hard decision decoding, then continue with the definition of the soft decision decoding, following [10]. To build a decoder in this regime, we show how to "soften" the hard-decision decoder for AG-codes from [8] and analyse this new soft version. Finally, analogously to [4] we show that our soft decision decoder can be used to decode $\widetilde{C}_i$'s, and hence, due to the above theorem, to decode our construction-D lattices.

4.1 Hard decision decoding for AG-codes

Recall that we have a code $C(\mathcal{P}, G)$ defined as in Equation (1), where $\mathcal{P} = \{P_1, \ldots, P_n\}$ is a set of n distinct rational places of a function field $K/\mathbb{F}_q$ of genus $\mathfrak{g}$, and $G = \alpha P_\infty$ for some $\alpha > 2\mathfrak{g} - 2$, and hence the dimension of the code is $k = \alpha - \mathfrak{g} + 1$.

In the usual list-decoding problem (also known as *hard decision decoding*), we are given on input a word $\mathbf{y} \in \mathbb{F}_q^n$, and we need to find a list of codewords that are close to $\mathbf{y}$.

Briefly, the decoding proceeds in two steps. The first one is called the **interpolation step**. The goal here is to find a polynomial $Q(y) \in K[y]$ (e.g., a polynomial whose coefficients are functions from the function field K) that satisfies two properties:
1. $Q(\mathbf{y}_i)[P_i]$ is zero of certain "multiplicity" r for all $i \leq n$;
2. for any function $f \in \mathcal{L}(\ell P_\infty)$, we have $Q(f) \in \mathcal{L}(\ell P_\infty)$ for some integer parameter ℓ.

In our setting, K is Garcia-Stichtenot function field K_e defined in Equation (2). The notation $Q(\mathbf{y}_i)[P_i]$ should be interpreted as follows: we first substitute $\mathbf{y}_i \in \mathbb{F}_q$ for the y-variable in $Q(y)$ and obtain a function from K. Then we evaluate this function in the rational point P_i. For the correct polynomial $Q(y)$, the result should be 0, and this gives constraints on the coefficients of Q. For the appropriate choices of r and ℓ, [8, Section 4] show that such Q exists and can be efficiently found via solving a system of linear equations over $\mathbb{F}_q$.

The second step of the decoder is the **factorisation step** that consists of factoring $Q(y)$ over K to obtain factors of the form $(y - f_i)^r$, where f_i's form a list of potential encoded messages. Shoklorahi-Wasserman demonstrate in [16, Appendix B] an algorithm that factors $Q(y)$ in time polynomial in $n, k, \deg Q$. Alternatively, a root-finding algorithm from [17] can be used. This factorisation step will remain unchanged in the soft-decision decoding, which describe next. The reader can refer to [8, Section 4] for the details on hard list-decoding for AG-codes.

4.2 Soft decision decoding for AG-codes

For a code of length n defined over $\mathbb{F}_q$, in *soft decision decoding* instead of $\mathbf{y}$, we are given a *reliability matrix* $\Pi \in \mathbb{R}^{|\mathbb{F}_q| \times n}$, where $\Pi_{i,j}$ describes the probability that the transmitted codeword has a symbol $\alpha_i \in \mathbb{F}_q$ in the jth position. Here we assume a fixed ordering on $\mathbb{F}_q$, i.e., $\mathbb{F}_q = [\alpha_1, \ldots, \alpha_q]$.

Upon receiving the reliability matrix Π, the KV-decoder from [10] decoder first converts it into a multiplicity matrix $M \in \mathbb{Z}^{|\mathbb{F}_q| \times n}$ with non-negative entries. In particular, they show that for a list-decoding with an output list bounded by S, the matrix M is a scaling of Π, namely

Lemma 5 ([10, Lemma 16]). *For a reliability matrix Π, and S – an upper bound on the decoder's output list, we have*

$$M = \lfloor \lambda \Pi \rfloor,$$

where λ is a real number that can be efficiently computed from Π and S.

We shall make use of the following notion of the *matrix cost*.

Definition 2. *For a matrix $M \in \mathbb{Z}^{|\mathbb{F}_q| \times n}$ with non-negative entries, its cost $C(M)$ is defined as*

$$C(M) = \frac{1}{2} \sum_{i=1}^{q} \sum_{j=1}^{n} M_{i,j}(M_{i,j} + 1).$$

We now can formulate the **interpolation step** of the soft decision decoding process for AG-codes. In the definition below the integer parameter ℓ has the same meaning as in the hard decision decoding, and we discuss this value later in the analysis.

Definition 3 (Soft interpolation step). *Given a matrix $M \in \mathbb{Z}^{|\mathbb{F}_q| \times n}$ and an integer $\ell > 0$, find $Q \in K[y]$ such that*

1. *$Q(\alpha_i)[P_j]$ is zero of multiplicity $M_{i,j}$ for all $M_{i,j} > 0$.*
2. *$Q(f) \in \mathcal{L}(\ell P_\infty)$ for any $f \in \mathcal{L}(\ell P_\infty)$.*

Note the difference between hard and soft decoding in condition 1.: while hard decoding imposes the same multiplicity for all pairs (α_i, P_i), soft decoding allows these multiplicities to vary. We also remark that condition 2. is equivalent to saying that $\nu_{P_\infty}(Q(f)) \geq -\ell$. It has the same meaning as imposing an upper-bound on the so-called weighted degree of Q as it is done in [10] for Reed-Solomon code. For AG-codes it is more natural to talk about valuations, rather than weighted-degrees. [1]

Below we give Algorithm 4.1 that describes the soft-decision interpolation step. It is almost the same as in [8, Section 4], the difference is in the number of constraints coming from varying 'multiplicities' for $Q(\alpha_i)[P_j]$, e.g. Step 6 in the algorithm. However this minor change influences the choice of ℓ, and then leads to modifications in the analysis of the soft-decision decoding.

Next we discuss the above algorithm, show its correctness (following [8]) and the decoding quality (adapting [10] to AG-codes).

Precomputations.

The main steps in the precomputations are computing a basis of the Rieman-Roch space $\mathcal{L}(\ell P_\infty)$. Thanks to Shum et al. [9, Theorem 7], we can construct in $\mathrm{poly}(n, \log q)$ time a basis for $\mathcal{L}(\ell P_\infty)$. These are $\ell - \mathfrak{g} + 1$ rational functions $\phi_1, \ldots, \phi_{\ell-\mathfrak{g}+1}$. By a proper ordering of these functions, one can guarantee that they satisfy both conditions of Step 3. Guruswami-Sudan show in [8, Lemma 16] that the ψ functions from Step 4 can also be efficiently found. Finally, we note that our choice of ℓ ensures that $\ell > \alpha$ for the parameters from Theorem 3: the inequality holds as $2C(M) > \sum_{i,j} M_{i,j} > \sum_{i,j} \Pi_{i,j} = n$ and $\alpha < n$. The latter bound is deduced by observing the values ℓ_i from Theorem 3.

Correctness.

Let us first show that the polynomial Q exists under our choice of parameters. The next lemma can be compared with [9, Lemma 19]. As we choose ℓ in Step 1 of Algorithm 4.1 that satisfies the lower bound from the lemma, a Q will be found. The shape of Equation (6) comes from the definition of the so-called shifts of $Q(y)$ given in [8]. We refer the reader to [8, Section 4] on how these equations are deduced.

---

[1]Guruswami-Sudan [8] instead of valuations $\nu_P(f)$ consider orders $\mathrm{ord}(f, P)$. These two notions are related as $\nu_P(f) = -\mathrm{ord}(f, P)$.

Algorithm 4.1 SOFT-DECISION INTERPOLATION FOR AG-CODES (ADAPTED FROM [8])

Input: multiplicity matrix $M \in \mathbb{Z}^{|\mathbb{F}_q| \times n}$,
function field K_e of genus $\mathfrak{g}$,
a code $C = (\mathcal{P} = \{P_1, \ldots, P_n\}, \alpha P_\infty)$.

Output: $Q \in K_e[y]$ that satisfies conditions in Definition 3.

PRECOMPUTATIONS

1: Let $\ell = \lceil \mathfrak{g} + \sqrt{2C(M)\alpha} \rceil$
2: Let $s = \lfloor \frac{\ell - \mathfrak{g}}{\alpha} \rfloor$
3: Compute $\phi_1, \ldots, \phi_{\ell - \mathfrak{g}+1}$ – basis functions of $\mathcal{L}(\ell P_\infty)$ s.t.
    (1) $\nu_{P_\infty}(\phi_i) \geq -(i + \mathfrak{g} - 1)$ for all i,
    (2) $\phi_1, \ldots, \phi_{\alpha - \mathfrak{g}+1}$ – basis functions of $\mathcal{L}(\alpha P_\infty)$.
4: For each $P_i \in \mathcal{P}$, compute $\psi_1^{(i)}, \ldots, \psi_{\ell - \mathfrak{g}+1}^{(i)}$ – basis of zeros s.t. for $1 \leq j_1 \leq \ell - \mathfrak{g}+1$,
    $\phi_{j_1} = \sum_{j_3=1}^{\ell - \mathfrak{g}+1} \alpha_{P_i, j_1, j_3} \psi_{j_3}^{(i)}$.

SOLVING LINEAR SYSTEM

5: Express $Q \in K_e[y]$ as

$$Q(y) = \sum_{j_2=0}^{s} \sum_{j_1=1}^{\ell - \mathfrak{g}+1-\alpha j_2} q_{j_1,j_2} \phi_{j_1} y^{j_2} \tag{5}$$

6: For each $P_j \in \mathcal{P}$ and $\alpha_i \in \mathbb{F}_q$ s.t. $M_{i,j} > 0$, obtain $\frac{1}{2} M_{i,j}(M_{i,j} + 1)$ equations in q_{j_1,j_2} of the form

$$q_{j_3,j_4} := \sum_{j_2=j_4}^{s} \sum_{j_1=1}^{\ell - \mathfrak{g}+1-\alpha j_2} \binom{j_2}{j_4} \alpha_i^{j_2-j_4} \alpha_{P_j,j_1,j_3} q_{j_1,j_2} = 0, \tag{6}$$

for all $j_3 \geq 1, j_4 \geq 0$ s.t. $j_3 + j_4 - 1 < M_{i,j}$.
7: Solve the system of $C(M)$ equations in variables $\{q_{j_1,j_2}\}$.
8: Return Q.

Lemma 6. *For $\ell > \mathfrak{g} + \sqrt{2C(M)\alpha}$, a polynomial Q exists and can be found in $\mathrm{poly}(\ell)$ time.*

Proof. The system of equations from Step 4 of Algorithm 4.1 will have a solution as soon as the number of equations is smaller than the number of unknowns $\{q_{j_1,j_2}\}$. We have $\sum_{j_2=0}^{s} (\ell - \mathfrak{g} + 1 - \alpha j_2) > \frac{(\ell-\mathfrak{g})(\ell-\mathfrak{g}+2)}{\alpha}$. The total number of equations is $C(M)$. For our choice of ℓ, it holds that $\frac{(\ell-\mathfrak{g})(\ell-\mathfrak{g}+2)}{2\alpha} > C(M)$.

As the number of unknowns is bounded from above by ℓ^2, we can find $\{q_{j_1,j_2}\}$ using Gaussian elimination in $\mathrm{poly}(\ell)$ time. $\qquad \square \qquad \square$

13

Now let us verify that the found Q satisfies the two properties from Definition 3. We refer the reader to [8, Section 4] for a discussion on why Equations (6) in the unknowns $\{q_{j_1,j_2}\}$ guarantee that $Q(\alpha_i)[P_j]$ is zero of multiplicity $M_{i,j}$. The second property, $Q(f) \in \mathcal{L}(\ell P_\infty), \forall f \in \mathcal{L}(\alpha P_\infty)$, is guaranteed by Equation (5). Indeed, from the properties of $\nu(\cdot)$, $\nu_{P_\infty}(\phi_i)$ and $\nu_{P_\infty}(f)$, we have

$$\nu_{P_\infty}(Q(f)) \geq \min_{j_1,j_2}\{\nu_{P_\infty}(\psi_{j_1}) + j_2\nu_{P_\infty}(f)\} \geq \min_{j_1,j_2}\{-j_1 - \mathfrak{g} + 1 - \alpha j_2\} \geq -\ell.$$

Decoding quality.

The next definitions from [10] help to describe the codewords that will be found by factoring Q.

Definition 4. *To a codeword* $\mathbf{c} \in \mathbb{F}_q^n$ *associate a matrix* $[c] \in \mathbb{Z}^{|\mathbb{F}_q| \times n}$ *s.t.* $[c]_{i,j} = 1$ *iff* $\mathbf{c}_i = \alpha_j$, *and otherwise* $[c]_{i,j} = 0$.

Definition 5 (Matrix inner product)**.** *For two* $q \times n$ *matrices* A, B *defined over the same domain, let their inner product be*

$$\langle A, B \rangle = \sum_{i=1}^{q}\sum_{j=1}^{n} A_{i,j} \cdot B_{i,j}.$$

Definition 6 (Vector's score)**.** *For a vector* $\mathbf{v} \in \mathbb{F}_q^n$, *its score with respect to the multiplicity matrix* M *is*

$$S_M(\mathbf{v}) = \langle M, [\mathbf{v}] \rangle.$$

The following lemma describes the codewords that will be found by factoring Q relative to their score (cf. [10, Theorem 3]).

Lemma 7. *For* $Q(y)$ *found by Algorithm 4.1, we have that* $Q(y)$ *has a factor* $y - f(x)$ *where* $\mathbf{c} = (f(P_1), \ldots, f(P_n))$ *is a codeword, if*

$$S_M(\mathbf{c}) > \ell.$$

Proof. The goal of the proof is to show that $Q(f)$ is identical to 0.

Notice that due to the fact that $[\mathbf{c}]$ has only one non-zero entry per column, $S_M(\mathbf{c}) = \langle M, [\mathbf{c}] \rangle = M_1 + M_2 + \ldots M_n$, where $M_i = M_{i,j}$ for i s.t. $\mathbf{c}_j = \alpha_i$. By construction, $Q(y)$ passes through the point $(P_j, \alpha_i) = (P_j, c_j)$ with multiplicity $M_{i,j} = M_i$. We can show the following:

Claim 1. *For* f *s.t.* $\mathbf{c} = (f(P_1), \ldots, f(P_n))$, *it holds that* $\nu_{P_j}(Q(f)) \geq M_j$ *for all* $1 \leq j \leq n$.

of the claim. As in [8], define $Q^{(j)} := Q(x, y + \alpha_j)$. Then $Q(f) = Q^{(j)}(f - \alpha_j) = Q^{(j)}(f - c_j) = Q^{(j)}(f - f(P_j))$. Further, Guruswami-Sudan show that $Q(f)$ can be expressed as

$$Q(f) = \sum_{j_4=0}^{s}\sum_{j_3=1}^{\ell-\mathfrak{g}+1} q_{j_3,j_4}\psi_{j_3}^{(j)}(f - f(P_j))^{j_4},$$

14

for q_{j_3,j_4} defined in Equation (6). As is guaranteed by the output of Algorithm 4.1, we have $q_{j_3,j_4} = 0$ for $j_3 + j_4 \leq M_j$. Additionally, we have that $\nu_{P_j}(\psi_{j_3}^{(j)}) \geq j_3 - 1$ (see [8]), and $\nu_{P_j}((f - f(P_j)^{j_4}) \geq j_4$. Therefore, $\nu_{P_j}(Q(f)) \geq \min_{j_3,j_4}\{\nu_{P_j}(\psi_{j_3}^{(j)}) + \nu_{P_j}((f - f(P_j)^{j_4})\} = \min_{j_3,j_4}\{j_3 - 1 + j_4\} = M_j.$ $\square$ $\square$

From the claim it follows that $\sum_{P_j} \nu_{P_j}(Q(f)) \geq \sum_{j=1}^{n} M_j = S_M(\mathbf{c})$. On the other hand, since $Q(f) \in \mathcal{L}(\ell P_\infty)$, $\nu_{P_\infty}(Q(f)) \geq -\ell$. Consider the principal divisor $(Q(f))$ and its degree. It holds that

$$\deg(Q(f)) \geq \sum_{P_i} \nu_{P_i}(Q(f)) + \nu_{P_\infty}(Q(f)) = S_M(\mathbf{c}) - \ell > 0.$$

As the divisor is principal with a positive degree, we conclude that the function $Q(f)$ is zero. $\square$ $\square$

From the above theorem and by our choice of ℓ, the condition on a codeword $\mathbf{c}$ to be decoded can be formulated as $S_M(\mathbf{c}) > \lceil \mathfrak{g} + \sqrt{2C(M)\alpha} \rceil = \lceil \mathfrak{g} + \sqrt{2C(M)(k + \mathfrak{g} - 1)} \rceil$. Let us compare this result for AG-codes with the one from [10, Corollary 5] for Reed-Solomon codes. The latter states that a codeword $\mathbf{c}$ will be found by the soft-decision decoder if $S_M(\mathbf{c}) > \sqrt{2C(M)(k-1)}$. Indeed, as Reed-Solomon codes are codes of genus 0, plugging in $\mathfrak{g} = 0$ into our bound gives the result from [10].

Koetter-Vardy also give a condition on when a codeword will be found relative to the reliability matrix Π rather than to the multiplicity matrix, in case the output list size of the decoder is bounded. One can indeed stop the factorization process of Q once the required number of factors are found. We make a similar statement in the case of AG-codes. The following theorem is analogous to [10, Theorem 17].

Theorem 5 (Adapted from [10, Theorem 17])**.** *Given on input a list-size bound S, and a reliability matrix Π, algebraic soft-decision decoding that uses Algorithm 4.1 for the interpolation step, gives a list that contains a codeword $\mathbf{c}$ if*

$$\frac{\langle \Pi, [\mathbf{c}] \rangle}{\langle \Pi, \Pi \rangle} \geq \frac{\sqrt{k + \mathfrak{g} - 1}}{1 - \frac{1}{S}\left(\frac{1}{R} + \frac{\sqrt{|\mathbb{F}_q|}}{2\sqrt{R}}\right)},$$

where $R = \frac{k}{n}$ is the code-rate.

Proof. The proof follows the one from [10, Theorem 17] with the following modifications:

1. From the shape of Q given in Equation (5), it follows that factoring Q cannot produce more than s factors, hence $S \leq s$.

   By the choice of s given in Algorithm 4.1, we have

$$s < \frac{\ell - \mathfrak{g}}{\alpha} < \frac{\sqrt{2C(M)\alpha}}{\alpha} = \frac{\sqrt{2C(M)}}{\sqrt{k + \mathfrak{g} - 1}} = \frac{\sqrt{\langle M, M \rangle + \langle M, \mathbf{1} \rangle}}{\sqrt{k + \mathfrak{g} - 1}} =: L_k(M).$$

15

In the above, we used the fact that $2C(M) = \langle M, M \rangle + \langle M, \mathbf{1} \rangle$, where $\mathbf{1}$ is the all-one matrix. So $L_k(M)$ is an upper bound on S.

This is essentially a restatement of [10, Theorem 15], where again, setting $\mathfrak{g} = 0$, we get the Reed-Solomon case.

2. From the above, it is possible to express λ from Lemma 5. In particular, looking at the expression given in [10, Eq.(37)], we change $\frac{(k-1)L_k(M)^2}{\langle \Pi, \Pi \rangle}$ to $\frac{(k+\mathfrak{g}-1)L_k(M)^2}{\langle \Pi, \Pi \rangle}$.

3. The condition from Lemma 7, $S_M(C) > \ell$, can be then translated to

$$\langle M, [\mathbf{c}] \rangle > \ell > \mathfrak{g} + \sqrt{2C(M)\alpha} = \mathfrak{g} + L_k(M)(k+\mathfrak{g}-1) > L_k(M)(k+\mathfrak{g}-1).$$

4. In all remaining expressions for F_1, F_2, F_3 in the proof of [10, Theorem 17]we replace $(k-1)$ by $(k+\mathfrak{g}-1)$, which gives the statement of the theorem. $\qquad \square$ $\qquad \square$

Again, as with Lemma 7, the result of Theorem 5 can be seen as a generalization of the bound $\frac{\langle \Pi, [\mathbf{c}] \rangle}{\langle \Pi, \Pi \rangle} > \frac{\sqrt{k-1}}{1 - \frac{1}{L}\left(\frac{1}{R} + \frac{\sqrt{|\mathbb{F}_q|}}{2\sqrt{R}}\right)}$ from [10, Theorem 17] for $\mathfrak{g}$ different from 0.

4.3 Subfield subcodes decoding

Mook-Peikert in [4] suggest to use Koetter-Vardy soft-decision decoder for decoding BCH codes, which are subfield subcodes of Reed-Solomon codes. In particular, they propose a way to construct a reliability matrix Π for a received word $\mathbf{y}$, such that Koetter-Vardy's decoder outputs only codewords from the subfiled subcode. The method is generic and works for any subfield subcodes, including those of our interest. We do not give the details here and refer the reader to [4, Section 3]. Instead we state their [4, Theorem 3.4] adapted to our setting. The bound on the list S comes directly from the proofs in [4] and our bound from Theorem 5.

Theorem 6 (Adapted from [4, Theorem 3.4])**.** *For $\varepsilon > 0$, R – code rate, and d – mininal distance of Garcia-Stichtenoth codes defined over $\mathbb{F}_q$, there exists an algorithm for decoding subfield subcodes of Garcia-Stichtenoth codes that, upon receiving on input $\mathbf{y} \in \mathbb{R}_p^n$, calls Koetter-Vardy soft-decision decoder with the bound on the list size*

$$S = \frac{1/R + 1/\sqrt{2R}}{1 - \sqrt{\frac{R+\mathfrak{g}/n}{\varepsilon + (1-\varepsilon)(R+\mathfrak{g}/n)}}}, \tag{7}$$

and outputs codewords $\mathbf{c} \in \mathbb{F}_p^n$ from the subfield subcode that satisfy $\|\mathbf{y} - \mathbf{c}\| < (1-\varepsilon)\frac{d}{2}$, in time polynomial in n, $\log q$, and $1/\varepsilon$.

In the above expression for S, note that $\mathfrak{g}/n \approx 1/r = o(1)$. Moreover, for our choice of parameters in constructions of the Garcia-Stichtenoth codes C_i's, we have $R = \frac{k}{n} = \frac{\ell_i - \mathfrak{g} + 1}{n} = 1 - \frac{p^{2i} + \mathfrak{g} - 1}{n}$, for $i \leq L$. From our choice of L from Theorem 3, we conclude that $1/R$ is at most a constant, and $S = \mathcal{O}(1)$.

Moreover, for the minimal distances of Garcia-Stichtenoth codes, we have $d_i \geq n - \ell_i = p^{2i}$ (see Theorem 2). Therefore, Theorem 6 gives a decoder that decodes $\widetilde{C}_i$ up to distance $\leq p^i\sqrt{(1-\varepsilon)/2}$. It means that we can apply Theorem 4 and obtain an efficient

decoder for our lattices as as describe in the theorem below (cf. [4, Theorem 5.6]). Combined with Theorem 3 the above theorem gives our Theorem 1.

Theorem 7. *There exists an efficient algorithm that receiving on input $\mathbf{y} \in \mathbb{R}^n$, $\varepsilon > 0$, and running a decoder from Theorem 6 on list-sizes $S = \mathcal{O}(1)$, outputs a list of $\mathbf{v} \in \Lambda$ such that $\|\mathbf{y} - \mathbf{v}\| \leq \lambda_1(\Lambda)\sqrt{(1-\varepsilon)/2}$ in time $S^L = \mathrm{poly}(n)$.*

References

[1] Barnes, E.S., Wall, G.E.: Some extreme forms defined in terms of abelian groups. Journal of the Australian Mathematical Society **1**(1), 47–63 (1959)

[2] Grigorescu, E., Peikert, C.: List-decoding Barnes–Wall lattices. IEEE Conference on Computational Complexity **26**, 365–392 (2017)

[3] Ducas, L., Pierrot, C.: Polynomial time bounded distance decoding near Minkowski's bound in discrete logarithm lattices. Designs, Codes and Cryptography **87**(8), 1737–1748 (2019)

[4] Mook, E., Peikert, C.: Lattice (list) decoding near Minkowski's inequality. IEEE Trans. Inf. Theor. **68**(2), 863–870 (2022)

[5] Barnes, E.S., Sloane, N.J.A.: New lattice packings of spheres. Canadian Journal of Mathematics (1), 117–130 (1983)

[6] Bennett, H., Peikert, C.: Hardness of the (Approximate) Shortest Vector Problem: A Simple Proof via Reed-Solomon Codes. https://arxiv.org/abs/2202.07736

[7] Vlăduţ, S.: Lattices with exponentially large kissing numbers. Moscow Journal of combinatorics and number theory **8**(2), 163–177 (2019)

[8] Guruswami, V., Sudan, M.: Improved decoding of Reed-Solomon and algebraic-geometric codes. In: Proceedings 39th Annual Symposium on Foundations of Computer Science (Cat. No.98CB36280), pp. 28–37 (1998)

[9] Shum, K.W., Aleshnikov, I., Kumar, P.V., Stichtenoth, H., Deolalikar, V.: A low-complexity algorithm for the construction of algebraic-geometric codes better than the Gilbert-Varshamov bound. IEEE Transactions on Information Theory **47**(6), 2225–2241 (2001)

[10] Kotter, R., Vardy, A.: Algebraic soft-decision decoding of Reed-Solomon codes. In: 2000 IEEE International Symposium on Information Theory (Cat. No.00CH37060), p. 61 (2003)

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

[12] Stichtenoth, H.: Algebraic Function Fields and Codes, 2nd edn. Springer, ???

(2008)

[13] Guruswami, V., Xing, C.: Optimal rate list decoding over bounded alphabets using algebraic-geometric codes. J. ACM **69**(2) (2022)

[14] Garcia, A., Stichtenoth, H.: On the asymptotic behaviour of some towers of function fields over finite fields. Journal of Number Theory **61**(2), 248–273 (1996)

[15] Peikert, C.: A decade of lattice cryptography. Found. Trends Theor. Comput. Sci. **10**(4), 283–424 (2016)

[16] Shokrollahi, M.A., Wasserman, H.: Decoding algebraic-geometric codes beyond the error-correction bound. In: Proceedings of the Thirtieth Annual ACM Symposium on Theory of Computing. STOC '98, pp. 241–248 (1998)

[17] Gao, S., Shokrollahi, M.A.: Computing roots of polynomials over function fields of curves. In: Coding Theory and Cryptography, pp. 214–228 (2000)

Declaration

Competing interests