Electronic Colloquium on Computational Complexity, Report No. 136 (2025)

Robust Local Testability of Tensor Products of Constant-Rate Algebraic Geometry Codes

Sumegha Garg* Akash Kumar Sengupta†

Abstract

We study the robust local testability of tensor products of two Algebraic-Geometry (AG) codes. In particular, we prove that *constant rate* AG codes are robust locally testable. This significantly generalizes the seminal result of Polishchuk-Spielman [PS94], which proved robust local testability of Reed-Solomon codes. We establish an algebraic-geometric framework that enables us to geometrically interpret codewords in tensor products of AG codes. Thereby, we use tools from intersection theory of algebraic surfaces to prove a divisibility criterion for AG codes, that generalizes the bivariate divisibility result of Polishchuk-Spielman.

Over the years, robust local testability of tensor products has played a key role in the development of classical locally testable codes (LTCs) as well as quantum Low Density Parity Check (qLDPC) codes and quantum Locally Testable Codes (qLTCs). To the best of our knowledge, after Reed-Solomon codes, our result provides the first explicit family of robustly locally testable codes with constant rate and linear dual-distance. Moreover, our result, when combined with [GG24], yields new explicit families of good quantum CSS codes of length N which are locally testable with locality $O(\sqrt{N})$ and constant soundness.

*Department of Computer Science, Rutgers University, Piscataway, New Jersey, USA.
Email: sumegha.garg@rutgers.edu

†Department of Pure Mathematics and Department of Computer Science, University of Waterloo, Canada.
Email: aksengup@uwaterloo.ca

ISSN 1433-8092

Contents

1 Introduction

Tensor product of vector spaces is a fundamental algebraic operation that takes as input two vector spaces V, W over a field $\mathbb{K}$, and yields another vector space denoted as $V \otimes W$. This tensor product space is a universal object capturing linear-algebraic properties of all bilinear maps on $V \times W$. Since linear codes are vector spaces by definition, the tensor product operation provides a natural way of generating a new linear code from two given linear codes. Given two linear codes $\mathcal{C}_1 \subseteq \mathbb{F}_q^m$, $\mathcal{C}_2 \subseteq \mathbb{F}_q^n$ over a finite field $\mathbb{F}_q$, their tensor product $\mathcal{C}_1 \otimes \mathcal{C}_2 \subseteq \mathbb{F}_q^{nm}$ admits a succinct description in terms of matrices. Indeed, the *tensor product code* $\mathcal{C}_1 \otimes \mathcal{C}_2 \subseteq \mathbb{F}_q^{nm}$ can be identified as the space of all $n \times m$ matrices M whose rows are codewords of $\mathcal{C}_1$ and columns are codewords of $\mathcal{C}_2$.

Tensor products have turned out to be an immensely successful tool for constructing codes with good properties in classical as well as quantum coding theory [BSS06, DEL+22, LZ22, PK21]. One such highly desired property of codes is that of *local testability*. A *locally testable code* (LTC) is an error-correcting code which admits very efficient probabilistic membership tests. More specifically, a locally testable code $\mathcal{C} \subseteq \mathbb{F}_q^n$ has a tester that makes a small number of coordinate queries to a given word $x \in \mathbb{F}_q^n$ and accepts if x is a codeword, and rejects with constant probability if x is far from every codeword. LTCs can be viewed as the combinatorial core of Probabilistically Checkable Proofs (PCPs) and they play an important role in TCS.

Ben-Sasson and Sudan introduced the use of tensor products to construct LTCs and defined the notion of *robust local testability* [BSS06]. They considered a natural membership test for a tensor code $\mathcal{C}_1 \otimes \mathcal{C}_2 \subseteq \mathbb{F}^{n \times m}$ based on its defining property. Given a matrix $M \in \mathbb{F}^{n \times m}$, we know that $M \in \mathcal{C}_1 \otimes \mathcal{C}_2$ iff all the rows belong to $\mathcal{C}_1$ and all the columns belong to $\mathcal{C}_2$. So we can define a test as follows: pick a random row (or column) of M, accept iff it belongs to $\mathcal{C}_1$ (or $\mathcal{C}_2$). The notion of robust local testability captures the robustness of this membership test. In particular, a tensor product code $\mathcal{C}_1 \otimes \mathcal{C}_2$ is *robustly testable* if the following holds: for any matrix $M \subseteq \mathbb{F}^{n \times m}$, if the expected distance of a uniformly chosen row of M from $\mathcal{C}_1$ is small, and also the expected distance of a uniformly chosen column is small, then M is close to $\mathcal{C}_1 \otimes \mathcal{C}_2$ (see Definition 1.1).

The first known instances of robustly locally testable tensor products originated in the algebraic parts of the development of PCPs in early 1990s. In particular, the bivariate testing results of [BFLS91, PS94], that preceded the definition of robust local testability already showed that tensor product of Reed-Solomon codes are robustly testable. This robust local testability of tensor products of Reed-Solomon codes was used extensively in the celebrated PCP constructions. Ever since robust local testability has played a major role in several developments as noted below. It was a long-standing open problem to construct LTCs with constant rate, where robustly testable tensor codes had led to the first combinatorial construction of LTCs (and strong LTCs) of almost constant rate in [Mei08, Vid13]. More recently, the breakthroughs of [DEL+22, PK22] constructed LTCs of constant rate, distance and locality (so called c^3-LTCs) and settled the c^3-conjecture. Robust local testability of tensor products played an essential role in their constructions as it acts as the only source of redundancies in the local constraints. Moreover, robust local testability of Reed-Solomon codes also played a role in the breakthrough result showing $\mathrm{MIP}^* = \mathrm{RE}$ in [JNV+21].

In the quantum setting, it is still a major challenge to obtain such quantum Locally Testable Codes (qLTCs) with optimal parameters [AE15, EH17]. However, a flurry of recent works have achieved remarkable progress where robust local testability and its homological-algebraic variants have led to the construction of good quantum codes with best-known parameters so far [HHO21, PK22, BE21, LZ22, DHLV23]. These works are based on the connection between quantum codes and chain complexes in homological algebra, and use tensor products of chain complexes to construct good quantum codes. As an essential component, these constructions require classical codes which satisfy variants of the robust local testability property such as the product expansion property and two-way robustness. These variants are all equivalent to robust local testability in the case of two codes, and impose stronger constraints that imply robustness in the case of more than two codes but not vice versa.

In particular, [PK22] utilized the product expansion property to construct asymptotically good families of quantum Low Density Parity Check (qLDPC) codes and positively resolved the qLDPC conjecture. Recently, [DLV24] used the two-way robustness property to construct almost-good quantum LTCs with constant relative rate, inverse-polylogarithmic relative distance and soundness, and constant-size parity checks. Moreover, [GG24] showed that robust testability of Reed-Solomon codes yields explicit constructions of asymptotically

good quantum CSS codes, which are locally testable with square number of queries and constant soundness.

Given this plethora of applications of robust local testability of tensor products, a motivating question is the following:

What properties of codes $\mathcal{C}_1, \mathcal{C}_2$ guarantee robust local testability of the tensor product code $\mathcal{C}_1 \otimes \mathcal{C}_2$?

Ben-Sasson and Sudan [BSS06] asked whether $\mathcal{C}_1 \otimes \mathcal{C}_2$ is robustly testable for all codes $\mathcal{C}_1, \mathcal{C}_2$ of sufficiently large relative distance. This question was answered in the negative by Valiant [Val05] who constructed codes $\mathcal{C}_1 \otimes \mathcal{C}_2$ of relative distance arbitrarily close to 1, such that $\mathcal{C}_1 \otimes \mathcal{C}_2$ is not robustly testable. Subsequently, [CR05] provided examples of codes with constant rate and constant relative distance such that their tensor product is not robustly testable, and [GM12] constructed a code whose tensor product with itself is not robustly testable.

These counterexamples for general codes suggest that robust local testability of $\mathcal{C}_1 \otimes \mathcal{C}_2$ is a rather special property[1]. Indeed, robust local testability of $\mathcal{C}_1 \otimes \mathcal{C}_2$ has been established for very few classes of codes so far. In particular, the aforementioned bivariate testing result of [PS94] showed that tensor product of Reed-Solomon codes is robustly testable. [DSW06] showed that the tensor product of two codes is robustly testable if one of them is a special type of LDPC code, namely a smooth code. The works of [PK22, KP22, LZ22] showed that the tensor product of random linear codes is robustly testable with high probability. In [GSW24], it was shown that tensor product of Algebraic-Geometry codes of length n and rate $O(n^{-\frac{1}{2}})$ are robustly testable.

So far Reed-Solomon codes have been the only explicit family of robustly testable codes with asymptotically good parameters, i.e. constant rate, linear distance and linear dual-distance. Although LDPC codes can be explicitly constructed, their dual distance is constant. On the other hand, [GSW24] provided explicit families of AG codes with super-constant dual distance, but these codes have a strong restriction of the rate being $O(n^{-\frac{1}{2}})$.

In this paper, we prove robust local testability of tensor products of Algebraic-Geometry codes with optimal parameters, i.e. constant rate, linear distance and linear dual distance (Theorem 1.2). Our result, when combined with [GG24], yields new explicit good quantum CSS codes which are locally testable with low locality and constant soundness. In order to prove robust local testability of AG codes, we develop a geometric approach for studying tensor codes using intersection theory on algebraic surfaces. In particular, we set-up a correspondence between tensor codewords and curves on algebraic surfaces. Using intersection theoretic tools, we generalize the celebrated bivariate divisibility lemma of Polishchuk-Spielman [PS94] to the setting of AG codes. In the following subsections we will discuss our results, key ideas and technical contributions, some of which are interesting in their own right.

1.1 Robust local testability of Algebraic-Geometry codes

First let us formally define robust testability of tensor products. For a vector $F \in \mathbb{F}_q^n$ and a code $\mathcal{C} \subseteq \mathbb{F}_q^n$, we use $\delta(F, \mathcal{C})$ to denote the distance of F to the nearest codeword in C (see Section 2.2).

Definition 1.1. [Robust testability of tensor product] Let $0 \leq \rho \leq 1$. For codes $\mathcal{C}_1 \subseteq \mathbb{F}_q^m$ and $\mathcal{C}_2 \subseteq \mathbb{F}_q^n$, we say that $(\mathcal{C}_1, \mathcal{C}_2)$ is ρ-robust, or equivalently $\mathcal{C}_1 \otimes \mathcal{C}_2$ is ρ-robustly testable, if for every $F \in \mathbb{F}_q^{n \times m}$, we have

$$\rho \cdot \delta(F, \mathcal{C}_1 \otimes \mathcal{C}_2) \leq \frac{1}{2}[\delta(F, \mathcal{C}_1 \otimes \mathbb{F}_q^n) + \delta(F, \mathbb{F}_q^m \otimes \mathcal{C}_2)]$$

The parameter ρ quantifies the robustness of the natural membership test for the tensor code $\mathcal{C}_1 \otimes \mathcal{C}_2$. If the rows of F are close to $\mathcal{C}_1$ and the columns of F are close to $\mathcal{C}_2$, then the average distance, i.e. the right hand side of the inequality, is small. Therefore the ρ-robustly testable condition implies that the distance of F to $\mathcal{C}_1 \otimes \mathcal{C}_2$ is also small.

[1] In [BSS06], it was shown that the tensor product of *three or more* codes is robustly testable and it was used to construct LTCs. However, in order to construct good classical and quantum codes with optimal parameters it is necessary to have robust testability of tensor product of *two codes* or in the case of more than two codes, strictly stronger properties such as product expansion are necessary. This necessitates the study of robust local testability for special classes of codes.

Our main result will show tensor products of Algebraic-Geometry (AG) codes are robustly locally testable. AG codes were first constructed by Goppa [Gop77, Gop81, Gop83] and these codes serve as a generalization of Reed-Solomon codes and BCH codes. Below we will discuss an informal definition and basic properties of AG-codes. We will defer the precise technical definition of AG codes to Section 2.

Algebraic-Geometry codes. A general recipe for constructing a linear code $\mathcal{C} \subseteq \mathbb{F}_q^n$ is as follows. Consider a finite set $\mathcal{S} = \{s_1, \cdots, s_n\}$ and a finite dimensional vector space $\mathcal{F}$ consisting of functions $f : \mathcal{S} \to \mathbb{F}_q$. Consider the set of evaluations $\mathcal{C} = \{(f(s_1), \cdots, f(s_n)) \mid f \in \mathcal{F}\}$. Then $\mathcal{C} \subseteq \mathbb{F}_q^n$ is a linear code of block length n over $\mathbb{F}_q$. If we take $\mathcal{S} \subseteq \mathbb{F}_q$ and then any univariate polynomial $f(x) \in \mathbb{F}_q[x]$ defines a function $\mathcal{S} \to \mathbb{F}_q$ by evaluating the polynomial. By restricting the degree of the polynomials, we can obtain a finite dimensional vector space and the corresponding evaluation code is the Reed-Solomon code

$$\mathrm{RS}(n,k) = \{(f(s))_{s\in\mathcal{S}} \mid f(x) \in \mathbb{F}_q[x] \text{ and } \deg(f) < k\}.$$

AG codes are generalizations of Reed-Solomon codes where $\mathcal{S}$ is taken to be a set of points on an algebraic curve X and the set $\mathcal{F}$ is a space of rational functions on the curve. Here an algebraic curve is an one dimensional geometric object defined by polynomial equations over a finite field $\mathbb{F}_q$. For example, if $f(x,y) \in \mathbb{F}_q[x,y]$ is a irreducible polynomial, the set of all zeros of f, i.e. $X := \{(a,b) \mid f(a,b) = 0\} \subseteq \mathbb{F}_q^2$ is an algebraic curve. Moreover, rational functions on the algebraic curve X are functions of the form $\{f/g \mid f, g \in \mathbb{F}_q[x,y], g|_X \not\equiv 0\}$, i.e. quotients of polynomials f, g such that g does not vanish at all points of X. For a rational function $h = f/g$, the set where the denominator g vanishes is called the set of poles of h. If we choose $\mathcal{S} = X \setminus \{p\}$ for some point $p \in X$ and let $\mathcal{F}$ be a space of rational functions with no poles in $\mathcal{S}$, then we can evaluate every rational function $h \in \mathcal{F}$ at the points of $\mathcal{S}$. In order to ensure finite dimensionality, we need to impose an upper bound on the order of vanishing of h at its possible pole p, similar to restriction on the degree in case of Reed-Solomon codes. Given an algebraic curve X, a point $p \in X$ and fixing a degree ℓ, we can define the corresponding AG-code as

$$\mathcal{C}(X,p,\ell) := \{(h(s))_{s\in S} \mid \text{ the only possible pole of } h \text{ is at } p \text{ with order of vanishing at most } \ell\}.$$

Every algebraic curve has a non-negative integer g associated with it, the so called *genus* of the algebraic curve. The genus of X governs several algebraic-geometric and arithmetic properties of X. Moreover, the genus also governs the parameters of AG codes, such as the rate. If $|\mathcal{S}| = n$ and genus of X is g, then the linear code $\mathcal{C}(X,p,k) \subseteq \mathbb{F}_q^n$ is of length n, dimension at least $\ell - g$ and distance at least $n - \ell$. We will say that $\mathcal{C}(X,p,\ell)$ is an AG code of length n, genus g and degree ℓ.

AG codes have numerous useful properties, for example, they can be explicitly constructed and can be efficiently decoded. Similar to Reed-Solomon codes, AG codes also satisfy the multiplicative property, i.e. the Hadamard product of two codewords from $\mathcal{C}(X,p,\ell_1), \mathcal{C}(X,p,\ell_2)$ is a codeword in $\mathcal{C}(X,p,\ell_1+\ell_2)$. Moreover, AG codes exhibit several properties which make them better suited for applications than Reed-Solomon and random codes. For instance, one can construct arbitrarily long AG codes over a given fixed field, whereas the length of a Reed-Solomon code can be at most the field size q. Furthermore, AG codes are famously known to surpass the Gilbert–Varshamov bound, which also shows the existence of AG codes that are better than random codes. We refer to [Sti09, Ste12, CR21] for more details and exposition on AG codes.

Main result. In this paper, we prove the following result showing tensor products of AG codes are robustly testable.

Theorem 1.2 (Informal version of Theorem 6.2)**.** *For all $\epsilon \in (0,1)$, there exists $\rho(\epsilon) > 0$ such that the following holds. Let $\mathcal{C}_1$ and $\mathcal{C}_2$ be two AG codes of length n, genus g_1, g_2 and degrees ℓ_1 and ℓ_2 respectively. Suppose that $4 + g_1 + \ell_1 + g_2 + \ell_2 < (1-\epsilon)n$. Then the tensor product code $\mathcal{C}_1 \otimes \mathcal{C}_2$ is $\rho(\epsilon)$-robustly testable.*

Our result generalizes the robust local testability of Reed-Solomon codes [PS94]. Since Reed-Solomon codes are special cases of AG codes of genus 0, we obtain the robust local testability of Reed-Solomon codes

a special case of our result. Theorem 1.2 establishes robust testability for constant rate AG codes and it also generalizes the robust testability of AG codes of length n and rate $O(n^{-\frac{1}{2}})$ [GSW24][2].

After Reed-Solomon codes, our result provides the first explicit family of robustly locally testable codes with constant rate and linear dual-distance. Since the length of a Reed-Solomon code over $\mathbb{F}_q$ is at most q, our result provides the first explicit family of robustly testable codes with these optimal parameters where the length n can be arbitrarily large for fixed $\mathbb{F}_q$ (see Example 2.5 for existence of such codes).

Moreover, Theorem 1.2 is *optimal* since the inequality $4+g_1+\ell_1+g_2+\ell_2 < (1-\epsilon)n$ can not be relaxed. Indeed, [KP22] showed that the tensor product of a code and its dual code is never robustly testable. More specifically, if $\{\mathcal{C}_n\}$ is family of codes of length n, then $\mathcal{C}_n \otimes \mathcal{C}_n^{\perp}$ is not ρ-robustly testable for any fixed $\rho > 0$, as $n \to \infty$. If we let $\mathcal{C}_n = \mathcal{C}(X, p, \ell_1)$ be an AG code of length n, genus g and degree ℓ_1, then the dual $\mathcal{C}_n^{\perp}$ is also an AG code of length n, genus g and degree $\ell_2 := 2g - 2 + n - \ell_1$. For any ϵ and fixed $\rho(\epsilon)$, this provides examples of AG codes $\mathcal{C}_n, \mathcal{C}_n^{\perp}$ of length n, genus $g = \Theta(n)$ and degrees $\ell_1 = \Theta(n), \ell_2 = \Theta(n)$ such that $(1-\epsilon)n \leq 4 + 2g + \ell_1 + \ell_2$ and $\mathcal{C}_n \otimes \mathcal{C}_n^{\perp}$ is not $\rho(\epsilon)$-robustly testable as $n \to \infty$.

In order to prove Theorem 1.2, we establish a divisibility criterion for tensor products of AG codes, which generalizes the bivariate divisibility lemma of [PS94], and it is of independent interest as well.

1.2 Generalized divisibility for AG codes

The key ingredient that led to robust testability of Reed-Solomon codes is an algebraic statement regarding divisibility of bivariate polynomials. This so called divisibility lemma due to Polishchuk-Spielman [PS94] is the following statement.

Lemma 1.3 (Bivariate divisibility)**.** *[PS94, Lemma 8] Let $E(x,y)$ be a polynomial of degree (b,a) and $N(x,y)$ be a polynomial of degree $(b+d, a+d)$. If there exist distinct $x_1, \cdots, x_n$ such that $E(x_i, y)$ divides $N(x_i, y)$ for $1 \leq i \leq n$, distinct $y_1, \cdots, y_n$ such that $E(x, y_j)$ divides $N(x, y_j)$ for $1 \leq i \leq n$, and if*

$$n > \min\{2b + 2d, 2a + 2d\},$$

then $E(x,y)$ divides $N(x,y)$.

Here the degree of a bivariate polynomial $P(x,y)$ is the *bi-degree*, i.e. $P(x,y)$ has degree (d,e) iff P has degree d in the x variable and degree e in the y variable. Note that if $P(x,y) \in \mathbb{F}_q[x,y]$, then $P(x,c)$ is a univariate polynomial in $\mathbb{F}_q[x]$ when we fix $y = c$ (a constant). Similarly, if $\ell \subseteq \mathbb{F}_q^2$ is a line defined by $y = mx + c$, then the restriction $P|_\ell := P(x, mx+c)$ is a univariate polynomial in $\mathbb{F}_q[x]$. If $E(x,y)$ divides $N(x,y)$ as bivariate polynomials in $\mathbb{F}_q[x,y]$, i.e. $N(x,y) = Q(x,y)E(x,y)$ for some $Q(x,y) \in \mathbb{F}_q[x,y]$, then $E|_\ell$ divides $N|_\ell$ as univariate polynomials for all lines ℓ (as long as $E|_\ell$ is not identically 0). The divisibility lemma essentially provides a converse of this, and helps deduce bivariate divisibility from univariate divisibility. It says that if $E|_\ell$ divides $N|_\ell$ for restrictions to sufficiently many axis-parallel lines ℓ in $\mathbb{F}_q^2$ (in both x and y directions), then E divides N as bivariate polynomials in $\mathbb{F}_q[x,y]$.

This bivariate divisibility lemma has played a key role in several developments especially in algebraic property testing. For instance, Friedl and Sudan used this divisibility lemma for multivariate low-error low-degree testing [FS95], and more recently a variant of the divisibility lemma was used for low-degree testing in the high-error regime [HKSS24]. In [BSCI+23], a version of this lemma was used for studying proximity of affine subspaces of $\mathbb{F}_q^n$ to a Reed-Solomon code, and led to a near-optimal proximity gap result. In another direction, variants of the divisibility lemma were used to construct high-rate multivariate polynomial evaluation codes [KKS24].

Before we state our generalization of the bivariate divisibility lemma, let us recall the natural correspondence between bivariate polynomials and codewords in tensor product of Reed-Solomon codes. We will then rephrase the divisibility lemma in terms of tensor codewords.

[2]The result of [GSW24] works in the more general setting of abstract AG codes. However the explicit family provided there involves usual AG codes from algebraic curves.

Since a non-zero polynomial of degree d in $\mathbb{F}_q[x]$ can have at most d number of zeroes, we have a one-to-one correspondence, assuming $d < n$,

$$\left\{\text{Codewords in } \mathrm{RS}(n,d)\right\} \longleftrightarrow \left\{P(x) \in \mathbb{F}_q[x], \deg(P) < d\right\}$$

Given a bivariate polynomial $P \in \mathbb{F}_q[x,y]$ of bi-degree (d,e) and $x_i, y_j \in \mathbb{F}_q$ for $i,j \in [n]$, we may evaluate it on the pairs (x_i, y_j) to construct a $n \times n$-matrix M defined by $M_{ij} := P(x_i, y_j)$. Note that every row of M is given by evaluation of the univariate polynomial $P(x_i, y)$, and hence it is a codeword in $\mathrm{RS}(n,e)$. Similarly, every column is a codeword in $\mathrm{RS}(n,d)$. Therefore, by definition, we have that M is a codeword of the tensor product code $\mathrm{RS}(n,e) \otimes \mathrm{RS}(n,d)$. Moreover, [PS94, Proposition 4], shows that the converse is also true, i.e. every tensor codeword M is an evaluation of a bivariate polynomial $P(x,y)$. In fact, P is uniquely determined by the tensor codeword M if $d, e < n$. Therefore we have a one-to-one correspondence between bivariate polynomials and tensor codewords.

$$\left\{\text{Codewords in } \mathrm{RS}(n,e) \otimes \mathrm{RS}(n,d)\right\} \longleftrightarrow \left\{P(x,y) \text{ of bi-degree at most } (d,e)\right\}$$

If we view bivariate divisibility via this correspondence, we see that $E(x,y)$ divides $N(x,y)$, i.e. $E(x,y) = Q(x,y)N(x,y)$, iff there exists a codeword $Q \in \mathrm{RS}(n,d) \otimes \mathrm{RS}(n,d)$ such that $N(x_i,y_j) = E(x_i,y_j)Q(x_i,y_j)$ for all $i,j \in [n]$. In other words, $E(x,y)$ divides $N(x,y)$ in $\mathbb{F}_q[x,y]$ iff the corresponding tensor codeword E divides N under the Hadamard product of codes.

Moreover, the information that $E(x_i,y)$ divides $N(x_i,y)$ can be packaged into the equivalent statement that there is a codeword $R \in \mathrm{RS}(n,d) \otimes \mathbb{F}_q$ such that $E(x_i,y_j)R(x_i,y_j) = N(x_i,y_j)$ for all $i,j \in [n]$. Similarly there is a codeword $C \in \mathbb{F}_q \otimes \mathrm{RS}(n,d)$ such that $E(x_i,y_j)C(x_i,y_j) = N(x_i,y_j)$. Note that R, C might not be in $\mathrm{RS}(n,e) \otimes \mathrm{RS}(n,d)$, i.e. they might not be given by bivariate polynomials. However, the bivariate divisibility lemma says that if n is large enough, then there exists such a codeword $Q \in \mathrm{RS}(n,d) \otimes \mathrm{RS}(n,d)$.

Our generalized divisibility lemma (Lemma 5.3) shows that the same statement holds with Reed-Solomon codes replaced by AG codes. We now state a simplified version of our generalized divisibility lemma for AG codes. In the following lemma, we let X be an algebraic curve of genus g, fix a point $p \in X$ and denote the AG codes $\mathcal{C}(X,p,\ell)$ as $\mathcal{C}(\ell)$. Here the notion of divisibility is with respect to the Hadamard product. In particular, given tensor codewords $E \in \mathcal{C}(a) \otimes \mathcal{C}(b)$ and $N \in \mathcal{C}(a+d) \otimes \mathcal{C}(b+d)$, we say that E divides N if there exists a codeword $Q \in \mathcal{C}(d) \otimes \mathcal{C}(d)$ such that

$$N(x_i,y_j) = E(x_i,y_j)Q(x_i,y_j)$$

for all $i,j \in [n]$.

Lemma 1.4 (Generalized divisibility for AG codes)**.** *Let $E \in \mathcal{C}(a) \otimes \mathcal{C}(b)$ and $N \in \mathcal{C}(a+d) \otimes \mathcal{C}(b+d)$ be tensor codewords. Suppose there exist codewords $R \in \mathcal{C}(d) \otimes \mathbb{F}_q^n$ and $C \in \mathbb{F}_q^n \otimes \mathcal{C}(d)$ such that*

$$E(x_i,y_j)R(x_i,y_j) = E(x_i,y_j)C(x_i,y_j) = N(x_i,y_j)$$

for all $i,j \in [n]$. If $n > a+b+2d$, then E divides N.

In Lemma 5.3, we prove this divisibility criterion in full generality. In particular, we allow AG codes from two different curves X, Y and the lemma applies to the general definition of AG codes using divisors on algebraic curves (Definition 2.2). Although we phrased the lemma above in terms of codewords in the tensor product code, it is really a statement about rational functions on algebraic curves. We note that all the previous variants of bivariate divisibility only worked for polynomials, whereas ours is the first one to deal with rational functions on algebraic curves. Thus our proof requires new techniques and ideas. We set up a one-to-one correspondence between tensor codewords and curves on algebraic surfaces. This enables us to apply algebraic-geometric techniques from intersection theory of algebraic surfaces. In Section 1.4, we will discuss our algebraic-geometric approach and these technical developments in more detail. We now note an application of our main result towards construction of quantum locally testable codes.

1.3 Application: good quantum codes

Quantum Low Density Parity Check (qLDPC) codes are quantum counterparts of classical LDPC codes and these codes are known to be very useful for fault-tolerant quantum computation. Although good families of classical LDPC codes were known since 1960s, constructions of qLDPC codes with asymptotically good parameters were unavailable up until very recently. Starting with the work on fiber bundle codes [HHO21], a series of further breakthroughs [PK21, BE21, PK22] finally provided constructions of asymptotically good qLDPC codes using the lifted product construction, which is a generalization of tensor products of classical codes. Subsequently, two other families of asymptotically good qLDPC codes were constructed in [LZ22, DHLV23] using the left-right Cayley-complex, which had also led to the construction of c^3-LTCs in [DEL$^+$22]. Quantum locally testable codes (qLTC) with optimal parameters are still out of reach. However, [DLV24] constructed almost-good quantum LTCs with constant relative rate, inverse-polylogarithmic relative distance and soundness, and constant-size parity checks.

Several of these constructions of asymptotically good quantum codes employ robust local testability of tensor products of random codes. A natural problem is to find new constructions of asymptotically good qLDPC codes and qLTCs, and perhaps a construction that uses robust testability of explicit codes such as Reed-Solomon codes. In [BH14], homological products were used to give a probabilistic construction of quantum codes of length N with distance $\Theta(N)$ and stabilizer-weight $\Theta(\sqrt{N})$. In [GG24], this construction was derandomized, and by using robust local testability of Reed-Solomon codes this work obtained explicit constructions of such quantum codes. Before stating our application to quantum codes, we recall the basic notions of quantum codes below.

The simplest construction of quantum codes is due to Calderbank, Shor, and Steane (CSS) [CS96]. These so called quantum CSS codes are a pair of classical codes (Q_X, Q_Z) with an orthogonality property $Q_X^{\perp} \subseteq Q_Z$. If Q is defined over $\mathbb{F}_q$ and it is a quantum code of length n, dimension k and distance d, then we say that Q is a $[[n,k,d]]_q$ code[3]. If Q_X, Q_Z are AG codes, then we will say that Q is a quantum AG code. For an algebraic curve X of genus g and a point $p \in X$, let us denote the AG code $\mathcal{C}(X,p,\ell)$ as $\mathcal{C}(\ell)$ as before. If we let $Q_X = Q_Z = \mathcal{C}(\ell)$, then by appropriately choosing ℓ, we can ensure the orthogonality property. Hence the pair $Q = (Q_X, Q_Z)$ is a quantum AG code, which we denote as $\mathcal{Q}(\ell)$. This construction provides explicit asymptotic families of quantum AG codes of constant rate and relative distance over any finite field $\mathbb{F}_q$.

Our main result, when combined with [GG24, Theorem 2.4], directly yields new explicit families of locally testable quantum codes as follows.

Corollary 1.5 (Informal version of Corollary 6.5)**.** *Let $\mathbb{F}_q$ be a finite field of characteristic 2, such that $q \geq 2^{16}$. Fix $\frac{7}{\sqrt{q}-4} < \epsilon < \frac{1}{8}(1-\frac{14}{\sqrt{q}})$. For any n, we let $N = n^2$. There exist $\ell_1 = \Theta_\epsilon(n)$ and $\ell_2 = \Theta_\epsilon(n)$ such that the homological product of the quantum AG codes $\mathcal{Q}(\ell_1)$ and $\mathcal{Q}(\ell_2)$ is a $[[N, \Theta(N), \Theta(N)]]_q$ quantum CSS code that is locally testable with locality $O(\sqrt{N})$ and soundness $\Omega(1)$.*

In [GG24, Corollary 4.4], robust testability of Reed-Solomon codes was used to prove the analogous result for homological products of quantum Reed-Solomon codes. Our result generalizes this to the case of quantum AG codes. Note that the result of [GG24] also provided locally testable quantum codes with same asymptotic order of parameters as in Corollary 1.5. However, due to the use of Reed-Solomon codes, the length N of the quantum code $\mathcal{Q}$ was restricted to be at most q^2. On the other hand, Corollary 1.5 provides quantum codes of arbitrarily large length N over a fixed field $\mathbb{F}_q$.

1.4 Technical contributions and overview of proofs

The key technical result for obtaining robust local testability of AG codes is our generalized divisibility lemma (Lemma 1.4). In order to prove this divisibility result, we will establish an algebraic-geometric framework for interpreting tensor codewords as geometric objects. In particular, we will build a correspondence between tensor AG codewords and curves on algebraic surfaces. This framework will enable us to interpret divisibility

[3]Here the notions of dimension and distance of a quantum code Q are dependent on both of the classical codes Q_X and Q_Z. We refer to Section 2.6 for the precise definition.

of AG codewords as a geometric problem about containment of curves. Finally, we will use intersection theoretic techniques to study both local and global behaviour of tensor codewords, which will lead us to the proof of generalized divisibility. Our method is a generalization of the Bezout-type argument for obtaining bivariate divisibility in [PS94]. We start by reviewing the ideas behind the proof of bivariate divisibility.

Bivariate divisibility

The bivariate divisibility lemma in [PS94], as well as its variants [Spi95, BSCI+23, KKS24], are all based on Bezout's theorem in algebraic geometry. In algebraic terms, Bezout's theorem says that if $E, N \in \mathbb{F}_q[x, y]$ are bivariate polynomials without common factors and of degrees d, e respectively, then E, N can have at most de number of common zeroes in $\mathbb{F}_q^2$, even when counted with multiplicities. Here the notion of intersection multiplicity at a common zero captures the information about the derivatives of the polynomials. Thus Bezout's theorem is a generalization of the fact that a degree d univariate polynomial can have at most d roots even when the roots are counted with their multiplicities.

Now the bivariate divisibility problem is the following. We have two bivariate polynomials $E, N \in \mathbb{F}_q[x, y]$ such that the univariate polynomial $E|_\ell$ divides $N|_\ell$ for restrictions to n number of axis-parallel lines $\ell \subseteq \mathbb{F}_q^2$. If n is sufficiently large compared to degrees of E, N, then E must divide N as bivariate polynomials in $\mathbb{F}_q[x, y]$. The proofs of the bivariate divisibility results can be summarized in the following steps.

1. *Reduction to coprime polynomials.* One can show that we may replace E, N by $E/\gcd(E, N)$ and $N/\gcd(E, N)$ without loss of generality, and assume that E, N do not have any common factors, i.e. they are coprime polynomials.

2. *Lower bound on local intersection multiplicities.* By assumption, we have that $E|_\ell$ divides $N|_\ell$, and both are univariate polynomials. Hence, if x is a root of $E|_\ell$ of multiplicity m, then it is also a root of $N|_\ell$ of multiplicity at least m. Using this we can obtain a lower bound for the intersection multiplicity at the common zeroes of E, N that lie on the given n number of axis-parallel lines.

3. *Global upper bound on total number of common zeroes.* Now, if E does not divide N, the we may apply Bezout's theorem. Hence, we can obtain a global upper bound on the total number of common zeroes (with multiplicities) in terms of the degrees of E, N.

4. *Compare the bounds.* If n is sufficiently large compared to the degrees of E, N, then the lower bound ends up being larger than the upper bound. This leads to a contradiction, and hence we must have that E divides N.

The outline above immediately leads to a weaker version of the bivariate divisibility lemma (see [Spi95, Proposition 4.2.22]), where n needs to be much larger than the bound in Lemma 1.3. Polishchuk-Spielman [PS94] adapted Bezout's theorem algebraically, and they used properties of resultants of polynomials and unique factorization to obtain the lower and upper bounds in the steps above. In particular, their algebraic adaptation provided an improved upper bound in Step 3, leading to Lemma 1.3 with a better inequality. However, these algebraic tools are specific to polynomials and make the technique less amenable to generalizations.

On the other hand, one can equivalently view the steps above in a geometric way using the algebra-geometry dictionary. In particular, each bivariate polynomial $E, N \in \mathbb{F}_q[x, y]$ gives rise to an algebraic curve in $\mathbb{F}_q^2$, which we may as well denote by $E, N \subseteq \mathbb{F}_q^2$. Then the divisibility $E|N$ implies the containment of the corresponding algebraic curves, i.e. $E \subseteq N$. In Section 3, we illustrate this geometric perspective by proving a version of bivariate divisibility (see Lemma 3.1) using properties of plane algebraic curves. In particular, in Lemma 3.7, we note that the lower bound of Step 2 is a consequence of basic properties of non-singular algebraic curves[4]. Similarly, this geometric perspective was also used to obtain a version of bivariate (and multivariate) divisibility in [KKS24] that deals with lines in general position instead of axis-parallel lines (see Section 1.5 for a comparison).

[4]Lemma 3.7 is a more general version of the similar statements in [Spi95, KKS24], which dealt with lines instead of non-singular curves in general.

Generalized divisibility for AG codes

The results discussed above dealt with divisibility problems for polynomials. In our setting of AG codes, we are presented with new challenges arising from rational functions on algebraic curves. Moreover, the geometry of higher genus algebraic curves is significantly more complex than that of genus 0 curves. Thus AG codes pose novel geometric challenges which were not present in the case of Reed-Solomon codes and polynomial evaluations. Below we will discuss the divisibility problem for AG codes and our algebraic-geometric tools that enables us to carry out analogues of the steps outlined above in this more general setting of AG codes.

Formalizing divisibility. Recall that in our setting of AG codes, the notion of divisibility is with respect to the Hadamard product. In other words, given two tensor AG codes $E \in \mathcal{C}(a) \otimes \mathcal{C}(b)$ and $N \in \mathcal{C}(a+d) \otimes \mathcal{C}(b+d)$, we say that E divides N if there exists a codeword $Q \in \mathcal{C}(d) \otimes \mathcal{C}(d)$ such that

$$N(x_i, y_j) = E(x_i, y_j)Q(x_i, y_j)$$

for all $i, j \in [n]$. When E, N are tensor Reed-Solomon codes, their divisibility under Hadamard product is equivalent to divisibility as bivariate polynomials in $\mathbb{F}_q[x, y]$ via the correspondence described earlier. Now the tensor AG codewords E, N are defined as evaluations of rational functions on an algebraic curve X, instead of polynomials. Although rational functions can be described as quotients of polynomials modulo the ideal of X, the divisibility of tensor AG codewords under the Hadamard product does not translate to an algebraic notion of divisibility. Indeed, the set of rational functions form a field, and there always exists a rational function, namely $Q = N/E$, such that $N = EQ$.

On the other hand, the geometric perspective in the setting of Reed-Solomon codes says that if E divides N as tensor codewords then we have a containment of corresponding plane algebraic curves $E \subseteq N$ in $\mathbb{F}_q^2$. In fact, Hilbert's Nullstellensatz implies a stronger statement over the algebraic closure $\overline{\mathbb{F}_q}$. In particular, an irreducible polynomial E divides N as bivariate polynomials iff the corresponding algebraic curves satisfy $E \subseteq N$ as subsets of $\overline{\mathbb{F}_q}^2$. Motivated by this observation, we extend this geometric perspective to AG codes and interpret tensor AG codewords in terms of curves on algebraic surfaces.

Tensor codewords and divisors on algebraic surfaces. Given a bivariate rational function $h = \frac{F(x,y)}{G(x,y)}$, one can associate a natural geometric object to it as follows. Let $F = F_1^{r_1} \cdots F_a^{r_a}$ and $G = G_1^{s_1} \cdots G_b^{s_b}$ be the irreducible factorizations in $\mathbb{F}_q[x, y]$. Then the bivariate polynomials F_i, G_j each give rise to algebraic curves $F_i, G_j \subseteq \mathbb{F}_q^2$. Therefore the natural algebraic-geometric object corresponding to the rational function h is the collection of curves $\{F_i, G_j \mid i \in [a], j \in [b]\}$ along with their multiplicities r_i, s_j. Here the algebraic curves G_j can be thought of as the set of poles of h and similarly F_i are the set of zeroes of h. This leads us to interpret rational functions via the well-established notion of *divisors* in algebraic-geometry. A divisor on an algebraic surface S is a finite $\mathbb{Z}$-linear combination of curves $\sum_{i=1}^{r} a_i C_i$, where $C_i \subseteq S$ are irreducible curves. Thus, the divisor corresponding to the rational function h above is given by $\sum_i r_i F_i - \sum_j s_j G_j$ on the algebraic surface $\mathbb{F}_q^2$.

In Section 4.3, we use algebraic-geometric tools to adapt the above in a coding-theoretic setting. In particular, suppose X, Y are two algebraic curves and let $\mathcal{C}_X(a), \mathcal{C}_Y(b)$ be AG codes defined by evaluations of rational functions on X, Y respectively. For each tensor AG codeword $D \in \mathcal{C}_X(a) \otimes \mathcal{C}_Y(b)$, we associate a divisor on the algebraic surface $X \times Y$ [5].

$$\left\{\text{Codewords in } \mathcal{C}_X(a) \otimes \mathcal{C}_Y(b)\right\} \longrightarrow \left\{\text{Divisors on the algebraic surface } X \times Y\right\}$$

In fact, by studying the zeroes and poles of rational functions, we show a stronger statement that the map above is a bijection onto a natural subclass $\mathcal{L}_{a,b}$ of divisors on $X \times Y$. This natural subclass $\mathcal{L}_{a,b}$ is in spirit similar to the plane curves of bi-degree (a, b). However the notion of bi-degree is too weak in this general setting of product surfaces, and we work with finer intersection-theoretic properties of divisors.

[5] In the case of Reed-Solomon codes, the product surface corresponds to $\mathbb{F}_q \times \mathbb{F}_q = \mathbb{F}_q^2$.

A key feature is that we establish this correspondence over the algebraic closure $\overline{\mathbb{F}_q}$. Moreover, the correspondence over $\mathbb{F}_q$ is obtained by specializing to so called $\mathbb{F}_q$-rational divisors, i.e. divisors defined over the base field $\mathbb{F}_q$. This feature enables us to simultaneously apply intersection theoretic techniques over the algebraic closure as well as study tensor codewords over $\mathbb{F}_q$. Moreover, as an important property, we ensure that the divisors in $\mathcal{L}_{a,b}$ have only non-negative coefficients in its $\mathbb{Z}$-linear expression. In general, the divisors corresponding to bivariate rational functions discussed above can have negative coefficients. However the non-negativity property of $\mathcal{L}_{a,b}$ ensures that these divisors still behave as curves (see Section 4.3 for properties of this construction).

A geometric solution. The geometric framework above enables us to translate the divisibility of AG codes into a geometric problem about divisors on algebraic surfaces. In particular, given $E \in \mathcal{C}_X(a) \otimes \mathcal{C}_Y(b)$ and $N \in \mathcal{C}_X(a+d) \otimes \mathcal{C}(b+d)$ we consider the associated divisors on $X \times Y$, which we still denote by $E, N \subseteq X \times Y$. Now suppose there exist codewords $R \in \mathcal{C}_X(d) \otimes \mathbb{F}_q^n$ and $C \in \mathbb{F}_q^n \otimes \mathcal{C}_Y(d)$ as in Lemma 1.4. We translate this information into intersection theoretic properties of the divisors E, N when intersected with vertical and horizontal curves in the product surface $X \times Y$ in Lemma 5.1. In particular, the existence of such R (similarly C) implies that there are n number of horizontal (similarly vertical) curves F in $X \times Y$, such that every intersection point of $E \cap F$ appears as an intersection point of $N \cap F$ with at least the same multiplicity. Now, the condition on tensor codewords that E divides N also translates in terms of associated divisors. We have $E|N$ iff the corresponding divisors $E, N \subseteq X \times Y$ satisfy the condition that the divisor $N - E$ is an *effective* divisor, i.e. all the coefficients of curves appearing in $N - E$ are non-negative integers. With this geometric interpretation, we carry out the analogues of the steps in bivariate divisibility. However, these steps are more involved due to novel geometric challenges in this generalized framework.

Reduction to no common components. In this geometric framework the analogue of gcd is the notion common part of the divisors E, N. In particular, the common part is the divisor B which includes all the curves common to E, N with the coefficient taken to be smaller of the coeffcients appearing in E, N. Therefore, we would like to replace E, N by $E - B, N - B$ to assume they do not have common components. However, this seemingly harmless step already presents us with a technical obstacle that was not present for plane algebraic curves. The curves X, Y are of arbitrary genera, therefore the geometry of the product surface $X \times Y$ is intrinsically different from that of $\mathbb{F}_q \times \mathbb{F}_q$. In particular, the intersection theoretic properties of B are not determined by its bi-degree, due to the presence of new type of curves on $X \times Y$. Moreover, these new divisors $E - B, N - B$ are not necessarily from a subclass $\mathcal{L}_{d,e}$ corresponding to tensor codewords. However, using intersection theory on surfaces, we show that we can still effectively control the behaviour of these new divisors and we can indeed reduce to the case of E, N having no common components.

Lower bound on local intersection multiplicities. In order to obtain a lower bound on the local intersection multiplicities at the points of $E \cap N$, we utilize the non-singularity of the horizontal and vertical curves in $X \times Y$. In Lemma 4.12, we note a generalization of the lower bound for plane curves that were used in bivariate divisibility. In Lemma 5.2, we show that these local contributions add up to a global lower bound on the size of $E \cap N$ counted with multiplicities.

Global upper bound on intersection. For bivariate divisibility, the upper bound due to Bezout's theorem was provided by the intersection product $E \cdot N$ on the surface $\mathbb{P}^2$. Although Bezout's theorem does not apply directly on $X \times Y$, we still have a notion of intersection product and other tools from intersection theory. In particular, E, N are divisors corresponding to tensor codewords (i.e. they belong the corresponding classes $E \in \mathcal{L}_{a,b}, N \in \mathcal{L}_{a+d,b+d}$), then we can still compute their intersection number $E \cdot N$ in terms of a, b, d. However, we replaced E, N by $E - B, N - B$ in step 1, and these new divisors no longer belong to such subclasses of the form $\mathcal{L}_{r,s}$. Therefore, we can not explicitly compute the intersection product $E \cdot N$ just in terms of a, b, d. However, we show that we can still estimate this intersection product to provide an upper bound which is sufficient.

Given these steps above, we show that if $N - E$ was not an effective divisor, then the bounds contradict each other. Once we have established that $N - E$ is an effective divisor, we can use our correspondence to produce a tensor codeword Q. Moreover, our construction guarantees that Q is indeed defined over $\mathbb{F}_q$ and we get our desired divisibility result (see Section 5). Given our generalized divisibility lemma in Lemma 5.3, the main results on robust testability and the application to quantum codes follow by adapting standard arguments. We refer to Section 6 for details.

1.5 Related work

The work of [GSW24], defined an abstract generalization of AG codes based on basic properties of AG codes. These *abstract AG codes* are, by definition, linear codes that satisfy distance and dimension lower bounds similar to AG codes and are also required to satisfy the multiplication property. These codes are parameterized by their length n and dimension k and another parameter called genus g. [GSW24] proved that tensor products of abstract AG codes of length n are robustly testable provided $n = \Omega((k+g)^2)$. These abstract AG codes are not required to come from algebraic curves and provide a possibly larger class of codes. AG codes have an underlying geometry that is unavailable in the setting of abstract AG codes, hence the techniques of [GSW24] are completely linear algebraic. We use this underlying algebraic geometry of algebraic curves to establish robust testability for AG codes. Moreover, in the case of AG codes, our result improves upon theirs, as we establish robust testability for constant rate AG codes.

In [KKS24], a version of bivariate divisibility was proved, which deals with lines in general position instead of axis-parallel lines, and their work also proves a multivariate polynomial version of divisibility. Their proof also uses Bezout's theorem and intersection multiplicity and it is similar to the proof of bivariate divisibility provided in our Section 3. Their work involves only plane algebraic curves and polynomial functions. On the other hand, our main contribution on divisibility is in the setting of AG codes. Hence we employ more advanced algebraic-geometric techniques and work in a more general setting of rational functions on non-planar algebraic curves.

1.6 Organization

In Section 2, we discuss the necessary background on AG codes and the relevant algebraic-geometric notions. In Section 3, we illustrate our geometric perspective by proving a version of bivariate divisibility. In Section 4, we establish the correspondence between tensor AG codewords and divisors on surfaces. In Section 5 prove our generalized bivariate divisibility lemma. Finally, in Section 6, we prove robust local testability of AG codes and provide an application to quantum codes.

Acknowledgements

We would like to thank Madhu Sudan for his interest and helpful conversations. We are thankful to anonymous referees for useful comments on a previous draft.

2 Preliminaries

In this section we setup our notations and basic definitions regarding linear codes, AG codes and quantum codes. We will also discuss basic properties of AG codes and show the existence of error correcting tensor AG codewords, which will be useful for proving our main result.

2.1 Notations and conventions

Throughout $\mathbb{F}_q$ will denote a finite field of cardinality q, where q is a power of a prime p. For any field $\mathbb{K}$, we denote an algebraic closure by $\overline{\mathbb{K}}$. For any field $\mathbb{K}$ we denote the n-dimensional affine space as $\mathbb{A}^n_{\mathbb{K}}$. Similarly, we let $\mathbb{P}^n_{\mathbb{K}}$ be the projective space. Let $[n] := \{1, \cdots, n\}$ for any positive integer n. We will often identify

the vector space $\mathbb{F}_q^n$ with the space of functions $\{f : [n] \to \mathbb{F}\}$. For functions $f : [m] \to \mathbb{F}_q$ and $g : [n] \to \mathbb{F}_q$, we define $f \otimes g : [m] \times [n] \to \mathbb{F}_q$ as $(f \otimes g)(x, y) = f(x)g(y)$.

2.2 Linear codes.

A code of block length n over an alphabet Σ is a subset of Σ^n. A subset $C \subseteq \mathbb{F}_q^n$ is called a linear code if C is a vector subspace (or a $\mathbb{F}_q$-linear subspace) of $\mathbb{F}_q^n$. All codes considered in this paper will be linear codes defined over finite fields.

Distances. Let S be a finite set. For $f, g : S \to \mathbb{F}_q$ we use $\mathrm{dist}(f, g)$ to denote the absolute (non-normalized) Hamming distance between f and g, i.e., $\mathrm{dist}(f, g) = |\{x \in S \mid f(x) \neq g(x)\}|$. We define the normalized Hamming distance as

$$\delta(f, g) = \frac{1}{|S|}\mathrm{dist}(f, g)$$

For a vector $f \in \mathbb{F}_q^n$ and code $C \subseteq \mathbb{F}_q^n$, we use $\delta(f, C)$ to denote the distance of f to the nearest codeword in C, i.e. $\delta(f, C) = \min\{\delta(f, g) \mid g \in C\}$.

Hamming weight. For $x \in \mathbb{F}_q^n$, we define the Hamming weight of f as $|x| = \#\{i \in [n] \mid x_i \neq 0\}$, i.e. the number of non-zero entries of x. We will simply refer to $|x|$ as the weight of x.

Dual code. Given a code $C \subseteq \mathbb{F}_q^n$, the dual code of C, denoted $C^\perp$ is given by

$$C^\perp = \{x \in \mathbb{F}_q \mid x \cdot y = 0 \text{ for all } y \in C\}$$

where $x \cdot y = \sum_{i=1}^n x_i y_i$.

Parity check matrices. Given a code $C \subseteq \mathbb{F}_q^n$ with $\dim(C) = m$, a parity check matrix for C is a matrix $M \in \mathbb{F}_q^{n-m \times n}$ such that $C = \ker(M) \subseteq \mathbb{F}_q^n$. In other words, M is a generator matrix for the dual code $C^\perp$.

Hadamard product. For two codes $C_1, C_2 \subset \mathbb{F}_q^n$, the Hadamard product is defined as $C_1 \star C_2 = \{fg \mid f \in C_1, g \in C_2\}$. In other words, it is the space of component-wise products of codewords, i.e. we have $C_1 \star C_2 = \{(x_1 y_1, \cdots, x_n y_n) \mid x \in C_1, y \in C_2\}$.

Base change. Given a linear code $C \subseteq \mathbb{F}_q^n$, we define $\overline{C} \subseteq \overline{\mathbb{F}_q^n}$, to be the linear subspace given by $\overline{C} := C \otimes_{\mathbb{F}_q} \overline{\mathbb{F}_q}$, where $\otimes_{\mathbb{F}_q}$ is the tensor product operation on $\mathbb{F}_q$-vector spaces. We note that if $v_1, \cdots, v_r$ is a basis of C, then $v_1 \otimes 1, \cdots, v_r \otimes 1$ is a basis of $\overline{C}$ as a $\overline{\mathbb{F}}_q$-vector space. In particular, $\dim_{\mathbb{F}_q}(C) = \dim_{\overline{\mathbb{F}_q}}(\overline{C})$. We will often refer to $\overline{C}$ as the base change of C.

2.3 Algebraic curves, divisors and Riemann-Roch spaces

In this subsection, we recall the necessary geometric background for defining Algebraic Geometry codes. For the definitions of algebraic varieties, their function fields and morphisms of varieties we refer to the standard sources [Ful08, Sha13, Har77, Ste12]. For the commutative algebraic background we refer to [AM69, Eis13].

A curve will be an algebraic variety of dimension 1. Given an algebraic variety X defined over a field $\mathbb{K}$, we denote its function field by $\mathbb{K}(X)$. In the special case, when X is the zero set of an irreducible polynomial $F \in \mathbb{K}[x, y]$ over an algebraically closed field, we know that the function field $\mathbb{K}(X)$ is the field of fractions of the integral domain $\mathbb{K}[x, y]/(F)$. We will say that a variety X defined over a perfect field (such as an algebraically closed field or a finite field) is non-singular or smooth iff the local ring $\mathcal{O}_{X,P}$ is a regular local ring. If X is an algebraic curve, the condition of regular local ring is equivalent to $\mathcal{O}_{X,P}$ being a discrete valuation ring [Ste12, Theorem 4.9].

Divisors on curves. Let X be a non-singular algebraic curve over an algebraically closed field $\mathbb{K}$. A divisor D on X is a *finite* formal linear combination $\sum_P a_P P$, where $P \in X$ and $a_P \in \mathbb{Z}$ for all P. The finite set $\{P \in X \mid a_P \neq 0\}$ is called the support of D, denoted as $\mathrm{Supp}(D)$. We say that D is effective if $a_P \geq 0$ for all P and we write $D \geq 0$. The degree of a divisor $D = \sum_P a_P P$ is defined as $\deg(D) = \sum_P a_P$. The set of all divisors on X forms a group $\mathrm{Div}(X)$ [Ste12, Section 4.3]. Moreover, every point $P \in X$ defines a discrete valuation $\nu_P : \mathbb{K}(X) \to \mathbb{Z}$, with the associated discrete valuation ring $\mathcal{O}_{X,P}$. For any non-zero rational function $f \in \mathbb{K}(X)$, we define the divisor of f as $\mathrm{div}(f) = \sum_P \nu_P(f) P$. If $\nu_P(f) > 0$, we say that

P is a zero of f. Similarly, if $\nu_P(f) < 0$, we say that P is a pole of the rational function f. Two divisors D_1, D_2 are called linearly equivalent and we write $D_1 \sim D_2$ iff $D_1 - D_2 = \mathrm{div}(f)$ for some rational function.

Riemann-Roch space. For any divisor $D \in \mathrm{Div}(X)$, we define the corresponding linear system or the Riemann-Roch space as

$$\mathcal{L}(X, D) = \{f \mid \mathrm{div}(f) + D \geq 0\}$$

We know that $\mathcal{L}(X, D)$ is a finite dimensional vector space over $\mathbb{K}$ [Ste12, Section 4.3]. To every algebraic curve there is a canonically determined non-negative integer g, which is called the genus of g. We refer to [Ful08, Chapter 8] or [Har77, Section 2.8, Chapter IV] for detailed discussions on genus and its properties. One key property of the genus is given by the celebrated Riemann-Roch theorem (see [Sti09, Section 1.5], [Ste12, Theorem 4.27]), which will be very useful for us.

Curves over finite fields. We now discuss the analogues of the above concepts in the setting when $\mathbb{K} = \mathbb{F}_q$. A curve defined over $\mathbb{F}_q$ is called *absolutely irreducible* if it is an irreducible curve when considered over the algebraic closure $\overline{\mathbb{F}_q}$. In other words, the base change $\overline{X} := X \otimes_{\mathbb{F}_q} \overline{\mathbb{F}_q}$ is irreducible over $\overline{\mathbb{F}_q}$ [Ste12, Chapter 5]. The algebraic variety $\overline{X}$ can be thought of as the zero set of the same polynomials that define X, however we allow solutions with coordinates in $\overline{\mathbb{F}_q}$. Throughout this paper, we will alternatively use *geometrically irreducible* in place of absolutely irreducible. These two notions are equivalent (see [Sta24, Tag 0364]). We will say that a curve X over $\mathbb{F}_q$ is non-singular if it is non-singular over the algebraic closure, i.e. $\overline{X}$ is non-singular. Since we will always work with projective algebraic curves, we may assume that our curve $\overline{X}$ is contained in a projective space $\mathbb{P}^m_{\overline{\mathbb{F}_q}}$ for some m.

Given a point $(a_1, \cdots, a_n) \in \overline{\mathbb{F}_q}^n$, we will say that it is a $\mathbb{F}_q$-rational point iff $a_1, \cdots, a_n \in \mathbb{F}_q$. For the projective variety $\overline{X} \subseteq \mathbb{P}^n_{\overline{\mathbb{F}_q}}$, the notion of $\mathbb{F}_q$-rational points is defined as follows. A point $P = [a_0 : \cdots : a_n] \in \overline{X}$ is called an $\mathbb{F}_q$-rational point if $a_i \neq 0$ implies that $a_j/a_i \in \mathbb{F}_q$ for all j. Let $\sigma : \mathbb{P}^n_{\overline{\mathbb{F}_q}} \to \mathbb{P}^n_{\overline{\mathbb{F}_q}}$ be the Frobenius morphism given by $\sigma([x_0 : \cdots : x_n]) = [x_0^q : \cdots : x_n^q]$. Note that σ fixes the $\mathbb{F}_q$-rational points.

Let X be a non-singular projective algebraic curve over $\mathbb{F}_q$. We will denote the set of $\mathbb{F}_q$-rational points as $X(\mathbb{F}_q)$. We say that a divisor $D = \sum_P a_P P \in \mathrm{Div}(\overline{X})$ is a $\mathbb{F}_q$-rational divisor on X if $\sigma(D) = \sum_P a_P \sigma(P)$ [Ste12, Chapter 5, page 106]. Given X defined over $\mathbb{F}_q$, we may consider its function field over both $\mathbb{F}_q$ and $\overline{\mathbb{F}_q}$. We know that these two are related by by base change, in particular $\overline{\mathbb{F}_q}(X) = \mathbb{F}_q(X) \otimes_{\mathbb{F}_q} \overline{\mathbb{F}_q}$, where the tensor product operation is as $\mathbb{F}_q$-vector spaces. Moreover, we have an inclusion $\mathbb{F}_q(X) \subseteq \overline{\mathbb{F}_q}(X)$. For a $\mathbb{F}_q$-rational divisor D on X, we define the Riemann-Roch space over $\mathbb{F}_q$ as

$$\mathcal{L}_{\mathbb{F}_q}(X, D) = \mathcal{L}(X, D) \cap \mathbb{F}_q(X),$$

where the intersection is computed as subsets of $\overline{\mathbb{F}_q}(X)$. A consequence of the Riemann-Roch theorem is the following lower bound [6].

Theorem 2.1. *Let X be a geometrically irreducible non-singular projective algebraic curve of genus g over $\mathbb{F}_q$. Let D be $\mathbb{F}_q$-rational divisor on X. Then we have*

$$\dim(\mathcal{L}_{\mathbb{F}_q}(X, D)) \geq \deg(D) - g + 1.$$

2.4 Algebraic Geometry codes

In this section, we recall the definition of Algebraic-Geometry codes and their basic properties. We will use the geometric definition as defined in [Ste12, CR21]. For equivalent algebraic versions of the definitions we refer to [Gur04, Chapter 6] and [Sti09, Chapter 2].

Definition 2.2. [Ste12, Section 10.1] Let X be a geometrically irreducible non-singular projective algebraic curve over $\mathbb{F}_q$. Let $x_1, \cdots, x_n$ be distinct $\mathbb{F}_q$-rational points on X. Let $D = x_1 + \cdots + x_n$, as a $\mathbb{F}_q$-rational

[6] In fact, the Riemann-Roch theorem establishes an equality where the difference between $\dim(\mathcal{L}_{\mathbb{F}_q}(X, D))$ and $\deg(D) - g + 1$ is captured by $\dim(\mathcal{L}_{\mathbb{F}_q}(X, K - D))$, with K being a *canonical divisor* on X.

divisor on the curve X. Let H be a $\mathbb{F}_q$-rational divisor on X such that $\deg(H) \geq 0$ and $\mathrm{Supp}(D) \cap \mathrm{Supp}(H) = \emptyset$. We define the Algebraic Geometry code (AG code, also called geometric Goppa code) denoted $C_{\mathcal{L}}(X, D, H)$ as

$$C_{\mathcal{L}}(X, D, H) = \{(f(x_1), \cdots, f(x_n)) \mid f \in \mathcal{L}_{\mathbb{F}_q}(X, H)\} \subseteq \mathbb{F}_q^n.$$

Note that the only possible poles of f must be contained in $\mathrm{Supp}(H)$. Since $x_i \notin \mathrm{Supp}(H)$, we know that the evaluations $f(x_i)$ is well-defined. The code $C_{\mathcal{L}}(X, D, H)$ is a linear code of length n over $\mathbb{F}_q$.

AG codes have additional parameters such as the genus of the underlying curve X and the degree of the divisor H which govern the properties of the code. We define these associated notions below.

Genus of AG code. We define the genus of the code $C_{\mathcal{L}}(X, D, H)$ to be the genus of the curve X.

Degree of AG code. We define the degree of the AG code $C_{\mathcal{L}}(X, D, H)$ to be the degree of its defining divisor H, i.e. $\deg(C_{\mathcal{L}}(X, D, H)) := \deg(H)$. In particular, if the genus of X is g and $\deg(H) = \ell$, then we will say that $C_{\mathcal{L}}(X, D, H)$ is an AG code of genus g, length n and degree ℓ.

It is often customary to work with algebraic definitions of AG codes using the language of function fields as in [Gur04, Chapter 6] and [Sti09, Chapter 2]. These algebraic definitions are equivalent to the geometric definition above due to the equivalence between curves and function fields (see [CR21, Section 2.1]). Let us elaborate on this equivalence of geometric and algebraic definitions of AG codes.

Remark 2.3. Given an irreducible and reduced algebraic curve X over $\mathbb{F}_q$, its function field $\mathbb{F}_q(X)$ is a finitely generated extension of $\mathbb{F}_q$ which is of transcendence degree 1. In particular, $\mathbb{F}_q(X)$ is an algebraic function field of one variable over $\mathbb{F}_q$ [Sti09, Definition 1.1.1]. On the other hand, given an algebraic function field K over $\mathbb{F}_q$, there exists an irreducible, non-singular, projective curve X over $\mathbb{F}_q$ such that $\mathbb{F}_q(X) \simeq K$ (see [Poo06, Section 2.1] and [Poo08, Proposition 2.2.13]). More precisely, by [Sta24, Tag 0BY1] (or [Poo06, Section 2.1]), there is an equivalence of categories between

- the category of finitely generated field extension $K/\mathbb{F}_q$ of transcendence degree 1, and
- the category of irreducible, non-singular, projective curves and non-constanct morphisms.

For an irreducible, non-singular, projective algebraic curve X over $\mathbb{F}_q$, we know that X is geometrically irreducible iff the function field $\mathbb{F}_q(X)$ is geometrically irreducible over $\mathbb{F}_q$ [Sta24, Tag 054Q]. By [Sta24, Tag 0G33], $\mathbb{F}_q(X)$ is geometrically irreducible over $\mathbb{F}_q$ iff every element $\alpha \in \mathbb{F}_q(X)$ that is separably algebraic over $\mathbb{F}_q$ is in $\mathbb{F}_q$. Since an algebraic extension of $\mathbb{F}_q$ is separable, we conclude that X is geometrically irreducible over $\mathbb{F}_q$ iff the field $\mathbb{F}_q$ is algebraically closed in $\mathbb{F}_q(X)$. Therefore, we have a one-to-one correspondence (up to isomorphisms) between algebraic function fields $K/\mathbb{F}_q$ of one variable with a full constant field, and geometrically irreducible non-singular projective algebraic curves over $\mathbb{F}_q$. Moreover, under this correspondence, the divisors on the curve X correspond to places of the algebraic function field, and other algebraic notions such as genus of the function field and Riemann-Roch spaces also coincide with their geometric counterparts [Sti09, Appendix B]. Moreover, since [Sti09] works with algebraic function fields with a full constant field ([Sti09, Section 1.4]), we conclude that the algebraic definition of AG codes provided in [Sti09, Defintion 2.2.1] is equivalent to the geometric definition of [Ste12] used here.

The following result is well-known. We include a proof here for completeness.

Proposition 2.4. *Let X be a geometrically irreducible non-singular projective algebraic curve over $\mathbb{F}_q$. Let g be the genus of X. Let $x_1, \cdots, x_n \in X$ be $\mathbb{F}_q$-rational points and $D = \sum_i x_i$. Let $H \in \mathrm{Div}(X)$ be a $\mathbb{F}_q$-rational divisor with $\deg(H) \geq 0$ and $\mathrm{Supp}(D) \cap \mathrm{Supp}(H) = \emptyset$. Let $C_{\mathcal{L}}(X, D, H)$ be the corresponding AG code. Then we have*

1. $\dim(C_{\mathcal{L}}(X, D, H))) \geq \deg(H) - g$. *Moreover, if* $2g - 2 < \deg(H) < n$, *then* $\dim(C_{\mathcal{L}}(X, D, H)) = \deg(H) + 1 - g$
2. $\mathrm{dist}(C_{\mathcal{L}}(X, D, H)) \geq n - \deg(H)$.

3. *For any be a $\mathbb{F}_q$-rational divisor G with $\deg(G) \geq 0$ and $\mathrm{Supp}(D) \cap \mathrm{Supp}(G) = \emptyset$, we have that $C_{\mathcal{L}}(X, D, H) \star C_{\mathcal{L}}(X, D, G) \subseteq C_{\mathcal{L}}(X, D, H + G)$.*

4. *The dual code $(C_{\mathcal{L}}(X, D, G)^{\perp}$ is also an AG code given by $C_{\mathcal{L}}(X, D, H)$ where $\deg(H) = 2g - 2 + n - \deg(G)$.*

Proof. Let $\deg(H) = \ell$ and $\deg(G) = m$. (1) If $\ell < n$, then part (1) follows from [Ste12, Corollary 10.2]. So we prove it in the case when $\ell = n$.

Consider the $\mathbb{F}_q$-linear map $\varphi : \mathcal{L}_{\mathbb{F}_q}(X, H) \to \mathbb{F}_q^n$ defined by $f \mapsto (f(x_1), \cdots, f(x_n))$. If $f \in \ker(\varphi)$, then f has zeros at $x_1, \cdots, x_n$. In particular, $f \in \mathcal{L}_{\mathbb{F}_q}(X, H - (x_1 + \cdots + x_n))$. Note that $\deg(H - (x_1 + \cdots + x_n)) = 0$. If $f \neq 0$, then we must have that $H - (x_1 + \cdots + x_n) \sim 0$. Therefore we have that $\dim(\mathcal{L}_{\mathbb{F}_q}(X, H - (x_1 + \cdots + x_n))) = 1$. By the Riemann-Roch theorem, we have $\dim(\mathcal{L}_{\mathbb{F}_q}(X, H)) \geq \ell - g + 1$. Therefore, $\dim(\mathcal{C}(\ell)) \geq \dim(\mathcal{L}_{\mathbb{F}_q}(X, H)) - \dim(\ker(\varphi)) \geq \ell - g$.

(2) This part follows from [Ste12, Theorem 10.1].

(3) We know that if $f \in \mathcal{L}_{\mathbb{F}_q}(X, H)$ and $g \in \mathcal{L}_{\mathbb{F}_q}(X, G)$, then $fg \in \mathcal{L}_{\mathbb{F}_q}(X, H+G)$. Therefore, by definition of the Hadamard product, we have $C_{\mathcal{L}}(X, D, H) \star C_{\mathcal{L}}(X, D, G) \subseteq \mathcal{C}(X, D, H + G)$.

(4) Follows from [CR21, Theorem 12, Lemma 19].

□

Example 2.5. *Fix a finite field $\mathbb{F}_q$. Let $N_q(g)$ denote the maximum number of $\mathbb{F}_q$-rational points on a geometrically irreducible non-singular projective algebraic curve over $\mathbb{F}_q$ of genus g. The Ihara constant of $\mathbb{F}_q$ is defined as*

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

By [Iha81, TVZ82, VD83] we know that $A(q) = \sqrt{q} - 1$ if q is a square. Hence, for all $\gamma > 0$ sufficiently small, there exists a sequence of geometrically irreducible non-singular projective algebraic curves $\{X_i \mid i \in \mathbb{N}\}$ over $\mathbb{F}_q$ such that

$$\lim_{i \to \infty} \frac{|X_i(\mathbb{F}_q)|}{g(X_i)} = \sqrt{q} - 1 - \gamma.$$

For each X_i, we may choose a $\mathbb{F}_q$-rational point $p_i \in X_i$ and let $x_1, \cdots, x_{n_i}$ be the rest of the $\mathbb{F}_q$-rational points on X_i. Let $g_i := g(X_i)$ denote the genus. Note that $(\sqrt{q} - 2)g_i \leq n_i + 1 \leq \sqrt{q} g_i$ for sufficiently large i.

(1) For $q \geq 16$, we have $2g_i - 1 < n_i$. Let ℓ_i be a positive integer such that $2g_i - 2 < \ell_i < n_i$. Let $H_i = \ell_i p_i$, and $D_i = x_1 + \cdots + x_{n_i}$. Consider the AG codes $\mathcal{C}_i = \mathcal{C}_{\mathcal{L}}(X_i, D_i, H_i)$. Then we have a sequence of AG codes $\mathcal{C}_i$ of length n_i and genus g_i such that $n_i = \Theta(g_i)$ as $i \to \infty$. Moreover the rate of the code $\mathcal{C}_i$ is given by

$$R_i = \frac{\ell_i - g_i + 1}{n_i}$$

and the relative distance satisfies

$$\delta_i = \frac{n_i - \ell_i}{n_i}.$$

(2) Let $q \geq 144$. Let us fix a constant α such that $3 < \alpha < \frac{1}{2}(\sqrt{q} - 5)$, and let $\ell_i = \alpha g_i$ in the construction above. Then $\mathcal{C}_i$ are codes that have rates lower bounded by a positive constant and have linear dual-distance. Indeed, we have

$$R_i > \frac{(\alpha - 1)}{\sqrt{q}},$$

and the distance of the dual code satisfies

$$\mathrm{dist}(\mathcal{C}_i^{\perp}) \geq n_i - (2g_i - 2 + n_i - \ell_i) = \ell_i - 2g_i + 2 = \Theta(n_i).$$

Now let $\epsilon \in (0, 1)$ be such that $(1 - \epsilon) > \frac{2(1+\alpha)}{\sqrt{q} - 3}$. Then we have $4 + 2g_i + 2\ell_i < (1 - \epsilon)n_i$ for i sufficiently large. Hence the tensor code $\mathcal{C}_i \otimes \mathcal{C}_i$ satisfies the assumptions of Theorem 1.2.

2.5 Tensor codes and Robustness

We start by recalling the basics of tensor product of codes and the notion of robust local testability.

Let $C_1 \subseteq \mathbb{F}_q^m$ and $C_2 \subseteq \mathbb{F}_q^n$ be two codes. We define their tensor product as

$$C_1 \otimes C_2 = \text{span}(\{v \otimes w \mid f \in C_1, g \in C_2\}).$$

Note that $C_1 \otimes C_2 \subseteq \mathbb{F}_q^{mn}$ is a linear code. If we think of codewords $v \in C_1$ and $w \in C_2$ as row vectors, then we have a matrix given by the Kronecker product $v \otimes w^T$, where w^T denotes the transpose of w. Therefore, we may alternatively identify codewords of $C_1 \otimes C_2$ as matrices with the following property. A matrix M is a codeword of $C_1 \otimes C_2$ iff every row of M is a codeword of C_1 and every column of M is a codeword of C_2.

Let us recall the definition of robust testability of tensor codes.

Definition 1.1. [Robust testability of tensor product] Let $0 \leq \rho \leq 1$. For codes $\mathcal{C}_1 \subseteq \mathbb{F}_q^m$ and $\mathcal{C}_2 \subseteq \mathbb{F}_q^n$, we say that $(\mathcal{C}_1, \mathcal{C}_2)$ is ρ-robust, or equivalently $\mathcal{C}_1 \otimes \mathcal{C}_2$ is ρ-robustly testable, if for every $F \in \mathbb{F}_q^{n \times m}$, we have

$$\rho \cdot \delta(F, \mathcal{C}_1 \otimes \mathcal{C}_2) \leq \frac{1}{2}[\delta(F, \mathcal{C}_1 \otimes \mathbb{F}_q^n) + \delta(F, \mathbb{F}_q^m \otimes \mathcal{C}_2)]$$

Given two codewords $R \in C_1 \otimes \mathbb{F}_q^n$ and $C \in \mathbb{F}_q^m \otimes C_2$, we show that there exists a low-degree "error-correcting" tensor codeword E which is zero at the entries where R and C disagree. Finding such an error-correcting polynomial in now a standard technique, which was employed in [Sud92], and it served as the first step in [PS94]. The following result is a generalization in the setting of AG codes.

Lemma 2.6 (Error correcting tensor codeword)**.** *Fix $0 \leq \epsilon \leq 1$. Let $\mathcal{C}_1 = C_{\mathcal{L}}(X, D_1, G_1), \mathcal{C}_2 = C_{\mathcal{L}}(Y, D_2, G_2)$ be two AG codes of length n and genus g_1, g_2 respectively. Let $R \in \mathcal{C}_1 \otimes \mathbb{F}_q^n$ and $C \in \mathbb{F}_q^n \otimes \mathcal{C}_2$ be such that $\delta(R, C) = \epsilon^2$. Let $T = \{(x, y) \in [n] \times [n] \mid R(x, y) \neq C(x, y)\}$. For $i \in [2]$, let $d_i \geq \epsilon n + g_i + 1$ be two integers. Let H_1, H_2 be $\mathbb{F}_q$-rational divisors of degree d_1, d_2 on X, Y respectively, such that $\text{Supp}(H_i) \cap \text{Supp}(D_i) = \emptyset$. Then the following holds.*

1. *There exists a non-zero tensor codeword $E \in C_{\mathcal{L}}(X, D_1, H_1) \otimes C_{\mathcal{L}}(Y, D_2, H_2)$ such that $E(x, y) = 0$ for all $(x, y) \in T$.*
2. *There exists a non-zero codeword $N \in C_{\mathcal{L}}(X, D_1, G_1 + H_1) \otimes C_{\mathcal{L}}(Y, D_2, G_2 + H_2)$ such that*

$$E(x_i, y_j)R(x_i, y_j) = E(x_i, y_j)C(x_i, y_j) = N(x_i, y_j)$$

for all $(i, j) \in [n] \times [n]$, where $D_1 = x_1 + \cdots + x_n$ and $D_2 = y_1 + \cdots + y_n$.

Proof. (1) Since $\delta(R, C) = \epsilon^2$, we have that $\text{dist}(R, C) = \epsilon^2 n^2$. Therefore $|T| = \epsilon^2 n^2$, and let $T = \{t_1, \cdots, t_m\} \subseteq [n] \times [n]$ where $m := \epsilon^2 n^2$. Consider the linear map $\varphi : C_{\mathcal{L}}(X, D_1, H_1) \otimes C_{\mathcal{L}}(Y, D_2, H_2) \to \mathbb{F}_q^m$ defined as $E \mapsto (E(t_1), \cdots, E(t_m))$. Here $E(t_i)$ is the t_i-th entry of the $n \times n$-matrix E. Note that $\dim(C_{\mathcal{L}}(X, D_1, H_1)) \geq d_1 - g_1$ and $\dim(C_{\mathcal{L}}(Y, D_2, H_2)) \geq d_2 - g_2$ by Proposition 2.4. Hence $\dim(C_{\mathcal{L}}(X, D_1, H_1) \otimes C_{\mathcal{L}}(Y, D_2, H_2)) \geq (d_1 - g_1)(d_2 - g_2)$. Since $d_i \geq \epsilon n + g_i + 1$, we have that $(d_1 - g_1)(d_2 - g_2) > \epsilon^2 n^2 = m$. Therefore, $\ker(\varphi) \neq (0)$ and we may choose E to be any non-zero element in $\ker(\varphi)$.

(2) Let $E \in C_{\mathcal{L}}(X, D_1, H_1) \otimes C_{\mathcal{L}}(Y, D_2, H_2)$ be given by part (1) above. Then we have

$$E(x_i, y_j)R(x_i, y_j) = E(x_i, y_j)C(x_i, y_j)$$

for all $(i, j) \in [n] \times [n]$. We define $N(x_i, y_j) := E(x_i, y_j)R(x_i, y_j)$ for all $(i, j) \in [n] \times [n]$. Let N be the matrix defined as $N_{ij} = N(x_i, y_j)$. Let $N_i = (N(x_i, y_1), \cdots, N(x_i, y_n))$ denote i-th row of the matrix N. Then we have that

$$N_i = (E(x_i, y_1)R(x_i, y_1), \cdots, E(x_i, y_n)R(x_i, y_n)),$$

i.e. the component-wise product of the i-th rows of E and R. Since $E \in C_{\mathcal{L}}(X, D_1, H_1) \otimes C_{\mathcal{L}}(Y, D_2, H_2)$, we know that every row of E is in $C_{\mathcal{L}}(X, D_1, H_1)$ and every column of E is in $C_{\mathcal{L}}(Y, D_2, H_2)$. Now

$R \in C_{\mathcal{L}}(X, D_1, G_1) \otimes \mathbb{F}_q^n$. Hence every row of R is in $C_{\mathcal{L}}(X, D_1, G_1)$. Therefore, every row of N is in $C_{\mathcal{L}}(X, D_1, G_1 + H_1)$. Note that we also have $N(x_i, y_j) = E(x_i, y_j)C(x_i, y_j)$ for all $(i, j) \in [n] \times [n]$. Thus, similarly we have that every column of N is in $C_{\mathcal{L}}(Y, D_2, G_2 + H_2)$, as every column of C is in $C_{\mathcal{L}}(Y, D_2, H_2)$. Therefore, we have that $N \in C_{\mathcal{L}}(X, D_1, G_1 + H_1) \otimes C_{\mathcal{L}}(Y, D_2, G_2 + H_2)$.

Moreover, we have that $N \neq 0$. Indeed, since $E \neq 0$, we know that there exists $(a, b) \notin T$ such that $E(a, b) \neq 0$. As $(a, b) \notin T$, we have $R(a, b) \neq C(a, b)$. Therefore, we can not have that $R(a, b) = 0$ and $C(a, b) = 0$. Without loss of generality we may assume that $R(a, b) \neq 0$. Then we have $N(a, b) = R(a, b)E(a, b) \neq 0$. □

2.6 Quantum codes

In this section, we recall the necessary background on quantum codes and homological products. We will follow the exposition in [BH14, GG24]. We start by defining quantum CSS codes.

Definition 2.7. A quantum CSS code of length n over $\mathbb{F}_q$ is a pair $Q = (Q_X, Q_Z)$ such that

1. $Q_X, Q_Z \subseteq \mathbb{F}_q^n$ are (classical) linear codes,
2. $(Q_X)^\perp \subseteq Q_Z$.

We define the dimension of Q as $k := \dim(Q_Z) - \dim(Q_X^\perp)$ and rate $R := \frac{k}{n}$. Let d_X be the minimum weight of vectors in $Q_X \setminus (Q_Z)^\perp$ and similarly, let d_Z be the minimum weight of vectors in $Q_Z \setminus (Q_X)^\perp$. The distance of Q is defined to be $d := \min\{d_X, d_Z\}$. We will say that Q is a $[[n, k, d]]_q$ code.

qLDPC codes. We will say that a quantum CSS code Q is a quantum Low Density Parity Check (qLDPC) code of locality w if there exist parity check matrices H_X, H_Z for Q_X, Q_Z respectively such that every row and every column of H_X, H_Z have at most w non-zero entries.

qLTC. We will say that a quantum CSS code Q is a quantum Locally Testable Code (qLTC) of soundness ρ if there exist parity check matrices H_X, H_Z of Q_X, Q_Z repectively such that the following condition holds.

1. For every $s \in \mathrm{im}(H_X)$, there exists some $e \in \mathbb{F}_q^n$ with $H_X \cdot e = s$ such that $\frac{|s|}{n - \dim(Q_X)} \geq \rho \frac{|e|}{n}$.
2. For every $s \in \mathrm{im}(H_Z)$, there exists some $e \in \mathbb{F}_q^n$ with $H_Z \cdot e = s$ such that $\frac{|s|}{n - \dim(Q_Z)} \geq \rho \frac{|e|}{n}$.

Asymptotically good codes. A family of quantum codes is asymptotically good if the dimension and distance grow linearly as $n \to \infty$, i.e. it is a family of $[[n, k, d]]_q$ codes where $k = \Theta(n)$ and $d = \Theta(n)$ as $n \to \infty$. Moreover, the family is asymptotically good qLDPC if the locality w is bounded by a constant, i.e. $w = O(1)$ as $n \to \infty$.

Quantum AG codes. We define a quantum AG code to be a quantum CSS code Q where Q_X, Q_Z are Algebraic-Geometry codes as defined in Definition 2.2.

Example 2.8. *(Quantum AG codes.) Let X be a geometrically irreducible projective algebraic curve X over $\mathbb{F}_q$ of genus g. Suppose that X has at least n number of $\mathbb{F}_q$-rational points. Let ℓ be a positive integer such that $2g - 2 < \ell < n$. Fix distinct $\mathbb{F}_q$-rational points $P, P_1, \cdots, P_n \in X$ and let $D = P_1 + \cdots + P_n$ be the corresponding divisor.*

Consider the AG codes $Q_X := C_{\mathcal{L}}(X, D, \ell P)$ and $Q_Z := C_{\mathcal{L}}(X, D, \ell P)$, as defined in Definition 2.2. Suppose that $\frac{n}{2} + g - 1 \leq \ell$. Note that there exist AG codes with this constraint on the parameters. Indeed, for $q \geq 36$, we may take $\ell = \alpha g$, where $\frac{\sqrt{q}}{2} + 1 < \alpha < \sqrt{q} - 2$, in part (1) of Example 2.5.

Then $Q := (Q_X, Q_Z)$ is a quantum AG code of length n and dimension $k = 2\ell - n - 2g + 2$. Indeed, we have $Q_X^\perp = C_{\mathcal{L}}(X, D, (2g - 2 + n - \ell)P) \subseteq C_{\mathcal{L}}(X, D, \ell P) = Q_Z$ as $2g - 2 + n - \ell \leq \ell$. Moreover, $\dim(Q_X) = \dim(Q_Z) = \ell + 1 - g$ and $\dim(Q_X^\perp) = n + g - 1 - \ell$ by Proposition 2.4. Hence the dimension of Q is $k = \dim(Q_Z) - \dim((Q_X)^\perp) = (\ell + 1 - g) - (n - \ell + g - 1) = 2\ell - n + 2 - 2g$. Given X, D, P over $\mathbb{F}_q$, we denote such a quantum code Q as $\mathcal{Q}(X, D, \ell P)$.

We will use these quantum AG codes to construct locally testable codes via the homological product method as done in [GG24]. Homological product of chain complexes is a useful tool for constructing quantum CSS codes with good parameters.

Single-sector chain complex. A single-sector chain complex over $\mathbb{F}_q$ is pair $\mathcal{C} = (C, \partial^C)$ where a $C \subseteq \mathbb{F}_q$ is an $\mathbb{F}_q$-linear subspace and $\partial^C \circ \partial^C = 0$. Given a single sector chain complex $\mathcal{C} = (C, \partial^C)$, we define $B_*(\mathcal{C}) = \mathrm{im}(\partial^C)$ and $Z_*(\mathcal{C}) = \ker(\partial^C)$. Note that $B_*(\mathcal{C}) \subseteq Z_*(\mathcal{C})$ as $\partial^C \circ \partial^C = 0$. Moreover, we define the homology space as the quotient $H_*(\mathcal{C}) = Z_*(\mathcal{C})/B_*(\mathcal{C})$. The co-chain complex of $\mathcal{C}$ is the single sector chain complex $\mathcal{C}^* = (C, (\partial^C)^T)$. We similarly define $B_*(\mathcal{C}^*) = \mathrm{im}((\partial^C)^\perp)$, $Z^*(\mathcal{C}^*) = \ker((\partial^C)^T)$ and $H^*(\mathcal{C}^*) = Z^*(\mathcal{C})/B^*(\mathcal{C})$.

Homological product. Given two single-sector chain complexes $\mathcal{A} = (A, \partial^A)$ and $\mathcal{B} = (B, \partial^B)$ over a field $\mathbb{F}_q$ of characteristic 2. The homological product $\mathcal{C} = \mathcal{A} \otimes \mathcal{B}$ is the single-sector chain complex given by $C = A \otimes B$ and $\partial^C = \partial^A \otimes I_B + I_A \otimes \partial^B$.

We note the following result from [BH14] and [GG24, Lemma 4.2], which shows that there is a correspondence between single-sector chain complexes and quantum CSS codes.

Proposition 2.9. *(1) Let $\mathcal{C} = (C, \partial^C)$ be a single-sector chain complex. Let $Q_X = \ker(\partial^C)^T$, where $(\partial^C)^T$ denote the transpose of ∂^C, and let $Q_Z = \ker \partial^A$. Then $Q := (Q_X, Q_Z)$ is a quantum CSS code.*

(2) Let $Q = (Q_X, Q_Z)$ be a $[[n, k, d]]_q$ quantum CSS code over a field $\mathbb{F}_q$ of characteristic 2 such that $\dim(Q_X) = \dim(Q_Z)$. Let H_X, H_Z be full-rank parity check matrices of Q_X, Q_Z respectively, i.e. $\ker H_X = Q_X$ and $\ker H_Z = Q_Z$. Then $\mathcal{C} = (\mathbb{F}_q^n, H_X^T H_Z)$ is a single-sector chain complex. Moreover, the quantum code associated with $\mathcal{C}$ (given by part (1) above), is Q.

(3) In both the parts above, we have $B_*(\mathcal{C}) = Q_X^\perp$, $Z_*(\mathcal{C}) = Q_Z$ and $\dim(H_*(\mathcal{C})) = \dim(Q_Z) - \dim(Q_X^\perp) = k$. For the associated cochain complex $\mathcal{C}^*$, we have $B^*(\mathcal{C}^*) = Q_Z^\perp$, $Z^*(\mathcal{C}^*) = Q_X$, and the associated quantum code is (Q_Z, Q_X).

3 Bivariate divisibility revisited

In this section we revisit [PS94] with a geometric point of view. We will prove the following version of bivariate divisibility, where we assume a stronger bound on n than in Lemma 1.3.

Lemma 3.1 (Special bivariate divisibility)**.** *Let $E(x, y)$ be a polynomial of degree (b, a) and $N(x, y)$ be a polynomial of degree $(b+d, a+d)$. Suppose there exist distinct $x_1, \cdots, x_n$ such that $E(x_i, y)$ divides $N(x_i, y)$ for $1 \le i \le n$, distinct $y_1, \cdots, y_n$ such that $E(x, y_j)$ divides $N(x, y_j)$ for $1 \le i \le n$. Suppose the following holds.*

1. *We have $n > 2a + 2b + 4d$.*
2. *$E(x, y_j)$ is a polynomial of degree b for all $j \in [n]$ and $E(x_i, y)$ is a polynomial of degree a for all $i \in [n]$.*

Then $E(x, y)$ divides $N(x, y)$.

As discussed in the introduction, we will consider the plane algebraic curves corresponding to the bivariate polynomials E and N, and study the intersection multiplicities of these curves at their intersection points. We will apply Bezout's theorem to obtain a upper bound on the total intersection multiplicity of the curves E and N. On the other hand, using Lemma 3.7, we will show that the divisibility assumptions on the univariate polynomials implies a lower bound on the local intersection multiplicities. We will see that these two bounds will contradict each other if $E(x, y)$ does not divide $N(x, y)$.

Our goal here is to illustrate the geometric perspective on bivariate divisibility and this section can be read independent of the rest of the paper. It is worthwhile to note that the proof of Lemma 3.1 presented here is not a special case of the proof of bivariate divisibility for AG codes (Lemma 5.3). In particular, here we will use Bezout's theorem on $\mathbb{P}^2$ (considered as compactification of $\mathbb{F}_q \times \mathbb{F}_q$) whereas in the proof of Lemma 5.3, the appropriate compactified surface is the product $\mathbb{P}^1 \times \mathbb{P}^1$ (in general $X \times Y$, where X, Y are projective

curves of arbitrary genus). Since the geometry of a product surface $X \times Y$ is much more complicated than $\mathbb{P}^2$, the arguments in this section do not capture the global parts of the proof of Lemma 5.3. However, the proof in this section still captures the intuition for the local phenomena involving intersection multiplicities.

3.1 Plane algebraic curves and intersection multiplicities.

In this subsection, we will recall the basics of plane algebraic curves and Bezout's theorem following [Ful08]. In Lemma 3.7, we will prove our inequality for local intersection multiplicities. We work over an algebraically closed field $\mathbb{K}$ throughout this subsection.

An *affine plane curve* will be an equivalence class of non-constant polynomials in $\mathbb{K}[x, y]$, under the equivalence relation $F \sim G$ iff $F = \lambda G$ for some non-zero scalar $\lambda \in \mathbb{K}$. By abuse of notation we will write F for the equivalence class of a polynomial F. A point P on an algebraic curve F will be a point $P \in \mathbb{A}^2_K$ such that $F(P) = 0$. The point $P = (\alpha, \beta)$ corresponds to a maximal ideal $\mathfrak{m} = (x - \alpha, y - \beta)$ in $\mathbb{K}[x, y]$. We define the local ring of the curve F at P to be the localization $\mathcal{O}_P(F) := (\mathbb{K}[x, y]/(F))_{\mathfrak{m}}$. When F is an irreducible polynomial, the local ring $\mathcal{O}_P(F)$ is the ring of all rational functions defined at P, as in [Ful08, Section 2.4]. A point P on F is a non-singular point iff the local ring $\mathcal{O}_P(F)$ is a discrete valuation ring. We will say that a curve F is non-singular iff all the points of F are non-singular. By [Ful08, Section 3.2, Theorem 1], P is a non-singular point of an irreducible curve F iff P is a simple point of F. Equivalently, P is non-singular iff there is a unique tangent line to F through P. Given two affine curves F, G and a point $P \in \mathbb{A}^2_{\mathbb{K}}$, we define the intersection multiplicity of F, G at P as

$$I(P, F \cap G) = \dim_{\mathbb{K}}((\mathbb{K}[x, y]/(F, G))_{\mathfrak{m}})$$

where $\mathfrak{m}$ is the maximal ideal corresponding to P, and $\mathbb{K}[x, y]/(F, G))_{\mathfrak{m}}$ is the localization of the ring $\mathbb{K}[x, y]/(F, G)$ at the maximal ideal $\mathfrak{m}$. Since the coordinate ring of $\mathbb{A}^2_{\mathbb{K}}$ is $\mathbb{K}[x, y]$, this definition matches with the description of the intersection multiplicity in [Ful08, Section 3.3,Theorem 3].

We refer to [Ful08, Chapters 4, 5] for the projective analogues of the above definitions of local rings and intersection multiplicities. We recall Bezout's theorem for projective plane curves below.

Theorem 3.2 (Bezout's theorem)**.** *[Ful08, Section 5.3] Let F, G be projective plane curves. Assume that F, G have no common components. Then we have*

$$\sum_P I(P, F \cap G) = \deg(F) \deg(G).$$

Remark 3.3. Given affine plane curves F, G, we may construct their homogenizations and obtain projective plane curves of the same degree. If F, G do not have common components then the corresponding projective plane curves will also not have any common components. Therefore, for two affine plane curves in $\mathbb{A}^2$, we have the upper bound provided by Bezout's theorem.

$$\sum_P I(P, F \cap G) \leq \deg(F) \deg(G).$$

In order to obtain our lower bound for proving Lemma 3.1, we need to study local intersection multiplicities a point of intersection of three plane curves. The natural question here is the following.

Question 3.4. *Let F, E, N be plane curves and $P \in F \cap E \cap N$. If the pairs F, E and F, N intersect at P with multiplicity at least m, i.e. $I(P, F \cap E) \geq m$ and $I(P, F \cap N) \geq m$, what can we say about $I(P, E \cap N)$? In particular, is $I(P, E \cap N) \geq m$?*

Example 3.5. *Note that in general we may not have that $I(P, E \cap N) \geq m$. Indeed, consider the plane curves given by the nodal cubic $F = y^2 - x^2(x + 1)$ and lines $E = y - x$, $N = y + x$. Let $P = (0, 0)$. Then the lines E and N are both tangent to F. Using the properties of intersection numbers [Ful08, Section 3.3], we compute that $I(P, F \cap E) = I(P, F \cap N) = 3$. However, $I(P, E \cap N) = 1$ as E, N are both lines.*

Example 3.6. *Let $P = (0,0)$, $F = y$, $E = y - x^2$ and $N = y - x^3$. The parabola E and the line F intersect at P with multiplicity 2, as x^2 has a multplicity 2 root at 0. Thus we have $I(P, F \cap E) = 2$. Similarly, we have $I(P, F \cap N) = 3$. Now, E, N are tangent at P and hence they intersect at P with multiplicity at least 2. In fact, we have $I(P, E \cap N) = 2$.*

Note that the nodal cubic curve F in Example 3.5 is singular at the point P, whereas in Example 3.6 the line F is non-singular. Indeed, this singularity at P is the obstruction towards obtaining the lower bound for the intersection multiplicity of E and N. We prove this in Lemma 3.7 below. In fact, the same proof generalizes to curves on non-singular algebraic surfaces in Lemma 4.12.

Lemma 3.7 (Intersection multiplicity lower bound)**.** *Let F, E, N be affine plane curves and $P \in F \cap E \cap N$. Suppose that P is a non-singular point of F. Then we have*

$$I(P, E \cap N) \geq \min\{I(P, F \cap E), I(P, F \cap N)\}.$$

Proof. Note that we have a surjection of rings $\mathbb{K}[x,y]/(E,N) \to \mathbb{K}[x,y]/(F,E,N)$. Therefore, by localizing with respect to the maximal ideal $\mathfrak{m}$ corresponding to P, we obtain a surjection $(\mathbb{K}[x,y]/(E,N))_{\mathfrak{m}} \to (\mathbb{K}[x,y]/(F,E,N))_{\mathfrak{m}}$. Hence we have that $I(P, E \cap N) = \dim_{\mathbb{K}}((\mathbb{K}[x,y]/(E,N))_{\mathfrak{m}}) \geq \dim_{\mathbb{K}}((\mathbb{K}[x,y]/(F,E,N))_{\mathfrak{m}})$. Therefore, it is enough to show that

$$\dim_{\mathbb{K}}((\mathbb{K}[x,y]/(F,E,N))_{\mathfrak{m}}) \geq \min\{I(P, F \cap E), I(P, F \cap N)\}.$$

Since localization commutes with quotients, we have that $(\mathbb{K}[x,y]/(F,E,N))_{\mathfrak{m}} = \mathcal{O}_P(F)/(E,N)$. As P is a non-singular point of F, we know that $\mathcal{O}_P(F)$ is a discrete valuation ring. Let t be the uniformizing parameter the DVR $\mathcal{O}_P(F)$. If E is 0 in $\mathcal{O}_P(F)$, then we have $I(P, F \cap E) = \infty$. Hence $(\mathbb{K}[x,y]/(F,E,N))_{\mathfrak{m}} = \mathcal{O}_P(F)/(E,N) = \mathcal{O}_P(F)/(N)$ as desired. Similarly, we are done if N is 0 in $\mathcal{O}_P(F)$. Therefore, we may assume that both E, N are non-zero in $\mathcal{O}_P(F)$. As $\mathcal{O}_P(F)$ is a discrete valuation ring, we have that $E = u_1 t^{\mathrm{ord}_P^F(E)}$ and $N = u_2 t^{\mathrm{ord}_P^F(N)}$, where u_1, u_2 are units and ord_P^F denotes the order as in [Ful08, Section 2.3]. By [Ful08, Section 3.3, Property 8], we have that $I(P, F \cap E) = \mathrm{ord}_P^F(E)$ and $I(P, F \cap N) = \mathrm{ord}_P^F(N)$. Without loss of generality, we may assume that $\mathrm{ord}_P^F(E) \leq \mathrm{ord}_P^F(N)$. Then we have $\mathcal{O}_P(F)/(E,N) = \mathcal{O}_P(F)/(E)$, as N is a multiple of E in $\mathcal{O}_P(F)$. Therefore, we have $\dim_{\mathbb{K}}(\mathcal{O}_P(F)/(E,N)) \geq I(P, F \cap E)$, which is the minimum by assumption. □

3.2 Proof of Lemma 3.1.

First, we reduce to the case where N, E do not have any common factors. Let $G(x,y) = \gcd(N,E)$. Suppose that $G(x,y)$ is of degree f in x and degree e in y. Let $N = G(x,y)\widetilde{N}(x,y)$ and $E = G(x,y)\widetilde{E}(x,y)$. It is enough to show that $\widetilde{E}$ divides $\widetilde{N}$. We will check that our assumptions still hold for these polynomials. Since $G(x,y)$ can be identically 0 for at most e values of y, we have that $\widetilde{E}(x,y_j)$ divides $\widetilde{N}(x,y_j)$ for at least $n-e$ number of y_j. Since $\deg(E(x,y_j)) = b$ for all $j \in [n]$, we have that $\deg(\widetilde{E}(x,y_j)) \geq b - f$ whenever $G(x,y_j)$ is not identically 0. In particular, we may assume that $\deg(\widetilde{E}(x,y_j)) = b - f$ for at least $n - 2e$ number of y_j, as the degree of $G(x,y_j)$ can be less than f for at most e number of additional y_j. Similarly, we have that $\widetilde{E}(x_i,y)$ is of degree $(a-e)$ and divides $\widetilde{N}(x_i,y)$ for at least $n - 2f$ number of x_i. Note that we have

$$n - 2e - 2f > 2(a-e) + 2(b-f) + 4d.$$

Therefore, we may replace n by $(n - 2e - 2f)$ and preserve condition (1) and (2) for the polynomials $\widetilde{E}$ and $\widetilde{N}$. Thus we may assume that E, N do not have any common factors. Furthermore we may assume that $\max\{a,b\} \geq 1$, i.e. E is a non-constant polynomial.

Let $\pi_1, \pi_2 : \mathbb{A}^2_{\overline{\mathbb{F}_q}} \to \mathbb{A}^1_{\overline{\mathbb{F}_q}}$ be the projections given by $\pi_1(x,y) = x$ and $\pi_2(x,y) = y$. Let $G_j := \pi_2^{-1}(y_j)$ denote the fiber over y_j. In other words, $G_j \subset \mathbb{A}^2_{\overline{\mathbb{F}_q}}$ is the zero set of the polynomial $(y - y_j)$. By abuse of notation, we continue to denote by $N, E \subset \mathbb{A}^2_{\overline{\mathbb{F}_q}}$ the algebraic curves corresponding to the bivariate

polynomials $N(x,y)$ and $E(x,y)$ respectively. Let H denote the algebraic curve given by the polynomial $H(x,y) := \prod_j (y - y_j) \in \mathbb{F}_q[x,y]$. Note that $H = \sqcup_j G_j \subset \mathbb{A}^2_{\mathbb{F}_q}$, i.e. H is the disjoint union of the horizontal lines $y = y_j$.

Note that $N(x,y), E(x,y)$ are polynomials of total degrees at most $a+b+2d$ and $a+b$ respectively. Since N, E do not have any common factors by assumption, the corresponding algebraic curves have no common components. Therefore, Bezout's theorem implies that

$$\sum_{P \in E \cap N} I(P, E \cap N) \leq \deg(E) \deg(N) \leq (a+b)(a+b+2d).$$

As $\deg(E(x, y_j)) = b$, the univariate polynomial $E(x, y_j)$ has b number of zeroes counted with multiplicities. Therefore we conclude that the total intersection multiplicity of E and G_j is given by $\sum_{P \in G_j \cap E} I(P, G_j \cap E) = b$ for all j. Therefore, we have

$$\sum_{P \in H \cap E} I(P, H \cap E) = \sum_j \sum_{P \in G_j \cap E} I(P, G_j \cap E) = nb.$$

Now we will show that every intersection point of $H \cap E$ is also an intersection point of $E \cap N$ (even when counted with multiplicities). This will lead to a contradiction as there would be too many points in $H \cap E$, since $na > (a+b)(a+b+2d)$.

First we note that $G_j \cap E \subset G_j \cap N$ for all $1 \leq j \leq n$, since $E(x, y_j)$ divides $N(x, y_j)$. Moreover, if $P \in G_j \cap E$ is a zero of $E(x, y_j)$ multiplicity m, then P is a zero of $N(x, y_j)$ of multiplicity at least m. Therefore, we have $I(P, G_j \cap E) \leq I(P, G_j \cap N)$ for all $1 \leq j \leq n$. Since G_j is non-singular, we have that $I(P, E \cap N) \geq I(P, G_j \cap E)$ for all $P \in G_j \cap E$, by applying Lemma 3.7 to the curves G_j, E, N.

Since H is a disjoint union of G_j's, we obtain that $I(P, E \cap H) \leq I(P, E \cap N)$ for all $P \in E \cap H$. Therefore, we have

$$nb = \sum_{P \in H \cap E} I(P, E \cap H) \leq \sum_{P \in E \cap N} I(P, E \cap N) = (a+b)(a+b+2d).$$

Similarly, we will have that $na \leq (a+b)(a+b+2d)$. Hence $n(a+b) \leq 2(a+b)(a+b+2d)$. This is a contradiction, since $n > 2a + 2b + 4d$ by assumption.

□

4 Divisors, Codes and Intersection theory

In this section we will interpret tensor products of AG codes geometrically and build our geometric tools to prove the generalized divisibility (Lemma 5.3) and generalized bivariate testing (Theorem 6.1). In particular, in Section 4.3, we will build a correspondence between tensor codewords and divisors on product surfaces. In Lemma 4.12, we will study local intersection multiplicities and prove the generalization of Lemma 3.7. Along the way we will review necessary background on algebraic curves, surfaces, divisors and intersection theory. We refer to [Ful08, Har77, Sti09, Ste12, Sha13, CR21] for more details on the algebraic-geometric background.

4.1 Divisors.

We will discuss the notions of divisors and Riemann-Roch space on higher dimensional algebraic varieties. For our applications, we will only need to consider surfaces, i.e. varieties of dimension 2. Moreover, we will work with surfaces over the algebraic closure $\overline{\mathbb{F}_q}$, and hence we work over the algebraic closure in this subsection.

Let X be a non-singular algebraic variety over $\overline{\mathbb{F}_q}$. A prime divisor on X is a irreducible closed subvariety D of codimension 1. A Weil divisor (or simply a divisor) on X is a finite $\mathbb{Z}$-linear combination of prime divisors. We denote the group of all divisors as $\mathrm{Div}(X)$, it is the free abelian group generated by the set of

all prime divisors. A divisor $\sum a_i D_i$ is called *effective* if $a_i \geq 0$ for all i. If $D = \sum a_i D_i$ is a divisor, then the set $\cup_{i, a_i \neq 0} D_i$ is called the *support* of D and is denoted by $\mathrm{Supp}(D)$.

Let $\overline{\mathbb{F}_q}(X)$ denote the function field of X. Every prime divisor D determines a discrete valuation $\nu_D : \overline{\mathbb{F}_q}(X) \to \mathbb{Z} \cup \{\infty\}$. Given a non-zero $f \in \overline{\mathbb{F}_q}(X)$ we define the divisor of f, as $\mathrm{div} f := \sum_D \nu_D(f) D$. We say that two divisors D_1, D_2 are linearly equivalent and denote $D_1 \sim D_2$ iff $D_1 - D_2 = \mathrm{div} f$ for some non-zero rational function f. Let $\varphi : X \to Y$ be a morphism of non-singular varieties X, Y and D a divisor on Y such that $\varphi(X) \not\subseteq \mathrm{Supp}(D)$. Then we can define a pull-back divisor $\varphi^*(D) \in \mathrm{Div}(X)$ [Sha13, Chapter 3, Section 1.2]. If $\iota : X \hookrightarrow Y$ is a subvariety with $X \not\subseteq \mathrm{Supp}(D)$, then we define the *restricted divisor* as $D|_X := \iota^*(D)$. Let $\varphi : X \to Y$ be a morphism of non-singular varieties X, Y such that $\varphi(X)$ is dense in Y. Then we have a pull-back homomorphism $\varphi^* : \mathrm{Div}(Y) \to \mathrm{Div}(X)$ [Sha13, Chapter 3, Section 1.2]. Moreover, the homomorphism φ^* preserves linear equivalence, i.e. if $D_1 \sim D_2$ then $\varphi^* D_1 \sim \varphi^* D_2$.

Given a divisor D on a non-singular variety X, we define the corresponding Riemann-Roch space as

$$\mathcal{L}(X, D) = \{f \in \overline{\mathbb{F}_q}(X) \mid \mathrm{div} f + D \geq 0\} \cup \{0\}$$

For simplicity, we will often write $\mathcal{L}(D)$ when X is evident from the context. The set $\mathcal{L}(D)$ is a vector space over $\overline{\mathbb{F}_q}$, where addition is induced by addition in the function field $\overline{\mathbb{F}_q}(X)$. If X is a projective variety, then $\mathcal{L}(D)$ is a finite dimensional vector space. Moreover, if $D_1 \sim D_2$, then there is an isomorphism $\mathcal{L}(D_1) \cong \mathcal{L}(D_2)$.

4.2 Evaluation maps.

Let X be a geometrically irreducible non-singular projective algebraic curve over $\mathbb{F}_q$. Let $x_1, \cdots, x_n \in X$ be $\mathbb{F}_q$-rational points and $D = x_1 + \cdots + x_n$. Let H a $\mathbb{F}_q$-rational divisor on X such that $\mathrm{Supp}(D) \cap \mathrm{Supp}(H) = \emptyset$.

$$\varphi_X : \mathcal{L}(X, H) \to \overline{\mathbb{F}_q}^n$$

be the evaluation map defined as $f \mapsto (f(x_1), \cdots, f(x_n))$. Note that here the Riemann-Roch space $\mathcal{L}(X, H)$ is defined over the algebraic closure $\overline{\mathbb{F}_q}$ and hence it consists of rational functions defined over $\overline{\mathbb{F}_q}$. Thus the image $\mathrm{im}(\varphi_X)$ is a linear subspace of $\overline{\mathbb{F}_q}^n$, and it is not contained in $\mathbb{F}_q^n$. In Definition 2.2, we defined the AG code $C_{\mathcal{L}}(X, D, H)$ as evaluations of rational functions defined over $\mathbb{F}_q$. In particular, let $\mathcal{L}_{\mathbb{F}_q}(X, H)$ denote the Riemann-Roch space of rational functions defined over $\mathbb{F}_q$, i.e.

$$\mathcal{L}_{\mathbb{F}_q}(X, H) = \{f \in \mathbb{F}_q(X) \mid \mathrm{div} f + H \geq 0\} \cup \{0\}.$$

We define

$$\varphi_{X, \mathbb{F}_q} : \mathcal{L}_{\mathbb{F}_q}(X, H) \to \mathbb{F}_q^n$$

to be the evaluation map defined as $f \mapsto (f(x_1), \cdots, f(x_n))$. Then we have $C_{\mathcal{L}}(X, D, H) = \mathrm{im}(\varphi_{X, \mathbb{F}_q})$. In the next result, we note that these two constructions are agree after base change. This result is stated in [Ste12, Chapter 5], and we provide a proof for completeness.

Proposition 4.1. *Let $C_{\mathcal{L}}(X, D, H) \subseteq \mathbb{F}_q^n$ be an AG code with $D = x_1 + \cdots + x_n$. Then, the base change $\overline{C_{\mathcal{L}}(X, D, H)} := C_{\mathcal{L}}(X, D, H)) \otimes_{\mathbb{F}_q} \overline{\mathbb{F}_q}$ is given by*

$$\overline{C_{\mathcal{L}}(X, D, H)} = \mathrm{im}(\varphi_X) = \{(f(x_1), \cdots, f(x_n)) \mid f \in \mathcal{L}(X, H))\}.$$

Proof. Note that we have $\mathcal{L}_{\mathbb{F}_q}(X, H) \subseteq \mathcal{L}(X, H)$. By [Sha13, Section 3.5, Example 3.7], we know that $\mathcal{L}(X, H)$ is generated over $\overline{\mathbb{F}_q}$ by $\mathcal{L}_{\mathbb{F}_q}(X, H)$. Therefore we have $\mathcal{L}(X, H) = \mathcal{L}_{\mathbb{F}_q}(X, H) \otimes_{\mathbb{F}_q} \overline{\mathbb{F}_q}$. Recall that $C_{\mathcal{L}}(X, D, H)$ is the image of the $\mathbb{F}_q$-linear map $\varphi_{X, \mathbb{F}_q} : \mathcal{L}_{\mathbb{F}_q}(X, H) \to \mathbb{F}_q^n$. Then we see that $\varphi_X = \varphi_{X, \mathbb{F}_q} \otimes_{\mathbb{F}_q} \overline{\mathbb{F}_q}$, and hence $\overline{C_{\mathcal{L}}(X, D, H)} = C_{\mathcal{L}}(X, D, H) \otimes_{\mathbb{F}_q} \overline{\mathbb{F}_q} = \mathrm{im}(\varphi_X)$. □

The following statement is a consequence of the proof of Proposition 2.4. We note it here for convenience.

Lemma 4.2. *Let $C_{\mathcal{L}}(X, D_1, H_1)$ and $C_{\mathcal{L}}(Y, D_2, H_2)$ be AG codes of length n over $\mathbb{F}_q$. Then we have the following.*

1. *If $\deg(H_1) < n$ then the evaluation map $\varphi_{X,\mathbb{F}_q} : \mathcal{L}_{\mathbb{F}_q}(X, H_1) \to \mathbb{F}_q^n$ is injective, and hence an isomorphism onto $C_{\mathcal{L}}(X, D_1, H_1)$.*
2. *If $\deg(H_i) < n$ for both $i = 1, 2$, then the map*

$$\varphi_{X,\mathbb{F}_q} \otimes \varphi_{Y,\mathbb{F}_q} : \mathcal{L}_{\mathbb{F}_q}(X, H_1) \otimes \mathcal{L}_{\mathbb{F}_q}(Y, H_2) \to \mathbb{F}_q^n \otimes \mathbb{F}_q^n$$

   is an isomorphism onto $C_{\mathcal{L}}(X, D_1, H_1) \otimes C_{\mathcal{L}}(X, D_2, H_2)$.

3. *The statements (1) and (2) above hold for the maps φ_X and φ_Y defined over the algebraic closure $\overline{\mathbb{F}_q}$.*

Proof. (1) Let $f \in \ker(\varphi_{X,\mathbb{F}_q})$ be a non-zero rational function and $D = \mathrm{div} f + H_1$ be the effective divisor on X which corresponds to f. Let $x_1, \cdots, x_n$ be the rational points corresponding to D_1. If $f \in \ker(\varphi_{X,\mathbb{F}_q})$, then f vanishes on $x_1, \cdots, x_n$, and hence $D - D_1$ is an effective divisor on X. Note that D is linearly equivalent to H_1, i.e. $D \sim H_1$. Therefore we have $\deg(D - D_1) = \deg(H_1) - n < 0$. This is a contradiction as degree of an effective divisor must be non-negative. Therefore, we must have $\ker(\varphi_X) = (0)$.

(2) By part (1) we have that $\varphi_{X,\mathbb{F}_q} : \mathcal{L}_{\mathbb{F}_q}(X, H_1) \to C_{\mathcal{L}}(X, D_1, H_1)$ is an isomorphism. Similarly, we have that $\varphi_{Y,\mathbb{F}_q} : \mathcal{L}_{\mathbb{F}_q}(Y, H_2) \to C_{\mathcal{L}}(Y, D_2, H_2)$ is also an isomorphism. Hence we must have that $\varphi_{X,\mathbb{F}_q} \otimes \varphi_{Y,\mathbb{F}_q}$ is an isomorphism onto $C_{\mathcal{L}}(X, D_1, H_1) \otimes C_{\mathcal{L}}(Y, D_2, H_2)$.

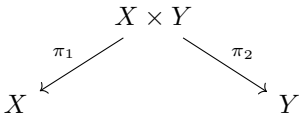
(3) Recall that we have $\mathcal{L}(X, H_1) = \mathcal{L}_{\mathbb{F}_q}(X, H_1) \otimes_{\mathbb{F}_q} \overline{\mathbb{F}_q}$ and that $\overline{C_{\mathcal{L}}(X, D_1, H_1)} = C_{\mathcal{L}}(X, D_1, H_1) \otimes_{\mathbb{F}_q} \overline{\mathbb{F}_q}$. Therefore, we obtain (3) by tensoring the isomorphisms given by (1) and (2) with $\_ \otimes \overline{\mathbb{F}_q}$.

□

4.3 Divisors associated to tensor codewords.

In this subsection we will construct divisors associated to tensor codewords. In particular, given two AG codes C_1, C_2 on curves X, Y, and a codeword in the tensor product $C_1 \otimes C_2$, we will associate a curve/divisor on the product surface $X \times Y$. First, let us formalize the set-up and prove a few preliminary results.

Let X, Y be irreducible non-singular projective algebraic curves over $\overline{\mathbb{F}_q}$. Consider the irreducible non-singular projective algebraic surface $X \times Y$ over $\overline{\mathbb{F}_q}$. Let $\pi_1 : X \times Y \to X$ and $\pi_2 : X \times Y \to Y$ be the projection morphisms.



Since π_1, π_2 are surjective, we have pull-back homomorphisms $\pi_1^* : \mathrm{Div}(X) \to \mathrm{Div}(X \times Y)$ and $\pi_2^* : \mathrm{Div}(Y) \to \mathrm{Div}(X \times Y)$. Let $H_1 \in \mathrm{Div}(X)$ and $H_2 \in \mathrm{Div}(Y)$ be two divisors. Consider the divisor $\pi_1^*(H_1) + \pi_1^*(H_2) \in \mathrm{Div}(X \times Y)$ and its Riemann-Roch space $\mathcal{L}(X \times Y, \pi_1^*(H_1) + \pi_1^*(H_2))$. Let $\mathcal{L}(X, H_1)$ and $\mathcal{L}(Y, H_2)$ denote Riemann-Roch spaces of H_1 and H_2 on X, Y respectively. Recall that we have a pull-back homomorphism between function fields $\pi_1^* : \mathbb{F}_q(X) \hookrightarrow \mathbb{F}_q(X \times Y)$ given by composition with π_1, and similarly we have $\pi_2^* : \mathbb{F}_q(Y) \hookrightarrow \mathbb{F}_q(X \times Y)$. By tensoring with $\overline{\mathbb{F}_q}$, we obtain the pull-back homomorphisms over the function fields over $\overline{\mathbb{F}_q}$.

Lemma 4.3. *Let $v_1, \cdots v_r \in \mathcal{L}(X, H_1)$ and $w_1, \cdots, w_s \in \mathcal{L}(Y, H_2)$ be $\overline{\mathbb{F}_q}$-linear bases which are defined over $\mathbb{F}_q$. Let ψ be the $\overline{\mathbb{F}_q}$-linear map*

$$\psi : \mathcal{L}(X, H_1) \otimes \mathcal{L}(Y, H_2) \to \overline{\mathbb{F}_q}(X \times Y)$$

defined by $\psi(v_i \otimes w_j) = \pi_1^*(v_i)\pi_2^*(w_j)$ for all $i \in [r], j \in [s]$. Similarly, let $\psi_{\mathbb{F}_q}$ be the homomorphism over the base field $\mathbb{F}_q$. Then we have the following.

1. *For any $v \in \mathcal{L}(X, H_1)$, we have $\pi_1^*(v) \in \mathcal{L}(X \times Y, \pi_1^*(H_1))$. Similarly, $\pi_2^*(w) \in \mathcal{L}(X \times Y, \pi_2^*(H_2))$ for any $w \in \mathcal{L}(Y, H_2)$.*

2. *The image of the map ψ is contained in $\mathcal{L}(X \times Y, \pi_1^*(H_1) + \pi_1^*(H_2))$.*

Proof. (1) Let $v \in \mathcal{L}(X, H_1)$. Then we have that $\mathrm{div}(v) + H_1$ is an effective divisor. Thus $\pi_1^*(\mathrm{div}(v) + H_1) = \pi_1^*(\mathrm{div}(v)) + \pi_1^*(H_1) = \mathrm{div}(\pi_1^* v) + \pi_1^*(H_1)$ is an effective divisor, since pull-back of an effective divisor by the projection morphism is effective. Therefore, $\pi_1^* v \in \mathcal{L}(X \times Y, \pi_1^*(H_1))$.

(2) We have that $\pi_1^*(v_i) \in \mathcal{L}(X \times Y, \pi_1^* H_1)$ and $\pi_2^*(w_j) \in \mathcal{L}(X \times Y, \pi_2^* H_2)$ by part (1). Hence we have that

$$\mathrm{div}(\pi_1^*(v_i)\pi_2^*(w_j)) + \pi_1^*(H_1) + \pi_2^*(H_2) = \mathrm{div}(\pi_1^*(v_i)) + \mathrm{div}(\pi_1^*(v_i)) + \pi_1^*(H_1) + \pi_2^*(H_2)$$

is effective. Therefore, $\pi_1^*(v_i)\pi_2^*(w_j) \in \mathcal{L}(X \times Y, \pi_1^*(H_1) + \pi_2^*(H_2))$. By $\overline{\mathbb{F}_q}$-linearity, we have that $\mathrm{im}(\psi) \subseteq \mathcal{L}(X \times Y, \pi_1^*(H_1) + \pi_2^*(H_2))$.

□

Corollary 4.4. *Let $C_{\mathcal{L}}(X, D_1, H_1)$ and $C_{\mathcal{L}}(Y, D_2, H_2)$ be AG codes of length n over $\mathbb{F}_q$. Let $x_1, \cdots, x_n \in X$ and $y_1, \cdots, y_n \in Y$ be the $\mathbb{F}_q$-rational points corresponding to D_1, D_2 respectively. Let $f \in \mathcal{L}_{\mathbb{F}_q}(X, H_1) \otimes \mathcal{L}_{\mathbb{F}_q}(Y, H_2)$. Then we have the following.*

1. *The corresponding codeword $(\varphi_{X,\mathbb{F}_q} \otimes \varphi_{Y,\mathbb{F}_q})(f) \in \mathbb{F}_q^{n \times n}$ is given by the matrix*

$$\begin{bmatrix} \psi(f)(x_1, y_1) & \psi(f)(x_2, y_1) & \cdots & \psi(f)(x_n, y_1) \\ \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot \\ \psi(f)(x_1, y_n) & f(x_2, y_n) & \cdots & \psi(f)(x_n, y_n) \end{bmatrix}$$

2. *In other words, let $D := (\varphi_{X,\mathbb{F}_q} \otimes \varphi_{Y,\mathbb{F}_q})(f) \in C_{\mathcal{L}}(X, D_1, H_1) \otimes C_{\mathcal{L}}(X, D_2, H_2)$. Then the rational function $\psi(f)$ is defined at (x_i, y_j) and we have $\psi(f)(x_i, y_j) = D(x_i, y_j)$.*

Proof. For any two rational functions $v \in \mathcal{L}_{\mathbb{F}_q}(X, H_1)$ and $w \in \mathcal{L}_{\mathbb{F}_q}(Y, H_2)$, we have $\varphi_{X,\mathbb{F}_q}(v) = (v(x_1), \cdots, v(x_n))$ and $\varphi_{Y,\mathbb{F}_q}(w) = (w(y_1), \cdots, w(y_n))$. Therefore, we note that the image $(\varphi_{X,\mathbb{F}_q} \otimes \varphi_{Y,\mathbb{F}_q})(v \otimes w)$ in $\mathbb{F}_q^{n \times n}$ is the Kronecker product of $\varphi_{X,\mathbb{F}_q}(v)$ and $\varphi_{Y,\mathbb{F}_q}(w)^T$. In particular, we have

$$(\varphi_{X,\mathbb{F}_q} \otimes \varphi_{Y,\mathbb{F}_q})(v \otimes w) = \varphi_{X,\mathbb{F}_q}(v) \otimes \varphi_{Y,\mathbb{F}_q}(w)^T = \begin{bmatrix} v(x_1)w(y_1) & v(x_2)w(y_1) & \cdots & v(x_n)w(y_1) \\ \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot \\ v(x_1)w(y_n) & v(x_2)w(y_n) & \cdots & v(x_n)w(y_n) \end{bmatrix}$$

Let $v_1, \cdots, v_r$ and $w_1, \cdots, w_s$ be $\mathbb{F}_q$-linear bases of $\mathcal{L}_{\mathbb{F}_q}(X, H_1)$ and $\mathcal{L}_{\mathbb{F}_q}(Y, H_2)$ respectively. By Proposition 4.1, we may assume that these are $\overline{\mathbb{F}_q}$-linear bases of $\mathcal{L}(X, H_1)$ and $\mathcal{L}(Y, H_2)$. Now $\pi_1^*(v_i)(x, y) = v_i(x)$ and $\pi_2^*(w_j)(x, y) = w(y)$. Therefore, the result holds when $f = v_i \otimes w_j$, since $\psi(v_i \otimes w_j) = \pi_1^*(v_i)\pi_2^*(w_j)$. In general, we may write $f = \sum_{i,j} a_{ij} v_i \otimes w_j$ where $a_{ij} \in \mathbb{F}_q$. Hence, by linearity of $\varphi_{X,\mathbb{F}_q} \otimes \varphi_{Y,\mathbb{F}_q}$ we have $(\varphi_{X,\mathbb{F}_q} \otimes \varphi_{Y,\mathbb{F}_q})(f) = \sum_{i,j} a_{ij} (\varphi_{X,\mathbb{F}_q} \otimes \varphi_{Y,\mathbb{F}_q})(v_i \otimes w_j)$. Now we have $\psi(f)(x_k, y_\ell) = \sum_{i,j} a_{ij} v_i(x_k) w_j(y_\ell)$, and we obtain the desired formula for $(\varphi_{X,\mathbb{F}_q} \otimes \varphi_{Y,\mathbb{F}_q})(f)$ by writing each $(\varphi_{X,\mathbb{F}_q} \otimes \varphi_{Y,\mathbb{F}_q})(v_k \otimes w_\ell)$ as matrices described above.

□

The rest of this subsection is devoted to our construction of divisors on product surfaces from tensor codewords. We will use the following definitions and notation.

Let X, Y be geometrically irreducible non-singular projective algebraic curves over $\mathbb{F}_q$, and let $\overline{X}, \overline{Y}$ denote their base changes to the algebraic closure $\overline{\mathbb{F}_q}$. Let H_1, H_2 be $\mathbb{F}_q$-rational divisors on X, Y respectively.

Let $x_1, \cdots, x_n \in X$ and $y_1, \cdots, y_n \in Y$ be $\mathbb{F}_q$ distinct rational points. We let $D_1 = x_1 + \cdots + x_n$ and $D_2 = y_1 + \cdots + y_n$, and assume that $\mathrm{Supp}(D_i) \cap \mathrm{Supp}(H_i) = \emptyset$. We have the following commutative diagram of $\mathbb{F}_q$-linear maps

$$\begin{array}{ccc} \mathcal{L}_{\mathbb{F}_q}(X, H_1) \otimes \mathcal{L}_{\mathbb{F}_q}(Y, H_2) & \xrightarrow{\psi_{\mathbb{F}_q}} & \mathcal{L}_{\mathbb{F}_q}(X \times Y, \pi_1^* H_1 + \pi_2^* H_2) \\ \downarrow{\scriptstyle \varphi_{X,\mathbb{F}_q} \otimes \varphi_{Y,\mathbb{F}_q}} & \nearrow_{\theta_{\mathbb{F}_q}} & \\ C_{\mathcal{L}}(X, D_1, H_1) \otimes C_{\mathcal{L}}(Y, D_2, H_2) & & \end{array}$$

By tensoring with $\overline{\mathbb{F}_q}$, we obtain a commutative diagram over the algebraic closure.

$$\begin{array}{ccc} \mathcal{L}(X, H_1) \otimes \mathcal{L}(Y, H_2) & \xrightarrow{\psi} & \mathcal{L}(\overline{X} \times \overline{Y}, \pi_1^* H_1 + \pi_2^* H_2) \\ \downarrow{\scriptstyle \varphi_X \otimes \varphi_Y} & \nearrow_{\theta} & \\ \overline{C_{\mathcal{L}}(X, D_1, H_1)} \otimes \overline{C_{\mathcal{L}}(Y, D_2, H_2)} & & \end{array}$$

If $\deg(H_i) < n$ for both $i = 1, 2$, then we know that the left vertical arrow is an isomorphism by Lemma 4.2. We define $\theta_{\mathbb{F}_q} := \psi_{\mathbb{F}_q} \circ (\varphi_{X,\mathbb{F}_q} \otimes \varphi_{Y,\mathbb{F}_q})^{-1}$ and similarly $\theta := \psi \circ (\varphi_X \otimes \varphi_Y)^{-1}$. Given any $D \in C_{\mathcal{L}}(X, D_1, H_1) \otimes C_{\mathcal{L}}(Y, D_2, H_2)$, we continue to denote by D the image under the inclusion $C_{\mathcal{L}}(X, D_1, H_1) \otimes C_{\mathcal{L}}(Y, D_2, H_2) \hookrightarrow \overline{C_{\mathcal{L}}(X, D_1, H_1)} \otimes \overline{C_{\mathcal{L}}(Y, D_2, H_2)}$. Recall that the image of the map ψ is contained in $\mathcal{L}(\overline{X} \times \overline{Y}, \pi_1^* H_1 + \pi_2^* H_2)$ by Lemma 4.3.

Definition 4.5 (Rational function associated to tensor codeword)**.** We define the *rational function associated to the tensor codeword* D to be the rational function

$$\theta(D) \in \mathcal{L}(\overline{X} \times \overline{Y}, \pi_1^* H_1 + \pi_2^* H_2),$$

Note that the rational function $\theta(D)$ is actually defined over the base field $\mathbb{F}_q$, as θ is given by the base change of the corresponding homomorphism $\theta_{\mathbb{F}_q}$ over $\mathbb{F}_q$.

Therefore, given a tensor codeword D, the above definition associates a rational function on the product surface over the algebraic closure. The following result shows that non-zero codewords give rise to non-zero rational functions.

Proposition 4.6. *Let $C_{\mathcal{L}}(X, D_1, H_1)$ and $C_{\mathcal{L}}(Y, D_2, H_2)$be AG codes of length n over $\mathbb{F}_q$, with $D_1 = \sum_i x_i$ and $D_2 = \sum_j y_j$. Suppose that $\deg(H_i) < n$ for $i = 1, 2$. Let $D \in C_{\mathcal{L}}(X, D_1, H_1) \otimes C_{\mathcal{L}}(Y, D_2, H_2)$ be a tensor codeword such that $D(x_i, y_j) \neq 0$ for some $i, j \in [n]$. Then the rational function $\theta(D)$ is non-zero.*

Proof. Since $\deg(H_i) < n$, we know that $\varphi_{X,\mathbb{F}_q} \otimes \varphi_{Y,\mathbb{F}_q}$ is an isomorphism by Lemma 4.2. Let $f = (\varphi_{X,\mathbb{F}_q} \otimes \varphi_{Y,\mathbb{F}_q})^{-1}(D)$. Hence D is given by the evaluation of f at all the pairs (x_i, y_j), by Corollary 4.4. Since there exists $i, j \in [n]$ such that $D(x_i, y_j) \neq 0$, we conclude that $\psi(f) \neq 0$. Similarly for $\theta_{\mathbb{F}_q}$. □

The proposition above shows that the map θ is injective. In the following lemma, we will show that the map θ is an isomorphism. In general, given two divisors A, B on an algebraic variety Z, we have a similar multiplication map $\mathcal{L}(Z, A) \otimes \mathcal{L}(Z, B) \to \mathcal{L}(Z, A + B)$. However, this map is not always an isomorphism. For instance, we may take Z to be an elliptic curve, let A be a divisor of degree 0 such that $A \neq 0$ and let $B = -A$. Then $\mathcal{L}(Z, A) = \mathcal{L}(Z, B) = \{0\}$, whereas $\mathcal{L}(Z, A + B) = \mathcal{L}(Z, 0)$ is a 1-dimensional vector space. Our situation in Lemma 4.7 is special since the divisors on the surface $Z = X \times Y$ are pull-backs of divisors on X and Y. Here this isomorphism occurs due to algebraic-geometric reasons rather than purely linear algebraic reasons. Hence, in order to prove this isomorphism, we will use the notions of sheaves and cohomology from [Har77].

Lemma 4.7. *Let $C_{\mathcal{L}}(X, D_1, H_1)$ and $C_{\mathcal{L}}(Y, D_2, H_2)$be AG codes of length n over $\mathbb{F}_q$, with $D_1 = \sum_i x_i$ and $D_2 = \sum_j y_j$. Suppose that $\deg(H_i) < n$ for $i = 1, 2$. The the maps $\theta_{\mathbb{F}_q}$ and θ are isomorphisms of vector spaces.*

Proof. Since $\theta = \theta_{\mathbb{F}_q} \otimes \overline{\mathbb{F}_q}$, it is enough to show the statement for θ. By Proposition 4.6, we know that θ is injective. Therefore it is enough to show that $C_{\mathcal{L}}(X, D_1, H_1) \otimes C_{\mathcal{L}}(Y, D_2, H_2)$ and $\mathcal{L}(\overline{X} \times \overline{Y}, \pi_1^* H_1 + \pi_2^* H_2)$ are of the same dimension. Let $Z = \overline{X} \times \overline{Y}$. We know that $\mathcal{L}(Z, \pi_1^* H_1 + \pi_2^* H_2) = H^0(Z, \mathcal{O}_Z(\pi_1^* H_1 + \pi_2^* H_2))$, which is the 0-th cohomology group of the sheaf $\mathcal{O}_Z(\pi_1^* H_1 + \pi_2^* H_2)$.

We have the following fiber product

$$\begin{array}{ccc} Z & \xrightarrow{\pi_2} & \overline{Y} \\ \downarrow{\scriptstyle \pi_1} & & \downarrow{\scriptstyle f} \\ \overline{X} & \xrightarrow{g} & \mathrm{Spec}(\overline{\mathbb{F}_q}) \end{array}$$

We have $\pi_{1,*}\pi_2^* H_2 \cong g^*(f_*(H_2)) \cong g^*(H^0(\overline{Y}, H_2))$ by [Har77, Proposition III.9.3]. Now, by using the projection formula [Har77, Exercise II.5.1], we obtain

$$\begin{aligned} H^0(X \times Y, \pi_1^* H_1 \otimes \pi_2^* H_2) &\cong (g \circ \pi_1)_*(\pi_1^* H_1 \otimes \pi_2^* H_2) \\ &\cong g_* \circ \pi_{1,*}(\pi_1^* H_1 \otimes \pi_2^* H_2) \\ &\cong g_*(H_1 \otimes \pi_{1,*}\pi_2^* H_2) \\ &\cong g_*(H_1 \otimes g^*(H^0(Y, H_2))) \\ &\cong g_*(H_1) \otimes (H^0(Y, H_2)) \\ &\cong H^0(\overline{X}, H_1) \otimes H^0(\overline{Y}, H_2). \end{aligned}$$

Since $H^0(\overline{X}, H_1) = \mathcal{L}(\overline{X}, H_1) \cong C_{\mathcal{L}}(X, D_1, H_1)$ and $H^0(\overline{Y}, H_2) = \mathcal{L}(\overline{Y}, H_2) \cong C_{\mathcal{L}}(Y, D_2, H_2)$, we conclude that the $\overline{\mathbb{F}_q}$-vector spaces $C_{\mathcal{L}}(X, D_1, H_1) \otimes C_{\mathcal{L}}(Y, D_2, H_2)$ and $\mathcal{L}(\overline{X} \times \overline{Y}, \pi_1^* H_1 + \pi_2^* H_2)$ are of the same dimension.

□

The following definition provides our key construction that associates divisors on product surfaces to tensor codewords. Recall that in the case of Reed-Solomon codes, tensor codewords are given by bivariate polynomials. As discussed in the introduction, the following construction is a generalization of the algebraic curves corresponding to bivariate polynomials.

Definition 4.8 (Divisor associated to a tensor codeword)**.** Let $C_{\mathcal{L}}(X, D_1, H_1)$ and $C_{\mathcal{L}}(X, D_2, H_2)$ be AG codes of length n over $\mathbb{F}_q$, with $D_1 = \sum_i x_i$ and $D_2 = \sum_j y_j$. Let $D \in C_{\mathcal{L}}(X, D_1, H_1) \otimes C_{\mathcal{L}}(X, D_2, H_2)$ be a tensor codeword such that $D(x_i, y_j) \neq 0$ for some $i, j \in [n]$. We define the *divisor associated to the tensor codeword* D to be the effective divisor

$$\mathrm{div}(\theta(D)) + \pi_1^*(H_1) + \pi_2^*(H_2) \in \mathrm{Div}(\overline{X} \times \overline{Y}).$$

Remark 4.9. Note that the rational function associated to D is non-zero by Proposition 4.6. Therefore the *divisor associated to the tensor codeword* D is a *well-defined* divisor on the product surface $\overline{X} \times \overline{Y}$ over the algebraic closure $\overline{\mathbb{F}_q}$. We also note that the rational function $\theta(D)$ is defined over the base field $\mathbb{F}_q$. Therefore the divisor D is an $\mathbb{F}_q$-rational divisor. Moreover it is an effective divisor linearly equivalent to the divisor $\pi_1^*(H_1) + \pi_2^*(mH_2)$. For simplicity, we will abuse notation and continue to denote the *divisor associated to the tensor codeword* D by the same letter, and write $D := \mathrm{div}(\theta(D)) + \pi_1^*(H_1) + \pi_2^*(H_2)$.

We note useful properties of divisors associated to tensor codewords below.

Lemma 4.10. *Let $C_{\mathcal{L}}(X, D_1, H_1)$ and $C_{\mathcal{L}}(X, D_2, H_2)$ be AG codes of length n over $\mathbb{F}_q$, with $D_1 = \sum_i x_i$ and $D_2 = \sum_j y_j$. Let $E \in C_{\mathcal{L}}(X, D_1, H_1) \otimes C_{\mathcal{L}}(X, D_2, H_2)$ be a non-zero tensor codeword. Let $E \in \mathrm{Div}(\overline{X} \times \overline{Y})$ and $\theta(E)$ denote the divisor and the rational function associated to the codeword E respectively. Let $F_i = \pi_1^{-1}(x_i)$ and $G_j = \pi_2^{-1}(y_j)$ be the fibers of the projection morphisms. Then we have the following.*

1. *(Poles of E). If $C \subseteq \mathrm{Supp}(\mathrm{div}(\theta(E)))$ is an irreducible curve such that $\mathrm{coeff}_C(\mathrm{div}(\theta(E))) < 0$, then $C \subseteq \mathrm{Supp}(\pi_1^* H_1)$ or $C \subseteq \mathrm{Supp}(\pi_2^* H_2)$.*

2. *Suppose that for some $i \in [n]$, we have $F_i \subseteq \mathrm{Supp}(E)$ and $\mathrm{coeff}_{F_i}(E) > 0$. Then the rational function $\theta(E)$ is defined at (x_i, y_j) and we have $\theta(E)(x_i, y_j) = 0$ for all $j \in [n]$.*

Proof. (1) Note that E is the divisor $\mathrm{div}(\theta(E)) + \pi_1^* H_1 + \pi_2^* H_2$. Since E is effective and $\mathrm{coeff}_C(\mathrm{div}(\theta(E))) < 0$, we must have that C appears with positive coefficient in $\pi_1^* H_1 + \pi_2^* H_2$. Therefore, we have $C \subseteq \mathrm{Supp}(\pi_1^* H_1)$ or $C \subseteq \mathrm{Supp}(\pi_2^* H_2)$.

(2) By applying Corollary 4.4 and base change to $\overline{\mathbb{F}_q}$, we conclude that $\theta(E)$ is defined at (x_i, y_j). Let η be the generic point of the irreducible curve F_i and $p := (x_i, y_j)$ for some j. Let us choose an affine open neighbourhood $p \in U = \mathrm{Spec}(A) \subset \overline{X} \times \overline{Y}$ such that $\theta(E)$ is a regular function on U, i.e. $\theta(E) \in A$. Note that we must have $\eta \in U$, and η is the generic point of the divisor $F_i \cap U$ in U. Let us continue to denote the prime ideals of A corresponding to η, p by the same letters. Recall that by definition of AG codes we have $x_i \notin \mathrm{Supp}(H_1)$. Hence $F_i \not\subseteq \mathrm{Supp}(\pi_1^* H_1)$. Moreover, since F_i maps dominantly to Y under π_2, we have that $F_i \not\subseteq \mathrm{Supp}(\pi_2^* H_2)$. Thus we must have that $\mathrm{coeff}_{F_i}(\mathrm{div}(\theta(E))) > 0$ as $\mathrm{coeff}_{F_i}(E) > 0$. Since $\mathrm{coeff}_{F_i}(\mathrm{div}(\theta(E))) > 0$, we know that $\nu_\eta(\theta(E))) > 0$ where ν_η is the discrete valuation on the discrete valuation ring A_η . In particular, $\theta(E)/1 \in A_\eta$ is contained in the maximal ideal ηA_η of the DVR $\mathcal{O}_\eta = A_\eta \subset K(A)$. Therefore, $\theta(E) \in \eta \subset A$. Hence we also have $\theta(E) \in p \subset A$, since $\eta \subset p$. Therefore $\theta(E)(p) = 0$ in A_p/pA_p, i.e. $\theta(E)(x_i, y_j) = 0$. □

4.4 Intersection theory on surfaces.

In this subsection we develop the necessary background on intersection theory on surfaces. We will use the definitions from [Har77, Chapter V]. The notions of intersection multiplicities and intersection product used here are a generalization of the notions for plane algebraic curves in [Ful08].

Let S be an irreducible non-singular projective algebraic surface over $\overline{\mathbb{F}_q}$. A curve on S will mean any effective divisor on S. For any point $P \in S$, we denote the corresponding local ring as $\mathcal{O}_{P,S}$.

Intersection multiplicity. If C and D are curves with no common irreducible component, and if $P \in C \cap D$, then we define the intersection multiplicity $(C \cdot D)_P$ of C and D at P to be the length of $\mathcal{O}_{P,S}/(f, g)$, where f, g are local equations of C, D at P. If $P \notin C \cap D$, then we define $(C \cdot D)_P = 0$.

We recall the following result regarding the intersection product on surfaces.

Theorem 4.11. *[Har77, Chapter V, Theorem 1.1, Proposition 1.4] There is a unique pairing $\mathrm{Div}(S) \times \mathrm{Div}(S) \to \mathbb{Z}$, denoted by $C \cdot D$ for any two divisors C, D, such that the following holds.*

1. *If C and D are non-singular curves meeting transversally, then $C \cdot D = |C \cap D|$, the number of points of $C \cap D$.*

2. *It is symmetric: $C \cdot D = D \cdot C$.*

3. *It is additive: $(C_1 + C_2) \cdot D = C_1 \cdot D + C_2 \cdot D$*

4. *It depends only on the linear equivalence classes: if $C_1 \sim C_2$ then $C_1 \cdot D = C_2 \cdot D$.*

5. *If C and D are divisors on X having no common irreducible component, then we have $C \cdot D = \sum_{P \in C \cap D} (C \cdot D)_P$.*

6. *Let C be an irreducible curve on S. If D is an effective divisor such that C is not a component of D. Then $D \cdot C \geq 0$. In particular, if $D - E$ is an effective divisor where D, C do not have common components, then $D \cdot C \geq E \cdot C$.*

Proof. Parts $(1) - (4)$ are the content of [Har77, Chapter V, Theorem 1.1]. Part (5) is the content of [Har77, Chapter V, Proposition 1.4]. For the first part of (6), note that we have $C \cdot D = \sum_{P \in C \cap D} (C \cdot D)_P$ by part (5). Moreover $(C \cdot D)_P \geq 0$ since the length of a module is a non-negative integer. Therefore $D \cdot C \geq 0$. For the second part, we apply the first part to the divisors $D - E$ and C and use additivity. □

Given a non-singular curve $C \subseteq S$ and a divisor $D \in \mathrm{Div}(S)$ such that $C \not\subseteq \mathrm{Supp}(D)$, we defined the restricted divisor $D|_C$ in Section 4.1. In the following result we provide an explicit formula for the restricted divisor. Moreover, we also generalize our local intersection multiplicity bound from Lemma 3.7.

Lemma 4.12. *Let S be a non-singular irreducible projective algebraic surface over $\overline{\mathbb{F}}_q$. Let $N, E \in \mathrm{Div}(S)$ be divisors and $F \subset S$ be a non-singular irreducible curve. Suppose that N, E are effective divisors without common components and $F \not\subseteq \mathrm{Supp}(N) \cup \mathrm{Supp}(E)$. Then we have the following.*

1. *The restricted divisor $N|_F \in \mathrm{Div}(F)$ on the curve F is given by*

$$N|_F = \sum_{P \in N \cap F} (N \cdot F)_P \cdot P.$$

   In particular, $\deg(N|_F) = N \cdot F$. *Similarly,* $E|_F = \sum_{P \in E \cap F} (E \cdot F)_P$ *and* $\deg(E|_F) = E \cdot F$.

2. *For all $P \in N \cap E \cap F$, we have*

$$(N \cdot E)_P \geq \min\{(N \cdot F)_P, (E \cdot F)_P\}.$$

3. *Suppose that $N|_F - E|_F$ is an effective divisor on F. Then, $E \cap F \subseteq N \cap F$. Moreover, $P \in N \cap E \cap F$, we have*

$$(N \cdot E)_P \geq (E \cdot F)_P.$$

Proof. (1) Since S is non-singular, any divisor on S is locally principal or a Cartier divisor by [Sha13, Chapter 3, Section 1.2] or [Har77, Chapter II, Proposition 6.11, Remark 6.11.2]. Therefore, we may assume that there is an open cover $S = \cup U_i$ and rational functions h_i such that the Cartier divisor defined by $\{(U_i, h_i)\}$ is N. Since N is effective, we may further assume that h_i are regular functions on U_i. Since $F \not\subset \mathrm{Supp}(N)$, the restricted divisor $N|_F$ is well-defined. Moreover F is non-singular. Hence we have that $N|_F$ is given by the Cartier divisor $\{(U_i \cap F, h_i|_F)\}$ on F, corresponding to the open cover $F = \cup(U_i \cap F)$ and the restricted regular functions $h_i|_F$.

Now, for any point (or a prime divisor) P on F, the coefficient of P in the divisor $N|_F$ is given by $\nu_P(h_i|_F)$ where $P \in U_i \cap F$. Now, the local ring $\mathcal{O}_{P,F}$ is a DVR. Hence, we have that $\nu_P(h_i|_F) = \mathrm{length}(\mathcal{O}_{P,F}/(h_i))$. Let f be a local equation of F in a neighbourhood of P in S. Now, we have $\mathcal{O}_{P,F} = \mathcal{O}_{P,S}/(f)$. Therefore the coefficient of P in $N|_F$ is given by

$$\nu_P(h_i|_F) = \mathrm{length}(\mathcal{O}_{P,F}/(h_i)) = \mathrm{length}(\mathcal{O}_{P,S}/(f, h_i)) = (N \cdot F)_P.$$

(2) Let $f, g, h \in \mathcal{O}_{P,S}$ denote the local equations of F, E, N at P respectively. We have a surjection $\mathcal{O}_{P,S}/(g, h) \to \mathcal{O}_{P,S}/(f, g, h)$. Therefore, we have

$$(N \cdot E)_P = \mathrm{length}(\mathcal{O}_{P,S}/(g, h)) \geq \mathrm{length}(\mathcal{O}_{P,S}/(f, g, h)).$$

Since F is non-singular, the local ring $\mathcal{O}_{P,S}/(f) \simeq \mathcal{O}_{P,F}$ is a DVR. Without loss of generality assume that $(E \cdot F)_P \leq (N \cdot F)_P$. Then we have that g divides h in $\mathcal{O}_{P,S}/(f)$. Therefore $\mathcal{O}_{P,S}/(f, g, h) \simeq \mathcal{O}_{P,S}/(f, g)$, and hence we have

$$(N \cdot E)_P = \mathrm{length}(\mathcal{O}_{P,S}/(g, h)) \geq \mathrm{length}(\mathcal{O}_{P,S}/(f, g)) = (E \cdot F)_P.$$

(3) Since $N|_F - E|_F$ is an effective divisor, we have that $(N \cdot F)_P \geq (E \cdot F)_P$ for all $P \in F$. If $P \in E \cap F$, the $(E \cdot F)_P \geq 1$. Hence we also have $(N \cdot F)_P \geq 1$ and $P \in N \cap F$. Moreover, by part (2), we have $(N \cdot E)_P \geq (E \cdot F)_P$.

□

In the following result, we note intersection properties of fibers of projection morphisms in a product surface.

Proposition 4.13. *Let X, Y be irreducible non-singular projective algebraic curves over $\overline{\mathbb{F}_q}$. Let $\pi_1 : X \times Y \to X$ and $\pi_2 : X \times Y \to Y$ be the projection morphisms. Let $x_1, x_2 \in X$ and $y_1, y_2 \in Y$ be distinct pairs of points. Let $F_i = \pi_1^{-1}(x_i)$ and $G_j = \pi_2^{-1}(y_j)$ be the fibers of the projection morphisms. Then we have the following.*

1. *We have $F_1 \cdot C = F_2 \cdot C$ for any irreducible curve $C \subseteq S$, and similarly for G_1 and G_2.*
2. *We have $F_1 \cdot F_2 = 0$, $G_1 \cdot G_2 = 0$ and $F_i \cdot G_j = 1$ for all $i, j \in [2]$.*
3. *For any effective divisor E, we have $E \cdot F_i \geq 0$ and $E \cdot G_j \geq 0$.*

Proof. (1) We note that any two fibers F_1, F_2 are algebraically equivalent and hence numerically equivalent [Har77, Chapter V, Exercise 1.7].

(2) Since $x_1 \neq x_2$, we have $F_1 \cap F_2 = \emptyset$. Hence $F_1 \cdot F_2 = 0$. Similarly for G_1 and G_2. Furthermore, F_i, G_j intersect transversely at the point (x_i, y_j) hence $F_i \cdot G_j = 1$.

(3) We may write $E = E' + mF_i$, where $F_i \not\subseteq \mathrm{Supp}(E')$. Then $E' \cap F_i \geq 0$, as these are effective divisors without common component Theorem 4.11. Since $F_i \cdot F_i = F_i \cdot F_j = 0$ for $i \neq j$, we see that $E \cdot F_i \geq 0$. Similarly we have $E \cdot G_j \geq 0$. □

In a product surface $X \times Y$, the fibers play the role of axis-parallel lines in $\overline{\mathbb{F}_q}^2$. Using this perspective, we can generalize the concept of bi-degree of bivariate polynomials in $\overline{\mathbb{F}_q}[x, y]$.

Definition 4.14. Let X, Y be irreducible non-singular projective algebraic curves over $\overline{\mathbb{F}_q}$. Let $D \in \mathrm{Div}(X \times Y)$. We will say that D is of type (e, f), if $D \cdot F = f$ and $D \cdot G = e$ for some (and, hence all) fibers $F = \pi_1^{-1}(x)$ and $G = \pi_2^{-1}(y)$, where $x \in X$ and $y \in Y$.

In the following result, we note properties of the type of divisors defined above. In particular, there is an upper bound for the self-intersection number $D^2 := D \cdot D$ in terms of the type of a divisor D. This will be crucial for obtaining our replacement of the Bezout-type bounds for the product surface $X \times Y$ in the proof of the generalized divisibility in Lemma 5.3.

Proposition 4.15. *Let X, Y be irreducible non-singular projective algebraic curves over $\overline{\mathbb{F}_q}$. Let $\pi_1 : X \times Y \to X$ and $\pi_2 : X \times Y \to Y$ be the projection morphisms. Let $F = \pi_1^{-1}(x)$ and $G = \pi_2^{-1}(y)$, for some $x \in X$ and $y \in Y$. Then we have the following.*

1. *Let $D \in \mathrm{Div}(X \times Y)$ be a divisor such that $D \sim aF + bG$ for some $a, b \in \mathbb{Z}$, where $\sim$ denotes linear equivalence. Then*
   (a) *D is of type (a, b), i.e. $D \cdot F = b$ and $D \cdot G = a$.*
   (b) *If $a, b > 0$, then $D \cdot E > 0$ for any effective divisor E.*
2. *If $D \in \mathrm{Div}(X \times Y)$ is an effective divisor of type $(0, 0)$, then $D = 0$.*
3. *Let $E, B \in \mathrm{Div}(X \times Y)$ be divisors of type (e, f) and (a, b) respectively. Suppose that $E - B$ is an effective divisor. Then we have $a \leq e$ and $b \leq f$.*
4. *Let $D \in \mathrm{Div}(X \times Y)$ be of type (e, f). Then we have $D^2 \leq 2ef$.*

Proof. (1.a) We have $D \cdot F = (aF + bG) \cdot F = aF \cdot F + bG \cdot F = b$. Similarly we have $D \cdot G = a$.

(1.b) By [Har77, Chapter V, Exercise 1.9.b], we know that $F + G$ is an ample divisor. Therefore, $(F + G) \cdot E > 0$ for any effective divisor E by [Har77, Chapter V, Theorem 1.10]. If $a, b > 0$, then we have $D \cdot E = (F + G) \cdot E + (a - 1)F \cdot E + (b - 1)G \cdot E$. Now, $F \cdot E \geq 0$ and $G \cdot E \geq 0$ by Proposition 4.13.

(2) If D is an effective divisor of type $(0, 0)$, then we have $D \cdot (F + G) = 0$. This is a contradiction if $D \neq 0$, since $(F + G) \cdot D > 0$ by part (1.b).

(3) Since $E - B$ is effective, we have $(E - B) \cdot F = E \cdot F - B \cdot F = f - b \geq 0$ by Proposition 4.13. Similarly we have $a \leq e$.

(4) This is the content of [Har77, ChapterV, Exercise 1.9.b].

□

5 Generalized divisibility for AG codes

In this section we will prove our generalized divisibility result in Lemma 5.3. Along the way we will generalize other intermediate steps of [PS94] to the setting of AG codes. We start with the following lemma which is a geometric generalization of [PS94, Lemma 4].

Lemma 5.1. *Let $C_{\mathcal{L}}(X, D_1, H_1)$ and $C_{\mathcal{L}}(Y, D_2, H_2)$ be two AG codes of length n over $\mathbb{F}_q$, with $D_1 = \sum_i x_i$ and $D_2 = \sum_j y_j$. Let M_1, M_2 be divisors on X, Y respectively such that $\deg(M_i) + \deg(H_i) < n$ and $\mathrm{Supp}(M_i) \cap \mathrm{Supp}(D_i) = \emptyset$. Suppose $N \in C_{\mathcal{L}}(X, D_1, M_1 + H_1) \otimes C_{\mathcal{L}}(Y, D_2, M_2 + H_2)$, $E \in C_{\mathcal{L}}(X, D_1, M_1) \otimes C_{\mathcal{L}}(Y, D_2, M_2)$, $R \in C_{\mathcal{L}}(X, D_1, H_1) \otimes \mathbb{F}_q^n$ and $C \in \mathbb{F}_q^n \otimes \mathcal{C}_{\mathcal{L}}(Y, D_2, H_2)$ are non-zero codewords such that*

$$E(x_i, y_j)R(x_i, y_j) = E(x_i, y_j)C(x_i, y_j) = N(x_i, y_j)$$

for all $i, j \in [n]$.

Let $F_i = \pi_1^{-1}(x_i)$ and $G_j = \pi_2^{-1}(y_j)$ be the fibers of the projection morphisms $\pi_1 : X \times Y \to X$ and $\pi_2 : X \times Y \to Y$. Let $N, E \in \mathrm{Div}(\overline{X} \times \overline{Y})$ denote the divisors associated to the codewords N, E respectively. Then we have the following.

1. *If $F_i \subseteq \mathrm{Supp}(E)$ for some $i \in [n]$, then $F_i \subseteq \mathrm{Supp}(N)$. Similarly, if $G_j \subseteq \mathrm{Supp}(E)$, then $G_j \subseteq \mathrm{Supp}(N)$.*
2. *Let $i \in [n]$ be such that $F_i \not\subseteq \mathrm{Supp}(N)$. Then the restricted divisor $N|_{F_i} - E|_{F_i}$ is effective. Similarly, if $G_j \not\subseteq \mathrm{Supp}(N)$ for some $j \in [n]$, then $N|_{G_j} - E|_{G_j}$ is effective.*

Proof. Since N, E are non-zero codewords, we note that the associated divisors are well-defined by Proposition 4.6. Then the divisor associated to the codeword N, which we also denoted by N, is given by $\mathrm{div}(\theta(N)) + \pi_1^*(M_1+H_1) + \pi_2^*(M_2+H_2)$. Thus we have the linear equivalence $N \sim \pi_1^*(M_1+H_1) + \pi_2^*(M_2+H_2)$. Moreover, the divisor N is effective by construction. Therefore the possible poles of the rational function $\theta(N)$ must be contained in $\pi_1^*(M_1+H_1) + \pi_2^*(M_2+H_2)$ by Lemma 4.10. Similarly we have $E \sim \pi_1^* M_1 + \pi_2^* M_2$ and the only possible poles of E are contained $\pi_1^* M_1 + \pi_2^* M_2$. In other words, if a curve B appears with negative coefficient in the divisor $\mathrm{div}(\theta(N))$, then we have $B \subseteq \mathrm{Supp}(\pi_1^*(M_1+H_1) + \pi_2^*(M_2+H_2))$. Similarly for $\mathrm{div}(\theta(E))$. Fix $i \in [n]$ and let $\iota : F_i \hookrightarrow \overline{X} \times \overline{Y}$ be the inclusion map. Note that $\pi_2 \circ \iota : F_i \xrightarrow{\sim} \overline{Y}$ is an isomorphism.

(1) Now suppose that $F_i \subseteq \mathrm{Supp}(E)$. Note that F_i can not have negative coefficient in $\mathrm{div}(\theta(E))$. Indeed, we have $F_i \subseteq \mathrm{Supp}(\pi_1^* D_1)$ and $\mathrm{Supp}(\pi_1^* D_1) \cap \mathrm{Supp}(\pi_1^* M_1) = \emptyset$. Moreover, F_i dominates $\overline{Y}$ under the projection π_2, whereas $\pi_2^* M_2$ does not. Therefore, as F_i is in the support of E, we must have that $\mathrm{coeff}_{F_i}(\mathrm{div}(\theta(E))) > 0$. Then $\theta(E)(x_i, y_j) = 0$ for all $j \in [n]$ by Lemma 4.10. Therefore $E(x_i, y_j) = \theta(E)(x_i, y_j) = 0$ for all y_j by Corollary 4.4. Hence we have $\theta(N)(x_i, y_j) = N(x_i, y_j) = E(x_i, y_j)R(x_i, y_j) = 0$ for all $j \in [n]$. If $F_i \not\subseteq \mathrm{Supp}(N)$, then $\iota^*(\theta(N))$ is a well-defined non-zero rational function. Moreover the divisor $N|_{F_i}$ is well-defined effective divisor by Lemma 4.12. Since $N|_{F_i} = \mathrm{div}(\iota^*(\theta(N))) + M_2 + H_2$ on F_i, we have $\iota^*(\theta(N)) \in \mathcal{L}(F_i, M_2 + H_2)$. This is a contradiction, since $\deg(M_2 + H_2) < n$ and $\iota^*(\theta(N))$ vanishes on n number of points (x_i, y_j) on F_i.

(2) Now suppose that $F_i \not\subseteq \mathrm{Supp}(N)$. Then we also have $F_i \not\subseteq \mathrm{Supp}(E)$ by part (1). Hence, $\iota^*(\theta(N)), \iota^*(\theta(E))$ are non-zero rational functions on F_i. Furthermore, we have the restricted divisors given by $N|_{F_i} = \mathrm{div}(\iota^*(\theta(N))) + M_2 + H_2$ and $E|_{F_i} = \mathrm{div}(\iota^*(\theta(E))) + M_2$. Since $C \in \mathbb{F}_q^n \otimes C_{\mathcal{L}}(Y, D_2, H_2)$, we know that the i-th column $C_i \in C_{\mathcal{L}}(Y, D_2, H_2)$ is a codeword. Therefore, by using the isomorphism in Lemma 4.2, we have a non-zero rational function $\gamma_i := \varphi_{F_i}^{-1}(C_i) \in \mathcal{L}(F_i, H_2)$.

We will show that $\iota^*(\theta(N)) = \iota^*(\theta(E)) \cdot \gamma_i$ as rational functions in the function field $\overline{\mathbb{F}_q}(F_i)$. Then we will have $\mathrm{div}(\iota^*(\theta(N)) = \mathrm{div}(\iota^*(\theta(E))) + \mathrm{div}(\gamma_i)$. Hence we will have that $N|_{F_i} - E|_{F_i} = \mathrm{div}(\gamma_i) + H_2$ is effective, since $\gamma \in \mathcal{L}(F_i, H_2)$. The rest of the proof will be devoted to showing that $\iota^*(\theta(N)) - \iota^*(\theta(E)) \cdot \gamma_i = 0$ as a rational function in $\overline{\mathbb{F}_q}(F_i)(F_i)$.

Note that $\iota^*(\theta(E)) \cdot \gamma_i \in \mathcal{L}(F_i, M_2 + H_2)$. Therefore, $\iota^*(\theta(N)) - \iota^*(\theta(E)) \cdot \gamma_i \in \mathcal{L}(F_i, M_2 + H_2)$. Note that by Corollary 4.4, we have that $\iota^*(\theta(N))(x_i, y_j) = N(x_i, y_j)$ and $\iota^*(\theta(E))(x_i, y_j) = E(x_i, y_j)$ for all

$j \in [n]$. Since $\gamma_i \in \mathcal{L}(F_i, H_2)$, the only possible poles of γ_i are contained in $\mathrm{Supp}(H_2)$. Hence, the rational function γ_i is defined at $(x_i, y_j) \in F_i$ for $j \in [n]$. Moreover, we have $\gamma_i(x_i, y_j) = C(x_i, y_j)$, since the codeword C_i is the evaluation of the rational function γ_i, by definition of γ_i. Therefore, on the curve F_i, we have $(\iota^*(\theta(N)) - \iota^*(\theta(E)) \cdot \gamma_i)(x_i, y_j) = 0$ for all $j \in [n]$. If $\iota^*(\theta(N)) - \iota^*(\theta(E)) \cdot \gamma_i \neq 0$, then this is a contradiction, as $\deg(M_2 + H_2) < n$ and $\iota^*(\theta(N)) - \iota^*(\theta(E)) \cdot \gamma_i \in \mathcal{L}(F_i, M_2 + H_2)$. Therefore we must have that $\iota^*(\theta(N)) - \iota^*(\theta(E)) \cdot \gamma_i = 0$ as desired.

□

The following result provides a lower-bound on the intersection number $N \cdot E$ in terms of the type of the divisors N, E. This lower bound is generalizes the lower bound obtained in the proof of special bivariate divisibility in Lemma 3.1.

Lemma 5.2 (Lower bound for intersection product)**.** *Let X, Y be irreducible non-singular projective algebraic curves over $\overline{\mathbb{F}}_q$. Let $x_1, \cdots, x_n \in X$ be points with corresponding fibers $F_i = \pi_1^{-1}(x_i)$ in $X \times Y$. Let $N, E \in \mathrm{Div}(X \times Y)$ be effective divisors of type (d, e) and (a, b) respectively. Suppose that the following conditions hold.*

1. *We have $a, b, d, e \geq 0$ and $e \geq b$.*
2. *The divisors N, E do not have any common components.*
3. *For all fibers F_i such that $F_i \not\subseteq \mathrm{Supp}(N)$, the restricted divisor $N|_{F_i} - E|_{F_i}$ is an effective divisor on the curve F_i.*

Then we have

$$N \cdot E \geq nE \cdot F_i = nb$$

Proof. First we will reduce to the case where none of the fibers F_i are in $\mathrm{Supp}(N)$. Suppose that r of the fibers F_i are in Supp(N). Without loss of generality, suppose $F_1, \cdots, F_r \subseteq \mathrm{Supp(N)}$ and let $f_i = \mathrm{mult}_N(F_i) \geq 1$. Then we have that $N' := N - (f_1F_1 + \cdots + f_rF_r)$ is an effective divisor. Now the divisor N' is of type $(d-f, e)$, where $f = f_1 + \cdots + f_r$. We also have that the fibers $F_i \not\subseteq \mathrm{Supp}(N')$ for all $i \in [n]$. Furthermore, for all $r+1 \leq j \leq n$, we have that $N|_{F_j} = N'|_{F_j}$, since $F_i \cap F_j = \emptyset$ for $i \in [r]$. Hence we have that $N'|_{F_j} - E|_{F_j}$ is effective for all $r+1 \leq j \leq n$. Since $E \cdot F_i = b$, we have that

$$N \cdot E = N' \cdot E + (f_1 + \cdots + f_r)b \geq N' \cdot E + rb.$$

Therefore it is enough to show that $N' \cdot E \geq (n-r)b$. Hence we may replace N by N' and n by $(n-r)$, and assume that none of the fibers F_i are in $\mathrm{Supp}(N)$.

Now we will reduce to the case where none of the fibers are in $\mathrm{Supp}(E)$. Without loss of generality, suppose that $F_1, \cdots, F_s \subseteq \mathrm{Supp}(E)$ for some $1 \leq s \leq n$. Let $c_i = \mathrm{mult}_E(F_i)$. Then we may write $E' := E - (c_1F_1 + \cdots + c_sF_s)$, where none of the fibers are in $\mathrm{Supp}(E')$. Note that E' is of type $(a-c, b)$, where $c = c_1 + \cdots + c_s$. We also have that $E|_{F_j} = E'|_{F_j}$ for all $s+1 \leq j \leq n$. Now, since $N \cdot F_i = e$, we have

$$N \cdot E = N \cdot E' + (c_1 + \cdots + c_s)e \geq N \cdot E' + sb.$$

Therefore it is enough to show that $N \cdot E' \geq (n-s)b$, and hence we may replace E by E' and n by $n-s$.

Now we may assume that $F_i \not\subseteq \mathrm{Supp}(N) \cup \mathrm{Supp}(E)$ for all $i \in [n]$. Since N, E do not have common components, we have that $N \cdot E = \sum_{P \in N \cap E} (N \cdot E)_P$ by Theorem 4.11. Similarly, $E \cdot F_i = \sum_{P \in E \cap F_i} (E \cdot F_i)_P$ for all fibers $i \in [n]$. Note that $E|_{F_i} = \sum_{P \in E \cap F_i} (E \cdot F_i)_P \cdot P$ and $N|_{F_i} = \sum_{P \in N \cap F_i} (N \cdot F_i)_P \cdot P$ by Lemma 4.12. Since $N|_{F_i} - E|_{F_i}$ is effective for all $i \in [n]$, we have that $(N \cdot F_i)_P \geq (E \cdot F_i)_P$ and $F_i \cap E \subset F_i \cap N$ by Lemma 4.12. In particular, $F_i \cap E \cap N = F_i \cap E$ for all $i \in [n]$. Furthermore, we have that $(N \cdot E)_P \geq (E \cdot F_i)_P$ for all $P \in F_i \cap E \cap N$ by Lemma 4.12. Note that $F_i \cap F_j = \emptyset$ for $1 \leq i \neq j \leq n$. Therefore we have

$$N \cdot E = \sum_{P \in N \cap E} (N \cdot E)_P \geq \sum_{i=1}^{n} \sum_{P \in F_i \cap N \cap E} (N \cdot E)_P \geq \sum_{i=1}^{n} \sum_{P \in F_i \cap E} (E \cdot F_i)_P = nb.$$

□

The following result is a generalization of the bivariate divisibility results in Lemma 1.3 and Lemma 3.1.

Lemma 5.3 (Generalized divisibility for AG codes)**.** *Let $C_{\mathcal{L}}(X, D_1, H_1), C_{\mathcal{L}}(X, D_1, M_1)$ and $C_{\mathcal{L}}(Y, D_2, H_2), C_{\mathcal{L}}(Y, D_2, M_2)$ be AG codes of length n over $\mathbb{F}_q$, with $D_1 = \sum_i x_i$ and $D_2 = \sum_j y_j$. Suppose $N \in C_{\mathcal{L}}(X, D_1, M_1 + H_1) \otimes C_{\mathcal{L}}(Y, D_2, M_2 + H_2)$, $E \in C_{\mathcal{L}}(X, D_1, M_1) \otimes C_{\mathcal{L}}(Y, D_2, M_2)$, $R \in C_{\mathcal{L}}(X, D_1, H_1) \otimes \mathbb{F}_q^n$ and $C \in \mathbb{F}_q^n \otimes \mathcal{C}_{\mathcal{L}}(Y, D_2, H_2)$ are non-zero codewords. Suppose that the following two conditions hold.*

1. *We have $n > \deg(M_1) + \deg(H_1) + \deg(M_2) + \deg(H_2)$.*
2. *We have*
$$E(x_i, y_j)R(x_i, y_j) = E(x_i, y_j)C(x_i, y_j) = N(x_i, y_j)$$
for all $i, j \in [n]$.

Then there exists a codeword $Q \in C_{\mathcal{L}}(X, D_1, H_1) \otimes C_{\mathcal{L}}(Y, D_2, H_2)$ such that

$$N(x_i, y_j) = E(x_i, y_j)Q(x_i, y_j)$$

for all $i, j \in [n]$.

Proof. Let $\deg(M_i) = m_i$ and $\deg(H_i) = \ell_i$. Let $N, E \in \mathrm{Div}(\overline{X} \times \overline{Y})$ be the divisors corresponding to the codewords N, E respectively. Note that the divisors N, E are of type $(m_1+\ell_1, m_2+\ell_2)$ and (m_1, m_2) respectively, by Proposition 4.15. Let $\mathrm{Supp}(N) \cap \mathrm{Supp}(E) = \{B_1, \cdots, B_r\}$ and $a_i = \mathrm{mult}_N(B_i)$, $b_i = \mathrm{mult}_E(B_i)$ be the corresponding multiplicities. Let B be the common part of N, E, i.e. $B = \sum_{i=1}^r \min\{a_i, b_i\}B_i$. Let $N' = N - B$ and $E' = E - B$. In the following we will show that $E' = 0$.

Note that N', E' are without common components, by construction. Suppose that B is of type (e, f). Then we know that $e \leq m_1$ and $f \leq m_2$ by Proposition 4.15.

Moreover, we have that N' is of type $(m_1 - e + \ell_1, m_2 - f + \ell_2)$, and similarly E' is of type $(m_1 - e, m_2 - f)$. Let $F_i = \pi_1^{-1}(x_i)$ be the fibers of the projection $\pi_1 : X \times Y \to X$. Without loss of generality, suppose that $F_1, \cdots, F_r \in \mathrm{Supp}(B)$. Then $B - (F_1 + \cdots + F_r)$ is effective, and we have

$$e = B \cdot G \geq (F_1 + \cdots + F_r) \cdot G = r,$$

where G denotes the class of a fiber of the second projection, i.e. $G = \pi_2^{-1}(y)$ for some y. Therefore, at most e of the fibers can be in $\mathrm{Supp}(B)$, and after re-indexing, we may assume that $F_i \not\subseteq \mathrm{Supp}(B)$ for all $1 \leq i \leq (n - e)$.

By Lemma 5.1, we know that for any $F_i \not\subseteq \mathrm{Supp}(N)$, we have that $F_i \not\subseteq \mathrm{Supp}(E)$ and the restricted divisor $N|_{F_i} - E|_{F_i}$ is effective. Now, we have

$$N|_{F_i} - E|_{F_i} = (N' + B)|_{F_i} - (E' + B)_{F_i} = N'|_{F_i} - E'|_{F_i}.$$

Now suppose that $F_i \notin \mathrm{Supp}(N')$ for some $i \in [n - e]$. Since $F_i \not\subseteq \mathrm{Supp}(B)$, we have $F_i \not\subseteq \mathrm{Supp}(N)$. Thus we have that $N'|_{F_i} - E'|_{F_i}$ is effective for any $F_i \not\subseteq \mathrm{Supp}(N')$ where $i \in [n - e]$. Therefore, by applying Lemma 5.2 to the divisors N', E' and the first $(n - e)$ fibers F_i, we obtain that

$$N' \cdot E' \geq (n - e)(m_2 - f). \tag{1}$$

Similarly, by applying the argument to the fibers $G_i = \pi_2^{-1}(y_i)$, we obtain that

$$N' \cdot E' \geq (n - f)(m_1 - e). \tag{2}$$

Now we have

$$N' \cdot E' = (N - B) \cdot (E - B) = N \cdot (E - B) - E \cdot B + B^2.$$

We have that $N \sim \pi_1^*(M_1+H_1)+\pi_2^*(M_2+H_2)$ and $E \sim \pi_1^* M_1 + \pi_2^* M_2$, which are of type $(m_1+\ell_1, m_2+\ell_2)$ and (m_1, m_2) respectively. By Proposition 4.15, we know that $B^2 \leq 2ef$. Hence we have

$$\begin{aligned} N' \cdot E' &= N \cdot (E-B) - E \cdot B + B^2 \\ &= (m_1+\ell_1)(m_2-f) + (m_2+\ell_2)(m_1-e) - m_1 f - m_2 e + B^2 \\ &\leq (m_1+\ell_1)(m_2-f) + (m_2+\ell_2)(m_1-e) - m_1 f - m_2 e + 2ef \\ &= (m_2-f)(m_1+\ell_1-e) + (m_1-e)(m_2+\ell_2-f). \end{aligned} \tag{3}$$

Hence we have the inequality

$$N' \cdot E' \leq (m_2-f)(m_1+\ell_1-e) + (m_1-e)(m_2+\ell_2-f). \tag{4}$$

Now we will show that we must have $m_1 = e$ and $m_2 = f$.

Case 1. Suppose that $m_1 = e$ *or* $m_2 = f$. Without loss of generality we may assume that $m_1 = e$. Then we have $N' \cdot E' \leq (m_2-f)\ell_1$ by inequality (4). However, we also know that $N' \cdot E' \geq (n-e)(m_2-f)$ by inequality (1). If $m_2 \neq f$ then this is a contradiction, since $n > m_1 + \ell_1$ by assumption and $m_1 \geq e$. Therefore in this case we must also have $m_2 = f$, as desired.

Case 2. Suppose that $m_1 \neq e$ *and* $m_2 \neq f$. Since $n > m_1+\ell_1+m_2+\ell_2$, we have $n-e > (m_1+\ell_1-e)+(m_2+\ell_2)$ and $n-f > (m_2+\ell_2-f)+(m_1+\ell_1)$. Since $m_1-e > 0$ and $m_2-f > 0$, we have strict inequalities

$$(n-e)(m_2-f) > (m_1+\ell_1-e)(m_2-f) + (m_2+\ell_2)(m_2-f) \tag{5}$$

$$(n-f)(m_1-e) > (m_2+\ell_2-f)(m_1-e) + (m_1+\ell_1)(m_1-e) \tag{6}$$

Now the inequalities (1),(4) and (5) imply that we must have

$$(m_1-e)(m_2+\ell_2-f) > (m_2+\ell_2)(m_2-f). \tag{7}$$

Similarly, inequalities (2),(4) and (6) imply that

$$(m_2-f)(m_1+\ell_1-e) > (m_1+\ell_1)(m_1-e) \tag{8}$$

Now inequality (7) implies that $(m_1-e) > (m_2-f)$. Similarly, inequality (8) implies that $(m_2-f) > (m_1-e)$. This is a contradiction. Hence we must have that $m_1 = e$ and $m_2 = f$.

Now, we note that $E' = E - B$ is an effective divisor of type $(0,0)$. Hence $E' = 0$, by Proposition 4.15. Since $E' = 0$, then we have that $N - E$ is a non-zero effective divisor and $N - E \sim \pi_1^* H_1 + \pi_2^* H_2$. We recall that the divisors $N, E \in \mathrm{Div}(\overline{X} \times \overline{Y})$ are defined over the base field $\mathbb{F}_q$ by Remark 4.9. Hence $N - E$ is an $\mathbb{F}_q$-rational divisor and let $g \in \mathcal{L}_{\mathbb{F}_q}(X \times Y, \pi_1^* H_1 + \pi_2^* H_2)$ be the corresponding rational function. Hence, it suffices to let $Q \in C_{\mathcal{L}}(X, D_1, H_1) \otimes C_{\mathcal{L}}(Y, D_2, H_2)$ be the codeword associated to $N - E$. More specifically, we let $Q = (\theta_{\mathbb{F}_q})^{-1}(g)$, where $\theta_{\mathbb{F}_q}$ is the isomorphism given by Lemma 4.7.

□

6 Main result and applications

First we prove our generalization of the bivariate testing result of [PS94, Theorem 9]. Given our generalized divisibility lemma (see Lemma 5.3), the following result is obtained by adapting the combinatorial argument in [PS94].

Theorem 6.1. *Fix $0 \leq \epsilon \leq 1$. Let $C_{\mathcal{L}}(X, D_1, H_1)$ and $C_{\mathcal{L}}(Y, D_2, H_2)$ be AG codes of length n over $\mathbb{F}_q$ and genus g_1, g_2 respectively. Let $D_1 = \sum_i x_i$ and $D_2 = \sum_j y_j$. Let $R \in C_{\mathcal{L}}(X, D_1, H_1) \otimes \mathbb{F}_q^n$ and $C \in \mathbb{F}_q^n \otimes C_{\mathcal{L}}(Y, D_2, H_2)$ be codewords such that $\delta(R, C) = \epsilon$. Suppose that $n > 2\sqrt{\epsilon} n + g_1 + g_2 + 4 + \deg(H_1) + \deg(H_2)$. Then there exists a codeword $Q \in C_{\mathcal{L}}(X, D_1, H_1) \otimes C_{\mathcal{L}}(Y, D_2, H_2)$ such that the set*

$$A = \{(x_i, y_j) \mid R(x_i, y_j) \neq Q(x_i, y_j) \text{ or } C(x_i, y_j) \neq Q(x_i, y_j)\},$$

satisfies

$$|A| \leq 2\epsilon n^2.$$

In particular, we have $\delta(R,Q) + \delta(Q,C) \leq 4\epsilon$.

Proof. For simplicity, we will alternatively use $(i,j) \in [n] \times [n]$ in place of (x_i, y_j). We define

$$T = \{(x,y) \in [n] \times [n] \mid R(x,y) \neq C(x,y)\}.$$

Let $d_i = \lceil \sqrt{\epsilon} n + g_i + 1 \rceil$. Choose $\mathbb{F}_q$-rational divisors M_1, M_2 on X, Y respectively such that $\deg(M_i) = d_i$ and $\mathrm{Supp}(M_i) \cap \mathrm{Supp}(D_i) = \emptyset$. For instance, we may choose a point $x \notin \mathrm{Supp}(D_1)$ and let $M_1 = d_1 x$. By Lemma 2.6, there exists a non-zero codeword $E \in C_{\mathcal{L}}(X, D_1, M_1) \otimes C_{\mathcal{L}}(Y, D_2, M_2)$ such that $E(x,y) = 0$ for all $(x,y) \in T$. Furthermore, there exists a non-zero $N \in C_{\mathcal{L}}(X, D_1, M_1 + H_1) \otimes C_{\mathcal{L}}(Y, D_2, M_2 + H_2)$ such that

$$E(x,y)R(x,y) = E(x,y)C(x,y) = N(x,y)$$

for all $(x,y) \in [n] \times [n]$. Now, $n > d_1 + d_2 + \deg(H_1) + \deg(H_2)$. Therefore, by Lemma 5.3, there exists a codeword $Q \in C_{\mathcal{L}}(X, D_1, H_1) \otimes C_{\mathcal{L}}(Y, D_2, H_2)$ such that

$$E(x,y)R(x,y) = E(x,y)C(x,y) = Q(x,y)E(x,y)$$

for all $(x,y) \in [n] \times [n]$.

Let us call a row good if R agrees with Q everywhere on that row. Similarly, we call a column good if C agrees with Q everywhere on that column. Otherwise, we call the row or column bad. Let b_r be the number of bad rows and b_c be the number of bad columns.

First, we will show that $b_c \leq d_1$ and $b_r \leq d_2$. We know that if $E(x,y) \neq 0$, then $R(x,y) = Q(x,y) = C(x,y)$. Suppose that E is not identically zero on the i-th column. Then $E(x_j, y_i) = 0$ for at most d_2 values of x_j, as the i-th column of E is a codeword in $C_{\mathcal{L}}(Y, D_2, M_2)$. Therefore, for at least $n - d_2 > \deg(H_2)$ values of x_j, we have $E(x_j, y_i) \neq 0$, and consequently $Q(x_j, y_i) = R(x_j, y_i)$. Since $Q \in C_{\mathcal{L}}(X, D_1, H_1) \otimes C_{\mathcal{L}}(Y, D_2, H_2)$ and $C \in \mathbb{F}_q^n \otimes C_{\mathcal{L}}(X, D_2, H_2)$, we conclude that $Q(x_j, y_i) = C(x_j, y_i)$ everywhere on the i-th column. Hence, if E is not identically zero on a column, it must be a good column. Since E can be identically zero on at most d_1 number of columns, we conclude that $b_c \leq d_1$. Similarly, we have $b_r \leq d_2$.

Recall that

$$A = \{(x,y) \in [n] \times [n] \mid R(x,y) \neq Q(x,y) \text{ or } C(x,y) \neq Q(x,y)\}.$$

We define

$$Z = \{(x,y) \in [n] \times [n] \mid R(x,y) = C(x,y) \text{ and } R(x,y) \neq Q(x,y)\}.$$

Then we have $A \subseteq T \sqcup Z$, and hence $|A| \leq |T| + |Z|$. Since $|T| = \epsilon n^2$, it is enough to show that $|Z| \leq |T|$. Note that all entries of Z must lie in bad rows and bad columns, since $R(x,y) = C(x,y) \neq Q(x,y)$ for all $(x,y) \in Z$.

Case 1. Suppose that $d_1 + \deg(H_1) \geq d_2 + \deg(H_2)$. Then we have $n > 2(\deg(H_2) + d_2)$. In particular, $n - \deg(H_2) - d_2 > \frac{n}{2}$. We will show that for any bad column, the number of entries from T is strictly larger than the number of entries from Z.

Note that C and Q can agree on at most $\deg(H_2)$ entries in a bad column. Otherwise $C = Q$ everywhere on that column, which is a contradiction. Therefore, there are at least $n - \deg(H_2) - b_r$ entries (x,y) in any bad column, such that $R(x,y) = Q(x,y)$ and $C(x,y) \neq Q(x,y)$. Hence, $R(x,y) \neq C(x,y)$, and $(x,y) \in T$ for all such (x,y). In particular, any bad column contains at least $n - \deg(H_2) - b_r \geq n - \deg(H_2) - d_2 > \frac{n}{2}$ number of entries from T. Hence, the number of entries from Z is smaller than the number of entries from T in any bad column. Hence $|Z| \leq |T|$, as Z is contained in the union of bad columns.

Case 2. Suppose that $d_2 + \deg(H_2) > d_1 + \deg(H_1)$. By the same argument as in Case 1, we conclude that for any bad row, the number of entries from T is strictly larger than the number of entries from Z. We are done similarly as Z is contained in the union of bad rows.

Therefore, we have $|Z| \leq |T|$ in both cases. This shows that $|A| \leq 2\epsilon n^2$. Now, note that if $R(x,y) \neq Q(x,y)$, then $(x,y) \in A$. Hence $\delta(R,Q) \leq 2\epsilon$. Similarly, we have $\delta(Q,C) \leq 2\epsilon$. Therefore we have $\delta(R,Q) + \delta(Q,C) \leq 4\epsilon$.

□

By a standard argument, Theorem 6.1 implies robust testability of tensor products of AG codes. For instance, the proof of [GSW24, Theorem 2.4] holds with minor modifications.

Theorem 6.2. *Let $c_0 > 1$ and $\rho = \frac{1}{3}(\frac{c_0-1}{2c_0})^2$. Let $C_{\mathcal{L}}(X, D_1, H_1)$ and $C_{\mathcal{L}}(Y, D_2, H_2)$ be two AG codes of length n, genus g_1, g_2 respectively over $\mathbb{F}_q$. Suppose that $n > c_0(g_1 + g_2 + 4 + \deg(H_1) + \deg(H_2))$. Then the tensor product code $C_{\mathcal{L}}(X, D_1, H_1) \otimes C_{\mathcal{L}}(Y, D_2, H_2)$ is ρ-robustly testable.*

Proof. Let $F \in \mathbb{F}_q^{n\times n}$. Let $R \in C_{\mathcal{L}}(X, D_1, H_1) \otimes \mathbb{F}_q^n$ and $C \in \mathbb{F}_q^n \otimes C_{\mathcal{L}}(Y, D_2, H_2)$ be the vectors closest to F in their respective codes. Let $\deg(H_i) = \ell_i$. Suppose that $\delta(R, C) = \epsilon$. We consider two cases as follows.

Case 1. Suppose that $\sqrt{\epsilon} < \frac{c_0-1}{2c_0}$. Then we have that $\frac{1}{1-2\sqrt{\epsilon}} < c_0$. Hence we have

$$n > c_0(g_1 + g_2 + 4 + \ell_1 + \ell_2) > \frac{1}{1-2\sqrt{\epsilon}}(g_1 + g_2 + 4 + \ell_1 + \ell_2).$$

Therefore, $n > 2\sqrt{\epsilon}n + g_1 + g_2 + 4 + \ell_1 + \ell_2$. By Theorem 6.1, we know that there exists $Q \in C_{\mathcal{L}}(X, D_1, H_1) \otimes C_{\mathcal{L}}(Y, D_2, H_2)$ such that $\delta(Q, R) + \delta(Q, C) \leq 4\epsilon$. Therefore we have

$$\begin{aligned}
\delta(F, Q) &\leq \min(\delta(F, R) + \delta(R, Q), \delta(F, C) + \delta(C, Q)) \\
&\leq \frac{1}{2}(\delta(F, R) + \delta(R, Q) + \delta(F, C) + \delta(C, Q)) \\
&\leq \frac{1}{2}(\delta(F, R) + \delta(F, C) + 4\epsilon) \\
&\leq \frac{5}{2}(\delta(F, R) + \delta(F, C)),
\end{aligned}$$

where the last inequality holds since $\epsilon = \delta(R, C) \leq \delta(F, R) + \delta(F, C)$. Hence we have that

$$\frac{1}{5}\delta(F, Q) \leq \frac{1}{2}(\delta(F, R) + \delta(F, C)).$$

In particular, $\rho \cdot \delta(F, Q) \leq \frac{1}{2}(\delta(F, R) + \delta(F, C))$, as $\rho < \frac{1}{5}$.

Case 2. Suppose that $\sqrt{\epsilon} \geq \frac{c_0-1}{2c_0}$. Then we have $\delta(R, C) \geq (\frac{c_0-1}{2c_0})^2 = 3\rho > 2\rho$ and hence $\rho \leq \frac{1}{2}\delta(R, C)$. Now we have

$$\rho \cdot \delta(F, Q) \leq \rho \leq \frac{1}{2}\delta(R, C) \leq \frac{1}{2}(\delta(F, R) + \delta(F, C)).$$

Therefore, we are done since $\delta(F, C_{\mathcal{L}}(X, D_1, H_1) \otimes C_{\mathcal{L}}(Y, D_2, H_2)) \leq \delta(F, Q)$, and $\delta(F, R) = \delta(F, C_{\mathcal{L}}(X, D_1, H_1) \otimes \mathbb{F}_q^n)$, $\delta(F, C) = \delta(F, \mathbb{F}_q^n \otimes C_{\mathcal{L}}(Y, D_2, H_2))$ by assumption.

□

We note the following reformulation of Theorem 6.2.

Corollary 6.3. *Let $\epsilon \in [0, 1)$ and $\rho(\epsilon) = \frac{\epsilon^2}{12}$. Let $C_{\mathcal{L}}(X, D_1, H_1)$ and $C_{\mathcal{L}}(Y, D_2, H_2)$ be two AG codes of length n, genus g_1, g_2 respectively over $\mathbb{F}_q$. If $4 + g_1 + \deg(H_1) + g_2 + \deg(H_2) < (1 - \epsilon)n$, then the tensor product code $C_{\mathcal{L}}(X, D_1, H_1) \otimes C_{\mathcal{L}}(Y, D_2, H_2)$ is $\rho(\epsilon)$-robustly testable.*

Proof. Let $c_0 = \frac{1}{1-\epsilon}$. Then $c_0 > 1$, and we have $c_0(4 + g_1 + \deg(H_1) + g_2 + \deg(H_2)) < n$. Hence Theorem 6.2 applies and we have $\rho(\epsilon) = \frac{\epsilon^2}{12}$.

□

Theorem 6.2 combined with the results of [GG24] directly yields new families of quantum CSS codes which are locally testable with constant soundness. [GG24, Corollary 4.4] proved the following result for quantum Reed-Solomon codes using the robust testability of Reed-Solomon codes [PS94]. As an application of our main result we obtain a generalization of their result to the setting of quantum AG codes. The proof of [GG24] goes through with our modified conditions on the parameters in this extended setting of AG codes. We provide more details here for convenience.

Proposition 6.4. *For any $\epsilon > 0$, there exist $\Delta(\epsilon) > 0$ and $\rho(\epsilon) > 0$ such that the following holds. For $i = 1, 2$, let $Q^i = (Q^i_X, Q^i_Z)$ be quantum AG codes of length n, rate R_i over a field $\mathbb{F}_q$ of characteristic 2 with the following conditions.*

1. *Q^i_X, Q^i_Z are AG codes of genus g and degrees $\ell_i \leq (1-\epsilon)n$.*
2. *$\dim(Q^i_X) = \dim(Q^i_Z)$.*
3. *$\ell_1 - \ell_2 > \epsilon n + 4g + 2$.*
4. *$\ell_1 + \ell_2 > (1+\epsilon)n + 6g$.*

Let $\mathcal{C}_i$ be the single-sector chain complex obtained from Q^i. Then the quantum CSS code associated with the homological product $\mathcal{A} = \mathcal{C}_1 \otimes \mathcal{C}_2$ is a $[[n^2, R_1R_2n^2, \Delta(\epsilon)n^2]]_q$ code that is locally testable with locality at most $2n$ and soundness at least $\rho(\epsilon)$.

Proof. Let $Q(\mathcal{A})$ denote the quantum code associated to the homological product complex $\mathcal{A}$. Since Q^i is a length n code, the single sector chain complex $\mathcal{C}_i = (C_i, \partial^{C_i})$ has $C = \mathbb{F}_q^n$. Since $\mathcal{A} = (C_1 \otimes C_2, \partial^{C_1} \otimes I + I \otimes \partial^{C_2})$ and $C_1 \otimes C_2 = \mathbb{F}_q^{n^2}$, we have that length of $Q(\mathcal{A})$ is n^2. Moreover, any row or column of the matrix $\partial^{C_1} \otimes I + I \otimes \partial^{C_2}$ has at most $2n$ non-zero entries. Hence the locality of the quantum code $Q(\mathcal{A})$ is at most $2n$. By the Künneth formula [BH14, Lemma 1] or [GG24, Proposition 3.23], we know that $H_*(\mathcal{A}) = H_*(\mathcal{C}_1) \otimes H_*(\mathcal{C}_2)$. Hence, by Proposition 2.9, we have $\dim(Q(\mathcal{A})) = \dim(Q^1)\dim(Q^2) = R_1R_2n^2$.

Therefore, it remains to compute the distance and soundness of $Q(\mathcal{A})$.

Distance bound. Recall that $d(Q(\mathcal{A})) = \min\{d_X(Q(\mathcal{A})), d_Z(Q(\mathcal{A}))\}$. First let us bound $d_Z(Q(\mathcal{A}))$. By Proposition 2.9, we have $B_*(\mathcal{C}_1) = (Q^1_X)^\perp$, and $Z_*(\mathcal{C}_2) = Q^2_Z$. Note that $(Q^1_X)^\perp$ and Q^2_Z are AG codes of genus g and degrees $(2g-2+n-\ell_1)$ and ℓ_2. By condition (3) and Corollary 6.3, we know that $(Q^1_X)^\perp \otimes Q^2_Z$ is $\rho(\epsilon)$-robust. By [GG24, Theorem 4.1], we have $d_Z(Q(\mathcal{A})) \geq \epsilon\rho(\epsilon)n^2$, as $d(Z_*(\mathcal{C}_1)) = d(Q^1_Z) \geq \epsilon n$.

Now we bound $d_X(Q(\mathcal{A}))$. By Proposition 2.9, we see that $d_X(Q(\mathcal{A})) = d_Z(Q(\mathcal{A}^*))$, where $\mathcal{A}^*$ is the associated cochain complex of $\mathcal{A}$. Now we will apply the above argument to $\mathcal{A}^*$. Note that $\mathcal{A}^* = \mathcal{C}_1^* \otimes \mathcal{C}_2^*$, and $\mathcal{C}_i^*$ is associated to the quantum code (Q^i_Z, Q^i_X). Therefore, $B_*(\mathcal{C}_1^*) = (Q^1_Z)^\perp$ and $Z_*(\mathcal{C}_2^*) = Q^2_X$, which are AG codes of genus g and degrees $(2g-2+n-\ell_1)$ and ℓ_2. Therefore, we are done by Corollary 6.3 as above. We let $\Delta(\epsilon) = \epsilon\rho(\epsilon)$.

Soundness bound. Now we check that the soundness is at least $\rho(\epsilon)$. By [GG24, Definition 3.13], the soundness of $Q(\mathcal{A})$ is given by $\rho(Q(\mathcal{A})) = \min\{\frac{1}{\mu_*(\mathcal{A})}, \frac{1}{\mu^*(\mathcal{A})}\}$, where μ_* and μ^* are the (co)filling constants.

Let us first show a lower bound on $\frac{1}{\mu_*(\mathcal{A})}$. Note that $B_*(\mathcal{C}_1) = (Q^1_X)^\perp$ and $B_*(\mathcal{C}_2) = (Q^2_X)^\perp$, which are AG codes of genus g and degrees $(2g-2+n-\ell_1)$ and $(2g-2+n-\ell_2)$ respectively. By condition (4) and Corollary 6.3, we know that $(Q^1_X)^\perp \otimes (Q^2_X)^\perp$ is $\frac{\epsilon^2}{12}$-robust. Let $\Delta_i = d(Q^i_Z)/n$ be the relative distance. By [GG24, Theorem 4.1], we know that

$$\frac{1}{\mu_*(\mathcal{A})} \geq \frac{\epsilon^2}{12} \cdot \min\{\frac{\epsilon^2}{12}, \Delta_1, \Delta_2\}.$$

Now, $\Delta_i = d(Q^i_Z)/n \geq \epsilon$ by condition (1) and Proposition 2.4. Therefore, we have $\frac{1}{\mu_*(\mathcal{A})} \geq (\frac{\epsilon^2}{12})^2$. Similarly, $\frac{1}{\mu_*(\mathcal{A})}$ is bounded below by $(\frac{\epsilon^2}{12})^2$. Therefore, we may take $\rho(\epsilon) = (\frac{\epsilon^2}{12})^2$. □

Now we note that there exist families of quantum AG codes satisfying the assumptions of Proposition 6.4, and as a corollary we obtain good quantum codes which are locally testable with constant soundness.

Corollary 6.5. *Let $q = 2^{2m}$ where $m \geq 8$. Fix $\frac{7}{\sqrt{q}-4} < \epsilon < \frac{1}{8}(1 - \frac{14}{\sqrt{q}})$. Let $Q^1 := Q(X, D, \ell_1 P)$ and $Q^2 := Q(X, D, \ell_2 P)$ be two quantum AG codes as constructed in Example 2.8 with $\ell_1 = \alpha_1 g$ and $\ell_2 = \alpha_2 g$ where*

$$\alpha_1 = \lfloor (1-\epsilon)(\sqrt{q}-2) \rfloor - 1 \text{ and } \alpha_2 = \lfloor (1-3\epsilon)(\sqrt{q}-2) \rfloor - 1.$$

Let $\mathcal{C}_i$ be the single-sector chain complex obtained from Q^i. Then the quantum CSS code $\mathcal{Q}(\mathcal{A})$ associated with the homological product $\mathcal{A} = \mathcal{C}_1 \otimes \mathcal{C}_2$ is a $[[N, \Theta(N), \Theta(N)]]_q$ code. Moreover, $\mathcal{Q}(\mathcal{A})$ is locally testable with locality at most $2\sqrt{N}$ and soundness at least $\rho := (\frac{\epsilon^2}{12})^2$.

Proof. First, we have $q \geq 2^{16}$. Hence $\frac{7}{\sqrt{q}-4} < \frac{1}{8}(1 - \frac{14}{\sqrt{q}})$, and ϵ can be chosen in the given interval. Moreover, we have

$$\frac{\sqrt{q}}{2} + 1 < \lfloor (1-3\epsilon)(\sqrt{q}-2) \rfloor - 1,$$

and hence we may choose α_1, α_2 as above in the construction given by Example 2.8. Now let us check that the assumptions of Proposition 6.4 apply as $g, n \to \infty$.

We have $\alpha_1 = \lfloor (1-\epsilon)(\sqrt{q}-2) \rfloor - 1$ and $\alpha_2 = \lfloor (1-3\epsilon)(\sqrt{q}-2) \rfloor - 1$. Therefore,

$$\alpha_2 g < \alpha_1 g < (1-\epsilon)(\sqrt{q}-2)g < (1-\epsilon)n$$

as $(\sqrt{q}-2)g < n+1 < \sqrt{q}g$ in the construction of Example 2.5 (and Example 2.8). Hence $\ell_1 = \alpha_1 g, \ell_2 = \alpha_2 g$ satisfies condition (1). By the construction in Example 2.8, we know that $\dim(Q^i_X) = \dim(Q^i_Z)$ for $i \in [2]$. Thus we have condition (2).

Now we have

$$\alpha_1 - \alpha_2 = \lfloor (1-\epsilon)(\sqrt{q}-2) \rfloor - \lfloor (1-3\epsilon)(\sqrt{q}-2) \rfloor \geq 2\epsilon(\sqrt{q}-2) - 2 > \epsilon\sqrt{q} + 4$$

as $\epsilon > \frac{7}{\sqrt{q}-4}$. Hence $\ell_1 - \ell_2 = (\alpha_1 - \alpha_2)g > \epsilon n + 4g + 2$ as $g, n \to \infty$. Therefore, condition (3) is satisfied.

We have

$$\begin{aligned} \alpha_1 + \alpha_2 &= \lfloor (1-\epsilon)(\sqrt{q}-2) \rfloor + \lfloor (1-3\epsilon)(\sqrt{q}-2) \rfloor - 2 \\ &\geq (2-4\epsilon)(\sqrt{q}-2) - 4 \\ &> (1+\epsilon)\sqrt{q} + 6 \end{aligned}$$

as $\epsilon < \frac{1}{8}(1 - \frac{14}{\sqrt{q}})$. Therefore, $\ell_1 + \ell_2 = (\alpha_1 + \alpha_2)g > (1+\epsilon)n + 6g$ as $g, n \to \infty$, and we have condition (4).

Hence Proposition 6.4 applies. Since $N = n^2$, we have that $\mathcal{Q}(\mathcal{A})$ is a $[[N, R_1 R_2 N, \Theta(N)]]_q$ code with locality $\leq 2\sqrt{N}$ and soundness $\geq \rho$. Now note that the dimension of Q^1 is $k_1 = 2\ell_1 - n + 2 - 2g = \Theta(n)$ by Example 2.8. Hence the rate of Q^1 satisfies $R_1 = \Theta(1)$ as $n \to \infty$. Similarly, we have $k_2 = 2\ell_2 - n + 2 - 2g = \Theta(n)$, and hence $R_2 = \Theta(1)$ as $n \to \infty$. Therefore we have that the dimension of $\mathcal{Q}(\mathcal{A})$ is $\Theta(N)$. □

References

[AE15] Dorit Aharonov and Lior Eldar. Quantum locally testable codes. *SIAM Journal on Computing*, 44(5):1230–1262, 2015.

[AM69] M. F. Atiyah and I. G. MacDonald. *Introduction to Commutative Algebra*. Addison Wesley Publishing Company, 1969.

[BE21] Nikolas P Breuckmann and Jens N Eberhardt. Balanced product quantum codes. *IEEE Transactions on Information Theory*, 67(10):6653–6674, 2021.

[BFLS91] László Babai, Lance Fortnow, Leonid A Levin, and Mario Szegedy. Checking computations in polylogarithmic time. In *Proceedings of the twenty-third annual ACM symposium on Theory of computing*, pages 21–32, 1991.

[BH14] Sergey Bravyi and Matthew B Hastings. Homological product codes. In *Proceedings of the forty-sixth annual ACM symposium on Theory of computing*, pages 273–282, 2014.

[BSCI+23] Eli Ben-Sasson, Dan Carmon, Yuval Ishai, Swastik Kopparty, and Shubhangi Saraf. Proximity gaps for reed–solomon codes. *Journal of the ACM*, 70(5):1–57, 2023.

[BSS06] Eli Ben-Sasson and Madhu Sudan. Robust locally testable codes and products of codes. *Random Structures & Algorithms*, 28(4):387–402, 2006.

[CR05] Don Coppersmith and Atri Rudra. On the robust testability of product of codes. *ECCC TR05-104*, 2005.

[CR21] Alain Couvreur and Hugues Randriambololona. Algebraic geometry codes and some applications. In *Concise encyclopedia of coding theory*, pages 307–362. Chapman and Hall/CRC, 2021.

[CS96] A Robert Calderbank and Peter W Shor. Good quantum error-correcting codes exist. *Physical Review A*, 54(2):1098, 1996.

[DEL+22] Irit Dinur, Shai Evra, Ron Livne, Alexander Lubotzky, and Shahar Mozes. Locally testable codes with constant rate, distance, and locality. In *Proceedings of the 54th Annual ACM SIGACT Symposium on Theory of Computing*, pages 357–374, 2022.

[DHLV23] Irit Dinur, Min-Hsiu Hsieh, Ting-Chun Lin, and Thomas Vidick. Good quantum ldpc codes with linear time decoders. In *Proceedings of the 55th annual ACM symposium on theory of computing*, pages 905–918, 2023.

[DLV24] Irit Dinur, Ting-Chun Lin, and Thomas Vidick. Expansion of high-dimensional cubical complexes: with application to quantum locally testable codes. In *2024 IEEE 65th Annual Symposium on Foundations of Computer Science (FOCS)*, pages 379–385. IEEE, 2024.

[DSW06] Irit Dinur, Madhu Sudan, and Avi Wigderson. Robust local testability of tensor products of ldpc codes. In *International Workshop on Approximation Algorithms for Combinatorial Optimization*, pages 304–315. Springer, 2006.

[EH17] Lior Eldar and Aram W Harrow. Local hamiltonians whose ground states are hard to approximate. In *2017 IEEE 58th annual symposium on foundations of computer science (FOCS)*, pages 427–438. IEEE, 2017.

[Eis13] David Eisenbud. *Commutative algebra: with a view toward algebraic geometry*, volume 150. Springer Science & Business Media, 2013.

[FS95] Katalin Friedl and Madhu Sudan. Some improvements to total degree tests. In *Proceedings Third Israel Symposium on the Theory of Computing and Systems*, pages 190–198. IEEE, 1995.

[Ful08] William Fulton. Algebraic curves. *An Introduction to Algebraic Geom*, 54, 2008.

[GG24] Louis Golowich and Venkatesan Guruswami. Quantum ldpc codes of almost linear distance via homological products. *arXiv preprint arXiv:2411.03646*, 2024.

[GM12] Oded Goldreich and Or Meir. The tensor product of two good codes is not necessarily robustly testable. *Information Processing Letters*, 112(8-9):351–355, 2012.

[Gop77] Valerii Denisovich Goppa. Codes associated with divisors. *Problemy Peredachi Informatsii*, 13(1):33–39, 1977.

[Gop81] Valerii Denisovich Goppa. Codes on algebraic curves. In *Sov. Math.-Dokl*, volume 24, pages 170–172, 1981.

[Gop83] Valerii Denisovich Goppa. Algebraico-geometric codes. *Math. USSR-Izv*, 21(1):75–91, 1983.

[GSW24] Sumegha Garg, Madhu Sudan, and Gabriel Wu. Testing tensor products of algebraic codes. *arXiv preprint arXiv:2410.22606*, 2024.

[Gur04] Venkatesan Guruswami. *List decoding of error-correcting codes: winning thesis of the 2002 ACM doctoral dissertation competition*, volume 3282. Springer Science & Business Media, 2004.

[Har77] Robin Hartshorne. *Algebraic geometry*, volume 52. Springer Science & Business Media, 1977.

[HHO21] Matthew B Hastings, Jeongwan Haah, and Ryan O'Donnell. Fiber bundle codes: breaking the n 1/2 polylog (n) barrier for quantum ldpc codes. In *Proceedings of the 53rd Annual ACM SIGACT Symposium on Theory of Computing*, pages 1276–1288, 2021.

[HKSS24] Prahladh Harsha, Mrinal Kumar, Ramprasad Saptharishi, and Madhu Sudan. An improved line-point low-degree test. In *2024 IEEE 65th Annual Symposium on Foundations of Computer Science (FOCS)*, pages 1883–1892. IEEE, 2024.

[Iha81] Yasutaka Ihara. Some remarks on the number of rational points of algebraic curves over finite fields. *J. Fac. Sci. Tokyo*, 28(3):721–724, 1981.

[JNV+21] Zhengfeng Ji, Anand Natarajan, Thomas Vidick, John Wright, and Henry Yuen. Mip*= re. *Communications of the ACM*, 64(11):131–138, 2021.

[KKS24] Swastik Kopparty, Mrinal Kumar, and Harry Sha. High rate multivariate polynomial evaluation codes. *arXiv preprint arXiv:2410.13470*, 2024.

[KP22] Gleb Kalachev and Pavel Panteleev. Two-sided robustly testable codes. *arXiv preprint arXiv:2206.09973*, 2022.

[LZ22] Anthony Leverrier and Gilles Zémor. Quantum tanner codes. In *2022 IEEE 63rd Annual Symposium on Foundations of Computer Science (FOCS)*, pages 872–883. IEEE, 2022.

[Mei08] Or Meir. Combinatorial construction of locally testable codes. In *Proceedings of the fortieth annual ACM symposium on Theory of computing*, pages 285–294, 2008.

[PK21] Pavel Panteleev and Gleb Kalachev. Quantum ldpc codes with almost linear minimum distance. *IEEE Transactions on Information Theory*, 68(1):213–229, 2021.

[PK22] Pavel Panteleev and Gleb Kalachev. Asymptotically good quantum and locally testable classical ldpc codes. In *Proceedings of the 54th Annual ACM SIGACT Symposium on Theory of Computing*, pages 375–388, 2022.

[Poo06] Bjorn Poonen. Lectures on rational points on curves. *University of California, Berkeley*, 2006.

[Poo08] Bjorn Poonen. Rational points on varieties. *Graduate Studies in Mathematics*, 186(337):5, 2008.

[PS94] Alexander Polishchuk and Daniel A Spielman. Nearly-linear size holographic proofs. In *Proceedings of the twenty-sixth annual ACM symposium on Theory of computing*, pages 194–203, 1994.

[Sha13] Igor R Shafarevich. *Basic algebraic geometry 1: Varieties in projective space*. Springer Science & Business Media, 2013.

[Spi95] Daniel Alan Spielman. *Computationally E cient Error-Correcting Codes and Holographic Proofs*. PhD thesis, Massachusetts Institute of Technology, 1995.

[Sta24] The Stacks project authors. The stacks project. https://stacks.math.columbia.edu, 2024.

[Ste12] Serguei A Stepanov. *Codes on algebraic curves*. Springer Science & Business Media, 2012.

[Sti09] Henning Stichtenoth. *Algebraic function fields and codes*, volume 254. Springer Science & Business Media, 2009.

[Sud92] Madhu Sudan. *Efficient checking of polynomials and proofs and the hardness of approximation problems*. University of California, Berkeley, 1992.

[TVZ82] Michael A Tsfasman, SG Vlăduţ, and Th Zink. Modular curves, shimura curves, and goppa codes, better than varshamov-gilbert bound. *Mathematische Nachrichten*, 109(1):21–28, 1982.

[Val05] Paul Valiant. The tensor product of two codes is not necessarily robustly testable. In *International Workshop on Approximation Algorithms for Combinatorial Optimization*, pages 472–481. Springer, 2005.

[VD83] Sergei G Vlăduţ and Vladimir Gershonovich Drinfeld. Number of points of an algebraic curve. *Functional analysis and its applications*, 17(1):53–54, 1983.

[Vid13] Michael Viderman. Strong ltcs with inverse poly-log rate and constant soundness. In *2013 IEEE 54th Annual Symposium on Foundations of Computer Science*, pages 330–339. IEEE, 2013.

ECCC ISSN 1433-8092

https://eccc.weizmann.ac.il