HIGHER GENUS UNIVERSALLY DECODABLE MATRICES (UDMG)

STEVE LIMBURG, DAVID GRANT, MAHESH K. VARANASI

Abstract. We introduce the notion of Universally Decodable Matrices of Genus g (UDMG), which for $g = 0$ reduces to the notion of Universally Decodable Matrices (UDM) introduced in [8]. A UDMG is a set of L matrices over a finite field $\mathbb{F}_q$, each with K rows, and a linear independence condition satisfied by collections of $K + g$ columns formed from the initial segments of the matrices. We consider the mathematical structure of UDMGs and their relation to linear vector codes. We then give a construction of UDMG based on curves of genus g over $\mathbb{F}_q$, which is a natural generalization of the UDM constructed in [8] from $\mathbb{P}^1$. We provide upper (and constructable lower) bounds for L in terms of K, q, g, and the number of columns of the matrices.We will show there is a fundamental trade off (Theorem 5.4) between L and g, akin to the Singleton bound for the minimal Hamming distance of linear vector codes.

Introduction

Universally Decodable Matrices (UDM) over finite fields were introduced by Tavildar and Viswanath in [4] to build examples of *approximately universal codes* (defined below), which were designed to solve an important problem in coding over parallel channels in slow-fading wireless communications systems. Recently Vontobel and Ganesan gave a general construction for UDMs in [8]. (See also [2].)

In this paper we introduce a natural and useful generalization of UDMs we call *Universally Decodable Matrices of Genus g* (UDMGs). We then generalize the construction of UDMs given in [8] and find bounds for the size of a UDMG that apply in a more general setting than that considered in [4] and [8].

Despite (or perhaps because of) their utilitarian origin, these sets of matrices can be studied as an abstract mathematical structure in

Date: December 12, 2013.
2010 *Mathematics Subject Classification.* 94B60, 94B05,11T71.
Key words and phrases. Universally decodable matrices, algebraic geometric codes. The first author was partially supported by Department of Education GAANN grant P200A060220.

their own right, and as such have a rich and beautiful theory, including relations to traditional linear vector codes — which in some sense they generalize. Before we detail this structure, let us describe in more detail the communications problem which inspired their consideration and to which they provide a solution.

Communication Motivation for UDMG. First let us review the terminology we need from communications theory. Digital communication over a wireless channel takes place via the transmission of complex numbers whose magnitude and argument determine the amplitude and phase of the radio-frequency wave over which they are transmitted (the channel itself is randomly time-varying and is defined probabilistically). The radio wave is received by an antenna and sampled at the symbol rate, so if $x \in \mathbb{C}$ is the transmitted information-bearing complex-valued symbol, the corresponding discrete-time complex received signal will be $y = hx+n$, where h and n are realizations of complex random variables, respectively called the *fading coefficient* and the *noise* of the channel. We assume that the noise is an additive complex Gaussian random variable of mean 0 and variance 1. If the realization h is constant over all T timeslots that we will employ the channel, we say the channel is *slow-fading*. A set of L channels is called a *parallel* channel, and its elements are called its *subchannels*. An important example of a parallel channel is one that results in wide-band communication through the use of a technique called orthogonal frequency division multiplexing (OFDM) [5].

Therefore given a set W of messages (information), we can transmit it over L-parallel subchannels for T timeslots via an injection $i : W \to \mathrm{Mat}_{L\times T}(\mathbb{C})$. There is a great deal of application-specific engineering that goes into constructing i, and it is useful to write it as the composition of an *encoding* map κ from W into a set C of *codewords*, and a map $\mu : C \to \mathrm{Mat}_{L\times T}(\mathbb{C})$ called *modulation*. We will call the quadruple (W, κ, C, μ) a *coding scheme* (or just a *code*). The *rate* of the code is $\log_2 |W|/T$. The *power* of the code is $\frac{1}{T|C|}\sum_{x\in C} ||\mu(x)||^2$, where $||\ \cdot\ ||$ denotes the Frobenius norm, which by our normalizing choice of the noise is the same as the *signal-to-noise ratio* (SNR), which we denote as $SNR(C, \mu)$.

Recently [4] gave a definition of what it means for a sequence of codes for a slow-fading parallel channel to be "approximately universal" (for the experts, this was meant to capture the notion of what it means for the sequence of codes to optimally trade off diversity and multiplexing gain, no matter the choice of the distribution of the fading coefficients).

So as to not bring us too far afield, we will use an operational definition of approximately universal given in Theorem 5.1 of [4]:

Suppose we have a slow-fading parallel channel with L subchannels. For each natural number n, suppose we have a coding scheme $(W_n, \kappa_n, C_n, \mu_n)$ for our channel, employed for T timeslots, of rate R_n, and signal-to-noise ratio SNR_n, such that SNR_n tends to ∞ as n does. Then we say the sequence is *approximately universal* if for every pair of distinct T-tuples of codewords $v, w \in C_n^T$,

$$\prod_{1 \leq i \leq L} \| d_i \|^2 \geq \frac{1}{2^{R_n + o(\log(SNR_n))}},$$

where d_i is the i^{th}-row of the $L \times T$ matrix $(\mu_n(v) - \mu_n(w))/\sqrt{SNR_n}$.

Given a coding scheme (W, κ, C, μ) for one timeslot, for any T, we can extend κ and μ entry-by-entry to functions κ^T and μ^T of the vectors W^T and C^T, to get the *T-iterated* coding scheme $(W^T, \kappa^T, C^T, \mu^T)$ for T timeslots. Using the arithmetic-geometric mean inequality as in the proof of the following Lemma, it is not hard to see that if a sequence of coding schemes for one timeslot is approximately universal, then for any T, the corresponding sequence of T-iterated coding schemes is approximately-universal. So for the purpose of building examples of sequences of approximately universal coding schemes, it suffices to build examples for one timeslot. So we will assume henceforth that $T = 1$. We also need the following simplification:

Lemma 0.1. *For each natural number n, suppose we have a coding scheme $(W_n, C_n, \kappa_n, \mu_n)$ for our parallel channel with L-subchannels, of rate R_n, and signal-to-noise ratio SNR_n, such that SNR_n tends to ∞ as n does, and that μ_n is real-valued. Suppose that for every pair of distinct codewords $v, w \in C_n$,*

$$\prod_{1 \leq i \leq L} d_i^2 \geq \frac{1}{2^{2R_n + o(\log(SNR_n))}},$$

where d_i is the i^{th}-entry of the vector $(\mu_n(v) - \mu_n(w))/\sqrt{SNR_n}$. Then the complexified coding scheme

$$(W_n \times W_n, \kappa_n \times \kappa_n, C_n \times C_n, \mu_n \times 0 + 0 \times i\mu_n)$$

is approximately universal.

Proof. First of all, $SNR(C_n \times C_n, \mu_n \times 0 + 0 \times i\mu_n) = 2SNR(C_n, \mu_n)$ and the rate of $(W_n \times W_n, \kappa_n \times \kappa_n, C_n \times C_n, \mu_n \times 0 + 0 \times i\mu_n)$ is $2R_n$. So for distinct vectors $(v_1, v_2), (w_1, w_2) \in C_n \times C_n$, we need to compute a lower bound for the i^{th} entry of

$$((\mu_n(v_1) - \mu_n(w_1))^2 + (\mu_n(v_2) - \mu_n(w_2))^2)/2SNR_n,$$

and multiply over all $1 \leq i \leq L$. If $v_1 = w_1$, we see that $\frac{1}{2^{2R_n+L+o(\log(SNR_n))}}$ is a lower bound for this product, which is of the form needed for the definition of approximately universal. A similar bound holds if $v_2 = w_2$, so now assume that $v_1 \neq v_2$ and that $w_1 \neq w_2$. Then the arithmetic-geometric-mean inequality gives:

$$\prod_{1\leq i\leq L} \frac{(\mu_n(v_1)-\mu_n(w_1))^2+(\mu_n(v_2)-\mu_n(w_2))^2}{2SNR_n} \geq$$

$$\prod_{j=1,2}(\prod_{1\leq i\leq L} \frac{(\mu_n(v_j)-\mu_n(w_j))^2}{SNR_n})^{1/2} \geq \frac{1}{2^{2R_n+f(n)}},$$

where $f(n)$ is a function of n that is $o(\log SNR_n)$ so is $o(\log 2SRN_n)$. □

UDMs were constructed in [4] because they can be used to build a sequence of approximately universal codes. We will now show how to generalize this construction. Let q be a power of a prime, $\mathbb{F}_q$ the field with q elements, and N a natural number.

Let $\mathcal{M} = \{M_i | 1 \leq i \leq L\}$ be a collection of $N \times N$ matrices with entries in $\mathbb{F}_q$. If g is a non-negative integer, we say that $\mathcal{M}$ is a set of (square) Universally Decodable Matrices of Genus g (UDMG) of length L if for every L-tuple $(\lambda_1, ..., \lambda_L)$ of non-negative integers, the matrix formed by concontenating the first λ_i columns of M_i is of full rank whenever $\sum_{i=1}^{L} \lambda_i \geq N + g$.

Assume now for every N greater than some N_0, we have a UDMG $\mathcal{M} = \{M_i | 1 \leq i \leq L\}$ of length L such that $L(N_0 - g) \geq N_0$. Let $K_i \in \mathbb{F}_q^N$ be the kernel of the linear transformation $\rho_i : \mathbb{F}_q^N \to \mathbb{F}_q^N$ given by multiplication by M_i. Since M_i has rank at least $N - g$ by design, the dimension of K_i is some $\delta_i \leq g$. Let K be the span of K_i for $1 \leq i \leq L$, and W_N be a complementary space in $\mathbb{F}_q^N$ to K, that is, $W_N + K = \mathbb{F}_{q^N}$ and $W_N \cap K = \{0\}$. Since the dimension of K is some $\Delta \leq \sum_{i=1}^{L} \delta_i \leq gL$, the dimension of W_N is at least $N - Lg$. Note that by construction, ρ_i is injective when restricted to W_N. We then define $\kappa_N(v) = \{\rho_1(v), ..., \rho_L(v)\}$ for $v \in W_N$, and $C_n = \kappa_N(W_N) \subseteq \mathrm{Mat}_{N\times L}(\mathbb{F}_q^N)$. The modulation map $\mu_N : C_n \to \mathbb{C}^L$ will be the column-by-column extension of a map $\mu_0 : \mathbb{F}_q^N \to \mathbb{C}$, which we will now describe in detail. Given the result of Lemma 0.1, there is no reason not to build our example with μ_0 being real-valued.

There is a standard map $p_{q^N} : \mathbb{F}_q^N \to \mathbb{R}$, built as follows. Arbitrarily identify $\mathbb{F}_q$ with $I_q = \{0, 1, ..., q-1\}$ and extend this identification

entry-by-entry from $\mathbb{F}_q^N \to I_q^N$. Now for any $a = (a_1, ..., a_N) \in I_q^N$, let $p_{q^N}(a) =$

$$a_1 q^{N-1} + \cdots + a_{N-1} q + a_N - \frac{q^N - 1}{2}$$
$$= (a_1 - \frac{q-1}{2}) q^{N-1} + \cdots + (a_{N-1} - \frac{q-1}{2}) q + (a_N - \frac{q-1}{2}).$$

This maps I_q^N to q^N unit-spaced points on the real line symmetrically placed about the origin. The map p_{q^N} is standardly called q^N-*PAM* (pulse-amplitude modulation). The modulation map we need to take is a weighted version of q^N-PAM.

We define $\mu_0(a_1, ...a_N) =$

$$(a_1 - \frac{q-1}{2}) q^{N-1} w_1 + \cdots + (a_{N-1} - \frac{q-1}{2}) q w_{N-1} + (a_N - \frac{q-1}{2}) w_N,$$

where $w_i = (1 + \frac{(q-1)(N+1-i)+1}{qN})$ for $1 \le i \le L$. Note that $1 \le w_i \le 2$.

The reason for these weights is the following:

Lemma 0.2. *If two codewords $a = (a_1, ...a_L)$ and $b = (b_1, ..., b_L)$ in C_N have $a_i = b_i$ for $i = 1, ..., m$ for some $1 \le m < L$, but $a_{m+1} \ne b_{m+1}$, then*

$$|\mu_0(a) - \mu_0(b)| > q^{(N-m-1)}/N.$$

Proof. Without loss of generality, we can assume $\mu_0(a) > \mu_0(b)$, and then $\mu_0(a) - \mu_0(b)$ is minimized when $a_{m+1} = b_{m+1} + 1$, and $a_i = 0, b_i = q - 1$ for $m + 2 \le i \le N$. Hence $|\mu_0(a) - \mu_0(b)| \ge$

$$w_{m+1} q^{N-m-1} - (q-1) \sum_{k=1}^{N-m-1} w_{m+1+k} q^{N-m-1-k} = 1 + q^{N-m-1}/N,$$

using the combinatorial identities $\sum_{i=0}^{\ell} x^i = (x^{\ell+1} - 1)/(x - 1)$ and x times its derivative: $\sum_{i=1}^{\ell} i x^i = \frac{x}{(x-1)^2}(\ell x^{\ell+1} - (\ell + 1)x^\ell + 1)$. □

Hence it is also appropriate to refer to μ_0 as a *gapped* version of q^N-PAM, as they do in [4].

Lemma 0.3. *There are positive constants α and β that depend on q, g, and L, but not on N, such that,*

$$\frac{\alpha q^{2N}}{N^2} \le SNR(C_N, \mu_N) \le \beta q^{2N}.$$

Proof. First note that $SNR(C_N, \mu_N) =$

$$\frac{1}{|C_N|} \sum_{c \in C_N} ||\mu_N(c)||^2 = \frac{1}{|W_N|} \sum_{v \in W_N} \sum_{i=1}^{L} \mu_0(\rho_i(v))^2 = \sum_{i=1}^{L} \sigma_i$$

where

$$\sigma_i = \frac{1}{|W_N|}\sum_{v\in W_N}\mu_0(\rho_i(v))^2 = \frac{1}{|Z_i|}\sum_{z\in Z_i}\mu_0(z)^2,$$

where $Z_i = \rho_i(W_N)$.

To get an upper bound on σ_i we note:

$$\frac{1}{|Z_i|}\sum_{z\in Z_i}\mu_0(z)^2 \leq \frac{1}{q^{N-Lg}}\sum_{z\in I_q^N}\mu_0(z)^2$$

$$\leq \frac{1}{q^{N-Lg}}\sum_{a\in I_q^N}((a_1-\frac{q-1}{2})q^{N-1}w_1+\cdots+(a_{N-1}-\frac{q-1}{2})qw_{N-1}+(a_N-\frac{q-1}{2})w_N)^2$$

$$= \frac{1}{q^{N-Lg}}\sum_{a\in I_q^N}((a_1-\frac{q-1}{2})q^{N-1})^2w_1^2+\cdots+((a_{N-1}-\frac{q-1}{2})q)^2w_{N-1}^2+((a_N-\frac{q-1}{2}))^2w_N^2,$$

the sum of the cross terms vanishing because of the invariance of the set $\{a-(q-1)/2|a\in I_q\}$ under negation. Since $w_i\leq 2$, σ_i is bounded above by

$$\frac{4}{q^{N-Lg}}\sum_{a\in I_q^N}((a_1-\frac{q-1}{2})q^{N-1})^2+\cdots+((a_N-\frac{q-1}{2}))^2 \leq$$

$$\frac{4}{q^{N-Lg}}\sum_{a\in I_q^N}(\frac{q-1}{2})^2q^{2N-2}+\cdots+(\frac{q-1}{2})^2 = \frac{4}{q^{N-Lg}}q^N(\frac{q-1}{2})^2(q^{2N-2}+\cdots+1)$$

$$= 4q^{Lg}(\frac{q-1}{2})^2\frac{q^{2N}-1}{q^2-1} \leq q^{Lg}(\frac{q-1}{q+1})q^{2N}.$$

Summing over $1\leq i\leq L$, we get $SNR(C_N,\mu_N)\leq \beta q^{2N}$, where $\beta = Lq^{Lg}$.

The lower bound for σ_i depends of the parity of q. First let us assume q is odd, and set $z_0 = (\frac{q-1}{2},...,\frac{q-1}{2})\in I_q^N$. Then $\mu_0(z_0)=0$, so

$$\sigma_i = \frac{1}{|Z_i|}\sum_{z\in Z_i}\mu_0(z)^2 \geq \frac{1}{q^{N-\Delta}}\sum_{z\in Z_i}|\mu_0(z)-\mu_0(z_0)|^2 \geq \frac{1}{q^{N-\Delta}}\sum_{z\in Z_i}\frac{q^{2(N-m_0(z)-1)}}{N^2},$$

by Lemma 0.2, where $m_0(z)$ is the number of initial entries where z and z_0 agree. Each addend decreases in size as $m_0(z)$ increases, so if Z' is the subset of elements in I_q^N which agree with z_0 for their first initial Δ entries, then we have

$$\sigma_i \geq \frac{1}{q^{N-\Delta}}\sum_{z\in Z'}\frac{q^{2(N-m_0(z)-1)}}{N^2} = \frac{1}{N^2q^{N-\Delta}}(q-1)(q^{3(N-\Delta-1)}+\cdots q^3+1)$$

$$= \frac{q-1}{(q^3-1)N^2q^{N-\Delta}}(q^{3(N-\Delta)}-1) \geq \frac{1}{(3q^2)N^2q^{N-\Delta}}q^{3(N-\Delta)}/2.$$

Summing over $1 \leq i \leq L$, we see that when q is odd we can take $\alpha = L/6q^{2gL+2}$.

When q is even, $\mu_0(z)$ for $z \in I_q^N$ is minimized when z is $z_0 = (q/2+1, ..., q/2+1)$ or $z_1 = (q/2, ..., q/2)$. Hence

$$\sigma_i = \frac{1}{|Z_i|}\sum_{z\in Z_i}\mu_0(z)^2 \geq \frac{1}{q^{N-\Delta}}\sum_{z\in Z_i}(\mu_0(z)^2 - \mu_0(z_0)^2) =$$

$$= \frac{1}{q^{N-\Delta}}\sum_{z\in Z_i}|\mu_0(z)-\mu_0(z_0)||\mu_0-\mu_0(z_1)| \geq \frac{1}{q^{N-\Delta}}\sum_{z\in Z_i}\frac{q^{(N-m_0(z)-1)+(N-m_1(z)-1)}}{N^2},$$

by Lemma 0.2, where $m_0(z)$ and $m_1(z)$ are respectively the number of initial entries where z agrees with z_0 and z_1. Note that either $m_0(z)$ or $m_1(z)$ vanishes, since z_0 and z_1 differ in all entries. Again, each addend decreases in size as $m_0(z)$ or $m_1(z)$ increases, so if Z' is the subset of elements in I_q^N which agree with z_0 or z_1 for their first initial $\Delta+1$ entries, then we have

$$\sigma_i \geq \frac{1}{q^{N-\Delta}}\sum_{z\in Z'}\frac{q^{(N-m_0(z)-1)+(N-m_1(z)-1)}}{N^2} = \frac{q^{N-1}}{N^2q^{N-\Delta}}2(q-1)(q^{2(N-\Delta-2)}+\cdots q^2+1)$$

$$= \frac{2(q-1)q^{\Delta-1}}{(q^2-1)N^2}(q^{2(N-\Delta-1)}-1) \geq \frac{q^{\Delta-1}}{(2q)N^2}q^{2(N-\Delta-1)}.$$

Summing over $1 \leq i \leq L$, we see that when q is even we can take $\alpha = L/2q^{gL+4}$.

□

Theorem 0.4. *Fix $L > 0, g \geq 0$. Suppose for some N_0, for $N \geq N_0$ we have a sequence of UDMG $\mathcal{M}_N$ of genus g of size $N \times N$ and length L, with $L(N_0 - g) \geq N_0$. Then the corresponding sequence of codes $(W_N, \kappa_N, C_N, \mu_N)$ built from $\mathcal{M}_N$ as above is approximately universal.*

Proof. Our proof is modeled on that in Appendix IV of [4] . Fix an $N \geq N_0$, with $L(N_0 - g) \geq N_0$, and a UDMG $\mathcal{M} = \{M_1, ..., M_L\}$ of genus g and length L consisting of $N \times N$ matrices. Keep notation as above. Let $v, w \in W_N$ be distinct, so for every $1 \leq i \leq L$, $M_iv \neq M_iw$. Suppose that M_iv and M_iw agree in precisely the first λ_i entries. Hence by Lemma 0.2,

$$|\mu_0(M_iv) - \mu_0(M_iw)| \geq q^{N-\lambda_i-1}/N,$$

so if $d_i = |\mu_0(M_iv) - \mu_0(M_iw)|/\sqrt{SNR(C_N, \mu_N)}$, then by Lemma 0.3

$$d_i \geq q^{-\lambda_i-1}/N\sqrt{\beta}.$$

Since $\mathcal{M}$ is a UDMG of genus g, and since $v \neq w$, we must have $\sum_{1\leq i\leq L} \lambda_i < N + g$. Hence

$$\begin{aligned}\prod_{1\leq i\leq L} d_i^2 &\geq \prod_{1\leq i\leq L} q^{-2\lambda_i - 2}/\beta N^2 \\ &= \left(\frac{1}{\beta q^2 N^2}\right)^L q^{-2\sum_{i=1}^L \lambda_i} \\ &> \left(\frac{1}{\beta q^2 N^2}\right)^L q^{-2N-2g} \\ &= \frac{1}{\beta^L q^{2L+2g} N^{2L}} q^{-2N} \\ &= \frac{1}{\beta^L q^{2L+2g} N^{2L}} \frac{1}{2^{2(R_N+\Delta)}},\end{aligned}$$

where recall $R_N = \log_2(W_N)$ is the rate of the code, and Δ is the codimension of W_N in $\mathbb{F}_{q^N}$, which is at most gL. Since

$$\log \beta^L q^{2L+2g} N^{2L} 2^{2\Delta} = o(\log(\alpha q^{2N}/N^2)),$$

the Theorem follows from Lemmas 0.1 and 0.3. □

The reason we include N_0 in our formulation is that we will show (see §5) that for fixed N and q, there is a bound for the number of parallel channels L a message can be reliably sent over in terms of the genus g of a UDMG. As a result, allowing UDMGs (and not just only UDMs) offer new possibilities for coding design on slow-fading parallel channels, allowing for a larger value of L for fixed q and N.

Outline of the Paper. In §1 we give the abstract mathematical model of UDMG and derive their basic properties, including the vector-space realization of UDMG, equivalence of UDMG, and introduce sub- and quotient-UDMG. In §2 we relate UDMG to linear vector codes, suggesting that the former is something of a generalization of the latter. Section 3 gives our construction of UDMG of genus g based on curves of genus g (which we call "Goppa UDMG"). In [8] (Proposition 14) they construct a UDM so that the matrix formed by concatenating the first row of each matrix in the UDM is the generator matrix for a Reed-Solomon code. Similarly in Theorem 3.8 we show that the matrix formed by concatenating the first column of each of the matrices in a Goppa UDMG is the generating matrix for a corresponding Goppa code. In §4 we provide an example of a Goppa UDMG worked out for a curve of genus 1. The final §5 gives upper and constructable

lower bounds on the number of matrixes in a UDMG in terms of its parameters.

1. Mathematical Model of UDMG

We first present the most general definition of Universally Decodable Matrices of genus g, and then specialize to the class of most interest in communications applications.

To fix notation, for a prime power q, let $\mathbb{F}_q$ be the field with q elements, and for any $N, K > 0$, let $\mathcal{M}_{K\times N}(\mathbb{F}_q)$ denote the $K \times N$ matrices with entries in $\mathbb{F}_q$. For any set S of column vectors in $\mathbb{F}_q^K$, we let $\mathrm{sp}(S)$ be the span of S over $\mathbb{F}_q$. We denote the i^{th} entry of a vector v by $(v)_i$ and likewise denote the j^{th}-column of a matrix M by $(M)_j$. All our vector spaces will be finite dimensional. We define an integer vector α to be greater than or equal to another integer vector β of the same length, if every entry of α is greater than or equal to the corresponding entry of β. If $\eta \in \mathbb{Z}$, we let $\vec{\eta}$ denote the column vector all of whose entries are η and whose length is determined by context. For any vector $\mathbf{N} = (N_1, ..., N_L)$ of integers, we will let $N = N(\mathbf{N}) = \sum_{i=1}^{L} N_i$.

Definition 1.1. For any positive integer L, let $\mathbf{N} = (N_1, ..., N_L)$ be a vector of non-negative integers. Fix $K > 0, g \geq 0$. Let $\mathbf{M} = \{M_1, \ldots, M_L\}$ be a set of L matrices with $M_i \in \mathcal{M}_{K\times N_i}(\mathbb{F}_q)$. For any $0 \leq \lambda_i \leq N_i$ such that $\sum_{1=1}^{L} \lambda_i = K + g$, the collection $\mathfrak{A}$ of the first λ_i columns from each M_i is called an *allowable set of columns* from $\mathbf{M}$.

We say that $\mathbf{M}$ is a (set of) Universally Decodable Matrices of genus g (UDMG) if for every allowable set of columns $\mathfrak{A}$ of $\mathbf{M}$, $\mathrm{sp}(\mathfrak{A}) = \mathbb{F}_q^K$. If so, we say that $\mathbf{M}$ is a $(L, \mathbf{N}, K, q, g)$-UDMG. The space of all UDMG with *parameters* $(L, \mathbf{N}, K, q, g)$ will be denoted as $\mathcal{U}(L, \mathbf{N}, K, q, g)$. We call the parameters $(L, \mathbf{N}, K, q, g)$ respectively the *size*, *length*, *height*, *alphabet cardinality*, and *genus* of $\mathbf{M}$.

If in addition there is a positive integer η such that $N_i = \eta$, $1 \leq i \leq L$, $\mathbf{M}$ will be called η-*regular*, and the set of such will be denoted by $\mathcal{U}(L, \vec{\eta}, K, q, g)$.

Remark 1.2. It is only interesting to study UDMG $\mathbf{M}$ which have at least one set of allowable columns, i.e., those for which $N \geq K + g$. Similarly, if any $N_i > K + g$, $(M_i)_j$ for $K + g < j \leq N_i$ is never an element of an allowable set of columns, so we will only be interested in considering UDMG for which every $N_i \leq K + g$. Anomalous behavior occurs when $K = 1$, since then for any $g \geq 0$ and any $\mathbf{N}$, we can have a code of unbounded size by taking each $M_i = \vec{1}$ (of length N_i).

These considerations lead to the following:

Definition 1.3. A UDMG $\mathbf{M} \in \mathcal{U}(L, \mathbf{N}, K, q, g)$ we be called *non-degenerate* if $N \geq K + g$, $N_i \leq K + g$ for each $1 \leq i \leq L$, and $K \geq 2$. The set of such will be denoted $\mathcal{U}_n(L, \mathbf{N}, K, q, g)$. A UDMG which is not nondegenerate will be called *degenerate*.

Remark 1.4. (1) We will be concerned throughout with the problems of finding *upper bounds* for L, by which we mean $B_u = B_u(\mathbf{N}, K, q, g)$ such that $\mathcal{U}_n(L, \mathbf{N}, K, q, g)$ is empty for $L > B_u$, and *constructable lower bounds* for L, by which we mean $B_\ell = B_\ell(\mathbf{N}, K, q, g)$ such that there exists an $L \geq B_\ell$ such that $\mathcal{U}_n(L, \mathbf{N}, K, q, g)$ is non-empty.

(2) In the definition of UDMG we do not require g to be minimal, so for any $0 \leq g \leq \tilde{g}$, $\mathcal{U}(L, \mathbf{N}, K, q, g) \subseteq \mathcal{U}(L, \mathbf{N}, K, q, \tilde{g})$. However a non-degenerate UDMG with parameters $(L, \mathbf{N}, K, q, g)$ is not necessarily a non-degenerate UDMG with parameters $(L, \mathbf{N}, K, q, \tilde{g})$

(3) Similarly, given any $\mathcal{A} = (A_1, ..., A_L) \in \mathcal{U}(L, \mathbf{N}, K, q, g)$, we can *truncate* it to produce an $\mathcal{A}' \in \mathcal{U}(L', \mathbf{N}', K, q, g)$ for $\mathbf{N} \geq \mathbf{N}' \geq \vec{0}$,by taking A'_i to be the first N'_i columns of A_i for all $1 \leq i \leq L$. Here L' is the number of non-zero N'_i in $\mathbf{N}'$. We call such an $\mathcal{A}'$ a *subUDMG* of $\mathcal{A}$. (Taking $\mathbf{N}' = \vec{0}$ produces what could only be called the *empty* UDMG.) If each $N'_i < N_i$, we say that $\mathcal{A}'$ is a proper *subUDMG* of $\mathcal{A}$.

Dual to the notion of subUDMG is taking a quotient of a UDMG by a proper subUDMG. To explain this construction, it will be necessary to view UDMGs through a different guise. Indeed, note that the definition of a UDMG considers the span of allowable columns of a set of matrices, and not the columns themselves. Hence it is sometimes useful to consider just the spans of the columns of a matrix in a UDMG, and not the columns themselves. We build up the requisite notions as follows.

Definition 1.5. Take $K, N > 0$, and $M \in \mathcal{M}_{K \times N}(\mathbb{F}_q)$. For any $1 \leq j \leq N$, let $V(M)_j$ denote the span over $\mathbb{F}_q$ of the first j columns of M. We set $V(M) = \{V(M)_1, ..., V(M)_N\}$ and call it the *vector space realization* of M.

For any positive integer N, let $\mathbf{N} = (N_1, ..., N_L)$ be a vector of positive integers. If $\mathbf{M} = \{M_1, \ldots, M_L\}$ is a set of L matrices with $M_i \in \mathcal{M}_{K \times N_i}(\mathbb{F}_q)$, we set $V(\mathbf{M}) = \{V(M_1), ..., V(M_L)\}$ and call it the *vector space realization* of $\mathbf{M}$.

Note that all $V(M_i)_j$ are subspaces of $\mathbb{F}_q^K$.

Definition 1.6. If W is an $\mathbb{F}_q$-vector space, and $C : V_1, ..., V_N$ is an ordered list of N subspaces, we call C a *chain* of subspaces of W if $V_1 \subseteq \cdots \subseteq V_N$. We say the chain is *closely nested* if $\dim(V_1) \leq 1$ and $\dim(V_{i+1}/V_i) \leq 1$ for each $1 \leq i < N$.

For any $M \in \mathcal{M}_{K\times N}(\mathbb{F}_q)$, $V(M)$ is a chain of closely nested subspaces of $\mathbb{F}_q^K$. Conversely, given a chain $C : V_1 \subseteq \cdots \subseteq V_N$ of closely nested subspaces of $\mathbb{F}_q^K$, one can form a matrix $M \in \mathcal{M}_{K\times N}(\mathbb{F}_q)$, such that $C = V(M)$ by setting $V_0 = 0$, and for each $0 \leq i < N$ choosing $(M)_{i+1} \in \mathbb{F}_q^K$ to be a generator of V_{i+1}/V_i if the quotient is 1-dimensional, and arbitrarily in V_{i+1} if $V_{i+1} = V_i$.

Definition 1.7. We define a closely nested chain $C : V_1 \subseteq \cdots \subseteq V_N$ of subspaces of an $\mathbb{F}_q$-vector space W to be *isomorphic* to a closely nested chain $C' : V_1' \subseteq \cdots \subseteq V_N'$ of subspaces of an $\mathbb{F}_q$-vector space W', if there is an $\mathbb{F}_q$-vector space isomorphism $\phi : W \to W'$ such that $\phi(V_i) = V_i'$ for all $1 \leq i \leq N$.

Remark 1.8. We extend this notion of isomorphism (element-by-element) to isomorphisms of ordered collections of closely nested chains of a vector space.

With this we can now define two UDMGs to be *isomorphic* if their vector space realizations are isomorphic ordered collections of closely nested chains of some $\mathbb{F}_q^K$.

Given a set of matrices, one can test whether it is a UDMG in terms of its vector space realization.

Definition 1.9. For any positive integer L, let $\mathbf{N} = (N_1, ..., N_L)$ be a vector of positive integers. Fix $K > 0$, and let W be a vector space over $\mathbb{F}_q$ of dimension K. For each $1 \leq i \leq L$, let $C_i : V_1^i \subseteq \cdots \subseteq V_{N_i}^i$ be a closely nested chain of subspaces of W, and $\mathbf{C} = \{C_1, ..., C_L\}$ be the ordered collection of these chains. A vector $\Lambda = (\lambda_1, ..., \lambda_L)$ of integers with $1 \leq \lambda_i \leq N_i$, such that $\sum_{i=1}^L \lambda_i \geq K + g$ is called an *allowable vector* for $\mathbf{C}$. We say that $\mathbf{C}$ is a (set of) Universally Decodable Vector Spaces of genus g (UDVSG) if for every allowable vector $\Lambda = (\lambda_1, ..., \lambda_L)$ of $\mathbf{C}$, the vector space sum $\sum_{i=1}^L V_{\lambda_i}^i = W$. If so, we say that $\mathbf{C}$ is a $(L, \mathbf{N}, K, q, g)$-UDVSG attached to W.

We have concocted these definitions so that the vector space realization of an $(L, \mathbf{N}, K, q, g)$-UDMG is a $(L, \mathbf{N}, K, q, g)$-UDVSG, and conversely, that any $(L, \mathbf{N}, K, q, g)$-UDVSG attached to some W is isomorphic to the vector space realization of some $(L, \mathbf{N}, K, q, g)$-UDMG. Therefore the notion of UDVSM gives a coordinate-free way to study UDGMs. This is precisely what we need to make sense of quotients of a UDMG.

Definition 1.10. We define a closely nested chain $C : V_1 \subseteq \cdots \subseteq V_N$ of subspaces of an $\mathbb{F}_q$-vector space W to be *reduced* if V_1 is non-trivial and *irredundant* if it is reduced and $V_{i+1} \neq V_i$ for all $1 \leq i < N$. We call

a collection of closely nested chains of subspaces of W to be be *reduced* or *irredundant* if every chain is reduced or irredundant. Likewise we call a collection of matrices to be *reduced* or *irredundant* if its vector space realization is.

Remark 1.11. (1) Any closely nested sequence of subspaces can be *pruned* by removing any initial 0-subspaces to make it reduced, and then be further pruned by removing any repeated subspaces to make it irredundant. We can correspondingly *prune* a matrix by removing any initial 0-columns or by removing any column in the span of the previous columns.

(2) It is the regular, irredundant UDMG which are most important in the engineering application described in the Introduction (where we considered only square UDMG for ease of exposition). The reason for irredundancy is that one would not waste power by transmitting a zero codeword or one known to be in the span of previous ones since we are assuming the channel transmits reliably what it does not erase. The reason for regularity is that each channel will be used for the same amount of time.

We note that the η-regular, irredundant UDMGs of size L, genus 0, and height K over $\mathbb{F}_q$ comprise precisely the set $\mathcal{U}(L, \vec{\eta}, K, q, 0)$, which coincides with the space of all (L, η, K, q)-UDMs defined in [8].

(3) In complete analogy to truncating a UDMG to form a subUDMG (or a proper subUDMG), one can truncate a UDVSG by truncating its chains to form a subUDVSG (or proper UMVSG if every chain is truncated.).

(4) Likewise we can define a UDVSG to be non-degenerate if it is the vector space realization of a non-degenerate UDMG.

The following will be a fundamental notion for us.

Definition 1.12. Let $C : V_1 \subseteq V_2 \subseteq \cdots \subseteq V_N$ be a chain of subspaces of an $\mathbb{F}_q$-vector space W. Let B be any subspace of W. We define the quotient chain C_B of C modulo B to be the chain

$$(V_1 + B)/B \subseteq \cdots \subseteq (V_N + B)/B,$$

of subspaces of W/B.

Proposition 1.13. Let W be an $\mathbb{F}_q$-vectors space and B a subspace of W. If C is a closely nested chain of subspaces of W, then C_B is a closely nested chain of subspaces of W/B.

Proof. We just have to check that given two vector spaces $W_1 \subseteq W_2$ with $\dim(W_2/W_1) = 1$, then the dimension of $V = ((W_2+B)/B)/((W_1+B)/B)$ is at most 1. But V is isomorphic to $(W_2/(W_2 \cap B))/(W_1/(W_1 \cap$

$B))$ which has dimension $\dim(W_2/W_1) - \dim((W_2 \cap B)/(W_1 \cap B)) \leq 1$. □

Remark 1.14. If C is a reduced (or irredundant) chain, then in general, C_B will not be reduced (or irredundant), but one can of course prune C_B to produce a reduced (or irredundant) chain.

Theorem 1.15. *Let $\mathbf{C} = \{C_1, ..., C_L\}$ be a $(L, \mathbf{N}, K, q, g)$-UDVSG attached to an $\mathbb{F}_q$-vector space W of dimension K. Write the chain C_i as $V_1^i \subseteq \cdots \subseteq V_{N_i}^i$. Let $\mathbf{S}$ be a proper subUDVSG of $\mathbf{C}$ of length $\mathbf{N}' < \mathbf{N}$. Let B be the vector space sum of all subspaces in the chains of $\mathbf{S}$, which is $\sum_{i=1}^L V_{N_i'}^i$ (where we set $V_0^i = \{0\}$). Let $r = \max(K - \sum_{i=1}^L \mathbf{N}_i', 0)$. Then $\dim(B) = (K-r) - d$ for some $0 \leq d \leq \min(K-r, g)$. Furthermore, let $\mathbf{C}/\mathbf{S}$ be $\{(C_1)_B, ..., (C_L)_B\}$ with the first μ_i subspaces of each $(C_i)_B$ pruned, for each $1 \leq i \leq L$. Then $\mathbf{C}/\mathbf{S}$ is an $(L, \mathbf{N} - \mathbf{N}', d + r, q, g - d)$-UDVSG, which we call the quotient of C by S.*

Proof. First let us verify that if $r = \max(K - \sum_{i=1}^L \mathbf{N}_i', 0)$, and $\dim(B) = (K-r) - d$, then $0 \leq d \leq \min(K-r, g)$. First of all $d \geq 0$ if $r = 0$ since $\dim(B) \leq \dim(W) = K$. On the other hand, if $r > 0$, by the definition of closely nested, $\dim B \leq \sum_{i=1}^L \mathbf{N}_i' = K - r$. Now we need to show $d \leq g$. First of all, if $\mathbf{N}'$ is an allowable vector, then $r = 0$ and the dimension of B is K, so $d = 0$. Now suppose $\mathbf{N}'$ is not an allowable vector, and for a contradiction, that $d > g$. Then there is an allowable vector $\lambda \geq \mathbf{N}'$ with $\sum_{i=1}^L = K + g$, and so that $\sum_{i=1}^L (\lambda_i - \mathbf{N}_i') \leq (K+g) - (K-r) = g + r$. Hence $\dim(\sum_{1=1}^L (V^i)_{\lambda_i}) \leq \dim(B) - r - d + g + r < K$, a contradiction of the definition of UDVSG.

Proposition 1.13 gives that each $(C_i)_B$, $1 \leq i \leq L$ is a closely nested chain of subspaces of W/B, which has dimension $d+r$. That the size of $\tilde{\mathbf{C}}/\mathbf{S}$ is L follows from that each $\mathbf{N}_i' \leq N_i - 1$. So to verify that $\mathbf{C}/\mathbf{S}$ is a $(L, \mathbf{N} - \mathbf{N}', d+r, q, g-d)$-UDVSG attached to W/B, we need just to take any vector $\lambda = (\lambda_1, ..., \lambda_L)$, with $\sum_{i=1}^L \lambda_i = (d+r) + (g-d) = g + r$, and check that $\sum_{i=1}^L (V_{\mathbf{N}_i' + \lambda_i}^i + B)/B) = W/B$. But this follows since $\sum_{i=1}^L (\lambda_i + \mathbf{N}_i') \geq K + g$, so $\sum_{i=1}^L V_{\mathbf{N}_i' + \lambda_i}^i = W$. □

Remark 1.16. 1) If S is the empty UDVSG, then $\mathbf{C}/\mathbf{S} = \mathbf{C}$.

2) Even if $\mathbf{C}$ is nondegenerate, it can happen that $\tilde{\mathbf{C}}/\mathbf{S}$ is not.

Definition 1.17. The quotient of a UDMG $\mathbf{C}$ by a proper subUDMG $\mathbf{S}$ is a UDMG isomorphic to the quotient of $V(\mathbf{C})$ by $V(\mathbf{S})$ (so is only defined up to isomorphism).

2. Relationship between UDMGs and linear vector codes

If C is an $[n, k, d]$ $\mathbb{F}_q$-linear vector code (that is, a k-dimensional subspace of $\mathbb{F}_q^n$ whose minimal Hamming distance is d), then the Singleton Bound states that $n + 1 - d - k \geq 0$ see [6] or [9]. We standardly call $s = n + 1 - d - k$ the *Singleton Defect* of C [1]. If $s = 0$ then C is a maximal distance separating *MDS code*. More generally, linear codes of defect s are called A^{s}MDS codes

Proposition 2.1. Let $\mathbf{M} = \{M_i\}_{1 \leq i \leq L}$ be an $(L, \mathbf{N}, K, q, g)$ UDMG, and G be the $K \times L$ matrix whose i^{th}-column is the first column of M_i. Then if $L \geq K + g$, G is the generating matrix for some $\mathbb{F}_q$-linear $[L, K, d]$-code $\tilde{C}$ of defect at most g. In particular, if $g = 0$, $\tilde{C}$ is an MDS-code.

Proof. Since $L \geq K + g$ and $\mathbf{M}$ is a UDMG of genus g, G has rank K over $\mathbb{F}_q$. We just have to bound the minimum distance of $\tilde{C}$. If $v \in \tilde{C}$ is non-zero, there is an invertible $K \times K$ matrix M over $\mathbb{F}_q$ such that v is a row of MG. Since G is a matrix whose every $K \times (K + g)$ minor has rank K, the same is true of MG. Hence v has at most $K + g - 1$ zero entries, so has Hamming weight at least $L + 1 - K - g$. Hence the Singleton defect of $\tilde{C}$ is at most g. □

Bounds on the size of MDS codes have been extensively studied (they are the subject of the famed "MDS"-conjecture), and still comprise an active area of research. Although there are sporadic better results, the best known bound for a general $[n, k, d]$ $\mathbb{F}_q$-linear MDS code is that $n \leq k + q - 1$ (see [1] or [6]).

We will make use of the generalization of this bound to A^{s}MDS codes:

Lemma 2.2. [1] *Let C be a $[n, k, d]$ $\mathbb{F}_q$-linear code of Singleton defect s. Then*

$$n \leq k - 2 + (q + 1)(s + 1).$$

Cognizant of Proposition 2.1, in [8], for $L \geq K$, they construct a UDMG $\mathbf{M}$ with parameters $(L, \vec{K}, K, q, 0)$ whose associated linear vector code $\tilde{C}$ is a Reed-Solomon code with parameters $[L, K, L - K + 1]$. The Reed-Soloman codes are the classic non-trivial example of MDS codes. In the next section we generalize this construction to more generally build UDMG $\mathbf{M}$ with parameters $(L, \vec{K}, K, q, g)$, whose associated linear vector codes $\tilde{C}$ are Goppa codes constructed from curves of genus g over $\mathbb{F}_q$, and have parameters $[L, K, d]$ for some $d \geq L - K + 1 - g$, so have Singleton Defect $s \leq g$ (see Remark 3.6, Theorem 3.7, and Theorem 3.8).

We cannot help from noting that since every linear code over $\mathbb{F}_q$ is an A^{s}MDS codes for some s, there is a sense in which UDMG are generalizations of linear vector codes over $\mathbb{F}_q$. This leads to the tantalizing question of what the dual of a UDMG should be, and what properties it would have. Likewise, is there a good notion of what the spectrum of a UDMG should be?

.

3. Goppa UDMGs

Everything we require on the theory of curves over finite fields and their associated Goppa codes can be found in [9]. We will recall what we need by way of establishing notation.

By a *curve* X over $\mathbb{F}_q$ we mean a one-dimensional non-singular projective variety (always taken to be irreducible) over the algebraic closure $\bar{\mathbb{F}}_q$ of $\mathbb{F}_q$ which is defined over $\mathbb{F}_q$ We will let $X(\bar{\mathbb{F}}_q)$denote the points of X defined over $\bar{\mathbb{F}}_q$ and $X(\mathbb{F}_q)$ be the subset of points defined over $\mathbb{F}_q$. A *divisor* D on X is an element of the free abelian group generated by $X(\bar{\mathbb{F}}_q)$, so can be written as $D = \sum_{P \in X(\bar{\mathbb{F}}_q)} n(P)P$, where all but finitely many $n(P) \in \mathbb{Z}$ vanish. The set of P for which $n(P) \neq 0$ is called the *support* of D and written as $\mathrm{supp}(D)$. We write $\deg(D)$ for the *degree* of D, which is $\sum_{P \in X(\bar{\mathbb{F}}_q)} n(P)$. We put a partial order on divisors by saying $D \geq 0$ if each $n(P) \geq 0$. Let $\bar{\mathbb{F}}_q(X)$ and $\mathbb{F}_q(X)$ respectively denote the field of functions on X and the subfield of functions defined over $\mathbb{F}_q$. For every $P \in X(\bar{\mathbb{F}}_q)$ we let v_P be the discrete valuation on $\bar{\mathbb{F}}_q(X)$ that measures the order of zero (or pole) at P of a function. To every non-zero $f \in \bar{\mathbb{F}}_q(X)$ we can associate a divisor $(f) = \sum_{P \in X(\bar{\mathbb{F}}_q)} v_P(f)P$. Likewise, if ω is a differential on X, for every $P \in X(\bar{\mathbb{F}}_q)$, we can let t_P be a uniformizer in the valuation ring of $\bar{\mathbb{F}}_q(X)$ associated to v_P, and define $v_P(\omega) = v_P(\omega/dt_P)$, which is independent of the choice of t_P. Then we define the divisor of ω to be $(\omega) = \sum_{P \in X(\bar{\mathbb{F}}_q)} v_P(\omega)P$. We put an equivalence relation on divisors by saying that D_1 and D_2 are *linearly equivalent* if $D_1 - D_2$ is the divisor of a function: if so we write $D_1 \sim D_2$. For any differential ω we set $\kappa = (\omega)$ which is called a canonical divisor of X, which is well-defined up to linear equivalence since the ratio of any two differentials is a function.

Definition 3.1. Let D be a divisor on X. Let

$$\mathcal{L}(D) = \{f \in \bar{\mathbb{F}}_q(X) - \{0\} | (f) \geq -D\} \cup \{0\}.$$

The space $\mathcal{L}(D)$ is a finite dimensional $\bar{\mathbb{F}}_q$-vector space, and we let $l(D)$ denote its dimension. If D is defined over $\mathbb{F}_q$ (i.e., is fixed by the Galois group of $\bar{\mathbb{F}}_q$ over $\mathbb{F}_q$), then $\mathcal{L}(D)$ has a basis that lies in $\mathbb{F}_q(X)$.

For any divisor D and point $P \in X(\bar{\mathbb{F}}_q)$ not in the support of D, we can define an *increasing zero basis at* P for $\mathcal{L}(D)$ to be an ordered basis $(f_1, ..., f_{\ell(D)})$ such that for all $1 \leq i < \ell(D)$, $v_P(f_{i+1}) > v_P(f_i)$. (One can also do decreasing pole bases.) Such bases exist because v_P is a discrete valuation and $\bar{\mathbb{F}}_q$ is the redisue field of v_P. If D and P are defined over $\mathbb{F}_q$, the increasing zero basis can be taken to have elements in $\mathbb{F}_q(X)$, in which case we call it *an increasing zero basis at* P *over* $\mathbb{F}_q$.

Every non-zero function on X has the same number of poles and zeros, so a function without a pole is a constant, and has a trivial divisor. In other words:

Lemma 3.2. *If* $\deg(D) < 0$ *then* $l(D) = 0$. *Likewise,* $\mathcal{L}(0) = \bar{\mathbb{F}}_q$ *so* $l(0) = 1$.

Fundamental to the subject is the Riemann-Roch Theorem.

Theorem 3.3. *(Riemann-Roch) For any curve* X *there is a non-negative integer* g *called its genus, such that for any canonical divisor* κ *on* X*, and any divisor* D*,*

$$l(D) - l(\kappa - D) = \deg(D) - g + 1.$$

Note that setting $D = 0$ gives $l(\kappa) = g$. Then setting $D = \kappa$ gives that $\deg \kappa = 2g - 2$.

Corollary 3.4. It now follows from Lemma 3.2 that if $\deg(D) > 2g-2$, then $l(D) = 1 - g + \deg(D)$.

Definition 3.5. [9] Let X be a curve over $\mathbb{F}_q$ and $\mathbf{P} = \{P_1, \ldots, P_n\} \subseteq X(\mathbb{F}_q)$. Let D be a divisor on X over $\mathbb{F}_q$, with $\mathrm{supp}(D) \cap \mathbf{P} = \varnothing$. Then $\mathbf{C}(X, \mathbf{P}, D) = \{(f(P_1), \ldots, f(P_n)) | f \in \mathcal{L}(D)\}$ is the *Goppa code* associated with $(X, \mathbf{P}, D)$ and has parameters $[n, l(D) - l(D - \mathbf{P}), d]$, for some $d \geq n - \deg(D)$, as an $\mathbb{F}_q$-linear vector code.

Remark 3.6. Note in particular that if $n > \deg(D)$, then the parameters simplify to $[n, l(D), d]$, so by the Riemann-Roch Theorem, the Singleton defect of $\mathbf{C}(X, \mathbf{P}, D)$ is less than or equal to g.

We now have what we need to construct our Goppa UDMGs. Our construction directly generalizes the one given in [8], once their results

on bivariate polynomials are reinterpreted in terms of statements about the arithmetic and geometry of the projective line $\mathbb{P}^1$ over $\mathbb{F}_q$. Our construction produces an $\mathcal{A} \in \mathcal{U}(L, \vec{K}, K, q, g)$ but we can always truncate this to an $\tilde{\mathcal{A}} \in \mathcal{U}(L, \mathbf{N}, K, q, g)$ as in Remark 1.4 where each $N_i \leq K$.

Theorem 3.7. *Let X be a curve of genus g over $\mathbb{F}_q$, and fix any $K > g-1$. Let $a = K + g - 1$, D be a divisor of degree a on X defined over $\mathbb{F}_q$, and $\mathbf{P} = \{P_1, ..., P_L\} \subseteq X(\mathbb{F}_q)$ be such that $\operatorname{Supp} D \cap \mathbf{P} = \varnothing$. Let B_0 be any ordered basis for $\mathcal{L}(D)$ as an $\mathbb{F}_q$-vector space, and for $1 \leq i \leq L$, let B_i be an increasing zero basis for $\mathcal{L}(D)$ at P_i over $\mathbb{F}_q$. For $1 \leq i \leq L$, let M_i be the change-of-basis matrix from B_0 to B_i, which is a $K \times K$ matrix. Then the set $\mathbf{M} = \{M_1, ..., M_L\}$ is a UDMG with parameters $(L, \vec{K}, K, q, g)$. We will call $\mathbf{M}$ the Goppa UDMG associated with $(X, \mathbf{P}, D)$, and it is nondegenerate if $L, K \geq 2$.*

Proof. For the size of each M_i, note that $K > g-1$ implies that $a > 2g-2$, so $\ell(D) = a-g+1 = K$ by Corollary 3.4. If we write $B_i = \{B_{ij}\}$, $1 \leq j \leq K$, then it follows by induction that $v_{P_i}(B_{i,j+1}) \geq j$ since

$$v_{P_i}(B_{i,j+1}) > v_{P_i}(B_{ij}) \geq j - 1,$$

for $1 \leq j < K$. Since $\operatorname{Supp} D \cap \mathbf{P} = \varnothing$ we lose no generality by taking $B_{i1}(P_i) = 1$. By construction, writing B_i as column vectors, we have

$$M_i B_i = B_0, \tag{1}$$

for each $1 \leq i \leq K$. To prove the theorem, we must verify that given any allowable set of columns $0 \leq \lambda_i \leq K$ such that $\sum_{i=1}^{L} \lambda_i = K + g = a + 1$, that if μ_i is the $K \times \lambda_i$ matrix consisting of the first λ_i columns of M_i, and M is the $K \times (K+g)$ matrix formed by concatenating μ_i for $1 \leq i \leq L$, then M has rank K. Equivalently, we need to show that every row vector u of length K with entries in $\mathbb{F}_q$ in the left-nullspace of M is the zero vector. Note that $uM = 0$ implies $uN_i = 0$, for all $1 \leq i \leq L$. Set $f = uB_0$, which is the zero function precisely when u is the zero vector. By (1), $f = uM_iB_i$ for each $1 \leq i \leq L$. However, $uN_i = 0$ then implies that $v_{P_i}(f) \geq v_{P_i}(B_{i,\lambda_i+1}) \geq \lambda_i$. Thus $f \in \mathcal{L}(E)$, where $E = D - \lambda_1 P_1 - \ldots - \lambda_L P_L$. But $\deg(E) < 0$ and so $l(E) = 0$ by Lemma 3.2. Hence $f = 0$, $u = 0$, and M is of full rank. Thus $\mathbf{M} \in \mathcal{U}(L, \vec{K}, K, q, g)$. □

Theorem 3.8. *With notation as in Theorem 3.7, the matrix formed by concatenating the first column of each $\{M_i\}$, $1 \leq i \leq L$, is the generating matrix for the Goppa code associated with $(X, \mathbf{P}, D)$.*

Proof. A generating matrix for the Goppa code with parameters $(X, \mathbf{P}, D)$ has entries $g_{ij} = f_i(P_j)$, for $1 \leq i \leq K$, $1 \leq j \leq L$, where $\{f_i\}$,

$1 \leq i \leq K$, is any basis for $\mathcal{L}(D)$ defined over $\mathbb{F}_q$. In particular, we can take $f_i = B_{0i}$, $1 \leq i \leq K$, as this basis.

Recall that M_j is defined to be the matrix satisfying $M_j B_j = B_0$, for $1 \leq j \leq K$. Thus we have $M_j B_j(P_j) = B_0(P_j)$. But B_j is an increasing zero basis at P_j, so $B_{jk}(P_j) = 0$ for $2 \leq k \leq L$. We took $B_{j1}(P_j) = 1$, so $B_{0i}(P_j) = (M_j)_{i,1}$ as desired. □

4. An example of a Goppa UDMG of genus 1

Example 1. Let X be the curve in $\mathbb{P}^2$ defined by the equation $S^2T = R^3 + RT^2 + T^3$ over $\mathbb{F}_5$. Since the cubic is nonsingular over $\bar{\mathbb{F}}_5$, X is a nonsingular projective curve of genus 1 over $\mathbb{F}_5$ [3]. Set

$$\mathbf{P} = \{P_1, P_2, P_3, P_4, P_5, P_6, P_7, P_8, P_9\} =$$

$$\{[0,1,1], [4,2,1], [3,4,1], [0,4,1], [4,3,1], [3,1,1], [2,1,1], [2,4,1], [0,1,0]\},$$

which is all of $X(\mathbb{F}_5)$, and let D be the degree 3 divisor cut out by the hyperplane $S + R = 0$ on X. Since the hyperplane is defined over $\mathbb{F}_5$, the same is true of D, and one checks that none of the points in $\mathbf{P}$ are in the support of D. To build the Goppa UDMG associated with $(\mathcal{C}, \mathbf{P}, D)$, we need to calculate an increasing zero basis for $\mathcal{L}(D)$ about each point in $\mathbf{P}$. Let $Q = [0,1,0]$. If $r = R/T, s = S/T \in \mathbb{F}_q(C)$, then a standard fact about genus 1 curves give that $1, r, s$ span $\mathcal{L}(3Q)$, and that the divisor of $r + s$ is $D - 3Q$ (see [3], Chapter 3). Hence $\alpha = 1/(r+s)$, $\beta = r/(r+s)$, and $\gamma = s/(r+s)$ span $\mathcal{L}(D)$. Let B_i, $1 \leq i \leq 9$, be an increasing zero basis for $\mathcal{L}(D)$ about the point P_i. Then we can take:

$$B_1^t = (\alpha, \beta, \gamma - 3\beta - \alpha), \quad B_2^t = (\alpha, \beta - 4\alpha, \gamma - \beta + 2\alpha),$$

$$B_3^t = (\alpha, \beta - 3\alpha, \gamma - \beta + 4\alpha), \quad B_4^t = (\alpha, \beta, \gamma - 2\beta - 4\alpha),$$

$$B_5^t = (\alpha, \beta - 4\alpha, \gamma - 4\beta - 2\alpha), \quad B_6^t = (\alpha, \beta - 3\alpha, \gamma + \beta - 4\alpha),$$

$$B_7^t = (\alpha, \beta - 2\alpha, \gamma - 4\beta + 2\alpha), \quad B_8^t = (\alpha, \beta - 2\alpha, \gamma - \beta + \alpha),$$

$$\text{and } B_9^t = (\gamma, \beta, \alpha),$$

where the superscript t denotes taking the transpose. Let $B_0 = B_1$ and let M_i be the change of basis matrix that satisfies

$$M_i B_i = B_0.$$

Then we get:

$$M_1 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} M_2 = \begin{pmatrix} 1 & 0 & 0 \\ 4 & 1 & 0 \\ 4 & 3 & 1 \end{pmatrix} M_3 = \begin{pmatrix} 1 & 0 & 0 \\ 3 & 1 & 0 \\ 4 & 3 & 1 \end{pmatrix},$$

$$M_4 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 3 & 4 & 1 \end{pmatrix} M_5 = \begin{pmatrix} 1 & 0 & 0 \\ 4 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix} M_6 = \begin{pmatrix} 1 & 0 & 0 \\ 3 & 1 & 0 \\ 1 & 1 & 1 \end{pmatrix},$$
$$M_7 = \begin{pmatrix} 1 & 0 & 0 \\ 2 & 1 & 0 \\ 4 & 1 & 1 \end{pmatrix} M_8 = \begin{pmatrix} 1 & 0 & 0 \\ 2 & 1 & 0 \\ 4 & 3 & 1 \end{pmatrix} M_9 = \begin{pmatrix} 1 & 0 & 1 \\ 3 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}.$$

By Theorem 3.7, the set $\mathbf{M} = \{M_1, \ldots, M_9\} \in \mathcal{U}(9, \vec{3}, 3, 5, 1)$. We note that $\mathbf{M}$ is an example of a genus 1 UDMG which is not a UDM. This follows from setting $\lambda_i = 0$ for $i = 1, 2, 3, 4, 5, 9$ and $\lambda_6 = \lambda_7 = \lambda_8 = 1$, so $\sum_{i=1}^{9} \lambda_i = 3$, and seeing that the resulting matrix

$$\begin{pmatrix} 1 & 1 & 1 \\ 3 & 2 & 2 \\ 1 & 4 & 4 \end{pmatrix}$$

is not of full rank. Also note that concatenating the first column of each M_i, $1 \leq i \leq 9$, gives

$$M = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 4 & 3 & 0 & 4 & 3 & 2 & 2 & 3 \\ 0 & 4 & 4 & 3 & 0 & 1 & 4 & 4 & 1 \end{pmatrix}$$

which is a generating matrix for the Goppa code associated with $(X, \mathbf{P}, D)$ by Theorem 3.8.

It is seemingly non-trivial to check that $\mathbf{M}$ is a UDMG of genus 1 without using Theorem 3.7.

Remark 4.1. It is clear that from our construction of a Goppa UDMG $\mathbf{M}$ associated to a curve X of genus g over $\mathbb{F}_q$ that its size L is bounded by $\#(X(\mathbb{F}_q))$. Bounds on the number of points on a curve over a finite field are given by the famous Hasse-Weil-Serre Theorem:

Theorem 4.2. *Let X be a curve of genus g defined over $\mathbb{F}_q$. Then*

$$q + 1 - g\lfloor 2\sqrt{q} \rfloor \leq \#(X(\mathbb{F}_q)) \leq q + 1 + g\lfloor 2\sqrt{q} \rfloor.$$

These bounds are not always sharp, so in order to build Goppa UDMG of fixed genus g and maximal size, we want to find curves of genus g over a given finite field that have the maximal known number of rational points. The problem of finding such curves is very well-studied and is a continual area of active research. The role that the work of Tsfasman, Vladut, and Zink on this problem played in the construction of Goppa codes with parameters that beat the Gilbert-Varshamov bound for linear vector codes over finite fields is described in [9]. For

the latest on which curves of which genus over which finite fields are known to have the most rational points, see the website [7].

5. Upper bounds on the size of UDMGs

Our first bound comes from our work in section 2. Combining Lemma 2.2 with Proposition 2.1 gives:

Theorem 5.1. *For non-degenerate* $\mathbf{M} \in \mathcal{U}(L, \mathbf{N}, K, q, g)$ *we have*

$$\#(\mathbf{M}) = L \leq K - 2 + (g+1)(q+1).$$

This is only a good bound when $\mathbf{N} = \vec{1}$: we will now use it to get a better bound for many choices of parameters, by taking the quotient of a UDMG by an appropriate proper subUDMG to reduce to the case where $\mathbf{N} = \vec{1}$.

Definition 5.2. Let $\mathbf{M}$ be a nondegenerate UDMG in $\mathcal{U}(L, \mathbf{N}, K, q, g)$. Suppose that each $N_i \geq 2$, $1 \leq i \leq L$. Then we break such UDMGs into two classes. If $\sum_{i=1}^{L}(N_i - 1) \geq K - 2$, we will say $\mathbf{M}$ is of *Class* 1. Otherwise, we will say $\mathbf{M}$ is of *Class* 2.

Lemma 5.3. *Suppose we have a non-degenerate* $\mathbf{M} \in \mathcal{U}(L, \mathbf{N}, K, q, g)$ *with each* $N_i \geq 2$, *and that* $\mathbf{M}$ *is of Class* 1. *Then there is an integer* d *with* $0 \leq d \leq \min(g, K-2)$ *such that there exists a corresponding* $\tilde{\mathbf{M}} \in \mathcal{U}(L, \vec{1}, d+2, q, g-d)$.

Proof. Let $\mathbf{M}$ be as in the statement of the Lemma and $V(\mathbf{M})$ be its vector space realization. Let $\nu = (\nu_1, \ldots, \nu_L)$ be such that $\nu_i \leq N_i - 1$ and $\sum_{i=1}^{L} \nu_i = K - 2$. Let $\mathbf{S}$ be the proper subUDVSG of $\mathbf{M}$ gotten by truncating the i^{th} chain of $\mathbf{M}$ to a chain of length ν_i. By Theorem 1.15 (which applies with $r = 2$), we have that $V(\mathbf{M})/\mathbf{S}$ is a UDVSG with parameters $(L, N - \nu, d+2, q, g-d)$ for some d with $0 \leq d \leq \min(K-2, g)$. Now take $\tilde{\mathbf{M}}$ be the UDMG corresponding to the truncation of $\mathbf{M}/\mathbf{S}$ in which every chain has been truncated to its first subspace. Then $\tilde{\mathbf{M}} \in \mathcal{U}(L, \vec{1}, d+2, q, g-d)$. □

Theorem 5.4. *Let* $\mathbf{M}$ *be a non-degenerate UDMG in* $\mathcal{U}(L, \mathbf{N}, K, q, g)$ *with each* $N_i \geq 2$. *Let* $\gamma_{\mathbf{M}} = \min_{i=1}^{L} N_i$. *If* $\mathbf{M}$ *is of Class* 1, *we have*

$$L \leq (g+1)(q+1).$$

Otherwise we have

$$g + 3 \leq L \leq \frac{K-2}{\gamma_{\mathbf{M}} - 1}.$$

Proof. Suppose $\mathbf{M}$ is of *Class* 1, so $N-L=\sum_{i=1}^{L}(N_i-1)\geq K-2$. By Lemma 5.3 we get a corresponding $\tilde{\mathbf{M}}\in\mathcal{U}(L,\vec{1},d+2,q,g-d)$ for some $0\leq d\leq \min(g,K-2)$. If $\tilde{\mathbf{M}}$ is degenerate then it must be because $L\cdot 1<(d+2)+(g-d)=g+2\leq(g+1)(q+1)$. If $\tilde{\mathbf{M}}$ is nondegenerate, then by Theorem 5.1 we get $L\leq d+(g-d+1)(q+1)\leq(g+1)(q+1)$. So in either case the result follows.

Now suppose $\mathbf{M}$ is of *Class* 2, so $N-L<K-2$. Since $N\geq\gamma_{\mathbf{M}}L$ we get $L<\frac{K-2}{\gamma_{\mathbf{M}}-1}$. Finally, since $\mathbf{M}$ is non-degenerate, we have $K+g\leq N<K+L-2$, so subtracting K yields $g+2<L$. □

Remark 5.5. 1) Theorem 5.4 agrees with the bound in Lemma 9 of [8], for $\mathbf{M}\in\mathcal{U}(L,\vec{\eta},K,q,0)$ in the region $\eta\leq K\leq 2\eta$. Moreover, Theorem 5.4 is tighter than the bound in Lemma 10 of [8] when $K=2\eta+1$ and provides a bound on L for all $\eta\leq K$. Of course our bound is of a slightly different nature since we assume $\eta\geq 2$ throughout and their bound also includes the $\eta=1$ case.

2) If we have an $\mathbf{M}\in\mathcal{U}(L,\vec{2},2,q,0)$ then we can create an $\hat{\mathbf{M}}\in\mathcal{U}(L,\vec{2},2,q,g)$ by taking $g+1$ copies of each matrix in $\mathbf{M}$. They show in [8] the existence of an $\mathbf{M}\in\mathcal{U}(q+1,\vec{2},2,q,0)$ and so we see that the bound $L\leq(g+1)(q+1)$ is sharp for UDMG in $\mathcal{U}(L,\vec{2},2,q,g)$.

3) Theorem 5.4 is not sharp for all classes of UDMGs. We now present another bound on L for certain UDMGs and give an example where this new bound is sharper then the bound in Theorem 5.4.

Lemma 5.6. *For nondegenerate $\mathcal{A}\in\mathcal{U}(L,\mathbf{N},K,q,g)$ with $N_i\geq K-1$ for each $1\leq i\leq L$, we have the bound*

$$\binom{K-2+L}{K-1}\leq\binom{K+g-1}{K-1}\frac{q^K-1}{q-1}.$$

Proof. Let $\mathbf{M}=\{M_1,...,M_L\}$ be in $\mathcal{U}(L,\mathbf{N},K,q,g)$ with $N_i\geq K-1$ for all i. Let $\mathfrak{P}$ be the set of all partitions of $K-1$ into L non-negative integers. Then it is well-known that

$$\#(\mathfrak{P})=\binom{K-2+L}{K-1}. \tag{2}$$

For each partition $\lambda=(\lambda_1,...,\lambda_L)\in\mathfrak{P}$, let $\Xi(\lambda)$ be the set of columns formed from the first λ_j columns of $M_j,\ 1\leq j\leq L$.

Since the codimension 1 subspaces of $\mathbb{F}_q^K$ are in one-to-one correspondence with the points in $\mathbf{P}^{K-1}(\mathbb{F}_q)$, there are $\frac{q^K-1}{q-1}$ subspaces of dimension $K-1$ in $\mathbb{F}_q^K$. Order them arbitrarily and let the j^{th} subspace

be denoted S_j, $1 \leq j \leq \frac{q^K-1}{q-1}$. We define a map $\Upsilon : \mathfrak{P} \to \mathbb{F}_2^{\frac{q^K-1}{q-1}}$ where

$$\Upsilon(\lambda)_j := \begin{cases} 0 & \text{if span } sp(\Xi(\lambda)) \not\subseteq S_j. \\ 1 & \text{if span } sp(\Xi(\lambda)) \subseteq S_j. \end{cases}$$

For $1 \leq j \leq (q^K-1)/(q-1)$, let T_j be the set of $\lambda \in \mathfrak{P}$ such that $\Upsilon(\lambda)_j = 1$, and let y_j be the cardinality of T_j. If the union U_j of $\Xi(\lambda)$ for all $\lambda \in T_j$ contained $K+g$ columns, then since $\mathbf{M} \in \mathcal{U}(L, \mathbf{N}, K, q, g)$, $sp(U_j)$ would be K-dimensional, which is impossible since $sp(U_j) \subseteq S_j$. Hence U_j contains at most $K+g-1$ columns, so there are at most $\binom{K+g-1}{K-1}$ such $\Xi(\lambda) \in T_j$ and $y_j \leq \binom{K+g-1}{K-1}$.

Note that $\Upsilon(\lambda)$ is guaranteed to have at least one non-zero entry since $\Xi(\lambda)$ is a set of $K-1$ columns. Putting this together we have:

$$\#(\mathfrak{P}) \leq \sum_{\lambda \in \mathfrak{P}} \sum_{j=1}^{\frac{q^K-1}{q-1}} \Upsilon(\lambda)_j =$$

$$\sum_{j=1}^{\frac{q^K-1}{q-1}} \sum_{\lambda \in \mathfrak{P}} \Upsilon(\lambda)_j \leq \sum_{j=1}^{\frac{q^K-1}{q-1}} \binom{K+g-1}{K-1} \leq \binom{K+g-1}{K-1} \frac{q^K-1}{q-1}.$$

Thus by the formula for $\#(\mathfrak{P})$ in (2) we have

$$\binom{K-2+L}{K-1} \leq \binom{K+g-1}{K-1} \frac{q^K-1}{q-1}.$$

□

Note that Lemma 5.6 gives an upper bound on L because the left hand side is a polynomial in L, which is increasing as a function of the positive integers, and the right hand side is a number depending only on the other parameters of the UDMG.

Example 2. Consider a non-degenerate $\mathbf{M} \in \mathcal{U}(L, \vec{\eta}, 4, 2, 2)$ with $\eta \geq 4$, so we have $L(\eta-1) = N - L \geq K-2$ and $\mathbf{M}$ is of class 1. Then from Theorem 5.4 we get $L \leq 9$. We can apply Lemma 5.6 to get the upper bound $\binom{2+L}{3} \leq 150$, which implies $L \leq 8$. Thus there are cases when Lemma 5.6 gives a sharper upper bound than Theorem 5.4.

References

1. A. Faldum and W. Willems, *Codes of small defect*, Designs, Codes and Cryptography **10** (1997), no. 3, 341–350.
2. A. Ganesan and P.O. Vontobel, *On the existence of universally decodable matrices*, Information Theory, IEEE Transactions on **53** (2007), no. 7, 2572–2575.
3. J.H. Silverman, *The arithmetic of elliptic curves*, Springer Verlag, 2009.

4. S. Tavildar and P. Viswanath, *Approximately universal codes over slow-fading channels*, Information Theory, IEEE Transactions on **52** (2006), no. 7, 3233–3258.
5. D. Tse and P. Viswanath, *Fundamentals of wireless communication*, Cambridge University Press, 2005.
6. M.A.A. Tsfasman and S.G. Vladut, *Algebraic-geometric codes*, Kluwer Academic Publishers, 1991.
7. G. Van Der Geer and M. Van Der Vlugt, *Tables of curves with many points*, http://www.manypoints.org.
8. P.O. Vontobel and A. Ganesan, *On universally decodable matrices for space–time coding*, Designs, Codes and Cryptography **41** (2006), no. 3, 325–342.
9. J.L. Walker, *Codes and curves*, American Mathematical Society and Institute for Advanced Study, 2000.

Department of Mathematics, University of Colorado at Boulder, Boulder, Colorado 80309-0395 USA
E-mail address: limburg@colorado.edu

Department of Mathematics, University of Colorado at Boulder, Boulder, Colorado 80309-0395 USA
E-mail address: grant@colorado.edu

Department of Electrical and Computer Engineering, University of Colorado at Boulder, Boulder, Colorado 80309-0425 USA
E-mail address: varanasi@colorado.edu