# THE EQUIVALENCE OF SPACE-TIME CODES AND CODES DEFINED OVER FINITE FIELDS AND GALOIS RINGS

DAVID GRANT AND MAHESH K. VARANASI

ABSTRACT. Space-time codes for a wide variety of channels have the property that the diversity of a pair of codeword matrices is measured by the vanishing or non-vanishing of polynomials in the entries of the matrices. We show that for every such channel: I) There is an appropriately-defined notion of approximation of space-time codes such that each code is arbitrarily well approximated by one whose alphabet lies in the field of algebraic numbers; II) Each space-time code whose alphabet lies in the field of algebraic numbers is an appropriately-defined lift from a corresponding space-time code defined over a finite field or a "scaled" lift from a galois ring of arbitrary characteristic. This implies that all space-time codes can be designed over finite fields or over galois rings of arbitrary characteristic and then lifted to complex matrices with entries in a number field.

## INTRODUCTION

A space-time code $\mathcal{S}$ is a finite subset of the $M \times T$ complex matrices $\mathrm{Mat}_{M\times T}(\mathbb{C})$ used to describe the amplitude-phase modulation of a radio frequency carrier signal in a frame of $T$ symbols transmitted over each of $M$ transmit antennas. We call the set of entries of all the matrices in $\mathcal{S}$ its *alphabet*. [1]

The main design criterion for the construction of space-time codes is the error correcting capability of the code, so we seek to minimize the pair-error probability of decoding one codeword $C_1$ into another $C_2$. This probability will depend on how the wireless channel is modeled, but one can typically bound this probability from above by an asymptotic in the inverse of the signal-to-noise ratio SNR, whose lead term is a multiple of $(1/\mathrm{SNR})^d$ for some integer $d$. We call $d = d(C_1, C_2)$ the *diversity* of the pair $(C_1, C_2)$. The minimum value $d_{\mathcal{S}}$ for $d(C_1, C_2)$ over all $C_1 \neq C_2, C_1, C_2 \in \mathcal{S}$ is called the *diversity order* of $\mathcal{S}$. Hence one seeks to maximize $d_{\mathcal{S}}$.

Channels for which space-time codes have been considered and diversity order defined as above include:

EXAMPLE 1. Fast-fading Rayleigh channels with additive white Gaussian noise (AWGN). Here the diversity $d(C_1, C_2)$ is the number of non-zero columns of $C_1 - C_2$, so we will call these *column distance* codes.

This work was partially supported by NSF grant CCF 0434410. The first named author was enjoying the hospitality of the Mathematical Sciences Research Institute as this paper was being completed.

[1] In this section and in section 6 we use some common terminology from digital communications theory: see [22], e.g., for definitions and details.

EXAMPLE 2. Quasi-static fading Rayleigh channels with AWGN. Here $d(C_1, C_2)$ is the rank of the difference of the codewords, $\mathrm{rk}(C_1 - C_2)$, so we will call these *rank* codes.

EXAMPLE 3. Channels which are a combination of those in Examples (1) and (2), a multiple block Rayleigh fading channel with AWGN, which is quasi-static for each of $L$ blocks representing $\rho$ time slots. Here $T = L\rho$, and each $M \times T$ codeword $C$ consists of $L$ submatrices $\{C^i\}_{i=1}^L$, each of size $M \times \rho$. The diversity $d(C_1, C_2)$ is $\sum_{i=1}^L \mathrm{rk}((C_1)^i - (C_2)^i)$. We call these *sum-of-ranks* codes.

EXAMPLE 4. Rayleigh fading channels with AWGN, where we allow for spatial correlation at the transmit and receive antennas and for temporal correlation [21].

Let $U$ denote the number of receive antennas. Let $Q$ and $P$ denote $M \times M$ and $U \times U$ matrices which are square roots of the spatial correlation matrices at the transmit and receive antennas. Suppose that there is a $U \times M$ matrix of fading coefficients $H(t)$ which describes the fading of the $t^{th}$-column of a codeword, for $1 \leq t \leq T$, and that the elements of $H(t)$ are i.i.d. zero-mean complex Gaussian variables, but that the $T$-length vector of each of the entries of $H(t)$ for $1 \leq t \leq T$ has a $T \times T$ temporal correlation matrix $\Sigma$. Then in [21] it is shown that for codewords $C_1, C_2$,

$$d(C_1, C_2) = \mathrm{rk}\left(((C_1 - C_2)^* Q^* Q (C_1 - C_2) \odot \Sigma) \otimes P^* P\right), \tag{1}$$

where $\odot$ and $\otimes$ respectively denote the Hadamard and Kronecker products, and $*$ denotes the conjugate transpose. We call these *spatio-temporal correlated* codes.

Note that if $P$ has rank 1, and $Q$ is the identity, then (1) simplifies to:

$$d(C_1, C_2) = \mathrm{rk}\left((C_1 - C_2)^* (C_1 - C_2) \odot \Sigma\right).$$

Then the diversity in each of Examples (1), (2), and (3) is a special case of this formula for different choices of $\Sigma$ (respectively, $\Sigma$ is the $T \times T$ identity $I_T$; $\Sigma = 1_{TT}$, where $1_{JK}$ denotes the $J \times K$ matrix all of whose entries are 1; and $\Sigma$ is the block diagonal matrix with $L$ blocks each consisting of $1_{\rho\rho}$).

Each diversity is a nicely-behaved integer-valued function on the space of pairs of complex matrices. For example, those in Examples (1)-(3) define a metric on $\mathrm{Mat}_{M \times T}(\mathbb{C})$. More remarkable for our purposes is that each diversity in Examples (1)-(4) is determined by whether or not certain polynomials in the entries of the matrices of $\mathcal{S}$ vanish. This shared algebraic structure allows us to show that:

I) There is an appropriately-defined notion of approximation of space-time codes such that each of these space-time codes is arbitrarily well approximated by one whose alphabet lies in the field of algebraic numbers.

II) Each of these space-time codes whose alphabet lies in the field of algebraic numbers is an appropriately-defined lift from a corresponding space-time code defined over a finite field or a "scaled" lift from a galois ring of arbitrary characteristic.

We conclude that each of these space-time codes is in essence derived from one defined over a finite field or a galois ring of arbitrary characteristic. Therefore such codes defined over finite fields and galois rings becomes a central object of study.

The import of this to code construction is the converse problem: Given space-time codes defined over finite fields and galois rings, how can one lift them to space-time codes? We give examples in the final section to show how the Golden

Code [1], [5] — and indeed all codes from cyclic divisions algebras — can be lifted from codes over finite fields and galois rings. See [9], [13], [14], [15], [16] for what has already been done in using codes over finite fields and Galois rings to build space-time codes.

First we want to make the notions in (I) and (II) precise and to prove these assertions.

To do so, we define a "Generalized Space-Time Code" that abstracts the algebraic properties of all the examples above. Indeed, with so many different models leading to so many different design criteria, it is useful to have a mathematical analysis that simultaneously addresses all these possible models. This level of abstraction not only allows knowledge learned for code design from one model to be applied to all models, the long history of mathematics shows that the very abstraction itself can be a guide to what good codes should look like.

Interestingly, even in this very general setting, there is a generalization of the Singleton bound for the corresponding codes defined over finite fields.

In section 1 of this paper we define Generalized Space-Time Codes and verify that the codes in Examples (1)-(4) are all examples of such. In section 2 we define a notion of equivalence of Generalized Space-Time Codes, and show that each code is arbitrarily well approximated by equivalent ones whose defining polynomials are defined over, and whose alphabet is contained in, the field of algebraic numbers — a so-called "Arithmetic Space-Time Code." (See [2], [3], [4], [7], [8], [10], [11], [12], [18], [20] for some more of the work on the construction of arithmetic space-time codes.)

In sections 3 and 4 we respectively define a notion of equivalence between Arithmetic Space-Time Codes and corresponding space-time codes defined over finite fields and galois rings, and show that each of the former is equivalent to one of the latter (and that the galois rings can be chosen to be of arbitrary characteristic). In section 5, we derive a Singleton bound for space-time codes defined over finite fields. In the final section 6, we discuss the problem that motivates this undertaking: how space-time codes defined over finite fields and galois rings can be lifted to complex space-time codes.

## 1. Generalized and Arithmetic Space-Time Schemes and Codes

We will start off by showing — as we noted in the introduction — that each diversity in Examples (1)-(4) is determined by whether certain sets of polynomials in the entries of the matrices of codewords do or do not vanish. All our notions are borrowed from algebraic geometry. To make the paper accessible to a wider audience, we recall the most basic algebraic geometric definitions and relegate finer points to footnotes. A good introductory reference for almost all the algebraic geometry we will use is [19]. All the rest and the requisite commutative algebra can be found in [6].

Let $R$ be any subring of $\mathbb{C}$. Fix integers $M$ and $T$, and let $x_{ij}$, $1 \leq i \leq M, 1 \leq j \leq T$ be independent indeterminates. Let $X$ denote the $M \times T$ matrix $[x_{ij}]$, and let $A$ be the polynomial ring $R[X] = R[x_{ij}]_{1 \leq i \leq M, 1 \leq j \leq T}$. For any $f \in A$ and $N = [n_{ij}] \in \mathrm{Mat}_{M \times T}(\mathbb{C})$, we define $f(N)$ by evaluating $x_{ij}$ as $n_{ij}$.

EXAMPLE 1 (cont.) Let $\ell_r = \{\prod_{k=1}^{r} x_{i_k, j_k} | 1 \leq j_1 < \cdots < j_r \leq T, 1 \leq i_k \leq M\}$, for $1 \leq r \leq T$. Let $\ell_0 = \{1\}$ and $\ell_{T+1} = \{0\}$. Then $d(C_1, C_2) = r$ precisely when $f(C_1 - C_2) = 0$ for all $f \in \ell_{r+1}$ and $f(C_1 - C_2) \neq 0$ for some $f \in \ell_r$.

EXAMPLE 2 (cont.) Let $\ell_r$ be the set of $r \times r$ minors of $X$ for $1 \leq r \leq n = \min(M, T)$. Let $\ell_0 = \{1\}$ and $\ell_{n+1} = \{0\}$. Then $d(C_1, C_2) = r$ precisely when $f(C_1 - C_2) = 0$ for all $f \in \ell_{r+1}$ and $f(C_1 - C_2) \neq 0$ for some $f \in \ell_r$.

EXAMPLE 3 (cont.) Mapping a codeword $C = \{C^i\}_{i=1}^L$ into the $ML \times T$ matrix $\omega(C)$ which has $C^1, ..., C^L$ stacked sequentially along the diagonal, then $d(C_1, C_2) = \mathrm{rk}(\omega(C_1) - \omega(C_2))$, so a sum-of-ranks code can be realized as a rank code for $ML \times T$ matrices. Specifically, vertically partition $X$ into $L$ matrices of size $M \times \rho$, and let $\ell_r$ be the set of $r \times r$ minors of $\omega(X)$ for $1 \leq r \leq n = \min(ML, T)$. Let $\ell_0 = \{1\}$ and $\ell_{n+1} = \{0\}$. Then $d(C_1, C_2) = r$ precisely when $f(C_1 - C_2) = 0$ for all $f \in \ell_{r+1}$ and $f(C_1 - C_2) \neq 0$ for some $f \in \ell_r$.

EXAMPLE 4 (cont.) The expression in (1) can be greatly simplified. Since $\Sigma$ is positive semi-definite, we can write it as $\Sigma = B^*B$ for some $T \times T$ matrix $B$. Let $D = Q(C_1 - C_2)$. Let $D \sharp B$ be the $MT \times T$ matrix whose rows are indexed by the set $\{(j,k) | 1 \leq j \leq M, 1 \leq k \leq T\}$ ordered lexicographically, and whose columns are indexed by $1 \leq i \leq T$, and whose $(j,k)i$-th entry is $D_{ji}B_{ki}$. In other words,

$$B \sharp D = (B \otimes 1_{M1}) \odot (1_{T1} \otimes D).$$

(Recall that if $E$ is an $M \times T$ matrix and $F$ is an $M' \times T'$ matrix, and if the sets $\{(i,i') | 1 \leq i \leq M, 1 \leq i' \leq M'\}$ and $\{(j,j') | 1 \leq j \leq T, 1 \leq j' \leq T'\}$ are ordered lexicographically, then the $(i,i')(j,j')$-th entry of $E \otimes F$ is $E_{ij}F_{i'j'}$.) Then a direct calculation shows that $D^*D \odot B^*B = (D \sharp B)^*(D \sharp B)$. Hence

$$d(C_1, C_2) = \mathrm{rk}((D \sharp B) \otimes P).$$

Let $\ell_r$ be the set of $r \times r$ minors of $((QX) \sharp B) \otimes P)$ for $1 \leq r \leq n = T \,\mathrm{rk}\, P$. Let $\ell_0 = \{1\}$ and $\ell_{n+1} = \{0\}$. Then $d(C_1, C_2) = r$ precisely when $f(C_1 - C_2) = 0$ for all $f \in \ell_{r+1}$ and $f(C_1 - C_2) \neq 0$ for some $f \in \ell_r$.

Note in Examples (1)–(3) the polynomials in $\ell_r$ have coefficients in $\mathbb{Q}$, whereas in Example (4), the polynomials have coefficients in the $\mathbb{Q}$-algebra of $\mathbb{C}$ finitely generated over $\mathbb{Q}$ by the entries of $P, Q$, and $B$. In all examples, all the polynomials are homogeneous.

These examples lead to the following definitions.

For any finite subset $\ell \subset A$ of homogeneous polynomials, we let $Z((\ell))$ denote the subset of $\mathrm{Mat}_{M \times T}(\mathbb{C})$ of matrices $N$ such that $f(N) = 0$ for all $f \in \ell$. We call $Z((\ell))$ *a homogeneous algebraic set* in $\mathrm{Mat}_{M \times T}(\mathbb{C})$ *defined over* $R$[2]. Note that $\mathrm{Mat}_{M \times T}(\mathbb{C}) = Z((0))$, and $\emptyset = Z((1))$ are homogeneous algebraic sets defined over any $R$.

**Definition 1.** *Let $R$ be a subring of $\mathbb{C}$ that is a finitely generated $\mathbb{Q}$-algebra, and $A = R[X]$. An $M \times T$ generalized space-time scheme (GSTS) of length $n$ defined over $R$ is a set $V = \{V_i | 1 \leq r \leq n\}$ of homogeneous algebraic sets $V_r$ defined over $R$ such that*

$$\emptyset = V_0 \subseteq \cdots \subseteq V_r \subseteq \cdots \subseteq V_{n+1} = \mathrm{Mat}_{M \times T}(\mathbb{C}).$$

*For any $N \in \mathrm{Mat}_{M \times T}(\mathbb{C})$, define $d_V(N) = r$ if $N \in V_{r+1} - V_r$. Then the function $d_V$ is the diversity function of $V$.*

[2]We are using homogeneous algebraic set to refer to an affine algebraic set which is an affine cone over a projective algebraic set.

Setting $V_r = Z((\ell_r))$, we see from the above that the diversity function for the GSTSs defined by the $\ell_r$ in Examples (1)-(4) match the diversities for column distance codes, rank codes, sum-of-ranks codes, and spatio-temporal correlated codes, respectively.

A few technical points are in order. From now on we take $R$ to be a subring of $\mathbb{C}$ that is a finitely-generated $\mathbb{Q}$ algebra. Then $R$ is a noetherian ring, so $A = R[X]$ is a noetherian ring. We call an ideal in $A$ a *homogeneous ideal* if it can be generated by homogeneous polynomials. For any homogeneous ideal $J \subseteq A$, we let $Z(J)$ denote the subset of $\mathrm{Mat}_{M\times T}(\mathbb{C})$ of matrices $N$ such that $f(N) = 0$ for all $f \in J$.

We claim that every homogeneous algebraic set is $Z(J)$ for some homogeneous ideal $J$. On the one hand, if $\ell = \{f_1, ..., f_m\}$ is a finite set of homogeneous polynomials, and we let $J = (f_1, ...., f_m)$ denote the ideal generated by the elements of $\ell$, it follows that $Z((\ell)) = Z(J)$. On the other hand, it is easy to show that if $J$ is a homogeneous ideal, $f \in J$, and $f = \sum f_i$, where $f_i$ is homogeneous of degree $i$, then $f_i \in J$ for all $i$. Therefore, since $A$ is noetherian, any ideal is generated by a finite number of elements, so every homogeneous ideal $J$ is generated by a finite set of homogeneous polynomials $\ell$. Then $Z(J) = Z((\ell))$, establishing the claim.

Let $V = Z(J)$ be a homogeneous algebraic set. Then to $V$ we can attach a homogeneous ideal in $A$, $I(V) = \{f \in A | f(N) = 0, \forall N \in V\}$[3] . We have $Z(I(V)) = V$, and we get inclusion reversing maps between homogeneous ideals $J$ and homogeneous algebraic sets $V$ by

$$J \to Z(J)$$
$$V \to I(V).$$

Let $\mathcal{A}$ be a finite subset of $\mathbb{C}$, and let $\mathrm{Mat}_{M\times T}(\mathcal{A})$ denote the subset of matrices in $\mathrm{Mat}_{M\times T}(\mathbb{C})$ whose entries lie in $\mathcal{A}$.

**Definition 2.** *Let $\mathcal{A}$ be a finite subset of $\mathbb{C}$, $\mathcal{C}$ a subset of $\mathrm{Mat}_{M\times T}(\mathcal{A})$, and $V$ an $M \times T$ GSTS defined over $R$ of length $n$. We call the pair $\mathcal{S} = (\mathcal{C}, V)$ an $M \times T$ generalized space-time code (GSTC) of length $n$ defined over $\mathcal{A}$ and $R$, and define*

$$d_{\mathcal{S}} = \min_{C_1 \neq C_2 \in \mathcal{C}} d_V(C_1 - C_2)$$

*as the diversity order of $\mathcal{S}$. We call $\mathcal{A}$ the alphabet of $\mathcal{S}$ and $\mathcal{C}$ the codewords of $\mathcal{S}$.*

Let $\bar{\mathbb{Q}}$ denote the field of all algebraic numbers in $\mathbb{C}$. A good reference for all the number theory we will use is [17].

**Definition 3.** *A GSTS where $R \subset \bar{\mathbb{Q}}$ is called an arithmetic space-time scheme (ASTS).*

**Definition 4.** *A GSTC $\mathcal{S} = (\mathcal{C}, V)$, where $V$ is an ASTS and where the alphabet $\mathcal{A}$ of $\mathcal{S}$ is contained in $\bar{\mathbb{Q}}$, is called an arithmetic space-time code (ASTC).*

## 2. Every GSTC is arbitrarily well approximated by an ASTC

The goal of this section is to make the notions in its title precise. The first task is to come up with a definition of what it means for a subring of $\mathbb{C}$ which is a finitely generated algebra over $\mathbb{Q}$ to be approximated by a subring of $\bar{\mathbb{Q}}$ which is a finitely generated algebra over $\mathbb{Q}$ (which is therefore a number field). There are some pathologies we must avoid.

[3]Hilbert's Nullstellensatz [6] says that $I(Z(J)) = \{f \in A | \exists m, f^m \in J\}$.

If $R$ is $\mathbb{Q}[\alpha_1, ...., \alpha_m]$, the algebra finitely generated over $\mathbb{Q}$ by the complex numbers $\alpha_1, ..., \alpha_m$, the first natural guess of what an "$\epsilon$-approximation" to $R$ in $\bar{\mathbb{Q}}$ would be is a ring $R' = \mathbb{Q}[\beta_1, ..., \beta_m]$, where $\beta_i \in \bar{\mathbb{Q}}$ and $|\alpha_i - \beta_i| < \epsilon$. Since $\bar{\mathbb{Q}}$ is dense in $\mathbb{C}$, this can be achieved for any $\epsilon > 0$. However, unless some care is taken in the approximation, homogeneous algebraic sets defined over $R$ can behave very differently from the corresponding homogeneous algebraic sets defined over $R'$.

For example, if $R = \mathbb{Q}[\pi^{1/2}, \pi^{1/3}]$, then $V = Z(x + \pi^{1/3}y, \pi^{1/2}x + \pi^{5/6}y)$ is a line in $(x, y)$-space. If we set $\epsilon = .01$, and approximate $\pi^{1/3}, \pi^{1/2}$, and $\pi^{5/6}$ respectively by $1.46, 1.77$, and $2.60$, the resulting homogeneous algebraic set $Z(x+1.46y, 1.77x+2.60y)$ defined over $R' = \mathbb{Q}$ is now a point in $(x, y)$ space. This drop in dimension [4] occurs because the map from $R$ to $R'$ is not a $\mathbb{Q}$-algebra homomorphism.

On the other hand, with this approximation, the homogeneous algebraic set $Z(x + (1.77)\pi^{1/3}y, x + (1.46)\pi^{1/2}y)$, which is a point, gets sent to the homogeneous algebraic set $Z(x + (1.77)(1.46)y, x + (1.46)(1.77)y)$, which is a line. This jump in dimension occurs because we did not take $\epsilon$ small enough.

To remedy this, we go to our second natural guess:

**Definition 5.** *For any $\epsilon > 0$, we call a $\mathbb{Q}$-algebra homomorphism*

$$\phi : R = \mathbb{Q}[\alpha_1, ...., \alpha_m] \to \bar{\mathbb{Q}}$$

*an $\epsilon$-approximation of $R$ with respect to $\alpha_1, ..., \alpha_m$ if $|\phi(\alpha_i) - \alpha_i| < \epsilon$.*

Note that this definition depends on a choice of generators for $R$ as a $\mathbb{Q}$-algebra. However, if $\beta_1, ..., \beta_\ell$ is another set of generators, for every $\epsilon > 0$ there exists a $\delta > 0$ such that every $\delta$-approximation of $R$ with respect to $\beta_1, ..., \beta_\ell$ is an $\epsilon$-approximation of $R$ with respect to $\alpha_1, ..., \alpha_m$.

If $\phi$ is an $\epsilon$-approximation of $R$, then it induces a ring homomorphism $\phi_* : R[X] \to \bar{\mathbb{Q}}[X]$ by acting on coefficients of polynomials. Note that $\phi_*$ also maps homogeneous ideals of $R[X]$ to homogeneous ideals of $\bar{\mathbb{Q}}[X]$. This in turn induces a map $\phi_*$ from homogeneous algebraic sets $V = Z(I)$ defined over $R$ to homogeneous algebraic sets $\phi_*(V) = Z(\phi_*(I))$ defined over $R'$.

**Theorem 1.** *Let $V = Z(I)$ be a homogeneous algebraic set defined over $R = \mathbb{Q}[\alpha_1, ..., \alpha_m]$. Then for $\epsilon$ sufficiently small, and every $\epsilon$-approximation $\phi$ of $R$ with respect to $\alpha_1, ..., \alpha_m$, $\phi_*(V)$ has the same dimension as $V$.*

The proof of this theorem would take us too far afield.[5] In any case, the theorem gives us confidence that our definition of $\epsilon$-approximation is a reasonable one.

**Definition 6.** *Let $V = \{V_1, ..., V_n\}$ be a GSTS of length $n$ over $R$, and $\phi$ be an $\epsilon$-approximation of $R$. Then $\phi_*(V) = \{\phi_* V_1, ..., \phi_* V_n\}$ is an ASTS of length $n$*

[4]Here we can write a homogeneous algebraic set as a union of complex analytic spaces and take its dimension to be the maximum of the dimension of these spaces. Over an arbitrary algebraically closed field $k$, every homogeneous algebraic set is the union of its components — homogeneous algebraic subsets which are irreducible in the Zariski topology. We take the dimension of a homogeneous algebraic set to be the maximum of the dimensions of its components, and the dimension of an irreducible homogeneous algebraic set to be e.g., the transcendence degree of its function field over $k$. Equivalent definitions of dimension are in [6].

[5]Since the dimension of $V$ is the maximum of the dimensions of its irreducible components, it suffices to prove the theorem with $I$ replaced by any minimal prime containing it. Then Corollary 14.6 of [6] implies that the dimensions of $V$ and $\phi_*(V)$ are the same so long as $\phi(\alpha_1, ..., \alpha_m)$ is taken to lie in some Zariski open set containing $(\alpha_1, ..., \alpha_m)$. This suffices since Zariski open sets are open in the complex topology.

*(since $\phi_*$ preserves inclusions of homogeneous algebraic sets). If $\epsilon$ is sufficiently small such that the dimension of $\phi_*(V_i)$ is the same as the dimension of $V_i$ for all $1 \leq i \leq n$, we say that $\phi$ is an $\epsilon$-equivalence from $V$ to $\phi_*(V)$.*

**Theorem 2.** *For every GSTS $V$, and every $\epsilon > 0$, there is an ASTS $V'$ which is $\epsilon$-equivalent to $V$.*

*Proof.* By Theorem 1, if $V$ is defined over $R = \mathbb{Q}[\alpha_1, ..., \alpha_m]$, we need only show that $\epsilon$-approximations of $R$ exist for every $\epsilon > 0$. Given $R$, there is a surjective homomorphism $\tau : B = \mathbb{Q}[y_1, ..., y_m] \to R$, where $y_i$ are indeterminates, sending $y_i$ to $\alpha_i$. Let $\alpha$ denote the vector $(\alpha_1, ..., \alpha_m)$. Then the kernel of $\tau$ is the ideal $I$ of all polynomials in $B$ that vanish at $\alpha$, and $R \cong B/I$. Since $B$ is noetherian, there is a finite set $f_1, ..., f_n$ of generators for $I$. Suppose there are $\beta_1, ...., \beta_m \in \bar{\mathbb{Q}}$, with $|\alpha_i - \beta_i| < \epsilon$, such that if $\beta = (\beta_1, ..., \beta_m)$, then $f_i(\beta) = 0$ for all $1 \leq i \leq n$. Then the map $\phi : B \to \bar{\mathbb{Q}}$ defined by $\phi(y_i) = \beta_i$ descends to a homomorphism $\phi : R \cong B/I \to \bar{\mathbb{Q}}$ sending $\alpha_i$ to $\beta_i$, so is our desired $\epsilon$-approximation. That such a $\beta$ exists is the following lemma, applied with $E = \mathbb{Q}$. □

**Lemma 1.** *Let $E$ be a subfield of $\mathbb{C}$, and $\bar{E}$ the algebraic closure of $E$ in $\mathbb{C}$. Let $\{\alpha_1, ..., \alpha_m\} \subset \mathbb{C}$, and suppose that $f_1, ..., f_n \in \bar{E}[x_1, ..., x_m]$ vanish at $\alpha = (\alpha_1, ..., \alpha_m)$. Then for every $\epsilon > 0$, there exists $\beta_1, ..., \beta_m \in \bar{E}$ with $|\alpha_j - \beta_j| < \epsilon$, $1 \leq j \leq m$, such that $f_1, ..., f_n$ vanish at $\beta = (\beta_1, ..., \beta_m)$.*

*Proof. Step One:* If $T$ is an invertible linear transformation over $\bar{E}$, it suffices to prove the lemma for $\alpha_i' = T(\alpha_i), 1 \leq i \leq m$.

Indeed then $f_i'(x_1, ..., x_m) = f_i(T^{-1}(x_1), ..., T^{-1}(x_m))$ vanishes at $\alpha_1', ..., \alpha_m'$, for $1 \leq i \leq n$, so for any $\delta > 0$ there exist $\beta_j'$, $1 \leq j \leq m$, at which all $f_i'$ vanish, with $|\alpha_j' - \beta_j'| < \delta$. Then the $f_i$ vanish at $\beta_j = T^{-1}(\beta_j')$, and since $T^{-1}$ is continuous, we can take $\delta$ sufficiently small such that $|\alpha_j - \beta_j| < \epsilon$.

*Step Two:* The lemma holds if $\alpha_1, ..., \alpha_m$ are algebraically independent over $\bar{E}$.

Indeed then all $f_j$ must be the zero polynomial, and we can pick any $\beta_j \in \bar{E}$ with $|\alpha_j - \beta_j| < \epsilon$.

*Step Three:* The lemma is true for $\alpha_1, ..., \alpha_m$ if it holds for $\alpha_1, ..., \alpha_{m-1}$, and $\alpha_m$ is integral over $\bar{E}[\alpha_1, ..., \alpha_{m-1}]$.

Indeed, let $h$ be the minimal polynomial in $x_m$ of $\alpha_m$ over $\mathcal{R} = \bar{E}[\alpha_1, ..., \alpha_{m-1}]$, so $h = \sum_{k=0}^{\ell} h_k(\alpha_1, ..., \alpha_{m-1}) x_m^k$ for some $\ell$ and $h_k \in \bar{E}[x_1, ..., x_{m-1}]$. By assumption $h$ is monic, i.e., $h_\ell = 1$.

Likewise, $f_i = \sum_{k=0}^{l_i} f_{ik}(x_1, ..., x_{m-1}) x_m^k$ for some $\ell_i$ and $f_{ik} \in \bar{E}[x_1, .., x_{m-1}]$. Let $g_i = f_i(\alpha_1, ..., \alpha_{m-1}, x_m) \in \mathcal{R}[x_m]$, which vanishes when $x_m = \alpha_m$. By the minimality of $h$, $g_i$ is $h$ times a polynomial with coefficients in the fraction field of $\mathcal{R}$. Since $h$ is monic, the coefficients actually lie in $\mathcal{R}$. So there is some polynomial $q_i(x_1, ..., x_m)$ defined over $\bar{E}$ such that $g_i = q_i(\alpha_1, ..., \alpha_{m-1}, x_m)h$. In other words, if

$$\begin{aligned} \mu_i(x_1, ..., x_m) &= f_i - (\sum_{k=0}^{\ell} h_k(x_1, ..., x_{m-1}) x_m^k) q_i(x_1, ..., x_m) \\ &= \sum_{j=0}^{p_i} \mu_{ij}(x_1, ..., x_{m-1}) x_m^j, \end{aligned}$$

for some $p_i$, then the $\mu_{ij}$ all vanish at $\alpha_1, ..., \alpha_{m-1}$ and are defined over $\bar{E}$. Hence by hypothesis, for any $\delta > 0$ there exist $\beta_1, ..., \beta_{m-1}$ in $\bar{E}$ with $|\beta_j - \alpha_j| < \delta$,

$1 \leq j \leq m-1$, at which all $\mu_{ij}$ vanish. Hence

$$f_i(\beta_1, ..., \beta_{m-1}, x_m) = q_i(\beta_1, ..., \beta_{m-1}, x_m) \sum_{k=0}^{\ell} h_k(\beta_1, ..., \beta_{m-1}) x_m^k,$$

and all $f_i$ will vanish at any value of $x_m$ at which $h'(x_m) = \sum_{k=0}^{\ell} h_k(\beta_1, ..., \beta_{m-1}) x_m^k$ does.

By the continuity of the $h_k$ and the continuity of the roots of a polynomial in its coefficients, for $\delta$ sufficiently small, there is a $\beta_m$ in $\bar{E}$ which is a root of $h'$ such that $|\beta_m - \alpha_m| < \epsilon$. Shrinking $\delta$ if necessary, we have $|\alpha_j - \beta_j| < \epsilon$ for all $1 \leq j \leq m$, and all $f_i$ vanish at $\beta = (\beta_1, ..., \beta_m)$.

*Step 4.* Note that $\mathcal{R} = \bar{E}[\alpha_1, ..., \alpha_m]$ is an integral domain that is finitely generated over an infinite field. By Noether Normalization [6], there is an invertible linear transformation $T$ over $\bar{E}$ such that if $\alpha_i' = T(\alpha_i)$, then $\mathcal{R} = \bar{E}[\alpha_1', ..., \alpha_m']$, there is some $1 \leq q \leq m$ such that $\alpha_1', ..., \alpha_q'$ are algebraically independent over $\bar{E}$, and $\alpha_{q+1}', ..., \alpha_m'$ are integral over $\bar{E}[\alpha_1', ..., \alpha_q']$. By Step 2, the lemma holds for $\alpha_1', ..., \alpha_q'$. Applying Step 3 sequentially for $\alpha_{q+1}'$ to $\alpha_m'$, the lemma holds for $\alpha_1', ..., \alpha_m'$. Finally Step 1 shows that the lemma holds for $\alpha_1, ..., \alpha_m$, as desired. □

Given the theorem, we will say that every GSTS is *arbitrarily well approximated* by an ASTS. As a result, for engineering applications, we can focus our attention on the latter. Note that ASTSs are defined over $\bar{\mathbb{Q}}$, but since for such a $V = \{V_r\}$ of length $n$ there is a finite set of homogeneous generators for each $I(V_r)$, we get that each generating polynomial, and hence $V$, is defined over some number field.

One advantage of considering ASTSs is that the GSTCs built from them can in some sense be arbitrarily well approximated by ASTCs. To make this precise, we need to think of GSTCs as a *function* of the alphabet $\mathcal{A}$. We do so by incorporating the following notion.

**Definition 7.** *Let $V$ be a GSTS and $\mathcal{S}_1 = (\mathcal{C}_1, V)$ and $\mathcal{S}_2 = (\mathcal{C}_2, V)$ GSTCs on alphabets $\mathcal{A}_1$ and $\mathcal{A}_2$, respectively. Suppose that there is a bijection $\phi : \mathcal{A}_1 \to \mathcal{A}_2$ that induces a bijection $\mathcal{C}_1 \to \mathcal{C}_2$ (which we will also denote by $\phi$) acting on matrices entry-by-entry. If for every $C_1 \neq C_2 \in \mathcal{C}$, $d_V(\phi(C_1) - \phi(C_2)) = d_V(C_1 - C_2)$, we say that $\phi$ is an alphabet equivalence from $\mathcal{S}_1$ to $\mathcal{S}_2$, and that $\mathcal{S}_1$ and $\mathcal{S}_2$ are alphabet equivalent.*

Since $\bar{\mathbb{Q}}$ is dense in $\mathbb{C}$, one can approximate a given alphabet in $\mathbb{C}$ arbitrarily well by an alphabet consisting of algebraic numbers. However, as in the case of approximating GSTSs by ASTSs, unless one proceeds carefully, the diversity function of the difference of corresponding matrices can go up or down.

For example, for $2 \times 2$ rank codes with an alphabet of $\pi^{1/3}, \pi^{1/2}, \pi^{5/6}$, approximated within $\epsilon = .01$ respectively by 1.46, 1.77, and 2.60, the rank 1 matrix

$$\begin{pmatrix} 1 & \pi^{1/3} \\ \pi^{1/2} & \pi^{5/6} \end{pmatrix}$$

becomes rank 2, because the approximations do not induce a $\bar{\mathbb{Q}}$-algebra homomorphism of $\bar{\mathbb{Q}}[\pi^{1/3}, \pi^{1/2}]$ to $\bar{\mathbb{Q}}$, whereas the rank 2 matrix

$$\begin{pmatrix} 1.46 & \pi^{1/3} \\ 1.77 & \pi^{1/2} \end{pmatrix}$$

drops to rank 1 because $\epsilon$ is not small enough.

**Theorem 3.** *Let $V$ be an ASTS defined over a number field $K$. If $\mathcal{S}_1 = (\mathcal{C}_1, V)$ is a GSTC on an alphabet $\mathcal{A}_1$, then for every $\epsilon > 0$, there is an alphabet equivalent ASTC $\mathcal{S}_2 = (\mathcal{C}_2, V)$ on an alphabet $\mathcal{A}_2$, with the elements of $\mathcal{A}_2$ within $\epsilon$ of the corresponding elements of $\mathcal{A}_1$.*

*Proof.* Suppose that $V$ has length $n$ and $\ell_r$ is a finite set of homogeneous generators for $I(V_r)$ for every $1 \leq r \leq n$.

First of all, there is a bound $B_1$ such that for every $\epsilon < B_1$, the elements of $\mathcal{A}_1$ remain distinct when perturbed by at most $\epsilon$. So the matrices of $\mathcal{C}_1$ remain distinct when perturbed by at most $\epsilon$. Second since $\mathcal{A}_1$ and hence $\mathcal{C}$ is a finite set, it suffices to show for any fixed pair $C_1 \neq C_2 \in \mathcal{C}_1$, that there is an $\epsilon < B_1$ such that $d_V(\phi(C_1) - \phi(C_2)) = d_V(C_1 - C_2)$ whenever the elements of $\mathcal{A}_1$ are perturbed by at most $\epsilon$. To achieve this, we need to check two things. The first is if for some $1 \leq r \leq n$ and some $f \in \ell_r$, that $f(C_1 - C_2) \neq 0$, then the same is true when the elements of $\mathcal{A}_1$ are perturbed by at most $\epsilon$. This follows since the non-vanishing of a polynomial is an open condition. The second thing we need to show is that we can perturb $\mathcal{A}_1$ by an arbitrarily small $\epsilon$ to an alphabet in $\bar{\mathbb{Q}}$ in such a way that if all $f$ in any $\ell_r$ vanish at $C_1 - C_2$, then they still do so when $C_1$ and $C_2$ are perturbed. This follows from Lemma 1, applied with $E = K$. □

Given Theorems 2 and 3, we will say that GSTCs are *arbitrarily well approximated* by ASTCs. Therefore, for engineering applications, one really needs only to consider the latter. Since every ASTC has a finite alphabet $\mathcal{A} \subset \bar{\mathbb{Q}}$, in fact $\mathcal{A}$ lies in some number field. We will say that an ASTC $\mathcal{S} = (\mathcal{C}, V)$ is *defined over* a number field $K$ if both $V$ is defined over $K$ and the alphabet of $\mathcal{C}$ is contained in $K$. Recall that an ASTS is always defined over some number field, so every ASTC is defined over a number field.

## 3. Reducing ASTCs to codes defined over finite fields

Let $p$ be a prime, $e$ be a positive integer, $q = p^e$, $F = \mathbb{F}_q$, the field with $q$ elements, and $\bar{F}$ an algebraic closure of $F$. Let $A = F[X] = F[x_{ij}]_{1 \leq i \leq M, 1 \leq j \leq T}$. As before, for any homogeneous ideal $I \subseteq A$, we let $Z(I)$ denote the subset of $\mathrm{Mat}_{M \times T}(\bar{F})$ of matrices $N$ such that $f(N) = 0$ for all $f \in I$, which we call *a homogeneous algebraic set defined over $F$.*

**Definition 8.** *An $M \times T$ finite space-time scheme (FSTS) of length $n$ is a set of homogeneous algebraic sets $V = \{V_i | 1 \leq i \leq n\}$ defined over $F$ such that*

$$\emptyset = V_0 \subseteq \cdots \subseteq V_r \subseteq \cdots \subseteq V_{n+1} = \mathrm{Mat}_{M \times T}(\bar{F}).$$

*For any $N \in \mathrm{Mat}_{M \times T}(\bar{F})$, define $d_V(N) = r$ if $N \in V_{r+1} - V_r$. Then the function $d_V$ is the diversity function of the FSTS.*

**Definition 9.** *Let $\mathcal{A}$ be a finite subset of $\bar{F}$, $\mathcal{C}$ a subset of $\mathrm{Mat}_{M \times T}(\mathcal{A})$, and $V$ an $M \times T$ FSTS defined over $F$ of length $n$. We call the pair $\mathcal{S} = (\mathcal{C}, V)$ an $M \times T$ finite space-time code (FSTC) of length $n$ defined over $\mathcal{A}$ and $F$, and define*

$$d_{\mathcal{S}} = \min_{C_1 \neq C_2 \in \mathcal{C}} d_V(C_1 - C_2)$$

*as the diversity order of $\mathcal{S}$. We call $\mathcal{A}$ the alphabet of $\mathcal{S}$ and $\mathcal{C}$ the codewords of $\mathcal{S}$.*

Let $K$ be a number field, and let $\mathcal{O}_K$ denote the ring of integers in $K$. Let $\mathfrak{p}$ be a non-zero prime ideal of $\mathcal{O}_K$, so $F = \mathcal{O}_K/\mathfrak{p}$ is a finite field with $q = p^e$ elements for

some prime $p$ and some $e$. Let $\psi : \mathcal{O}_K \to F$ be the natural projection. We extend $\psi$ coefficient-by-coefficient to polynomials over $\mathcal{O}_K$, and then element-by-element to ideals in $\mathcal{O}_K$.

Let $\mathcal{S} = (\mathcal{C}, V)$ be an ASTC defined over $K$. We need to discuss the notions of what it means to *reduce* $V$ and $\mathcal{S}$ modulo $\mathfrak{p}$.

**Definition 10.** *Let $V = \{V_i\}$ be an ASTS of length $n$ defined over $K$. Let $J_r = I(V_r) \cap \mathcal{O}_K[X]$ for $1 \leq r \leq n$, so*

$$(0) \subseteq J_n \subseteq \cdots \subseteq J_r \subseteq \cdots \subseteq J_1 \subseteq (1).$$

*Let $\mathfrak{p} \subset \mathcal{O}_K$ be a prime ideal, $F = \mathcal{O}_K/\mathfrak{p}$, and $\psi : \mathcal{O}_K \to F$ the natural projection. Then $M_r = \psi(J_r)$ are homogeneous ideals in $F[X]$ such that*

$$(0) \subseteq M_n \subseteq \cdots \subseteq M_r \subseteq \cdots \subseteq M_1 \subseteq (1),$$

*so if $V'_r = Z(M_r)$, $\{V'_r\}$ defines a FSTS of length $n$ defined over $F$, which we call the reduction of $V$ modulo $\mathfrak{p}$ and denote as $\psi(V)$.*

To reduce an ASTC defined over $K$ modulo $\mathfrak{p}$, we first have to make sure that we can reduce its alphabet, which is a finite set which lies in $K$. Given any non-zero element $\alpha \in K$, we can uniquely write its principal ideal $(\alpha) = \mathfrak{a}/\mathfrak{b}$, where $\mathfrak{a}$ and $\mathfrak{b}$ are relatively prime ideals in $\mathcal{O}_K$. We call $\mathfrak{b}$ the *denominator* of $\alpha$. The map $\psi$ extends naturally to all the elements of $K$ whose denominators are not divisible by $\mathfrak{p}$.

Note that each $\alpha \in K$ has only finitely many primes ideals dividing its denominator. Given an ASTC $\mathcal{S} = (\mathcal{C}, V)$, let $\mathcal{A}$ be the alphabet of $\mathcal{S}$, and $D_{\mathcal{A}}$ be the finite set of all primes ideals dividing the denominator of some element of $\mathcal{A}$, which we call the *denominator* of $\mathcal{A}$.

**Definition 11.** *Let $\mathcal{S} = (\mathcal{C}, V)$ be an ASTC with alphabet $\mathcal{A}$ defined over a number field $K$, and $\mathfrak{p}$ a prime in $\mathcal{O}_K$, $\mathfrak{p} \notin D_{\mathcal{A}}$. Let $\psi : \mathcal{O}_K \to F = \mathcal{O}_K/\mathfrak{p}$ be the natural projection. We extend $\psi$ element-by-element to sets to define $\psi(\mathcal{A})$, then extend entry-to-entry to matrices to define $\psi(C)$ for $C \in \mathcal{C}$, and finally extend element-by-element to collections of matrices to define $\psi(\mathcal{C})$. Then $\psi(\mathcal{S}) = (\psi(\mathcal{C}), \psi(V))$ is a FSTC defined over $F$, which we call the reduction of $\mathcal{S}$ modulo $\mathfrak{p}$.*

*In addition, if $\psi : \mathcal{A} \to \psi(\mathcal{A})$ is an injection, and if for every $C_1 \neq C_2 \in \mathcal{C}$, $d_{\psi(V)}(\psi(C_1) - \psi(C_2)) = d_V(C_1 - C_2)$, we say that $\psi$ is an algebraic equivalence from $\mathcal{S}$ to $\psi(\mathcal{S})$.*

We can show that every ASTC is algebraically equivalent to an FSTC.

**Theorem 4.** *Let $\mathcal{S} = (\mathcal{C}, V)$ be an ASTC of length $n$ defined over a number field $K$. Then except for finitely-many prime ideals $\mathfrak{p} \subset \mathcal{O}_K$, the reduction map $\psi : \mathcal{O}_K \to \mathcal{O}_K/\mathfrak{p}$ induces an algebraic equivalence from $\mathcal{S}$ to $\psi(\mathcal{S})$, the reduction of $\mathcal{S}$ modulo $\mathfrak{p}$.*

*Proof.* As in Definition 10, let $J_r = I(V_r) \cap \mathcal{O}_K[X]$ for $1 \leq r \leq n$. Since $\mathcal{O}_K[X]$ is Noetherian, there is a finite set of homogeneous generators $\ell_r$ for $J_r$.

Let $D_{\mathcal{A}}$ be the denominator of the alphabet of $\mathcal{S}$. Since there are infinitely-many primes in $\mathcal{O}_K$, we need only check that there are only finitely-many $\mathfrak{p} \notin D_{\mathcal{A}}$ such that the elements of $\mathcal{A}$ do not remain distinct when reduced mod $\mathfrak{p}$, or such that if $C_1 \neq C_2 \in \mathcal{C}$, $f \in \ell_r$, for some $1 \leq r \leq n$, are such that $f(C_1 - C_2) \neq 0$, then $\psi(f)(\psi(C_1) - \psi(C_2)) = 0$. (Note that if $f(C_1 - C_2) = 0$, then since $\psi$ is a ring

homomorphism, automatically $\psi(f)(\psi(C_1) - \psi(C_2)) = 0$). These $\mathfrak{p}$ are precisely the set $Y$ of primes that divide any of the finite set of non-zero numbers

$$\{a_i - a_j | a_i \neq a_j \in \mathcal{A}\} \cup \{f(C_1 - C_2) | f(C_1 - C_2) \neq 0, C_1 \neq C_2 \in \mathcal{C}, f \in \ell_r, 1 \leq r \leq n\}.$$

That $Y$ is finite follows from the uniqueness of the factorization of non-zero ideals into the product of prime ideals in $\mathcal{O}_K$. □

## 4. Reducing ASTCs to codes defined over galois rings

We want to extend the results of the last section to codes defined over galois rings of arbitrary characteristic, because for engineering applications, it is most convenient to work over rings of characteristic 2. We will show that for a "scaled" version of an ASTC $\mathcal{S} = (\mathcal{C}, V)$ with alphabet $\mathcal{A}$, that for every prime ideal $\mathfrak{p} \subset \mathcal{O}_K$, there is an $m$ such that the reduction map $\psi : \mathcal{O}_K \to \mathcal{O}_K/\mathfrak{p}^m$ induces an appropriately defined algebraic equivalence from $\mathcal{S}$ to an analogously defined space-time code defined over the galois ring $\mathcal{O}_K/\mathfrak{p}^m$ with alphabet $\psi(A)$ and codewords $\{\psi(C) | C \in \mathcal{C}\}$.

Let us make these notions precise. Let $p$ be any prime, $K$ a number field, and $\mathfrak{p}$ a prime ideal of the ring of integers $\mathcal{O}_K$ of $K$ dividing $p$. For any $m$, $W = \mathcal{O}_K/\mathfrak{p}^m$ is a galois ring of characteristic $p$. (In fact, every galois ring of characteristic $p$ arises in this fashion for some $K, \mathfrak{p}$ and $m$.)

Let $A = W[X] = W[x_{ij}]_{1 \leq i \leq M, 1 \leq j \leq T}$. To state the definition of homogeneous algebraic set, we need an analogue of an algebraic closure for $W$. Let $\mathcal{O}_{K,\mathfrak{p}}$ be the completion of $\mathcal{O}_K$ at $\mathfrak{p}$, and let $\mathcal{O}_{\mathfrak{p}}^{ur}$ be the maximal unramified extension of $\mathcal{O}_{K,\mathfrak{p}}$. We will let $\bar{W} = \mathcal{O}_{\mathfrak{p}}^{ur}/\mathfrak{p}^m$. Note that when $m = 1$, this is nothing other than the algebraic closure of the finite field $\mathcal{O}_K/\mathfrak{p}$ ([6], p. 154). Given a homogeneous ideal $I \subset A$, we let $Z(I)$ denote the elements in $\mathrm{Mat}_{M \times T}(\bar{W})$ at which every polynomial in $I$ vanishes, which we call a *homogeneous algebraic set* defined over $W$.

**Definition 12.** *An $M \times T$ galois ring space-time scheme (RSTS) of length $n$ is a set of homogeneous algebraic sets $V = \{V_i | 1 \leq i \leq n\}$ defined over $W$ such that*

$$\emptyset = V_0 \subseteq \cdots \subseteq V_r \subseteq \cdots \subseteq V_{n+1} = \mathrm{Mat}_{M \times T}(\bar{W}).$$

*For any $N \in \mathrm{Mat}_{M \times T}(\bar{W})$, define $d_V(N) = r$ if $N \in V_{r+1} - V_r$. We call the function $d_V$ the diversity function of $V$.*

**Definition 13.** *Let $\mathcal{A}$ be a finite subset of $\bar{W}$, $\mathcal{C}$ a subset of $\mathrm{Mat}_{M \times T}(\mathcal{A})$, and $V$ an $M \times T$ RSTS defined over $W$ of length $n$. We call the pair $\mathcal{S} = (\mathcal{C}, V)$ an $M \times T$ galois ring space-time code (RSTC) of length $n$ defined over $\mathcal{A}$ and $W$, and define*

$$d_{\mathcal{S}} = \min_{C_1 \neq C_2 \in \mathcal{C}} d_V(C_1 - C_2)$$

*as the diversity order of $\mathcal{S}$. We call $\mathcal{A}$ the alphabet of $\mathcal{S}$ and $\mathcal{C}$ the codewords of $\mathcal{S}$.*

Let $\psi : \mathcal{O}_K \to W$ be the natural projection. We extend $\psi$ coefficient-by-coefficient to polynomials over $\mathcal{O}_K$, and then element-by-element to ideals of polynomials over $\mathcal{O}_K$. We also extend $\psi$ entry-by-entry to matrices over $\mathcal{O}_K$, and then to collection of matrices over $\mathcal{O}_K$.

Reducing an ASTS $V$ modulo $\mathfrak{p}^m$ to an RSTS $\psi(V)$ follows the same procedure as reducing modulo $\mathfrak{p}$ *mutatis mutandis*: the tricky thing is reducing ASTCs. Let $\mathcal{S} = (\mathcal{C}, V)$ be an ASTC defined over $K$. To reduce $\mathcal{S}$ modulo $\mathfrak{p}^m$, we first have to make sure that we can reduce its alphabet $\mathcal{A}$, which is a finite set in $K$. As we saw in the last section, this can only be achieved for every $\mathfrak{p}^m$ if in fact $\mathcal{A} \subset \mathcal{O}_K$.

**Definition 14.** *An ASTC $\mathcal{S}(\mathcal{C}, V)$ defined over a number field $K$ is called an integral space-time code (ISTC) defined over $K$ if its alphabet $\mathcal{A}$ is contained in the ring of integers $\mathcal{O}_K$ of $K$.*

**Definition 15.** *Let $\mathcal{S} = (\mathcal{C}, V)$ with alphabet $\mathcal{A}$ be an ISTC defined over a number field $K$ and $\mathfrak{p}$ a non-zero prime ideal in the ring of integers of $K$. Let $\psi : \mathcal{O}_K \to \mathcal{O}_K/\mathfrak{p}^m$ be the natural projection. We define the reduction of $\mathcal{S} = (\mathcal{C}, V)$ modulo $\mathfrak{p}^m$ to be the RSTC $\psi(S) = (\psi(\mathcal{C}), \psi(V))$.*

*If in addition, $\psi : \mathcal{A} \to \psi(\mathcal{A})$ is an injection, and if for every $C_1 \neq C_2 \in \mathcal{C}$, $d_{\psi(V)}(\psi(C_1) - \psi(C_2)) = d_V(C_1 - C_2)$, we say that $\psi$ is an algebraic equivalence from $\mathcal{S}$ to $\psi(\mathcal{S})$.*

We can now show that every ISTC is algebraically equivalent to an RSTC for chosen $\mathfrak{p}$ and some $m$.

**Theorem 5.** *Let $\mathcal{S} = (\mathcal{C}, V)$ be an ISTC of length $n$ defined over a number field $K$, and $\mathfrak{p}$ a non-zero prime ideal in the ring of integers of $K$. Then there is an $m$ such that the reduction map $\psi : \mathcal{O}_K \to \mathcal{O}_K/\mathfrak{p}^m$ induces an algebraic equivalence from $\mathcal{S}$ to $\psi(\mathcal{S})$.*

*Proof.* As in the proof of Theorem 4, for $1 \leq r \leq n$, let $\ell_r$ be a finite set of homogeneous generators of $J_r = I(V_r) \cap \mathcal{O}_K[X]$.

We need only check that there is an $m$ such that the elements of $\mathcal{A}$ remain distinct when reduced mod $\mathfrak{p}^m$, and such that if $C_1 \neq C_2 \in \mathcal{C}$, $f \in \ell_r$, for some $1 \leq r \leq n$, are such that $f(C_1 - C_2) \neq 0$, then $\psi(f)(\psi(C_1) - \psi(C_2)) \neq 0$. (Again, if $f(C_1 - C_2) = 0$, then automatically $\psi(f)(\psi(C_1) - \psi(C_2)) = 0$). That is, we need an $m$ such that $\mathfrak{p}^m$ does not divide any of the finite set of non-zero numbers

$$\{a_i - a_j | a_i \neq a_j \in \mathcal{A}\} \cup \{f(C_1 - C_2) | f(C_1 - C_2) \neq 0, C_1 \neq C_2 \in \mathcal{C}, f \in \ell_r, 1 \leq r \leq n\}.$$

That $m$ exists follows from the uniqueness of the factorization of ideals into the product of prime ideals in $\mathcal{O}_K$. □

Note that in the definition of a GSTS $V$, all the algebraic sets are homogeneous, so for any $r$, $M \in V_r$ if and only if $\alpha M \in V_r$ for any non-zero complex number $\alpha$. Hence GSTCs have another notion of equivalence, which we will call *scaling*. Let $\mathcal{S} = (\mathcal{C}, V)$ be any GSTC with alphabet $\mathcal{A}$. Extending the map $\sigma_\alpha : \mathbb{C} \to \mathbb{C}$ defined by $\sigma_\alpha(x) = \alpha x$ to sets, entry-by-entry to matrices, and then to sets of matrices, we immediately get that $(\sigma_\alpha(\mathcal{C}), V)$ is a GSTC with alphabet $\sigma_\alpha(\mathcal{A})$. We will let $\alpha(\mathcal{S}) = (\sigma_\alpha(\mathcal{C}), V)$, and call it $\mathcal{S}$ *scaled by* $\alpha$. Note that for any $C_1, C_2 \in \mathcal{C}$, $d_{\alpha(\mathcal{S})}(\sigma_\alpha(C_1), \sigma_\alpha(C_2)) = d_{\mathcal{S}}(C_1, C_2)$.

**Definition 16.** *We call the two GSTCs $\mathcal{S}_1 = (\mathcal{C}_1, V)$ and $\mathcal{S}_2 = (\mathcal{C}_2, V)$ scale equivalent if there is a non-zero $\alpha$ such that $\mathcal{S}_2 = \alpha(\mathcal{S}_1)$. Note that this is an equivalence relation on GSTCs.*

We immediately get the following.

**Theorem 6.** *Let $\mathcal{S} = (\mathcal{C}, V)$ be an ASTC defined over a number field $K$ whose alphabet $\mathcal{A}$ has denominator $\mathfrak{b}$. Then for any $\alpha \in \mathcal{O}_K$ divisible by $\mathfrak{b}$, the equivalent scaled $\alpha(\mathcal{S})$ is an ISTC.*

**Corollary 1.** *Every GSTC is arbitrarily well approximated by an ASTC, which is scale equivalent to an ISTC, which is in turn algebraically equivalent to a RSTC defined over a galois ring of any given characteristic $p$.*

## 5. A Singleton Bound For Linear FSTCs

We will say an FSTC $\mathcal{S} = (\mathcal{C}, V)$ defined over some $\mathbb{F}_q$ is *linear* if $\mathcal{C}$ is a vector space over $\mathbb{F}_q$, that an $M \times T$ linear FSTC defined over $\mathbb{F}_q$ of dimension $k$ and diversity order $d = d_{\mathcal{S}}$ has parameters $[M, T, k, d]$, and in this case that $\mathcal{S}$ is an $[M, T, k, d]$-code.

There is a general notion of a "Singleton bound" for such codes $V = \{V_r\}$, making use of the Chevalley-Warning Theorem, which depends upon the degrees of homogeneous generators of $I(V_r)$.

**Theorem 7.** *a) (Chevalley-Warning) Let $f_1, ..., f_t$ be homogeneous polynomials of degrees $d_1, ..., d_t$ in $m$ variables over a finite field. If $\sum_{i=1}^{t} d_t < m$, then there is an $\alpha \in \mathbb{F}_q^m$, $\alpha \neq (0, ..., 0)$, such that $f_1(\alpha) = \cdots = f_t(\alpha) = 0$.*

*b) Let $V = \{V_r\}$ be a FSTS of length $n$ defined over $\mathbb{F}_q$, $\ell_r$ a set of homogeneous generators for $I(V_r)$, and $\delta_r = \sum_{f \in \ell_r} \deg f$, for each $1 \leq r \leq n$. Let $\mathcal{S} = (\mathcal{C}, V)$ be a linear $[M, T, k, d]$-code. If $d \geq r$, then $k \leq \delta_r$.*

*Proof.* Suppose that $N_1, ..., N_k$ is a basis for $\mathcal{C}$. Then for every $f \in \ell_r$, if $z_1, ..., z_k$ are indeterminates, then $f'(z_1, ..., z_k) = f(\sum_{i=1}^{k} z_i N_i)$ either vanishes or is a homogeneous polynomial in $z_1, ..., z_k$ of degree $\deg f$. If $k > \delta_r$, then by (a), there is a common non-trivial zero $(z'_1, ..., z'_k)$ of all the $f'$ for $f \in \ell_r$, so there is a non-zero matrix $N = \sum_{i=1}^{k} z'_i N_i \in V_r \cap \mathcal{C}$. Therefore $d_V(N, 0) < r$ and hence $d < r$. □

EXAMPLE 2 (cont.) The bound in (b) is only interesting if it beats the trivial bound of $k \leq MT$. It is in general quite weak, but is occasionally sharp. For example, if $\mathcal{S}$ is a rank $[M, M, k, d]$ code over $\mathbb{F}_q$, then we can take $\ell_M$ as the degree $m$ polynomial which is the determinant $\det X = \det[x_{ij}]_{1 \leq i,j \leq M}$, so $\delta_M = M$. Hence if $d = M$, (b) gives $k \leq M$, which is sharp.

## 6. Lifting codes defined over finite fields and galois rings to Space-Time codes

The main result of this paper is that every GSTC can be arbitrarily well approximated by an ASTC, which in turn reduces to an algebraically equivalent FSTC, and is scale equivalent to an ISTC, which reduces to an algebraically equivalent RSTC over a galois ring of arbitrary characteristic.

In practice for code construction, one would want to go the other way: start with an FSTC or RSTC and *use* it to construct an ASTC or ISTC. We call this process *lifting*, which is the inverse operation to reducing. More precisely, we say an ASTC (or ISTC) $\mathcal{S}$ over a number field $K$ is *lifted* from an FSTC (or RSTC) $\mathcal{S}'$ if $\mathcal{S}'$ is a reduction of $\mathcal{S}$ modulo a prime $\mathfrak{p}$ (or $\mathfrak{p}^m$) in $\mathcal{O}_K$. Note that we do not require that $\mathcal{S}$ be algebraically equivalent to $\mathcal{S}'$. On the other hand, the proofs of Theorems 4 and 5 show that if $\mathcal{S} = (\mathcal{C}, V)$ is a lift of $\mathcal{S}' = (\mathcal{C}, V')$, and $C'_1, C'_2 \in \mathcal{C}'$ lift to $C_1, C_2 \in \mathcal{C}$, then

$$d_V(C_1, C_2) \geq d_{V'}(C'_1, C'_2). \tag{2}$$

*Remark 1.* In [13] lifting was done from rank codes defined over $\mathbb{Z}[i]/2^m$ to rank codes over $K = \mathbb{Q}(\sqrt{-1})$ whose alphabets were in QAM-constellations by the method we just described. The same method was used to lift from finite fields to the Gaussian integers in [16].

*Remark 2.* We have seen that scaling is one type of equivalence of GSTCs, but another is *shift equivalence*, where we shift the alphabet $\mathcal{A}$ of a GSTC by adding

a constant, and then correspondingly shift every entry of every codeword by that constant. Since the diversity order of a GSTS is defined in terms of the *difference* of two codewords, this changes nothing essential. This gives us a slightly more general notion of lifting, where we lift as above and then replace the lifted ASTC by a shift equivalent one. This was exploited in the lifting methods used in [9], [14], and [15].

To recall how this was done, let $p$ be a prime number, $\zeta$ a primitive $p$-th root of unity, and $K = \mathbb{Q}(\zeta)$, so $\mathbb{Z}[\zeta]$ is the ring on integers of $K$. Then we have an isomorphism $\psi : \mathbb{Z}[\zeta]/(1-\zeta) \to \mathbb{Z}/p\mathbb{Z}$ sending $\zeta$ to 1. Under this isomorphism, $\xi_i = (\zeta^i - 1)/(\zeta - 1)$, for $0 \leq i \leq p-1$, are representatives for $\mathbb{Z}/p\mathbb{Z}$, so FSTCs defined over $\mathbb{Z}/p\mathbb{Z}$ can be lifted to ISTCs on the alphabet $\mathcal{A} = \{\xi_i\}$. Then $\mathcal{A}$ can be scaled by multiplying by $\zeta - 1$, and then in turn shifted by adding 1 to get equivalent ISTCs on the alphabet $\{\zeta^i\}$, the $p$-ary PSK constellation. This method is generalized in [9], [14], and [15] for lifting codes from $\mathbb{Z}/p^m\mathbb{Z}$ to the $p^m$-ary PSK constellation, by taking the $p$-adic expansion of codes defined over $\mathbb{Z}/p^m\mathbb{Z}$ and considering them as $m$-tuples of codes defined over $\mathbb{Z}/p\mathbb{Z}$. One could expand the theory of RSTCs given in section 5 to encompass such constructions as well, but we will not pursue this here.

*Remark 3.* One problem with these methods is that linear codes defined over $\mathcal{O}_k/\mathfrak{p}^m$ (that is, codes which are free $\mathcal{O}_k/\mathfrak{p}^m$-modules) do not necessarily lift to codes whose alphabets (information symbols) lie in a lattice. The advantage of having the information symbols lie in a lattice is that decoding (in principle) can then be done with a sphere decoder, so decoding can be done with the LLL algorithm and the complexity of decoding is expected to be tractable.

There is a simple way to get around this. To lift a linear RSTC $\mathcal{S}' = (\mathcal{C}', V')$ of diversity order $d$ defined over $\mathcal{O}_K/\mathfrak{p}^m$ to a code defined over $\mathcal{O}_K$, if $V$ is an ASTS defined over $K$ which reduces to $V'$, then one can arbitrarily lift a basis $\alpha_1, ..., \alpha_k$ for $\mathcal{C}'$ to matrices $A_1, ..., A_k$ with entries in $\mathcal{O}_K$, and let $\mathcal{C} = \{\sum_{i=1}^k b_i A_i | b_i \in D\}$, where $D$ is some fixed set of representatives in $O_K$ for $\mathcal{O}_K/\mathfrak{p}^m$. Note that $\mathcal{S} = (\mathcal{C}, V)$ reduces to $\mathcal{S}'$, and that by (2), the diversity order of $\mathcal{S}$ is at least $d$ (and a gain in diversity order only helps in applications). If $p$ is the rational prime contained in $\mathfrak{p}$, and $p$ does not divide the discriminant of $K$, then as an additive group, $\mathcal{O}_K/\mathfrak{p}^m \cong (\mathbb{Z}/p^m\mathbb{Z})^f$ for some $f$, so $D$ can be chosen so that the information symbols lie in a lattice.

EXAMPLE 5. Recall that the so-called Golden Code [1], [5] is a rank code whose (infinite) set of codewords are of the form

$$\frac{1}{\sqrt{5}} \begin{pmatrix} \alpha(a+b\theta) & \alpha(c+d\theta) \\ i\bar{\alpha}(c+d\bar{\theta}) & \bar{\alpha}(a+b\bar{\theta}) \end{pmatrix},$$

where $a, b, c, d \in \mathbb{Z}[i]$, $\theta = (1+\sqrt{5})/2$, $\alpha = 1 + i - i\theta$, and where a bar denotes the automorphism of $K = \mathbb{Q}(\sqrt{5}, i)$ over $\mathbb{Q}(i)$ that takes $\sqrt{5}$ to $-\sqrt{5}$. In practice, the alphabet is finite, giving rise to a rank code, with $a, b, c, d$ restricted to some QAM-constellation.

Let $\mathcal{C}$ be the ASTC over $K$ gotten by taking $a, b, c, d \in \{\pm 1 \pm i\}$, the 4-QAM constellation. Let $\mathfrak{p}$ be either of the 2 primes in $\mathcal{O}_K$ that divides 7. Then one can check that $\psi : \mathcal{O}_K \to \mathcal{O}_K/\mathfrak{p} = \mathbb{F}_{49}$ induces an algebraic equivalence from $\mathcal{C}$ to its reduction $\mathcal{C}' = \psi(\mathcal{C})$ over $\mathbb{F}_{49}$. Hence $\mathcal{C}$ is a lift of $\mathcal{C}'$.

## References


[1] J-C. Belfiore, G. Rekaya and E. Viterbo. *The Golden Code: A $2 \times 2$ full-rate space-time code with nonvanishing determinants.* IEEE Trans. Inform. Theory **51**. No. 4, (2005), 1432–1436.

[2] J-C. Belfiore and G. Rekaya. *Quaternionic lattices for space-time coding.* Proceedings of the Information Theory Workshop. IEEE, Paris, 31 March - 4 April 2003.

[3] M. O. Damen, A. Tewfik, and J-C. Belfiore. *A construction of a space-time code based on number theory.* IEEE Trans. Inform. Theory, **48** (2002)

[4] M. O. Damen, K. Abel-Meraim, and J-C. Belfiore. *Diagonal algebraic space-time block codes.* IEEE Trans. Inform. Theory. **48** (2002)

[5] P. Dayal and M. K. Varanasi, *An optimal two transmit antenna space-time code and its stacked extensions.* IEEE Trans. Inform. Theory **51**, No. 12 (2005), 4348–4355.

[6] D. Eisenbud. "Commutative Algebra with a view towards Algebraic Geometry," Springer, 1999.

[7] P. Elia, K. R. Kumar, S. Pawar, P. V. Kumar, and H. Lu. *Explicit Space-Time Codes Achieving The Diversity-Multiplexing Gain Tradeoff.* ISIT Proceedings (2005) 896–900.

[8] P. Elia, B. A. Sethuraman, and P. V. Kumar. *Perfect SpaceTime Codes for Any Number of Antennas.* IEEE Trans. Inform. Theory **53**, No. 11 (2007), 3853–3868.

[9] A. R. Hammonds and H. El Gamal. *On the theory of space-time codes for PSK modulation.* IEEE Trans. Inform. Theory **46**. No. 2 (2000), 524–542.

[10] T. Kiran and B. Sundar Rajan. *STBC-schemes with nonvanishing determinant for certain number of transmit antennas.* IEEE Trans. Inform. Theory **51** (2005), 2984–2992.

[11] T. Kiran and B. Sundar Rajan. *Optimal Rate-Diversity Tradeoff STBCs from Codes over Arbitrary Finite Fields.* Proc. 2005 IEEE ICC (2005), 435–457.

[12] T. Kiran and B. Sundar Rajan. *Optimal STBCs from Codes Over Galois Rings.* Proc. IEEE ICPWC (2005), 120–124.

[13] Y. Liu, M. P. Fitz, and O. Y. Takeshita. *A rank criterion for QAM space-time codes.* IEEE Trans. Inform. Theory **48**. No. 12, (2002), 3062–3079.

[14] H-f. Lu and P. V. Kumar. *Rate-Diversity tradeoff of space-time codes with fixed alphabet and optimal constructions for PSK modulation.* IEEE Trans. Inform. Theory **49**. No. 10, (2003), 2747–2751.

[15] H-f. Lu and P. V. Kumar. *A unified construction of space-time codes with optimal rate-diversity tradeoff.* IEEE Trans. Inform. Theory **51**, No. 5 (2005), 1709–1730.

[16] P. Lusina, E. Gabidulin, and M. Bossert. *Maximal rank distance codes as space-time codes.* IEEE Trans. Inform. Theory **49**. No. 10, (2003), 2757–2760.

[17] J. Neukirch, "Algebraic Number Theory," Springer, Berlin, 1999.

[18] F. Oggier, G. Rekaya, J-C. Belfiore, and E. Viterbo. *Perfect Space-Time Block Codes.* IEEE Trans. Inform. Theory, **52** (2006), 3885–3902.

[19] M. Reid. "Undergraduate Algebraic Geometry", London Mathematica l Society Student Texts, 12. Cambridge University Press, Cambridge-New York, 1988.

[20] B. A. Sethuraman, B. Sundar Rajan, and V. Shashidhar. *Full-diversity, high-rate space-time block codes from division algebras.* IEEE Trans. Inform. Theory **49**, (2003) 2596–2616.

[21] M. K. Varanasi and P. Dayal, *Unified multi-antenna code design for fading channels with spatio-temporal correlations.* IEEE Trans. Wireless Systems **5**, No. 8 (2006), 2266–2276.

[22] S. Wilson. "Digital Modulation and Coding," Prentice Hall, Upper Saddle River, NJ, 1996



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