Divisors on Division Algebras and Error Correcting Codes

Patrick J. Morandi
Department of Mathematical Sciences
New Mexico State University
Las Cruces, NM 88003
pmorandi@nmsu.edu

B.A. Sethuraman*
Department of Mathematics
California State University, Northridge
Northridge, CA 91330
al.sethuraman@csun.edu

1 Introduction

Recall that a (linear) code is just a k-subspace C of k^n, where k is some finite field. The elements of C are referred to as *codewords,* and the *dimension* of the code, $\dim(C)$, is just the dimension of C as a k-space. The *length* of the code is the dimension of the ambient space k^n; that is, the length of C is n. The *minimum distance,* $d(a, b)$ between two codewords $a = (a_1, \ldots, a_n)$ and $b = (b_1, \ldots, b_n)$ is defined by $d(a, b) = |\{i \mid a_i \neq b_i\}|$, and the *minimum distance of the code,* $d(C)$, is defined by $d(C) = \min\{d(a, b) \mid a, b \in C, a \neq b\}$. The *weight,* $w(a)$, of a codeword $a = (a_1, \ldots, a_n)$ is defined by $w(a) = |\{i \mid a_i \neq 0\}|$. The linearity of the code ensures that $d(C)$ is also equal to $\min\{w(a) \mid a \in C, a \neq 0\}$.

*Supported in part by a grant from the N.S.F.

A major goal in coding theory is to construct codes whose minimum distance and dimension are large relative to their length. *Goppa Codes* were introduced by Goppa in [3] (in a form dual to the one we consider here), and are effective at achieving this goal. One starts with a smooth geometrically irreducible projective curve X/k (and thus, a function field F/k), and a divisor $E = P_1 + \cdots + P_n$, where the P_i are prime divisors of degree 1. One fixes a divisor G such that the support of E and G are disjoint (this guarantees that any $f \in \mathcal{L}(G)$ is automatically in each valuation ring $\mathcal{O}_{P_i}$). One then considers the evaluation map $\mathrm{ev} : \mathcal{L}(G) \to k^n$ given by $f \mapsto (f(P_1), \ldots, f(P_n))$, where by $f(P_i)$, we mean the residue of f with respect to the valuation at P_i. Since ev is k-linear, the image is a k-subspace of k^n; this is the Goppa code associated to the curve X/k and the divisors E and G.

We provide in this paper an analogous construction of codes using division algebras D defined over the function field F/k. The structure of such a D is of course well-understood from class field theory; we exploit this structure in our construction. Places of the field F/k are now replaced by maximal orders, selected to form a *sheaf* of maximal orders over X. By work of various authors (see [9], [11], and [12]), one has an analogous definition of divisors in this situation, as well as a definition of the spaces $\mathcal{L}(G)$ for any division algebra divisor G, and a noncommutative Riemann-Roch Theorem.

Our code is actually an l-code, where l is a finite extension of k that arises naturally as the residue of D. The function field lF is a maximal subfield of our division algebra; we prove that under certain conditions our l-code is the same as the commutative Goppa code obtained by restricting our division algebra divisors in a suitable manner to lF.

2 Maximal Orders and Divisors

As mentioned in the introduction, we will use maximal orders in our construction of codes. We recall here the basic properties of maximal orders over discrete valuation rings. A good reference for maximal orders is Reiner's book [5]. Let A be an integral domain with quotient field F and let S be an F-central simple algebra. A subring B of S with $B \supseteq A$ is an A-*order* if B is a finitely-generated A-module and if $BF = S$. If B is maximal with respect to inclusion among all A-orders in S, then B is said to be a *maximal order* over A.

If A is a discrete valuation ring with quotient field F, then the following properties hold for maximal A-orders in an F-central simple algebra S:

1. Maximal A-orders exist and are unique up to conjugation.
2. If B is a maximal A-order in S, then the Jacobson radical $J(B)$ is the unique maximal ideal of B, and every ideal of B is a power of $J(B)$.
3. There is a $b \in B$ with $J(B) = Bb = bB$.
4. The residue ring $\overline{B} = B/J(B)$ is simple and finite dimensional over $\overline{A} = A/J(A)$.

Proofs of these properties can be found in [5, Theorems 18.3, 18.7].

In this paper we need to make use of value functions. If A is a discrete valuation ring and if B is a maximal A-order in S, then we can define a function $w : S - \{0\} \to \mathbb{Z}$ in the following way: For $b \in B$, we set $w(b) = n$ if $BbB = J(B)^n$. More generally, if $s \in S$, write $s = b\alpha^{-1}$ with $b \in B$ and $\alpha \in A$, and set $w(s) = w(b) - w(\alpha)$. It is not hard to see that w is well defined and that w satisfies the following properties:

1. $w(s + t) \geq \min\{w(s), w(t)\}$;
2. $w(st) \geq w(s) + w(t)$, and $w(st) = w(s) + w(t)$ if $s \in Z(S)$;
3. $B = \{s \in S \mid w(s) \geq 0\} \cup \{0\}$ and $J(B) = \{s \in S \mid w(s) > 0\} \cup \{0\}$.

Moreover, w is uniquely determined by B. We call w the value function on S corresponding to B. We will denote by Γ_B the *value group* of B; that is, $\Gamma_B = \mathrm{im}(w_B) = \mathbb{Z}$. We refer the reader to [6, Sec. 2] for more information about value functions.

Suppose that X is a smooth geometrically irreducible projective curve defined over a field k, and let F be the function field of X. Let S be a central simple F-algebra, and suppose that we have a maximal $\mathcal{O}_P$-order B_P in S for each $P \in X$. Let w_P be the value function on S corresponding to B_P. Note that w_P depends on both the point P and the choice of maximal order B_P. Let e_P be the index $[\mathbb{Z} : w_P(F^*)]$. We will call e_P the *ramification index* of S/F with respect to P.

We will be working with sheaves of maximal orders on X. We call a sheaf Λ of rings on X a sheaf of maximal orders in S if $\Lambda(U)$ is a maximal

$\mathcal{O}(U)$-order in S for every proper open subset U of X. Let $\mathcal{S}$ be the constant sheaf $\mathcal{S}(U) = S$ on X. We recall that any sheaf of maximal orders on X is isomorphic to a subsheaf of $\mathcal{S}$. Here is a sketch of the argument. Let ζ be the generic point of X. If Λ is a sheaf of $\mathcal{O}_X$-maximal orders in S, then the structure maps $\varphi_U : \Lambda(U) \to \Lambda_\zeta$ extend by bilinearity to a map $\theta_U : \Lambda(U) \otimes_{\mathcal{O}(U)} \mathcal{O}_\zeta \to \Lambda_\zeta$. Now $\mathcal{O}_\zeta = F$, and for every proper open set U, $\Lambda(U)$ is a maximal $\mathcal{O}(U)$ order, so the map $\Lambda(U) \otimes_{\mathcal{O}(U)} F \to S$ induced by the inclusion $\Lambda(U) \subseteq S$ is an isomorphism. For every proper open set U, we thus have a map $\theta'_U : S \to \Lambda_\zeta$. θ'_U is an injection as S is simple. Since any $z \in \Lambda_\zeta$ is in $\varphi_V(\Lambda(V))$ for some open V, we find $z \in \theta_V(\Lambda(V) \otimes_{\mathcal{O}(V)} \mathcal{O}_\zeta)$. We may assume $V \subseteq U$. The structure map $\varphi_{UV} : \Lambda(U) \to \Lambda(V)$ induces an isomorphism $\Lambda(U) \otimes_{\mathcal{O}(U)} \mathcal{O}_\zeta \cong \Lambda(V) \otimes_{\mathcal{O}(V)} \mathcal{O}_\zeta$ (as each side is isomorphic to S), so we find $z \in \theta_U(\Lambda(U) \otimes_{\mathcal{O}(U)} \mathcal{O}_\zeta)$ as well. Thus, $\Lambda_\zeta \cong S$. We thus have injective maps $\varphi_U : \Lambda(U) \to \Lambda_\zeta \cong S$ for each proper open set $U \subseteq X$. Using the sheaf property of $\Lambda(X)$ and the fact that the structure map $\varphi_X : \Lambda(X) \to \Lambda_\zeta$ factors through $\Lambda(U)$ for every proper open set U, it is easy to see that φ_X is injective as well. Since $\varphi_U = \varphi_V \varphi_{UV}$ for open sets $V \subseteq U$, we have an injective sheaf map from Λ to the constant sheaf $\mathcal{S}$.

Lemma 1 *Suppose for every $P \in X$ that there is a maximal $\mathcal{O}_P$-order B_P in S, and let w_P be the value function on S corresponding to B_P. Then, for each $s \in S$, we have $w_P(s) \geq 0$ for all but finitely many P if and only if there is a sheaf Λ of maximal $\mathcal{O}_X$-orders on X such that for each $P \in X$, the stalk Λ_P is equal to B_P.*

Proof: Suppose there is a sheaf $\Lambda \subseteq \mathcal{S}$ of maximal orders such that $\Lambda_P = B_P$ for each $P \in X$. Let $s \in S$. If U is any proper open subset of X, we may write $s = b\alpha^{-1}$ with $b \in \Lambda(U)$ and $\alpha \in \mathcal{O}(U)$. There is a nonempty open subset V of U such that $\alpha^{-1} \in \mathcal{O}(V)$, so $s \in \Lambda(V)$. Thus, for each $P \in V$ we have $w_P(s) \geq 0$. Since the complement of V in X is finite, $w_P(s) \geq 0$ for all but finitely many P.

Conversely, suppose that we have a maximal $\mathcal{O}_P$-order B_P for each $P \in X$, and that if w_P is the value function associated to B_P, then, for any $s \in S$, we have $w_P(s) \geq 0$ for all but finitely many P. We define a sheaf Λ on X by

$$\Lambda(U) = \bigcap_{P \in U} B_P$$

for all open subsets U of X with structure maps being the obvious inclusions. It is proved in [7, Ex. 3.4] that $\Lambda(U)$ is a maximal $\mathcal{O}(U)$-order for each proper open subset U, and so $\Lambda \subseteq \mathcal{S}$ is a sheaf of maximal orders on X. Moreover, in [7, Ex. 3.4], it is shown that $\Lambda(U)\mathcal{O}_P = B_P$ if $P \in U$. This shows that $\Lambda_P = B_P$ for each P. ∎

We now describe the divisor group on S and state a generalization of the Riemann-Roch theorem. If S is a central simple F-algebra, let Λ be a sheaf of maximal $\mathcal{O}_X$-orders on X. For each P let w_P be the value function on S corresponding to the maximal $\mathcal{O}_P$-order Λ_P. The *divisor group* $\mathrm{div}(S)$ is the free abelian group on the set $\{\Lambda_P\}_{P\in X}$. While this group depends on the choice of sheaf Λ, we will not deal with more than one sheaf of maximal orders at a time, so we will not need to worry about this dependence. For $E = \sum_P n_P \Lambda_P$, we define $\deg(E) = \sum_P n_P[\overline{\Lambda_P} : k]$ and $\mathrm{supp}(E) = \{\Lambda_P \mid n_P \neq 0\}$. Each $s \in S$ defines a divisor $(s) = \sum_P w_P(s)\Lambda_P$. We point out that this sum is finite by Lemma 1. Unlike the case of fields where principal divisors have degree 0, we see in the next lemma that the degree of a principal divisor (s) is non-positive, and can be negative. In the proof below we need to work with elements of $\mathrm{div}(F)$ and of $\mathrm{div}(S)$. When we talk about an element $E \in \mathrm{div}(F)$, we will write $\deg_F(E)$ for the degree of E as an F-divisor.

Lemma 2 *Let $s \in S$. Then $\deg((s)) \leq 0$. Moreover, $\deg((s)) = 0$ if and only if $s \in S^*$ and $s\Lambda_P s^{-1} = \Lambda_P$ for every $P \in X$.*

Proof: Let v_P be the normalized valuation on F with valuation ring $\mathcal{O}_P$. Then $w_P|_F = e_P v_P$, where e_P is the ramification index at P of S over F. Moreover, by [6, Prop. 2.6], if $n = \deg(S)$, then $w_P(s) \leq n^{-1} w_P(\mathrm{Nrd}(s))$. With these facts in mind, we see that

$$
\begin{aligned}
\deg((s)) &= \sum_P w_P(s)[\overline{\Lambda_P} : k] \\
&= \sum_P w_P(s)[\overline{\Lambda_P} : \overline{\mathcal{O}_P}] \cdot [\overline{\mathcal{O}_P} : k] \\
&\leq \sum_P \frac{1}{n} w_P(\mathrm{Nrd}(s))[\overline{\Lambda_P} : \overline{\mathcal{O}_P}] \deg_F(P) \\
&= \sum_P \frac{1}{n} e_P [\overline{\Lambda_P} : \overline{\mathcal{O}_P}] v_P(\mathrm{Nrd}(s)) \deg_F(P) \\
&= \sum_P n v_P(\mathrm{Nrd}(s)) \deg_F(P) = n \deg_F((\mathrm{Nrd}(s))) \\
&= 0.
\end{aligned}
$$

The second to last equality holds since $[S : F] = e_P[\overline{\Lambda_P} : \overline{\mathcal{O}_P}]$ for all $P \in X$ by [5, Theorems 13.3, 18.2, Corollary 17.5].

For the second statement, we note that the inequalities above show that $\deg((s)) < 0$ if and only if $w_P(s) < n^{-1}w_P(\mathrm{Nrd}(s))$ for some P. However, if $s \in S^*$, then $w_P(s) = n^{-1}w_P(\mathrm{Nrd}(s))$ if and only if $s\Lambda_P s^{-1} = \Lambda_P$ by [6, Prop. 2.6]. Therefore, if $s \in S^*$, then $\deg((s)) = 0$ if and only if $s\Lambda_P s^{-1} = \Lambda_P$ for every $P \in X$. To finish the argument, given that $\deg((s)) = 0$, we show that s must be in S^*. Pick a point $P \in X$, and set $J(\Lambda_P) = \pi_P\Lambda_P$, where $\pi_P\Lambda_P\pi_P^{-1} = \Lambda_P$. We have $s = \pi_P^n u$ for some u with $w_P(u) = 0$, and where $n = w_P(s)$. If $w_P(s) = n^{-1}w_P(\mathrm{Nrd}(s))$, then $0 = w_P(\mathrm{Nrd}(u))$, which forces $u \in \Lambda_P^* \subseteq S^*$ by the argument immediately preceding [6, Prop. 2.6]. Therefore, $s = \pi_P^n u \in S^*$. ∎

Example. Let p be an odd prime, let k be a finite field of characteristic p, let $a \in k^* - k^{*2}$, and let D be the quaternion algebra

$$D = \left(\frac{a, t}{k(t)}\right).$$

Let $1, i, j, k$ be the standard quaternion basis for D. The field $k(t)$ is the function field of $\mathbb{P}^1$, so points are in 1-1 correspondence with irreducible polynomials over k, except for the point P_∞ at infinity which corresponds to the dvr $k[t^{-1}]_{(t^{-1})}$. If a point P corresponds to $p(t) \neq t$, then we can choose $\Lambda_P = \left(\frac{a,t}{\mathcal{O}_P}\right)$. Let P_0 be the point corresponding to t. There are unique maximal orders over $\mathcal{O}_{P_0}$ and $\mathcal{O}_{P_\infty}$, which can be shown to be $\left(\frac{a,t}{\mathcal{O}_{P_0}}\right)$ and $\left(\frac{a,t^{-1}}{\mathcal{O}_{P_\infty}}\right)$, respectively. Construct a sheaf Λ as in the proof of Lemma 1. (The condition $w_P(d) \geq 0$ almost everywhere is easily verified: every $d \in D^*$ is of the form b/α for some $b \in \left(\frac{a,t}{k[t]}\right)$ and some $\alpha \in k[t] - \{0\}$. Then $d \in \Lambda_P$ for all P such that $P \neq P_\infty$ and $\alpha^{-1} \in \mathcal{O}_P$.) With this sheaf, we verify that the divisor of $1 + j$ is equal to $-P_\infty$, so $(1 + j)$ has negative degree. By Proposition 9 ahead (with $x = j$), we find that 1 and j form a strongly orthogonal basis for $D/k(t)(\sqrt{a})$, so $w_P(1 + j) = \min(w_P(1), w_P(j))$ for all $P \in X$. Since t is a unit in $\mathcal{O}_P$ for all P except those that correspond to t or $1/t$, and since $j^{-1} = t^{-1}j$, we find that j conjugates Λ_P to itself for all such P. By [6, Prop. 2.6], $w_P(j) = 0$ for all such P. As for P_0 and P_∞, the maximal orders at these points are valuation rings, and $w_{P_0}(j) = 1$, and $w_{P_\infty}(j) = -1$. Thus, $(1 + j) = -P_\infty$ as claimed.

We define a map $\phi_S : \mathrm{div}(F) \to \mathrm{div}(S)$ by $\phi_S(\sum_P n_P P) = \sum_P (n_P e_P \Lambda_P)$. The main property of this map that we need is given in the following lemma.

Lemma 3 *If $E \in \mathrm{div}(F)$, then $\deg(\phi_S(E)) = [S : F] \deg_F(E)$.*

Proof: If $E = \sum_P n_P P$, then we have

$$\begin{aligned}
\deg(\phi_S(E)) &= \sum_P n_P e_P \deg(\Lambda_P) = \sum_P n_P e_P [\overline{\Lambda_P} : k] \\
&= \sum_P n_P e_P [\overline{\Lambda_P} : \overline{\mathcal{O}_P}][\overline{\mathcal{O}_P} : k] \\
&= \sum_P n_P [S : F] \deg(P) = [S : F] \deg(E).
\end{aligned}$$

∎

If E, E' are divisors on S, we write $E \geq E'$ if $E - E' = \sum n_P \Lambda_P$ with each $n_P \geq 0$. Let $\mathcal{L}(E) = \{s \in S \mid (s) + E \geq 0\}$, a k-subspace of S. As a consequence of Lemma 2, we point out that if $\deg(E) < 0$, then $\mathcal{L}(E) = 0$. To see this, if $f \in \mathcal{L}(E)$ is nonzero, then $(f) + E \geq 0$, so $\deg((f) + E) = \deg((f)) + \deg(E) \leq \deg(E) < 0$, a contradiction to the condition $(f) + E \geq 0$. Let $\mathcal{C}$ be a canonical divisor on F, and set $\mathcal{K} = \phi_S(\mathcal{C}) + \sum_P (e_P - 1)\Lambda_P \in \mathrm{div}(S)$. We now state the generalization of the Riemann-Roch theorem to this setting.

Theorem 4 (Riemann-Roch) *Let $g = \max_{E \in \mathrm{div}(S)}\{\deg(E) + 1 - \dim(\mathcal{L}(E))\}$. Then g exists, and for all divisors E, we have $\dim(\mathcal{L}(E)) = \deg(E) + 1 - g + \dim(\mathcal{K} - E)$.*

A proof of this theorem can be found in [12, Satz 12] or [11, Theorem 3.17]. We would like to thank J.-L Colliot-Thélène for telling us about Witt's paper. Analogous to the commutative case, we have $\deg(\mathcal{K}) = 2g - 2$. By the definition of $\mathcal{K}$ and Lemma 3, if g_F is the genus of F, we see that

$$g = [S : F](g_F - 1) + 1 + \frac{1}{2}\sum_P (e_P - 1)\deg(\Lambda_P)$$

In the next section, in order to construct sheaves of maximal orders, we will use the fact that if U is a proper open subset of X, then $\bigcap_{P \in U} \mathcal{O}_P$ is a Dedekind domain of F. This is a standard result, but we give a proof here for the convenience of the reader.

Lemma 5 *If U is a proper open subset of X, then $\bigcap_{P\in U}\mathcal{O}_P$ is a Dedekind domain of F.*

Proof: Let $X - U = \{Q_1, \ldots, Q_n\}$, let $E = \sum_i n_i Q_i \in \operatorname{div}(F)$, and let $E_i = E - Q_i$, where the n_i are positive integers. If we choose the n_i large enough, then by the Riemann-Roch theorem, $\dim(\mathcal{L}(E))$ is larger than each $\dim(\mathcal{L}(E_i))$ since $\deg(E) > \deg(E_i)$ for each i. Each of these are finite-dimensional k-vector spaces, so $\mathcal{L}(E)$ properly contains the union $\bigcup_i \mathcal{L}(E_i)$. Choose $x \in \mathcal{L}(E)$ such that $x \notin \mathcal{L}(E_i)$ for each i. Then $(x) + E \geq 0$ but $(x) + E_i \not\geq 0$ for each i. This forces $v_{P_i}(x) = -n_i$ for each i, and $v_P(x) \geq 0$ for each $P \in U$. Consequently, the valuation rings of F that contain x are precisely the $\mathcal{O}_P$ for $P \in U$. Note that $x \notin k$, so F is algebraic over $k(x)$. A valuation ring of F/k contains x if and only if it contains $k[x]$, so we see that the integral closure of $k[x]$ in F is $\bigcap_{P\in U}\mathcal{O}_P$. However, since $k[x]$ is a Dedekind domain of $k(x)$, the ring $\bigcap_{P\in U}\mathcal{O}_P$ is a Dedekind domain of F by [5, Theorem 4.4]. ∎

3 The Construction of the Code

Let F/k be a function field in one variable over the finite field k. One has the following sequence from class field theory (see the discussion in [5, pages 277–278] for instance)

$$0 \longrightarrow \operatorname{Br}(F) \longrightarrow \oplus_P \operatorname{Br}(F_P) \longrightarrow \mathbb{Q}/\mathbb{Z} \longrightarrow 0, \tag{1}$$

where the sum in the middle term is over all the places of the field F. For any $D \in \operatorname{Br}(F)$, $D \otimes_F F_P$ is trivial almost everywhere; thus the second map in the sequence above, which is simply the sum of the various restriction maps, is well-defined. It is well-known that for each P, there is a canonical map $\operatorname{Inv} : \operatorname{Br}(F_P) \to \mathbb{Q}/\mathbb{Z}$ which is an isomorphism, and the third map above is just the sum of the Inv maps for each P. The map Inv can be explicitly described as follows: any division algebra D/F_P of degree r is isomorphic to the cyclic algebra $(W/F_P, \sigma, \pi^i)$, where W is the unique unramified field extension of F_P of degree r, π is a uniformizer for F_P, σ is a generator of the Galois group of the cyclic field extension W/F_P chosen so as to induce the Frobenius automorphism at the residue level, and $1 \leq i < r$ with $\gcd(i, r) = 1$. With this isomorphism at hand, $\operatorname{Inv}(D)$ is defined to be i/r. (See the discussion in [5, pages 263–266] for the description of division algebras over local fields.)

D is said to be *ramified* at a place P if $D \otimes_F F_P$ is not split. Moreover, if $\mathrm{Inv}(D \otimes_F F_P) = i/s$ with $\gcd(i, s) = 1$, then s is said to be the *local index* of D at P, and $\mathrm{ind}(D)$ is simply the least common multiple of the various local indices (see [5, Theorem 32.19]).

Now let X/k be a smooth geometrically irreducible projective curve, and F/k the associated function field. Let $P_1, \ldots, P_n$ be places of F/k of degree 1. Choose integers $r, j_1, \ldots, j_n$ such that $1 \leq j_i < r$, $\gcd(j_i, r) = 1$, and $\sum_i (j_i/r) = 0$ in $\mathbb{Q}/\mathbb{Z}$. Thus, the exact sequence (1) shows that there is a division algebra D/F ramified at exactly the places P_i, and at each P_i, D has local index r. It follows that $\mathrm{ind}(D) = r$ as well. Also, the residue field of F_{P_i} is just k since the P_i have degree 1, and if l/k is the unique extension of k of degree r, then lF_{P_i} is the unique unramified extension of F_{P_i} of degree r. Thus, by the discussion in the previous paragraph, $D \otimes_F F_{P_i}$ is isomorphic to $(lF_{P_i}/F_{P_i}, \sigma_i, \pi^{j_i})$, where σ_i is a generator of $\mathrm{Gal}(lF_{P_i}/F_{P_i})$ chosen so as to induce the Frobenius automorphism on l/k.

We first show that $L = lF$ is a maximal subfield of D. For any place Q of L, let P be the corresponding place of F induced by Q. The completion of L at Q is isomorphic to the compositum lF_P. If P is not one of the selected P_i, then $D \otimes_F F_P$ is already split, so $(D \otimes_F L) \otimes_L L_Q = (D \otimes_F F_P) \otimes_{F_P} lF_P$ is split. If P is one of the selected P_i, then, as remarked in the last paragraph, lF_P is a maximal subfield of $D \otimes_F F_P$, so once again, $(D \otimes_F L) \otimes_L L_Q = (D \otimes_F F_P) \otimes_{F_P} lF_P$ is split. It follows that $D \otimes_F L$ is split everywhere, so by our exact sequence (1), L splits D. Since $[L : F] = r$ (as k is algebraically closed in F, this follows from the geometric irreducibility of X/k), L is indeed a maximal subfield of D/F.

We construct a sheaf of maximal orders Λ on our curve X as follows: Let $A = \bigcap \mathcal{O}_Q$, where the intersection runs across all places Q of F *except* the chosen places P_i. As described in Lemma 5, A is a Dedekind domain. Since $l \subset D$, lA is a free finitely generated A module. Choose a basis $\{b_1 = 1, b_2, \ldots, b_r\}$ of D/L, and consider the free A module $M = \bigoplus_{i=1}^{n} (lA) b_i$. Then $MF = D$, and $lA \subseteq O_l(M)$, where $O_l(M) = \{x \in D \mid xM \subseteq M\}$. As discussed in [5, page 109], $O_l(M)$ is an A-order in D, and is hence contained in a maximal A-order; call this maximal order B. Then, for each place Q of F ($Q \notin \{P_1, \ldots, P_n\}$), $B \otimes_A \mathcal{O}_Q$ is a maximal $\mathcal{O}_Q$ order. We set $\Lambda_Q = B \otimes_A \mathcal{O}_Q$.

As for the places $P_1, \ldots, P_n$, there is a unique maximal order over each $\mathcal{O}_{P_i}$ which is in fact a valuation ring. (This follows, for instance, from [5, Theorems 12.8 and 11.5]. We set Λ_{P_i} to be this maximal $\mathcal{O}_{P_i}$ order.

Now let w_Q be the value function associated with this choice of maximal orders and consider the sheaf of rings Λ given by the assignment $U \mapsto \bigcap_{Q\in U} \Lambda_Q$. Exactly as in the argument in the proof of Lemma 1, any $s \in D$ can be written as $b\alpha^{-1}$ for some $b \in \Lambda(U)$, where $U = X - \{P_1, \ldots, P_n\}$, and for all but finitely many points $Q \in U$, $\alpha^{-1} \in \Lambda_Q$. It follows that $w_Q(s) \geq 0$ for all but finitely many points $Q \in U$. Since the complement of U contains only finitely many points, Lemma 1 shows that Λ is indeed a sheaf of maximal orders, whose stalk at each point $Q \in X$ is Λ_Q.

We let $\mathcal{P}$ be the D-divisor $\Lambda_{P_1} + \cdots + \Lambda_{P_n}$, and we let G be any D-divisor whose support is disjoint from the P_i, and such that $\mathcal{L}(G) \neq \{0\}$. The condition on the supports guarantees that any $f \in \mathcal{L}(G)$ is automatically in each Λ_{P_i}. Since each Λ_{P_i} is just the valuation ring corresponding to the P_i-adic valuation, the factor ring $\Lambda_{P_i}/J(\Lambda_{P_i})$, where $J(\Lambda_{P_i})$ is the maximal ideal of Λ_{P_i}, is just the residue field of D with respect to the P_i-adic valuation. The residue of D is the same as the residue of the completion $D \otimes_F F_{P_i}$, which is just l. We thus have, exactly as in the commutative case, a map

$$\begin{array}{rlcl} \mathrm{ev}: & \mathcal{L}(G) & \longrightarrow & l^n \\ & f & \mapsto & (f(P_1), \ldots, f(P_n)), \end{array}$$

where we have written $f(P_i)$ for the residue of f modulo the maximal ideal $J(\Lambda_{P_i})$ of Λ_{P_i}.

By our choice of maximal orders above, the field l is contained in every maximal order Λ_Q for $Q \notin \{P_1, \ldots, P_n\}$. Since each Λ_{P_i} is a valuation ring, and since any valuation on l must be trivial, l must be contained in each Λ_{P_i} as well. It follows that for *any* Q, $w_Q(x) \geq 0$ for all $x \in l^*$. Hence, for any Q, any $x \in l^*$, and any $f \in \mathcal{L}(G)$,

$$w_Q(xf) \geq w_Q(x) + w_Q(f) \geq w_Q(f) \geq -w_Q(G),$$

so $xf \in \mathcal{L}(G)$. Thus, besides being a k-space, $\mathcal{L}(G)$ is also an l-space. Moreover, $x(P_i)$ is just x for any P_i, as the P_i-adic valuation is trivial on l. It follows from this that the map ev above is an l-linear map. (In fact, each $x \in l^*$ conjugates each Λ_Q to itself, so by [6, Prop. 2.6 and Lemma 2.2], $w_Q(x) = 0$, and $w_Q(xf) = w_Q(x) + w_Q(f) = w_Q(f)$.)

The image of ev is thus an l-subspace of l^n; this will be our noncommutative Goppa code associated to D/F and the divisors $\mathcal{P}$ and G. We denote it $C_D(\mathcal{P}, G)$.

We point out that while different choices in our sheaf construction may lead to different (e.g., non-isomorphic) sheaves, the ring of constants $\bigcap_{Q \in X} \Lambda_Q$ is uniquely determined up to isomorphism by the division algebra D since k is finite, by a theorem of Schofield [10, Theorem 1.1]. We are working with a specific choice of sheaf to see that l is a subring of the ring of constants. In fact, it is not hard to see that $l = \bigcap_{Q \in X} \Lambda_Q$, so l is the full ring of constants of the sheaf Λ.

We determine in the next proposition the minimum distance and the dimension of the code $C_D(\mathcal{P}, G)$. The methods are analogous to those used for commutative Goppa codes (see [3]). Note that since $\overline{\Lambda_{P_i}} = l$ for each i, we have $\deg(\Lambda_{P_i}) = r = [l : k]$. Therefore, $\deg(\mathcal{P}) = rn$.

Proposition 6 *$\dim(C_D(\mathcal{P}, G)) = \dim(\mathcal{L}(G)) - \dim(\mathcal{L}(G-\mathcal{P}))$, and $d(C_D(\mathcal{P}, G)) \geq n - r^{-1} \deg(G)$. Moreover, if $\deg(G) < rn$, then $\dim(C_D(\mathcal{P}, G)) = \dim \mathcal{L}(G)) \geq \deg(G) + 1 - g$, where g is the genus of D.*

Proof: The kernel of ev is $\{f \in \mathcal{L}(G) \mid v_{P_i}(f) \geq 1, i = 1, \ldots, n\}$, which is precisely $\mathcal{L}(G-\mathcal{P})$. The result on the dimension immediately follows. As for the distance, write d for $d(C_D(\mathcal{P}, G))$ and let $f \in \mathcal{L}(G)$, $f \neq 0$, be such that $w(\mathrm{ev}(f)) = d$. Then f is in the maximal ideal of exactly $n - d$ of the Λ_{P_i}, say $\Lambda_{P_{i_1}}, \ldots, \Lambda_{P_{i_{n-d}}}$. It follows that $f \in \mathcal{L}(G - (\Lambda_{P_{i_1}} + \cdots + \Lambda_{P_{i_{n-d}}}))$. Hence, $\mathcal{L}(G - (\Lambda_{P_{i_1}} + \cdots + \Lambda_{P_{i_{n-d}}})) \neq \{0\}$. It follows that $\deg(G - (\Lambda_{P_{i_1}} + \cdots + \Lambda_{P_{i_{n-d}}})) \geq 0$, since $\mathcal{L}(H) = \{0\}$ for a divisor H of negative degree. Thus, $\deg(G) - r(n-d) \geq 0$, or $d \geq n - r^{-1} \deg(G)$.

For the second statement, if $\deg(G) < rn = \deg(\mathcal{P})$, then $\deg(G - \mathcal{P}) < 0$, so $\mathcal{L}(G - \mathcal{P}) = \{0\}$. It follows from the paragraph above that ev is then an injective map. Moreover, by the Riemann-Roch theorem, we have $\dim(C_D(\mathcal{P}, G)) = \dim(\mathcal{L}(G)) \geq \deg(G) + 1 - g$. ∎

4 Relation between $C_D(\mathcal{P}, G)$ and $C_L(\psi(\mathcal{P}), \psi(G))$

We continue to use the notation of the previous sections: $P_1, \ldots, P_n$ are rational points on X, and D is a division algebra with center F, the function field of X/k, such that the local index of D at each P_i is equal to the index r of D, and the local index of D at any point $P \neq P_i$ is 1. Recall that we have a sheaf Λ of maximal orders on D, that Λ is a subsheaf of the constant sheaf $U \mapsto D$, and that each stalk Λ_P contains l. Note that since

l/k is a cyclic Galois extension and l, F are linearly disjoint over k, the extension L/F is also cyclic Galois. Let σ be a generator of $\mathrm{Gal}(L/F)$. Since L is a maximal subfield of D, we may write D as a cyclic crossed product $D = (L/F, \sigma, a) = \bigoplus_{i=0}^{r-1} Lx^i$, where $x^r = a \in F$ and $xbx^{-1} = \sigma(b)$ for all $b \in L$. We will make use of this description of D in a number of places below.

If K is a field extension of F, recall the canonical map $\psi_K : \mathrm{div}(F) \to \mathrm{div}(K)$ that satisfies $\psi_K(P) = \sum e_{Q/P} Q$, where the sum is over all K-points Q lying over P, and where $e_{Q/P}$ is the ramification index of Q over P. In terms of valuations, $e_{Q/P}$ is the ramification index of K/F relative to the valuation ring of K corresponding to Q. We will refer to this valuation ring by $\mathcal{O}_{K,Q}$. For our maximal subfield $lF = L$ of D, we write ψ for ψ_L. We also view the map ψ as a map from $\mathrm{div}(D)$ to $\mathrm{div}(L)$ by sending Λ_P to $\psi(P)$. Since L/F is everywhere unramified, $e_{Q/P} = 1$ for every P and every Q lying over P, and, for each of the points P_i, there is a unique point Q_i lying over P_i. This follows from the fundamental equality $[L : F] = \sum_{Q/P} e_{Q/P} f_{Q/P}$, where $f_{Q/P} = [\overline{\mathcal{O}_{L,Q}} : \overline{\mathcal{O}_P}]$, and from the fact that the residue field of any point extending P_i is l, an extension of $k = \overline{\mathcal{O}_{P_i}}$ of degree $[L : F]$. As above, let $\mathcal{P} = \sum_i \Lambda_{P_i}$ and let G be a divisor with $\mathrm{supp}(G) \cap \{\Lambda_{P_1}, \ldots, \Lambda_{P_n}\} = \varnothing$. In the next lemma we compare our code with a Goppa code constructed from the algebraic function field L/l. To refer to such a Goppa code we denote it by $C_L(E', G')$ if E', G' are appropriately chosen divisors on L.

Lemma 7 *The space $\mathcal{L}(\psi(G))$ is canonically isomorphic to $\mathcal{L}(G) \cap L$, and, with the identification of $\mathcal{L}(\psi(G))$ as a subspace of $\mathcal{L}(G)$, the image $\mathrm{ev}(\mathcal{L}(\psi(G)))$ of $\mathcal{L}(\psi(G))$ under the evaluation map $\mathrm{ev} : \mathcal{L}(G) \to l^n$ is the Goppa code $C_L(\psi(\mathcal{P}), \psi(G))$.*

Proof: Let $f \in L$ satisfy $(f) + \psi(G) \geq 0$ in $\mathrm{div}(L)$. Given $P \in X - \{P_1, \ldots, P_n\}$, let $Q_1, \ldots, Q_g$ be the extensions of P to L. Let n_P be the coefficient of Λ_P in G. Thus, n_P is the coefficient of each Q_i in $\psi(G)$. Consequently, $v_{Q_i}(f) + n_P \geq 0$ for each i. Let π be a uniformizer for $\mathcal{O}_P$. Then π is a uniformizer for each Q_i since L/F is everywhere unramified. So, $v_{Q_i}(\pi^{n_P} f) \geq 0$ for all i, so $\pi^{n_P} f$ lies in all of the valuation rings that extend $\mathcal{O}_P$. But this means that $\pi^{n_P} f$ is in the integral closure of $\mathcal{O}_P$ in L, which is $l\mathcal{O}_P$. (To see this, if B is the integral closure of $\mathcal{O}_P$ in L, take a basis $l_1, \ldots, l_r$ of l/k, and let $l'_1, \ldots, l'_r$ be the dual basis relative to $\mathrm{Tr}_{l/k}$. Then $l'_1, \ldots, l'_r$ is also an F-basis of L. Suppose that $b \in B$, and write $b = \sum_j l'_j a_j$ with $a_j \in F$. Then $bl_i = \sum_j l_i l'_j a_j$, so $\mathrm{Tr}_{L/F}(bl_i) = \sum_j \mathrm{Tr}_{l/k}(l_i l'_j) a_j = a_i$.

But, $\mathrm{Tr}_{L/F}(B) \subseteq \mathcal{O}_P$, so each $a_i \in \mathcal{O}_P$. Thus, $B = \sum l'_j \mathcal{O}_P = l\mathcal{O}_P$.) Hence, $\pi^{n_P} f \in \Lambda_P$. Since π is also a uniformizer for Λ_P and is in its center, we have $w_P(\pi^{n_P} f) = w_P(f) + n_P \geq 0$, so $f \in \mathcal{L}(G)$. For $P \in \{P_1, \ldots, P_n\}$, $l\mathcal{O}_{P_i}$ is the unique valuation ring extending $\mathcal{O}_{P_i}$, and if say v'_i denotes this valuation on L, then $(f) + \psi(G) \geq 0$ implies that $v'_i(f) \geq 0$ for each i, which implies that $f \in \Lambda_{P_i}$ for each i. Thus, $w_{P_i}(f) \geq 0$ for each i. Therefore, $\mathcal{L}(\psi(G)) \subseteq \mathcal{L}(G) \cap L$.

For the reverse inclusion, take $f \in \mathcal{L}(G) \cap L$. Then, for $P \in X - \{P_1, \ldots, P_n\}$, $w_P(f) + n_P \geq 0$. If $\pi \in \mathcal{O}_P$ is a uniformizer for $\mathcal{O}_P$ and Λ_P, then $f = \pi^{-n_P} u$ for some $u \in \Lambda_P$. But this puts u in $\Lambda_P \cap L$, which is integral over $\mathcal{O}_P$. Thus, u is in every valuation ring of L extending $\mathcal{O}_P$; in other words, $v_Q(f) \geq -n_P$ for every valuation ring of L extending $\mathcal{O}_P$. For $P \in \{P_1, \ldots, P_n\}$, we have $w_{P_i}(f) \geq 0$, so $f \in \Lambda_{P_i} \cap L$. As before, Λ_{P_i} is a valuation ring, so $\Lambda_{P_i} \cap L$ is the (unique) valuation ring of L that extends $\mathcal{O}_{P_i}$. Thus, $v_{P_i}(f) \geq 0$ for each i. Thus, we have proven $\mathcal{L}(\psi(G)) = \mathcal{L}(G) \cap L$.

Consider $\mathrm{ev} : \mathcal{L}(G) \to l^n$, where $\mathrm{ev}(f) = (f(P_1), \ldots, f(P_n))$. If $f \in \mathcal{L}(\psi(G))$, we claim that $f(Q_i) = f(P_i)$ for each i, and so $\mathrm{ev}(\mathcal{L}(\psi(G))) = \{(f(Q_1), \ldots, f(Q_n)) \mid f \in \mathcal{L}(\psi(G))\}$. This is $C_L(\psi(\mathcal{P}), \psi(G))$, finishing the proof of the lemma once we prove the claim. To do this, note that if $\mathfrak{m}_{L,Q_i}$ is the maximal ideal of $\mathcal{O}_{L,Q_i}$, then $f(Q_i) = f + \mathfrak{m}_{L,Q_i} \in \overline{\mathcal{O}_{L,Q_i}} = l = \overline{\Lambda_{P_i}}$. Also, viewing $f \in D$, we have $f(P_i) = f + J(\Lambda_{P_i})$. But, Λ_{P_i} contains $\mathcal{O}_{L,Q_i}$ and $J(\Lambda_{P_i}) \cap \mathcal{O}_{L,Q_i} = \mathfrak{m}_{L,Q_i}$, so $f + \mathfrak{m}_{L,Q_i} = f + J(\Lambda_{P_i})$. In other words, $f(Q_i) = f(P_i)$. ∎

We say that an L-basis $d_1, \ldots, d_r$ of D is an *orthogonal basis* with respect to a maximal order $\Lambda_P \in X$ with associated value function w_P, provided that $w_P(\sum_i l_i d_i) = \min_i\{w_P(l_i d_i)\}$ for all $l_i \in L$. If, in addition, $w_P(\sum_i l_i d_i) = \min_i \{w_P(l_i) + w_P(d_i)\}$, we will call the L-basis $d_1, \ldots, d_r$ a *strongly orthogonal basis* with respect to Λ_P.

Lemma 8 *With $D = \bigoplus_{i=0}^{r-1} Lx^i$ as in the beginning of this section,*

1. *If D is split at P, let $d_1, \ldots, d_r$ be units in Λ_P such that $\overline{d_1}, \ldots, \overline{d_r}$ is a basis for $\overline{\Lambda_P}$ over $\overline{\Lambda_P \cap L}$. Then $d_1, \ldots, d_r$ is a strongly orthogonal basis for D with respect to Λ_P.*

2. *If $P = P_i$, then $1, x, \ldots, x^{r-1}$ is a strongly orthogonal basis for D with respect to Λ_P.*

Proof: Suppose that $d_1, \ldots, d_r$ are units in Λ_P such that $\overline{d_1}, \ldots, \overline{d_r}$ is a basis for $\overline{\Lambda_P}$ over $\overline{\Lambda_P \cap L}$. Note that $w_P(d_i) = 0$ for each i, and that since

$d_i \in \Lambda_P^*$, we have $w_P(ed_i) = w_P(e)$ for all $e \in D$ by the definition of the value function w_P (or by [6, Lemma 2.2]). Suppose that $\min_i \{w_P(l_i d_i)\} = w_P(l_k)$. Then $w_P(l_k) = t$ for some $t \in \mathbb{Z}$, so if π is a uniformizer for $\mathcal{O}_P$, then $w_P(\pi^{-t} l_i) \geq 0$ for all i, and $w_P(\pi^{-t} l_k) = 0$. These facts hold since $\pi \in F = Z(D)$. Thus, we may assume that $w_P(l_i) \geq 0$ for all i and $w_P(l_k) = 0$. Then $\overline{\sum_i l_i d_i} = \sum_i \overline{l_i}\, \overline{d_i} \neq 0$ since $\overline{l_k} \neq 0$, so $w_P\left(\sum_i l_i d_i\right) = 0$, as desired.

For the second part, suppose that $P = P_i$ is one of the rational points at which the local index of D is equal to $r = \mathrm{ind}(D)$. Let $\mathrm{Inv}(D_P) = k/r + \mathbb{Z}$ with $\gcd(k, r) = 1$. Then $D_P = (lF_P/F_P, \sigma, \pi^k)$ for some uniformizer π of $\mathcal{O}_P$. Since $x^r = \pi^k u$ for some unit $u \in \mathcal{O}_P^*$, and since $w_P|_F = rv_P$ if v_P is the normalized valuation on F with valuation ring $\mathcal{O}_P$, we see that $w_P(x^i) = ik$. Moreover, L/F is unramified at P, so the value group of L is $r\mathbb{Z}$. Thus, since $\gcd(r, k) = 1$, the values $w_P(x^i)$ are distinct modulo the value group of L. If $\sum_i l_i x^i \in D$, each term $l_i x^i$ has distinct value, so $w_P\left(\sum_i l_i x^i\right) = \min_i w_P(l_i x^i) = \min_i \{w_P(l_i) + w_P(x^i)\}$; the latter equality holds since w_P is a valuation on D. This shows that $1, x, \ldots, x^{r-1}$ is a strongly orthogonal basis of D over L with respect to Λ_P. ∎

Proposition 9 *The set $\{1, x, \ldots, x^{r-1}\}$ is an orthogonal basis with respect to each Λ_P for $P \in X$.*

Proof: Let $P \in X$. If $P = P_i$, then the x^i form a strongly orthogonal basis with respect to Λ_P by Lemma 8. Next, suppose that D is split at P. Recall from the proof of Lemma 7 that $l\mathcal{O}_P$ is the integral closure of $\mathcal{O}_P$ in L. From this, we see that $B = l\mathcal{O}_P$ is contained in the stalk Λ_P. By [4, Prop. 1.3], there are $z_i \in \Lambda_P$ such that $\Lambda_P = \oplus_{i=0}^{r-1} B z_i$ with $z_i b = \sigma^i(b) z_i$ for $b \in L$, and $z_i z_j = f(\sigma^i, \sigma^j) z_{i+j}$ for some normalized cocycle f with values in B. Since D is split at P, the maximal order Λ_P is Azumaya over $\mathcal{O}_P$. Thus, $J(\Lambda_P) = \mathfrak{m}_P \Lambda_P = \oplus_{i=0}^{r-1} \mathfrak{m}_P B z_i$, where $\mathfrak{m}_P$ is the maximal ideal of $\mathcal{O}_P$. However, by [4, Prop. 3.1], $J(\Lambda_P) = \oplus_{i=0}^{r-1} I_i z_i$, where I_i is the product of the maximal ideals M of B for which $f(\sigma^i, \sigma^{-i}) \notin M$. Since $\mathfrak{m}_P B$ is the product of all the maximal ideals of B, unique factorization of ideals in B forces $f(\sigma^i, \sigma^{-i}) \notin M$ for every maximal ideal M of B, so $f(\sigma^i, \sigma^{-i}) \in B^*$ for each i. Then, from the cocycle condition, we see that $\sigma^i(f(\sigma^{-i}, \sigma^j)) f(\sigma^i, \sigma^{-i+j}) = f(\sigma^i, \sigma^{-i}) f(1, \sigma^j) \in B^*$, so all cocycle values are in fact in B^*. Consequently, the residue ring $\overline{A}$ is equal to the crossed product $(\overline{B}/\overline{\mathcal{O}_P}, \sigma, \overline{f}) = \oplus_{i=0}^{r-1} \overline{B}\,\overline{z_i}$, so the $\overline{z_i}$ are linearly independent over $\overline{B}$. Therefore, the z_i form a strongly orthogonal basis with respect to Λ_P by

Lemma 8. Note also that $w_P(z_i) = 0$ for each i from this description of the residue ring $\overline{A}$. To see that the powers of x form an orthogonal basis with respect to Λ_P, write $x^i = \alpha_i z_i$ with $\alpha_i \in L$. We have

$$w_P\left(\sum_i l_i x^i\right) = w_P\left(\sum_i l_i \alpha_i z_i\right) = \min_i \{w_P(l_i \alpha_i z_i)\} = \min_i \left\{w_P(l_i x^i)\right\},$$

since $z_0, \ldots, z_{r-1}$ is an orthogonal basis of D with respect to Λ_P. Thus, the x^i form an orthogonal basis. ∎

Theorem 10 *If G is a divisor on D with* $\deg(G) < rn$ *and* $\operatorname{supp}(G) \cap \{\Lambda_{P_1}, \ldots, \Lambda_{P_n}\} = \varnothing$*, then* $\mathcal{L}(G) \subseteq L$.

Proof: Let $f = \sum_i l_i x^i \in \mathcal{L}(G)$, so $w_Q(f) + w_Q(G) \geq 0$ for all Q. However, $w_Q(f) = \min_i\{w_Q(l_i x^i)\} \leq w_Q(l_0)$ by Proposition 9, so $l_0 \in \mathcal{L}(G)$. Let $f' = \sum_{i=1}^{r-1} l_i x^i = f - l_0 \in \mathcal{L}(G)$. Then $w_{P_j}(f') \geq 0$ for all j. Since $w_{P_j}(f') = \min_{i>0}\{w_{P_j}(l_i) + i w_{P_j}(x)\}$, again by Proposition 9, each $w_{P_j}(l_i) + i w_{P_j}(x) \geq 0$. But $i w_{P_j}(x) \neq 0$ in $\Gamma_{\Lambda_{P_j}} / \Gamma_{\Lambda_{P_j} \cap L}$ for each $i \neq 0$, so in fact $w_{P_j}(l_i) + i w_{P_j}(x) > 0$ for each i. Consequently, $w_{P_j}(f') > 0$ for each j. The coefficient of Λ_{P_j} in $(f') + G$ is then at least 1. The degree of Λ_{P_j} is r since the residue ring of Λ_{P_j} is l. This, together with $(f') + G \geq 0$, forces $\deg((f') + G) \geq rn$, while $\deg((f') + G) = \deg((f')) + \deg(G) \leq \deg(G) < rn$, a contradiction unless $f' = 0$. Therefore, $f = l_0 \in L$. ∎

Corollary 11 *Let G be a divisor on D with* $\operatorname{supp}(G) \cap \{\Lambda_{P_1}, \ldots, \Lambda_{P_n}\} = \varnothing$, *and suppose that* $\deg(G) < rn = \deg(\mathcal{P})$. *If ψ is the natural map ψ :* $\operatorname{div}(F) \to \operatorname{div}(L)$*, then the code $C_D(\mathcal{P}, G)$ is equal to the code* $C_L(\psi(\mathcal{P}), \psi(G))$.

Proof: We have seen in Lemma 7 that $C_L(\psi(\mathcal{P}), \psi(G))$ is equal to the subcode $\operatorname{ev}(\mathcal{L}(G) \cap L)$ of $C_D(\mathcal{P}, G)$. Since $\mathcal{L}(G) \subseteq L$, this image is equal to $C_D(\mathcal{P}, G)$. ∎

References

[1] S. Chase, D. Harrison, A. Rosenberg, Galois theory and cohomology of commutative rings, *Mem. Amer. Math. Soc.* **52**, (1965), 1–19.

[2] E. Formanek, *The Polynomial Identities and Invariants of $n \times n$ Matrices*, CBMS Notes, Vol. 78, Amer. Math. Soc. Providence, 1991.

[3] V. D. Goppa, Codes on algebraic curves, *Soviet Math. Dokl.*, **24** (1981), 170–172.

[4] D. Haile, Crossed-product orders over discrete valuation rings, *J. Algebra* **105** (1987), 116–148.

[5] I. Reiner, *Maximal Orders*, Academic Press, London, 1975.

[6] P. Morandi, Value functions on central simple algebras, *Trans. Amer. Math. Soc.* **315**, 1989, 605–622.

[7] P. Morandi, Noncommutative Prüfer rings, *J. Algebra* **161**, (1993), 324–341.

[8] M. Orzech and C. Small, *The Brauer Group of Commutative Rings*, Marcel Dekker, Inc., New York, 1975.

[9] M. Van den Bergh and J. Van Geel, A duality theorem for orders in central simple algebras over function fields, *J. Pure Appl. Algebra* **31** (1984), 227–239.

[10] M. Van den Bergh and J. Van Geel, Algebraic elements in division algebras over function fields of curves, Israel J. Math. **52** (1985), 33–45.

[11] J. Van Geel, *Places and Valuations in Noncommutative Ring Theory*, Marcel Dekker, Inc., New York, 1981.

[12] E. Witt, Riemann-Rochster satz und Z-funcktion im hyperkomplexen, *Math. Ann.* **110** (1934), 12–28.