UNIVERSITATIS IAGELLONICAE ACTA MATHEMATICA, FASCICULUS XXXIX
2001

RESIDUAL REPRESENTATION OF ALGEBRAIC-GEOMETRIC CODES

by Reinhold Hübl

Dedicated to T. Winiarski on the occasion of his sixtieth birthday.

Abstract. In this paper residues and duality theory for curves are used to construct error-correcting codes and to find estimates for their parameters. Results of Goppa are extended to singular curves.

In an attempt to find long codes with good parameters, algebraic-geometric codes have been introduced by Goppa [**4**]. The construction is based on the (residual) evaluation of the space of sections of a line bundle on a non-singular curve over a finite field at the points in the support of a given divisor. The explicit construction and description of these codes faces two major difficulties:

i) To get long codes with good parameters it is necessary to construct non-singular curves of high genus (due to the Hasse-Weil-Serre resp. the Drinfeld-Vladut bound).

ii) To make this codes explicit and computable, it is necessary to determine the global space of sections of line bundles on curves.

Both tasks are in general not easy to achieve and require deep insights into the theory of function fields of transcendence degree 1 over finite fields and the geometry of their nonsingular models (cf. [**18**], [**19**], [**20**], [**3**], [**5**], [**6**]).

In this note we propose an extension of Goppa's techniques in two directions: The extension to the case of singular curves and to divisors that are not necessarily the sum of simple rational points. Whereas the nonsingular model of a function field might be very hard to determine, it is often quite easy to find and describe explicitly a singular model, and if we remove the restriction to divisors with support that is rational over the base field, it is possible to construct long codes with the help of comparatively simple curves. Eventually

Partially supported by a Heisenberg-Stipendium of the DFG.

we hope that this generalization will allow us to determine families of good algebraic-geometric codes in a way more simple and explicit than it can be done so far.

In the first part of this paper we will provide the necessary details about duality theory for general curves over finite (or more generally perfect) fields, and in particular we will recall the construction of residues using regular differential forms and traces. This can be done very explicitly and constructively and the theorems known for smooth curves hold in this context with only minor modifications. In the second part of this paper these results are applied to construct codes and estimate their parameters.

1. Regular differential forms and residues. The theory of residues for algebraic varieties over perfect fields has been described in various degrees of generality and in various degrees of explicity, cf. [**13**], [**16**], [**21**], [**9**]. In most cases this requires a lot of preparation, and often these approaches are not constructive. In case of curves over finite fields we can give a very short description. This approach is based on a corresponding description in the smooth case, as it is carried out for instance in [**10**].

Let k be a finite field (or more generally a perfect field) of positive characteristics $p > 0$. Furthermore let K/k be a field extension (not necessarily finitely generated) such that $\dim_K \Omega^1_{K/k} = 1$.

Remark 1.1. i) Let K/k be an algebraic function field of transcendence degree 1. Then $\dim_K \Omega^1_{K/k} = 1$.

ii) Let K/k be an algebraic function field of transcendence degree 1, let v be a (discrete) valuation of K/k and let $\widehat{K}$ be the completion of K with respect to v. Then $\dim_k \Omega^1_{\widehat{K}/k} = 1$. In fact, as k is perfect, in this situation $\widehat{K}/\widehat{K}^p$ is finite of degree p, $\widehat{K} = \widehat{K}^p[t]$ where we may choose t to be a regular parameter of v, and therefore

$$\Omega^1_{\widehat{K}/k} = \Omega^1_{\widehat{K}/\widehat{K}^p} = \widehat{K}dt.$$

In the above situation let L/K be a finite and separable field extension. Then $\Omega^1_{L/k} = L \otimes_K \Omega^1_{K/k}$ canonically, and therefore we can define a trace

$$\sigma_{L/K} : \Omega^1_{L/k} \longrightarrow \Omega^1_{K/k}$$

by $\sigma_{L/K}(l \otimes \omega) = \mathrm{Tr}_{L/K}(l) \cdot \omega$ for $l \in L$ and $\omega \in \Omega^1_{K/k}$, where $\mathrm{Tr}_{L/K} : L \to K$ denotes the canonical trace of the field extension L/K. More generally, if L/K is a finite étale extension, then $L = L_1 \times \cdots \times L_n$ with finite separable field extensions L_i/K, and $\Omega^1_{L/k} = \Omega^1_{L_1/k} \times \cdots \times \Omega^1_{L_n/k}$, and we define

$$\sigma_{L/K}((\omega_1, \ldots, \omega_n)) = \sum_{i=1}^{n} \sigma_{L_i/K}(\omega_i)$$

and this definition now also extends in an obvious way to the case that K is a direct product of such field extensions of k.

THEOREM 1.2. *i) If M/L is another étale extension, then*

$$\sigma_{M/K} = \sigma_{L/K} \circ \sigma_{M/K}.$$

ii) $\sigma_{L/K} \circ d_{L/k} = d_{K/k} \circ Tr_{L/K}$.
iii) For $l \in L^\times$ we have

$$\sigma_{L/K}\left(\frac{d_{L/k}(y)}{y}\right) = \frac{d_{K/k}(N_{L/K}(y))}{N_{L/K}(y)}$$

where $N_{L/K} : L \to K$ is the canonical norm.
iv) $\sigma_{L/K}$ induces an L-linear isomorphism

$$\sigma : \Omega^1_{L/k} \longrightarrow Hom_K(L, \Omega^1_{K/k}), \quad \omega \longmapsto (l \longmapsto \sigma_{L/K}(l\omega)).$$

PROOF. i) is clear by construction.

ii) and iii): We may assume that K and L are fields. Let N be the normal closure of L/K (i.e. if we write $L = K[x]$ for some primitive element x with minimal polynomial $f(X)$ over K, then N is a splitting field of $f(X)$ over K). Then $L \otimes_K N/N$ is a finite étale extension, $L \otimes_K N = N \times \cdots \times N$ is a direct product of $n := [L : K]$ copies of N, and $\Omega^1_{L \otimes_K N/k} = \Omega^1_{N/k} \times \cdots \times \Omega^1_{N/k}$. Furthermore the compatibility of the canonical trace of a finite projective algebra with base change implies that the diagram

$$\begin{tikzcd}
\Omega^1_{L/k} \arrow[r, "\iota=\mathrm{can}"] \arrow[d, "\sigma_{L/K}"'] & \Omega^1_{L\otimes_K N/k} \arrow[d, "\sigma_{L\otimes_K N/N}"] \\
\Omega^1_{K/k} \arrow[r, "\iota=\mathrm{can}"] & \Omega^1_{N/k}
\end{tikzcd}$$

commutes. As N/K is separable, ι is injective, and as

$$\sigma_{L\otimes_K N/N}((\omega_1, \ldots, \omega_n)) = \sum_{i=1}^{n} \omega_i.$$

ii) and iii) follow immediately.

iv) As both sides are L-vectorspaces of dimension 1, it suffices to show that $\sigma \neq 0$. This is however clear, as $\mathrm{Tr}_{L/K}$, hence also $\sigma_{L/K}$, is surjective. $\square$

Suppose now that R/k is an affine domain of dimension 1, and let $L = Q(R)$ be its field of fractions. Furthermore let $P := k[t] \to R$ be a separating noetherian normalization (i.e. t is a separating transcendence basis of L/k and R is finite as a module over P; note that such a normalization always exists, cf. [**13**]), and let $K = k(t) = Q(k[t])$. Then the above assumptions are satisfied in this situation, and a trace $\sigma_{L/K}$ is defined. Thus we get a canonical injection

$$\iota_R : \mathrm{Hom}_P(R, \Omega^1_{P/k}) \hookrightarrow \mathrm{Hom}_K(L, \Omega^1_{K/k}) \xrightarrow{\sigma^{-1}} \Omega^1_{L/k}$$

and we define, following [**14**], the module of regular differential forms of R/k to be

$$\omega^1_{R/k} := \mathrm{im}(\iota_R).$$

Remark 1.3. i) $\omega^1_{R/k} = \{\omega \in \Omega^1_{L/k} : \sigma_{L/K}(r\omega) \in \Omega^1_{P/k} \text{ for all } r \in R\}$.

ii) The definition of $\omega^1_{R/k}$ does not depend on the special choice of a separating noetherian normalization $k[t] \to R$.

iii) If $f \in R$ then

$$\left(\omega^1_{R/k}\right)_f = \omega^1_{R_f/k}.$$

In particular for any $\mathfrak{p} \in \mathrm{Spec}(R)$ the module

$$\omega^1_{R_\mathfrak{p}/k} := \left(\omega^1_{R/k}\right)_\mathfrak{p}$$

is an invariant of the algebra $R_\mathfrak{p}/k$ only. If $\widehat{R}$ denotes the completion of $R_\mathfrak{p}$, and if $t \in \widehat{R}$ is a separating parameter (i.e. a nonzerodivisor contained in the maximal ideal of $\widehat{R}$ such that $Q(\widehat{R})$ is étale over $k((t))$), then

$$(*) \qquad P := k[[t]] \hookrightarrow \widehat{R}$$

is finite and $\sigma_{Q(\widehat{R})/Q(P)}$ induces an isomorphism

$$\sigma : \widehat{\omega^1_{R_\mathfrak{p}/k}} \longrightarrow \mathrm{Hom}_P(\widehat{R}, \Omega^1_{P/k}).$$

Thus we will write $\omega^1_{\widehat{R}/k} := \widehat{\omega^1_{R_\mathfrak{p}/k}}$, and we note that this is an invariant of $\widehat{R}/k$, which can be defined directly as generalized complementary module, using noetherian normalizations of type $(*)$ (cf. [**13**], [**9**]).

iv) If $R = k[T_1, \ldots, T_d]/I$ where $I \subseteq P := k[T_1, \ldots, T_d]$ is locally generated by a regular sequence, then

$$\omega^1_{R/k} = \mathrm{Hom}_R(\bigwedge^{d-1} I/I^2, R) \otimes_R \Omega^d_{P/k}/I\Omega^d_{P/k}.$$

v) There exists a canonical map

$$c_{R/k} : \Omega^1_{R/k} \to \omega^1_{R/k}$$

which is an isomorphism if and only if R/k is smooth.

Proof. The proofs of these properties can be found in [**14**], [**8**] or [**13**]. □

Definition. An algebraic curve over k is a projective reduced and irreducible scheme X/k of dimension 1.

Remark 1.4. Let X/k be an algebraic curve.

i) X has a unique generic point ξ and $L := \mathcal{O}_{X,\xi}$ is an algebraic field extension of k of transcendence degree 1, called the field of rational functions of X/k.

ii) X is covered by finitely many open affine subsets $U_i = \mathrm{Spec}(R_i)$ $(i = 1,\dots,n)$, with affine reduced and irreducible algebras R_i/k of dimension 1, and the modules $\omega^1_{R_i/k}$ glue to define a sheaf $\omega^1_{X/k}$.

iii) There exists a graded domain $S = \bigoplus_{n\in\mathbb{N}} S_n$, finitely generated over k, with $S_0 = k$ and $S = S_0[S_1]$ such that

$$X = \mathrm{Proj}(S).$$

In this case $\omega^2_{S/k}$ is a well-defined, graded submodule of $\Omega^2_{Q(S)/k}$, and

$$\omega^1_{X/k} = \widetilde{\omega^2_{S/k}}$$

is the $\mathcal{O}_X$-module associated with it (cf. [**7**]).

Let X/k be a curve with field L of rational functions, let $x \in X$ be a closed point and set $R := \mathcal{O}_{X,x}$. Then R is a local domain of dimension 1 with maximal ideal $\mathfrak{m} = \mathfrak{m}_x$ and $\widehat{R}$, its $\mathfrak{m}$-adic completion, is a reduced local ring whose full ring of fractions we denote by $\widehat{L}$. By $\mathfrak{p}_1,\dots,\mathfrak{p}_l$ we denote the minimal primes of $\widehat{R}$, and by $R_i := \widehat{R}/\mathfrak{p}_i$ the analytic branches of X at x $(i = 1,\dots,l)$. If $\overline{R_i}$ is the integral closure of R_i in $Q(R_i) = L_i$, then by Cohen's structure theorem $\overline{R_i} = \kappa_i[[t_i]]$ for a uniquely determined coefficient subfield $\kappa_i \subseteq \overline{R_i}$ which is a finite and separable extension of k. In this situation we have (as in 1.1)

$$\Omega^1_{L_i/k} = \Omega^1_{L_i/L_i^p} = \Omega^1_{L_i/\kappa_i((t_i^p))} = L_i dt_i$$

and therefore any $\omega_i \in \Omega^1_{L_i/k}$ has a unique representation

$$\omega_i = f_i dt_i \quad \text{for some } f_i = \sum_{n\in\mathbb{Z}} a_n^{(i)} t_i^n \in L_i.$$

Whereas f_i depends on the choice of t_i, it is well known that

Lemma 1.5. *$a_{-1}^{(i)}$ is independent of the special choice of t_i.*

Proof. [**12**], (17.1), see also [**20**], (2.2.19). □

Definition. For $\omega_i \in \Omega^1_{L_i/k}$ set

$$\operatorname{Res}_{R_i/k}(\omega_i) := \operatorname{Res}_{\overline{R_i}/k}(\omega_i) := \operatorname{Tr}_{\kappa_i/k}(a^{(i)}_{-1})$$

and for $\omega \in \Omega^1_{\widehat{L}/k}$ with image $\omega_i \in \Omega^1_{L_i/k}$ set

$$\operatorname{Res}_{\widehat{R}/k}(\omega) := \sum_{i=1}^{l} \operatorname{Res}_{R_i/k}(\omega_i).$$

Finally for $\omega \in \Omega^1_{L/k}$ with image $\widehat{\omega} \in \Omega^1_{\widehat{L}/k}$ we define

$$\operatorname{Res}_{X/k,x}(\omega) = \operatorname{Res}_{\widehat{R}/k}(\widehat{\omega})$$

and call it the residue of ω at x.

Proposition 1.6 (trace formula). *i) Let $P \subseteq R$ be a finite generically étale extension of complete semi-local rings such that $\dim(P) = \dim(R) = 1$ and assume that P and R are reduced and residually finite over k. Let $L = Q(R)$ and $K = Q(P)$. Then*

$$\operatorname{Res}_{R/k}(\omega) = \operatorname{Res}_{P/k}(\sigma_{L/K}(\omega)).$$

ii) Let $\pi : X \to Y$ be a finite map of algebraic curves such that the corresponding extension $K \hookrightarrow L$ of rational function fields is separable. Let $y \in Y$ be a point and let $\omega \in \Omega^1_{L/k}$ be a meromorphic differential form on X. Then

$$\sum_{x \in \pi^{-1}(y)} \operatorname{Res}_{X/k,x}(\omega) = \operatorname{Res}_{Y/k,y}(\sigma_{L/K}(\omega)).$$

Proof. It obviously suffices to prove i).

i) Let $t \in P$ be an element such that $k[[t]] \subseteq P$ is finite and generically étale. Such a t exists as $\Omega^1_{K/k}$ hat K-dimension 1 by [**12**], (13.10). As $\sigma_{L/k((t))} = \sigma_{K/k((t))} \circ \sigma_{L/K}$ it suffices to prove the trace formula for $k[[t]] \subseteq P$ and $k[[t]] \subseteq R$, i.e. we may assume that $P = k[[t]]$. Let $R_1, \ldots, R_l$ be the analytic branches of R. Then

$$\operatorname{Res}_{R/k}(\omega) = \sum_{i=1}^{l} \operatorname{Res}_{R_i/k}(\omega_i) = \sum_{i=1}^{l} \operatorname{Res}_{\overline{R_i}/k}(\omega_i)$$

and

$$\sigma_{L/K}(\omega) = \sum_{i=1}^{l} \sigma_{L_i/K}(\omega_i)$$

and we may replace R by $\overline{R_i}$ and thus assume that $R = \kappa[[\tau]]$ for some finite separable extension κ/k. Then we have

$$k[[t]] \subseteq \kappa[[t]] \subseteq \kappa[[\tau]]$$

and it suffices to consider the two cases $k[[t]] \subseteq \kappa[[t]]$ and $\kappa[[t]] \subseteq \kappa[[\tau]]$ separately.

1.) $P = k[[t]] \subseteq \kappa[t]] = R$. Then we have

$$\Omega^1_{L/k} = \kappa \otimes_k \Omega^1_{K/k} \quad \text{ and } \sigma_{L/K} = \mathrm{Tr}_{\kappa/k} \otimes_k \mathrm{id}_{\Omega^1_{K/k}}$$

and form this the claim is immediate.

2.) $P = \kappa[[t]] \subseteq \kappa[[\tau]] = R$. We may assume that $\omega = \frac{d\tau}{\tau^m}$ for some $m \in \mathbb{N}$. Let v be the valuation of R and let $n = v(t)$ (i.e. $t \cdot R = \tau^n \cdot R$).

α) $p \nmid n$: In this case there exists a regular parameter τ' of R such that $(\tau')^n = at$ for some $a \in \kappa^\times$. We may replace τ by τ' and t by at and thus assume that $T^n - t$ is the minimal polynomial of τ over K. Writing $-m = \rho n + \lambda$ for some $\rho \in \mathbb{Z}$ and some $\lambda \in \{0, \dots, n-1\}$, we get

$$\sigma_{L/K}\left(\frac{d\tau}{\tau^m}\right) = \sigma_{L/K}\left(t^\rho \frac{\tau^\lambda}{n\tau^{n-1}}\, dt\right) = \begin{cases} t^\rho dt & \text{if } \lambda = n-1 \\ 0 & \text{otherwise} \end{cases}$$

and the claim follows.

β) $p|n$: Let again $\omega = \frac{d\tau}{\tau^m}$. Assume first that $p \nmid (m-1)$. Then $\omega = df$ for some $f \in L$, and therefore

$$\mathrm{Res}_{R/k}(df) = 0$$

and (using 1.2 ii)

$$\mathrm{Res}_{P/k}(\sigma_{L/K}(df)) = \mathrm{Res}_{P/k}(d\mathrm{Tr}_{L/K}(f)) = 0$$

(as can be seen easily by differentiating the Laurent series expansion of $\mathrm{Tr}_{L/K}(f)$). Thus we are left with the case that $m = ep + 1$ for some $e \in \mathbb{N}$. If $e = 0$ then

$$\sigma_{L/K}\left(\frac{d\tau}{\tau}\right) = \frac{dN_{L/K}(\tau)}{N_{L/K}(\tau)}$$

and as $N_{L/K}(\tau)$ is a regular parameter of P, the claim follows. If $e > 0$ we have to show that $\mathrm{Res}_{P/k}(\sigma_{L/K}\left(\frac{d\tau}{\tau^{ep+1}}\right)) = 0$. If $C^{-1} : \Omega^1_{L/k} \to \Omega^1_{L/k}/dL$ denotes the Cartier operator (given by $C^{-1}(fd\tau) = f^p\tau^{p-1}d\tau + dL$), then clearly $\mathrm{Res}_{R/k}(C^{-1}(\omega)) = \mathrm{Res}_{R/k}(\omega)^p$, and $\sigma_{L/K} \circ C^{-1} = C^{-1} \circ \sigma_{L/K}$. Hence we may apply the inverse of the Cartier-Operator and it suffices to show that

$$\mathrm{Res}_{P/k}(\sigma_{L/K}\left(\frac{d\tau}{\tau^{e+1}}\right)) = 0.$$

If $p \nmid e$ we are done again by the above case, and if $p|e$ we continue this procedure successively till we reach the case $p \nmid e$. $\square$

Proposition 1.7. $\omega^1_{X/k,x} \subseteq ker(\mathrm{Res}_{X/k,x})$.

Proof. By the trace formula for residues and the construction of $\omega^1_{X/k}$ it suffices to prove this for $X = \mathbb{P}^1_k$, in which case it is obvious. $\square$

Theorem 1.8 (residue theorem). *If* $\omega \in \Omega^1_{L/k}$ *then*

$$\sum_{x \in X} \mathrm{Res}_{X/k,x}(\omega) = 0.$$

Proof. Again apply the trace formula to reduce to the case $X = \mathbb{P}^1_k$. In this case it is well known and also easy to see by using expansion of rational functions by partial fractions (cf. [**15**], I, thm. 8). $\square$

Remark 1.9. The above construction of resdiues via power series expansion is very convenient from a mathematical point of view, however from a constructive point of view it is very difficult to handle. There are however other methods to calculate residues that are much better adapted to constructive approaches (see for instance [**1**] or [**11**]). In particular in case of an algebraic curve given by homogeneous equations (i.e. in terms of its homogeneous coordinate ring) the situation is fairly well understood.

2. Local and global duality. Duality theory for algebraic varieties and more generally for morphisms of schemes has been studied to a great extend over the last few decades. Duality theory for curves is contained in this as a very special situation. However in this case (as in §1) the whole theory can be developed very explicitly and very constructively. This is of interest in particular with respect to applications such as the construction of algebraic codes. Thus we include a short description of duality for curves (though it again is a special case of general Grothendieck duality theory; see also [**16**], [**13**], [**21**]). We also derive the version of the Riemann-Roch theorem needed in §3. Our definition of degree is a special case of the one used in [**17**], where the Riemann-Roch theorem is treated in terms of standard bases and with techniques going back to F.K. Schmidt and P. Roquette.

So let again k be a perfect field of positive characteristic, let X/k be an algebraic curve, let $x \in X$ be a closed point and let $R = \widehat{\mathcal{O}_{X,x}}$. As in 1.3 iii) we write $\omega^1_{R/k}$ for $\widehat{\omega}^1_{\mathcal{O}_{X,x}/k}$, the completion of $\omega^1_{\mathcal{O}_{X,x}/k}$. Furthermore let M be a torsion free and finite R-module (i.e. each non-zerodivisor of R is also a non-zerodivisor of M), and set $M^\vee := \mathrm{Hom}_R(M, \omega^1_{R/k})$

THEOREM 2.1 (local duality). *In the above situation for any local parameter π of R and any $n \in \mathbb{N}$ the pairing*

$$\rho_{n,\pi} : M/\pi^n M \times M^\vee/\pi^n M^\vee \longrightarrow k$$

given by $\rho_{n,\pi}(m + \pi^n M, \lambda + \pi^n M^\vee) = \mathrm{Res}_{R/k}\left(\frac{\lambda(m)}{\pi^n}\right)$ *is non-degenerate.*

PROOF. First we assume $R = k[[\pi]]$. In this case M is already free as an R-module, and we may assume that $M = R$. Then $M/\pi^n M = R/\pi^n R$ has a k-basis $1, \pi, \ldots, \pi^{n-1}$ and $M^\vee/\pi^n M^\vee = \Omega^1_{R/k}/\pi^n\Omega^1_{R/k}$ has a k-basis $d\pi, \pi d\pi, \ldots, \pi^{n-1}d\pi$. As

$$\rho_{n,\pi}(\pi^i, \pi^j d\pi) = \mathrm{Res}_{R/k}\left(\frac{\pi^{i+j}d\pi}{\pi^n}\right) = \begin{cases} 1 & \text{if } i+j = n-1 \\ 0 & \text{otherwise} \end{cases}$$

the claim follows in this case.

In general, the map $P = k[[\pi]] \to R$ is finite and it induces by 1.3 iii) and the Hom-Tensor-adjointness an isomorphism

$$\sigma : M^\vee = \mathrm{Hom}_R(M, \omega^1_{R/k}) \longrightarrow \mathrm{Hom}_P(M, \omega^1_{P/k}) = M^*$$

and via σ the pairing $\rho_{n,\pi}$ gets identified with

$$\rho^P_{n,\pi} : M/\pi^n M \times M^*/\pi^n M^* \longrightarrow k$$

by the trace formula, hence is non-degenerate. $\square$

Now let again X/k by a curve with field of rational functions L. Viewing $\Omega^1_{L/k}$ as a constant sheaf on X we obtain an exact sequence

$$(*) \qquad 0 \longrightarrow \omega^1_{X/k} \longrightarrow \Omega^1_{L/k} \longrightarrow \Omega^1_{L/k}/\omega^1_{X/k} \longrightarrow 0$$

where $\Omega^1_{L/k}/\omega^1_{X/k} = \bigoplus_{x\in X} \Omega^1_{L/k}/\omega^1_{X/k,x}$ (the latter being viewed as a direct sum of skyscraper sheaves, supported on $\{x\}$). In particular $(*)$ is an injective resolution $\mathcal{I}^\bullet$ of $\omega^1_{X/k}$ and the maps $\mathrm{Res}_{X/k,x}$ induce by 1.7 a morphism

$$\mathrm{Tr} : \Gamma(X, \Omega^1_{L/k}/\omega^1_{X/k}) = \bigoplus_{x\in X} \Omega^1_{L/k}/\omega^1_{X/k,x} \longrightarrow k$$

given by $\mathrm{Tr}((\overline{\omega_x})) = \sum_{x\in X} \mathrm{Res}_{X/k,x}(\omega_x)$. By the residue theorem, Tr gives a morphism $\Gamma(X, \mathcal{I}^\bullet) \to k$ of complexes, hence induces a map

$$\int_X : H^1(X, \omega^1_{X/k}) \longrightarrow k$$

in cohomology, which we call the global integral of X/k.

Theorem 2.2 (global duality). *For each coherent $\mathcal{O}_X$-module $\mathcal{M}$ the global integral $\int_X$ defines an isomorphism*

$$\delta_{\mathcal{M}} : \operatorname{Hom}_{\mathcal{O}_X}(\mathcal{M}, \omega^1_{X/k}) \longrightarrow \operatorname{Hom}_k(H^1(X, \mathcal{M}), k)$$
$$\alpha \longmapsto \int_X \circ H^1(X, \alpha).$$

Proof. i) Let $X = \mathbb{P}^1_k$ and let $\mathcal{M} = \mathcal{O}_X(\rho)$ for some $\rho \in \mathbb{Z}$. Then $\omega^1_{X/k} = \mathcal{O}_X(-2)$. Thus if $\rho \geq -1$ both sides vanish, and we are done. If $\rho \leq -2$, then

$$\operatorname{Hom}_{\mathcal{O}_X}(\mathcal{M}, \omega^1_{X/k}) = \Gamma(X, \mathcal{O}_X(-\rho - 2))$$

with k-basis $1, t, \ldots, t^{-\rho-2}$ and $H^1(X, \mathcal{O}_X(\rho))$ has a k-basis $\left[\frac{dt}{t}\right], \ldots, \left[\frac{dt}{t^{-\rho-1}}\right]$, where we describe $H^1(X, \mathcal{M})$ as the cokernel of the map

$$\varphi : \Gamma(U, \mathcal{M}) \oplus \Gamma(U', \mathcal{M}) \longrightarrow \Gamma(U \cap U', \mathcal{M}), \quad (a, b) \longmapsto b - a$$

where $U = \operatorname{Spec}(k[t])$ and where $U' = \operatorname{Spec}(k[\frac{1}{t}])$. As $\int_X \left[\frac{t^j dt}{t^i}\right] = \delta_{i,j+1}$ the claim follows in this case.

ii) Let $X = \mathbb{P}^1_k$. If $\mathcal{M} = \bigoplus_{i=1}^r \mathcal{O}_X(\rho_i)$ the claim follows obviously from i). If $\mathcal{M}$ is arbitrary, it has a presentation

$$\mathcal{F}_1 \longrightarrow \mathcal{F}_0 \longrightarrow \mathcal{M} \longrightarrow 0$$

with $\mathcal{F}_l = \bigoplus_{j=1}^{r_l} \mathcal{O}_X(\rho_{l,j})$ and the claim follows from the five-lemma and the right-exactness of $H^1(X, -)$.

iii) Let X be arbitrary. Then there exists a finite map $\pi : X \to \mathbb{P}^1_k = \mathbb{P}$, which is generically étale, and we have via the trace on the level of the corresponding rational function fields

$$\operatorname{Hom}_{\mathcal{O}_X}(\mathcal{M}, \omega^1_{X/k}) = \operatorname{Hom}_{\mathcal{O}_X}(\mathcal{M}, \mathcal{H}om_{\mathcal{O}_{\mathbb{P}}}(\pi_*\mathcal{O}_X, \omega^1_{\mathbb{P}/k})) = \operatorname{Hom}_{\mathcal{O}_{\mathbb{P}}}(\pi_*\mathcal{M}, \omega^1_{\mathbb{P}/k})$$

and

$$\operatorname{Hom}_k(H^1(X, \mathcal{M}), k) = \operatorname{Hom}_k(H^1(\mathbb{P}, \pi_*\mathcal{M}), k).$$

Via these isomorphisms $\delta^X_{\mathcal{M}}$ gets identified with $\delta^{\mathbb{P}}_{\pi_*\mathcal{M}}$ by the trace formula for global integrals (which is immediate from the trace formula for residues), and the theorem follows. □

Let again X/k be an arbitrary curve and let L be the field of rational functions on the curve X.

Definition. $\mathfrak{F}(X) := \{\mathcal{L} \subseteq L : \mathcal{L}$ is a finitely generated $\mathcal{O}_X$-module and $\mathcal{L} \neq (0)\}$ is called the semi-group of fractional ideals of $\mathcal{O}_X$.

Let $\mathcal{L} \in \mathfrak{F}(X)$. Then both $\mathcal{O}_X/\mathcal{L} \cap \mathcal{O}_X$ and $(\mathcal{L} + \mathcal{O}_X)/\mathcal{O}_X$ are coherent torsion sheaves on X.

Definition. $\deg(\mathcal{L}) := \dim_k H^0(X, (\mathcal{L}+\mathcal{O}_X)/\mathcal{O}_X) - \dim_k H^0(X, \mathcal{O}_X/\mathcal{L}\cap\mathcal{O}_X)$ is called the degree of $\mathcal{L}$.

Remark 2.3. i) This definition of the degree of a fractional ideal is also used in [**17**], where also a variant of the Riemann-Roch theorem for coherent torsion-free sheaves of higher rank can be found.

ii) As $\dim_L \Omega^1_{L/k} = 1$, there exists an isomorphism $\varphi : \Omega^1_{L/k} \to L$. Via φ we may view $\mathcal{K}_X := \varphi(\omega^1_{X/k})$ as a fractional ideal (the canonical ideal of X). Though $\mathcal{K}_X$ itself depends on φ, its degree $\deg(\mathcal{K}_X)$ does not.

Remark 2.4 (Properties of $\deg(\mathcal{F})$). Let $\mathcal{F} \in \mathfrak{F}(X)$ be a fractional ideal.

i) We have

$$\begin{aligned}\deg(\mathcal{F}) &= \sum_{x\in X} [\dim_k((\mathcal{F}_x + \mathcal{O}_{X,x})/\mathcal{O}_{X,x}) - \dim_k(\mathcal{O}_{X,x}/\mathcal{F}_x \cap \mathcal{O}_{X,x})] \\ &= \sum_{x\in X} [\dim_k(\mathcal{F}_x/\mathcal{F}_x \cap \mathcal{O}_{X,x}) - \dim_k(\mathcal{O}_{X,x}/\mathcal{F}_x \cap \mathcal{O}_{X,x})] \\ &= \sum_{x\in X} [\dim_k((\mathcal{F}_x + \mathcal{O}_{X,x})/\mathcal{O}_{X,x}) - \dim_k((\mathcal{F}_x + \mathcal{O}_{X,x})/\mathcal{F}_x)]\,.\end{aligned}$$

ii) If $\mathcal{F}$ is the fractional ideal of a principal Cartier divisor, i.e. $\mathcal{F} = \mathcal{O}_X \cdot f$ for some $f \in L$, then

$$\deg(\mathcal{F}) = 0.$$

iii) If $\mathcal{F} \cong \mathcal{L}$, then $\deg(\mathcal{F}) = \deg(\mathcal{L})$.

iv) If $\mathcal{F} \subseteq \mathcal{L}$, then $\deg(\mathcal{F}) \le \deg(\mathcal{L})$. More precisely

$$\deg(\mathcal{L}) - \deg(\mathcal{F}) = \sum_{x\in X} \dim_k(\mathcal{L}_x/\mathcal{F}_x).$$

v) If $\mathcal{L}$ is an invertible sheaf, then $\mathcal{F} \otimes_{\mathcal{O}_X} \mathcal{L} \in \mathfrak{F}(X)$ and

$$\deg(\mathcal{F} \otimes \mathcal{L}) = \deg(\mathcal{F}) + \deg(\mathcal{L}).$$

Proof. i) is clear by the very definition.

ii) By [**2**], (A.3.1) we reduce to the case that X is a regular curve, and in this situation the assertion is well-known (and easy to prove).

iii) Any isomorphism $\mathcal{F} \cong \mathcal{L}$ is induced by some isomorphism $f : L \to L$ (i.e. $f \in L^\times$). Thus it is easy to see that it suffices to show: If $\mathcal{G} \subseteq L$ is a free $\mathcal{O}_X$-module (of rank 1), then

$$\sum_{x\in X} [\dim_k((\mathcal{L}_x + \mathcal{O}_{X,x})/\mathcal{O}_{X,x}) - \dim_k(\mathcal{O}_{X,x}/\mathcal{L}_x \cap \mathcal{O}_{X,x})] =$$
$$\sum_{x\in X} [\dim_k((\mathcal{L}_x + \mathcal{G}_x)/\mathcal{G}_x) - \dim_k(\mathcal{G}_x/\mathcal{L}_x \cap \mathcal{G}_x)]\,.$$

For this note first that

$$(\mathcal{L}_x + \mathcal{O}_{X,x})/\mathcal{O}_{X,x} = \mathcal{L}_x/\mathcal{L}_x \cap \mathcal{O}_{X,x}$$
$$(\mathcal{L}_x + \mathcal{G}_x)/\mathcal{G}_x = \mathcal{L}_x/\mathcal{L}_x \cap \mathcal{G}_x.$$

As

$$\begin{aligned}\dim_k(\mathcal{L}_x/\mathcal{L}_x \cap \mathcal{O}_{X,x} \cap \mathcal{G}_x) - \dim_k(\mathcal{O}_{X,x}/\mathcal{O}_{X,x} \cap \mathcal{L}_x \cap \mathcal{G}_x) \\ = \dim_k(\mathcal{L}_x/\mathcal{L}_x \cap \mathcal{O}_{X,x}) - \dim_k(\mathcal{O}_{X,x}/\mathcal{O}_{X,x} \cap \mathcal{L}_x)\end{aligned}$$

the claim follows.

iv) In this situation we have

$$\begin{aligned}\deg(\mathcal{L}) &= \sum_{x\in X} [\dim_k(\mathcal{L}_x/\mathcal{O}_{X,x} \cap \mathcal{L}_x) - \dim_k(\mathcal{O}_{X,x}/\mathcal{O}_{X,x} \cap \mathcal{L}_x)] \\ &= \sum_{x\in X} [\dim_k(\mathcal{L}_x/\mathcal{O}_{X,x} \cap \mathcal{F}_x) - \dim_k(\mathcal{O}_{X,x}/\mathcal{O}_{X,x} \cap \mathcal{F}_x)] \\ &= \sum_{x\in X} \dim_k(\mathcal{L}_x/\mathcal{F}_x) + \deg(\mathcal{F}).\end{aligned}$$

v) It suffices to show that for each $x \in X$:

$$\begin{aligned}\dim_k(\mathcal{F}_x \otimes \mathcal{L}_x/\mathcal{O}_{X,x} \cap \mathcal{F}_x \otimes \mathcal{L}_x) - \dim_k(\mathcal{O}_{X,x}/\mathcal{O}_{X,x} \cap \mathcal{F}_x \otimes \mathcal{L}_x) \\ = \dim_k \mathcal{F}_x/\mathcal{O}_{X,x} \cap \mathcal{F}_x) - \dim_k(\mathcal{O}_{X,x}/\mathcal{O}_{X,x} \cap \mathcal{F}_x) \\ + \dim(\mathcal{L}_x/\mathcal{L}_x \cap \mathcal{O}_{X,x}) - \dim_k(\mathcal{O}_{X,x}/\mathcal{L}_x \cap \mathcal{O}_{X,x}).\end{aligned}$$

In view of iii) (resp. the calculations in its proof) we may assume that $\mathcal{O}_{X,x} \subseteq \mathcal{F}_x$ and $\mathcal{O}_{X,x} \subseteq \mathcal{L}_x$. Furthermore write $\mathcal{L}_x = g \cdot \mathcal{O}_{X,x}$. Then

$$\begin{aligned}\dim_k(\mathcal{F}_x \otimes \mathcal{L}_x/\mathcal{O}_{X,x}) - \dim_k(\mathcal{F}_x/\mathcal{O}_{X,x}) \\ = \dim_k(\mathcal{F}_x \cdot g/\mathcal{O}_{X,x}) - \dim_k(\mathcal{F}_x \cdot g/\mathcal{O}_{X,x} \cdot g) = \dim_k(\mathcal{O}_{X,x} \cdot g/\mathcal{O}_{X,x})\end{aligned}$$

and the claim follows. □

Corollary 2.5. *If* $H^0(X, \mathcal{F}) \neq (0)$, *then* $\deg(\mathcal{F}) \geq 0$.

Proof. Let $f \in H^0(X, \mathcal{F})$ and let $\mathcal{L} = \mathcal{O}_X \cdot f$ be the principal Cartier divisor determined by f. Then we have a canonical inclusion $\mathcal{L} \subseteq \mathcal{F}$, implying

$$\deg(\mathcal{F}) \geq \deg(\mathcal{L}) = 0$$

by 2.4. □

Definition. $g_X = \dim_k H^0(X, \omega^1_{X/k})$ is called the genus of X.

$h_X := \dim_k H^0(X, \mathcal{O}_X)$ is called the dimension of regular functions on X.

For a fractional ideal $\mathcal{L} \in \mathfrak{F}(X)$ we set

$$\mathcal{L}^\vee := \mathcal{H}om_{\mathcal{O}_X}(\mathcal{L}, \omega^1_{X/k})$$

Theorem 2.6 (Riemann-Roch). *Let $\mathcal{L}$ be a fractional ideal of X. Then*

$$\dim_k H^0(X,\mathcal{L}) = \dim_k H^0(X,\mathcal{L}^\vee) + \deg(\mathcal{L}) - g_X + h_X.$$

Proof. i) By the duality theorem we have to show

$$\chi(\mathcal{L}) = \deg(\mathcal{L}) - g_X + h_X$$

where $\chi(\mathcal{L}) = \dim_k H^0(X,\mathcal{L}) - \dim_k H^1(X,\mathcal{L})$ denotes the Euler-characteristics of $\mathcal{L}$.

ii) We may assume that $\mathcal{L} \subseteq \mathcal{O}_X$ or that $\mathcal{O}_X \subseteq \mathcal{L}$: This follows form the long exact cohomology sequence associated to

$$0 \to \mathcal{O}_X \cap \mathcal{L} \to \mathcal{L} \to \mathcal{L}/\mathcal{L} \cap \mathcal{O}_X \cong (\mathcal{L} + \mathcal{O}_X)/\mathcal{O}_X \to 0.$$

iii) If $\mathcal{O}_X \subseteq \mathcal{L} \subseteq \mathcal{L}'$ with $\mathcal{L}'/\mathcal{L} \cong \kappa(x)$ for some $x \in X$, then 2.6 holds for $\mathcal{L}$ if and only if it holds true for $\mathcal{L}'$. This follows from the long exact cohomology sequence associated to

$$0 \longrightarrow \mathcal{L} \longrightarrow \mathcal{L}' \longrightarrow \kappa(x) \longrightarrow 0$$

(where here $\kappa(x)$ denotes the skyscraper sheaf whose stalk at x is equal to $\kappa(x)$), and the fact, that $\deg(\mathcal{L}') = \deg(\mathcal{L}) + [\kappa(x) : k]$. A similar statement we have for $\mathcal{L}' \subseteq \mathcal{L} \subseteq \mathcal{O}_X$.

iv) The Riemann-Roch-theorem holds for $\mathcal{O}_X$ by the very definition.

From i) – iv) it follows by induction, that 2.6 holds in general. □

Lemma 2.7 (cf. [**14**], (4.19)). *For each $\mathcal{F} \in \mathfrak{F}(X)$ the canonical map*

$$\alpha : \mathcal{F} \longrightarrow \mathcal{H}om_{\mathcal{O}_X}(\mathcal{H}om_{\mathcal{O}_X}(\mathcal{F}, \omega^1_{X/k}), \omega^1_{X/k}) = \mathcal{F}^{\vee\vee}$$

is an isomorphism

Proof. The assertion is local in X, so we may assume that $X = \operatorname{Spec}(R)$, that $\mathcal{F} = \widetilde{M}$ for some fractional R-module $M \subseteq L$, and that there exists a separating noetherian normalization

$$P := k[t] \longrightarrow R.$$

Via Hom-Tensor adjointness, α corresponds to the canonical map

$$\widetilde{\alpha} : M \longrightarrow \operatorname{Hom}_P(\operatorname{Hom}_P(M, \Omega^1_{P/k}), \Omega^1_{P/k}).$$

As M is torsion-free as a P-module, it is P-projective, and therefore $\widetilde{\alpha}$ is obviously bijective. □

Corollary 2.8. $\deg(\mathcal{L}^\vee) = 2(g_X - h_X) - \deg(\mathcal{L})$.

PROOF. By the Riemann-Roch theorem (applied twice) and 2.7 we have

$$\begin{aligned}\dim_k H^0(X,\mathcal{L}^\vee) &= \dim_k H^0(X,\mathcal{L}^{\vee\vee}) + \deg(\mathcal{L}^\vee) - (g_X - h_X)\\ &= \dim_k H^0(X,\mathcal{L}) + \deg(\mathcal{L}^\vee) - (g_X - h_X)\\ &= \dim_k H^0(X,\mathcal{L}^\vee) + \deg(\mathcal{L}) - (g_X - h_X) + \deg(\mathcal{L}^\vee) - (g_X - h_X)\end{aligned}$$

and from this the corollary follows. □

COROLLARY 2.9. *If* $\deg(\mathcal{L}) > 2(g_X - h_X)$ *then*

$$\dim_k H^0(X,\mathcal{L}) = \deg(\mathcal{L}) - (g_X - h_X).$$

PROOF. In this situation we have that $\deg(\mathcal{L}^\vee) < 0$, hence by 2.5: $\dim_k H^0(X,\mathcal{L}^\vee) = 0$. Thus the corollary follows from the Riemann-Roch theorem. □

3. Residual representation of codes. Let $k = \mathbb{F}_q$ be a finite field with $q = p^e$ elements, let X/k be an algebraic curve and let L be its field of rational functions. A Cartier divisor D on X is a family $\{(U_i, f_i)\}$ consisting of open affine subsets $U_i \subseteq X$ and meromorphic functions $f_i \in L \setminus \{0\}$ such that

$$\frac{f_i}{f_j} \in \mathcal{O}_X^*(U_i \cap U_j) \quad \text{for all } i, j.$$

By $\mathrm{Div}^C(X)$ we denote the collection of Cartier divisors on X, where we identify two Cartier divisors $D = \{(U_i, f_i)\}_{i\in I}$ and $D' = \{(V_j, g_j)\}_{j\in J}$ if there exists a common refinement $\{W_l\}_{l\in L}$ of $\{U_i\}_{i\in I}$ and $\{V_j\}_{j\in J}$ (together with $\alpha : L \to I$ and $\beta : L \to J$) such that $\frac{f_{\alpha(l)}|W_l}{g_{\beta(l)}|W_l} \in \mathcal{O}_X^*(W_l)$ for all $l \in L$.

Associated with a Cartier-divisor $\{(U_i, f_i)\}$ we have an invertible sheaf $\mathcal{L}(D) \subseteq L$ defined by

$$\mathcal{L}(D)(V) := \{g \in L : g \in \frac{1}{f_i}\mathcal{O}_{X,x} \text{ for all } x \in V \cap U_i \text{ and all } i\}$$

for $V \subseteq X$ open.

REMARK 3.1. The map

$$\mathcal{L} : \mathrm{Div}^C(X) \longrightarrow \mathfrak{F}(X), \quad D \longmapsto \mathcal{L}(D)$$

defines a bijection onto the subset of invertible fractional ideals.

The divisor D is called effective, if $\mathcal{O}_{X,x} \subseteq \mathcal{L}(D)_x$ for all $x \in X$, and in this case

$$\deg_x(D) := \dim_k(\mathcal{L}(D)_x/\mathcal{O}_{X,x})$$

is called the local degree of D at x. In this situation we have that $f_i \in \mathcal{O}_{X,x}$ for all $x \in U_i$, and we call the image of f_i in $\mathcal{O}_{X,x}$ a local equation for D at x and denote it by f_x.

Remark 3.2. The local equation $f_x \in \mathcal{O}_{X,x}$ of D at x is – up to a unit of $\mathcal{O}_{X,x}$ – independent of the special choice of an i with $x \in U_i$.

For a fractional ideal $\mathcal{F} \in (X)$ we define its support by

$$\sup(\mathcal{F}) := \{x \in X : \mathcal{F}_x \neq \mathcal{O}_{X,x}\}$$

and for a Cartier-divisor D we set

$$\sup(D) := \sup(\mathcal{L}(D)).$$

Remark 3.3. $\sup(\mathcal{F}) \subseteq X$ is a proper, closed subset of X (hence in particular it is finite) for all fractional ideals $\mathcal{F} \in \mathfrak{F}(X)$.

As in §2 we define $\mathcal{F}^\vee := \mathcal{H}om_{\mathcal{O}_X}(\mathcal{F}, \omega^1_{X/k})$, and we note that this sheaf is canonically contained in the constant sheaf $\mathrm{Hom}_L(L, \Omega^1_{L/k}) = \Omega^1_{L/k}$.

Let D be an effective Cartier-divisor of degree n and let $\mathcal{F}$ be a fractional ideal with $\sup(\mathcal{F}) \cap \sup(D) = \emptyset$. For $x \in \sup(D)$ let $n(x)$ be the local degree of D at x, and let $f_x \in \mathcal{O}_{X,x}$ be a local equation for D at x. Then $n(x) = \dim_k(\mathcal{O}_{X,x}/f_x\mathcal{O}_{X,x})$, and we choose $t_1^{(x)}, \dots, t_{n(x)}^{(x)} \in \mathcal{O}_{X,x}$ in such a way, that their residue classes in $\mathcal{O}_{X,x}/f_x\mathcal{O}_{X,x}$ form a k-basis of this space. Let $\sup(D) = \{x_1, \dots, x_m\}$ and define

$$C := C_{D,\mathcal{F},t} : H^0(X, \mathcal{F}^\vee \otimes \mathcal{L}(D)) \longrightarrow \mathbb{F}_q^n = \mathbb{F}_q^{n(x_1)} \oplus \cdots \oplus \mathbb{F}_q^{n(x_m)}$$

by

$$C_{D,\mathcal{F},t}(\omega) = (\rho_{x_1,t}(\omega), \dots, \rho_{x_m,t}(\omega))$$

where

$$\rho_{x_j,t}(\omega) = (\mathrm{Res}_{X/k,x_j}(t_1^{(x_j)}\omega), \dots, \mathrm{Res}_{X/k,x_j}(t_{n(x_j)}^{(x_j)}\omega)).$$

Definition. $C_\Omega(D, \mathcal{F}, t) := \mathrm{im}(C_{D,\mathcal{F},t}) \subseteq \mathbb{F}_q^n$ is called the algebraic-geometric code defined by $\mathcal{F}$ and D (and $t = (t_1^{(x_1)}, \dots, t_{n(x_m)}^{(x_m)})$).

Remark 3.4. Assume that X is a smooth curve and $\mathcal{L} = \mathcal{L}(E)$ with a divisor $E = \sum_{i=1}^n x_i$ and with $\kappa(x_i) = \mathbb{F}_q$. Then we have $n(x) = 1$ for any $x \in \sup(E)$, and we may take $t_1^{(x)} = 1$ for all $x \in \sup(E)$. Then $C_\Omega(E, \mathcal{F}) := C_\Omega(E, \mathcal{F}, t)$ is the usual *residual Goppa-Code* (cf. [**18**], [**20**]).

Remark 3.5. Let $x \in \sup(D)$ and let f_x be a local equation of D at x. As

$$\mathcal{F}^\vee \otimes \mathcal{L}(D)_x = f_x^{-1} \cdot \omega^1_{X/k,x}$$

we obtain a well-defined map

$$p_x : H^0(X, \mathcal{F}^\vee \otimes \mathcal{L}(D)) \longrightarrow \omega^1_{X/k,x}/f_x \cdot \omega^1_{X/k,x}$$

given by

$$p_x(\omega) = f_x\omega + f_x \cdot \omega^1_{X/k,x}.$$

By local duality we furthermore get an isomorphism

$$\omega^1_{X/k,x}/f_x \cdot \omega^1_{X/k,x} \longrightarrow \mathrm{Hom}_k(\mathcal{O}_{X,x}/f_x \cdot \mathcal{O}_{X,x}, k)$$

given by

$$\omega + f_x \cdot \omega^1_{X/k,x} \longmapsto (a \longmapsto \mathrm{Res}_{X/k,x}\left(\frac{a\omega}{f_x}\right))$$

and thus the map

$$q_{x,t} : \omega^1_{X/k,x}/f_x \cdot \omega^1_{X/k,x} \longrightarrow \mathbb{F}_q^{n(x)}$$

defined by

$$q_{x,t}(\omega + f_x \cdot \omega^1_{X/k,x}) = \left(\mathrm{Res}_{X/k,x}\left(\frac{t_1^{(x)}\omega}{f_x}\right), \ldots, \mathrm{Res}_{X/k,x}\left(\frac{t_{n(x)}^{(x)}\omega}{f_x}\right)\right)$$

is bijective with

$$\rho_{x,t} = q_{x,t} \circ p_x.$$

In particular $\omega \in \ker(\rho_{x,t})$ if and only if $\omega \in \ker(p_x)$.

Proposition 3.6. *In the above situation*

$$ker(C_{D,\mathcal{F},t}) = H^0(X, \mathcal{F}^\vee).$$

In particular $C_{D,\mathcal{F},t}$ is injective, whenever $\deg(\mathcal{F}) > 2g_X - 2h_X$*, and* $C_\Omega(D, \mathcal{F}, t)$ *is an* $[\deg(D), \deg(D) + g_X - h_X - \deg(\mathcal{F})]_q$*-code whenever* $2(g_X - h_X) < \deg(\mathcal{F}) < n$*.*

Proof. Let $\omega \in H^0(X, \mathcal{F}^\vee \otimes \mathcal{L}(D))$ with $p_x(\omega) = 0$ for all $x \in \sup(D)$. Then by the very definition of p_x we have:

$$\begin{aligned}
\omega &\in H^0(X, \mathcal{F}^\vee \otimes \mathcal{L}(D)) \cap \bigcap_{x \in \sup(D)} \omega^1_{X/k,x} \\
&= H^0(X, \mathcal{F}^\vee \otimes \mathcal{L}(D)) \cap \bigcap_{x \in \sup(D)} \mathcal{F}^\vee_x \\
&\qquad\qquad (\text{as } \mathcal{F}^\vee_x = \omega^1_{X/k,x} \text{ for all } x \in \sup(D)) \\
&= \bigcap_{x \in X \setminus \sup(D)} (\mathcal{F}^\vee \otimes \mathcal{L}(D))_x \cap \bigcap_{x \in \sup(D)} (\mathcal{F}^\vee \otimes \mathcal{L}(D))_x \cap \bigcap_{x \in \sup(D)} \mathcal{F}^\vee_x \\
&= \bigcap_{x \in X} \mathcal{F}^\vee_x \\
&= H^0(X, \mathcal{F}^\vee)
\end{aligned}$$

and in view of 2.9 and 2.10 the claim follows. $\square$

THEOREM 3.7. *Let D be an effective Cartier divisor on X, let $\mathcal{F}$ be a fractional ideal with* $\sup(\mathcal{F}) \cap \sup(D) = \emptyset$ *and let* $\sup(D) = \{x_1, \ldots, x_m\}$. *For* $i = 1, \ldots, m$ *set* $n(x) := \deg_x(\mathcal{L}(D)) = \dim_k(\mathcal{L}(D)_x/\mathcal{O}_{X,x})$ *and define*

$$\rho := max\{l \in \mathbb{N} : \text{there exist } i_1, \ldots, i_l \quad \text{with } \sum_{\mu=1}^{l} n(x_{i_\mu}) \leq n - \deg(\mathcal{F}) + 2(g_X - h_X)\}.$$

Then

$$d(C_\Omega(D, \mathcal{F}, t)) \geq m - \rho.$$

DEFINITION. $d^*(D, \mathcal{F}) := m - \rho$ is called the designed distance of $C_\Omega(D, \mathcal{F})$.

PROOF. For $x \in \sup(\mathcal{L}(D))$ denote by $\mathfrak{I}(x)$ the skyscraper sheaf with

$$\mathfrak{I}(x)_x = (\mathcal{F}^\vee \otimes \mathcal{L}(D))_x/\mathcal{F}_x^\vee \qquad \mathfrak{I}(x)_y = 0 \text{ for } y \neq x.$$

As $\sup(\mathcal{F}) \cap \sup(D) = \emptyset$ we have

$$\dim_k H^0(X, \mathfrak{I}(x)) = n(x).$$

Furthermore the canonical map

$$\mathcal{F}^\vee \otimes \mathcal{L}(D) \longrightarrow \mathfrak{I}(x)$$

is a surjection of sheaves, whose kernel is a fractional ideal which we denote by $\mathcal{K}(x)$. By 2.4 iv) we get that $\deg(\mathcal{K}(x)) = \deg(\mathcal{F}^\vee \otimes \mathcal{L}(D)) - n(x)$. Inductively we define for any points $x_1, \ldots, x_\delta \in \sup(D)$ the sheaf $\mathcal{K}(x_1, \ldots, x_\delta)$ as the kernel of the canonical surjection

$$\mathcal{K}(x_1, \ldots, x_{\delta-1}) \longrightarrow \mathfrak{I}(x_\delta)$$

and we obtain $\deg(\mathcal{K}(x_1, \ldots, x_\delta)) = \deg(\mathcal{F}^\vee \otimes \mathcal{L}(D)) - \sum_{i=1}^{\delta} n(x_i)$.

Now assume that $\omega \in H^0(X, \mathcal{F}^\vee \otimes \mathcal{L}(D)) \setminus \{0\}$ and let $x_1, \ldots, x_\delta \in \sup(D)$ such that $p_{x_i}(\omega) = 0$ for $i = 1, \ldots, \delta$. Then

$$\omega \in H^0(X, \mathcal{K}(x_1, \ldots, x_\delta)) \setminus \{0\}$$

hence by 2.5

$$\deg(\mathcal{F}^\vee \otimes \mathcal{L}(D)) - \sum_{i=1}^{\delta} n(x_i) = \deg(\mathcal{K}(x_1, \ldots, x_\delta)) \geq 0$$

and therefore and by 2.8 and 2.4 $\delta \leq \rho$. By the local duality theorem this implies

$$d(C_\Omega(D, \mathcal{F}, t)) \geq m - \rho.$$

□

Corollary 3.8. *Let X be a curve of genus g_X (possible singular) and let D be a Cartier divisor with* $\sup(D) = \{x_1, \dots, x_n\}$ *($n > 0$) and $n(x_i) = 1$ for $i = 1, \dots, n$. Let $\mathcal{F}$ be a fractional ideal with* $\sup(D) \cap \sup(\mathcal{F}) = \emptyset$ *and with* $2g_X - 2 < \deg(\mathcal{F}) < n$*, and let $C = C_\Omega(D, \mathcal{F}, t)$. Then C is an $[n, k, d]_q$-Code with*

- $n = \deg(D)$.
- $k = n - \deg(\mathcal{F}) + g_X - 1$.
- $d \geq \deg(\mathcal{F}) - 2g_X + 2$.

Proof. It remains to note that $h_X = 1$ as X has an $\mathbb{F}_q$-rational point. $\square$

Example 3.9. Let D be a Cartier divisor on x with $\sup(D) = \{x_1, \dots, x_m\}$ and assume that $n(x_i) = 2$ for $i = 1, \dots, m$. Then

$$d(C_\Omega(D, \mathcal{F}, t)) \geq m - \lceil m + g_X - h_X - \frac{\deg(\mathcal{F})}{2} + 1 \rceil$$

where for an $a \in \mathbb{R}$ we set

$$\lceil a \rceil = \min\{n \in \mathbb{Z} : n \geq a\}.$$

Crucial for any type of code is the availability of a decoding algorithm. To find such an algorithm it is usually necessary to know the dual code. For this let $\mathcal{F}, D$ and (for any $x \in \sup(D)$) $t_1^{(x)}, \dots, t_{n(x)}^{(x)}$ be as at the beginning of this section. Let $f \in H^0(X, \mathcal{F})$ and let $x \in \sup(D)$. Then $\mathcal{F}_x = \mathcal{O}_{X,x}$, and therefore we get a well-defined canonical morphism

$$\varepsilon_x : H^0(X, \mathcal{F}) \longrightarrow \mathcal{O}_{X,x} \longrightarrow \mathcal{O}_{X,x}/d_x\mathcal{O}_{X,x}$$

where d_x is a local equation of D at x. Thus we get a unique representation

$$\varepsilon_x(f) = a_x(1, f) \cdot t_1^{(x)} + \cdots + a_x(n(x), f) \cdot t_{n(x)}^{(x)}$$

and we define

$$\delta_{x,t} : H^0(X, \mathcal{F}) \longrightarrow \mathbb{F}_q^{n(x)}$$

by $\delta_{x,t}(f) = (a_x(1, f), \dots, a_x(n(x), f))$ and

$$\mathrm{Ev}_{D,\mathcal{F},t} : H^0(X, \mathcal{F}) \longrightarrow \mathbb{F}_q^n = \mathbb{F}_q^{n(x_1)} \oplus \cdots \oplus \mathbb{F}_q^{n(x_m)}$$

by $\mathrm{Ev}_{D,\mathcal{F},t}(f) = (\delta_{x_1,t}(f), \dots, \delta_{x_m,t}(f))$.

Definition. $C(D, \mathcal{F}, t) := \mathrm{im}(\mathrm{Ev}_{D,\mathcal{F},t})$.

Remark. In case $X/\mathbb{F}_q$ is a smooth curve, $D = \sum_{i=1}^n x_i$ is a divisor with $\mathbb{F}_q$-rational points x_i and $t_1^{(x)} = 1$ for all $x \in \sup(D)$, the code $C(D, \mathcal{F}, t)$ is the *geometric Goppa-Code* as constructed in [**18**], II.2.1; see also [**20**], 3.1.1.

On $\mathbb{F}_q^n$ we have a canonical non-degenerate pairing (*standard inner product*)

$$\langle\ \ ,\ \ \rangle : \mathbb{F}_q^n \times \mathbb{F}_q^n \longrightarrow \mathbb{F}_q^n$$

given by $\langle (a_1, \ldots, a_n), (b_1, \ldots, b_n)\rangle = \sum_{i=1}^n a_i b_i$.

THEOREM 3.10. *$C(D, \mathcal{F}, t)$ is the code dual to $C_\Omega(D, \mathcal{F}, t)$ with respect to the standard inner product of $\mathbb{F}_q^n$.*

PROOF. Let $f \in H^0(X, \mathcal{F})$ and let $\omega \in H^0(X, \mathcal{F}^\vee \otimes \mathcal{L}(-D))$.

i) If $x \in X \setminus \sup(D)$ then $f \cdot \omega \in \omega^1_{X/k,x}$: This is clear as we have via the canonical identification $L \otimes \Omega^1_{L/k} = \Omega^1_{L/k}$:

$$f \cdot \omega \in H^0(X, \mathcal{F} \otimes \mathcal{F}^\vee \otimes \mathcal{L}(-D)) \subseteq H^0(X, \omega^1_{X/k} \otimes \mathcal{L}(-D)).$$

ii) Let $x \in \sup(D)$ and write

$$\rho_{x,t}(\omega) = (\mathrm{Res}_{X/k,x}(t_1^{(x)}\omega), \ldots, \mathrm{Res}_{X/k,x}(t_{n(x)}^{(x)}\omega))$$

and

$$\delta_{x,t}(f) = (a_x(1, f), \ldots, a_x(n(x), f)).$$

Then

$$\begin{aligned}\sum_{j=1}^{n(x)} a_x(j, f)\, \mathrm{Res}_{X/k,x}(t_j^{(x)}\omega)) &= \mathrm{Res}_{X/k,x}\left(\sum_{j=1}^{n(x)} t_j^{(x)} a_x(j, f)\omega\right)\\ &= \mathrm{Res}_{X/k,x}(f\omega).\end{aligned}$$

Thus with $\sup(D) = \{x_1, \ldots, x_m\}$ and with

$$C_{D,\mathcal{F},t}(\omega) = (r_1, \ldots, r_n), \quad \mathrm{Ev}_{D,\mathcal{F},t}(f) = (a_1, \ldots, a_n)$$

we have

$$\begin{aligned}\sum_{i=1}^n a_i r_i &= \sum_{j=1}^m \mathrm{Res}_{X/k,x_j}(f\omega)\\ &= \sum_{x \in X} \mathrm{Res}_{X/k,x}(f\omega)\\ &= 0\end{aligned}$$

by the residue theorem. Thus

$$C(D, \mathcal{F}, t) \subseteq C_\Omega(D, \mathcal{F}, t)^\perp.$$

iv) As in 3.6 one shows that $\ker(\mathrm{Ev}_{D,\mathcal{F},t}) = H^0(X, \mathcal{F}\otimes\mathcal{L}(-D))$. Combining this with the above we conclude (using the Riemann-Roch theorem and 2.4 v)):

$$\begin{aligned}
\dim_k C_\Omega(D,\mathcal{F},t) =\ & \dim_k H^0(X, \mathcal{F}^\vee \otimes \mathcal{L}(D)) - \dim_k H^0(X, \mathcal{F}^\vee) \\
=\ & \dim_k H^0(X, \mathcal{F} \otimes \mathcal{L}(-D)) + \deg(\mathcal{F}^\vee \otimes \mathcal{L}(D)) - (g_X - h_X) \\
& - \big[\dim_k H^0(X, \mathcal{F}) + \deg(\mathcal{F}^\vee) - (g_X - h_X)\big] \\
=\ & \deg(\mathcal{L}(D)) + \dim_k H^0(X, \mathcal{F} \otimes \mathcal{L}(-D)) - \dim_k H^0(X, \mathcal{F}) \\
=\ & n - \dim_k C(D,\mathcal{F},t)
\end{aligned}$$

and from this we conclude by counting dimensions

$$C_\Omega(D,\mathcal{F},t)^\perp = C(D,\mathcal{F},t).$$

□

REMARK 3.11. Using 3.10 one can try to generalize the basic decoding algorithm for the geometric Goppa Codes (cf. [**20**], (3.3.1) resp. [**18**], VII.5) to the more general situation of this section. In this situation the syndrome has to be defined by

$$[b,f] := \sum_{j=1}^{m} \sum_{i_j=1}^{n(x_j)} b_{j,i_j} a_{x_j}(i_j, f).$$

Suppose that $h_1, \ldots, h_t$ is an $\mathbb{F}_q$-basis of $H^1(X,\mathcal{F})$. If $a = c + e$ is the received word where $c \in C_\Omega(\mathcal{F}, D)$ is the word originally sent and where $e = (e_{j,i_j})_{j=1,\ldots,m;i_j=1,\ldots,n(x_j)}$ is an error-vector, then e is a solution of

$$(*) \qquad \sum_{j=1}^{m} \sum_{i_j=1}^{n(x_j)} a_{x_j}(i_j, h_\tau) Z_{j,i_j} = [a, h_\tau] \qquad \text{for all } \tau \in \{1, \ldots, t\}.$$

If we assume that $\|e\| \leq t < \frac{1}{2} d^*(D,\mathcal{F})$ (for some fixed t), then e is the unique solution of $(*)$ of weight at most t, and if we can find this unique solution of minimal weight, we can correct a and recover the original word c.

The system $(*)$ however has many other solutions. If $n(x) = 1$ for all $x \in \sup(D)$ (and X possible singular), then one can use an auxiliary Cartier-divisor $\mathcal{F}_1 = \mathcal{L}(F_1)$ (just as in [**18**], VII.5 or [**20**], (3.3.1) and under the assumptions stated there) to reduce $(*)$ to a system of linear equations, having e as its unique solution. In the general case we are (so far) not yet able to make this reduction. If we set

$$n(D) := \{n(x) : x \in \sup(D)\}$$

then we need to find an auxiliary Cartier-divisor $\mathcal{F}_1 = \mathcal{L}(F_1)$ satisfying

(1) $\sup(\mathcal{F}_1) \cap \sup(D) = \emptyset$.

(2) $\deg(\mathcal{F}_1) < \deg(\mathcal{F}) - 2(g_X - h_X) - t \cdot n(D)$.
(3) $\dim_k H^0(X, \mathcal{F}_1) > t \cdot n(D)$.

In this situation we can find an error-locating function g (similarly to [**18**], [**20**]), and if $n(x) = n(D)$ and $\mathcal{O}_{X,x}/d_x\mathcal{O}_{X,x}$ is a field for all $x \in \sup(D)$, then we can modify the basic decoding algorithm to cover our present situation as well. In general however we are not yet able to bound the total number of zeroes of $\mathrm{Ev}_{D,\mathcal{F},t}(g)$.

EXAMPLE 3.12. Let $X = \mathbb{P}^1_{\mathbb{F}_q}$ and let $\mathbb{P}^1_{\mathbb{F}_q}(\mathbb{F}_q) = \{a_1, \ldots, a_q, \infty\}$. In this situation all fractional ideals of X are given by Weil divisors and conversely. Let $D = \sum_{j=1}^q 2x_j$ and let $\mathcal{F} = l \cdot \infty$ for some $l \geq 0$. The field of rational functions of X is $L = \mathbb{F}_q(t)$, and X has an open affine cover consisting of the two rings $R = \mathbb{F}_q[t]$ and $R' = \mathbb{F}_q[\frac{1}{t}]$, where $\mathrm{Spec}(R)$ is the finite part of X, and where we identify the finite $\mathbb{F}_q$-rational points $a_i \in \mathbb{P}^1_{\mathbb{F}_q}(\mathbb{F}_q)$ with the prime ideals $(t - a_i) \subseteq R$. For each $a \in \sup(D)$ we have $n(a) = 2$, and we may choose

$$t_1^{(a)} = 1, \qquad t_2^{(a)} = t - a.$$

The space $H^0(X, \mathcal{F}^\vee \otimes \mathcal{L}(D))$ has an $\mathbb{F}_q$-basis

$$\frac{dt}{g(t)},\, t\frac{dt}{g(t)},\, \ldots,\, t^{2q-l-2}\frac{dt}{g(t)}$$

with $g(t) = \prod_{i=1}^q (t - a_i)^2$ and in this situation we have

- $\mathrm{Res}_{X/k,a_i}\left(\frac{dt}{g(t)}\right) = \frac{\sum_{j\neq i} \frac{-2}{a_i - a_j}}{\prod_{j\neq i}(a_i - a_j)^2}$.
- $\mathrm{Res}_{X/k,a_i}\left(\frac{t^\lambda dt}{g(t)}\right) = a_i^{\lambda-1}\left(\frac{\lambda - \sum_{j\neq i}\frac{2a_i}{a_i - a_j}}{\prod_{j\neq i}(a_i - a_j)^2}\right)$ (if $\lambda > 0$).
- $\mathrm{Res}_{X/k,a_i}\left((t - a_i)\frac{t^\lambda dt}{g(t)}\right) = \frac{a_i^\lambda}{\prod_{j\neq i}(a_i - a_j)^2}$.

Thus – up to equivalence – a generating matrix of $C_\Omega(D, \mathcal{F}, t)$ if given by the matrix G with

$$G = \begin{pmatrix} \sum_{j\neq 1}\frac{-2}{a_j - a_1} & 1 & \sum_{j\neq 2}\frac{-2}{a_j - a_2} & 1 & \cdots \\ 1 - \sum_{j\neq 1}\frac{2a_1}{a_j - a_1} & a_1 & 1 - \sum_{j\neq 2}\frac{2a_2}{a_j - a_2} & a_2 & \cdots \\ a_1\left(2 - \sum_{j\neq 1}\frac{2a_1}{a_j - a_1}\right) & a_1^2 & a_2\left(2 - \sum_{j\neq 2}\frac{2a_2}{a_j - a_2}\right) & a_2^2 & \cdots \\ \vdots & \vdots & \vdots & \vdots & \ddots \\ a_1^{l-1}\left(l - \sum_{j\neq 1}\frac{2a_1}{a_j - a_1}\right) & a_1^l & a_2^{l-1}\left(l - \sum_{j\neq 2}\frac{2a_2}{a_j - a_2}\right) & a_2^l & \cdots \end{pmatrix}.$$

The minimum distance of this code satisfies the a–priori bound

$$d(C_\Omega) \geq q - \lceil q - \frac{l}{2} \rceil.$$

If we concatenate $C_\Omega(D, \mathcal{F}, t)$ (in the obvious way) with a $[3,2,2]_q$-parity check code, then the minimum distance of the resulting code C satisfies

$$d(C) \geq 2\lfloor \frac{l}{2} \rfloor.$$

EXAMPLE 3.13. Let again $X = \mathbb{P}^1_{\mathbb{F}_q}$, let D be as in 3.12, and let $\mathcal{F}$ be an arbitrary divisor of degree l on X with $\sup(D) \cap \sup(\mathcal{F}) = \emptyset$. Then $\mathcal{F} = l \cdot \infty + (f)$ where (f) denotes the principal divisor associated to $f \in \mathbb{F}_q(t)^\times$ for a suitable f. Then $H^0(X, \mathcal{F}^\vee \otimes \mathcal{L}(D))$ has an $\mathbb{F}_q$-basis

$$\frac{dt}{f(t)g(t)}, t\frac{dt}{f(t)g(t)}, \ldots, t^{2q-l-2}\frac{dt}{f(t)g(t)}$$

with $g(t)$ as in 3.12, and the associated code $C_\Omega(D, \mathcal{F}, t)$ can be described similarly, using

$$-\operatorname{Res}_{X/k,a_i}\left(\frac{t^\lambda dt}{f(t)g(t)}\right) = a_i^{\lambda-1}\left(\frac{\lambda - \sum_{j\neq i}\frac{2a_i}{a_i-a_j}}{\prod_{j\neq i}(a_i-a_j)^2 \cdot f(a_i)} - \frac{a_i^\lambda}{\prod_{j\neq i}(a_i-a_j)^2 \cdot f(a_i)^2}\right)$$

$$-\operatorname{Res}_{X/k,a_i}\left((t-a_i)\frac{t^\lambda dt}{f(t)g(t)}\right) = \frac{a_i^\lambda}{\prod_{j\neq i}(a_i-a_j)^2 \cdot f(a_i)}.$$

PROBLEM 3.14. Assume we are in the situation of 3.12/3.13.

i) What is the actual minimum distance of the codes of 3.12 resp. 3.13?

ii) Is there a canonical choice of a divisor $\mathcal{F}$ (i.e. of a rational function $f \in \mathbb{F}_q(t)$) in 3.13 which maximizes the minimum distance of $C_\Omega(D, \mathcal{F}, t)$?

iii) Is there a canonical choice of a basis $t_1^{(a)}, t_2^{(a)}$ of $\mathcal{O}_{X,a}/\mathfrak{m}_a^2$ in 3.12/3.13 which maximizes the minimum distance of $C_\Omega(D, \mathcal{F}, t)$?

EXAMPLE 3.15. Let $S := \mathbb{F}_{p^2}[X,Y,Z]/(X^{p+1}+Y^{p+1}-Z^{p+1})$ and set $C := \operatorname{Proj}(S)$. Then C is a maximal curve with genus $g = \frac{p(p-1)}{2}$ and $p^2+1+p^2(p-1)$ points rational over $\mathbb{F}_{p^2}$ (Hermitian curve). Here we have

$$\omega_C = \mathcal{O}_C(p-2)$$

and if we fix ∞ as a distinguished point and take $\mathcal{F} = \mathcal{O}_C(a \cdot \infty)$, then we have

$$\Gamma(C, \mathcal{O}_C(m \cdot (p+1) \cdot \infty)) = \Gamma(C, \mathcal{O}_C(m)) = S_m$$

is the homogeneous component of degree m of S. Thus in this situation algebraic-geometric codes can be constructed and calculated rather explicitly. This however can also be achieved using calculations from F. K. Schmidt (cf. [**18**]).

EXAMPLE 3.16. More generally let

$$S = \mathbb{F}_q[X_0, \ldots, X_n]/(F_1, \ldots, F_{n-1})$$

be a (reduced and irreducible) complete intersection with homogeneous polynomials $F_1, \ldots, F_{n-1}$ and let $C = \mathrm{Proj}(S)$. If $d_i = \deg(F_i)$, then

$$\omega_C = \mathcal{O}_C(-n-1+\sum_{i=1}^{n-1} d_i).$$

Furthermore if $G \in S$ is a homogeneous non-zerodivisor of degree l, if $D := \mathfrak{V}_+(G)$ and if $E = \mathfrak{V}_+(X_0^a)$ then

$$H^0(C, \mathcal{L}(E)^\vee \otimes \mathcal{L}(D)) \cong S_{\sum d_i + l - a - n - 1}.$$

In this situation also residues can be calculated very explicitly and algorithmically, cf. [**1**], and thus algebraic-geometric codes may be viewed as being pretty well understood in this situation.

Garcia and Stichtenoth have provided explicit examples of towers of function fields $\{L_n\}$ over $\mathbb{F}_{q^2}$ such that the corresponding nonsingular models C_n satisfy

$$(*) \qquad \frac{\#C_n(\mathbb{F}_{q^2})}{g(C_n)} \longrightarrow q-1 \quad \text{as } n \to \infty$$

(cf. [**3**]). The nonsingular models C_n however are very hard to determine. It is fairly easy to find global complete intersections $C_n' \subseteq \mathbb{P}^n$ with field of rational functions L_n, however all the obvious choices for C_n' do not satisfy $(*)$. This raises the following

QUESTION 3.17. Is it possible to (explicitly) find families of global complete intersections $C_n \subseteq \mathbb{P}^n_{\mathbb{F}_{q^2}}$ with the following properties:

(1) $g(C_n) \longrightarrow \infty \qquad$ as $n \to \infty$.
(2) $\frac{\#C_n(\mathbb{F}_{q^2})}{g(C_n)} \longrightarrow q-1 \quad$ as $n \to \infty$.

REMARK 3.18. For general algebraic varieties (or even curves) no good general constructive approach to residues is known so far. In case $X = \mathbb{P}^1_{\mathbb{F}_q}$ we can describe residues rather explicitly in terms of derivatives and canonical traces $\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}$. Also in case of plane curves (or more generally globally complete intersection curves) fairly explicit algorithms to calculate residues can be developed (cf. [**11**]). Note in this context, that any function field $L/\mathbb{F}_q$ of transcendence degree 1 has a (possibly singular) model $X/\mathbb{F}_q$ in $\mathbb{P}^2_{\mathbb{F}_q}$.

References

1. Ertl S., Hübl R., *The Jacobian Formula for Laurent Polynomials,* Univ. Iagell. Acta Math. **37** (1999), 51–67.
2. Fulton W., *Intersection Theory,* Springer, Berlin, 1984.
3. Garcia A., Stichtenoth H., *A Tower of Artin–Schreier Extensions of Function Fields attaining the Drinfeld–Vladut Bound,* Invent. Math. **121** (1995), 211–222.
4. Goppa V.D., *Algebraico–Geometric Codes,* Math. USSR Izv. **21** (1983), 75–91.
5. Haché G., *Construction effective des Codes Géométriques,* These, Paris, 1996.
6. Hache G., Le Brigand D., *Effective Construction of Algebraic Geometry Codes,* IEEE Trans. Infom. Theory **41** (1995), 1615–1628.
7. Hübl R., Kunz E., *Integration of Differential Forms on Schemes,* J. reine angew. Math. **410** (1990), 53–83.
8. Hübl R., Seibert G., *The Adjunction Morphism for Regular Differential Forms and Duality for Projective Morphisms.* Comp. Math. **106** (1997), 87–123.
9. Hübl R., *Algebraic Aspects of the Theory of Residues.* Preprint, available via: `http://www.physik.uni-regensburg.de/~hur22158.script.html`
10. Hübl R., *Codierungstheorie und algebraische Kurven.* Manuscript, available via: `http://www.physik.uni-regensburg.de/~hur22158.script.html`
11. Hübl R., *Explicit Calculation of Residues and Residue Symbols.* In preparation.
12. Kunz E., *Kähler Differentials,* Vieweg, Wiesbaden, 1986.
13. Kunz E., *Residuen und Dualität auf projektiven algebraischen Varietäten,* Regensburger Trichter **19**, 1985.
14. Kunz E., Waldi R., *Regular Differential Forms,* Contemporary Math. **79**, AMS, Providence, 1988.
15. Lang S., *Introduction to algebraic and abelian functions,* Addison Wesley, Reading, 1972.
16. Lipman J., *Dualizing Sheaves, Differentials and Residues on Algebraic Varieties,* Astérisque **117**, 1984.
17. Rauscher W., *Torsionsfreie kohärente Garben auf projektiven algebraischen Kurven,* Dissertation, Regensburg, 1993.
18. Stichtenoth H., *Algebraic Function Fields and Codes,* Springer, Berlin, 1993.
19. Stichtenoth H., *Algebraic Geometric Codes,* Proc. Symp. Appl. Math. **50** (1995), 139–157.
20. Tsfasman M.A., Vladut S.G., *Algebraic–Geometric Codes,* Kluwer, Dordrecht, 1991.
21. Yekutieli A., *An explicit Construction of the Grothendieck Residue Complex,* Astérisque **208**, 1992.

Received December 20, 2000

Universität Regensburg
NWF I - Mathematik
93040 Regensburg
Germany