International Journal of Mathematics and
Computer Science, **10**(2015), no. 1, 1–11

Riemann-Roch Spaces and Linear Network Codes

Johan P. Hansen

Department of Mathematics
Aarhus University
Nordre Ringgade 1, 8000 Aarhus C
Denmark

email: matjph@imf.au.dk

(Received March 10, 2015, Accepted March 25, 2015)

Abstract

We construct linear network codes utilizing algebraic curves over finite fields and certain associated Riemann-Roch spaces and present methods to obtain their parameters.

In particular, we treat the Hermitian curve and the curves associated with the Suzuki and Ree groups all having the maximal number of points for curves of their respective genera.

Linear network coding transmits information in terms of a basis of a vector space and the information is received as a basis of a possibly altered vector space. Ralf Koetter and Frank R. Kschischang introduced a metric on the set of vector spaces and showed that a minimal distance decoder for this metric achieves correct decoding if the dimension of the intersection of the transmitted and received vector space is sufficiently large.

The vector spaces in our construction have minimal distance bounded from below in the above metric making them suitable for linear network coding.

Notation

- $\mathbb{F}_q$ is the finite field with q elements of characteristic p.

Key words and phrases: Linear network codes, Riemann-Roch theorem for curves.
AMS (MOS) Subject Classifications: 68M10, 90B18, 94A05.
ISSN 1814-0432, 2015, http://ijmcs.future-in-tech.net
Part of this work was done while visiting Institut de Mathématiques de Luminy, Marseille, France. I am grateful for the hospitality I have received. This work was supported by the Danish Council for Independent Research, grant no. DFF-4002-00367.

- $\mathbb{F} = \overline{\mathbb{F}_q}$ is an algebraic closure of $\mathbb{F}_q$.
- $G(l, N)$ is the Grassmannian of l-dimensional $\mathbb{F}$-linear subspaces of $\mathbb{F}^N$ and $G(l, N)(\mathbb{F}_q)$ its $\mathbb{F}_q$-rational points, i.e. l-dimensional $\mathbb{F}_q$-linear subspaces of $\mathbb{F}_q^N$.

1 Introduction

Linear network coding

In linear network coding transmission is obtained by transmitting a number of packets into the network and each packet is regarded as a vector of length N over a finite field $\mathbb{F}_q$. The packets travel the network through intermediate nodes, each forwarding $\mathbb{F}_q$-linear combinations of the packets it has available. Eventually the receiver tries to infer the originally transmitted packages from the packets that are received, see [2] and [10].

Ralf Koetter and Frank R. Kschischang [12] endowed the Grassmannian $G(l, N)(\mathbb{F}_q)$ of l-dimensional $\mathbb{F}_q$-linear subspaces of $\mathbb{F}_q^N$ with the metric

$$\begin{aligned} \operatorname{dist}(V_1, V_2) := \quad & \dim_{\mathbb{F}_q}(V_1 + V_2) - \dim_{\mathbb{F}_q}(V_1 \cap V_2) = && (1.1) \\ & \dim(V_1) + \dim(V_2) - 2\dim(V_1 \cap V_2) \ , && (1.2) \end{aligned}$$

where $V_1, V_2 \in G(l, N)(\mathbb{F}_q)$.

Definition 1. *A linear network code $\mathcal{C} \subseteq G(l, N)(\mathbb{F}_q)$ is a set of l-dimensional $\mathbb{F}_q$-linear subspaces of $\mathbb{F}_q^N$.*

The size of the code $\mathcal{C} \subseteq G(l, N)(\mathbb{F}_q)$ is denoted by $|\mathcal{C}|$ and the minimal distance by

$$D(\mathcal{C}) := \min_{V_1, V_2 \in \mathcal{C}, V_1 \neq V_2} \operatorname{dist}(V_1, V_2) \ . \tag{1.3}$$

The linear network code $\mathcal{C}$ is said to be of type $[N, l, \log_q |\mathcal{C}|, D(\mathcal{C})]$. Its normalized weight is $\lambda = \frac{l}{N}$, its rate is $R = \frac{\log_q(|\mathcal{C}|)}{Nl}$ and its normalized minimal distance is $\delta = \frac{D(\mathcal{C})}{2l}$.

Ralf Koetter and Frank R. Kschischang [12] showed that a minimal distance decoder for this metric achieves correct decoding if the dimension of the intersection of the transmitted and received vector-space is sufficiently large. Also they obtained Hamming, Gilbert-Varshamov and Singleton coding bounds.

Algebraic curves and Riemann-Roch spaces

Let X be an absolutely irreducible, projective algebraic curve of genus g defined over the finite field $\mathbb{F}_q$. Let $X(\mathbb{F}_q)$ be the $\mathbb{F}_q$-rational points on X.

To any subset $S \subseteq X(\mathbb{F}_q)$ and any positive integer k, we associate the divisor $\sum_{P\in S} P \in \mathrm{Div}(X)$ and the Riemann-Roch spaces

$$V = \mathrm{L}\Big(k \sum_{P\in S} P\Big) \subseteq \mathrm{L}\Big(k \sum_{P\in X(\mathbb{F}_q)} P\Big) = W \ . \tag{1.4}$$

Certain collections of such subspaces $V \subseteq W$ will comprise our linear network code with ambient space W.

The general construction and applications in concrete cases

In our construction, we obtain a subspace as in (1.4) for each subset $S \subseteq X(\mathbb{F}_q)$ of given size s. Using the Riemann-Roch theorem we are able to determine all the parameters of the resulting linear network codes depending on the number of $\mathbb{F}_q$-rational points on the curve X and its genus g.

The potential of our construction relies on the ability to find curves with many $\mathbb{F}_q$-rational points, which is in fact possible. We recollect some of the theory of bounds on the number of $\mathbb{F}_q$-rational on curves in 2.1.

In 2.2 we discuss the Hermitian curve and the Deligne-Lutzig curves associated with the Suzuki and Ree groups all having the maximal number of points for curves of their genera.

2 Construction of linear network codes from algebraic curves and Riemann-Roch spaces

Let X be a absolutely irreducible and projective algebraic curve of genus g defined over the finite field $\mathbb{F}_q$. Let $X(\mathbb{F}_q)$ be the set of $\mathbb{F}_q$-rational points on

X and $n = |X(\mathbb{F}_q)|$ their number.

For a fixed positive integer k, let $k \cdot \sum_{P \in X(\mathbb{F}_q)} P \in \operatorname{Div}(X)$ be the Frobenius invariant divisor of degree kn with support in all of the $\mathbb{F}_q$-rational points. The ambient vector space W of the linear network codes is the associated Riemann-Roch space

$$W = \mathrm{L}\Big(k \cdot \sum_{P \in X(\mathbb{F}_q)} P\Big) \ . \tag{2.5}$$

From Riemann-Roch we have

$$\begin{cases} N = \dim W \geq kn + 1 - g \\ N = \dim W = kn + 1 - g \quad \text{for } kn \geq 2g - 1 \end{cases} \tag{2.6}$$

We refer to [4] for the general theory of Riemann-Roch spaces.

Remark 2.1. *Let $D \in \operatorname{Div}(X)$ be a Frobenius-invariant divisor on X, then the vector space $\mathrm{L}(D)$ has a basis of Frobenius-invariant vectors and*

$$\dim \mathrm{L}(D) = \dim_{\mathbb{F}} \mathrm{L}(D) = \dim_{\mathbb{F}_{||}} \mathrm{L}(D)^{Fr} \ , \tag{2.7}$$

where $\mathrm{L}(D)^{Fr} \subseteq \mathrm{L}(D)$ denotes the subspace of Frobenius-invariant vectors in $\mathrm{L}(D)$.

As all our divisors are Frobenius-invariant and we will consistently use (2.7).

Definition 2. *For a fixed positive integer s, the linear network code $\mathcal{C}_{k,s}$ of linear subspaces of W in (2.5) is constructed by associating to any subset $S \subseteq X(\mathbb{F}_q)$ of size s, the Frobenius-invariant divisor $k \cdot \sum_{P \in S} P$ of degree ks and its Riemann-Roch space $V = \mathrm{L}\Big(k \cdot \sum_{P \in S} P\Big)$.*

Specifically

$$\mathcal{C}_{k,s} = \Big\{ V = \mathrm{L}\Big(k \cdot \sum_{P \in S} P\Big) \subseteq W \ \Big| \ S \subseteq X(\mathbb{F}_q), \ |S| = s \Big\} \ . \tag{2.8}$$

As for the dimension $l = \dim V$ of the linear subspaces $V = \mathrm{L}\Big(k \cdot \sum_{P \in S} P\Big)$ in the network code, the theorem of Riemann-Roch gives

$$\begin{cases} l = \dim V = \dim \mathrm{L}\Big(k \cdot \sum_{P \in S} P\Big) \geq ks + 1 - g \\ l = \dim V = \dim \mathrm{L}\Big(k \cdot \sum_{P \in S} P\Big) = ks + 1 - g \quad \text{for } ks \geq 2g - 1 \end{cases} \tag{2.9}$$

with S of size s, see [4].

As for the intersection of two linear subspaces $V_1 = \mathrm{L}\Big(k \cdot \sum_{P \in S_1} P\Big)$ and $V_2 = \mathrm{L}\Big(k \cdot \sum_{P \in S_2} P\Big)$ in the network code, we have from the definition of the Riemann-Roch spaces

$$V_1 \cap V_2 = \mathrm{L}\Big(k \cdot \sum_{P \in S_1} P\Big) \cap \mathrm{L}\Big(k \cdot \sum_{P \in S_2} P\Big) = \mathrm{L}\Big(k \cdot \sum_{P \in S_1 \cap S_2} P\Big) \tag{2.10}$$

If $S_1 \cap S_2 = \emptyset$, then $V_1 \cap V_2 = 0$ and $\dim V_1 \cap V_2 = 0$.
If $S_1 \cap S_2 \neq \emptyset$, then the theorem of Riemann-Roch gives

$$\begin{cases} \dim V_1 \cap V_2 \geq k|S_1 \cap S_2| + 1 - g \\ \dim V_1 \cap V_2 = k|S_1 \cap S_2| + 1 - g \text{ for } k|S_1 \cap S_2| \geq 2g - 1 \end{cases} \tag{2.11}$$

as the divisor $k \cdot \sum_{P \in S_1 \cap S_2}$ has degree $k|S_1 \cap S_2| > 0$.

Theorem 1. *Let X be an absolutely irreducible and projective algebraic curve of genus g defined over the finite field $\mathbb{F}_q$. Let $X(\mathbb{F}_q)$ be the $\mathbb{F}_q$-rational points on X and $n = |X(\mathbb{F}_q)|$ their number.*

Let $\mathcal{C}_{k,s}$ be the linear network code of Definition 2.

Assume k, s are positive integers with $ks \geq 2g - 1$.

The dimension N of the ambient space W is

$$N = \dim W = kn + 1 - g \ . \tag{2.12}$$

The dimension l of the vector spaces $V \in \mathcal{C}_{k,s}$ is

$$l = \dim V = ks + g - 1 \ . \tag{2.13}$$

The size of the code is

$$|\mathcal{C}_{k,s}| = \binom{n}{s} \ . \tag{2.14}$$

If $s = 1$ the minimum distance of the code is

$$D(\mathcal{C}_{k,s}) = 2(k + g - 1) \ . \tag{2.15}$$

If $s > 1$, assume $k(s-1) \geq 2g - 1$. The minimum distance of the code is

$$D(\mathcal{C}_{k,s}) = 2k \ . \tag{2.16}$$

Proof. The claim (2.12) follows from (2.6) and (2.13) follows from (2.9). The claim in (2.14) is obvious as there is a distinct vector space in the linear network code for each choice of s points among the n points in $|X(\mathbb{F}_q)|$.

Finally, (2.15) and (2.16) follow from (2.11), as we obtain the minimal distance between two distinct vector spaces $V_1 = \mathrm{L}\Big(k \cdot \sum_{P \in S_1} P\Big)$ and $V_2 = \mathrm{L}\Big(k \cdot \sum_{P \in S_2} P\Big)$ in the network code when their intersection has maximal dimension.

In case $s = 1$ the intersection always has dimension 0. From the definition of the metric in (1.1) and (2.13), we conclude

$$\operatorname{dist}(V_1, V_2) = 2(k + 1 - g) \ . \tag{2.17}$$

In case $s > 1$ the maximal dimension of the intersection is obtained when $|S_1 \cap S_2| = s - 1$ and under the assumption $k(s-1) \geq 2g - 1$, we have

$$\dim V_1 \cap V_2 = k|S_1 \cap S_2| + 1 - g = k(s-1) + 1 - g \ . \tag{2.18}$$

From the definition of the metric in (1.1) and (2.13), we conclude

$$\operatorname{dist}(V_1, V_2) = 2(ks + 1 - g) - 2(k(s-1) + 1 - g) = 2k \ . \tag{2.19}$$

□

Corollary 1. *Under the assumptions of the theorem and in the notation of Definition 1 the normalized weight of the code $\mathcal{C}_{k,s}$ is*

$$\lambda = \frac{ks+1-g}{kn+1-g} \ . \tag{2.20}$$

The rate of the code is

$$R = \frac{\log_q \left(\binom{n}{s}\right)}{(kn+1-g)(ks+1-g)} \ . \tag{2.21}$$

The normalized minimal distance δ of the code satisfies

$$\delta \geq \frac{2g-1}{(s+1)g-1} \ . \tag{2.22}$$

Proof. Only the claim on the normalized minimal distance is non-trivial.

In case $s=1$, two distinct vector spaces in the linear network code has trivial intersection and the normalized minimal distance δ is 1.

In case $s>1$, we get from the theorem that

$$\delta = \frac{2k}{2(ks+1-g)} = \frac{1}{s+\frac{1-g}{k}} \ . \tag{2.23}$$

By assumption $k \geq \frac{2g-1}{s-1}$ and (2.22) follows. □

2.1 Sizes of the codes and the number of rational points on the curves

Let $\mathbb{F}_q$ be the field with q elements, and let X be a projective and absolutely irreducible algebraic curve of genus g defined over $\mathbb{F}_q$.

In order to produce linear network codes of large size, curves with a larger number $|X(\mathbb{F}_q)|$ of $\mathbb{F}_q$-rational points are needed.

The Hasse-Weil bound asserts

$$1+q-2g\sqrt{q} \leq |X(\mathbb{F}_q)| \leq 1+g+2g\sqrt{q} \ . \tag{2.24}$$

For a given genus g, the Hasse-Weil bound (2.24) can often be improved, in particular when the genus g is large compared to the field size q.

Let $N_q(g)$ be the maximum number of $\mathbb{F}_q$-rational points on any curve over $\mathbb{F}_q$ of genus g.

Then

$$\limsup_{g \to \infty} \frac{N_q(g)}{g} = \sqrt{q} - 1 \tag{2.25}$$

for square cardinalities q.

Drinfeld and Vladut [3] derived the bound

$$\limsup_{g \to \infty} \frac{N_q(g)}{g} \leq \sqrt{q} - 1 \tag{2.26}$$

for fixed q.

Ihara [11] proved that

$$\limsup_{g \to \infty} \frac{N_q(g)}{g} = \sqrt{q} - 1 \tag{2.27}$$

for square cardinalities q. This was again proved by Tsfasman, Vladut and Zink in [15].

Garcia and Stichtenoth [5] wrote down explicit towers of field extensions in realizing the equality in (2.25), see also [6], [1] and [14]. For the general theory of function fields see [13].

Here we will not study the linear network codes constructed from the towers of Garcia and Stichtenoth, but proceed to present codes from Deligne-Lusztig curves all having the maximal number of $\mathbb{F}_q$-rational points allowed for their genera.

2.2 Linear network codes from Deligne-Luztig Curves

Linear network codes can be constructed from Riemann-Roch spaces on Deligne-Lusztig curves associated to a connected reductive algebraic group G defined over a finite field $\mathbb{F}_q$. These curves was originally introduced in [3].

The Deligne-Lusztig curves used in the construction of the codes have in some cases many $\mathbb{F}_q$-rational points. In fact, the maximal number in relation to their genera as determined by the explicit formulasof Weil.

The relevant groups for Deligne-Lusztig curves are groups of $\mathbb{F}_q$-rank 1. There are only four such groups: $A_1(q)$, ${}^2A_2(q^2)$, ${}^2B_2(q^2 = 2^{2k+1})$, ${}^2G_2(q^2 = 3^{2k+1})$.

The corresponding Deligne-Lusztig curves are smooth, projective curves over $\mathbb{F}_q$.

In [7] the genera of and the number of rational points on the corresponding curves are determined in all 4 cases:

i) A_1: $X = \mathbb{P}^1$. It has genus 0 and $1 + q$ over $\mathbb{F}_q$

ii) ${}^2A_2$: The Fermat curve $X : x^{q+1} + y^{q+1} = z^{q+1}$ of degree $q + 1$. It has genus $q(q - 1)/2$ and $1 + q^3$ points over $\mathbb{F}_{q^2}$.

iii) ${}^2B_2$: The Deligne-Lusztig curve of Suzuki type. It has genus $q(q^2 - 1)/\sqrt{2}$ and $1 + q^4$ points over $\mathbb{F}_{q^2}$.

iv) ${}^2G_2$: The Deligne-Lusztig curve of Ree type. It has genus $\sqrt{3}q(q^4 - 1)/2 + q^2(q^2 - 1)/2$ and has $1 + q^6$ points over $\mathbb{F}_{q^2}$.

See also [9] for the curves of Suzuki type, where bases for the vector spaces $\mathrm{L}(P)$ are determined and [8] for the curves of Ree type.

The parameters of the resulting linear network codes are obtained by substituting the values of g and $|X(\mathbb{F}_q)|$ in the formulas of Theorem 1 and Corollary 1.

References

[1] Alp Bassa, Arnaldo Garcia, Henning Stichtenoth, A new tower over cubic finite fields, *Mosc. Math. J.*, **8**, no. 3, 2008, 401–418.

[2] Philip A. Chou, Yunnan Wu, Kamal Jain, Practical network coding, 2003.

[3] P. Deligne and G. Lusztig. Representations of reductive groups over finite fields, *Ann. of Math. (2)*, **103**, no. 1, 1976, 103–161.

[4] William Fulton, *Algebraic curves*, Advanced Book Classics, Addison-Wesley Publishing Company, Advanced Book Program, Redwood City, CA, 1989. An introduction to algebraic geometry, Notes written with the collaboration of Richard Weiss, Reprint of 1969 original.

[5] Arnaldo García, Henning Stichtenoth, A tower of Artin-Schreier extensions of function fields attaining the Drinfeld-Vlăduţ bound, *Invent. Math.*, **121**, no. 1, 1995, 211–222.

[6] Arnaldo Garcíia, Henning Stichtenoth, Explicit towers of function fields over finite fields, In *Topics in geometry, coding theory and cryptography*, volume 6 of *Algebr. Appl.*, Springer, Dordrecht, 2007, 1–58.

[7] Johan P. Hansen. Deligne-Lusztig varieties and group codes, In *Coding theory and algebraic geometry (Luminy, 1991)*, volume 1518 of *Lecture Notes in Math.*, Springer, Berlin, 1992, 63–81.

[8] Johan P. Hansen, Jens Peter Pedersen, Automorphism groups of Ree type, Deligne-Lusztig curves and function fields, *J. Reine Angew. Math.*, **440**, 1993, 99–109.

[9] Johan P. Hansen, Henning Stichtenoth, Group codes on certain algebraic curves with many rational points, *Appl. Algebra Engrg. Comm. Comput.*, **1**, no. 1, 1990, 67–77.

[10] Tracey Ho, Muriel Médard, Ralf Koetter, David R. Karger, Michelle Effros, Jun Shi, Ben Leong, A random linear network coding approach to multicast, *IEEE TRANS. INFORM. THEORY*, **52**, no. 10, 2006, 4413–4430.

[11] Yasutaka Ihara. Some remarks on the number of rational points of algebraic curves over finite fields, *J. Fac. Sci. Univ. Tokyo Sect. IA Math.*, **28**, no. 3, 1982, 721–724.

[12] Ralf Koetter, Frank R. Kschischang, Coding for errors and erasures in random network coding, *IEEE Transactions on Information Theory*, **54** no. 8, 2008, 3579–3591.

[13] Henning Stichtenoth. *Algebraic function fields and codes*, volume 254 of *Graduate Texts in Mathematics*. Springer-Verlag, Berlin, second edition, 2009.

[14] Henning Stichtenoth. Recursive towers of function fields over finite fields. In *Arithmetic of finite fields*, volume 6087 of *Lecture Notes in Comput. Sci.*, Springer, Berlin, 2010, 1–6.

[15] M. A. Tsfasman, S. G. Vlăduţ, and Th. Zink. Modular curves, Shimura curves, and Goppa codes, better than Varshamov-Gilbert bound. *Math. Nachr.*, **109**, 1982, 21–28.