FORMS AND LINEAR NETWORK CODES

JOHAN P. HANSEN

Abstract. We present a general theory to obtain linear network codes utilizing forms and obtain explicit families of equidimensional vector spaces, in which any pair of distinct vector spaces intersect in the same small dimension. The theory is inspired by the methods of the author utilizing the osculating spaces of Veronese varieties.

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 af 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 are equidistant in the above metric and the distance between any pair of vector spaces is large making them suitable for linear network coding.

The parameters of the resulting linear network codes are determined.

Notation.

- $\mathbb{F}_q$ is the finite field with q elements of characteristic p.
- $\mathbb{F} = \overline{\mathbb{F}_q}$ is an algebraic closure of $\mathbb{F}_q$.
- $R_d = \mathbb{F}[X_0, \ldots, X_n]_d$ and $R_d(\mathbb{F}_q) = \mathbb{F}_q[X_0, \ldots, X_n]_d$ the homogenous polynomials of degree d with coefficients in $\mathbb{F}$ and $\mathbb{F}_q$.
- $R = \mathbb{F}[X_0, \ldots, X_n] = \oplus_d R_d$ and $R(\mathbb{F}_q) = \mathbb{F}_q[X_0, \ldots, X_n] = \oplus_d R_d(\mathbb{F}_q)$.
- $G(l, N)$ 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

1.1. **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

Date: March 7, 2013.

the receiver tries to infer the originally transmitted packages from the packets that are recieved, see [CWJJ03] and [HMK+06].

Ralf Koetter and Frank R. Kschischang [KK08] 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

$$\mathrm{dist}(V_1,V_2) := \dim_{\mathbb{F}_q}(V_1+V_2) - \dim_{\mathbb{F}_q}(V_1 \cap V_2), \tag{1}$$

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

$$D(\mathcal{C}) := \min_{V_1,V_2 \in \mathcal{C}, V_1 \neq V_2} \mathrm{dist}(V_1,V_2)\ . \tag{2}$$

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 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.

2. Explicit construction of linear network codes from normalized homogenous polynomials

Let $\mathcal{N}(e)$ be the normalized homogenous polynomials over $\mathbb{F}_q$ of degree e in $X_0,\ldots,X_n$ corresponding to monic polynomials in the single variable case. Specifically, $\mathcal{N}(e) = \mathbb{F}_q[X_0,\ldots,X_n]_e/\sim$, where $F_1 \sim F_2$ iff $F_1 = cF_2$ for some constant $c \in \mathbb{F}_q^*$. Let $\mathcal{I}(e) \subseteq \mathcal{N}(e)$ be the irreducible normalized homogenous polynomials.

For any subset $\mathcal{B} \subseteq \mathbb{F}_q[X_0,\ldots,X_n]_e/\sim$ of normalized homogenous polynomials of degree e, we define the linear network code $\mathcal{C}_\mathcal{B}$ as a collection of $\mathbb{F}_q$-linear subspaces V_G, one for each $G \in \mathcal{B}$, in the vector space of all homogenous forms of degree d .

Definition 2. *Let $G \in \mathbb{F}_q[X_0,\ldots,X_n]_e/\sim$ be a normalized homogenous polynomial in $X_0,\ldots,X_n$ of degree e with coefficients in $\mathbb{F}_q$. Assume that $G \neq 0$.*

Let $d \geq e$ and consider the $\mathbb{F}_q$-linear injective morphism

$$\begin{array}{ccc} \mathbb{F}_q[X_0,\ldots,X_n]_{d-e} & \to & \mathbb{F}_q[X_0,\ldots,X_n]_d \\ F & \mapsto & G\cdot F \end{array} \tag{3}$$

with image

$$V_G := G\cdot\mathbb{F}_q[X_0,\ldots,X_n]_{d-e} \subseteq \mathbb{F}_q[X_0,\ldots,X_n]_d = \mathbb{F}_q^N\ , \tag{4}$$

which is a $\mathbb{F}_q$-linear subspace of dimension $l = \binom{n+d-e}{n}$ in the ambient vector space of dimension $N = \binom{n+d}{n}$.

For any subset $\mathcal{B} \subseteq \mathbb{F}_q[X_0, \ldots, X_n]_e/\sim$ of normalized homogenous polynomials of degree e, the linear network code $\mathcal{C}_\mathcal{B} \subseteq G(l, N)(\mathbb{F}_q)$ consists of all the linear subspaces in the vector space $\mathbb{F}_q[X_0, \ldots, X_n]_d$ of homogenous forms of degree d with $d \geq e$, that are realized as images (4) for some $G \in \mathcal{B}$.

$$\mathcal{C}_\mathcal{B} = \{V_G = G \cdot \mathbb{F}_q[X_0, \ldots, X_n]_{d-e} |\ G \in \mathcal{B}\} \subseteq G(l, N)(\mathbb{F}_q)\ . \tag{5}$$

In [Han12] we studied the resulting linear network codes $\mathcal{C}_B$, when $\mathcal{B}$ is the set of normalized homogenous polynomials which are powers of linear terms, see Corollary 5. This amounted to the study of the osculating spaces of Veronese varieties.

In the present paper we present the resulting linear network codes $\mathcal{C}_B \subseteq G(l, N)(\mathbb{F}_q)$, when $\mathcal{B}$ more generally is any set of normalized homogenous polynomials in $\mathbb{F}_q[X_0, \ldots, X_n]_e/\sim$, where each pair of unequal polynomials has the constants as their only common divisors generalising the above result. In particular we treat the case where $\mathcal{B}$ is the set of all irreducible normalized polynomials, see Corollary 4.

Theorem 3. *Let $\mathcal{B} \subset \mathbb{F}_q[X_0, \ldots, X_n]_e/\sim$ be a set of normalized homogenous polynomials of degree e, such that for any pair $G_1, G_2 \in \mathcal{B}$, with $G_1 \neq G_2$, their only commen divisors are the constants.*

For $d \geq e$, let $\mathcal{C}_\mathcal{B} \subseteq G(l, N)(\mathbb{F}_q)$ be the corresponding linear network code, as defined in Definition 2.

The packet length of $\mathcal{C}_\mathcal{B}$ is $N = \binom{n+d}{n}$, the dimension of the ambient vector space. The vector spaces in the linear network code are equidimensional of dimension $l = \binom{n+d-e}{n}$ as $\mathbb{F}_q$-linear subspaces of the ambient $N = \binom{n+d}{n}$-dimensional $\mathbb{F}_q$-vectorspace $\mathbb{F}_q^N$.

The number of vector spaces in the linear network code $\mathcal{C}_\mathcal{B}$ is the number $|\mathcal{B}|$ of elements in $\mathcal{B}$.

The elements in the code are equidistant in the metric $\operatorname{dist}(V_1, V_2)$ of (1) of Section 1.1. Let $V_1, V_2 \in \mathcal{C}_\mathcal{B}$ be vector spaces with $V_1 \neq V_2$.

If $d - e < e$, then $\dim_{\mathbb{F}_q}(V_1 \cap V_2) = 0$ and

$$\operatorname{dist}(V_1, V_2) = 2 \binom{n+d-e}{n} \tag{6}$$

If $d - e \geq e$, then $\dim_{\mathbb{F}_q}(V_1 \cap V_2) = \binom{n+d-2e}{n}$ and

$$\operatorname{dist}(V_1, V_2) = 2 \left(\binom{n+d-e}{n} - \binom{n+d-2e}{n} \right) \tag{7}$$

Proof. The morphism in (3) maps injectively to the $\mathbb{F}_q$-vectorspace $\mathbb{F}_q[X_0, \ldots, X_n]_d$ of dimension $N = \dim_{\mathbb{F}_q} \mathbb{F}_q[X_0, \ldots, X_n]_d = \binom{n+d}{n}$. The dimension of the image is $l = \dim_{\mathbb{F}_q} V_G = \dim_{\mathbb{F}_q} \mathbb{F}_q[X_0, \ldots, X_n]_{d-e} = \binom{n+d-e}{n}$.

Let $V_{G_1}, V_{G_2} \in \mathcal{C}_{\mathcal{B}}$ be two vector spaces with $V_{G_1} \neq V_{G_2}$. Assume that $H \in V_{G_1} \cap V_{G_2}$ with $H \neq 0$. Then $H = G_1F_1 = G_2F_2$ with $F_i \in \mathbb{F}_q[X_0, \ldots, X_n]_{d-e}$. By unique factorization this implies that G_1 divides F_2 and there is a unique $K \in \mathbb{F}_q[X_0, \ldots, X_n]_{d-2e}$ such that $F_2 = G_1K$.

If $\deg F_2 = d - e < e = \deg G_1$, this is impossible and $V_{G_1} \cap V_{G_2} = 0$ proving (6) by the definition of the metric in (1).

If $\deg F_2 = d - e \geq e = \deg G_1$ then $H = G_2F_2 = G_2G_1K$ for a unigue $K \in \mathbb{F}_q[X_0, \ldots, X_n]_{d-2e}$. Therefore

$$\dim_{\mathbb{F}_q} V_{G_1} \cap V_{G_2} = \dim_{\mathbb{F}_q} \mathbb{F}_q[X_0, \ldots, X_n]_{d-2e} = \binom{n+d-2e}{n} \tag{8}$$

proving (7) by the definition of the metric in (1).

□

2.1. **The case when $\mathcal{B}$ is the set of all irreducible normalized polynomials.** Let $\mathcal{N}(e) = \mathbb{F}_q[X_0, \ldots, X_n]_e/\sim$ be the normalized homogenous polynomials of degree e.

As $\mathbb{F}_q[X_0, \ldots, X_n]_e$ is a vector space af dimension $\binom{n+e}{n}$ over $\mathbb{F}_q$, we have the following formula for the number $N(e)$ of normalized homogenous polynomials of degree e:

$$N(e) := |\mathcal{N}(e)| = \frac{q^{\binom{n+e}{n}} - 1}{q-1} \,. \tag{9}$$

Let $\mathcal{I}(e) \subseteq \mathcal{N}(e)$ be the irreducible normalized homogenous polynomials and let $I(e) := |\mathcal{I}(e)|$ be their number.

The number af products of a_i elements from $\mathcal{I}(i)$ is $\binom{\mathcal{I}(i)+a_i-1}{a_i}$. Using unique factorisation in $\mathbb{F}_q[X_0, \ldots, X_n]$, we get that

$$N(e) = \sum_{1a_1+2a_2+\ldots ea_e=e} \binom{I(1)+a_1-1}{a_1} \cdots \binom{I(i)+a_e-1}{a_e} \,. \tag{10}$$

and the rekursive formula for $I(e)$:

$$\begin{aligned} I(e) =& N(e) \\ &- \sum_{1a_1+2a_2+\ldots(e-1)a_{e-1}=e} \binom{I(1)+a_1-1}{a_1} \cdots \binom{I(i)+a_{e-1}-1}{a_{e-1}} \end{aligned} \tag{11}$$

Similar expressions in the non-homogenous case are obtained in [Bod08], [HM09], [Car65] and [Car63].

The same rekursive method permits to construct the elements in $\mathcal{I}(e)$ in the present case.

Corollary 4. *Let $\mathcal{I} \subset \mathbb{F}_q[X_0, \ldots, X_n]_e/\sim$ be the set of all irreducible normalized homogenous polynomials of degree e.*

For $d \geq e$, let $\mathcal{C}_{\mathcal{I}} \subseteq G(l, N)(\mathbb{F}_q)$ be the corresponding linear network code, as defined in Definition 2.

The packet length of $\mathcal{C}_{\mathcal{I}}$ is $N = \binom{n+d}{n}$, the dimension of the ambient vector space. The vector spaces in the linear network code are equidimensional of dimension $l = \binom{n+d-e}{n}$ as linear subspaces of the ambient $N = \binom{n+d}{n}$-dimensional $\mathbb{F}_q$-vectorspace $\mathbb{F}_q^N$.

The number of vector spaces in the linear network code $\mathcal{C}_{\mathcal{I}}$ is the number $|\mathcal{I}|$ of elements in $\mathcal{I}$ and is determined rekursively by the formula (11).

The elements in the code are equidistant in the metric $\operatorname{dist}(V_1, V_2)$ *of (1) of Section 1.1. Let $V_1, V_2 \in \mathcal{C}_{\mathcal{B}}$ be vector spaces with $V_1 \neq V_2$.*

If $d - e < e$, then $\dim_{\mathbb{F}_q}(V_1 \cap V_2) = 0$ *and*

$$\operatorname{dist}(V_1, V_2) = 2 \begin{pmatrix} n+d-e \\ n \end{pmatrix} \tag{12}$$

If $d - e \geq e$, then $\dim_{\mathbb{F}_q}(V_1 \cap V_2) = \binom{n+d-2e}{n}$ *and*

$$\operatorname{dist}(V_1, V_2) = 2 \left(\begin{pmatrix} n+d-e \\ n \end{pmatrix} - \begin{pmatrix} n+d-2e \\ n \end{pmatrix} \right). \tag{13}$$

Parameters for the linear network codes $\mathcal{C}_{\mathcal{I}(e)} \subseteq G(l, N)(\mathbb{F}_2)$ constructed from $\mathbb{F}_2[X_0, X_1, X_2]$ are given in Table 1 for $d = 1, 2, \ldots, 10$ and $e = 1, 2, \ldots, 5$.

2.2. **The case when $\mathcal{B}$ is the set of powers of linear normalized polynomials.** In [Han12] we studied the resulting linear network codes $\mathcal{C}_B$, when $\mathcal{B}$ is the set of normalized homogenous polynomials which are powers of linear terms. This amounted to the study of the osculating spaces of Veronese varieties.

Let $\mathcal{L}(e) \subseteq \mathcal{N}(e)$ be the set of e-fold powers of normalized homogenous linear polynomials and let $|\mathcal{L}(e)| = N(1) = \frac{q^{\binom{n+1}{n}}-1}{q-1}$ denote their number.

Corollary 5. *For $d \geq e$, let $\mathcal{C}_{\mathcal{L}} \subseteq G(l, N)(\mathbb{F}_q)$ be the corresponding linear network code, as defined in Definition 2.*

The packet length of $\mathcal{C}_{\mathcal{L}}$ is $N = \binom{n+d}{n}$, the dimension of the ambient vector space. The vector spaces in the linear network code are equidimensional of dimension $l = \binom{n+d-e}{n}$ as linear subspaces of the ambient $N = \binom{n+d}{n}$-dimensional $\mathbb{F}_q$-vectorspace.

The number of vector spaces in the linear network code $\mathcal{C}_{\mathcal{L}}$ is the number $|\mathcal{L}(e)| = N(1) = \frac{q^{\binom{n+1}{n}}-1}{q-1}$ of elements in $\mathcal{L}$. The elements in the code are equidistant in the metric $\operatorname{dist}(V_1, V_2)$ *of (1) of Section 1.1. Let $V_1, V_2 \in \mathcal{C}_{\mathcal{B}}$ be vector spaces with $V_1 \neq V_2$.*

TABLE 1. Parameters for the linear network codes $\mathcal{C}_{\mathcal{I}(e)} \subseteq G(l,N)(\mathbb{F}_2)$ with $\mathcal{I}(e) \subseteq \mathbb{F}_2[X_0,X_1,X_2]_e$, see Corollary 4

e	$\lvert\mathcal{C}\rvert$	d / N	1 / 3	2 / 6	3 / 10	4 / 15	5 / 21	6 / 28	7 / 36	8 / 45	9 / 55	10 / 66
1	7	l	1	3	6	10	15	21	28	36	45	55
		D	2	6	6	8	10	12	14	16	18	20
		λ	0,333	0,500	0,600	0,667	0,714	0,750	0,778	0,800	0,818	0,833
		δ	1,000	1,000	0,500	0,400	0,333	0,286	0,250	0,222	0,200	0,182
		R	0,936	0,156	0,047	0,019	0,009	0,005	0,003	0,002	0,001	0,001
2	35	l		1	3	6	10	15	21	28	36	45
		D		2	6	12	14	18	22	26	30	34
		λ		0,167	0,300	0,400	0,476	0,536	0,583	0,622	0,655	0,682
		δ		1,000	1,000	1,000	0,700	0,600	0,524	0,464	0,417	0,378
		R		0,855	0,171	0,057	0,024	0,012	0,007	0,004	0,003	0,002
3	694	l			1	3	6	10	15	21	28	36
		D			2	6	12	20	24	30	36	42
		λ			0,100	0,200	0,286	0,357	0,417	0,467	0,509	0,545
		δ			1,000	1,000	1,000	1,000	0,800	0,714	0,643	0,583
		R			0,944	0,210	0,075	0,034	0,017	0,010	0,006	0,004
4	26089	l				1	3	6	10	15	21	28
		D				2	6	12	20	30	36	44
		λ				0,067	0,143	0,214	0,278	0,333	0,382	0,424
		δ				1,000	1,000	1,000	1,000	1,000	0,857	0,786
		R				0,978	0,233	0,087	0,041	0,022	0,013	0,008
5	1862994	l					1	3	6	10	15	21
		D					2	6	12	20	30	42
		λ					0,048	0,107	0,167	0,222	0,273	0,318
		δ					1,000	1,000	1,000	1,000	1,000	1,000
		R					0,992	0,248	0,096	0,046	0,025	0,015

If $d-e<e$, *then* $\dim_{\mathbb{F}_q}(V_1\cap V_2)=0$ *and*

$$\operatorname{dist}(V_1,V_2)=2\begin{pmatrix}n+d-e\\ n\end{pmatrix} \tag{14}$$

If $d-e\geq e$, *then* $\dim_{\mathbb{F}_q}(V_1\cap V_2)=\binom{n+d-2e}{n}$ *and*

$$\operatorname{dist}(V_1,V_2)=2\left(\begin{pmatrix}n+d-e\\ n\end{pmatrix}-\begin{pmatrix}n+d-2e\\ n\end{pmatrix}\right). \tag{15}$$

REFERENCES

[Bod08] Arnaud Bodin. Number of irreducible polynomials in several variables over finite fields. *Amer. Math. Monthly*, 115(7):653–660, 2008.

[Car63] L. Carlitz. The distribution of irreducible polynomials in several indeterminates. *Illinois J. Math.*, 7:371–375, 1963.

[Car65] L. Carlitz. The distribution of irreducible polynomials in several indeterminates. II. *Canad. J. Math.*, 17:261–266, 1965.

[CWJJ03] Philip A. Chou, Yunnan Wu, Kamal Jain, and Kamal Jain. Practical network coding. 2003.

[Han12] J. P. Hansen. Osculating Spaces of Varieties and Linear Network Codes. *ArXiv e-prints*, October 2012.

[HM09] Xiang-dong Hou and Gary L. Mullen. Number of irreducible polynomials and pairs of relatively prime polynomials in several variables over finite fields. *Finite Fields Appl.*, 15(3):304–331, 2009.

[HMK+06] Tracey Ho, Muriel Médard, Ralf Koetter, David R. Karger, Michelle Effros, Jun Shi, and Ben Leong. A random linear network coding approach to multicast. *IEEE TRANS. INFORM. THEORY*, 52(10):4413–4430, 2006.

[KK08] Ralf Koetter and Frank R. Kschischang. Coding for errors and erasures in random network coding. *IEEE Transactions on Information Theory*, 54(8):3579–3591, 2008.

Department of Mathematics, Aarhus University
E-mail address: matjph@imf.au.dk