Random Network Codes and Algebraic Curves

Matteo Bonini

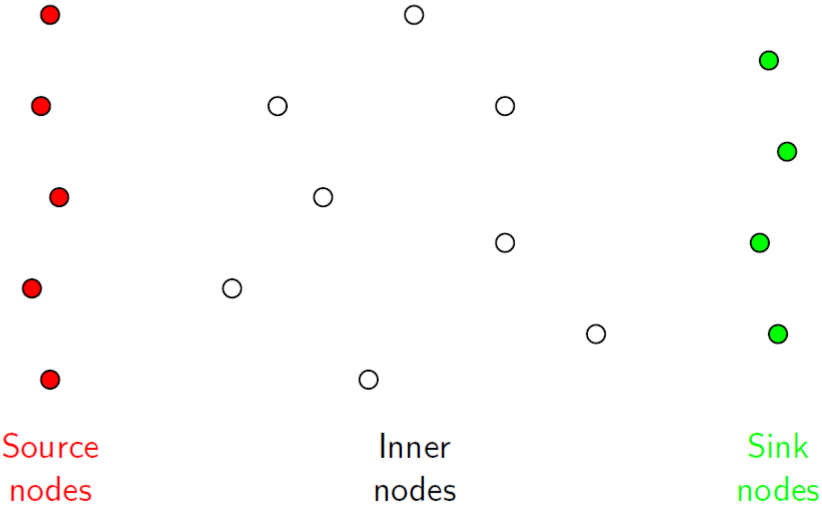
(joint work with Daniele Bartoli and Massimo Giulietti)

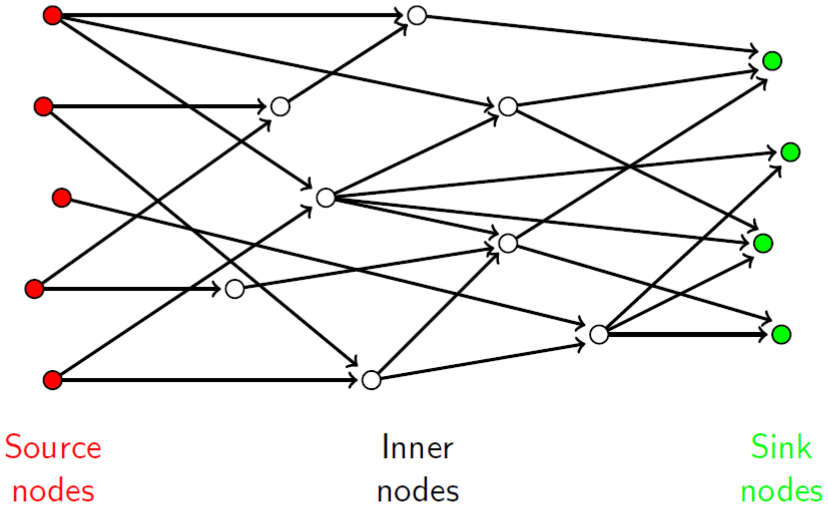
University of Trento

17 December 2015

Source nodes

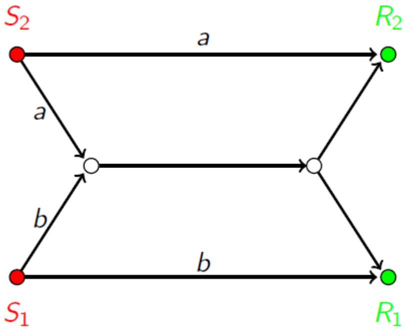

Source nodes
Sink nodes


Source nodes
Inner nodes
Sink nodes



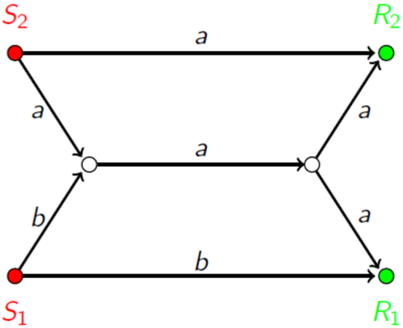
Source
nodes
Inner
nodes
Sink
nodes

Butterfly Network



S_1 sends only b
S_2 sends only a

Butterfly Network



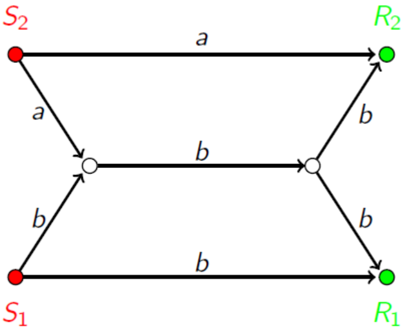
S_1 sends only b

S_2 sends only a

R_1 receives a AND b

R_2 receives only a

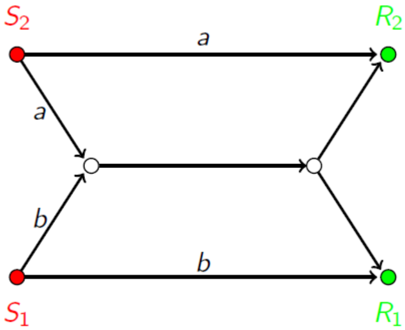
Butterfly Network



S_1 sends only b
S_2 sends only a

R_1 receives only b
R_2 receives a AND b

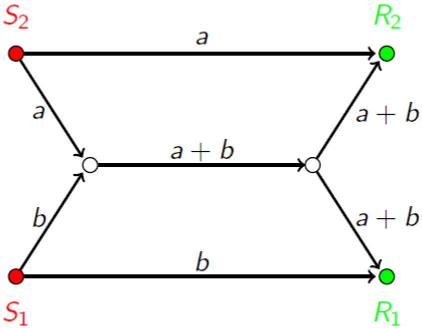
Butterfly Network



S_1 sends only b

S_2 sends only a

Butterfly Network



S_1 sends only b
S_2 sends only a

R_1 receives b AND $a+b \Rightarrow a$
R_2 receives a AND $a+b \Rightarrow b$

Random Network Coding

- Random network coding uses the same idea of the butterfly network.

Random Network Coding

- Random network coding uses the same idea of the butterfly network.
- The sources send linear vector spaces injecting a basis into the network.

Random Network Coding

- Random network coding uses the same idea of the butterfly network.
- The sources send linear vector spaces injecting a basis into the network.
- The inner nodes make a random linear $\mathbb{F}_q$-combination of the vectors received.

Random Network Coding

- Random network coding uses the same idea of the butterfly network.
- The sources send linear vector spaces injecting a basis into the network.
- The inner nodes make a random linear $\mathbb{F}_q$-combination of the vectors received.
- The vector space that arrives to the sinks is the same sent from the sources.

- $\mathbb{F}_q$ is the finite field with $q = p^h$ elements, where p is prime.

- $\mathbb{F}_q$ is the finite field with $q = p^h$ elements, where p is prime.
- $\mathbb{K} = \overline{\mathbb{F}_q}$.

- $\mathbb{F}_q$ is the finite field with $q = p^h$ elements, where p is prime.
- $\mathbb{K} = \overline{\mathbb{F}_q}$.

Definition

The set of all $\mathbb{F}_q$-linear subspaces of $\mathbb{F}_q^N$ with fixed dimension $\ell \leq N$ is named **Grassmannian** $\mathcal{G}_q(N, \ell)$.

- $\mathbb{F}_q$ is the finite field with $q = p^h$ elements, where p is prime.
- $\mathbb{K} = \overline{\mathbb{F}_q}$.

Definition

The set of all $\mathbb{F}_q$-linear subspaces of $\mathbb{F}_q^N$ with fixed dimension $\ell \leq N$ is named **Grassmannian** $\mathcal{G}_q(N, \ell)$.

Definition [Kötter, Kschischang. 2008]

We define the subspace distance $d : \mathcal{G}_q(N, \ell) \times \mathcal{G}_q(N, \ell) \to \mathbb{Z}_+$ by

$$d(U, V) := \dim(U + V) - \dim(U \cap V).$$

From Grassman's formula we have that

$$\begin{aligned} d(U, V) &= \dim(U) + \dim(V) - 2\dim(U \cap V) \\ &= 2\ell - 2\dim(U \cap V) \end{aligned}$$

Definition

A **Network Code** is a set $C \subseteq \mathcal{G}_q(n,\ell)$. C is a $[N, \ell, \log_q |C|, D(C)]$-code where:

- N $\rightarrow$ lenght
- $\log_q |C|$ $\rightarrow$ dimension
- $D(C) := \min_{\substack{U, V \in C \\ U \neq V}} d(U,V)$ $\rightarrow$ minimum distance

Definition

A **Network Code** is a set $C \subseteq \mathcal{G}_q(n, \ell)$. C is a $[N, \ell, \log_q |C|, D(C)]$-code where:

- $N \rightarrow$ lenght
- $\log_q |C| \rightarrow$ dimension
- $D(C) := \min_{\substack{U, V \in C \\ U \neq V}} d(U, V) \rightarrow$ minimum distance

Definition

Given a $[N, \log_q |C|, D(C)]$-code

- $\lambda = \frac{\ell}{N} \rightarrow$ normalized weight
- $R = \frac{\log_q(|C|)}{N\ell} \rightarrow$ rate
- $\delta = \frac{D(C)}{2\ell} \rightarrow$ normalized minimum distance

Riemann-Roch Spaces

- $\mathcal{X} : F(X,Y) = 0$ is a curve an absolutely irreducible, projective algebraic curve of genus g defined over $\mathbb{F}_q$.

Riemann-Roch Spaces

- $\mathcal{X} : F(X, Y) = 0$ is a curve an absolutely irreducible, projective algebraic curve of genus g defined over $\mathbb{F}_q$.
- $\mathcal{X}(\mathbb{F}_q)$ the set of the $\mathbb{F}_q$-rational points of $\mathcal{X}$.

Riemann-Roch Spaces

- $\mathcal{X} : F(X,Y) = 0$ is a curve an absolutely irreducible, projective algebraic curve of genus g defined over $\mathbb{F}_q$.
- $\mathcal{X}(\mathbb{F}_q)$ the set of the $\mathbb{F}_q$-rational points of $\mathcal{X}$.

Definition

Let $\alpha = \frac{G+(F)}{H+(F)}$ be a rational function and $P \in \mathcal{X}(\mathbb{F}_q)$.

- P is a zero if $G(P) = 0$ and $H(P) \neq 0$.

Riemann-Roch Spaces

- $\mathcal{X} : F(X, Y) = 0$ is a curve an absolutely irreducible, projective algebraic curve of genus g defined over $\mathbb{F}_q$.
- $\mathcal{X}(\mathbb{F}_q)$ the set of the $\mathbb{F}_q$-rational points of $\mathcal{X}$.

Definition

Let $\alpha = \frac{G+(F)}{H+(F)}$ be a rational function and $P \in \mathcal{X}(\mathbb{F}_q)$.

- P is a zero if $G(P) = 0$ and $H(P) \neq 0$.
- P is a pole if $G(P) \neq 0$ and $H(P) = 0$.

$V_P(\alpha)$ the multiplicity of P as zero or pole.

Riemann-Roch Spaces

- $\mathcal{X} : F(X,Y) = 0$ is a curve an absolutely irreducible, projective algebraic curve of genus g defined over $\mathbb{F}_q$.
- $\mathcal{X}(\mathbb{F}_q)$ the set of the $\mathbb{F}_q$-rational points of $\mathcal{X}$.

Definition

Let $\alpha = \frac{G+(F)}{H+(F)}$ be a rational function and $P \in \mathcal{X}(\mathbb{F}_q)$.

- P is a zero if $G(P) = 0$ and $H(P) \neq 0$.
- P is a pole if $G(P) \neq 0$ and $H(P) = 0$.

$V_P(\alpha)$ the multiplicity of P as zero or pole.

- A divisor is in the form $D = m_1 P_1 + \ldots m_r P_r$

Riemann-Roch Spaces

- $\mathcal{X} : F(X, Y) = 0$ is a curve an absolutely irreducible, projective algebraic curve of genus g defined over $\mathbb{F}_q$.
- $\mathcal{X}(\mathbb{F}_q)$ the set of the $\mathbb{F}_q$-rational points of $\mathcal{X}$.

Definition

Let $\alpha = \frac{G+(F)}{H+(F)}$ be a rational function and $P \in \mathcal{X}(\mathbb{F}_q)$.

- P is a zero if $G(P) = 0$ and $H(P) \neq 0$.
- P is a pole if $G(P) \neq 0$ and $H(P) = 0$.

$V_P(\alpha)$ the multiplicity of P as zero or pole.

- A divisor is in the form $D = m_1 P_1 + \dots m_r P_r$
- $\mathcal{L}(D) = \{\alpha \neq 0 \text{ rational function} \big| V_{P_i}(\alpha) + m_i \geq 0, i = 1, \dots, r\} \cup \{0\}$

Riemann-Roch Theorem

Riemann-Roch Theorem

Let W be a divisor with $\deg W = 2g - 2$ and D a divisor, then $\dim_{\mathbb{F}_q} \mathcal{L}(D) = \deg D + 1 - g + \dim_{\mathbb{F}_q} \mathcal{L}(W - D)$.

Riemann-Roch Theorem

Riemann-Roch Theorem

Let W be a divisor with $\deg W = 2g - 2$ and D a divisor, then
$\dim_{\mathbb{F}_q} \mathcal{L}(D) = \deg D + 1 - g + \dim_{\mathbb{F}_q} \mathcal{L}(W - D)$.

Corollary

If $\deg D > 2g - 2$ then $\dim_{\mathbb{F}_q} \mathcal{L}(D) = \deg D + 1 - g$.

Hansen's Costruction

- $D = \sum_{P \in \mathcal{X}_{\mathbb{F}_q}} P$, $\deg(D) = n := |\mathcal{X}_{\mathbb{F}_q}|$

Hansen's Costruction

- $D = \sum_{P \in \mathcal{X}_{\mathbb{F}_q}} P$, $\deg(D) = n := |\mathcal{X}_{\mathbb{F}_q}|$
- $\mathcal{L}(D) = \left\{ \alpha \neq 0 \text{ rational function} \middle| V_{P_i}(\alpha) \geq -1,\ i = 1, \ldots, n \right\} \cup \{0\}$

Hansen's Costruction

- $D = \sum_{P \in \mathcal{X}_{\mathbb{F}_q}} P$, $\deg(D) = n := |\mathcal{X}_{\mathbb{F}_q}|$
- $\mathcal{L}(D) = \left\{\alpha \neq 0 \text{ rational function} \middle| V_{P_i}(\alpha) \geq -1,\ i = 1, \dots, n\right\} \cup \{0\}$

Construction of the code

- $k \geq 0$, $0 < s \leq n$ fixed integers.

Hansen's Costruction

- $D = \sum_{P \in \mathcal{X}_{\mathbb{F}_q}} P$, $\deg(D) = n := |\mathcal{X}_{\mathbb{F}_q}|$
- $\mathcal{L}(D) = \left\{ \alpha \neq 0 \text{ rational function} \middle| V_{P_i}(\alpha) \geq -1,\ i = 1, \ldots, n \right\} \cup \{0\}$

Construction of the code

- $k \geq 0$, $0 < s \leq n$ fixed integers.
- $\mathcal{W} = \mathcal{L}(kD)$ ambient space.

Hansen's Costruction

- $D = \sum_{P \in \mathcal{X}_{\mathbb{F}_q}} P$, $\deg(D) = n := |\mathcal{X}_{\mathbb{F}_q}|$
- $\mathcal{L}(D) = \left\{ \alpha \neq 0 \text{ rational function} \middle| V_{P_i}(\alpha) \geq -1,\ i = 1, \ldots, n \right\} \cup \{0\}$

Construction of the code

- $k \geq 0$, $0 < s \leq n$ fixed integers.
- $\mathcal{W} = \mathcal{L}(kD)$ ambient space.
- Chosen $S \subset \mathcal{X}(\mathbb{F}_q)$ such that $|S| = s$ consider the divisor $D_S := \sum_{P \in S} P$, $\deg D_S = s$.

Hansen's Costruction

- $D = \sum_{P \in \mathcal{X}_{\mathbb{F}_q}} P$, $\deg(D) = n := |\mathcal{X}_{\mathbb{F}_q}|$
- $\mathcal{L}(D) = \left\{\alpha \neq 0 \text{ rational function} \middle| V_{P_i}(\alpha) \geq -1,\ i = 1, \ldots, n\right\} \cup \{0\}$

Construction of the code

- $k \geq 0$, $0 < s \leq n$ fixed integers.
- $\mathcal{W} = \mathcal{L}(kD)$ ambient space.
- Chosen $S \subset \mathcal{X}(\mathbb{F}_q)$ such that $|S| = s$ consider the divisor $D_S := \sum_{P \in S} P$, $\deg D_S = s$.

$$\boxed{\mathcal{H}_{k,s} := \{V = \mathcal{L}(kD_S) \subset \mathcal{W} \ : \ |S| = s\}}$$

Hansen's Costruction

- $D = \sum_{P \in \mathcal{X}_{\mathbb{F}_q}} P$, $\deg(D) = n := |\mathcal{X}_{\mathbb{F}_q}|$
- $\mathcal{L}(D) = \left\{\alpha \neq 0 \text{ rational function} \middle| V_{P_i}(\alpha) \geq -1,\ i = 1, \dots, n\right\} \cup \{0\}$

Construction of the code

- $k \geq 0$, $0 < s \leq n$ fixed integers.
- $\mathcal{W} = \mathcal{L}(kD)$ ambient space.
- Chosen $S \subset \mathcal{X}(\mathbb{F}_q)$ such that $|S| = s$ consider the divisor $D_S := \sum_{P \in S} P$, $\deg D_S = s$.

$$\boxed{\mathcal{H}_{k,s} := \{V = \mathcal{L}(kD_S) \subset \mathcal{W} \ : \ |S| = s\}}$$

- $nk > 2g - 2 \Rightarrow \dim_{\mathbb{F}_q} \mathcal{W} = kn + 1 - g$

Hansen's Costruction

- $D = \sum_{P \in \mathcal{X}_{\mathbb{F}_q}} P$, $\deg(D) = n := |\mathcal{X}_{\mathbb{F}_q}|$
- $\mathcal{L}(D) = \left\{ \alpha \neq 0 \text{ rational function} \middle| V_{P_i}(\alpha) \geq -1,\ i = 1, \ldots, n \right\} \cup \{0\}$

Construction of the code

- $k \geq 0$, $0 < s \leq n$ fixed integers.
- $\mathcal{W} = \mathcal{L}(kD)$ ambient space.
- Chosen $S \subset \mathcal{X}(\mathbb{F}_q)$ such that $|S| = s$ consider the divisor $D_S := \sum_{P \in S} P$, $\deg D_S = s$.

$$\boxed{\mathcal{H}_{k,s} := \{ V = \mathcal{L}(kD_S) \subset \mathcal{W} \ : \ |S| = s \}}$$

- $nk > 2g - 2 \Rightarrow \dim_{\mathbb{F}_q} \mathcal{W} = kn + 1 - g$
- $ks > 2g - 2 \Rightarrow \dim_{\mathbb{F}_q} V = ks + 1 - g$

Theorem (Hansen, 2015)

If $ks > 2g - 2$

$$\mathcal{H}_{k,s} \text{ is a } \left[\underbrace{kn+1-g}_{N}, \underbrace{ks+1-g}_{\ell}, \log_q \binom{n}{s}, D(\mathcal{H}_{k,s})\right] \text{-code}$$

$$D(\mathcal{H}_{k,s}) = \begin{cases} 2k, & s > 1; \\ 2(k+1-g), & s = 1. \end{cases}$$

Hansen

Family $\mathcal{A}_{k,s}$

$S \subset \mathcal{X}(\mathbb{F}_q), |S| = s$ $\Rightarrow$

S multiset
$Supp(S) \subset \mathcal{X}(\mathbb{F}_q)$
$|S| = s$

Hansen

Family $\mathcal{A}_{k,s}$

$$\boxed{S \subset \mathcal{X}(\mathbb{F}_q), |S| = s} \Rightarrow \boxed{\begin{array}{l} S \text{ multiset} \\ Supp(S) \subset \mathcal{X}(\mathbb{F}_q) \\ |S| = s \end{array}}$$

Construction of the code

- $k > 0$, $s > 0$ fixed integers.

Hansen

Family $\mathcal{A}_{k,s}$

$$S \subset \mathcal{X}(\mathbb{F}_q), |S| = s \Rightarrow \begin{array}{l} S \text{ multiset} \\ Supp(S) \subset \mathcal{X}(\mathbb{F}_q) \\ |S| = s \end{array}$$

Construction of the code

- $k > 0$, $s > 0$ fixed integers.
- $\mathcal{W} = \mathcal{L}(ksD)$ ambient space.

Hansen

Family $\mathcal{A}_{k,s}$

$S \subset \mathcal{X}(\mathbb{F}_q), |S| = s$ $\Rightarrow$ S multiset, $Supp(S) \subset \mathcal{X}(\mathbb{F}_q)$, $|S| = s$

Construction of the code

- $k > 0$, $s > 0$ fixed integers.
- $\mathcal{W} = \mathcal{L}(ksD)$ ambient space.

$$\mathcal{A}_{k,s} := \left\{ V = \mathcal{L}\left(k \sum_{P \in \mathcal{X}(\mathbb{F}_q)} m_P P\right) \subset \mathcal{W} \,\middle|\, \begin{array}{l} \sum_{P \in \mathcal{X}(\mathbb{F}_q)} m_P = s, \\ m_P \in \{0, \ldots s\} \end{array} \right\}$$

Hansen

Family $\mathcal{A}_{k,s}$

$S \subset \mathcal{X}(\mathbb{F}_q), |S| = s$ $\Rightarrow$ S multiset; $Supp(S) \subset \mathcal{X}(\mathbb{F}_q)$; $|S| = s$

Construction of the code

- $k > 0$, $s > 0$ fixed integers.
- $\mathcal{W} = \mathcal{L}(ksD)$ ambient space.

$$\mathcal{A}_{k,s} := \left\{ V = \mathcal{L}\left(k \sum_{P \in \mathcal{X}(\mathbb{F}_q)} m_P P \right) \subset \mathcal{W} \;\middle|\; \begin{array}{l} \sum_{P \in \mathcal{X}(\mathbb{F}_q)} m_P = s, \\ m_P \in \{0, \dots s\} \end{array} \right\}$$

- $nks > 2g - 2 \Rightarrow \dim_{\mathbb{F}_q} \mathcal{W} = nks + 1 - g$

Hansen

Family $\mathcal{A}_{k,s}$

$S \subset \mathcal{X}(\mathbb{F}_q), |S| = s$ $\Rightarrow$ S multiset, $Supp(S) \subset \mathcal{X}(\mathbb{F}_q)$, $|S| = s$

Construction of the code

- $k > 0$, $s > 0$ fixed integers.
- $\mathcal{W} = \mathcal{L}(ksD)$ ambient space.

$$\mathcal{A}_{k,s} := \left\{ V = \mathcal{L}\left(k \sum_{P \in \mathcal{X}(\mathbb{F}_q)} m_P P \right) \subset \mathcal{W} \;\middle|\; \begin{array}{l} \sum_{P \in \mathcal{X}(\mathbb{F}_q)} m_P = s, \\ m_P \in \{0, \dots s\} \end{array} \right\}$$

- $nks > 2g - 2 \Rightarrow \dim_{\mathbb{F}_q} \mathcal{W} = nks + 1 - g$
- $ks > 2g - 2 \Rightarrow \dim_{\mathbb{F}_q} V = ks + 1 - g$

Theorem

If $k > 2g - 2$

$$\mathcal{A}_{k,s} \text{ is a } \left[\underbrace{nks + 1 - g}_{N}, \underbrace{ks + 1 - g}_{\ell}, \log_q \binom{n+s-1}{s}, D(\mathcal{A}_{k,s})\right] \text{-code}$$

$$D(\mathcal{A}_{k,s}) = \begin{cases} 2k, & s > 1; \\ 2(k+1-g), & s = 1. \end{cases}$$

Family $\mathcal{A}_{k,s}$

Family $\mathcal{B}_{k,s,w}$

$\mathcal{A}_{k,s}$		$\mathcal{B}_{k,s,w}$
S multiset		S multiset
$Supp(S) \subset \mathcal{X}(\mathbb{F}_q)$	$\Rightarrow$	$Supp(S) \subset \mathcal{X}(\mathbb{F}_q)$
$\lvert S\rvert = s$, $m_P \in \{0, \dots, s\}$		$\lvert S\rvert = s$, $m_P \in \{0, \dots, w\}$

Family $\mathcal{A}_{k,s}$		Family $\mathcal{B}_{k,s,w}$
S multiset $Supp(S) \subset \mathcal{X}(\mathbb{F}_q)$ $\lvert S\rvert = s,\ m_P \in \{0, \dots, s\}$	$\Rightarrow$	S multiset $Supp(S) \subset \mathcal{X}(\mathbb{F}_q)$ $\lvert S\rvert = s,\ m_P \in \{0, \dots, w\}$

Construction of the code

- $k > 0,\ s > 0,\ 0 < w \leq s$ fixed integers.

Family $\mathcal{A}_{k,s}$		Family $\mathcal{B}_{k,s,w}$
S multiset $Supp(S) \subset \mathcal{X}(\mathbb{F}_q)$ $\|S\| = s,\ m_P \in \{0, \ldots, s\}$	$\Rightarrow$	S multiset $Supp(S) \subset \mathcal{X}(\mathbb{F}_q)$ $\|S\| = s,\ m_P \in \{0, \ldots, w\}$

Construction of the code

- $k > 0,\ s > 0,\ 0 < w \leq s$ fixed integers.
- $\mathcal{W} = \mathcal{L}(kwD)$ ambient space.

Family $\mathcal{A}_{k,s}$

Family $\mathcal{B}_{k,s,w}$

Family $\mathcal{A}_{k,s}$		Family $\mathcal{B}_{k,s,w}$
S multiset $Supp(S) \subset \mathcal{X}(\mathbb{F}_q)$ $\lvert S\rvert = s,\ m_P \in \{0, \dots, s\}$	$\Rightarrow$	S multiset $Supp(S) \subset \mathcal{X}(\mathbb{F}_q)$ $\lvert S\rvert = s,\ m_P \in \{0, \dots, w\}$

Construction of the code

- $k > 0,\ s > 0,\ 0 < w \leq s$ fixed integers.
- $\mathcal{W} = \mathcal{L}(kwD)$ ambient space.

$$\mathcal{B}_{k,s,w} := \left\{ V = \mathcal{L}\left(k \sum_{P \in \mathcal{X}(\mathbb{F}_q)} m_P P \right) \subset \mathcal{W} \,\middle|\, \begin{array}{l} \sum_{P \in \mathcal{X}(\mathbb{F}_q)} m_P = s, \\ m_P \in \{0, \dots w\} \end{array} \right\}$$

Family $\mathcal{A}_{k,s}$		Family $\mathcal{B}_{k,s,w}$
S multiset $Supp(S) \subset \mathcal{X}(\mathbb{F}_q)$ $\lvert S\rvert = s,\ m_P \in \{0,\dots,s\}$	$\Rightarrow$	S multiset $Supp(S) \subset \mathcal{X}(\mathbb{F}_q)$ $\lvert S\rvert = s,\ m_P \in \{0,\dots,w\}$

Construction of the code

- $k > 0,\ s > 0,\ 0 < w \leq s$ fixed integers.
- $\mathcal{W} = \mathcal{L}(kwD)$ ambient space.

$$\mathcal{B}_{k,s,w} := \left\{ V = \mathcal{L}\left(k \sum_{P \in \mathcal{X}(\mathbb{F}_q)} m_P P\right) \subset \mathcal{W} \;\middle|\; \begin{array}{l} \sum_{P \in \mathcal{X}(\mathbb{F}_q)} m_P = s, \\ m_P \in \{0, \dots w\} \end{array} \right\}$$

- $nkw > 2g - 2 \Rightarrow \dim_{\mathbb{F}_q} \mathcal{W} = nkw + 1 - g$

Family $\mathcal{A}_{k,s}$

Family $\mathcal{B}_{k,s,w}$

S multiset $Supp(S) \subset \mathcal{X}(\mathbb{F}_q)$ $\lvert S\rvert = s$, $m_P \in \{0, \ldots, s\}$	$\Rightarrow$	S multiset $Supp(S) \subset \mathcal{X}(\mathbb{F}_q)$ $\lvert S\rvert = s$, $m_P \in \{0, \ldots, w\}$

Construction of the code

- $k > 0$, $s > 0$, $0 < w \leq s$ fixed integers.
- $\mathcal{W} = \mathcal{L}(kwD)$ ambient space.

$$\mathcal{B}_{k,s,w} := \left\{ V = \mathcal{L}\left(k \sum_{P \in \mathcal{X}(\mathbb{F}_q)} m_P P \right) \subset \mathcal{W} \;\middle|\; \begin{array}{l} \sum_{P \in \mathcal{X}(\mathbb{F}_q)} m_P = s, \\ m_P \in \{0, \ldots w\} \end{array} \right\}$$

- $nkw > 2g - 2 \Rightarrow \dim_{\mathbb{F}_q} \mathcal{W} = nkw + 1 - g$
- $ks > 2g - 2 \Rightarrow \dim_{\mathbb{F}_q} V = ks + 1 - g$

Theorem

If $k > 2g - 2$ and $0 < w < s$

$$\boxed{\mathcal{B}_{k,s,w} \text{ is a } [\underbrace{nkw + 1 - g}_{N}, \underbrace{ks + 1 - g}_{\ell}, \log_q |\mathcal{B}_{k,s,w}|, 2k]\text{-code}}$$

$$|\mathcal{B}_{k,s,w}| = \sum_{i=0}^{t} (-1)^i \binom{n}{i} \binom{s - i(w+1) + n - 1}{n-1}$$

$$t = \min\left(n, \left\lfloor \frac{s}{b+1} \right\rfloor\right)$$

Family $\mathcal{B}_{k,s,w}$

Family $\mathcal{C}_{k,s,w}$

S multiset
$Supp(S) \subset \mathcal{X}(\mathbb{F}_q)$
$|S| = s,\ m_P \in \{0, \ldots, w\}$

$\Rightarrow$

S multiset
$Supp(S) \subset \mathcal{X}(\mathbb{F}_q)$
$\sum_{P \in \mathcal{X}(\mathbb{F}_q)} m_P = s$
$m_P \in \{\underbrace{s - w(n.1)}_{\overline{w}}, \ldots, w\}$

Family $\mathcal{B}_{k,s,w}$

Family $\mathcal{C}_{k,s,w}$

S multiset
$Supp(S) \subset \mathcal{X}(\mathbb{F}_q)$
$|S| = s,\ m_P \in \{0, \ldots, w\}$

$\Rightarrow$

S multiset
$Supp(S) \subset \mathcal{X}(\mathbb{F}_q)$
$\sum_{P \in \mathcal{X}(\mathbb{F}_q)} m_P = s$
$m_P \in \{\underbrace{s - w(n.1)}_{\overline{w}}, \ldots, w\}$

Construction of the code

- $k > 0,\ s > 0,\ 0 < w \leq s$ fixed integers.

Family $\mathcal{B}_{k,s,w}$		Family $\mathcal{C}_{k,s,w}$
S multiset $Supp(S) \subset \mathcal{X}(\mathbb{F}_q)$ $\|S\| = s,\ m_P \in \{0, \dots, w\}$	$\Rightarrow$	S multiset $Supp(S) \subset \mathcal{X}(\mathbb{F}_q)$ $\sum_{P \in \mathcal{X}(\mathbb{F}_q)} m_P = s$ $m_P \in \{\underbrace{s - w(n.1)}_{\overline{w}}, \dots, w\}$

Construction of the code

- $k > 0$, $s > 0$, $0 < w \leq s$ fixed integers.
- $\mathcal{W} = \mathcal{L}(kwD)$ ambient space.

Family $\mathcal{B}_{k,s,w}$

Family $\mathcal{C}_{k,s,w}$

S multiset
$Supp(S) \subset \mathcal{X}(\mathbb{F}_q)$
$|S| = s,\ m_P \in \{0, \ldots, w\}$

$\Rightarrow$

S multiset
$Supp(S) \subset \mathcal{X}(\mathbb{F}_q)$
$\sum_{P \in \mathcal{X}(\mathbb{F}_q)} m_P = s$
$m_P \in \{\underbrace{s - w(n.1)}_{\overline{w}}, \ldots, w\}$

Construction of the code

- $k > 0,\ s > 0,\ 0 < w \le s$ fixed integers.
- $\mathcal{W} = \mathcal{L}(kwD)$ ambient space.

$$\mathcal{C}_{k,s,w} := \left\{ V = \mathcal{L}\left(k \sum_{P \in \mathcal{X}(\mathbb{F}_q)} m_P P \right) \subset \mathcal{W} \;\middle|\; \begin{array}{l} \sum_{P \in \mathcal{X}(\mathbb{F}_q)} m_P = s, \\ m_P \in \{\overline{w}, \ldots w\} \end{array} \right\}$$

Theorem

If $k > 2g - 2$ and $0 < w < s$

$$\mathcal{C}_{k,s,w} \text{ is a } [\underbrace{nkw + 1 - g, ks + 1 - g}_{N}, \underbrace{ks + 1 - g}_{\ell}, \log_q |\mathcal{C}_{k,s,w}|]_q\text{-code}$$

$$|\mathcal{C}_{k,s,w}| = \sum_{i=0}^{t} (-1)^i \binom{n}{i} \binom{(nw - s + 1)(n - i - 1)}{n - 1}$$

$$t = \left\lfloor \frac{(nw - s)(n - 1)}{nw - s + 1} \right\rfloor$$

Normalized weight, rate, and normalized minimum distance

	Normalized weight	Rate	Normalized minimum distance
$\mathcal{H}_{k,s}$	$\frac{ks+1-g}{nk+1-g}$	$\frac{\log_q \binom{n}{s}}{(nk+1-g)(ks+1-g)}$	$\frac{1}{s+\frac{1-g}{k}}$
$\mathcal{A}_{k,s}$	$\frac{ks+1-g}{nks+1-g}$	$\frac{\log_q \binom{n+s-1}{s}}{(nks+1-g)(ks+1-g)}$	$\frac{1}{s+\frac{1-g}{k}}$
$\mathcal{B}_{k,s,w}$	$\frac{ks+1-g}{nkw+1-g}$	$\frac{\log_q \lvert\mathcal{B}_{k,s,w}\rvert}{(nkw+1-g)(ks+1-g)}$	$\frac{1}{s+\frac{1-g}{k}}$
$\mathcal{C}_{k,s,w}$	$\frac{ks+1-g}{nkw+1-g}$	$\frac{\log_q \lvert\mathcal{C}_{k,s,w}\rvert}{(nkw+1-g)(ks+1-g)}$	$\frac{1}{s+\frac{1-g}{k}}$

- In the new constructions s can be larger than n.

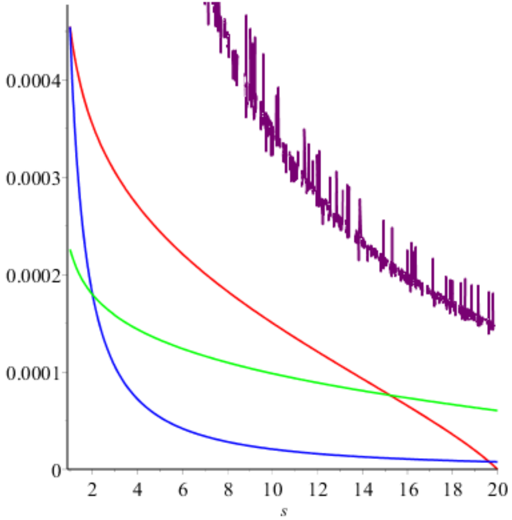
- In the new constructions s can be larger than n.
- We do not mind if n is small, so we are not constricted to choose only curves with many $\mathbb{F}_q$-rational points.

Rates of $\mathcal{H}_{k,s}$, $\mathcal{A}_{k,s}$, $\mathcal{B}_{k,s,w}$, $\mathcal{C}_{k,s,w}$ for $q = 16,\ 8 \leq n \leq 14,\ 1 \leq s < n,\ w = 3,\ k = 5$

(n,s)	$\mathcal{H}_{k,s}$	$\mathcal{A}_{k,s}$	$\mathcal{B}_{k,s,w}$	$\mathcal{C}_{k,s,w}$	(n,s)	$\mathcal{H}_{k,s}$	$\mathcal{A}_{k,s}$	$\mathcal{B}_{k,s,w}$	$\mathcal{C}_{k,s,w}$
(8, 1)	0.003750	0.003750	0.001250	0.008732	(12, 2)	0.002518	0.001309	0.000873	0.004617
(8, 2)	0.003005	0.001616	0.001077	0.004286	(12, 3)	0.002161	0.000788	0.000788	0.003040
(8, 3)	0.002420	0.000959	0.000959	0.002802	(12, 4)	0.001865	0.000542	0.000722	0.002251
(8, 4)	0.001915	0.000654	0.000868	0.002058	(12, 5)	0.001605	0.000403	0.000669	0.001778
(8, 5)	0.001452	0.000481	0.000792	0.001611	(12, 6)	0.001368	0.000315	0.000624	0.001461
(8, 6)	0.001002	0.000373	0.000728	0.001311	(12, 7)	0.001146	0.000254	0.000585	0.001234
(9, 1)	0.003522	0.003522	0.001174	0.008931	(12, 8)	0.000932	0.000211	0.000551	0.001064
(9, 2)	0.002872	0.001526	0.001017	0.004394	(12, 9)	0.000720	0.000179	0.000519	0.000931
(9, 3)	0.002368	0.000909	0.000909	0.002880	(13, 1)	0.002846	0.002846	0.000949	0.009440
(9, 4)	0.001938	0.000622	0.000826	0.002121	(13, 2)	0.002417	0.001251	0.000834	0.004670
(9, 5)	0.001551	0.000459	0.000758	0.001665	(13, 3)	0.002092	0.000755	0.000755	0.003079
(9, 6)	0.001184	0.000357	0.000700	0.001360	(13, 4)	0.001823	0.000521	0.000694	0.002282
(10, 1)	0.003322	0.003322	0.001107	0.009093	(13, 5)	0.001589	0.000388	0.000644	0.001804
(10, 2)	0.002746	0.001445	0.000964	0.004482	(13, 6)	0.001378	0.000303	0.000602	0.001485
(10, 3)	0.002302	0.000865	0.000865	0.002943	(13, 7)	0.001181	0.000245	0.000566	0.001256
(10, 4)	0.001929	0.000593	0.000788	0.002173	(13, 8)	0.000993	0.000204	0.000533	0.001085
(10, 5)	0.001595	0.000439	0.000726	0.001710	(13, 9)	0.000810	0.000173	0.000505	0.000950
(10, 6)	0.001286	0.000341	0.000673	0.001400	(13, 10)	0.000628	0.000148	0.000478	0.000843
(10, 7)	0.000987	0.000275	0.000627	0.001178	(14, 1)	0.002720	0.002720	0.000907	0.009486
(10, 8)	0.000686	0.000228	0.000586	0.001011	(14, 2)	0.002324	0.001199	0.000799	0.004705
(11, 1)	0.003145	0.003145	0.001048	0.009229	(14, 3)	0.002026	0.000725	0.000725	0.003102
(11, 2)	0.002628	0.001374	0.000916	0.004555	(14, 4)	0.001780	0.000501	0.000667	0.002307
(11, 3)	0.002232	0.000824	0.000824	0.002996	(14, 5)	0.001567	0.000373	0.000621	0.001827
(11, 4)	0.001901	0.000566	0.000754	0.002215	(14, 6)	0.001375	0.000292	0.000581	0.001511
(11, 5)	0.001609	0.000420	0.000697	0.001746	(14, 7)	0.001198	0.000237	0.000547	0.001252
(11, 6)	0.001341	0.000327	0.000648	0.001433	(14, 8)	0.001031	0.000197	0.000517	0.001106
(11, 7)	0.001087	0.000264	0.000606	0.001209	(14, 9)	0.000870	0.000167	0.000490	0.000974
(11, 8)	0.000837	0.000219	0.000568	0.001040	(14, 10)	0.000712	0.000144	0.000466	0.000865
(12, 1)	0.002987	0.002987	0.000996	0.009343	(14, 11)	0.000552	0.000125	0.000443	0.000768

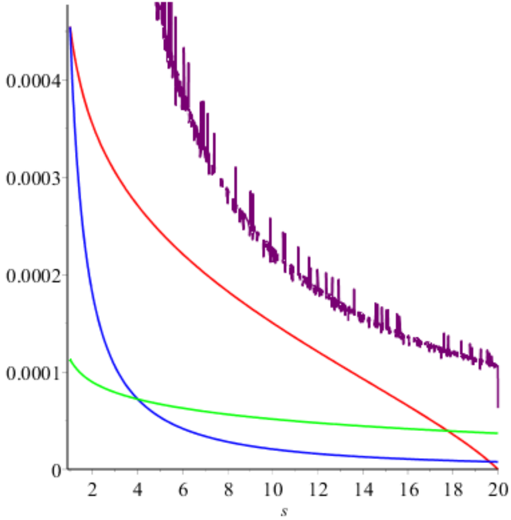
$\mathcal{H}_{k,s}$ $\mathcal{A}_{k,s}$ $\mathcal{B}_{k,s,w}$ $\mathcal{C}_{k,s,w}$

q=64 g=3 k=10 n=20 w=2



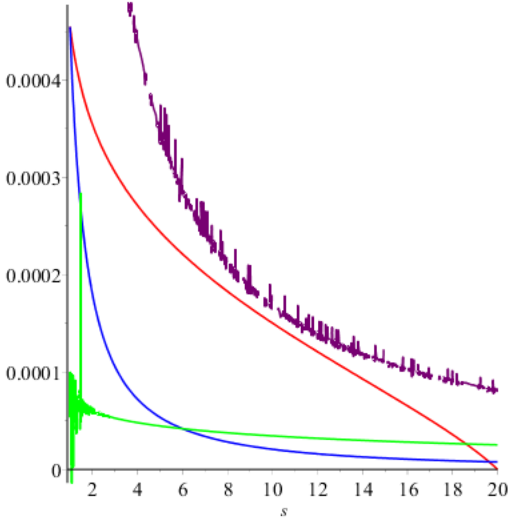
$\mathcal{H}_{k,s}$ $\mathcal{A}_{k,s}$ $\mathcal{B}_{k,s,w}$ $\mathcal{C}_{k,s,w}$

q=64 g=3 k=10 n=20 w=4



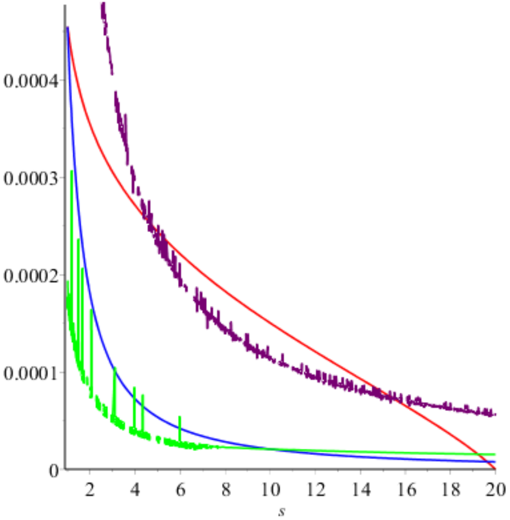
$\mathcal{H}_{k,s}$ $\mathcal{A}_{k,s}$ $\mathcal{B}_{k,s,w}$ $\mathcal{C}_{k,s,w}$

q=64 g=3 k=10 n=20 w=6



$\mathcal{H}_{k,s}$ $\mathcal{A}_{k,s}$ $\mathcal{B}_{k,s,w}$ $\mathcal{C}_{k,s,w}$

q=64 g=3 k=10 n=20 w=10



THANK YOU FOR YOUR ATTENTION