n applications of the footprint bound ($n \geq 3$)

Olav Geil
Aalborg University
Denmark

Universität Basel, 2012

PART 1: THE TOOLS

ILLUSTRATED WITH EXAMPLES OF POLYNOMIAL CODES

The tool

$\vec{X} = (X_1, \ldots, X_m)$
$F_1(\vec{X}), \ldots, F_s(\vec{X}) \in \mathbb{F}[\vec{X}]$

- Question: How many zeros do $F_1, \ldots, F_s$ have in common?
- Question: $I = \langle F_1(\vec{X}), \ldots, F_s(\vec{X}) \rangle$. How large is $\mathbb{V}_{\mathbb{F}}(I)$?

Tools:

- Footprint bound.
- Schwartz-Zippel bound (Ore-bound).

The tool

$\vec{X} = (X_1, \ldots, X_m)$
$F_1(\vec{X}), \ldots, F_s(\vec{X}) \in \mathbb{F}[\vec{X}]$

- Question: How many zeros do $F_1, \ldots, F_s$ have in common?
- Question: $I = \langle F_1(\vec{X}), \ldots, F_s(\vec{X}) \rangle$. How large is $\mathbb{V}_{\mathbb{F}}(I)$?

Tools:

- Footprint bound.
- Schwartz-Zippel bound (Ore-bound).

Monomial orderings

A monomial ordering $\prec$ is a total ordering on $\{\vec{X}^{\vec{\alpha}} | \vec{\alpha} \in \mathbb{N}_0^m\}$ such that

- $\vec{X}^{\vec{\alpha}} \prec \vec{X}^{\vec{\beta}} \Rightarrow \vec{X}^{\vec{\alpha}+\vec{\gamma}} \prec \vec{X}^{\vec{\beta}+\vec{\gamma}}$.
- Every subset has a unique smallest element.

Examples: $\prec_{lex}$, $\prec_{glex}$, $\prec_{grlex}$, $\prec_{wdeglex}$.

$X^2Y^3 \prec_{glex} XY^5$ because $5 < 6$.
$X^2Y^3 \prec_{glex} X^3Y^2$ because $5 = 5$ and $2 < 3$.

Monomial orderings

A monomial ordering $\prec$ is a total ordering on $\{\vec{X}^{\vec{\alpha}} | \vec{\alpha} \in \mathbb{N}_0^m\}$ such that

- $\vec{X}^{\vec{\alpha}} \prec \vec{X}^{\vec{\beta}} \Rightarrow \vec{X}^{\vec{\alpha}+\vec{\gamma}} \prec \vec{X}^{\vec{\beta}+\vec{\gamma}}$.
- Every subset has a unique smallest element.

Examples: $\prec_{lex}$, $\prec_{glex}$, $\prec_{grlex}$, $\prec_{wdeglex}$.

$X^2Y^3 \prec_{glex} XY^5$ because $5 < 6$.
$X^2Y^3 \prec_{glex} X^3Y^2$ because $5 = 5$ and $2 < 3$.

Footprint

$I \subseteq \mathbb{F}[\vec{X}]$.

$$\Delta_{\prec}(I) = \{\vec{X}^{\vec{\alpha}} \mid \vec{X}^{\vec{\alpha}} \text{ is not leading monomial of any polynomial in } I\}$$

If $I = \langle F(\vec{X}) \rangle$ then
$\Delta_{\prec}(I) = \{\vec{X}^{\vec{\alpha}} \mid \vec{X}^{\vec{\alpha}} \text{ does not divide } \mathrm{lm}(F)\}$.

More polynomials = analyzis more involved.

Footprint

$I \subseteq \mathbb{F}[\vec{X}]$.

$$\Delta_{\prec}(I) \;=\; \{\vec{X}^{\vec{\alpha}} \mid \vec{X}^{\vec{\alpha}} \text{ is not leading monomial of any polynomial in } I\}$$

If $I = \langle F(\vec{X}) \rangle$ then
$\Delta_{\prec}(I) = \{\vec{X}^{\vec{\alpha}} \mid \vec{X}^{\vec{\alpha}} \text{ does not divide } \mathrm{lm}(F)\}$.

More polynomials = analyzis more involved.

Footprint

$I \subseteq \mathbb{F}[\vec{X}]$.

$$\Delta_{\prec}(I) = \{\vec{X}^{\vec{\alpha}} \mid \vec{X}^{\vec{\alpha}} \text{ is not leading monomial of any polynomial in } I\}$$

If $I = \langle F(\vec{X}) \rangle$ then
$\Delta_{\prec}(I) = \{\vec{X}^{\vec{\alpha}} \mid \vec{X}^{\vec{\alpha}} \text{ does not divide } \mathrm{lm}(F)\}$.

More polynomials = analyzis more involved.

The main tools

Theorem:
$\{M + I \mid M \in \Delta_{\prec}(I)\}$ constitutes a basis for $\mathbb{F}[\vec{X}]/I$ as a vectorspace.

Corollary:
$|\mathbb{V}_{\mathbb{F}}(I)| \leq |\Delta_{\prec}(I)|$ (whenever latter is finite).

Proof: Consider $\{P_1, \ldots, P_n\} \subseteq \mathbb{V}_{\mathbb{F}}(I)$ and define $\mathrm{ev} : \mathbb{F}[\vec{X}]/I \rightarrow \mathbb{F}^n$ by $\mathrm{ev}(F + I) = (F(P_1), \ldots, F(P_n))$. Lagrange-polynomial type of argument proves that surjective.

The main tools

Theorem:
$\{M + I \mid M \in \Delta_{\prec}(I)\}$ constitutes a basis for $\mathbb{F}[\vec{X}]/I$ as a vectorspace.

Corollary:
$|\mathbb{V}_{\mathbb{F}}(I)| \leq |\Delta_{\prec}(I)|$ (whenever latter is finite).

Proof: Consider $\{P_1, \ldots, P_n\} \subseteq \mathbb{V}_{\mathbb{F}}(I)$ and define
$\mathrm{ev} : \mathbb{F}[\vec{X}]/I \rightarrow \mathbb{F}^n$ by $\mathrm{ev}(F + I) = (F(P_1), \ldots, F(P_n))$.
Lagrange-polynomial type of argument proves that surjective.

An importan special case

<u>Corollary:</u> Let $F(\vec{X}) \in \mathbb{F}_q[\vec{X}]$, $\mathrm{Im}(F) = X_1^{i_1} \cdots X_m^{i_m}$. Then F has at most $q^m - \prod_{s=1}^{m}(q - i_s)$ zeros.

Proof:

$$\begin{aligned} \text{number of zeros} &\leq |\Delta_{\prec}(\langle F(\vec{X})\rangle + \langle X_1^q - X_1, \ldots, X_m^q - X_m\rangle)| \\ &\leq |\{\vec{X}^{\vec{\alpha}} | 0 \leq \alpha_1 < q, \ldots, 0 \leq \alpha_m < q, \vec{X}^{\vec{i}} \not| \vec{X}^{\vec{\alpha}}\}|. \end{aligned}$$

Generalizes in a straightforward manner to any finite point ensemble $S_1 \times \cdots \times S_m$.

RM codes and Massey-Costello-Justesen codes

8	7	6	5	4	3	2	1
16	14	12	10	8	6	4	2
24	21	18	15	12	9	6	3
32	28	24	20	16	12	8	4
40	35	30	25	20	15	10	5
48	42	36	30	24	18	12	6
56	49	42	35	28	21	14	7
64	56	48	40	32	24	16	8

$\mathrm{RM}_8(5,2) = \{\mathrm{ev}(F) \mid \deg F \leq 5\}$ is $[64,21,24]$

$\mathrm{Span}_{\mathbb{F}_8}\left(\{\mathrm{ev}(\vec{X}^{\vec{\alpha}}) \mid \deg \vec{X}^{\vec{\alpha}} \leq 5\} \cup \{X^4Y^2, X^2Y^4\}\right)$ is $[64,23,24]$

$\mathrm{RM}_8(9,2) = \{\mathrm{ev}(F) \mid \deg F \leq 9\}$ is $[64,49,6]$

$$\mathrm{Span}_{\mathbb{F}_8}\Big(\{\mathrm{ev}(\vec{X}^{\vec{\alpha}}) \mid \deg \vec{X}^{\vec{\alpha}} \leq 9\}$$

$$\cup\{X^4Y^6, X^5Y^5, X^5Y^6, X^6Y^4, X^6Y^5\}\Big) \text{ is } [64,54,6]$$

RM codes and Massey-Costello-Justesen codes

8	7	6	5	4	3	2	1
16	14	12	10	8	6	4	2
24	21	18	15	12	9	6	3
32	28	24	20	16	12	8	4
40	35	30	25	20	15	10	5
48	42	36	30	24	18	12	6
56	49	42	35	28	21	14	7
64	56	48	40	32	24	16	8

$\mathrm{RM}_8(5,2) = \{\mathrm{ev}(F) \mid \deg F \leq 5\}$ is $[64, 21, 24]$

$\mathrm{Span}_{\mathbb{F}_8}\left(\{\mathrm{ev}(\vec{X}^{\vec{\alpha}}) \mid \deg \vec{X}^{\vec{\alpha}} \leq 5\} \cup \{X^4Y^2, X^2Y^4\}\right)$ is $[64, 23, 24]$

$\mathrm{RM}_8(9,2) = \{\mathrm{ev}(F) \mid \deg F \leq 9\}$ is $[64, 49, 6]$

$\mathrm{Span}_{\mathbb{F}_8}\Big(\{\mathrm{ev}(\vec{X}^{\vec{\alpha}}) \mid \deg \vec{X}^{\vec{\alpha}} \leq 9\}$

$\cup\{X^4Y^6, X^5Y^5, X^5Y^6, X^6Y^4, X^6Y^5\}\Big)$ is $[64, 54, 6]$

RM codes and Massey-Costello-Justesen codes

8	7	6	5	4	3	2	1
16	14	12	10	8	6	4	2
24	21	18	15	12	9	6	3
32	28	24	20	16	12	8	4
40	35	30	25	20	15	10	5
48	42	36	30	24	18	12	6
56	49	42	35	28	21	14	7
64	56	48	40	32	24	16	8

$\mathrm{RM}_8(5,2) = \{\mathrm{ev}(F) \mid \deg F \leq 5\}$ is $[64,21,24]$

$\mathrm{Span}_{\mathbb{F}_8}\left(\{\mathrm{ev}(\vec{X}^{\vec{\alpha}}) \mid \deg \vec{X}^{\vec{\alpha}} \leq 5\} \cup \{X^4Y^2, X^2Y^4\}\right)$ is $[64,23,24]$

$\mathrm{RM}_8(9,2) = \{\mathrm{ev}(F) \mid \deg F \leq 9\}$ is $[64,49,6]$

$\mathrm{Span}_{\mathbb{F}_8}\Big(\{\mathrm{ev}(\vec{X}^{\vec{\alpha}}) \mid \deg \vec{X}^{\vec{\alpha}} \leq 9\}$

$\cup\{X^4Y^6, X^5Y^5, X^5Y^6, X^6Y^4, X^6Y^5\}\Big)$ is $[64,54,6]$

RM codes and Massey-Costello-Justesen codes

8	7	6	5	4	3	2	1
16	14	12	10	8	6	4	2
24	21	18	15	12	9	6	3
32	28	24	20	16	12	8	4
40	35	30	25	20	15	10	5
48	42	36	30	24	18	12	6
56	49	42	35	28	21	14	7
64	56	48	40	32	24	16	8

$\mathrm{RM}_8(5,2) = \{\mathrm{ev}(F) \mid \deg F \leq 5\}$ is $[64,21,24]$

$\mathrm{Span}_{\mathbb{F}_8}\left(\{\mathrm{ev}(\vec{X}^{\vec{\alpha}}) \mid \deg \vec{X}^{\vec{\alpha}} \leq 5\} \cup \{X^4Y^2, X^2Y^4\}\right)$ is $[64,23,24]$

$\mathrm{RM}_8(9,2) = \{\mathrm{ev}(F) \mid \deg F \leq 9\}$ is $[64,49,6]$

$$\mathrm{Span}_{\mathbb{F}_8}\Big(\{\mathrm{ev}(\vec{X}^{\vec{\alpha}}) \mid \deg \vec{X}^{\vec{\alpha}} \leq 9\}$$

$$\cup\{X^4Y^6, X^5Y^5, X^5Y^6, X^6Y^4, X^6Y^5\}\Big) \text{ is } [64,54,6]$$

RM codes and Massey-Costello-Justesen codes

8	7	6	5	4	3	2	1
16	14	12	10	8	6	4	2
24	21	18	15	12	9	6	3
32	28	24	20	16	12	8	4
40	35	30	25	20	15	10	5
48	42	36	30	24	18	12	6
56	49	42	35	28	21	14	7
64	56	48	40	32	24	16	8

$\mathrm{RM}_8(5,2) = \{\mathrm{ev}(F) \mid \deg F \leq 5\}$ is $[64, 21, 24]$

$\mathrm{Span}_{\mathbb{F}_8}\left(\{\mathrm{ev}(\vec{X}^{\vec{\alpha}}) \mid \deg \vec{X}^{\vec{\alpha}} \leq 5\} \cup \{X^4Y^2, X^2Y^4\}\right)$ is $[64, 23, 24]$

$\mathrm{RM}_8(9,2) = \{\mathrm{ev}(F) \mid \deg F \leq 9\}$ is $[64, 49, 6]$

$$\mathrm{Span}_{\mathbb{F}_8}\Big(\{\mathrm{ev}(\vec{X}^{\vec{\alpha}}) \mid \deg \vec{X}^{\vec{\alpha}} \leq 9\}$$

$$\cup\{X^4Y^6, X^5Y^5, X^5Y^6, X^6Y^4, X^6Y^5\}\Big) \text{ is } [64, 54, 6]$$

Weighted Reed-Muller codes

Point set $S_1 \times \cdots \times S_m$, $S_i \subseteq \mathbb{F}_q$.

$F_1(\vec{X}) = \prod_{x \in S_1}(X_1 - x), \ldots, F_m(\vec{X}) = \prod_{x \in S_m}(X_m - x)$.

$I_q = \langle F_1(\vec{X}), \ldots, F_m(\vec{X}) \rangle$.

$\Delta(I_q) = \{X_1^{i_1} \cdots X_m^{i_m} \mid 0 \leq i_1 < |S_1|, \ldots, 0 \leq i_m < |S_m|\}$.

$$\begin{aligned} & \mathrm{RM}(S_1, \ldots, S_m, u, w_1, \ldots w_m) \\ = \; & \mathrm{Span}_{\mathbb{F}_q}\{\mathrm{ev}(X_1^{i_1} \cdots X_m^{i_m}) \mid i_1 w_1 + \cdots + i_m w_m \leq u, \\ & \qquad 0 \leq i_1 < |S_1|, \ldots, 0 \leq i_m < |S_m|\} \end{aligned}$$

Weighted Reed-Muller codes

Point set $S_1 \times \cdots \times S_m$, $S_i \subseteq \mathbb{F}_q$.

$F_1(\vec{X}) = \prod_{x \in S_1}(X_1 - x), \ldots, F_m(\vec{X}) = \prod_{x \in S_m}(X_m - x)$.

$I_q = \langle F_1(\vec{X}), \ldots, F_m(\vec{X}) \rangle$.

$\Delta(I_q) = \{X_1^{i_1} \cdots X_m^{i_m} \mid 0 \leq i_1 < |S_1|, \ldots, 0 \leq i_m < |S_m|\}$.

$$\begin{aligned} & \mathrm{RM}(S_1, \ldots, S_m, u, w_1, \ldots w_m) \\ = \quad & \mathrm{Span}_{\mathbb{F}_q}\{\mathrm{ev}(X_1^{i_1} \cdots X_m^{i_m}) \mid i_1 w_1 + \cdots + i_m w_m \leq u, \\ & \qquad 0 \leq i_1 < |S_1|, \ldots, 0 \leq i_m < |S_m|\} \end{aligned}$$

Weighted Reed-Muller codes

Point set $S_1 \times \cdots \times S_m$, $S_i \subseteq \mathbb{F}_q$.

$F_1(\vec{X}) = \prod_{x \in S_1}(X_1 - x), \ldots, F_m(\vec{X}) = \prod_{x \in S_m}(X_m - x)$.

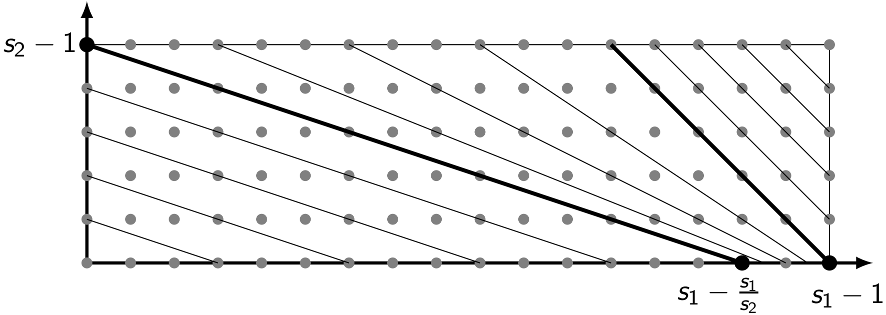
$I_q = \langle F_1(\vec{X}), \ldots, F_m(\vec{X}) \rangle$.

$\Delta(I_q) = \{X_1^{i_1} \cdots X_m^{i_m} \mid 0 \leq i_1 < |S_1|, \ldots, 0 \leq i_m < |S_m|\}$.

$$\begin{aligned} & \mathrm{RM}(S_1, \ldots, S_m, u, w_1, \ldots w_m) \\ = \ & \mathrm{Span}_{\mathbb{F}_q}\{\mathrm{ev}(X_1^{i_1} \cdots X_m^{i_m}) \mid i_1 w_1 + \cdots + i_m w_m \leq u, \\ & \qquad 0 \leq i_1 < |S_1|, \ldots, 0 \leq i_m < |S_m|\} \end{aligned}$$

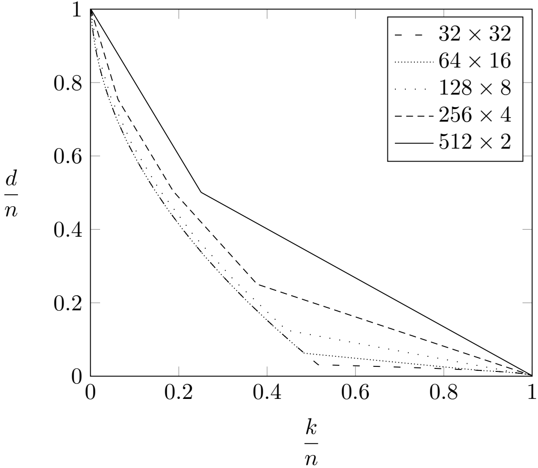
Optimal choice of weights

The case $|S_1| = 18$, $|S_2| = 6$:



Region I, region II, region III.

Optimally weighted Reed-Muller codes



Some improvement in region I.

Substantial improvement in region II. Region II increases.

A combinatorial result

Proposition: Consider $S \times \cdots \times S$ (finite) and $F(\vec{X}) \in \mathbb{F}[\vec{X}]$. Let $\mathrm{lm}(F) = \vec{X}^{\vec{\alpha}}$ with respect to LEXICOGRAPHIC ordering. The number of zeros is at most

$$|S|^m - \prod_{t=1}^{m}(|S| - \alpha_t).$$

Proof: (by induction after m).
Reformulate result as "number of non-zeros is at least..."
Clearly true for $m = 1$.
Induction step: Write

$$F(\vec{X}) = F_0(X_1, \ldots, X_{m-1}) + F_1(X_1, \ldots, X_{m-1})X_m + \cdots + F_{\alpha_m}(X_1, \ldots, X_{m-1})X_m^{\alpha_m}.$$

A combinatorial result

Proposition: Consider $S \times \cdots \times S$ (finite) and $F(\vec{X}) \in \mathbb{F}[\vec{X}]$. Let $\mathrm{lm}(F) = \vec{X}^{\vec{\alpha}}$ with respect to LEXICOGRAPHIC ordering. The number of zeros is at most

$$|S|^m - \prod_{t=1}^{m} (|S| - \alpha_t).$$

Proof: (by induction after m).
Reformulate result as "number of non-zeros is at least..."
Clearly true for $m = 1$.
Induction step: Write

$$\begin{aligned} F(\vec{X}) \ = \ & F_0(X_1, \ldots, X_{m-1}) + F_1(X_1, \ldots, X_{m-1}) X_m + \\ & \cdots + F_{\alpha_m}(X_1, \ldots, X_{m-1}) X_m^{\alpha_m}. \end{aligned}$$

Schwartz-Zippel bound (Ore bound)

Corollary:

Consider finite point ensemble $S \times \cdots \times S$ and $F(\vec{X})$ of degree $t < |S|$. Then F has at most $t|S|^{m-1}$ zeros.

Proof:

$$\begin{aligned} & \max\{|S|^m - \prod_{s=1}^{m}(|S| - \alpha_s) \mid \sum_{s=1}^{m} \alpha_s \leq t\} \\ = \;& |S|^m - |S|^{m-1}(|S| - t) \\ = \;& t|S|^{m-1}. \end{aligned}$$

(worst case is on the border).

Second smallest weight of RM codes

Theorem:
If I is radical and $\mathbb{F}$ is algebraically closed then $|\mathbb{V}_{\mathbb{F}}(I)| = |\Delta_{\prec}(I)|$ (whenever latter is finite).

Fact: $I_q = \langle F_1(\vec{X}), \ldots, F_s(\vec{X}), X_1^q - X_1, \ldots, X_m^q - X_m \rangle$ is radical.

To calculate exact footprint requires Buchberger's algorithm.

Gives closed formula descriptions of second smallest weight of any $\mathrm{RM}_q(s, 2)$.
Translates into closed formula descriptions for any $\mathrm{RM}_q(s, m)$.
Establishing the weights in general is a very hard problem.

Second smallest weight of RM codes

Theorem:
If I is radical and $\mathbb{F}$ is algebraically closed then $|\mathbb{V}_{\mathbb{F}}(I)| = |\Delta_{\prec}(I)|$ (whenever latter is finite).

Fact: $I_q = \langle F_1(\vec{X}), \ldots, F_s(\vec{X}), X_1^q - X_1, \ldots, X_m^q - X_m \rangle$ is radical.

To calculate exact footprint requires Buchberger's algorithm.

Gives closed formula descriptions of second smallest weight of any $\mathrm{RM}_q(s, 2)$.
Translates into closed formula descriptions for any $\mathrm{RM}_q(s, m)$.
Establishing the weights in general is a very hard problem.

Second smallest weight of RM codes

Theorem:
If I is radical and $\mathbb{F}$ is algebraically closed then $|\mathbb{V}_{\mathbb{F}}(I)| = |\Delta_{\prec}(I)|$ (whenever latter is finite).

Fact: $I_q = \langle F_1(\vec{X}), \ldots, F_s(\vec{X}), X_1^q - X_1, \ldots, X_m^q - X_m \rangle$ is radical.

To calculate exact footprint requires Buchberger's algorithm.

Gives closed formula descriptions of second smallest weight of any $\mathrm{RM}_q(s, 2)$.
Translates into closed formula descriptions for any $\mathrm{RM}_q(s, m)$.
Establishing the weights in general is a very hard problem.

Second smallest weight of RM codes

Theorem:
If I is radical and $\mathbb{F}$ is algebraically closed then $|\mathbb{V}_{\mathbb{F}}(I)| = |\Delta_{\prec}(I)|$ (whenever latter is finite).

Fact: $I_q = \langle F_1(\vec{X}, \ldots, F_s(\vec{X}), X_1^q - X_1, \ldots, X_m^q - X_m \rangle$ is radical.

To calculate exact footprint requires Buchberger's algorithm.

Gives closed formula descriptions of second smallest weight of any $\mathrm{RM}_q(s, 2)$.
Translates into closed formula descriptions for any $\mathrm{RM}_q(s, m)$.
Establishing the weights in general is a very hard problem.

PART 2: ONE-POINT ALGEBRAIC GEOMETRIC CODES

One-point algebraic geometric codes

$P_1, \ldots, P_n, Q$ rational places of function field over $\mathbb{F}_q$.

To construct $C_{\mathcal{L}}(D = P_1 + \cdots + P_n, vQ)$ we need basis for: $\cup_{s=0}^{v} \mathcal{L}(sQ) \subseteq \bigcup_{s=0}^{\infty} \mathcal{L}(sQ)$.

Everything, can be translated into affine variety description:

$\cup_{s=0}^{\infty} \mathcal{L}(sQ) = \mathbb{F}_q[X_1, \ldots, X_m]/I \quad \{P_1, \ldots, P_n\} \subseteq \mathbb{V}_{\mathbb{F}_q}(I)$.

Affine variety description includes determination of minimum distance via footprint bound.

One-point algebraic geometric codes

$P_1, \ldots, P_n, Q$ rational places of function field over $\mathbb{F}_q$.

To construct $C_{\mathcal{L}}(D = P_1 + \cdots + P_n, vQ)$ we need basis for: $\cup_{s=0}^{v} \mathcal{L}(sQ) \subseteq \bigcup_{s=0}^{\infty} \mathcal{L}(sQ)$.

Everything, can be translated into affine variety description:

$$\cup_{s=0}^{\infty} \mathcal{L}(sQ) = \mathbb{F}_q[X_1, \ldots, X_m]/I \qquad \{P_1, \ldots, P_n\} \subseteq \mathbb{V}_{\mathbb{F}_q}(I).$$

Affine variety description includes determination of minimum distance via footprint bound.

Weights versus valuation

Weierstrass semigroup:
$H(Q) = -\nu_Q\big(\cup_{s=0}^{\infty} \mathcal{L}(sQ)\big) = \langle w_1, \ldots , w_m\rangle$.

Definition: Given weights $w_1, \ldots , w_m$ define
$w(\vec{X}^{\vec{\alpha}}) = \vec{\alpha} \cdot (w_1, \ldots , w_m)$. Define $\prec_w$ by $\vec{X}^{\vec{\alpha}} \prec_w \vec{X}^{\vec{\beta}}$ if

- $w(\vec{X}^{\vec{\alpha}}) < w(\vec{X}^{\vec{\beta}})$
- or $w(\vec{X}^{\vec{\alpha}}) = w(\vec{X}^{\vec{\beta}})$ but $\vec{X}^{\vec{\alpha}} \prec_{\mathcal{M}} \vec{X}^{\vec{\beta}}$

($\prec_{\mathcal{M}}$ can be anything, for instance $\prec_{lex}$)

Example: $w(X) = q, w(Y) = q + 1$, $\prec_{\mathcal{M}}=\prec_{lex}$ with $X \prec_{lex} Y$.
$F(X, Y) = X^{q+1} - Y^q - Y$, $w(X^{q+1}) = w(Y^q) = q(q + 1)$ and
$\mathrm{Im}(F) = Y^q$.

Weights versus valuation

Weierstrass semigroup:
$H(Q) = -\nu_Q\big(\cup_{s=0}^{\infty} \mathcal{L}(sQ)\big) = \langle w_1, \ldots, w_m \rangle$.

Definition: Given weights $w_1, \ldots, w_m$ define $w(\vec{X}^{\vec{\alpha}}) = \vec{\alpha} \cdot (w_1, \ldots, w_m)$. Define $\prec_w$ by $\vec{X}^{\vec{\alpha}} \prec_w \vec{X}^{\vec{\beta}}$ if

- $w(\vec{X}^{\vec{\alpha}}) < w(\vec{X}^{\vec{\beta}})$
- or $w(\vec{X}^{\vec{\alpha}}) = w(\vec{X}^{\vec{\beta}})$ but $\vec{X}^{\vec{\alpha}} \prec_{\mathcal{M}} \vec{X}^{\vec{\beta}}$

($\prec_{\mathcal{M}}$ can be anything, for instance $\prec_{lex}$)

Example: $w(X) = q, w(Y) = q+1$, $\prec_{\mathcal{M}} = \prec_{lex}$ with $X \prec_{lex} Y$.
$F(X, Y) = X^{q+1} - Y^q - Y$, $w(X^{q+1}) = w(Y^q) = q(q+1)$ and $\mathrm{Im}(F) = Y^q$.

Order domain conditions

$I = \langle F_1(\vec{X}), \ldots, F_s(\vec{X}) \rangle \subseteq \mathbb{F}[\vec{X}]$ and $w_1, \ldots, w_m$ satisfy ODC if:

1. $\{F_1, \ldots, F_s\}$ is a Gröbner basis w.r.t. $\prec_w$.
2. F_i, $i = 1, \ldots, s$ contains exactly two monomials of highest weight.
3. No two monomials in $\Delta_{\prec_w}(\langle F_1, \ldots, F_s \rangle)$ are of the same weight.

Example: $I = \langle X^{q+1} - Y^q - Y \rangle \subseteq \mathbb{F}_{q^2}[X, Y]$

1. OK
2. OK
3. $\Delta_{\prec_w}(I) = \{X^i Y^j \mid 0 \leq j < q, 0 \leq i\}$ OK

Order domain conditions

$I = \langle F_1(\vec{X}), \ldots, F_s(\vec{X}) \rangle \subseteq \mathbb{F}[\vec{X}]$ and $w_1, \ldots, w_m$ satisfy ODC if:

1. $\{F_1, \ldots, F_s\}$ is a Gröbner basis w.r.t. $\prec_w$.
2. F_i, $i = 1, \ldots, s$ contains exactly two monomials of highest weight.
3. No two monomials in $\Delta_{\prec_w}(\langle F_1, \ldots, F_s \rangle)$ are of the same weight.

Example: $I = \langle X^{q+1} - Y^q - Y \rangle \subseteq \mathbb{F}_{q^2}[X, Y]$

1. OK
2. OK
3. $\Delta_{\prec_w}(I) = \{X^i Y^j \mid 0 \leq j < q, 0 \leq i\}$ OK

Presentation Theorem

Theorem (Miura, Pellikaan):

$\cup_{s=0}^{\infty}\mathcal{L}(sQ) = \mathbb{F}[\vec{X}]/I$ where I and corresponding weights satisfy order domain conditions.

Corollary:

$$\begin{aligned} & C_{\mathcal{L}}(P_1 + \cdots + P_n, vQ) \\ = \; & \mathrm{Span}_{\mathbb{F}_q}\{(M(P_1), \ldots, M(P_n)) \mid M \in \Delta_{\prec_w}(I), w(M) \leq v\}. \end{aligned}$$

Presentation Theorem

Theorem (Miura, Pellikaan):

$\cup_{s=0}^{\infty}\mathcal{L}(sQ)=\mathbb{F}[\vec{X}]/I$ where I and corresponding weights satisfy order domain conditions.

Corollary:

$$\begin{aligned} & C_{\mathcal{L}}(P_1+\cdots+P_n, vQ) \\ = \ & \mathrm{Span}_{\mathbb{F}_q}\{(M(P_1),\ldots,M(P_n)) \mid M \in \Delta_{\prec_w}(I), w(M)\leq v\}. \end{aligned}$$

Dimension and generator matrix

Remember in general $\{M + J \mid M \in \Delta_{\prec}(J)\}$ is a basis for $\mathbb{F}[\vec{X}]$.

Define $I_q = I + \langle X_1^q - X_1, \ldots, X_m^q - X_m \rangle$.

$\text{ev} : \mathbb{F}_q[\vec{X}](I_q \rightarrow \mathbb{F}_q^n$ given by $\text{ev}(F + I_q) = (F(P_1), \ldots, F(P_n))$ is a bijection.

$$\begin{aligned} & C_{\mathcal{L}}(P_1 + \cdots + P_n, vQ) \\ = \quad & \text{Span}_{\mathbb{F}_q}\{(M(P_1), \ldots, M(P_n)) \mid M \in \Delta_{\prec_w}(I_q), w(M) \leq v\}. \end{aligned}$$

Dimension can be read off directly. So can generator matrix.

Hermitian function field

$$I_9 = \langle X^4 - Y^3 - Y, X^9 - X, Y^9 - Y \rangle \subseteq \mathbb{F}_9[X, Y].$$

$$\begin{array}{cccccccccccc} 8 & 11 & 14 & 17 & 20 & 23 & 26 & 29 & 32 & 35 & 38 & \cdots \\ 4 & 7 & 10 & 13 & 16 & 19 & 22 & 25 & 28 & 31 & 34 & \cdots \\ 0 & 3 & 6 & 9 & 12 & 15 & 18 & 21 & 24 & 27 & 30 & \cdots \end{array}$$

$$H^*(Q) = w(\Delta_{\prec_w}(I_9)) \subseteq w(\Delta_{\prec_w}(I)) = H(Q).$$

What about minimum distance?

Applying the footprint bound

Let $I = \langle F_1(\vec{X}), \ldots, F_s(\vec{X}) \rangle$ and $w_1, \ldots, w_m$ satisfy ODC.

Code word $\vec{c} = \mathrm{ev}(F + I_q)$ where $\mathrm{Supp}(F) \subseteq \Delta_{\prec_w}(I_q)$.

Hamming weight equals
$n - |\Delta_{\prec_w}(\langle F(\vec{X}) \rangle + I_q)|$.

For every monomial M

$\mathrm{lm}\big(MF(\vec{X})$ rem $\{F_1(\vec{X}), \ldots, F_s(\vec{X})\}\big)$

DOES NOT BELONG TO $\Delta_{\prec_w}(\langle F(\vec{X}) \rangle + I_q)$.

We can easily detect the above leading monomial!

Applying the footprint bound

Let $I = \langle F_1(\vec{X}), \ldots, F_s(\vec{X})\rangle$ and $w_1, \ldots, w_m$ satisfy ODC.

Code word $\vec{c} = \mathrm{ev}(F + I_q)$ where $\mathrm{Supp}(F) \subseteq \Delta_{\prec_w}(I_q)$.

Hamming weight equals
$n - |\Delta_{\prec_w}(\langle F(\vec{X})\rangle + I_q)|$.

For every monomial M

$\mathrm{lm}\big(MF(\vec{X}) \;\; \text{rem} \;\; \{F_1(\vec{X}), \ldots, F_s(\vec{X})\}\big)$

DOES NOT BELONG TO $\Delta_{\prec_w}(\langle F(\vec{X})\rangle + I_q)$.

We can easily detect the above leading monomial!

The weights tell it all...

$w(\mathrm{Im}(MF(\vec{X})) = w(\mathrm{Im}\big(MF(\vec{X}) \ \text{ rem } \ \{F_1(\vec{X}), \ldots, F_s(\vec{X})\}\big))$
because:

- No two monomials in $F(\vec{X})$ are of the same weight (as no two monomials in $\Delta_{\prec_w}(I)$ are of the same weight).
- Every $F_i(\vec{X})$ has exactly two monomials of highest weight.

Hamming weight of $\vec{c}$

In conclusion we can estimate

$$\begin{aligned} & w_H(\vec{c}) \\ = \;& n - |\Delta_{\prec_w}(\langle F(\vec{X})\rangle + I_q)| \\ = \;& |\Delta_{\prec_w}(I_q)\backslash\Delta_{\prec_w}(\langle F(\vec{X})\rangle + I_q)| \\ \geq \;& |w(\Delta_{\prec_w}(I_q)) \cap \{w(M \cdot \mathrm{Im}(F)) | M \text{ a monomial}\}| \qquad (1) \\ \geq \;& n - |H(Q)\backslash\big(w(\mathrm{Im}(F)) + H(Q)\big)| \\ = \;& n - w(\mathrm{Im}(F)). \end{aligned}$$

Last line corresponds to Goppa bound. Last equality comes from semigroup theory.

Minimum distance of Hermitian codes

$I_9 = \langle X^4 - Y^3 - Y, X^9 - X, Y^9 - Y \rangle \subseteq \mathbb{F}_9[X, Y]$.

$$\begin{array}{ccccccccc} 19 & 16 & 13 & 10 & 7 & 4 & 3 & 2 & 1 \\ 23 & 20 & 17 & 14 & 11 & 8 & 6 & 4 & 2 \\ 27 & 24 & 21 & 18 & 15 & 12 & 9 & 6 & 3 \end{array}$$

Green=Goppa bound, Blue=Equation 1.

Improved code construction straight forward.

Everything works for general one-poing algebraic geometric code.

Minimum distance of Hermitian codes

$$I_9 = \langle X^4 - Y^3 - Y, X^9 - X, Y^9 - Y \rangle \subseteq \mathbb{F}_9[X, Y].$$

19	16	13	10	7	4	3	2	1
23	20	17	14	11	8	6	4	2
27	24	21	18	15	12	9	6	3

Green=Goppa bound, Blue=Equation 1.

Improved code construction straight forward.

Everything works for general one-poing algebraic geometric code.

Minimum distance of Hermitian codes

$I_9 = \langle X^4 - Y^3 - Y, X^9 - X, Y^9 - Y \rangle \subseteq \mathbb{F}_9[X, Y].$

19	16	13	10	7	4	3	2	1
23	20	17	14	11	8	6	4	2
27	24	21	18	15	12	9	6	3

Green=Goppa bound, Blue=Equation 1.

Improved code construction straight forward.

Everything works for general one-poing algebraic geometric code.

PART 3: SMALL-BIAS SPACES

Small-bias space

For program verification etc. we need a probability space

1. Random binary vector of length k.
2. Statistical property close to $\mathbb{F}_2^k$ with uniform distribution.
3. Size of $\mathcal{X}$ much smaller than $|\mathbb{F}_2^k|$.

Small-bias space - definition

Definition: A multiset $\mathcal{X} \subseteq \mathbb{F}_2^k$ is called an ϵ-bias space if

$$\frac{1}{|\mathcal{X}|}\left|\sum_{\vec{x}\in\mathcal{X}}(-1)^{\sum_{i\in T} x_i}\right| \leq \epsilon$$

for every $T \subseteq \{1, \ldots, k\}$.

Interpretation: If $\vec{x}$ appears $i(\vec{x})$ times in $\mathcal{X}$ then

$$\Pr(\vec{X} = \vec{x}) = \frac{i(\vec{x})}{|\mathcal{X}|}.$$

Small-bias space - definition

Definition: A multiset $\mathcal{X} \subseteq \mathbb{F}_2^k$ is called an ϵ-bias space if

$$\frac{1}{|\mathcal{X}|} \left| \sum_{\vec{x} \in \mathcal{X}} (-1)^{\sum_{i \in T} x_i} \right| \leq \epsilon$$

for every $T \subseteq \{1, \ldots, k\}$.

Interpretation: If $\vec{x}$ appears $i(\vec{x})$ times in $\mathcal{X}$ then

$$\Pr(\vec{X} = \vec{x}) = \frac{i(\vec{x})}{|\mathcal{X}|}.$$

Example

Generator matrix for Walsh-Hadamard code

$$\begin{bmatrix} 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 1 \end{bmatrix}$$

Columns constitute an 0-bias space (actually $\mathcal{X} = \mathbb{F}_2^4$)

From code to small-bias space

$$\begin{bmatrix} 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 1 \end{bmatrix}$$

A code is ϵ-balanced if for $\vec{c} \neq \vec{0}$: $\quad \frac{1-\epsilon}{2} \leq \frac{w_H(\vec{c})}{n} \leq \frac{1+\epsilon}{2}$.

$$\begin{array}{ccc} \epsilon - \text{bias set} & & \epsilon - \text{balanced code} \\ \mathcal{X} = \{\vec{x}_1, \ldots, \vec{x}_n\} & \Leftrightarrow & G = [\vec{x}_1, \ldots, \vec{x}_n] \end{array}$$

From code to small-bias space

$$\begin{bmatrix} 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 1 \end{bmatrix}$$

A code is ϵ-balanced if for $\vec{c} \neq \vec{0}$: $\frac{1-\epsilon}{2} \leq \frac{w_H(\vec{c})}{n} \leq \frac{1+\epsilon}{2}$.

$$\begin{array}{c} \epsilon - \text{bias set} \\ \mathcal{X} = \{\vec{x}_1, \ldots, \vec{x}_n\} \end{array} \quad \Leftrightarrow \quad \begin{array}{c} \epsilon - \text{balanced code} \\ G = [\vec{x}_1, \ldots, \vec{x}_n] \end{array}$$

A standard construction

<u>Construction:</u>
Outer code: $[N, K, D]_{2^s}$.
Inner code: Walsh-Hadamard.
Concatenated code: $\epsilon = \frac{N-D}{N}$, $n = N2^s$, $k = Ks$.

- Reed-Solomon codes: $\mathcal{X} \subseteq \mathbb{F}_2^{\Omega(k)}$ and $|\mathcal{X}| = \mathcal{O}\left(\frac{k^2}{\epsilon^2 \log^2(k/\epsilon)}\right)$.
- AG-codes with deg $G > g$ (Drinfeld-Vladut)...
- Hermitian codes with deg $G < g$ (Ben-Aroy and Ta-Shma)...
- Norm-Trace codes with deg $G < g$...
- Product of Hermitian codes with deg $G > g$...
- Gilbert-Varhamov bound...
- LP-bound...

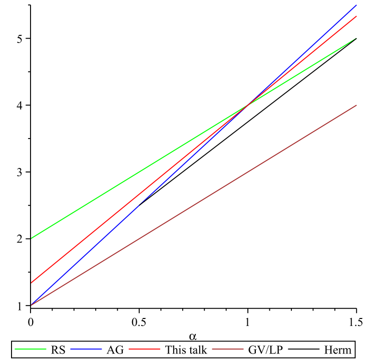
A standard construction

Construction:
Outer code: $[N, K, D]_{2^s}$.
Inner code: Walsh-Hadamard.
Concatenated code: $\epsilon = \frac{N-D}{N}$, $n = N2^s$, $k = Ks$.

- Reed-Solomon codes: $\mathcal{X} \subseteq \mathbb{F}_2^{\Omega(k)}$ and $|\mathcal{X}| = \mathcal{O}\left(\frac{k^2}{\epsilon^2 \log^2(k/\epsilon)}\right)$.
- AG-codes with deg $G > g$ (Drinfeld-Vladut)...
- Hermitian codes with deg $G < g$ (Ben-Aroy and Ta-Shma)...
- Norm-Trace codes with deg $G < g$...
- Product of Hermitian codes with deg $G > g$...
- Gilbert-Varhamov bound...
- LP-bound...

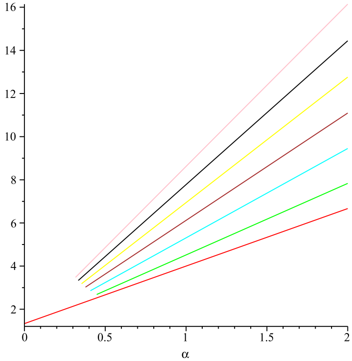
Asymptotic behaviour

Let $\epsilon = k^{-\alpha}$, $k \to \infty$ and consider $\log_k(|\mathcal{X}|) = f(\alpha)$



For $\alpha < 0.5$ AG-construction requires Garcia-Stichtenoth towers.

Comparison with Norm-Trace codes



Product of Hermitian codes

- q-ary Reed-Muller codes are products of Reed-Solomon codes.
- Remember improvement to RM-construction (Massey-Costello-Justesen).
- We consider similar construction with product of Hermitian codes.

Product of Hermitian order domains

$$I^{(2)} = \langle X_1^{q+1} - Y_1^q - Y_1, X_2^{q+1} - Y_2^q - Y_2 \rangle$$

$$I_{q^2}^{(2)} = \langle X_1^{q+1} - Y_1^q - Y_1, X_2^{q+1} - Y_2^q - Y_2, X_1^{q^2} - X_1, \\ Y_1^{q^2} - Y_1, Y_2^{q^2} - Y_2, X_2^{q^2} - X_2 \rangle$$

$$\mathbb{V}_{\mathbb{F}_{q^2}}(I_{q^2}^{(2)}) = \mathbb{V}_{\mathbb{F}_{q^2}}(I_{q^2}) \times \mathbb{V}_{\mathbb{F}_{q^2}}(I_{q^2}) = \{Q_1, \ldots, Q_{q^6}\}$$

Monomial ordering $\prec_w$

$w^{(2)}(X_1) = (q, 0)$, $w^{(2)}(Y_1) = (q+1, 0)$, $w^{(2)}(X_2) = (0, q)$, $w^{(2)}(Y_2) = (0, q+1)$.

$\prec_{\mathbb{N}_0^2}$ any monomial ordering on $\mathbb{N}_0^2$.

$$X_1^{\alpha_1^{(1)}} Y_1^{\beta_1^{(1)}} X_2^{\alpha_1^{(2)}} Y_2^{\beta_1^{(2)}} \prec_w^{(2)} X_1^{\alpha_2^{(1)}} Y_1^{\beta_2^{(1)}} X_2^{\alpha_2^{(2)}} Y_2^{\beta_2^{(2)}}$$

if one of the following two conditions holds:

1. $w^{(2)}(X_1^{\alpha_1^{(1)}} Y_1^{\beta_1^{(1)}} X_2^{\alpha_1^{(2)}} Y_2^{\beta_1^{(2)}}) \prec_{\mathbb{N}_0^2} w^{(2)}(X_1^{\alpha_2^{(1)}} Y_1^{\beta_2^{(1)}} X_2^{\alpha_2^{(2)}} Y_2^{\beta_2^{(2)}})$
2. $w^{(2)}(X_1^{\alpha_1^{(1)}} Y_1^{\beta_1^{(1)}} X_2^{\alpha_1^{(2)}} Y_2^{\beta_1^{(2)}}) = w^{(2)}(X_1^{\alpha_2^{(1)}} Y_1^{\beta_2^{(1)}} X_2^{\alpha_2^{(2)}} Y_2^{\beta_2^{(2)}})$ but $X_1^{\alpha_1^{(1)}} Y_1^{\beta_1^{(1)}} X_2^{\alpha_1^{(2)}} Y_2^{\beta_1^{(2)}} \prec_{\text{lex}} X_1^{\alpha_2^{(1)}} Y_1^{\beta_2^{(1)}} X_2^{\alpha_2^{(2)}} Y_2^{\beta_2^{(2)}}$.

Here, $X_1 \prec_{\text{lex}} Y_1 \prec_{\text{lex}} X_2 \prec_{\text{lex}} Y_2$ is assumed.

Monomial ordering $\prec_w$

$w^{(2)}(X_1) = (q,0),\ w^{(2)}(Y_1) = (q+1,0), w^{(2)}(X_2) = (0,q),$
$w^{(2)}(Y_2) = (0,q+1).$

$\prec_{\mathbb{N}_0^2}$ any monomial ordering on $\mathbb{N}_0^2$.

$$X_1^{\alpha_1^{(1)}} Y_1^{\beta_1^{(1)}} X_2^{\alpha_1^{(2)}} Y_2^{\beta_1^{(2)}} \prec_w^{(2)} X_1^{\alpha_2^{(1)}} Y_1^{\beta_2^{(1)}} X_2^{\alpha_2^{(2)}} Y_2^{\beta_2^{(2)}}$$

if one of the following two conditions holds:

1. $w^{(2)}(X_1^{\alpha_1^{(1)}} Y_1^{\beta_1^{(1)}} X_2^{\alpha_1^{(2)}} Y_2^{\beta_1^{(2)}}) \prec_{\mathbb{N}_0^2} w^{(2)}(X_1^{\alpha_2^{(1)}} Y_1^{\beta_2^{(1)}} X_2^{\alpha_2^{(2)}} Y_2^{\beta_2^{(2)}})$
2. $w^{(2)}(X_1^{\alpha_1^{(1)}} Y_1^{\beta_1^{(1)}} X_2^{\alpha_1^{(2)}} Y_2^{\beta_1^{(2)}}) = w^{(2)}(X_1^{\alpha_2^{(1)}} Y_1^{\beta_2^{(1)}} X_2^{\alpha_2^{(2)}} Y_2^{\beta_2^{(2)}})$
   but
   $X_1^{\alpha_1^{(1)}} Y_1^{\beta_1^{(1)}} X_2^{\alpha_1^{(2)}} Y_2^{\beta_1^{(2)}} \prec_{\text{lex}} X_1^{\alpha_2^{(1)}} Y_1^{\beta_2^{(1)}} X_2^{\alpha_2^{(2)}} Y_2^{\beta_2^{(2)}}$.

Here, $X_1 \prec_{\text{lex}} Y_1 \prec_{\text{lex}} X_2 \prec_{\text{lex}} Y_2$ is assumed.

$\{X_1^{q+1} - Y_1^q - Y_1, X_2^{q+1} - Y_2^q - Y_2, X_1^{q^2} - X_1, X_2^{q^2} - X_2\}$ is a Gröbner basis for $I_{q^2}^{(2)}$ with respect to $\prec_{w^{(2)}}$

$$\{X_1^{i_1} Y_1^{j_1} X_2^{i_2} Y_2^{j_2} + I_{q^2} \mid 0 \leq i_1, i_2 < q^2, 0 \leq j_1, j_2 < q\}$$

a basis for $\mathbb{F}_{q^2}[X_1, Y_1, X_2, Y_2]/I_{q^2}^{(2)}$.

$\mathrm{EV} : \mathbb{F}_{q^2}[X_1, Y_1, X_2, Y_2]/I^{(2)} \rightarrow \mathbb{F}_{q^2}^{q^6}$ is given by
$\mathrm{EV}(F(X_1, Y_1, X_2, Y_2) + I_{q^2}^{(2)}) = (F(Q_1,), \ldots, F(Q_{q^6}))$.

$\{X_1^{q+1} - Y_1^q - Y_1, X_2^{q+1} - Y_2^q - Y_2, X_1^{q^2} - X_1, X_2^{q^2} - X_2\}$ is a Gröbner basis for $I_{q^2}^{(2)}$ with respect to $\prec_{w^{(2)}}$

$$\{X_1^{i_1} Y_1^{j_1} X_2^{i_2} Y_2^{j_2} + I_{q^2} \mid 0 \leq i_1, i_2 < q^2, 0 \leq j_1, j_2 < q\}$$

a basis for $\mathbb{F}_{q^2}[X_1, Y_1, X_2, Y_2]/I_{q^2}^{(2)}$.

EV : $\mathbb{F}_{q^2}[X_1, Y_1, X_2, Y_2]/I^{(2)} \rightarrow \mathbb{F}_{q^2}^{q^6}$ is given by
$\mathrm{EV}(F(X_1, Y_1, X_2, Y_2) + I_{q^2}^{(2)}) = (F(Q_1,), \ldots, F(Q_{q^6}))$.

Value semigroup

Recall, $H(Q)$ Weierstrass semigroup for Q in Hermitian function field.

Recall, $H(Q) = w(\Delta_{\prec_w}(I))$ and $H^*(Q) = w(\Delta_{\prec_w}(I_{q^2}))$.

Define $H^{(2)} = H(Q) \times H(Q)$ and $\left(H^{(2)}\right)^* = H^*(Q) \times H^*(Q)$. We have

$$\left(H^{(2)}\right)^* = w^{(2)}(\Delta_{\prec_{w^{(2)}}}(I_{q^2}^{(2)}))$$

where no two monomials in $\Delta_{\prec_{w^{(2)}}}(I_{q^2}^{(2)})$ have the same weight.

Hamming weight

$\vec{c} = \mathrm{EV}(F(X_1, Y_1, X_2, Y_2) + I_{q^2}^{(2)})$ with
$\mathrm{Supp}(F(X_1, Y_1, X_2, Y_2)) \subseteq \Delta_{\prec_{w^{(2)}}}(I_{q^2}^{(2)})$.

Write $\lambda^{(2)} = (\lambda_1, \lambda_2) = w^{(2)}(\mathrm{Im}(F))$. We can estimate

$$\begin{aligned} |\Delta_{\prec_{w^{(2)}}}(\langle F(X_1, Y_1, X_2, Y_2)\rangle + I_{q^2}^{(2)})| &\leq |H^{(2)} - (\lambda^{(2)} + H^{(2)})| \\ &\leq q^6 - (q^3 - \lambda_1)(q^3 - \lambda_2). \end{aligned}$$

Hence, $w_H(\vec{c}) \geq (q^3 - \lambda_1)(q^3 - \lambda_2)$.

Hamming weight

$\vec{c} = \mathrm{EV}(F(X_1, Y_1, X_2, Y_2) + I_{q^2}^{(2)})$ with
$\mathrm{Supp}(F(X_1, Y_1, X_2, Y_2)) \subseteq \Delta_{\prec_{w^{(2)}}}(I_{q^2}^{(2)})$.

Write $\lambda^{(2)} = (\lambda_1, \lambda_2) = w^{(2)}(\mathrm{Im}(F))$. We can estimate

$$\begin{aligned} |\Delta_{\prec_{w^{(2)}}}(\langle F(X_1, Y_1, X_2, Y_2)\rangle + I_{q^2}^{(2)})| &\leq |H^{(2)} - (\lambda^{(2)} + H^{(2)})| \\ &\leq q^6 - (q^3 - \lambda_1)(q^3 - \lambda_2). \end{aligned}$$

Hence, $w_H(\vec{c}) \geq (q^3 - \lambda_1)(q^3 - \lambda_2)$.

Code construction

$$\tilde{E}(\delta) :=$$

$$\mathrm{Span}_{\mathbb{F}_{q^2}}\Big\{\mathrm{EV}(X_1^{i_1}Y_1^{j_1}X_2^{i_2}Y_2^{j_2}+I_{q^2}^{(2)}) \mid 0 \leq i_1, i_2 < q^2, 0 \leq j_1, j_2 < q,$$

$$(q^3 - w(X_1^{i_1}Y_1^{j_1}))(q^3 - w(X_2^{i_2}Y_2^{j_2})) \geq \delta\Big\}.$$

$d(\tilde{E}(\delta)) \geq \delta$.

To estimate dimension use ONLY genus and *conductor* $= 2g$.

Translates into calculation of volume.

Code construction

$$\tilde{E}(\delta) :=$$

$$\mathrm{Span}_{\mathbb{F}_{q^2}}\Big\{\mathrm{EV}(X_1^{i_1}Y_1^{j_1}X_2^{i_2}Y_2^{j_2}+I_{q^2}^{(2)}) \mid 0 \leq i_1, i_2 < q^2, 0 \leq j_1, j_2 < q,$$
$$(q^3 - w(X_1^{i_1}Y_1^{j_1}))(q^3 - w(X_2^{i_2}Y_2^{j_2})) \geq \delta\Big\}.$$

$d(\tilde{E}(\delta)) \geq \delta.$

To estimate dimension use ONLY genus and *conductor* $= 2g$.

Translates into calculation of volume.

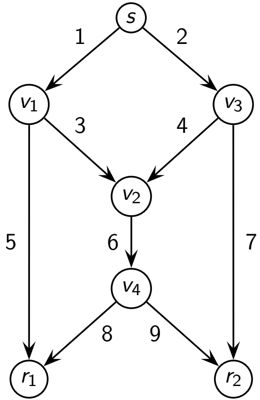
Small-bias space from $\tilde{E}(\delta)$

Theorem:
For any ϵ, $0 < \epsilon < 1$ using codes $\tilde{E}(\delta)$ as outer code one can construct ϵ-bias spaces with

$$\mathcal{X} \subseteq \mathbb{F}_2^{\Omega(k)}, \quad |\mathcal{X}| = O\left(\left(\frac{k}{\epsilon + (1-\epsilon)\ln(1-\epsilon)}\right)^{\frac{4}{3}}\right). \qquad (2)$$

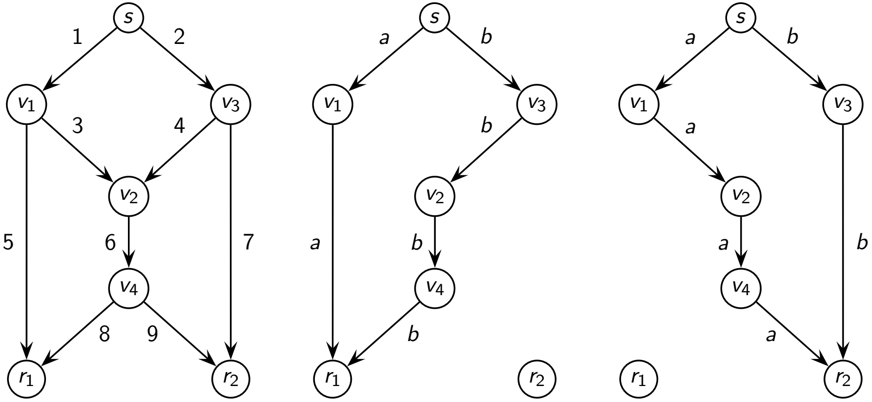
PART 4: LINEAR NETWORK CODING

Simplest possible network coding problem



Sender s wants to send two messages $a, b \in \mathbf{F}_2$ to both receivers r_1 and r_2 simultaneously.

Two partial solutions



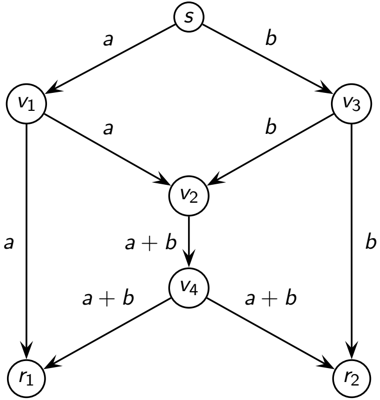
The network   Flow F_1 Flow F_2

The flow system is $\mathcal{F} = \{F_1, F_2\}$

$F_1 = \{(1,5),(2,4,6,8)\}, F_2 = \{(1,3,6,9),(2,7)\}$

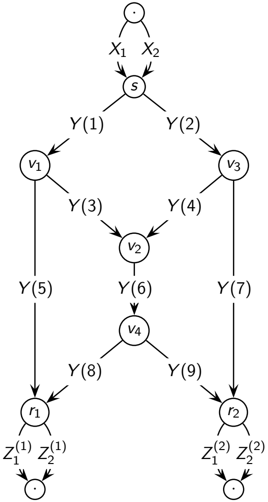
A solution

Routing is insufficient, but problem is solvable



Receiver r_1 can reconstruct b as $a + (a + b)$
Receiver r_2 can reconstruct a as $(a + b) + b$

Linear network coding



Alphabet is $\mathbf{F}_q$ and coefficients below belong to $\mathbf{F}_q$.

$$Y(j) = \sum_{i \in \mathrm{in}(j)} f_{i,j} Y(i) + \sum_{K(X_i) = \mathrm{tail}(j)} a_{i,j} X_i$$

$$Z_j^{(r_l)} = \sum_{i \in \mathrm{in}(r_l)} b_{i,j}^{(r_l)} Y(i)$$

Matrices

A is $h \times |E|$
$A_{i,j} = a_{i,j}$ if $K(X_i) = \mathrm{tail}(j)$
$A_{i,j} = 0$ else

F is $|E| \times |E|$
$F_{i,j} = f_{i,j}$ if $i \in \mathrm{in}(j)$
$F_{i,j} = 0$ else

For $l = 1, \ldots, |R|$

$B^{(r_l)}$ is $|E| \times h$
$B^{(r_l)}_{i,j} = b^{(r_l)}_{i,j}$ if $i \in \mathrm{in}(r_l)$
$B^{(r_l)}_{i,j} = 0$ else

Topological meaning of F^s

The $F_{i,j}$ "holds" information on all paths of length 2 starting in edge i and ending in edge j.

The (i,j)th entry of F^n "holds" information on all paths of length $n+1$ starting in edge i and ending in edge j.

$$\left(F^n\right)_{i,j} = \sum_{\substack{(i=j_0,j_1,\ldots,j_n=j) \\ \text{a path} \\ \text{in } G}} f_{i=j_0,j_1} f_{j_1,j_2} \cdots f_{j_{n-1},j_n=j}$$

G being cycle free $F^N = 0$ for some big enough N.

$I + F + \cdots + F^{N-1}$ holds information on all paths of any length.

Topological meaning of F^s

The $F_{i,j}$ "holds" information on all paths of length 2 starting in edge i and ending in edge j.

The (i,j)th entry of F^n "holds" information on all paths of length $n+1$ starting in edge i and ending in edge j.

$$\left(F^n\right)_{i,j} = \sum_{\substack{(i=j_0,j_1,\ldots,j_n=j) \\ \text{a path} \\ \text{in } G}} f_{i=j_0,j_1} f_{j_1,j_2} \cdots f_{j_{n-1},j_n=j}$$

G being cycle free $F^N = 0$ for some big enough N.

$I + F + \cdots + F^{N-1}$ holds information on all paths of any length.

Topological meaning of F^s

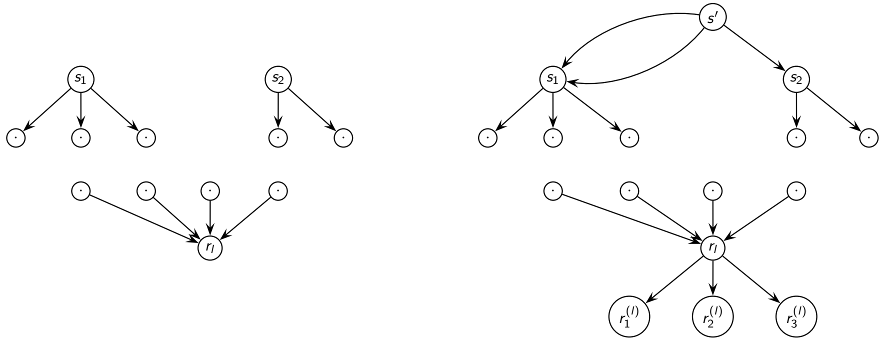
The $F_{i,j}$ "holds" information on all paths of length 2 starting in edge i and ending in edge j.

The (i,j)th entry of F^n "holds" information on all paths of length $n+1$ starting in edge i and ending in edge j.

$$\left(F^n\right)_{i,j} = \sum_{\substack{(i=j_0,j_1,\ldots,j_n=j)\\ \text{a path}\\ \text{in } G}} f_{i=j_0,j_1} f_{j_1,j_2} \cdots f_{j_{n-1},j_n=j}$$

G being cycle free $F^N = 0$ for some big enough N.

$I + F + \cdots + F^{N-1}$ holds information on all paths of any length.



Modification of network. In original network two sources at s_1 and one source at s_2.

In modified network the $a_{i,j}$'s and the $b_{i,j}^{(r_l)}$'s from the original network plays the same role as the $f_{i,j}$'s

Transfer matrix

Lemma:
$M^{(r_l)} = A(I + F + \cdots + F^{N-1})B^{(r_l)}$
holds information on all paths from s' to $\{r_1^{(l)}, \ldots, r_h^{(l)}\}$

From this we derive:

Theorem: $(X_1, \ldots, X_h)M^{(r_l)} = (Z_1^{(r_l)}, \ldots Z_h^{(r_l)})$

$M^{(r_l)}$ is called the transfer matrix for r_l

Transfer polynomial

For successful encoding/decoding we require
$M^{(r_1)} = \cdots = M^{(r_{|R|})} = I$

Relaxed requirement:
$\det(M^{(r_l)}) \neq 0$ for $l = 1, \ldots, |R|$.

Success iff
$\prod_{l=1,\ldots,|R|} \det(M^{(r_l)}) \neq 0$

Considered as a polynomial in the $a_{i,j}$'s, $f_{i,j}$'s and $b_{i,j}^{(r_l)}$'s this product is called the transfer polynomial.

Transfer polynomial

For successful encoding/decoding we require
$M^{(r_1)} = \cdots = M^{(r_{|R|})} = I$

Relaxed requirement:
$\det(M^{(r_l)}) \neq 0$ for $l = 1, \ldots, |R|$.

Success iff
$\prod_{l=1,\ldots,|R|} \det(M^{(r_l)}) \neq 0$

Considered as a polynomial in the $a_{i,j}$'s, $f_{i,j}$'s and $b_{i,j}^{(r_l)}$'s this product is called the transfer polynomial.

Transfer polynomial

For successful encoding/decoding we require
$M^{(r_1)} = \cdots = M^{(r_{|R|})} = I$

Relaxed requirement:
$\det(M^{(r_l)}) \neq 0$ for $l = 1, \ldots, |R|$.

Success iff
$\prod_{l=1,\ldots,|R|} \det(M^{(r_l)}) \neq 0$

Considered as a polynomial in the $a_{i,j}$'s, $f_{i,j}$'s and $b_{i,j}^{(r_l)}$'s this product is called the transfer polynomial.

Topological meaning of det M^{r_l}

<u>Theorem:</u> The permanent $\mathrm{per}(M^{(r_l)})$ is the sum of all monomial expressions in the $a_{i,j}$'s, $f_{i,j}$'s and $b_{i,j}^{(r_l)}$'s which correspond to a flow of size h from s' to $\{r_1^{(l)}, \ldots, r_h^{(l)}\}$ in the modified graph.

Proof: Apply the lemma carefully.

As a consequence $\det(M^{(r_l)})$ is a linear combination of the expressions corresponding to flows. The coefficients being 1 or -1.

In the transfer polynomial $\prod_{l=1,\ldots,|R|} \det(M^{(r_l)})$ every monomial corresponds to a flow system.

Coefficients are integers
which in $\mathbf{F}_q$ becomes elements in $\mathbf{F}_p$, p being the characteristic.

Topological meaning of det M^{r_l}

<u>Theorem:</u> The permanent $\mathrm{per}(M^{(r_l)})$ is the sum of all monomial expressions in the $a_{i,j}$'s, $f_{i,j}$'s and $b_{i,j}^{(r_l)}$'s which correspond to a flow of size h from s' to $\{r_1^{(l)}, \ldots, r_h^{(l)}\}$ in the modified graph.

Proof: Apply the lemma carefully.

As a consequence $\det(M^{(r_l)})$ is a linear combination of the expressions corresponding to flows. The coefficients being 1 or -1.

In the transfer polynomial $\prod_{l=1,\ldots,|R|} \det(M^{(r_l)})$ every monomial corresponds to a flow system.

Coefficients are integers
which in $\mathbf{F}_q$ becomes elements in $\mathbf{F}_p$, p being the characteristic.

Main theorem on linear network coding

Terms MAY cancel out when taking the product of the $\det(M^{(r_l)})$'s.

If all $\det(M^{(r_l)})$'s are different from 0 then so is the transfer polynomial.

Theorem: A multicast problem is solvable iff the graph contains a flow system of size h. If solvable then solvable with linear network coding whenever $q \geq |R|$.

Proof (almost): Necessity follows from unicast considerations. Assume a flow system exists. The transfer polynomial is non-zero and no indeterminate appears in power exceeding $|R|$. Therefore if $q > |R|$ then over $\mathbf{F}_q$ a non-zero solution exists according to the Schwarts-Zippel bound).

Main theorem on linear network coding

Terms MAY cancel out when taking the product of the $\det(M^{(r_l)})$'s.

If all $\det(M^{(r_l)})$'s are different from 0 then so is the transfer polynomial.

<u>Theorem:</u> A multicast problem is solvable iff the graph contains a flow system of size h. If solvable then solvable with linear network coding whenever $q \geq |R|$.

Proof (almost): Necessity follows from unicast considerations. Assume a flow system exists. The transfer polynomial is non-zero and no indeterminate appears in power exceeding $|R|$. Therefore if $q > |R|$ then over $\mathbf{F}_q$ a non-zero solution exists according to the Schwarts-Zippel bound).

Global coding vectors

In linear network coding we always have
$Y(i) = c_1 X_1 + \cdots + c_h X_h$ for some $c_1, \ldots, c_h \in \mathbf{F}_q$.

We shall call $(c_1, \ldots, c_h)$ the global coding vector for edge i.

A receiver that does not know how encoding was done can learn how to decode (if possible) as follows.

Senders inject into the system h message vectors
$(1, 0, \cdots, 0), (0, 1, 0 \ldots, 0), \ldots, (0, \ldots, 0, 1)$.

These generate the global coding vectors at each edge including the in edges of r_l.

If the received global coding vectors span $\mathbf{F}_q^h$ then proper $b_{i,j}^{(r_l)}$'s can be found.

Global coding vectors

In linear network coding we always have $Y(i) = c_1X_1 + \cdots + c_hX_h$ for some $c_1, \ldots, c_h \in \mathbf{F}_q$.

We shall call $(c_1, \ldots, c_h)$ the global coding vector for edge i.

A receiver that does not know how encoding was done can learn how to decode (if possible) as follows.

Senders inject into the system h message vectors $(1, 0, \cdots, 0), (0, 1, 0 \ldots, 0), \ldots, (0, \ldots, 0, 1)$.

These generate the global coding vectors at each edge including the in edges of r_l.

If the received global coding vectors span $\mathbf{F}_q^h$ then proper $b_{i,j}^{(r_l)}$'s can be found.

Global coding vectors

In linear network coding we always have
$Y(i) = c_1X_1 + \cdots + c_hX_h$ for some $c_1, \ldots, c_h \in \mathbf{F}_q$.

We shall call $(c_1, \ldots, c_h)$ the global coding vector for edge i.

A receiver that does not know how encoding was done can learn how to decode (if possible) as follows.

Senders inject into the system h message vectors
$(1, 0, \cdots, 0), (0, 1, 0 \ldots, 0), \ldots, (0, \ldots, 0, 1)$.

These generate the global coding vectors at each edge including the in edges of r_l.

If the received global coding vectors span $\mathbf{F}_q^h$ then proper $b_{i,j}^{(r_l)}$'s can be found.

Jaggi-Sanders algorithm

Jaggi-Sanders algorithm takes as input a solvable multicast problem.
It add a new source s' and moves all processes to this point and add edges $e_1, \ldots, e_h$ from s' to S.
In the extended graph a flow system is found.

The algorithm for every receiver keeps a list of edges corresponding to a cut.

Also it updates along the way encoding coefficients in such a way that the global coding vectors corresponding to any of the $|R|$ cuts at any time span the whole of $\mathbf{F}_q^h$.

Edges in the flow system are visited according to an ancestral ordering.

In every update at most one edge is replaced in a given cut.

The Jaggi-Sanders algorithm cont.

Lemma 1.1: Given a basis $\{\vec{b}_1, \ldots, \vec{b}_h\}$ for $\mathbf{F}_q^h$
and $\vec{c} \in \mathbf{F}_q^h$,
there is exactly one choice of $a \in \mathbf{F}_q$ such that
$\vec{c} + a\vec{b}_h \in \mathrm{span}_{\mathbf{F}_q}\{\vec{b}_1, \ldots, \vec{b}_{h-1}\}$.

From the Jaggi-Sanders algoritm we get $q \geq |R|$ is enough!!!
(the zero-solution does not work for any receiver)

Random network coding

In random network coding a (possible empty) subset of the $a_{i,j}'s, f_{i,j}'s$ are chosen *a priori* in such a way that the resulting network coding problem is still solvable.

Remaining encoding coefficients are chosen in a distributed manner.
They are chosen independently by uniform distribution.

The transfer polynomial with the *a priori* chosen coefficients plugged in considered as a polynomial with coefficients in $\mathbf{F}_q(b_{i,j}^{(r)'}s)$, is called the *a priori* transfer polynomial.

Random network coding

In random network coding a (possible empty) subset of the $a_{i,j}{}'s, f_{i,j}{}'s$ are chosen *a priori* in such a way that the resulting network coding problem is still solvable.

Remaining encoding coefficients are chosen in a distributed manner.
They are chosen independently by uniform distribution.

The transfer polynomial with the *a priori* chosen coefficients plugged in considered as a polynomial with coefficients in $\mathbf{F}_q(b_{i,j}^{(r)}{}'s)$, is called the *a priori* transfer polynomial.

Success probability

Assume the *a priori* transfer polynomial F is non-zero.

Let $X_1^{i_1} \cdots X_m^{i_m}$ be its leading monomial with respect to $\prec$.
The number of combinations of $a_{i,j}{}'s, f_{i,j}{}'s$ that plugged into F give a non-zero element in $\mathbf{F}_q(b_{i,j}^{(r)}{}'s)$ is at least $(q - i_1) \cdots (q - i_m)$

If q is big enough this is a possitive number.

Recall, $b_{i,j}^{(r_l)}$ appears in power at most 1.

For each of the above solutions:
$b_{i,j}^{(r_l)}$ can be chosen such that F evaluates to non-zero in $\mathbf{F}_q$.

In conclussion: $P_{\text{succ}} \geq (q - i_1) \cdots (q - i_m) = P_{\text{FP2}}$

Success probability

Assume the *a priori* transfer polynomial F is non-zero.

Let $X_1^{i_1} \cdots X_m^{i_m}$ be its leading monomial with respect to $\prec$.
The number of combinations of $a_{i,j}{}'s, f_{i,j}{}'s$ that plugged into F give a non-zero element in $\mathbf{F}_q(b_{i,j}^{(r)}{}'s)$ is at least $(q - i_1) \cdots (q - i_m)$

If q is big enough this is a possitive number.

Recall, $b_{i,j}^{(r_l)}$ appears in power at most 1.

For each of the above solutions:
$b_{i,j}^{(r_l)}$ can be chosen such that F evaluates to non-zero in $\mathbf{F}_q$.

In conclussion: $P_{\text{succ}} \geq (q - i_1) \cdots (q - i_m) = P_{\text{FP2}}$

Success probability

Assume the *a priori* transfer polynomial F is non-zero.

Let $X_1^{i_1} \cdots X_m^{i_m}$ be its leading monomial with respect to $\prec$.
The number of combinations of $a_{i,j}{}'s, f_{i,j}{}'s$ that plugged into F give a non-zero element in $\mathbf{F}_q(b_{i,j}^{(r)}{}'s)$ is at least $(q-i_1)\cdots(q-i_m)$

If q is big enough this is a possitive number.

Recall, $b_{i,j}^{(r_l)}$ appears in power at most 1.

For each of the above solutions:
$b_{i,j}^{(r_l)}$ can be chosen such that F evaluates to non-zero in $\mathbf{F}_q$.

In conclussion: $\quad P_{\mathrm{succ}} \geq (q-i_1)\cdots(q-i_m) = P_{\mathrm{FP2}}$

Success probability - cont.

Any monomial in transfer polynomial corresponds to a flow system

$$
\begin{aligned}
P_{\text{succ}} &\geq \min\{(q-i_1)\cdots(q-i_m) \mid X_1^{i_1}\cdots X_m^{i_m} \text{ corresponds} \\
&\qquad\qquad\qquad\qquad\qquad \text{to a flow system in } G\} \\
&= P_{\text{FP1}}
\end{aligned}
$$

Note

- not all flow systems need to appear in transfer polynomial
- not all monomials can be chosen as leading

Success probability - cont.

Lemma 1.2: Let $F \in k[X_1, \ldots, X_m] \backslash \{0\}$ where k is a field containing $\mathbf{F}_q$. Assume all monomials $X_1^{i_1} \cdots X_m^{i_m}$ in the support of F satisfies

1. $j_1, \ldots, j_m \leq d$, where d is some fixed number $d \leq q$.
2. $j_1 + \cdots + j_m \leq dN$ for some fixed integer N with $N \leq m$

The probability that F evaluates to a non-zero value when $(X_1, \ldots, X_m) \in \mathbf{F}_q^m$ is chosen by random (uniformly) and is plugged into F is at least

$$\left(\frac{q-d}{q}\right)^N$$

Proof 1: A lot of technical lemmas and the Schwartz-Zippel bound.

Proof 2: The footprint bound plus one simple observation.

Success probability - cont.

Every monomial in transfer polynomial comes from a flow system $\mathcal{F} = (F_1, \ldots, F_{|R|})$. Consider all possibe flows (not systems).

Let η' be the maximal number of encoding coefficients not chosen *a priori*. Then for all monomials we have cond. 1 and cond. 2 with

$d = |R|$ and $N = \eta'$

We get

$$P_{\text{succ}} \geq \left(\frac{q - |R|}{q}\right)^{\eta'} = P_{\text{Ho2}}$$

Clearly $\eta' \leq |E|$ which gives

$$P_{\text{succ}} \geq \left(\frac{q - |R|}{q}\right)^{|E|} = P_{\text{Ho1}}$$

Success probability - cont.

Every monomial in transfer polynomial comes from a flow system $\mathcal{F} = (F_1, \ldots, F_{|R|})$. Consider all possibe flows (not systems).

Let η' be the maximal number of encoding coefficients not chosen *a priori*. Then for all monomials we have cond. 1 and cond. 2 with

$d = |R|$ and $N = \eta'$

We get

$$P_{\text{succ}} \geq \left(\frac{q-|R|}{q}\right)^{\eta'} = P_{\text{Ho2}}$$

Clearly $\eta' \leq |E|$ which gives

$$P_{\text{succ}} \geq \left(\frac{q-|R|}{q}\right)^{|E|} = P_{\text{Ho1}}$$

Success probability - cont.

$$P_{\mathrm{Ho1}} \leq P_{\mathrm{Ho2}} \leq P_{\mathrm{FP1}} \leq P_{\mathrm{FP2}}$$

Applying the Jaggi-Sanders point of view one get "flow-bounds". These are always better than P_{Ho2}.

Combinatorial approach:

- Jaggi-Sanders visit edges in flowsystem one by one.
- Alternative approach by Balli, Yan and Zhang: Visit vertices in flowsystem one by one. Gives bound in terms of number of vertices.

Success probability - cont.

$$P_{\mathrm{Ho1}} \leq P_{\mathrm{Ho2}} \leq P_{\mathrm{FP1}} \leq P_{\mathrm{FP2}}$$

Applying the Jaggi-Sanders point of view one get "flow-bounds". These are always better than P_{Ho2}.

Combinatorial approach:

- Jaggi-Sanders visit edges in flowsystem one by one.
- Alternative approach by Balli, Yan and Zhang: Visit vertices in flowsystem one by one. Gives bound in terms of number of vertices.

Some general remarks

The use of algebra in Mathematics for Communication

- Algebra useful when constructing new objects.
- Algebra maybe cannot always compete with combinatorial methods when analyzing given combinatorial objects.
- Zeros over $\mathbb{F}_q$ of a polynomial, counted with multiplicity. Best strategy at the moment = combinatorial.