

One-point AG-codes from an affine-variety point of view

Olav Geil
Aalborg University
Denmark

East China Normal University, Shanghai, 2012

Monomial orderings

A monomial ordering \prec is a total ordering on $\{\vec{X}^{\vec{\alpha}} = X_1^{\alpha_1} \cdots X_m^{\alpha_m} \mid \vec{\alpha} \in \mathbb{N}_0^m\}$ 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 $\{\vec{X}^{\vec{\alpha}} = X_1^{\alpha_1} \cdots X_m^{\alpha_m} \mid \vec{\alpha} \in \mathbb{N}_0^m\}$ 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 $2 < 3$.

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

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

If $I = \langle F(\vec{X}) \rangle$ then

$$\Delta_{\prec}(I) = \{ \vec{X}^{\vec{\alpha}} \mid \vec{X}^{\vec{\alpha}} \text{ is not divisible with } \text{lm}(F) \}.$$

More polynomials = analysis more involved.

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

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

If $I = \langle F(\vec{X}) \rangle$ then

$$\Delta_{\prec}(I) = \{ \vec{X}^{\vec{\alpha}} \mid \vec{X}^{\vec{\alpha}} \text{ is not divisible with } \text{Im}(F) \}.$$

More polynomials = analysis more involved.

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

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

If $I = \langle F(\vec{X}) \rangle$ then

$$\Delta_{\prec}(I) = \{\vec{X}^{\vec{\alpha}} \mid \vec{X}^{\vec{\alpha}} \text{ is not divisible with } \text{Im}(F)\}.$$

More polynomials = analysis 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.

Definition:

$\mathbb{V}_{\mathbb{F}}(I)$ means set of common zeros of the polynomials in I .

Corollary:

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

Proof: Consider $\{P_1, \dots, P_n\} \subseteq \mathbb{V}_{\mathbb{F}}(I)$ and define $\text{ev} : \mathbb{F}[\vec{X}]/I \rightarrow \mathbb{F}^n$ by $\text{ev}(F + I) = (F(P_1), \dots, F(P_n))$.
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.

Definition:

$\mathbb{V}_{\mathbb{F}}(I)$ means set of common zeros of the polynomials in I .

Corollary:

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

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

An important special case

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

Proof:

$$\begin{aligned} \text{number of zeros} &\leq |\Delta_{\prec}(\langle F(\vec{X}) \rangle + \langle X_1^q - X_1, \dots, X_m^q - X_m \rangle)| \\ &\leq |\{\vec{X}^{\vec{\alpha}} \mid 0 \leq \alpha_1 < q, \dots, 0 \leq \alpha_m < q, \vec{X}^{\vec{i}} \nmid \vec{X}^{\vec{\alpha}}\}|. \end{aligned}$$

One-point algebraic geometric codes

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

To construct $C_{\mathcal{L}}(D = P_1 + \dots + P_n, \nu Q)$ we need basis for:

$$\bigcup_{s=0}^{\nu} \mathcal{L}(sQ) \subseteq \bigcup_{s=0}^{\infty} \mathcal{L}(sQ).$$

Everything, can be translated into affine variety description:

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

One-point algebraic geometric codes

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

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

Everything, can be translated into affine variety description:

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

Weights versus valuation

Weierstrass semigroup:

$$H(Q) = -\nu_Q \left(\bigcup_{s=0}^{\infty} \mathcal{L}(sQ) \right) = \langle w_1, \dots, w_m \rangle.$$

Definition: Given weights w_1, \dots, w_m define

$w(\vec{X}^{\vec{\alpha}}) = \vec{\alpha} \cdot (w_1, \dots, w_m)$. 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 $\text{Im}(F) = Y^q$.

Weights versus valuation

Weierstrass semigroup:

$$H(Q) = -\nu_Q\left(\bigcup_{s=0}^{\infty} \mathcal{L}(sQ)\right) = \langle w_1, \dots, w_m \rangle.$$

Definition: Given weights w_1, \dots, w_m define

$w(\vec{X}^{\vec{\alpha}}) = \vec{\alpha} \cdot (w_1, \dots, w_m)$. 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 $\text{Im}(F) = Y^q$.

Order domain conditions

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

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

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

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

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

Corollary:

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

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:

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

Dimension and generator matrix

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

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

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

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

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

Hermitian function field

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

8	11	14	17	20	23	26	29	32	35	38	...
4	7	10	13	16	19	22	25	28	31	34	...
0	3	6	9	12	15	18	21	24	27	30	...

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

What about minimum distance?

Applying the footprint bound

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

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

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

For every monomial M

$\text{Im}(MF(\vec{X}) \text{ rem } \{F_1(\vec{X}), \dots, F_s(\vec{X})\})$

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

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

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

For every monomial M

$\text{Im}(MF(\vec{X}) \text{ rem } \{F_1(\vec{X}), \dots, F_s(\vec{X})\})$

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...

$$w(\text{Im}(MF(\vec{X}))) = w(\text{Im}(MF(\vec{X}) \text{ rem } \{F_1(\vec{X}), \dots, F_s(\vec{X})\}))$$

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

$$\begin{aligned} & w_H(\vec{c}) \\ = & n - |\Delta_{\prec_w}(\langle F(\vec{X}) \rangle + I_q)| \\ = & |\Delta_{\prec_w}(I_q) \setminus \Delta_{\prec_w}(\langle F(\vec{X}) \rangle + I_q)| \\ \geq & |w(\Delta_{\prec_w}(I_q)) \cap \{w(M \cdot \text{Im}(F)) \mid M \text{ a monomial}\}| \\ = & |H^*(Q) \cap (w(\text{Im}(F)) + H(Q))| \tag{1} \\ \geq & n - |H(Q) \setminus (w(\text{Im}(F)) + H(Q))| \\ = & n - w(\text{Im}(F)). \end{aligned}$$

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

Hamming weight of \vec{c}

In conclusion we can estimate

$$\begin{aligned} & w_H(\vec{c}) \\ = & n - |\Delta_{\prec_w}(\langle F(\vec{X}) \rangle + I_q)| \\ = & |\Delta_{\prec_w}(I_q) \setminus \Delta_{\prec_w}(\langle F(\vec{X}) \rangle + I_q)| \\ \geq & |w(\Delta_{\prec_w}(I_q)) \cap \{w(M \cdot \text{Im}(F)) \mid M \text{ a monomial}\}| \\ = & |H^*(Q) \cap (w(\text{Im}(F)) + H(Q))| \tag{1} \\ \geq & n - |H(Q) \setminus (w(\text{Im}(F)) + H(Q))| \\ = & n - w(\text{Im}(F)). \end{aligned}$$

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

Hamming weight of \vec{c}

In conclusion we can estimate

$$\begin{aligned} & w_H(\vec{c}) \\ = & n - |\Delta_{\prec_w}(\langle F(\vec{X}) \rangle + I_q)| \\ = & |\Delta_{\prec_w}(I_q) \setminus \Delta_{\prec_w}(\langle F(\vec{X}) \rangle + I_q)| \\ \geq & |w(\Delta_{\prec_w}(I_q)) \cap \{w(M \cdot \text{Im}(F)) \mid M \text{ a monomial}\}| \\ = & |H^*(Q) \cap (w(\text{Im}(F)) + H(Q))| \tag{1} \\ \geq & n - |H(Q) \setminus (w(\text{Im}(F)) + H(Q))| \\ = & n - w(\text{Im}(F)). \end{aligned}$$

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

Hamming weight of \vec{c}

In conclusion we can estimate

$$\begin{aligned} & w_H(\vec{c}) \\ = & n - |\Delta_{\prec_w}(\langle F(\vec{X}) \rangle + I_q)| \\ = & |\Delta_{\prec_w}(I_q) \setminus \Delta_{\prec_w}(\langle F(\vec{X}) \rangle + I_q)| \\ \geq & |w(\Delta_{\prec_w}(I_q)) \cap \{w(M \cdot \text{Im}(F)) \mid M \text{ a monomial}\}| \\ = & |H^*(Q) \cap (w(\text{Im}(F)) + H(Q))| \tag{1} \\ \geq & n - |H(Q) \setminus (w(\text{Im}(F)) + H(Q))| \\ = & n - w(\text{Im}(F)). \end{aligned}$$

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

Hamming weight of \vec{c}

In conclusion we can estimate

$$\begin{aligned} & w_H(\vec{c}) \\ = & n - |\Delta_{\prec_w}(\langle F(\vec{X}) \rangle + I_q)| \\ = & |\Delta_{\prec_w}(I_q) \setminus \Delta_{\prec_w}(\langle F(\vec{X}) \rangle + I_q)| \\ \geq & |w(\Delta_{\prec_w}(I_q)) \cap \{w(M \cdot \text{Im}(F)) \mid M \text{ a monomial}\}| \\ = & |H^*(Q) \cap (w(\text{Im}(F)) + H(Q))| \tag{1} \\ \geq & n - |H(Q) \setminus (w(\text{Im}(F)) + H(Q))| \\ = & n - w(\text{Im}(F)). \end{aligned}$$

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

Hamming weight of \vec{c}

In conclusion we can estimate

$$\begin{aligned} & w_H(\vec{c}) \\ = & n - |\Delta_{\prec_w}(\langle F(\vec{X}) \rangle + I_q)| \\ = & |\Delta_{\prec_w}(I_q) \setminus \Delta_{\prec_w}(\langle F(\vec{X}) \rangle + I_q)| \\ \geq & |w(\Delta_{\prec_w}(I_q)) \cap \{w(M \cdot \text{Im}(F)) \mid M \text{ a monomial}\}| \\ = & |H^*(Q) \cap (w(\text{Im}(F)) + H(Q))| \tag{1} \\ \geq & n - |H(Q) \setminus (w(\text{Im}(F)) + H(Q))| \\ = & n - w(\text{Im}(F)). \end{aligned}$$

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

Minimum distance of Hermitian codes

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

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-point 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-point 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-point algebraic geometric code.

- ▶ Improved bound and improved code construction translates immediately to the general case of one-point AG codes where affine description is not known but $H^*(Q)$ is known.
- ▶ Generalization of one-point construction to higher transcendence degree. We have $\text{trdg} = r \Leftrightarrow w(X_i) \in \mathbb{N}_0^r$. Improved bound works (but Goppa bound does not).
- ▶ Let \mathbb{F}/\mathbb{F}_q be a function field that possesses a Weierstrass semigroup $\Lambda = \langle \lambda_1, \dots, \lambda_m \rangle$. The number of rational places is at most

$$\#(\Lambda \setminus \cup_{i=1}^m (q\lambda_i + \Lambda)) + 1.$$

- ▶ Improved bound and improved code construction translates immediately to the general case of one-point AG codes where affine description is not known but $H^*(Q)$ is known.
- ▶ Generalization of one-point construction to higher transcendence degree. We have $\text{trdg} = r \Leftrightarrow w(X_i) \in \mathbb{N}_0^r$. Improved bound works (but Goppa bound does not).
- ▶ Let \mathbb{F}/\mathbb{F}_q be a function field that possesses a Weierstrass semigroup $\Lambda = \langle \lambda_1, \dots, \lambda_m \rangle$. The number of rational places is at most

$$\#(\Lambda \setminus \cup_{i=1}^m (q\lambda_i + \Lambda)) + 1.$$

- ▶ Improved bound and improved code construction translates immediately to the general case of one-point AG codes where affine description is not known but $H^*(Q)$ is known.
- ▶ Generalization of one-point construction to higher transcendence degree. We have $\text{trdg} = r \Leftrightarrow w(X_i) \in \mathbb{N}_0^r$. Improved bound works (but Goppa bound does not).
- ▶ Let \mathbb{F}/\mathbb{F}_q be a function field that possesses a Weierstrass semigroup $\Lambda = \langle \lambda_1, \dots, \lambda_m \rangle$. The number of rational places is at most

$$\#(\Lambda \setminus \cup_{i=1}^m (q\lambda_i + \Lambda)) + 1.$$