Advanced Coding Theory and Cryptography

Notes by: Alex Pellegrini

Contents

Chapter 1

An introduction to Gröbner bases

Theorem 2.1.10 (Hilbert's Basis Theorem)

Proof. We proceed by induction on the number of variables. Let $I \subset A[X]$ be an ideal not finitely generated, we may assume it can be constructed by an infinite sequence $(f_i)_{i\in\mathbb{N}}$ of independent polynomials of minimal degree. "Independent" means that $f_i \in I \setminus J_i$ where we set $J_i :=< f_0, \dots, f_{i-1} >$. Now let $a_i := lc(f_i)$ be the leading coefficient of f_i and consider $J := a_0, a_1, \dots \subset A$. We know that J can be a basis for an ideal in A but since A is a Noetherian ring we have that there exists a finite basis for such ideal, say $J =< a_1, \dots, a_N >$. We claim that $I =< f_1, \dots, f_N >=: I'$.
Suppose by contrary that this is not true then take a polynomial $f_{N+1} \in I$, we want to show that it is a linear combination of elements of I', so first of all let's look at the leading coefficient:

$$a_{N+1} = u_1 a_1 + u_2 a_2 + \cdots + u_N a_N$$

this is true since A is Noetherian ring. Consider

$$g := \sum_{i=1}^{N} u_i f_i x^{deg(f_{N+1})-deg(f_i)} \in I'$$

it has the same degree and same leading coefficient as f_{N+1}. Now $f_{N+1} - g \notin I'$ and has degree strictly less than f_{N+1} contraddicting its minimality. Therefore $f_{N+1} - g$ must be 0 and $f_{N+1} \in I'$.

The induction follows since we can consider $A[X_1, \dots, X_m] = A'[X_m]$ where $A' := A[X_1, \dots, X_{m-1}]$ which we know is a Noetherian ring. □

Lemma 2.1.13 (Dickson's Lemma)

Proof. We proceed by induction on the number of variables, by first proving the case with one variable. So we are considering $\mathcal{M} = \{X_1^\alpha | \alpha \in \mathbb{N}\}$, and $T \subset \mathcal{M}$ a semigroup ideal. Since every $t_i \in T$ is of the form $t = X_1^{\alpha_i}$ we consider $\beta = \min\{\alpha_i | X_1^{\alpha_i} \in T\}$. We claim that $T =< X_1^\beta >$. Indeed let $t_j \in T$ then it is of the form $t_j = X_1^{\alpha_j}$ so $\frac{t_j}{t_i} = X_1^{\alpha_j - \beta}$ is well defined where $\alpha_j - \beta > 0$ by minimality of β. We can take $\gamma = \alpha_j - \beta$ hence:

$$t_j = X_1^\beta \cdot X_1^\gamma \in < X_1^\beta >= T$$

We prove the more general case so let be $m \in \mathbb{N}$ arbitrary and assume the lemma proved for $m - 1$.
Let $T \subset \mathcal{M} = \{X_1^{a_1} \cdots X_m^{a_m} \mid (a_1, \dots, a_m) \in \mathbb{N}^m\}$. Consider also the projection map $\pi(X_1^{a_1} \cdots X_m^{a_m}) = X_1^{a_1} \cdots X_{m-1}^{a_{m-1}}$. By induction hypothesis $\pi(T)$ is a finitely generated semigroup ideal so we can find a basis, say $\pi(T) =< t_1, \dots, t_k >$. Now let:

$$A_i := \min\{a_m \mid X_m^{a_m} | t, t \in T, \pi(t) = t_i\} \quad \forall i = 1, \dots, k$$

and furthermore

$$A := \min\{a_m \mid X_m^{a_m} \in T\}$$

We claim that $T =< t_1 X_m^{A_1}, \dots, t_k X_m^{A_k}, X_m^A >$ which is a finite set.
So pick an arbitrary $t \in T$ so $t = \pi(t) X_m^{a_{m_t}}$ for some $a_{m_t} \in \mathbb{N}$, we know that $\exists t_i$ such that $\pi(t) = s \cdot t_i$, therefore $t = s \cdot t_i \cdot X_m^{a_{m_t}}$ and by minimality of A_i we obtain that for:

$$t = s \cdot t_i \cdot X_m^{a_{m_t}} = s \cdot t_i \cdot X_m^{A_i} \cdot X_m^\gamma$$

for $\gamma = a_{m_t} - A_i$. Now $\forall t \in T$ we have proved that $t \in < t_i \cdot X_m^{A_i} >$ which is contained in $< t_1 X_m^{A_1}, \dots, t_k X_m^{A_k}, X_m^A >$ $\square$

Theorem 2.1.14

Proof. $\Rightarrow$ Let $f \in I$ then we can write:

$$f = \sum_{i=1}^{k} f_i \cdot p_i = f_1 \cdot p_1 + f_2 \cdot p_2 + \ldots + f_k \cdot p_k, \; f_i \in \mathcal{P}$$

So evaluating $f(A)$ means to evaluate every p_i so:

$$f(A) = f_1 \cdot p_1(A) + f_2 \cdot p_2(A) + \ldots + f_k \cdot p_k(A) =$$

$$= f_1 \cdot 0 + f_2 \cdot 0 + \cdots + f_k \cdot 0 = 0$$

$\Leftarrow$ Trivial by setting $f = p_i$ $\forall i = 1, \dots, k$

$\square$

Theorem 2.1.17

Proof. We already know that I and J are finitely generated so by keeping in mind that $I \subset J$ we can let:

$$I =< p_1, \ldots, p_k > \quad and \quad J =< p_1, \ldots, p_h >, \; h \geq k$$

Now pick $A \in \mathcal{V}_{\mathbb{F}}(J)$ arbitrary, for every $g \in I$ we have that $g \in J$ therefore $g(A) = 0$ which means that $A \in \mathcal{V}_{\mathbb{F}}(I)$ for every A. Therefore $\mathcal{V}_{\mathbb{F}}(J) \subset \mathcal{V}_{\mathbb{F}}(I)$ □

Proposition 2.2.6

Proof. Assume that

$$f = h_1 g_{i_1} + h_2 g_{i_2} + \ldots + h_s g_{i_s} + r_1 = k_1 g_{j_1} + k_2 g_{j_2} + \ldots + k_t g_{j_t} + r_2$$

with $g_{i_l}, g_{j_l} \in \mathcal{G}$ and $h_l, k_l, r_1, r_2 \in \mathcal{P}$. We obtain that neither r_1 nor r_2 are divisible by any $lm(g), g \in \mathcal{G}$. Therefore we can write:

$$0 = f - f = (h_1 g_{i_1} + h_2 g_{i_2} + \ldots + h_s g_{i_s} + r_1) - (k_1 g_{j_1} + k_2 g_{j_2} + \ldots + k_t g_{j_t} + r_2)$$

Hence:

$$r_2 - r_1 = (h_1 g_{i_1} + h_2 g_{i_2} + \ldots + h_s g_{i_s}) - (k_1 g_{j_1} + k_2 g_{j_2} + \ldots + k_t g_{j_t})$$

Now the LHS belongs to the ideal by definition, i.e. $\exists g \in \mathcal{G}$ such that $lm(g)|lm(r_2 - r_1)$ but $lm(r_2 - r_1)$ is $lm(r_2)$ or $lm(r_1)$, so the only way to be divisible is to be 0. □

Corollary 2.2.9

Proof. $\Rightarrow$ $\mathcal{V}(I) = \emptyset$ means that there exists $f \in I$ that has no roots in $\overline{\mathbb{K}}^m$, but this is possible only for a polynomial of degree 0, i.e. a constant, say c in the base field of K. $c = X^0 * c = 1 * c$ therefore $1 \in I$.

$\Leftarrow$ For $f = 1 \in I$ we have no roots, therefore $\mathcal{V}(I) = \emptyset$.

□

Lemma 2.2.13

Proof. Since $\gcd(lm(p_1), lm(p_2)) = 1$ we can write the S-polynomial as follows:

$$S(p_1, p_2) = p_1 lt(p_2) - p_2 lt(p_1)$$

We assume $lc(p_i) = 1, i = 1, 2$ therefore $lt(p_i) = lm(p_i)$ for reading simplicity. Furthermore we write $p_i = lm(p_i) + r_i$ hence:

$$p_1 lt(p_2) - p_2 lt(p_1) = lm(p_2)(lm(p_1) + r_1) - lm(p_1)(lm(p_2) + r_2) =$$

$$= lm(p_2)r_1 - lm(p_1)r_2 = r_1(p_2 - r_2) - r_2(p_1 - r_1) =$$

$$= r_1p_2 - r_2p_1$$

Now since $lm(r_1) < lm(p_1)$, $lm(r_2) < lm(p_2)$ and $\gcd(lm(p_1), lm(p_2)) = 1$ we have that $lm(S)$ is $lm(r_1p_2)$ or $lm(r_2p_1)$ but not both.
Assume $lm(S) = lm(r_1p_2)$ therefore $lm(S)$ is divisible by $lm(p_2)$ by a factor of $lm(r_1)$. Therefore in the division algorithm:

$$S \xrightarrow{p_2} r_1p_2 - r_2p_1 - lm(r_1)p_2 =$$

$$= (r_1 - lm(r_1))p_2 - r_2p_1$$

Which has the same form as the starting point, therefore we can repeat the algorithm til we obtain 0. □

Proposition 2.2.14

Proof. Set $J_i := lm(g) \mid g \in G_i$, we want to prove is that $G_{i+1} \supsetneq G_i$ implies that $J_{i+1} \supsetneq J_i$. By construction of the algorithm we have that $G_{i+1} = G_i \cup \{r\}$ hence $J_{i+1} = J_i \cup \{lm(r)\}$ because $lm(g) \nmid lm(r)$ for any $g \in G_i$. As we know J is a semigroup ideal of $\mathcal{P}$. But $\mathcal{P}$ is Noetherian which means that we do not have infinite ideal chains, or in other words J is finitely generated. So the algorithm stops. □

Chapter 2

Gröbner bases and 0-dim ideals

Theorem 3.1.4

Proof. To check that I is 0-dimensional we prove that its variety contains a finite number of points. Let $E :=< X_i^q - X_i \mid 1 \leq i \leq m >$ whose variety is exactly the vector space $\mathbb{F}_q^m$. Now let $J := I \setminus E$, it is easy to see that $\mathcal{V}(I) = \mathcal{V}(E) \cap \mathcal{V}(J) \subseteq \mathbb{F}_q^m$ hence $\#\mathcal{V}(I) \leq \#\mathbb{F}_q^m = q^m$ which is finite, thus I is 0-dimensional.

To prove that I is radical it is sufficient to show that $\sqrt{I} \subseteq I$ since the other way around is trivial by definition of radical ideal. Given a polynomial $f \in \sqrt{I}$ this belongs to I if and only if $\exists n \in \mathbb{N}$ such that $f^n \in I$ or in other words $f^n \equiv 0 \ rem\ I$. To begin with notice that $f^q \equiv f \ rem\ I$, indeed take:

$$f := a_1 X_1^{\alpha(1,1)} \cdots X_m^{\alpha(m,1)} + \cdots + a_n X_1^{\alpha(1,n)} \cdots X_m^{\alpha(m,n)}$$

Where $\alpha_{(i,j)} \in \mathbb{N}$ and $a_j \in \mathbb{F}$. Now by rising to the power of q e obtain:

$$\begin{gathered} f^q = (a_1 X_1^{\alpha(1,1)} \cdots X_m^{\alpha(m,1)} + \cdots + a_n X_1^{\alpha(1,n)} \cdots X_m^{\alpha(m,n)})^q = \\ = (a_1 X_1^{\alpha(1,1)} \cdots X_m^{\alpha(m,1)})^q + \cdots + (a_n X_1^{\alpha(1,n)} \cdots X_m^{\alpha(m,n)})^q = \\ = a_1 (X_1^q)^{\alpha(1,1)} \cdots (X_m^q)^{\alpha(m,1)} + \cdots + a_n (X_1^q)^{\alpha(1,n)} \cdots (X_m^q)^{\alpha(m,n)} = \\ = a_1 X_1^{\alpha(1,1)} \cdots X_m^{\alpha(m,1)} + \cdots + a_n X_1^{\alpha(1,n)} \cdots X_m^{\alpha(m,n)} \\ = f \mod I \end{gathered}$$

Therefore given $f \in \sqrt{I}$ then $f^n \in I \iff f^n \equiv 0 \mod I$ we can have two cases for n, i.e. $n < q$ and $n \geq q$ but we know that $f^n \equiv f^{n \mod q} \mod I$ so we can consider only the case $n < q$. So we can state the result as follows:

$$f \in \sqrt{I} \Rightarrow f^n \in I \Rightarrow f^n \cdot f^{q-n} \in I \iff f^q \in I \iff f \in I$$

We thus get that $I = \sqrt{I}$. $\square$

Lemma 3.1.9

Proof. Let $T^* := \{X_1^{z_1}, \dots, X_m^{z_m}, \} \subset T$, it is easy to see that $\Delta(T^*)$ forms an m-dimensional rectangle in the space of monomials, therefore we can compute its volume as follows:

$$\#\Delta(T^*) = \prod_{j=1}^{m} z_j$$

Now the remaining part of T forms an m-dimensional polyhedron which is contained in $\Delta(T)$ and has volume:

$$\prod_{j=1}^{m}(z_j - i_j)$$

so to compute the actual value of $\#\Delta(T)$ one must subtract such volume from $\#\Delta(T^*)$ obtaining:

$$\#\Delta(T) = \prod_{j=1}^{m} z_j - \prod_{j=1}^{m}(z_j - i_j)$$

□

Theorem 3.2.1

Proof. We have $S := \{P_1, \dots, P_k\}$ and want a Gröbner basis $\mathcal{G}'$ of $I' := \mathcal{I}(S)$. If $S = \{A\}$ with $A := (a_1, \dots, a_m)$ then $\mathcal{I}(S) =< (X_1 - a_1), \dots, (X_m - a_m) >$, notice that the leading monomials in the generating basis are relatively coprime therefore $\mathcal{S}(g_i, g_j) = 0 \ \forall \ i \neq j$ therefore it is also a Gröbner basis. What we want to prove in the general case is that given $f \in I$ there exist $g \in \mathcal{G}'$ such that $lm(g) \mid lm(f)$.

So let $f \in \mathcal{I}(S \cup \{B\})$, $B \in \mathbb{K}^m$ this means that $f(B) = 0 \ \forall \ P_i \in S \cup \{B\}$. It is easy to see that $f \in \mathcal{I}(S)$ so given $\mathcal{G}$ a Gröbner basis of $\mathcal{I}(S)$ we get that exist $g \in \mathcal{G}$ such that $lm(g) \mid lm(f)$. We distinguish three cases here:

1. If $g(B) = 0$ then $g \in \mathcal{G}'$ and this case is trivial.

2. Suppose $g(B) \neq 0$ and $lm(g) \succ lm(g_*)$. in this case:

$$g' := g - \frac{g(B)}{g_*(B)} \cdot g_*$$

Now $g'(B) = 0$ and the leading monomial is left unchanged so $lm(g') \mid lm(f)$ and so $g' \in \mathcal{G}'$.

3. Suppose $g = g_*$ then $g(B) \neq 0$. We claim that there exist $g_* \cdot (x_i - b_i)$, $0 \leq i \leq m$ such that $lm(g_* \cdot (x_i - b_i)) \mid lm(f)$. Obviously for every i it holds that $(g_* \cdot (x_i - b_i))(B) = 0$. We see that $lm(g_* \cdot (x_i - b_i)) = x_i \cdot lm(g_*)$, if our claim is false then it must be $lm(g_*) = lm(f)$ (the reasoning is as follows: if $lm(g_*) \mid lm(f)$ there must exist x_i such that $x_i \cdot lm(g) \mid lm(f)$ otherwise $lm(g_*) = lm(f)$) therefore keeping in mind that $f \in \mathcal{I}(S)$ we have that:

$$f = g_* + h_1 g_1 + \cdots + h_l \cdot g_l$$

with $g_l \in \mathcal{G}$ and $lm(g_i) \prec lm(g_*)$ therefore evaluating in B we obtain:

$$0 = f(B) = g_*(B) + h_1(B) g_1(B) + \cdots + h_l(B) \cdot g_l(B) = g_*(B) \neq 0$$

which is a contraddiction. So our claim is true and $g(x_i - b_i) \in \mathcal{G}'$ allowing $\mathcal{G}'$ to be a Gröbner basis.

□

Proposition 3.4.2

Proof. Recall that $N(I)$ is the set of monomials that are not leading monomials of elements of $I \subseteq \mathbb{F}[X_1, \ldots, X_m]$. Let $\mathcal{G}$ be a Gröbner basis of I. We want to prove that the elements of the set $\{M + I \mid M \in N(I)\}$ are linearly independent and they span all R.

It is easy to prove that they are linealry independent over F since they differ each other by at least a variable (e.g. X_1 and $X_1 X_2$) or a degree in at least one variable (e.g. $X_1 X_2$ and $X_1 X_2^2$).

To prove that they span all R let $f \in \mathbb{F}[X_1, \ldots, X_m]$ with $f \neq 0$, it belongs to a nonzero residue class in the quotient algebra $[f] \in R$ whose representative has leading monomial $lm(f \mod I) \in N(I)$ as otherwise there will exist $g \in \mathcal{G}$ such that $lm(g) \mid lm(f \mod I)$. This extends to all the other monomials $M_i \in Supp(f \mod I)$ simply because $M_i \prec lm(f \mod I)$. □

Chapter 3

Affine Variety Codes

Theorem 5.1.1

Proof. Write $\mathbb{F}^* = \mathbb{F}_q^* = \{P_1, \ldots, P_n\}$ where $n = q - 1$. Consider the generator matrix of RS_k:

$$G = \begin{pmatrix} 1_{|P_1} & \cdots & 1_{|P_n} \\ \vdots & \ddots & \vdots \\ X_{|P_1}^{k-1} & \cdots & X_{|P_n}^{k-1} \end{pmatrix} = \begin{pmatrix} 1 & 1 & \cdots & 1 \\ P_1 & P_2 & \cdots & P_n \\ \vdots & \vdots & \ddots & \vdots \\ P_1^{k-1} & P_2^{k-1} & \cdots & P_n^{k-1} \end{pmatrix}$$

Notice that a polynomial evaluation (codeword) in $\mathbb{F}[x]$ is precise combination of rows of G Suppose first that there are two polynomials giving the same codeword:

$$c_1 = (f_1(P_1), \ldots, f_1(P_n)) = (f_2(P_1), \ldots, f_2(P_n)) = c_2$$

Since $deg(f_1), deg(f_2) < k \leq n$, $f_1 - f_2$ is a polynomial of degree less than n which has n zeroes that is impossible unless $f_1 = f_2 \Rightarrow c_1 = c_2$. In other words there is no row in G that is a linear combination of the others. Hence $dim(G) = \#rows(G) = k$.

For the distance we prove both $\geq$ and $\leq$:

Notice that the weight of a codeword:

$$(f_1(P_1), \ldots, f_1(P_n)) = (f_2(P_1), \ldots, f_2(P_n))$$

is the number of points of $\mathbb{F}^*$ that are nonzeroes of f. Therefore let f be a polynomial with as many zeroes as possible, i.e. generating a minimum weight codeword. f has at most $k-1$ zeroes in $\mathbb{F}^*$ hence c can have at most $k-1$ zero coordinates which means that the code has distance $d = w_H(f) \geq n - k + 1$.

On the other hand consider the polynomial:

$$f = \prod_{i=1}^{k-1} (x - P_i)$$

it has degree $k-1$ and $k-1$ solutions therefore the codeword it generates has exactly weight $n-k+1$. So the bound is thight. $\square$

Theorem 5.2.1

Proof. Here we write $\mathbb{F}^m = \{P_1, \dots, P_n\}$ with $n = q^m$ Let $c \in RM_s \setminus \{0\}$ then again:

$$c = (f(P_1), \dots, f(P_n))$$

for some $f \in \mathbb{F}[X_1, \dots, X_m]$ and let $lm(f) = X_1^{i_1} \cdots X_m^{i_m}$. By definitionof the code $deg(f) \leq s \leq m(q-1) < q^m$ so f can have at most $deg(f)$ zeroes and thank to this we can say that $c = 0 \iff f = 0$.

Obviously $i_1 + \cdots + i_m \leq s$ and $0 \leq i_1, \dots, i_m \leq q-1$ since every coordinate of $P_{i,j}$ (the $j-th$ coordinate of P_i) is a value of $\mathbb{F}$ so it respects $P_{i,j}^q = P_{i,j}$.
Set $I := < f > + < X_1^q - X_1, \dots, X_m^q - X_m >$, it is 0-dimensional and radical by theorem 3.1.4. The zeroes of f over $\mathbb{F}^m$ are:

$$\mathcal{V}_{\mathbb{F}^>}(I) = N(I) \subseteq \Delta(I) = < X_1^q, \dots, X_m^q, X_1^{i_1} \cdots X_m^{i_m} >$$

Therefore we can compute a lower bound for the weight of c that is:

$$w_H(c) = n - N(I) \geq n - \#\Delta(I)$$

$$= q^m - (q^m - \prod_{j=1}^{m}(q - i_j)) = \prod_{j=1}^{m}(q - i_j)$$

$$= (q - i_1) \cdots (q - i_m) =: L$$

Now we need to minimize L we want as many $(q - i_h) = 1$ as possible, i.e. $i_h = q-1$, but since $s = a(q-1) + b$, we can do this only for a factors, so take:

$$i_1 = \cdots = i_a = q - 1 \quad and \quad i_{a+1} = b$$

Then $i_1 + \cdots + i_m = a(q-1) + b$ and so we get:

$$L = (q - (q-1))^a \cdot (q - b) \cdot q^{m-a-1} = (q - b) \cdot q^{m-a-1}$$

To show that this bound is thight we find a polynomial that generates a codeword of weight exactly L. Write $\mathbb{F} = \{\alpha_1, \dots, \alpha_q\}$ and consider the following polynomial:

$$g := (\prod_{l=1}^{q-1}(\prod_{i=1}^{a}(X_i - \alpha_l)))(\prod_{t=1}^{b}(X_{a+1} - \alpha_t))$$

So $lm(g) = X_1^{q-1} \cdots X_a^{q-1} X_{a+1}^b$, has degree $deg(g) = a(q-1) + b$ and has exactly $(q-b)q^{m-a-1}$ non zeroes. $\square$

Exercise 5.8.2

Proof. Let's check that g has actually the claimed number of nonzeroes, we have $q-1$ values that given to X_1 make g vanish, which means that there are $(q-1)q^{m-1}$ vectors in $\mathbb{F}^m$ that are zeroes because they make a factor of g containing X_1 vanish. We do the same for X_2 but without considering vectors already taken for X_1, i.e. we can take $(q-1)q^{m-2}$ vectors. We go on like this for $a+1$ variables obtaining:

$$\overbrace{(q-1)q^{m-1}+(q-1)q^{m-2}+\cdots+(q-1)q^{m-a}}^{R}+\overbrace{bq^{m-a-1}}^{Q}$$

Consider the two parts R and Q separately:

$$R=(q-1)(q^{m-a})\frac{(q^a-1)}{q-1}=(q^m-q^{m-a})$$

$$R+Q=(q^m-q^{m-a})+bq^{m-a-1}$$

Therefore the number of nonzeroes are:

$$\begin{aligned}q^m-(R+Q)&=q^m-(q^m-q^{m-a})-bq^{m-a-1}\\&=q^{m-a}-bq^{m-a-1}=qq^{m-a-1}-bq^{m-a-1}\\&=(q-b)q^{m-a-1}\end{aligned}$$

□

Lemma 5.3.1

Proof. Write again $\mathbb{F}^m=\{P_1,\ldots,P_n\}$ where $n=q^m$, and the simple field $\mathbb{F}=\{\alpha_1,\ldots,\alpha_q\}$. We can simply take the following polynomial:

$$f:=\prod_{j=1}^{m}\left(\prod_{t=1}^{i_j}(X_j-\alpha_t)\right)$$

See that $lm(f)=X_1^{i_1}\cdots X_m^{i_m}$, and now we check the number of nonzeroes by counting the number of zeroes as before. The number of zeroes of f is:

$$\#\mathcal{V}(<f>)=i_1q^{m-1}+i_2q^{m-2}(q-i_1)+\cdots+i_m\prod_{j=1}^{m-1}(q-i_j)$$

$$=q^m-\prod_{j=1}^{m}(q-i_j)$$

Hence the weight of a the codeword c generated by f will be:

$$w_H(c)=q^m-\#\mathcal{V}(<f>)=\prod_{j=1}^{m}(q-i_j)$$

□

Theorem 5.3.2

Proof. We first fix a monomial ordering $\prec$ and then take a nonzero codeword $c \in Hyp_q(s,m) - \{0\}$. Using the same notation as in Lemma 5.3.1 we have that:

$$c = (f(P_1), \ldots, f(P_n))$$

with $f \in \mathbb{F}[X_1, \ldots, X_m]$ non zero and having $lm(f) = X_1^{i_1} \cdots X_m^{i_m}$. Let's count the number of nonzeroes of f, call $I_q =< X_1^q - X_1, \ldots, X_m^q - X_m >$ $+ < f >$:

$$w_H(c) = q^m - \#N(I_q) \geq q^m - \#\Delta(I_q) = \prod_{j=1}^{m}(q - i_j) \geq q^m - s$$

Notice that the last inequality comes from the definition of hyperbolic code. We can now apply Lemma 5.3.1 to find a polynomial with that leading monomial and $q^m - s$ nonzero points. So the bound is tight. $\square$

Lemma 5.4.2

Proof. In order to minimize the value $\prod_{l=1}^{m}(q - i_l)$ we try to have as many small factors (i.e. $(q - i_l) = 1$) as possible. To do this we take $i_1 = s - 1$ and $i_2 = 1$ and $i_3 = \cdots = i_m = 0$. Hence the product becomes:

$$\prod_{l=1}^{m}(q - i_l) = q^m - \overline{s}_1 q^{m-1} + \overline{s}_2 q^{m-2} - \cdots (-1)^m \overline{s}_m$$

Where $\overline{s}_k$ for $1 \leq k \leq m$ is the k-th symmetric polynomial in the variables $\{i_1, \ldots, i_m\}$. Notice that for $k \geq 3$ every term of s_k is made up by three variables, which means that at least one of them must be 0. Notice furthermore that for the same reason:

$$\overline{s}_1 = i_1 + i_2 = s \quad and \quad \overline{s}_2 = i_1 \cdot i_2 = s - 1$$

Therefore what survives of the polynomial is:

$$\prod_{l=1}^{m}(q - i_l) = q^m - \overline{s}_1 q^{m-1} + \overline{s}_2 q^{m-2}$$

$$= q^m - s q^{m-1} + (s-1) q^{m-2}$$

$\square$

Lemma 5.4.3

Proof. We try to minimize the value $(s - i_1) \prod_{l=2}^{m} (q - i_l)$. Since $s \leq q - 1$ we procede by taking $i_2 = q - 1$ now by the relation $i_1 + \cdots + i_m = q$ we have 1 more to spend. To choose on which i_l we spend it consider the following argument for $a, b \in \mathbb{N}, a < b$:

$$(a - 1)b = ab - b < ab - a = a(b - 1)$$

Therefore by setting $a = s$ and $b = q$ the obvious choice will be $i_1 = 1$. Thus we get:

$$(s - 1) \prod_{l=3}^{m} (q - i_l) = (s - 1)(q^{m-3} - \overline{s}_1 q^{m-4} + \cdots (-1)^{m-2} \overline{s}_{m-2})$$

Now by the same argument we had in Lemma 5.4.2 we see that no $\overline{s}_k$ survives since all the $i_l = 0$ for $l \geq 3$. Hence the minimum value is $(s - 1)q^{m-2}$. $\square$