Algebraic Geometric Codes

Recitation 13

Shir Peleg

Tel Aviv University

June 1, 2022

Remainder - Riemann Hurwitz Genus Formula

Theorem 1

Let F/L be a separable finite extension of E/K. Denote by g_F, g_E their respective genus. Then,

$$2g_F - 2 = \frac{[F:E]}{[L:K]}(2g_E - 2) + \deg \mathit{Diff}(F/E).$$

Remainder - Riemann Hurwitz Genus Formula

Theorem 1

Let F/L be a separable finite extension of E/K. Denote by g_F, g_E their respective genus. Then,

$$2g_F - 2 = \frac{[F:E]}{[L:K]}(2g_E - 2) + \deg \mathit{Diff}(F/E).$$

Corollary 2

Let F/L be a separable finite extension of E/K. Denote by g_F, g_E their respective genus. Then, $g_F \geq g_E$.

Remainder - Riemann Hurwitz Genus Formula

Theorem 1

Let F/L be a separable finite extension of E/K. Denote by g_F, g_E their respective genus. Then,

$$2g_F - 2 = \frac{[F:E]}{[L:K]}(2g_E - 2) + \deg \mathit{Diff}(F/E).$$

Corollary 2

Let F/L be a separable finite extension of E/K. Denote by g_F, g_E their respective genus. Then, $g_F \geq g_E$.

Proof.

We have $[L:K] = [LE:E]$, and $E \subseteq LE \subseteq F$ and thus $\frac{[F:E]}{[L:K]} = [F:LE] \geq 1$.

Remainder - Riemann Hurwitz Genus Formula

Theorem 1

Let F/L be a separable finite extension of E/K. Denote by g_F, g_E their respective genus. Then,

$$2g_F - 2 = \frac{[F:E]}{[L:K]}(2g_E - 2) + \deg \mathit{Diff}(F/E).$$

Corollary 2

Let F/L be a separable finite extension of E/K. Denote by g_F, g_E their respective genus. Then, $g_F \geq g_E$.

Proof.

We have $[L:K] = [LE:E]$, and $E \subseteq LE \subseteq F$ and thus $\frac{[F:E]}{[L:K]} = [F:LE] \geq 1$.From Hurwitz thm $\mathrm{Diff}(F/E) \geq 0$ and so $\deg \mathrm{Diff}(F/E) \geq 0$. □

Luroth Theorem

Theorem 3

Let F/K be a rational function field and let $K \subsetneq E \subsetneq F$, then E is a rational function field.

Luroth Theorem

Theorem 3

Let F/K be a rational function field and let $K \subsetneq E \subsetneq F$, then E is a rational function field.

Proof.

We proved that $g_F = 0$. If F/E is separable, using Corollary 2 we get that $g_E = 0$.

Luroth Theorem

Theorem 3

Let F/K be a rational function field and let $K \subsetneq E \subsetneq F$, then E is a rational function field.

Proof.

We proved that $g_F = 0$. If F/E is separable, using Corollary 2 we get that $g_E = 0$. Thus, from a previous characterization, we either have that E is a rational function field, or a degree 2 extension of such. How can we differ?

Luroth Theorem

Theorem 3

Let F/K be a rational function field and let $K \subsetneq E \subsetneq F$, then E is a rational function field.

Proof.

We proved that $g_F = 0$. If F/E is separable, using Corollary 2 we get that $g_E = 0$. Thus, from a previous characterization, we either have that E is a rational function field, or a degree 2 extension of such. How can we differ? If E has a degree 1 place then it must be a rational function field.

Luroth Theorem

Theorem 3

Let F/K be a rational function field and let $K \not\subseteq E \not\subseteq F$, then E is a rational function field.

Proof.

We proved that $g_F = 0$. If F/E is separable, using Corollary 2 we get that $g_E = 0$. Thus, from a previous characterization, we either have that E is a rational function field, or a degree 2 extension of such. How can we differ? If E has a degree 1 place then it must be a rational function field. But F has a degree one place, $\mathfrak{P}_\infty$, and thus the place that sits under it must have degree one.

Luroth Theorem

Theorem 3

Let F/K be a rational function field and let $K \not\subseteq E \not\subseteq F$, then E is a rational function field.

Proof.

We proved that $g_F = 0$. If F/E is separable, using Corollary 2 we get that $g_E = 0$. Thus, from a previous characterization, we either have that E is a rational function field, or a degree 2 extension of such. How can we differ? If E has a degree 1 place then it must be a rational function field. But F has a degree one place, $\mathfrak{P}_\infty$, and thus the place that sits under it must have degree one.

If F/E is not separable, we can assume that F/E is purely inseparable (As, we can use $E = E_s$ and then $F = E_s$). As $F = K(t)$ for some t, it holds that $E = K(t^q)$ for some q. $\square$

Fermat's Theorem for Polynomials

Theorem 4

Let K be a field and let $n \geq 3$ s.t. $n, char(K)$ are coprime. Then there are no polynomials $0 \neq f, g, h \in K[Z]$, s.t.

$$f^n + g^n = h^n,$$

unless $f/h, g/h \in K^\times$.

Fermat's Theorem for Polynomials

Theorem 4

Let K be a field and let $n \geq 3$ s.t. $n, char(K)$ are coprime. Then there are no polynomials $0 \neq f, g, h \in K[Z]$, s.t.

$$f^n + g^n = h^n,$$

unless $f/h, g/h \in K^\times$.

Proof

Assume w.l.o.g K is algebraically closed.

Fermat's Theorem for Polynomials

Theorem 4

Let K be a field and let $n \geq 3$ s.t. $n, char(K)$ are coprime. Then there are no polynomials $0 \neq f, g, h \in K[Z]$, s.t.

$$f^n + g^n = h^n,$$

unless $f/h, g/h \in K^{\times}$.

Proof

Assume w.l.o.g K is algebraically closed. Consider the algebraic function field $F = K(x, y)$ where $x^n + y^n = 1$.

Fermat's Theorem for Polynomials

Theorem 4

Let K be a field and let $n \geq 3$ s.t. $n, char(K)$ are coprime. Then there are no polynomials $0 \neq f, g, h \in K[Z]$, s.t.

$$f^n + g^n = h^n,$$

unless $f/h, g/h \in K^\times$.

Proof

Assume w.l.o.g K is algebraically closed. Consider the algebraic function field $F = K(x, y)$ where $x^n + y^n = 1$. Denote by ζ_n the $n's$ primitive root of unity in $K^\times$.

Fermat's Theorem for Polynomials

Claim 4.1

It holds that $[F : K(x)] = n$, *and the places corresponding to the valuations* $v_{x-\zeta_n^i}$, *denoted by* $\mathfrak{p}_{\zeta_n^i}$, *are fully ramified in* F*. i.e. there is a unique* F*- place* $\mathfrak{P}_{\zeta_n^i}$ *s.t.* $e(\mathfrak{P}_{\zeta_n^i}/\mathfrak{p}_{\zeta_n^i}) = n$.

Fermat's Theorem for Polynomials

Claim 4.1

It holds that $[F : K(x)] = n$, *and the places corresponding to the valuations* $v_{x-\zeta_n^i}$, *denoted by* $\mathfrak{p}_{\zeta_n^i}$, *are fully ramified in* F. *i.e. there is a unique* F*- place* $\mathfrak{P}_{\zeta_n^i}$ *s.t.* $e(\mathfrak{P}_{\zeta_n^i}/\mathfrak{p}_{\zeta_n^i}) = n$.

Proof.

First note that $v_{x-\zeta_n^i}(x - \zeta_n^j) = \delta_{ij}$.

Claim 4.1

It holds that $[F : K(x)] = n$, and the places corresponding to the valuations $v_{x-\zeta_n^i}$, denoted by $\mathfrak{p}_{\zeta_n^i}$, are fully ramified in F. i.e. there is a unique F- place $\mathfrak{P}_{\zeta_n^i}$ s.t. $e(\mathfrak{P}_{\zeta_n^i}/\mathfrak{p}_{\zeta_n^i}) = n$.

Proof.

First note that $v_{x-\zeta_n^i}(x-\zeta_n^j) = \delta_{ij}$. Thus,

$$v_{x-\zeta_n^i}(x^n-1) = v_{x-\zeta_n^i}\left(\prod_{j=1}^{n}(x-\zeta_n^j)\right) = 1.$$

Fermat's Theorem for Polynomials

Claim 4.1

It holds that $[F : K(x)] = n$, and the places corresponding to the valuations $v_{x-\zeta_n^i}$, denoted by $\mathfrak{p}_{\zeta_n^i}$, are fully ramified in F. i.e. there is a unique F- place $\mathfrak{P}_{\zeta_n^i}$ s.t. $e(\mathfrak{P}_{\zeta_n^i}/\mathfrak{p}_{\zeta_n^i}) = n$.

Proof.

First note that $v_{x-\zeta_n^i}(x - \zeta_n^j) = \delta_{ij}$. Thus,

$$v_{x-\zeta_n^i}(x^n - 1) = v_{x-\zeta_n^i}\left(\prod_{j=1}^{n}(x - \zeta_n^j)\right) = 1.$$

It follows that for an extension $v_{\mathfrak{P}}$ of $v_{x-\zeta_n^i}$, we have that $v_{\mathfrak{P}}(x^n - 1) = e(\mathfrak{P}/\mathfrak{p}_{\zeta_n^i}) \cdot 1$.

Fermat's Theorem for Polynomials

Claim 4.1

It holds that $[F : K(x)] = n$, and the places corresponding to the valuations $v_{x-\zeta_n^i}$, denoted by $\mathfrak{p}_{\zeta_n^i}$, are fully ramified in F. i.e. there is a unique F- place $\mathfrak{P}_{\zeta_n^i}$ s.t. $e(\mathfrak{P}_{\zeta_n^i}/\mathfrak{p}_{\zeta_n^i}) = n$.

Proof.

First note that $v_{x-\zeta_n^i}(x-\zeta_n^j) = \delta_{ij}$. Thus,

$$v_{x-\zeta_n^i}(x^n-1) = v_{x-\zeta_n^i}\left(\prod_{j=1}^{n}(x-\zeta_n^j)\right) = 1.$$

It follows that for an extension $v_{\mathfrak{P}}$ of $v_{x-\zeta_n^i}$, we have that $v_{\mathfrak{P}}(x^n-1) = e(\mathfrak{P}/\mathfrak{p}_{\zeta_n^i}) \cdot 1$. On the other hand

$$n \leq n v_{\mathfrak{P}}(y) = v_{\mathfrak{P}}(x^n-1) = e(\mathfrak{P}/\mathfrak{p}_{\zeta_n^i}) \leq [F : K(x)] \leq n$$

Fermat's Theorem for Polynomials

Claim 4.1

It holds that $[F : K(x)] = n$, and the places corresponding to the valuations $v_{x-\zeta_n^i}$, denoted by $\mathfrak{p}_{\zeta_n^i}$, are fully ramified in F. i.e. there is a unique F- place $\mathfrak{P}_{\zeta_n^i}$ s.t. $e(\mathfrak{P}_{\zeta_n^i}/\mathfrak{p}_{\zeta_n^i}) = n$.

Proof.

First note that $v_{x-\zeta_n^i}(x-\zeta_n^j) = \delta_{ij}$. Thus,

$$v_{x-\zeta_n^i}(x^n - 1) = v_{x-\zeta_n^i}\left(\prod_{j=1}^{n}(x-\zeta_n^j)\right) = 1.$$

It follows that for an extension $v_{\mathfrak{P}}$ of $v_{x-\zeta_n^i}$, we have that $v_{\mathfrak{P}}(x^n - 1) = e(\mathfrak{P}/\mathfrak{p}_{\zeta_n^i}) \cdot 1$. On the other hand

$$n \leq n v_{\mathfrak{P}}(y) = v_{\mathfrak{P}}(x^n - 1) = e(\mathfrak{P}/\mathfrak{p}_{\zeta_n^i}) \leq [F : K(x)] \leq n$$

Thus $e(\mathfrak{P}/\mathfrak{p}_{\zeta_n^i}) = [F : K(x)] = n$ and from the fundamental inequality, it follows that $\mathfrak{P}_{\zeta_n^i} := \mathfrak{P}$ is unique and $\mathfrak{p}_{\zeta_n^i}$ is fully ramified. $\square$

Fermat's Theorem for Polynomials

Claim 4.2

Let $f, g, h \in K[Z]$ *as in the theorem. Write* $f_0 = \frac{f}{h}, g_0 = \frac{g}{h}$. *Then,*

$$F \cong K(f_0, g_0).$$

Fermat's Theorem for Polynomials

Claim 4.2

Let $f, g, h \in K[Z]$ as in the theorem. Write $f_0 = \frac{f}{h}, g_0 = \frac{g}{h}$. Then,

$$F \cong K(f_0, g_0).$$

Proof.

First note that $K(x) \to K(f_0) : x \to f_0$ is a field isomorphism.

Fermat's Theorem for Polynomials

Claim 4.2

Let $f, g, h \in K[Z]$ as in the theorem. Write $f_0 = \frac{f}{h}, g_0 = \frac{g}{h}$. Then,

$$F \cong K(f_0, g_0).$$

Proof.

First note that $K(x) \to K(f_0) : x \to f_0$ is a field isomorphism. Now, from the previous claim,

$$Y^n + x^n - 1 \in K(x)[Y],$$

is the minimal polynomial of y over $K(x)$.

Fermat's Theorem for Polynomials

Claim 4.2

Let $f, g, h \in K[Z]$ *as in the theorem. Write* $f_0 = \frac{f}{h}, g_0 = \frac{g}{h}$. *Then,*

$$F \cong K(f_0, g_0).$$

Proof.

First note that $K(x) \to K(f_0) : x \to f_0$ is a field isomorphism. Now, from the previous claim,

$$Y^n + x^n - 1 \in K(x)[Y],$$

is the minimal polynomial of y over $K(x)$. It follows that $T^n + f_0^n - 1$ is irreducible over $K(f_0)$, and therefore is the minimal polynomial of g_0 over $K(f_0)$.

Fermat's Theorem for Polynomials

Claim 4.2

Let $f, g, h \in K[Z]$ as in the theorem. Write $f_0 = \frac{f}{h}, g_0 = \frac{g}{h}$. Then,

$$F \cong K(f_0, g_0).$$

Proof.

First note that $K(x) \to K(f_0) : x \to f_0$ is a field isomorphism. Now, from the previous claim,

$$Y^n + x^n - 1 \in K(x)[Y],$$

is the minimal polynomial of y over $K(x)$. It follows that $T^n + f_0^n - 1$ is irreducible over $K(f_0)$, and therefore is the minimal polynomial of g_0 over $K(f_0)$. This implies that

$$F \cong K(f_0, g_0) \text{ via } x \to f_0, y \to g_0.$$

$\square$

Proof of Theorem 4.

From corollary 2 we get that $g_F = 0$. Apply the Riemann Hurwiz formula for $E = K(x)$ and F to obtain:

Fermat's Theorem for Polynomials

Proof of Theorem 4.

From corollary 2 we get that $g_F = 0$. Apply the Riemann Hurwiz formula for $E = K(x)$ and F to obtain:

$$2g_F - 2 = [F : E](2g_E - 2) + \deg \mathrm{Diff}(F/E)$$

From Hurwiz genus different theorem we get that $d(\mathfrak{P}/\mathfrak{p}) = e(\mathfrak{P}/\mathfrak{p}) - 1$, thus for the n places mentioned in Claim 4.1, we have that $d(\mathfrak{P}_{\zeta_n^i}/\mathfrak{p}_{\zeta_n^i}) = n - 1$ and therefore,

Fermat's Theorem for Polynomials

Proof of Theorem 4.

From corollary 2 we get that $g_F = 0$. Apply the Riemann Hurwiz formula for $E = K(x)$ and F to obtain:

$$-2 = -2n + \deg \mathrm{Diff}(F/E)$$

From Hurwiz genus different theorem we get that $d(\mathfrak{P}/\mathfrak{p}) = e(\mathfrak{P}/\mathfrak{p}) - 1$, thus for the n places mentioned in Claim 4.1, we have that $d(\mathfrak{P}_{\zeta_n^i}/\mathfrak{p}_{\zeta_n^i}) = n - 1$ and therefore,

$$-2 = -2n + \deg \mathrm{Diff}(F/E) \geq -2n + n(n-1),$$

Proof of Theorem 4.

From corollary 2 we get that $g_F = 0$. Apply the Riemann Hurwiz formula for $E = K(x)$ and F to obtain:

$$-2 = -2n + \deg \operatorname{Diff}(F/E)$$

From Hurwiz genus different theorem we get that $d(\mathfrak{P}/\mathfrak{p}) = e(\mathfrak{P}/\mathfrak{p}) - 1$, thus for the n places mentioned in Claim 4.1, we have that $d(\mathfrak{P}_{\zeta_n^i}/\mathfrak{p}_{\zeta_n^i}) = n - 1$ and therefore,

$$-2 = -2n + \deg \operatorname{Diff}(F/E) \geq -2n + n(n-1),$$

and

$$n^2 - 3n + 2 = (n-2)(n-1) \leq 0$$

Which is a implies that $n \leq 2$ as we wanted. $\square$

Hurwiz Theorem

Theorem 5

Let F be a function field, over an algebraically closed field K, with genus $g \geq 2$. Let $G \leq Aut(F/K)$ be a finite subgroup of automorphisms of F over K. Assume further that $char(K)$ and $|G|$ are coprime. Then, $|G| \leq 84(g-1)$

Proof.

Let $E = F^G$ be the fixed field of G. From Galois theorem we know that F/E is Galois and $[F:E] = |G| := n$.

Hurwiz Theorem

Theorem 5

Let F be a function field, over an algebraically closed field K, with genus $g \geq 2$. Let $G \leq Aut(F/K)$ be a finite subgroup of automorphisms of F over K. Assume further that $char(K)$ and $|G|$ are coprime. Then, $|G| \leq 84(g-1)$

Proof.

Let $E = F^G$ be the fixed field of G. From Galois theorem we know that F/E is Galois and $[F : E] = |G| := n$. Furthermore, E/K is transcendental and is a function field over K. In class we saw that in these settings, there is only finitely many divisors in E that are ramified in F. Denote then by $\mathfrak{p}_1, \ldots, \mathfrak{p}_k$.

Hurwiz Theorem

Proof.

As $[F : E]$ is normal, we have that over $\mathfrak{p}_i$ there are r_i places, that have ramification of $e_i \geq 2$. The degree is always $f_i = 1$ as K is algebraically closed.

Proof.

As $[F:E]$ is normal, we have that over $\mathfrak{p}_i$ there are r_i places, that have ramification of $e_i \geq 2$. The degree is always $f_i = 1$ as K is algebraically closed. We have,

$$e_i f_i r_i = [F:E] \Rightarrow r_i = \frac{|G|}{e_i}.$$

Hurwiz Theorem

Proof.

As $[F : E]$ is normal, we have that over $\mathfrak{p}_i$ there are r_i places, that have ramification of $e_i \geq 2$. The degree is always $f_i = 1$ as K is algebraically closed. We have,

$$e_i f_i r_i = [F : E] \Rightarrow r_i = \frac{|G|}{e_i}.$$

As $e_i \mid |G|$, we get that $e_i, char(K)$ are coprime, so we can use Dedekind different theorem to deduce that for each $\mathfrak{P}_{i,j}$ over $\mathfrak{p}_i$,

$$d(\mathfrak{P}_{i,j}/\mathfrak{p}_i) = e_i - 1.$$

Hurwiz Theorem

Proof.

Apply the genus formula to deduce:

$$2(g-1) = [F:E]2(g_E-1) + \sum_{i=1}^{k}\sum_{j=1}^{r_i}(e_i-1)$$

$$2(g-1) = |G|2(g_E-1) + \sum_{i=1}^{k}\frac{|G|}{e_i}(e_i-1)$$

$$2(g-1) = |G|\left(2(g_E-1) + \sum_{i=1}^{k}\left(1-\frac{1}{e_i}\right)\right)$$

Hurwiz Theorem

Proof.

Apply the genus formula to deduce:

$$2(g-1) = [F:E]2(g_E-1) + \sum_{i=1}^{k}\sum_{j=1}^{r_i}(e_i-1)$$

$$2(g-1) = |G|2(g_E-1) + \sum_{i=1}^{k}\frac{|G|}{e_i}(e_i-1)$$

$$2(g-1) = |G|\left(2(g_E-1) + \sum_{i=1}^{k}\left(1-\frac{1}{e_i}\right)\right)$$

$$|G| = \frac{2(g-1)}{2(g_E-1) + \sum_{i=1}^{k}\left(1-\frac{1}{e_i}\right)}$$

We get that

Hurwiz Theorem

Proof.

$$|G| = \frac{2(g-1)}{2(g_E - 1) + \sum_{i=1}^{k}\left(1 - \frac{1}{e_i}\right)}.$$

Thus, we need to show that $\frac{2}{2(g_E-1)+\sum_{i=1}^{k}\left(1-\frac{1}{e_i}\right)} \leq 84$ or equivalently,

Hurwiz Theorem

Proof.

$$|G| = \frac{2(g-1)}{2(g_E-1)+\sum_{i=1}^{k}\left(1-\frac{1}{e_i}\right)}.$$

Thus, we need to show that $\frac{2}{2(g_E-1)+\sum_{i=1}^{k}\left(1-\frac{1}{e_i}\right)} \leq 84$ or equivalently,

$$R := 2(g_E-1)+\sum_{i=1}^{k}\left(1-\frac{1}{e_i}\right) \geq \frac{1}{41}$$

Hurwiz Theorem

Proof.

$$|G| = \frac{2(g-1)}{2(g_E - 1) + \sum_{i=1}^{k}\left(1 - \frac{1}{e_i}\right)}.$$

Thus, we need to show that $\frac{2}{2(g_E-1)+\sum_{i=1}^{k}\left(1-\frac{1}{e_i}\right)} \leq 84$ or equivalently,

$$R := 2(g_E - 1) + \sum_{i=1}^{k}\left(1 - \frac{1}{e_i}\right) \geq \frac{1}{41}$$

Note that $R > 0$ as $g \geq 2$.

Hurwiz Theorem

Proof.

$$|G| = \frac{2(g-1)}{2(g_E - 1) + \sum_{i=1}^{k}\left(1 - \frac{1}{e_i}\right)}.$$

Thus, we need to show that $\frac{2}{2(g_E-1)+\sum_{i=1}^{k}\left(1-\frac{1}{e_i}\right)} \leq 84$ or equivalently,

$$R := 2(g_E - 1) + \sum_{i=1}^{k}\left(1 - \frac{1}{e_i}\right) \geq \frac{1}{41}$$

Note that $R > 0$ as $g \geq 2$. Note that, $1 - \frac{1}{e_i} \in \{\frac{1}{2}, \frac{2}{3}, \frac{3}{4}, \frac{4}{5}...\}$

Hurwiz Theorem

Proof.

$$|G| = \frac{2(g-1)}{2(g_E-1)+\sum_{i=1}^{k}\left(1-\frac{1}{e_i}\right)}.$$

Thus, we need to show that $\frac{2}{2(g_E-1)+\sum_{i=1}^{k}\left(1-\frac{1}{e_i}\right)} \leq 84$ or equivalently,

$$R := 2(g_E-1)+\sum_{i=1}^{k}\left(1-\frac{1}{e_i}\right) \geq \frac{1}{41}$$

Note that $R > 0$ as $g \geq 2$. Note that, $1-\frac{1}{e_i} \in \{\frac{1}{2}, \frac{2}{3}, \frac{3}{4}, \frac{4}{5}...\}$, Finally if $g_E \geq 2$ then $R \geq 2$. Thus, we should only consider the possibilities of $g_E = 1, g_E = 0$.

Hurwiz Theorem

Proof.

$$|G| = \frac{2(g-1)}{2(g_E-1)+\sum_{i=1}^{k}\left(1-\frac{1}{e_i}\right)}.$$

Thus, we need to show that $\frac{2}{2(g_E-1)+\sum_{i=1}^{k}\left(1-\frac{1}{e_i}\right)} \leq 84$ or equivalently,

$$R := 2(g_E-1)+\sum_{i=1}^{k}\left(1-\frac{1}{e_i}\right) \geq \frac{1}{41}$$

Note that $R > 0$ as $g \geq 2$. Note that, $1-\frac{1}{e_i} \in \{\frac{1}{2}, \frac{2}{3}, \frac{3}{4}, \frac{4}{5}...\}$, Finally if $g_E \geq 2$ then $R \geq 2$. Thus, we should only consider the possibilities of $g_E = 1, g_E = 0$.
Case analysis on board. □