A "PROTO-PELLET’S FORMULA" FOR THE MÖBIUS FUNCTION

ARDAVAN AFSHAR

Abstract. We give a short proof of “Pellet’s Formula” for the Möbius Function on $\mathbb{F}_q[T]$, deriving an intermediate formula (which we call “Proto-Pellet’s Formula”) along the way. We then construct and prove an analogous “Proto-Pellet’s Formula” for the Möbius Function for a number field (including the usual Möbius function on the integers).

1. Introduction

Let $q$ be an odd prime power, and let $\mathcal{M} = \{f \in \mathbb{F}_q[T] : f \text{ monic}\}$. Define the Möbius Function on $\mathcal{M}$ by

$$\mu(f) = \begin{cases} (-1)^r & \text{if } f = p_1 \cdots p_r \text{ distinct primes} \\ 0 & \text{else} \end{cases}$$

for $f \in \mathcal{M}$, in analogy with the usual Möbius Function on the integers. In $\mathcal{M}$ we have the following formula for $\mu$.

Theorem 1 (“Pellet’s Formula”). Let $f \in \mathcal{M}$, and let $\chi$ be the quadratic character on $\mathbb{F}_q$. Then

$$\mu(f) = (-1)^{\deg f} \chi(\text{disc } f)$$

a proof of which can be found, for example, as Lemma 4.1 in [Con1]. This is an important ingredient in the setting of $\mathbb{F}_q[T]$, such as in Sawin and Shusterman’s proof of the Chowla and Twin Prime conjectures in $\mathbb{F}_q[T]$ (see [S-S]).

We give another short proof of this formula, and in proving it, we derive an intermediate formula, which we call “Proto-Pellet’s Formula”. Let $\text{Frob}_q$ be the Frobenius element on $\mathbb{F}_q$, which sends $\alpha$ to $\alpha^q$, then we have

Theorem 2 (“Proto-Pellet’s Formula”). Let $f \in \mathcal{M}$ square free, then

$$\mu(f) = (-1)^{\deg f} \text{sign}(\text{Frob}_q|f)$$

where $\text{Frob}_q|f$ denotes the action of $\text{Frob}_q$ on the roots of $f$.

We then construct and prove an analogue of this formula for the Möbius Function for any number field $A/\mathbb{Q}$, which we define as follows. Let $\mathcal{O}_A$ be the ring of integers in $A$, and let $\mathcal{I}_A$ be the set of non-zero ideals in $\mathcal{O}_A$. Then the Möbius Function for $A/\mathbb{Q}$, $\mu_A : \mathcal{I}_A \to \{-1, 0, 1\}$ is defined by

$$\mu_A(I) = \begin{cases} (-1)^r & \text{if } I = p_1 \cdots p_r \text{ distinct prime ideals} \\ 0 & \text{else} \end{cases}$$

so that $\mu_A = \mu$ is the usual Möbius Function on the integers. To do this, we first pick some arbitrary additive function $\nu : \mathcal{I}_A \to \mathbb{N}$ to mimic the role of degree in $\mathbb{F}_q[T]$, and for each prime ideal $p$ we construct a polynomial $f_{p, \nu}$ whose Galois group is isomorphic to $\mathbb{Z}/\nu(p)\mathbb{Z}$ and generated by some homomorphism $\sigma_{p, \nu}$. We then lift these homomorphisms to an appropriate profinite Galois group and compose them to get a homomorphism $\sigma_\nu$ (which mimics the role of $\text{Frob}_q$ in $\mathbb{F}_q[T]$), and set $f_{I, \nu} = \prod_{p | I \text{ prime}} f_{p, \nu}$ to prove

Theorem 3 (“Proto-Pellet’s Formula” for number fields). Let $\nu : \mathcal{I}_A \to \mathbb{N}$ be an additive function. Then there exists a Galois homomorphism $\sigma_\nu \in \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ and a family of polynomials $(f_{I, \nu})_{I \in \mathcal{I}_A}$ such that, for all $I \in \mathcal{I}_A$ square-free

$$\mu_A(I) = (-1)^{\nu(I)} \text{sign}(\sigma_\nu|f_{I, \nu})$$

where $\sigma_\nu|f$ denotes the action of $\sigma_\nu$ on the roots of $f$. 

1
We begin with a proof of Theorem 2.

**Proof of Theorem 2.** For a square-free polynomial \( f = p_1 \cdots p_r \in \mathcal{M} \), notice that \( \text{Frob}_q \) acts on the roots of \( f \) as a product of cycles \( \tau_1, \ldots, \tau_r \), where \( \tau_i \) permutes the roots of \( p_i \) as a cycle of length \( \deg p_i \). This means that 
\[
\text{sign}(\text{Frob}_q|f) = (-1)^{\deg p_1 - 1} \cdots (-1)^{\deg p_r - 1} = (-1)^{\deg f - r}.
\]

To move from this to Pellet’s formula, we first define

**Definition 2.1.** For a polynomial \( f \), let \( \text{Aut}(f) \) be the automorphism group on the roots of \( f \) and let \( \text{Gal}(f) \) be its Galois closure. Let \( \text{Sym}(f) \) be the symmetric group, and \( \text{Alt}(f) \) the alternating group, on the roots of \( f \).

and then prove an auxiliary result

**Proposition 2.2.** Let \( K \) be a field and \( f \in K[T] \) square-free, and let \( \rho_f : \text{Gal}(f) \hookrightarrow \text{Sym}(f) \) be the natural inclusion map. Then \( \rho_f(\text{Gal}(f)) \subseteq \text{Alt}(f) \iff \text{disc} f \text{ is a square in } K^\times. \)

**Proof.** Let \( f \) have roots \( \alpha_1, \ldots, \alpha_n \in \overline{K} \) so that \( \text{disc} f = \text{disc}_K f = \prod_{i<j} (\alpha_i - \alpha_j)^2 \). Then we have that 
\[
\text{disc} f \text{ is a square in } K^\times \iff \forall \sigma \in \text{Gal}(f) \quad \sigma(\sqrt{\text{disc} f}) = \sqrt{\text{disc} f}
\]

\[
\iff \forall \sigma \in \text{Gal}(f) \quad \sigma \left( \prod_{i<j} (\alpha_i - \alpha_j) \right) = \prod_{i<j} (\alpha_i - \alpha_j)
\]

\[
\iff \forall \sigma \in \text{Gal}(f) \quad \prod_{i<j} (\alpha_i - \alpha_j) = \left( \prod_{i<j} \sigma(\alpha_i) - \sigma(\alpha_j) \right) = \text{sign}(\sigma) \prod_{i<j} (\alpha_i - \alpha_j)
\]

\[
\iff \forall \sigma \in \text{Gal}(f) \quad \text{sign}(\sigma) = 1.
\]

**Corollary 2.3.** Let \( f \in \mathcal{M} \) square-free, and let \( \chi \) be the quadratic character on \( \mathbb{F}_q \). Then 
\[
\text{sign}(\text{Frob}_q|f) = \chi(\text{disc} f)
\]

**Proof.** Let \( f \in \mathcal{M} \) square-free, \( \text{Gal}(f) \) is generated by \( \text{Frob}_q \), so by Proposition 2.2 we have that 
\[
\text{disc} f \text{ is a square in } \mathbb{F}_q^\times \iff \text{sign}(\text{Frob}_q|f) = 1
\]

from which the corollary follows.

So, combining Theorem 2 with Corollary 2.3 and noting that the discriminant vanishes on non-square-free polynomials, we get a proof of Theorem 1.

### 3. “Proto-Pellet’s Formula” in number fields

To begin, we pick some additive function \( \nu : \mathcal{I}_A \to \mathbb{N} \) to mimic the role of degree in \( \mathbb{F}_q[T] \).

Let \( \mathcal{P}_A \) be the set of prime ideals in \( A \), and put some order relation \( <_A \) on \( \mathcal{P}_A \): for example, one can order the prime ideals first by the size of their norm and then order those with the same norm arbitrarily (since there are only finitely many). For \( p \) a prime ideal, pick \( q = q(p, \nu) \) to be the minimal prime such that \( q \equiv 1 \mod \nu(p) \) and \( q \neq q(p', \nu) \) for some \( p' <_A p \) prime (which is always possible, by Dirichlet’s Theorem for primes in arithmetic progression). Then consider \( L = L_{p, \nu} = \mathbb{Q}(\zeta_q) \) where \( \zeta_q = e^{2\pi i/q} \) and note that \( \text{Gal}(L/\mathbb{Q}) \cong \mathbb{Z}/(q - 1)\mathbb{Z} \). So, since \( \nu(p) \) divides \( q - 1 \), there is some subgroup \( H \) of \( \text{Gal}(L/\mathbb{Q}) \) such that \( H \cong \mathbb{Z}/(\nu(p))/\mathbb{Z} \). Therefore, if we let \( K = K_{p, \nu} = L^H := \{ x \in L \mid \sigma(x) = x \ \forall \sigma \in H \} \), we know by the Galois Correspondence that \( \text{Gal}(K/\mathbb{Q}) \cong \mathbb{Z}/\nu(p)/\mathbb{Z} \).

Moreover, by the Primitive Element Theorem, there exists some \( \alpha_{p, \nu} \in L \) such that \( K = \mathbb{Q}(\alpha_{p, \nu}) \). So, if we let \( f_{p, \nu} \) be the minimal polynomial of \( \alpha_{p, \nu} \), then we have that \( \text{Gal}(f_{p, \nu}) \cong \mathbb{Z}/\nu(p)/\mathbb{Z} \) and is generated by some \( \sigma_{p, \nu} \) which acts as a \( \nu(p) \)-cycle on the roots of \( f_{p, \nu} \). In particular, this means that 
\[
\text{sign}(\sigma_{p, \nu}|f_{p, \nu}) = (-1)^{\nu(p) - 1}.
\]
Next, let $K_ν = \mathbb{Q}(\{α_{p, ν} \mid p \in \mathcal{P}_A\})$ and extend each $σ_{p, ν}$ to a map $σ_{p, ν} : Gal(K_ν/\mathbb{Q})$ by

$$
σ_{p, ν}(α_{p', ν}) = \begin{cases} 
σ_{p, ν}(α_{p, ν}) & \text{if } p = p' \\
α_{p', ν} & \text{if } p \neq p'
\end{cases}
$$

The fact that we can do this follows from Proposition 3.1. Then consider $σ_ν \in Gal(K_ν/\mathbb{Q})$ defined by $σ_ν(α_{p, ν}) = σ_{p, ν}(α_{p, ν})$ for all prime ideals $p \in \mathcal{P}_A$, so that by construction we have that $\text{sign}(σ_ν|f_{p, ν}) = \text{sign}(σ_{p, ν}|f_{p, ν})$. We observe that $σ_ν$ is well-defined by noting that it is a composition of the $σ_{p, ν}$ over all prime ideals $p \in \mathcal{P}_A$.

We take a brief aside to prove Proposition 3.1 as promised:

**Proposition 3.1.** Let $α_{p, ν}$ and $σ_{p, ν}$ be defined as above. Let $\{p, p_1, \cdots, p_k\}$ be a set of distinct prime ideals in $\mathcal{P}_A$. Then we can extend $σ_{p, ν}$ to a map $σ_{p, ν}^{(k)} \in Gal(\mathbb{Q}(\{α_{p', ν} \mid p' \in \{p, p_1, \cdots, p_k\}\})/\mathbb{Q})$ by

$$
σ_{p, ν}^{(k)}(α_{p', ν}) = \begin{cases} 
σ_{p, ν}(α_{p, ν}) & \text{if } p = p' \\
α_{p', ν} & \text{if } p' \in \{p_1, \cdots, p_k\}
\end{cases}
$$

**Proof.** We proceed by induction and note that the case $k = 0$ is trivially true. Suppose that the case $k = l$ is true, so that we have constructed our desired function $σ_{p, ν}$ on $K^{(l)}$, where $K^{(m)} := \mathbb{Q}(\{α_{p', ν} \mid p' \in \{p, p_1, \cdots, p_m\}\})$, and we seek to extend this to $σ_{p, ν}^{(l+1)}$ on $K^{(l+1)}$. Let $K = \mathbb{Q}(α_{p_1, ν})$ so that $K^{(l+1)} = K^{(l)}K$, and so that, by Theorem 1.1 of [Con2] there is an injective homomorphism

$$ρ : Gal(K^{(l+1)}/\mathbb{Q}) = Gal(K^{(l)}K/\mathbb{Q}) \to Gal(K^{(l)}/\mathbb{Q}) \times Gal(K/\mathbb{Q})$$

given by $ρ(σ) = (σ|_{K^{(l)}}, σ|_{K})$. If we can show that $ρ$ is an isomorphism, then we can set $σ_{p, ν}^{(l+1)} = ρ^{-1}(σ_{p, ν}^{(l)}, l)$ (where $l$ is the identity function) and then we are done.

So suppose that $ρ$ is not an isomorphism, which means that $|Gal(K^{(l+1)}/\mathbb{Q})| < |Gal(K^{(l)}/\mathbb{Q})||Gal(K/\mathbb{Q})|$ and so $[K^{(l+1)} : \mathbb{Q}] < [K^{(l)} : \mathbb{Q}][K : \mathbb{Q}]$. Now define $L^{(m)} = \mathbb{Q}(\{ζ_{q(p', ν)} \mid p' \in \{p, p_1, \cdots, p_m\}\})$ (where $q(p, ν)$ is defined as above) and observe that, by our assumption

$$[L^{(l+1)} : \mathbb{Q}] = [L^{(l+1)} : K^{(l+1)}][K^{(l+1)} : \mathbb{Q}] < [L^{(l+1)} : K^{(l+1)}][K^{(l)} : \mathbb{Q}][K : \mathbb{Q}]$$

and we can recursively compute

$$[L^{(l+1)} : K^{(l+1)}] = [L^{(l)}(ζ_{q(p_1, ν)}), L^{(l)}(ζ_{q(p_1, ν)}), \cdots, L^{(l)}(ζ_{q(p_1, ν)})] = \begin{pmatrix}
q(p_1, ν) - 1 & 1 & \cdots & 1 \\
1 & q(p_1, ν) - 1 & \cdots & 1 \\
\vdots & \ddots & \ddots & \vdots \\
1 & \cdots & 1 & q(p_1, ν) - 1
\end{pmatrix}
$$

and so

$$[L^{(l+1)} : \mathbb{Q}] \leq \begin{pmatrix}
q(p_1, ν) - 1 & 1 & \cdots & 1 \\
1 & q(p_1, ν) - 1 & \cdots & 1 \\
\vdots & \ddots & \ddots & \vdots \\
1 & \cdots & 1 & q(p_1, ν) - 1
\end{pmatrix}
$$

But, since $\{q(p', ν) \mid p' \in \{p, p_1, \cdots, p_{l+1}\}\}$ is a set of distinct primes, $\mathbb{Q}(\{ζ_{q(p', ν)} \mid p' \in \{p, p_1, \cdots, p_{l+1}\}\}) = \mathbb{Q}(ζ_{q(p_1, ν)}) - q(p_1, ν) - 1 = q(p_1, ν) - 1)$, which is a contradiction.

To put this all together, for $I \in \mathcal{I}_A$ we define $f_{I, ν} = \prod_{p \in \mathcal{P}_A \setminus \mathcal{P}_I} f_{p, ν}$, where the product counts prime ideals with multiplicity. This allows us to formulate the following analogue of a “Proto-Pellet’s Formula” for the Möbius function for $A$:

**Theorem 3.2.** Let $ν : \mathcal{I}_A \to \mathbb{N}$ be an additive function, and $I \in \mathcal{I}_A$ square-free. Then for $σ_ν$ and $f_{I, ν}$ as defined above, we have:

$$μ(I) = (-1)^{ν(I)} \text{sign}(σ_ν|f_{I, ν})$$
Proof. For $I \in \mathcal{I}_A$ square-free we have that $I = p_1 \cdots p_r$ for some distinct prime ideals $p_1, \cdots, p_r \in \mathcal{P}_A$ and so

$$\text{sign}(\sigma_{\nu}|f_{I,\nu}) = \prod_{p \in \mathcal{P}_A : p | I} \text{sign}(\sigma_{\nu}|f_{p,\nu}) = \prod_{p \in \mathcal{P}_A : p | I} (-1)^{\nu(p)-1} = (-1)^{\nu(I)-r} = (-1)^{\nu(n)}\mu(I)$$

Theorem 3 now follows as an immediate corollary.

Finally, we consider the trivial example as a check

Example 3.3. Let $\nu = \omega_A$ where $\omega_A(I) = \# \{ p \in \mathcal{P}_A : p | I \}$ so that $\omega_A(p) = 1$ for all prime ideals $p \in \mathcal{P}_A$. Then for each $p$, $\text{Gal}(\mathbb{F}_p/\mathbb{Q}) \cong \mathbb{Z}/\omega_A(p)\mathbb{Z}$ is trivial and $\sigma_{p,\omega_A}$ is just the identity map, which means that $\text{sign}(\sigma_{p,\omega_A}|f_{p,\omega_A}) = 1$. Therefore, for all square-free $I \in \mathcal{I}_A$, we have that $\text{sign}(\sigma_{\omega_A}|f_{I,\omega_A}) = 1$, which by Theorem 3.2 implies that $\mu_A(I) = (-1)^{\omega_A(I)}$, recovering the definition of $\mu_A$.

Acknowledgements

The author would like to thank Andrew Granville for his guidance, and Richard Hill for useful discussions. The research leading to these results has received funding from the European Research Council under the European Union’s Seventh Framework Programme (FP7/2007-2013), ERC grant agreement n° 670239.

References

[Con1] K. Conrad, *Irreducible values of polynomials: a non-analogy*, Number Fields and Function Fields: Two Parallel Worlds, 71-85, Progress in Mathematics, 239, Birkhauser, Basel, 2005.
[Con2] K. Conrad, *The Galois Correspondence at work*, https://kconrad.math.uconn.edu/blurbs/galoistheory/galoiscorrthms.pdf (retrieved 15 January 2020).
[S-S] W. Sawin, M. Shusterman, *On the Chowla and Twin Prime conjectures over $\mathbb{F}_q[T]$*, preprint, [arXiv:1808.04001], 2018.

Department of Mathematics, University College London, 25 Gordon Street, London, England

E-mail address: ardavan.afshar.15@ucl.ac.uk