Recursively Enumerable Subsets of $\mathbb{F}_q[Z]$

Jeroen Demeyer

Result

- Let $\mathbb{F}_q$ be the finite field with q elements, $q = p^h$, p prime ≥ 2.

Result

- Let $\mathbb{F}_q$ be the finite field with q elements, $q = p^h$, p prime ≥ 2.
- Theorem. Every recursively enumerable subset of $\mathbb{F}_q[Z]$ is Diophantine over $\mathbb{F}_q[W, Z]$.

Result

- Let $\mathbb{F}_q$ be the finite field with q elements, $q = p^h$, p prime ≥ 2.
- Theorem. Every recursively enumerable subset of $\mathbb{F}_q[Z]$ is Diophantine over $\mathbb{F}_q[W, Z]$.
- In the proof, I worked as much as possible in $\mathbb{F}_q[Z]$, there is only one place where I need the extra variable W.

Result

- Let $\mathbb{F}_q$ be the finite field with q elements, $q = p^h$, p prime ≥ 2.
- Theorem. Every recursively enumerable subset of $\mathbb{F}_q[Z]$ is Diophantine over $\mathbb{F}_q[W, Z]$.
- In the proof, I worked as much as possible in $\mathbb{F}_q[Z]$, there is only one place where I need the extra variable W.
- Eventually, one would like to prove that every r.e. subset of $\mathbb{F}_q[Z]$ is Diophantine over $\mathbb{F}_q[Z]$. This would be the analogon of DPRM for $\mathbb{F}_q[Z]$.

What was known

- Undecidability for $\mathbb{F}_q[Z]$ (Denef 79), by constructing a Diophantine model of $\mathbb{Z}$ using the Chebyshev polynomials.
  These are the solutions X_n, Y_n to the Pell equation

$$X^2 - (Z^2 - 1)Y^2 = 1$$

What was known

- Undecidability for $\mathbb{F}_q[Z]$ (Denef 79), by constructing a Diophantine model of $\mathbb{Z}$ using the Chebyshev polynomials.
  These are the solutions X_n, Y_n to the Pell equation

$$X^2 - (Z^2 - 1)Y^2 = 1$$

- Recursively enumerable sets are known to be Diophantine in
  - $\mathbb{Z}$ (DPRM 70).
  - $\mathcal{O}_K$ when $\mathbb{Z}$ is Diophantine in $\mathcal{O}_K$.
  - $\mathbb{Z}[Z]$ (Denef 79).
  - $\mathcal{O}_K[Z_1, \ldots, Z_n]$ with K a totally real number field (Zahidi 99).

3 steps

- Define a Diophantine model of $\mathbb{N}$ in $\mathbb{F}_q[Z]$.
  We will use $n \mapsto Z^n$.

3 steps

- Define a Diophantine model of $\mathbb{N}$ in $\mathbb{F}_q[Z]$.
  We will use $n \mapsto Z^n$.
- Show that we can solve the problem using a bounded universal quantifier.

3 steps

- Define a Diophantine model of $\mathbb{N}$ in $\mathbb{F}_q[Z]$.
  We will use $n \mapsto Z^n$.
- Show that we can solve the problem using
  a bounded universal quantifier.
- Hard part: eliminate the bounded universal quantifier
  (loosely based on the proof of DPRM).

A model of $\mathbb{N}$ in $\mathbb{F}_q[Z]$

- Let $n \in \mathbb{N}$ correspond with $Z^n \in \mathbb{F}_q[Z]$.

A model of $\mathbb{N}$ in $\mathbb{F}_q[Z]$

- Let $n \in \mathbb{N}$ correspond with $Z^n \in \mathbb{F}_q[Z]$.
- Constructed from the Chebyshev polynomials using

$$T^n = X_n \circ \left(\frac{T + T^{-1}}{2}\right) + \frac{T - T^{-1}}{2} Y_n \circ \left(\frac{T + T^{-1}}{2}\right)$$

A model of $\mathbb{N}$ in $\mathbb{F}_q[Z]$

- Let $n \in \mathbb{N}$ correspond with $Z^n \in \mathbb{F}_q[Z]$.
- Constructed from the Chebyshev polynomials using

$$T^n = X_n \circ \left(\frac{T + T^{-1}}{2}\right) + \frac{T - T^{-1}}{2} Y_n \circ \left(\frac{T + T^{-1}}{2}\right)$$

- T^{-1} is not a polynomial, but we can take a polynomial S to be the 'formal' inverse of T, and work modulo $TS - 1$.

A model of $\mathbb{N}$ in $\mathbb{F}_q[Z]$

- Let $n \in \mathbb{N}$ correspond with $Z^n \in \mathbb{F}_q[Z]$.
- Constructed from the Chebyshev polynomials using

$$T^n = X_n \circ \left(\frac{T + T^{-1}}{2}\right) + \frac{T - T^{-1}}{2} Y_n \circ \left(\frac{T + T^{-1}}{2}\right)$$

- T^{-1} is not a polynomial, but we can take a polynomial S to be the 'formal' inverse of T, and work modulo $TS - 1$.
- If S is large enough, then we can define T^n as the element of the congruence class of $T^n \bmod TS - 1$ having 'small' degree.

A model of $\mathbb{N}$ in $\mathbb{F}_q[Z]$

- Let $n \in \mathbb{N}$ correspond with $Z^n \in \mathbb{F}_q[Z]$.
- Constructed from the Chebyshev polynomials using

$$T^n = X_n \circ \left(\frac{T + T^{-1}}{2}\right) + \frac{T - T^{-1}}{2} Y_n \circ \left(\frac{T + T^{-1}}{2}\right)$$

- T^{-1} is not a polynomial, but we can take a polynomial S to be the 'formal' inverse of T, and work modulo $TS - 1$.
- If S is large enough, then we can define T^n as the element of the congruence class of $T^n \bmod TS - 1$ having 'small' degree.
- With some more work, we can define the exponential

$$(T, Z^n) \mapsto T^n$$

Defining the n-th polynomial

- $\mathbb{F}_q[Z]$ is countable, so we can enumerate

$$\mathbb{F}_q[Z] = \{P^{(0)}, P^{(1)}, P^{(2)}, \dots\}$$

Defining the n-th polynomial

- $\mathbb{F}_q[Z]$ is countable, so we can enumerate

$$\mathbb{F}_q[Z] = \{P^{(0)}, P^{(1)}, P^{(2)}, \dots\}$$

- For all recursively enumerable sets in $\mathbb{F}_q[Z]$ to be Diophantine, it suffices that the relation "X is the n-th polynomial" ($X = P^{(n)}$) is Diophantine.

Defining the n-th polynomial

- $\mathbb{F}_q[Z]$ is countable, so we can enumerate

$$\mathbb{F}_q[Z] = \{P^{(0)}, P^{(1)}, P^{(2)}, \dots\}$$

- For all recursively enumerable sets in $\mathbb{F}_q[Z]$ to be Diophantine, it suffices that the relation "X is the n-th polynomial" ($X = P^{(n)}$) is Diophantine.
- Let $\mathcal{S}$ be a r.e. subset of $\mathbb{F}_q[Z]$. This means that the set $\mathcal{S}^\theta := \{n \in \mathbb{N} \mid P^{(n)} \in \mathcal{S}\}$ is r.e., by DPRM it is Diophantine.

Defining the n-th polynomial

- $\mathbb{F}_q[Z]$ is countable, so we can enumerate

$$\mathbb{F}_q[Z] = \{P^{(0)}, P^{(1)}, P^{(2)}, \dots\}$$

- For all recursively enumerable sets in $\mathbb{F}_q[Z]$ to be Diophantine, it suffices that the relation "X is the n-th polynomial" ($X = P^{(n)}$) is Diophantine.
- Let $\mathcal{S}$ be a r.e. subset of $\mathbb{F}_q[Z]$. This means that the set $\mathcal{S}^\theta := \{n \in \mathbb{N} \mid P^{(n)} \in \mathcal{S}\}$ is r.e., by DPRM it is Diophantine.
  Then for $X \in \mathbb{F}_q[Z]$ we have

$$X \in \mathcal{S} \iff (\exists n)(X = P^{(n)} \ \wedge \ n \in \mathcal{S}^\theta)$$

Bounded universal quantifiers

- The bounded universal quantifier (b.u.q.) $(\forall k)_{\leq y}$ means "for all $k = 0, 1, \ldots, y$".

Bounded universal quantifiers

- The bounded universal quantifier (b.u.q.) $(\forall k)_{\leq y}$ means "for all $k = 0, 1, \ldots, y$".
- It is easy to define "X is the n-th polynomial" using existential quantifiers and one b.u.q.
  The idea is that a degree d polynomial can be defined with $d + 1$ equations.

Bounded universal quantifiers

- The bounded universal quantifier (b.u.q.) $(\forall k)_{\leq y}$ means "for all $k = 0, 1, \ldots, y$".
- It is easy to define "X is the n-th polynomial" using existential quantifiers and one b.u.q.
  The idea is that a degree d polynomial can be defined with $d + 1$ equations.
- The conclusion so far is that we 'only' need to get rid of this b.u.q. to prove the main theorem.

Cyclotomic polynomials

- **Definition.** The n-th cyclotomic polynomial $\Phi_n \in \mathbb{Z}[Z]$ is the minimal polynomial of a primitive n-th root of unity ζ_n:

$$\Phi_n(Z) = \prod_{k \in (\mathbb{Z}/n\mathbb{Z})^*} (Z - \zeta_n^k)$$

Cyclotomic polynomials

- **Definition.** The n-th cyclotomic polynomial $\Phi_n \in \mathbb{Z}[Z]$ is the minimal polynomial of a primitive n-th root of unity ζ_n:

$$\Phi_n(Z) = \prod_{k \in (\mathbb{Z}/n\mathbb{Z})^*} (Z - \zeta_n^k)$$

- These satisfy

$$Z^n - 1 = \prod_{d|n} \Phi_d(Z)$$

Cyclotomic polynomials

- Definition. The n-th cyclotomic polynomial $\Phi_n \in \mathbb{Z}[Z]$ is the minimal polynomial of a primitive n-th root of unity ζ_n:

$$\Phi_n(Z) = \prod_{k \in (\mathbb{Z}/n\mathbb{Z})^*} (Z - \zeta_n^k)$$

- These satisfy

$$Z^n - 1 = \prod_{d|n} \Phi_d(Z)$$

- If n is prime, we can Diophantinely define Φ_n as

$$X = \Phi_n \leftrightarrow (Z-1)X = Z^n - 1$$

(recall we had a model of $\mathbb{N}$ given by $n \mapsto Z^n$)

Cyclotomic polynomials over $\mathbb{F}_q$

- The cyclotomic polynomials are irreducible in $\mathbb{Z}[Z]$.
  Usually they factor in $\mathbb{F}_q[Z]$,
  but always in factors of equal degree.

Cyclotomic polynomials over $\mathbb{F}_q$

- The cyclotomic polynomials are irreducible in $\mathbb{Z}[Z]$.
  Usually they factor in $\mathbb{F}_q[Z]$,
  but always in factors of equal degree.
- Let a and b be primes with $b \nmid q-1$.
  The following are equivalent:
  - $a | \Phi_b(q)$.
  - The order of q in the group $(\mathbb{Z}/a\mathbb{Z})^*$ is equal to b.
  - All the factors of Φ_a over $\mathbb{F}_q$ have degree b.

Cyclotomic polynomials over $\mathbb{F}_q$

- The cyclotomic polynomials are irreducible in $\mathbb{Z}[Z]$. Usually they factor in $\mathbb{F}_q[Z]$, but always in factors of equal degree.
- Let a and b be primes with $b \nmid q-1$. The following are equivalent:
  - $a | \Phi_b(q)$.
  - The order of q in the group $(\mathbb{Z}/a\mathbb{Z})^*$ is equal to b.
  - All the factors of Φ_a over $\mathbb{F}_q$ have degree b.
- We can use this to find cyclotomic polynomials having factors of a prescribed degree.

Cyclotomic polynomials over $\mathbb{F}_q$

- The cyclotomic polynomials are irreducible in $\mathbb{Z}[Z]$.
  Usually they factor in $\mathbb{F}_q[Z]$,
  but always in factors of equal degree.
- Let a and b be primes with $b \nmid q-1$.
  The following are equivalent:
  - $a | \Phi_b(q)$.
  - The order of q in the group $(\mathbb{Z}/a\mathbb{Z})^*$ is equal to b.
  - All the factors of Φ_a over $\mathbb{F}_q$ have degree b.
- We can use this to find cyclotomic polynomials having factors of a prescribed degree.
  Example: degree 19 over $\mathbb{F}_{25}$.
  - $\Phi_{19}(25) = 191 \cdot 761 \cdot 6271 \cdot 19609 \cdot 213029 \cdot 3981071$.
  - $\Phi_{191}(Z)$ has 10 factors of degree 19 in $\mathbb{F}_{25}[Z]$.

Eliminating the bounded universal quantifier

Goal. Prove that the formula

$$(\forall k)_{\leq y}(\exists X_1, \ldots, X_m)\big(\Gamma(Z^y, Z^k, F_1, \ldots, F_n, X_1, \ldots, X_m) = 0\big)$$

is equivalent with a Diophantine formula (only $\exists$ quantifiers).

Eliminating the bounded universal quantifier

Goal. Prove that the formula

$$(\forall k)_{\leq y}(\exists X_1, \ldots, X_m)\big(\Gamma(Z^y, Z^k, F_1, \ldots, F_n, X_1, \ldots, X_m) = 0\big)$$

is equivalent with a Diophantine formula (only $\exists$ quantifiers).

- Let $\bar{X}^{(k)}$ $(0 \leq k \leq y)$ denote the solution vector to

$$\Gamma(Z^y, Z^k, \bar{F}, \bar{X}^{(k)}) = 0$$

Eliminating the bounded universal quantifier

Goal. Prove that the formula

$$(\forall k)_{\leq y}(\exists X_1, \ldots, X_m)\big(\Gamma(Z^y, Z^k, F_1, \ldots, F_n, X_1, \ldots, X_m) = 0\big)$$

is equivalent with a Diophantine formula (only $\exists$ quantifiers).

- Let $\bar{X}^{(k)}$ $(0 \leq k \leq y)$ denote the solution vector to

$$\Gamma(Z^y, Z^k, \bar{F}, \bar{X}^{(k)}) = 0$$

- Encode the $\bar{X}^{(k)}$ using the Chinese remainder theorem as $\bar{A} \equiv \bar{X}^{(k)} \bmod \Phi_{a_k}$, where a_k is a 'large' prime.

Eliminating the bounded universal quantifier

Goal. Prove that the formula

$$(\forall k)_{\leq y}(\exists X_1, \ldots, X_m)\big(\Gamma(Z^y, Z^k, F_1, \ldots, F_n, X_1, \ldots, X_m) = 0\big)$$

is equivalent with a Diophantine formula (only $\exists$ quantifiers).

- Let $\bar{X}^{(k)}$ $(0 \leq k \leq y)$ denote the solution vector to

$$\Gamma(Z^y, Z^k, \bar{F}, \bar{X}^{(k)}) = 0$$

- Encode the $\bar{X}^{(k)}$ using the Chinese remainder theorem as $\bar{A} \equiv \bar{X}^{(k)} \bmod \Phi_{a_k}$, where a_k is a 'large' prime.
- Note that $Z^k \equiv Z^c \bmod \Phi_{a_k}$ iff $k \equiv c \bmod a_k$.

Eliminating the bounded universal quantifier

- Let $\bar{X}^{(k)}$ $(0 \leq k \leq y)$ denote the solution vector to

$$\Gamma(Z^y, Z^k, \bar{F}, \bar{X}^{(k)}) = 0$$

- Encode the $\bar{X}^{(k)}$ using the Chinese remainder theorem as $\bar{A} \equiv \bar{X}^{(k)} \bmod \Phi_{a_k}$, where a_k is a 'large' prime.
- Note that $Z^k \equiv Z^c \bmod \Phi_{a_k}$ iff $k \equiv c \bmod a_k$.

Take such a $\bar{A}$ and c, then

$$\begin{cases} \Gamma(Z^y, Z^0, \bar{F}, \bar{X}^{(0)}) = 0 \\ \Gamma(Z^y, Z^1, \bar{F}, \bar{X}^{(1)}) = 0 \\ \vdots \\ \Gamma(Z^y, Z^y, \bar{F}, \bar{X}^{(y)}) = 0 \end{cases} \Rightarrow \begin{cases} \Gamma(Z^y, Z^c, \bar{F}, \bar{A}) \equiv 0 \bmod \Phi_{a_0} \\ \Gamma(Z^y, Z^c, \bar{F}, \bar{A}) \equiv 0 \bmod \Phi_{a_1} \\ \vdots \\ \Gamma(Z^y, Z^c, \bar{F}, \bar{A}) \equiv 0 \bmod \Phi_{a_y} \end{cases}$$

Eliminating the bounded universal quantifier

- Encode the $\bar{X}^{(k)}$ using the Chinese remainder theorem as $\bar{A} \equiv \bar{X}^{(k)} \bmod \Phi_{a_k}$, where a_k is a 'large' prime.
- Note that $Z^k \equiv Z^c \bmod \Phi_{a_k}$ iff $k \equiv c \bmod a_k$.

Take such a $\bar{A}$ and c, then

$$\begin{cases} \Gamma(Z^y, Z^0, \bar{F}, \bar{X}^{(0)}) = 0 \\ \Gamma(Z^y, Z^1, \bar{F}, \bar{X}^{(1)}) = 0 \\ \vdots \\ \Gamma(Z^y, Z^y, \bar{F}, \bar{X}^{(y)}) = 0 \end{cases} \Rightarrow \begin{cases} \Gamma(Z^y, Z^c, \bar{F}, \bar{A}) \equiv 0 \bmod \Phi_{a_0} \\ \Gamma(Z^y, Z^c, \bar{F}, \bar{A}) \equiv 0 \bmod \Phi_{a_1} \\ \vdots \\ \Gamma(Z^y, Z^c, \bar{F}, \bar{A}) \equiv 0 \bmod \Phi_{a_y} \end{cases}$$

$$\Rightarrow \Gamma(Z^y, Z^c, \bar{F}, \bar{A}) \equiv 0 \bmod \Phi_{a_0}\Phi_{a_1}\ldots\Phi_{a_y}$$

Eliminating the bounded universal quantifier

Take such a $\bar{A}$ and c, then

$$\begin{cases} \Gamma(Z^y, Z^0, \bar{F}, \bar{X}^{(0)}) = 0 \\ \Gamma(Z^y, Z^1, \bar{F}, \bar{X}^{(1)}) = 0 \\ \vdots \\ \Gamma(Z^y, Z^y, \bar{F}, \bar{X}^{(y)}) = 0 \end{cases} \Rightarrow \begin{cases} \Gamma(Z^y, Z^c, \bar{F}, \bar{A}) \equiv 0 \bmod \Phi_{a_0} \\ \Gamma(Z^y, Z^c, \bar{F}, \bar{A}) \equiv 0 \bmod \Phi_{a_1} \\ \vdots \\ \Gamma(Z^y, Z^c, \bar{F}, \bar{A}) \equiv 0 \bmod \Phi_{a_y} \end{cases}$$

$$\Rightarrow \Gamma(Z^y, Z^c, \bar{F}, \bar{A}) \equiv 0 \bmod \Phi_{a_0}\Phi_{a_1}\ldots\Phi_{a_y}$$

- We want the direction "$\Leftarrow$" also to hold. This will be the case if we can bound the degree of $\Gamma(Z^y, Z^k, \bar{F}, \bar{X}^{(k)})$.

Eliminating the bounded universal quantifier

Take such a $\bar{A}$ and c, then

$$\begin{cases} \Gamma(Z^y, Z^0, \bar{F}, \bar{X}^{(0)}) = 0 \\ \Gamma(Z^y, Z^1, \bar{F}, \bar{X}^{(1)}) = 0 \\ \vdots \\ \Gamma(Z^y, Z^y, \bar{F}, \bar{X}^{(y)}) = 0 \end{cases} \Rightarrow \begin{cases} \Gamma(Z^y, Z^c, \bar{F}, \bar{A}) \equiv 0 \bmod \Phi_{a_0} \\ \Gamma(Z^y, Z^c, \bar{F}, \bar{A}) \equiv 0 \bmod \Phi_{a_1} \\ \vdots \\ \Gamma(Z^y, Z^c, \bar{F}, \bar{A}) \equiv 0 \bmod \Phi_{a_y} \end{cases}$$

$$\Rightarrow \Gamma(Z^y, Z^c, \bar{F}, \bar{A}) \equiv 0 \bmod \Phi_{a_0}\Phi_{a_1}\ldots\Phi_{a_y}$$

- We want the direction "$\Leftarrow$" also to hold. This will be the case if we can bound the degree of $\Gamma(Z^y, Z^k, \bar{F}, \bar{X}^{(k)})$.
- For this, we need a Diophantine definition of "$\bar{A}$ has small degree modulo every Φ_{a_k}".

Eliminating the bounded universal quantifier

$$\begin{cases} \Gamma(Z^y, Z^0, \bar{F}, \bar{X}^{(0)}) = 0 \\ \Gamma(Z^y, Z^1, \bar{F}, \bar{X}^{(1)}) = 0 \\ \vdots \\ \Gamma(Z^y, Z^y, \bar{F}, \bar{X}^{(y)}) = 0 \end{cases} \Rightarrow \begin{cases} \Gamma(Z^y, Z^c, \bar{F}, \bar{A}) \equiv 0 \bmod \Phi_{a_0} \\ \Gamma(Z^y, Z^c, \bar{F}, \bar{A}) \equiv 0 \bmod \Phi_{a_1} \\ \vdots \\ \Gamma(Z^y, Z^c, \bar{F}, \bar{A}) \equiv 0 \bmod \Phi_{a_y} \end{cases}$$

$$\Rightarrow \Gamma(Z^y, Z^c, \bar{F}, \bar{A}) \equiv 0 \bmod \Phi_{a_0}\Phi_{a_1}\ldots\Phi_{a_y}$$

- We want the direction "$\Leftarrow$" also to hold. This will be the case if we can bound the degree of $\Gamma(Z^y, Z^k, \bar{F}, \bar{X}^{(k)})$.
- For this, we need a Diophantine definition of "$\bar{A}$ has small degree modulo every Φ_{a_k}".
- An other major problem is the Diophantine definition of the product $\Phi_{a_0}\Phi_{a_1}\ldots\Phi_{a_y}$ (where y is a variable).

A has small degree modulo every Φ_{a_k}

- Let $A(Z) \equiv X_k(Z) \bmod \Phi_{a_k}$ with X_k of small degree.

A has small degree modulo every Φ_{a_k}

- Let $A(Z) \equiv X_k(Z) \bmod \Phi_{a_k}$ with X_k of small degree.
- Set $B(W, Z) \equiv X_k(W) \bmod \Phi_{a_k}(Z)$.

A has small degree modulo every Φ_{a_k}

- Let $A(Z) \equiv X_k(Z) \bmod \Phi_{a_k}$ with X_k of small degree.
- Set $B(W, Z) \equiv X_k(W) \bmod \Phi_{a_k}(Z)$.
- In order for A to have small degree modulo $\Phi_{a_k}(Z)$:

A has small degree modulo every Φ_{a_k}

- Let $A(Z) \equiv X_k(Z) \bmod \Phi_{a_k}$ with X_k of small degree.
- Set $B(W, Z) \equiv X_k(W) \bmod \Phi_{a_k}(Z)$.
- In order for A to have small degree modulo $\Phi_{a_k}(Z)$:
  - (1) $B(W, Z)$ must depend only on W modulo $\Phi_{a_k}(Z)$.

A has small degree modulo every Φ_{a_k}

- Let $A(Z) \equiv X_k(Z) \bmod \Phi_{a_k}$ with X_k of small degree.
- Set $B(W, Z) \equiv X_k(W) \bmod \Phi_{a_k}(Z)$.
- In order for A to have small degree modulo $\Phi_{a_k}(Z)$:
  - (1) $B(W, Z)$ must depend only on W modulo $\Phi_{a_k}(Z)$.
  - (2) $B(W, Z)$ must have small degree as a polynomial in W modulo $\Phi_{a_k}(Z)$.

A has small degree modulo every Φ_{a_k}

- Let $A(Z) \equiv X_k(Z) \bmod \Phi_{a_k}$ with X_k of small degree.
- Set $B(W, Z) \equiv X_k(W) \bmod \Phi_{a_k}(Z)$.
- In order for A to have small degree modulo $\Phi_{a_k}(Z)$:
  - (1) $B(W, Z)$ must depend only on W modulo $\Phi_{a_k}(Z)$.
  - (2) $B(W, Z)$ must have small degree as a polynomial in W modulo $\Phi_{a_k}(Z)$.
- (1) We look at $\mathbb{F}_q[W, Z]/\big(\Phi_{a_k}(Z), \Phi_w(W)\big)$, we want B to be in the subring $\mathbb{F}_q[W]/\Phi_w(W)$. (for large w)
  Express this using a Frobenius automorphism.

A has small degree modulo every Φ_{a_k}

- Let $A(Z) \equiv X_k(Z) \bmod \Phi_{a_k}$ with X_k of small degree.
- Set $B(W, Z) \equiv X_k(W) \bmod \Phi_{a_k}(Z)$.
- In order for A to have small degree modulo $\Phi_{a_k}(Z)$:
  - (1) $B(W, Z)$ must depend only on W modulo $\Phi_{a_k}(Z)$.
  - (2) $B(W, Z)$ must have small degree as a polynomial in W modulo $\Phi_{a_k}(Z)$.
- (1) We look at $\mathbb{F}_q[W, Z]/\big(\Phi_{a_k}(Z), \Phi_w(W)\big)$, we want B to be in the subring $\mathbb{F}_q[W]/\Phi_w(W)$. (for large w) Express this using a Frobenius automorphism.
- (2) The degree of a polynomial $X \in \mathbb{F}_q[W]$ can be bounded with the formula

$$X = 0 \quad \text{or} \quad X | W^{q^{2u}} - W^{q^u}$$

Defining the product $\Phi_{a_0}\Phi_{a_1}\ldots\Phi_{a_y}$

- We don't really need to define $\Phi_{a_0}\Phi_{a_1}\ldots\Phi_{a_y}$, only that something is zero modulo this product ($\Rightarrow$ the ideal).

Defining the product $\Phi_{a_0}\Phi_{a_1}\ldots\Phi_{a_y}$

- We don't really need to define $\Phi_{a_0}\Phi_{a_1}\ldots\Phi_{a_y}$, only that something is zero modulo this product ($\Rightarrow$ the ideal).
- Assuming all a_k's are prime, we expand

$$\frac{Z^{a_0 a_1 \ldots a_y} - 1}{Z - 1} = \underbrace{\Phi_{a_0}\Phi_{a_1}\cdots\Phi_{a_y}}_{\text{need to define this}} \underbrace{\Phi_{a_0 a_1}\Phi_{a_0 a_2}\cdots\Phi_{a_0 a_1 \ldots a_y}}_{\text{all indices with } \geq 2 \text{ factors}}$$

Defining the product $\Phi_{a_0}\Phi_{a_1}\ldots\Phi_{a_y}$

- We don't really need to define $\Phi_{a_0}\Phi_{a_1}\ldots\Phi_{a_y}$, only that something is zero modulo this product ($\Rightarrow$ the ideal).
- Assuming all a_k's are prime, we expand

$$\frac{Z^{a_0 a_1 \ldots a_y} - 1}{Z - 1} = \underbrace{\Phi_{a_0}\Phi_{a_1}\cdots\Phi_{a_y}}_{\text{need to define this}} \underbrace{\Phi_{a_0 a_1}\Phi_{a_0 a_2}\cdots\Phi_{a_0 a_1 \ldots a_y}}_{\text{all indices with } \geq 2 \text{ factors}}$$

- Recall that $\mathbb{F}_q[Z]/\Phi_d \cong \left(\mathbb{F}_{q^{\operatorname{ord}(q \bmod d)}}\right)^{\varphi(d)/\operatorname{ord}(q \bmod d)}$

Defining the product $\Phi_{a_0}\Phi_{a_1}\ldots\Phi_{a_y}$

- We don't really need to define $\Phi_{a_0}\Phi_{a_1}\ldots\Phi_{a_y}$, only that something is zero modulo this product ($\Rightarrow$ the ideal).
- Assuming all a_k's are prime, we expand

$$\frac{Z^{a_0 a_1 \ldots a_y} - 1}{Z - 1} = \underbrace{\Phi_{a_0}\Phi_{a_1}\cdots\Phi_{a_y}}_{\text{need to define this}} \underbrace{\Phi_{a_0 a_1}\Phi_{a_0 a_2}\cdots\Phi_{a_0 a_1 \ldots a_y}}_{\text{all indices with } \geq 2 \text{ factors}}$$

- Recall that $\mathbb{F}_q[Z]/\Phi_d \cong \left(\mathbb{F}_{q^{\operatorname{ord}(q \bmod d)}}\right)^{\varphi(d)/\operatorname{ord}(q \bmod d)}$
- Take Q as a divisor of $Z^{a_0 a_1 \ldots a_k} - 1/Z - 1$. Then express that $(\mathbb{F}_q[Z]/Q)^*$ contains elements of 'high' order.

Defining the product $\Phi_{a_0}\Phi_{a_1}\ldots\Phi_{a_y}$

- We don't really need to define $\Phi_{a_0}\Phi_{a_1}\ldots\Phi_{a_y}$, only that something is zero modulo this product ($\Rightarrow$ the ideal).
- Assuming all a_k's are prime, we expand

$$\frac{Z^{a_0 a_1 \ldots a_y} - 1}{Z - 1} = \underbrace{\Phi_{a_0}\Phi_{a_1}\cdots\Phi_{a_y}}_{\text{need to define this}}\underbrace{\Phi_{a_0 a_1}\Phi_{a_0 a_2}\cdots\Phi_{a_0 a_1 \ldots a_y}}_{\text{all indices with } \geq 2 \text{ factors}}$$

- Recall that $\mathbb{F}_q[Z]/\Phi_d \cong \left(\mathbb{F}_{q^{\operatorname{ord}(q \bmod d)}}\right)^{\varphi(d)/\operatorname{ord}(q \bmod d)}$
- Take Q as a divisor of $Z^{a_0 a_1 \ldots a_k} - 1/Z - 1$. Then express that $(\mathbb{F}_q[Z]/Q)^*$ contains elements of 'high' order.
- This way it is impossible that Q contains any factors from $\Phi_{a_0}, \ldots, \Phi_{a_y}$. Now $P := (Z^{a_0 a_1 \ldots a_k} - 1/Z - 1)/Q$ will certainly contain these factors.

You are not expected to understand this

$$(\forall k)_{\leq y}(\exists X_1,\ldots,X_m)\Gamma(Z^y,Z^k,F_1,\ldots F_n,X_1,\ldots,X_m)$$

$$\Updownarrow$$

$$(\exists u,e,t)(\exists \bar{b}\in\mathbb{N})(\exists \bar{a}\in\mathbb{N})(\exists c)(\exists A_1,\ldots,A_m)(\exists P)(\exists r)(\exists Q,G,H,M)(\exists s,w)$$

$$F_1^2|(Z^{q^{2e}}-Z^{q^e})F_1\ \wedge\cdots\wedge\ F_n^2|(Z^{q^{2e}}-Z^{q^e})F_n\ \wedge\ d\big(2y+nq^{2e}+mq^{2u}\big)\leq t$$

$$\wedge\ \bar{b}\text{ is a product of }y+1\text{ primes }b_0,b_1,\ldots,b_y\text{ with }t<b_0<b_1<\ldots<b_y$$

$$\wedge\ \bar{a}\text{ is a product of }y+1\text{ primes }a_0<a_1<\ldots<a_y\text{, with }a_k|\Phi_{b_k}(q)$$

$$\wedge\ c\equiv k \bmod a_k\ (\text{for all } 0\leq k\leq y)\ \wedge\ r=(q-1)\Phi_{b_0}(q)\Phi_{b_1}(q)\ldots\Phi_{b_y}(q)$$

$$\wedge\ \Gamma(Z^y,Z^c,F_1,\ldots,F_n,A_1,\ldots,A_m)\equiv 0 \bmod P$$

$$\wedge\ (Z-1)PQ=\left(Z^{\bar{a}}-1\right)\ \wedge\ GH\equiv 1 \bmod Q\ \wedge\ (G^r-1)M\equiv 1 \bmod Q$$

$$\wedge\ s\text{ is prime}\ \wedge\ s>q^{2u}\ \wedge\ s\nmid(q-1)\varphi(a_0a_1\ldots a_y)\ \wedge\ w\text{ is prime}\ \wedge\ w|\Phi_s(q)$$

$$\wedge\ \bigwedge_{i=1}^{m}(\exists B_i,M_i^{(1)},M_i^{(2)},M_i^{(3)}\in\mathbb{F}_q[W,Z])\quad B_i^2M_i^{(1)}\equiv\left(W^{q^{2u}}-W^{q^u}\right)B_i \bmod P$$

$$\wedge\ \Phi_w(W)M_i^{(2)}\equiv B^{q^s}-B_i \bmod P\ \wedge\ (W-Z)M_i^{(3)}\equiv A_i-B_i \bmod P$$