Asymptotic distributions of the number of zeros of random polynomials in Hayes equivalence class over a finite field

Jason Z. Gao
School of Mathematics and Statistics
Carleton University
Ottawa, Ontario K1S5B6
Canada

Definitions and Notation

- $\mathbb{F}_q$ denotes the finite field with q elements, q is a power of a prime p, and $\mathbb{F}_q^* = \mathbb{F}_q \setminus \{0\}$.
- $\mathbb{F}_q[x]$ denotes the set of polynomials with coefficients in $\mathbb{F}_q$.
- $\deg(f)$ denotes the degree of the polynomial f.
- $\mathcal{M}$ denotes the set of monic polynomials in $\mathbb{F}_q[x]$, $\mathcal{M}_j := \{f \in \mathcal{M} : \deg(f) = j\}$.

Definitions and Notation

- $\mathbb{F}_q$ denotes the finite field with q elements, q is a power of a prime p, and $\mathbb{F}_q^* = \mathbb{F}_q \setminus \{0\}$.
- $\mathbb{F}_q[x]$ denotes the set of polynomials with coefficients in $\mathbb{F}_q$.
- $\deg(f)$ denotes the degree of the polynomial f.
- $\mathcal{M}$ denotes the set of monic polynomials in $\mathbb{F}_q[x]$, $\mathcal{M}_j := \{f \in \mathcal{M} : \deg(f) = j\}$.
- For $f \in \mathcal{M}_d$, $\hat{f} = x^d f(1/x)$ is called the *reciprocal* of f.

Definitions and Notation

- $\mathbb{F}_q$ denotes the finite field with q elements, q is a power of a prime p, and $\mathbb{F}_q^* = \mathbb{F}_q \setminus \{0\}$.
- $\mathbb{F}_q[x]$ denotes the set of polynomials with coefficients in $\mathbb{F}_q$.
- $\deg(f)$ denotes the degree of the polynomial f.
- $\mathcal{M}$ denotes the set of monic polynomials in $\mathbb{F}_q[x]$, $\mathcal{M}_j := \{f \in \mathcal{M} : \deg(f) = j\}$.
- For $f \in \mathcal{M}_d$, $\hat{f} = x^d f(1/x)$ is called the *reciprocal* of f.

For a non-negative integer ℓ and $Q \in \mathcal{M}_t$, two polynomials $f, g \in \mathcal{M}$ are *Hayes equivalent* with respect to ℓ and Q if $\gcd(f, Q) = \gcd(g, Q) = 1$ and

$$\hat{f}(x) \equiv \hat{g}(x) \pmod{x^{\ell+1}}, \qquad (1)$$

$$f(x) \equiv g(x) \pmod{Q}. \qquad (2)$$

Definitions and Notation

Condition (1) says that f and g have the same ℓ *leading coefficients*, that is,

$$\left[x^{\deg(f)-j}\right] f(x) = \left[x^{\deg(g)-j}\right] g(x), \quad 1 \leq j \leq \ell.$$

Definitions and Notation

Condition (1) says that f and g have the same ℓ *leading coefficients*, that is,

$$\left[x^{\deg(f)-j}\right] f(x) = \left[x^{\deg(g)-j}\right] g(x), \quad 1 \leq j \leq \ell.$$

The following two special cases are particularly interesting.

(a) $Q = 1$. In this case, condition (2) is null, and Hayes equivalence is defined by the ℓ leading coefficients.

(b) $Q = x^t$ for some $t > 0$. In this case, condition (2) says that f and g have the same t *ending coefficients*, that is

$$\left[x^{j}\right] f(x) = \left[x^{j}\right] g(x), \quad 0 \leq j \leq t-1.$$

The Hayes group

Let $\mathcal{E}^{\ell,Q}$ denote the set of all Hayes equivalence classes with respect to ℓ, Q, and let $\langle f\rangle$ denote the equivalence class represented by a polynomial $f \in \mathcal{M}$. It is known [Hayes 65] that $\mathcal{E}^{\ell,Q}$ is a group under the operation $\langle f\rangle\langle g\rangle = \langle fg\rangle$.

The Hayes group

Let $\mathcal{E}^{\ell,Q}$ denote the set of all Hayes equivalence classes with respect to ℓ, Q, and let $\langle f \rangle$ denote the equivalence class represented by a polynomial $f \in \mathcal{M}$. It is known [Hayes 65] that $\mathcal{E}^{\ell,Q}$ is a group under the operation $\langle f \rangle \langle g \rangle = \langle fg \rangle$. It is also known that

$$\mathcal{E}^{\ell,Q} \cong \mathcal{E}^{\ell,1} \times \mathcal{E}^{0,Q},$$

$$|\mathcal{E}^{\ell,Q}| = q^{\ell} \Phi_t(Q), \text{ where } \Phi_j(Q) := |\{f \in \mathcal{M}_j : \gcd(f, Q) = 1\}|.$$

The Hayes group

Let $\mathcal{E}^{\ell,Q}$ denote the set of all Hayes equivalence classes with respect to ℓ, Q, and let $\langle f \rangle$ denote the equivalence class represented by a polynomial $f \in \mathcal{M}$. It is known [Hayes 65] that $\mathcal{E}^{\ell,Q}$ is a group under the operation $\langle f \rangle \langle g \rangle = \langle fg \rangle$. It is also known that

$$\mathcal{E}^{\ell,Q} \cong \mathcal{E}^{\ell,1} \times \mathcal{E}^{0,Q},$$

$$|\mathcal{E}^{\ell,Q}| = q^{\ell} \Phi_t(Q), \text{ where } \Phi_j(Q) := |\{f \in \mathcal{M}_j : \gcd(f, Q) = 1\}|.$$

We shall use Iverson's bracket $[\![P]\!]$ which has value 1 if the predicate P is true and 0 otherwise.

Distribution of the number of zeros

Let $\mathcal{M}_k(\varepsilon)$ denote the set of polynomials in $\mathcal{M}$ which have degree $k + t + \ell$ and are equivalent to ε. It is known that $|\mathcal{M}_k(\varepsilon)| = q^k$.

Distribution of the number of zeros

Let $\mathcal{M}_k(\varepsilon)$ denote the set of polynomials in $\mathcal{M}$ which have degree $k+t+\ell$ and are equivalent to ε. It is known that $|\mathcal{M}_k(\varepsilon)| = q^k$.
Given $D \subseteq \mathbb{F}_q$ and $\varepsilon \in \mathcal{E}^{\ell,Q}$, let $Y_k(\varepsilon)$ be the number of zeros in D of a random polynomial $f \in \mathcal{M}_k(\varepsilon)$ (under uniform distribution). Some known work about the distribution of $Y_k(\varepsilon)$:

- For $D = \mathbb{F}_q$ and for all polynomials, that is, $\ell = 0, Q = 1$. [Knopfmacher-Knopfmacher 90]

Distribution of the number of zeros

Let $\mathcal{M}_k(\varepsilon)$ denote the set of polynomials in $\mathcal{M}$ which have degree $k+t+\ell$ and are equivalent to ε. It is known that $|\mathcal{M}_k(\varepsilon)| = q^k$.
Given $D \subseteq \mathbb{F}_q$ and $\varepsilon \in \mathcal{E}^{\ell,Q}$, let $Y_k(\varepsilon)$ be the number of zeros in D of a random polynomial $f \in \mathcal{M}_k(\varepsilon)$ (under uniform distribution). Some known work about the distribution of $Y_k(\varepsilon)$:

- For $D = \mathbb{F}_q$ and for all polynomials, that is, $\ell = 0, Q = 1$. [Knopfmacher-Knopfmacher 90]
- For polynomials with given leading coefficients, i.e., $\ell \geq 1, Q = 1$. This is related to the distance distribution of Reed-Solomon code. [Zhou-Wang-Wang 17, Li-Wan 20, Gao-Li 23]

Distribution of the number of zeros

Let $\mathcal{M}_k(\varepsilon)$ denote the set of polynomials in $\mathcal{M}$ which have degree $k+t+\ell$ and are equivalent to ε. It is known that $|\mathcal{M}_k(\varepsilon)| = q^k$.

Given $D \subseteq \mathbb{F}_q$ and $\varepsilon \in \mathcal{E}^{\ell,Q}$, let $Y_k(\varepsilon)$ be the number of zeros in D of a random polynomial $f \in \mathcal{M}_k(\varepsilon)$ (under uniform distribution). Some known work about the distribution of $Y_k(\varepsilon)$:

- For $D = \mathbb{F}_q$ and for all polynomials, that is, $\ell = 0, Q = 1$. [Knopfmacher-Knopfmacher 90]
- For polynomials with given leading coefficients, i.e., $\ell \geq 1, Q = 1$. This is related to the distance distribution of Reed-Solomon code. [Zhou-Wang-Wang 17, Li-Wan 20, Gao-Li 23]

Since $\gcd(f, Q) = 1$, we will assume $D \subseteq \{x \in \mathbb{F}_q : Q(x) \neq 0\}$, and set $n := |D|$.

Asymptotic distribution of $Y_k(\varepsilon)$

Theorem 1 Let $Q \in \mathcal{M}_t$ and $\varepsilon \in \mathcal{E}^{\ell,Q}$.

(a) As $k - r \to \infty$, we have

$$\mathbb{P}(Y_k(\varepsilon) = r) = \binom{n}{r}\left(\frac{1}{q}\right)^r \left(1 - \frac{1}{q}\right)^{n-r} (1 + o(1)).$$

(b) As $n, k - r \to \infty$ and for $r = o(\sqrt{n})$, we have

$$\mathbb{P}(Y_k(\varepsilon) = r) \sim e^{-n/q}\frac{1}{r!}\left(\frac{n}{q}\right)^r.$$

Asymptotic distribution of $Y_k(\varepsilon)$

Theorem 1 Let $Q \in \mathcal{M}_t$ and $\varepsilon \in \mathcal{E}^{\ell,Q}$.

(a) As $k - r \to \infty$, we have

$$\mathbb{P}(Y_k(\varepsilon) = r) = \binom{n}{r}\left(\frac{1}{q}\right)^r\left(1 - \frac{1}{q}\right)^{n-r}(1 + o(1)).$$

(b) As $n, k - r \to \infty$ and for $r = o(\sqrt{n})$, we have

$$\mathbb{P}(Y_k(\varepsilon) = r) \sim e^{-n/q}\frac{1}{r!}\left(\frac{n}{q}\right)^r.$$

Define $\mu_m(r) := \sum_{j=0}^{m}(-1)^j\binom{n-r}{j}q^{-j}$. We note

$$\left|\mu_m(r) - \left(1 - \frac{1}{q}\right)^{n-r}\right| \le \binom{n-r}{m+1}q^{-(m+1)} \le \frac{1}{(m+1)!}.$$

Asymptotics for large r

Theorem 2 Let $\varepsilon \in \mathcal{E}^{\ell,Q}$ and $D = \{x \in \mathbb{F}_q : Q(x) \neq 0\}$. Suppose either $\ell \geq 1$ or $\ell = 0, Q = x^t$. Then, uniformly for $0 \leq r \leq k + t + \ell$, as $k \to \infty$, we have

$$\mathbb{P}(Y_k = r) \sim \mu_{k+t+\ell-r}(r) \binom{n}{r} q^{-r},$$

provided that either of the following conditions holds:
(a) there are constants $c, c' \in (0,1)$ such that $t + \ell \leq c'\sqrt{n}$, $k \leq cn$ and

$$\frac{p-1}{p} c \ln \frac{1}{c} + (1-c) \ln \frac{1}{1-c} - \frac{1+c}{p} \ln(1+c) > c' \ln(2p).$$

(b) there are constants $c, c' \in (0,1)$ such that $t + \ell \leq c'\sqrt{n}$, $k \leq cn$, $p \geq c/c' \geq 1$ and $(1-c) \ln \frac{1}{1-c} > c' \ln \frac{1}{c'}$.

Outline of the proofs

It is convenient to define $\langle f \rangle = 0$ when $\gcd(f, Q) \neq 1$. Let

$$r(f) := |\{x \in D : f(x) = 0\}|,$$

and consider the following generating function:

$$G(z, u) = \sum_{f \in \mathcal{M}} \langle f \rangle z^{\deg(f)} u^{r(f)},$$

Outline of the proofs

It is convenient to define $\langle f \rangle = 0$ when $\gcd(f, Q) \neq 1$. Let

$$r(f) := |\{x \in D : f(x) = 0\}|,$$

and consider the following generating function:

$$G(z, u) = \sum_{f \in \mathcal{M}} \langle f \rangle z^{\deg(f)} u^{r(f)},$$

The standard generating function argument gives

$$G(z, u) = \frac{1}{1 - qz} z^{t+\ell} (1 + (u-1)z)^n \sum_{\varepsilon \in \mathcal{E}^{\ell, Q}} \varepsilon + \left(\sum_{j=0}^{t+\ell-1} z^j \sum_{g \in \mathcal{M}_j} \langle g \rangle \right) \prod_{\alpha \in D} \left(\langle 1 \rangle + (u-1) z \langle x - \alpha \rangle \right).$$

Generating function and moments

Let D_j be the set of all j-subsets of D, and

$$W_j(\varepsilon) = \sum_{g \in \mathcal{M}_{k+t+\ell-j}} \sum_{S \in D_j} \left[\!\!\left[\langle g \rangle \prod_{\alpha \in S} \langle x - \alpha \rangle = \varepsilon \right]\!\!\right]. \qquad (3)$$

Generating function and moments

Let D_j be the set of all j-subsets of D, and

$$W_j(\varepsilon) = \sum_{g \in \mathcal{M}_{k+t+\ell-j}} \sum_{S \in D_j} \left[\!\!\left[\langle g \rangle \prod_{\alpha \in S} \langle x - \alpha \rangle = \varepsilon \right]\!\!\right]. \qquad (3)$$

Proposition 1

$$\begin{aligned} \left[z^{k+t+\ell} \varepsilon \right] G(z,u) &= \sum_{j=0}^{k} q^{k-j} \binom{n}{j} (u-1)^j \\ &\quad + \sum_{j=k+1}^{k+t+\ell} W_j(\varepsilon)(u-1)^j, \\ \mathbb{E}\left(\binom{Y_k(\varepsilon)}{j} \right) &= [\![j \le k]\!] \binom{n}{j} q^{-j} \\ &\quad + [\![k+1 \le j \le k+t+\ell]\!] q^{-k} W_j(\varepsilon). \end{aligned}$$

Generating function and moments

Let D_j be the set of all j-subsets of D, and

$$W_j(\varepsilon) = \sum_{g\in\mathcal{M}_{k+t+\ell-j}} \sum_{S\in D_j} \left[\!\!\left[\langle g\rangle \prod_{\alpha\in S} \langle x-\alpha\rangle = \varepsilon \right]\!\!\right]. \qquad (3)$$

Proposition 1

$$\left[z^{k+t+\ell}\varepsilon\right] G(z,u) = \sum_{j=0}^{k} q^{k-j}\binom{n}{j}(u-1)^j + \sum_{j=k+1}^{k+t+\ell} W_j(\varepsilon)(u-1)^j,$$

$$\mathbb{E}\left(\binom{Y_k(\varepsilon)}{j}\right) = [\![j\le k]\!]\binom{n}{j}q^{-j} + [\![k+1\le j\le k+t+\ell]\!]q^{-k}W_j(\varepsilon).$$

Sieve formula and Bonferroni inequalities

Sieve formula Let Y be any random variable which takes non-negative integer values $0, 1, \ldots, M$. We have

$$\mathbb{P}(Y = r) = \sum_{j=r}^{M} (-1)^{j+r} \binom{j}{r} \mathbb{E}\left(\binom{Y}{j}\right).$$

Sieve formula and Bonferroni inequalities

Sieve formula Let Y be any random variable which takes non-negative integer values $0, 1, \ldots, M$. We have

$$\mathbb{P}(Y = r) = \sum_{j=r}^{M} (-1)^{j+r} \binom{j}{r} \mathbb{E}\left(\binom{Y}{j}\right).$$

Moreover, for each $r \le m \le M$, we have

$$\left| \mathbb{P}(Y = r) - \sum_{j=r}^{m-1} (-1)^{j+r} \binom{j}{r} \mathbb{E}\left(\binom{Y}{j}\right) \right| \le \binom{m}{r} \mathbb{E}\left(\binom{Y}{m}\right).$$

Sieve formula and Bonferroni inequalities

Sieve formula Let Y be any random variable which takes non-negative integer values $0, 1, \ldots, M$. We have

$$\mathbb{P}(Y = r) = \sum_{j=r}^{M} (-1)^{j+r} \binom{j}{r} \mathbb{E}\left(\binom{Y}{j}\right).$$

Moreover, for each $r \le m \le M$, we have

$$\left| \mathbb{P}(Y = r) - \sum_{j=r}^{m-1} (-1)^{j+r} \binom{j}{r} \mathbb{E}\left(\binom{Y}{j}\right) \right| \le \binom{m}{r} \mathbb{E}\left(\binom{Y}{m}\right).$$

This and Proposition 1 immediately give Theorem 1 by choosing $m = k$.

The function $A_j(a,b)$ and its bounds

Define

$$\begin{aligned} A_j(a,b) &= [z^j]\left((1-z)^{-ab}(1-z^p)^{-a(1-b)/p}\right) \\ &= \sum_{0\le i\le j/p} \binom{ab+j-ip-1}{j-ip}\binom{a(1-b)/p+i-1}{i}. \end{aligned}$$

The function $A_j(a,b)$ and its bounds

Define

$$A_j(a,b) = [z^j]\left((1-z)^{-ab}(1-z^p)^{-a(1-b)/p}\right)$$
$$= \sum_{0\le i\le j/p} \binom{ab+j-ip-1}{j-ip}\binom{a(1-b)/p+i-1}{i}.$$

Proposition 3 Let $b \in (0,1]$ and $a > 0$. Then

(a) For all $p > 0$, we have

$$\ln A_j(a,b) \le \frac{j}{p}\ln\frac{a+j}{j} + \frac{a(1-b)}{p}\ln\frac{a+j}{a} + ab\ln(2p),$$

(b) For $p \ge c_j/b \ge 1$, we have

$$\ln A_j(a,b) \le j\ln\frac{ab+j}{j} + ab\ln\frac{ab+j}{ab} + \frac{a\ln 4}{p}2^{-pab/j}.$$

Estimate for $W_j(\varepsilon)$ using Weil's bound

Proposition 2 Let $\varepsilon \in \mathcal{E}$, $k+1 \le j \le k+t+\ell$, $\gamma := \min\{1, (t+\ell-1)\sqrt{q}/n\}$, and $D = \{\alpha \in \mathbb{F}_q : Q(\alpha) \neq 0\}$. Suppose $\ell \ge 1$. Then

$$\left| W_j(\varepsilon) - \frac{\Phi_{k+t+\ell-j}(Q)}{\Phi_t(Q)} \binom{n}{j} q^{-\ell} \right|$$
$$\le \frac{|\mathcal{E}^{\ell,Q}| - 1}{|\mathcal{E}^{\ell,Q}|} \binom{t+\ell-1}{t+\ell+k-j} q^{(t+\ell+k-j)/2} A_j(n,\gamma).$$

Estimate for $W_j(\varepsilon)$ using Weil's bound

Proposition 2 Let $\varepsilon \in \mathcal{E}$, $k+1 \le j \le k+t+\ell$, $\gamma := \min\{1, (t+\ell-1)\sqrt{q}/n\}$, and $D = \{\alpha \in \mathbb{F}_q : Q(\alpha) \neq 0\}$. Suppose $\ell \ge 1$. Then

$$\left| W_j(\varepsilon) - \frac{\Phi_{k+t+\ell-j}(Q)}{\Phi_t(Q)} \binom{n}{j} q^{-\ell} \right| \le \frac{|\mathcal{E}^{\ell,Q}| - 1}{|\mathcal{E}^{\ell,Q}|} \binom{t+\ell-1}{t+\ell+k-j} q^{(t+\ell+k-j)/2} A_j(n,\gamma).$$

The proof uses *characters* χ over $\mathcal{E}^{\ell,Q}$:

$$W_j(\varepsilon) = \frac{1}{|\mathcal{E}^{\ell,Q}|} \sum_{\chi} \chi(\varepsilon^{-1}) \left(\sum_{g \in \mathcal{M}_{k+t+\ell-j}} \chi(g) \right) \sum_{S \in D_j} \prod_{\alpha \in S} \chi(x-\alpha),$$

Estimate for $W_j(\varepsilon)$ using Weil's bound

Proposition 2 Let $\varepsilon \in \mathcal{E}$, $k+1 \le j \le k+t+\ell$, $\gamma := \min\{1, (t+\ell-1)\sqrt{q}/n\}$, and $D = \{\alpha \in \mathbb{F}_q : Q(\alpha) \neq 0\}$. Suppose $\ell \geq 1$. Then

$$\left| W_j(\varepsilon) - \frac{\Phi_{k+t+\ell-j}(Q)}{\Phi_t(Q)} \binom{n}{j} q^{-\ell} \right| \le \frac{|\mathcal{E}^{\ell,Q}| - 1}{|\mathcal{E}^{\ell,Q}|} \binom{t+\ell-1}{t+\ell+k-j} q^{(t+\ell+k-j)/2} A_j(n,\gamma).$$

The proof uses *characters* χ over $\mathcal{E}^{\ell,Q}$:

$$W_j(\varepsilon) = \frac{1}{|\mathcal{E}^{\ell,Q}|} \sum_{\chi} \chi(\varepsilon^{-1}) \left(\sum_{g \in \mathcal{M}_{k+t+\ell-j}} \chi(g) \right) \sum_{S \in D_j} \prod_{\alpha \in S} \chi(x-\alpha),$$

Weil's bound for character sums, and and Li-Wan's "coordinate-sieve" formula.

Weil's bound

Weil's bound: for each $\chi \neq 1$ and $d \leq t + \ell - 1$, we have

$$\left| \sum_{g \in \mathcal{M}_d} \chi(g) \right| \leq \binom{t + \ell - 1}{d} q^{d/2}.$$

Weil's bound

Weil's bound: for each $\chi \neq 1$ and $d \leq t + \ell - 1$, we have

$$\left| \sum_{g \in \mathcal{M}_d} \chi(g) \right| \leq \binom{t+\ell-1}{d} q^{d/2}.$$

The condition $\ell \geq 1$ implies $\chi^i \neq 1$ when $p \nmid i$. This together with the condition $D = \{\alpha \in \mathbb{F}_q : Q(\alpha) \neq 0\}$ give

$$\left| \sum_{\alpha \in D} \chi^i(x - \alpha) \right| \leq \gamma n. \qquad (p \nmid i) \tag{4}$$

Theorem 2 holds for those D satisfying (4).

Coordinate-sieve formula

Let $\bar{D}^j := \{(x_1, \ldots, x_j) : x_i \in D$ are all distinct$\}$ and $c_i(\tau)$ be the number of cycles of length i in a permutation τ of j elements. Define $l(\tau) = \sum_i c_i, \quad l' = \sum_{i, p \nmid i} c_i$.

Coordinate-sieve formula

Let $\bar{D}^j := \{(x_1, \ldots, x_j) : x_i \in D$ are all distinct$\}$ and $c_i(\tau)$ be the number of cycles of length i in a permutation τ of j elements. Define $l(\tau) = \sum_i c_i, \quad l' = \sum_{i, p\nmid i} c_i$.

Li-Wan's "coordinate-sieve" formula gives

$$\begin{aligned}
&\left| \sum_{S \in D_j} \prod_{\alpha \in S} \chi(x - \alpha) \right| \\
&= \frac{1}{j!} \left| \sum_{(x_1, \ldots, x_j) \in \bar{D}^j} \prod_{i=1}^{j} \chi(x - x_i) \right| \\
&\leq \frac{1}{j!} \sum_{\tau} \prod_{p \mid i} \left| \sum_{\alpha \in D} \chi^i(x - \alpha) \right|^{c_i(\tau)} \prod_{p \nmid i} \left| \sum_{\alpha \in D} \chi^i(x - \alpha) \right|^{c_i(\tau)} \\
&\leq \frac{1}{j!} \sum_{\tau} n^{l(\tau) - l'(\tau)} (\gamma n)^{l'(\tau)} = A_j(n, \gamma).
\end{aligned}$$

Estimate for $\Phi_j(Q)$

Recall $\Phi_j(Q) := |\{f \in \mathcal{M}_j : \gcd(f, Q) = 1\}|$.

Estimate for $\Phi_j(Q)$

Recall $\Phi_j(Q) := |\{f \in \mathcal{M}_j : \gcd(f, Q) = 1\}|$. Let $\{P_i : i \in I\}$ be the set of distinct irreducible factors of Q, where $P_i \in \mathcal{M}_{d_i}$. Then the sieve formula gives

$$\Phi_j(Q) = \sum_{S \subseteq I} (-1)^{|S|} \left[\!\!\left[\sum_{i \in S} d_i \leq j \right]\!\!\right] q^{j - \sum_{i \in S} d_i},$$

$$q^j \left(1 - \sum_{i \in I} q^{-d_i} \right) \leq \Phi_j(Q) \leq q^j.$$

Estimate for $\Phi_j(Q)$

Recall $\Phi_j(Q) := |\{f \in \mathcal{M}_j : \gcd(f, Q) = 1\}|$. Let $\{P_i : i \in I\}$ be the set of distinct irreducible factors of Q, where $P_i \in \mathcal{M}_{d_i}$. Then the sieve formula gives

$$\Phi_j(Q) = \sum_{S \subseteq I} (-1)^{|S|} \left[\!\!\left[\sum_{i \in S} d_i \leq j \right]\!\!\right] q^{j - \sum_{i \in S} d_i},$$

$$q^j \left(1 - \sum_{i \in I} q^{-d_i}\right) \leq \Phi_j(Q) \leq q^j.$$

We note

$$|I| \leq \sum_{i \in I} d_i \leq t \leq \sqrt{n},$$

$$\Phi_j(Q) = q^j \left(1 + O\left(\sqrt{n}/q\right)\right).$$

Theorem 2 follows from Propositions 1–3.

Thanks. Questions?