Counting reducible, powerful, and relatively irreducible multivariate polynomials over finite fields

Alfredo Viola

Universidad de la República, Uruguay

CanaDAM 2013

Joint work with Joachim von zur Gathen and Konstantin Ziegler

The problem.

- Most univariate polynomials over a finite field are reducible.
- Random polynomials of degree up to n are irreducible with probability about $1/n$.
- In two or more variables, most polynomials are irreducible.
- [von zur Gathen 2008], gives precise approximations with exponentially decreasing error term (bivariate).
- [Bodin 2008], [Bodin 2010] studies bivariate and general case.
- In Section 3.6 of [Mullen and Panario 2013], the new Handbook of Finite Fields, there is a survey of these results.

Main contributions.

- Exact formulas for the numbers of reducible, s-powerful, and relatively irreducible polynomials.
- The latter also yields the number of absolutely irreducible polynomials.
- Of these R.V., only reducible polynomials had been treated in the literature, usually with much larger error terms.
- The formulas yield simple, yet precise, approximations to these numbers, with rapidly decaying relative errors.

Methodologies used.

- Generating functions.
  - Divergent power series (except at 0).
  - Power series with symbolic coefficients, namely rational functions in a variable representing the field size.
  - Yields in a straightforward manner exact formulas.
  - Then, coefficient comparisons yield tight approximations with exponentially decreasing relative error in bit size of the data.

- Combinatorial counting.
  - Yields "second order" approximations with explicit constants in the error term

Notation.

- Let the ring $F[x_1, \ldots, x_r]$ in $r \geq 1$ variables over a field F.
- $P_{r,n}^{\mathsf{all}}(F) = \{f \in F[x_1, \ldots, x_r] \colon \deg f = n\}$.
- Poly. of deg. at most n form an F-vector space of dimension

$$b_{r,n} = \binom{r+n}{r} = \frac{(r+n)^{\underline{r}}}{r!}, \quad (r+x)^{\underline{r}} = (r+x)\cdot(r-1+x)\cdots(1+x),$$

- Over a finite field $\mathbb{F}_q$ with q elements, we have

$$\#P_{r,n}^{\mathsf{all}}(\mathbb{F}_q) = q^{b_{r,n}} - q^{b_{r,n-1}} = q^{b_{r,n}}(1 - q^{-b_{r-1,n}}).$$

- The monic polynomials are those with leading coefficient 1. Let

$$P_{r,n}(F) = \{f \in P_{r,n}^{\mathsf{all}}(F) \colon f \text{ is monic}\}.$$

- Then

$$\#P_{r,n}(\mathbb{F}_q) = \frac{\#P_{r,n}^{\mathsf{all}}(\mathbb{F}_q)}{q-1} = q^{b_{r,n}-1}\frac{1 - q^{-b_{r-1,n}}}{1 - q^{-1}}.$$

Generating functions.

- Let C_n be the number of elements of size n in a class C. Then

$$\mathrm{C}(z) = \sum_{n \geq 0} \mathrm{C}_n z^n \in \mathbb{Z}_{\geq 0} [\![z]\!] .$$

- A power series is *original* if its constant term vanishes.

$$\log(1 - z) = -\sum_{n \geq 1} \frac{z^n}{n} \in \mathbb{Q} [\![z]\!]$$

  is original and substituting a power series f in another power series g is well-defined if f is original.
- Two combinatorial classes $\mathcal{A}$ and $\mathcal{B}$ are *isomorphic* if there is a size-preserving bijection $\mathcal{A} \to \mathcal{B}$ or equivalently if $\mathrm{A} = \mathrm{B}$.

Combinatorial classes.

- Let $\mathcal{A}$, $\mathcal{B}$ be combinatorial classes. The *disjoint union* is

$$\mathcal{A} \dot{\cup} \mathcal{B} = \{\{0\} \times \mathcal{A}\} \cup \{\{1\} \times \mathcal{B}\}.$$

- The size of an element $(0, a)$ or $(1, b)$ is defined as the size of a or b, respectively.
- $\mathcal{SEQ}(\mathcal{A}) = \{(\alpha_1, \ldots, \alpha_\ell) : \ell \geq 0, \alpha_i \in \mathcal{A}\}$ is the *sequence class*, where $|(\alpha_1, \ldots, \alpha_\ell)| = \sum_i |\alpha_i|$.
- It is a combinatorial class, if $\mathcal{A}$ contains no element of size 0.
- The *multiset class* is $\mathcal{MSET}(\mathcal{A}) = \mathcal{SEQ}(\mathcal{A})/\sim$, where $(\alpha_1, \ldots, \alpha_\ell) \sim (\beta_1, \ldots, \beta_\ell)$ if there is a permutation σ of $\{1, \ldots, \ell\}$ such that $\alpha_i = \beta_{\sigma(i)}$ for all i.
- This class contains all finite sequences of elements from $\mathcal{A}$ where repetition is allowed, but ordering ignored.

Combinatorial classes and generating functions.

Fact

Let $\mathcal{A}$, $\mathcal{B}$, and $\mathcal{C}$ be combinatorial classes.

1. *If $\mathcal{A} = \mathcal{B} \dot{\cup} \mathcal{C}$, then $\mathrm{A} = \mathrm{B} + \mathrm{C}$.*
2. *If $\mathcal{A} = \mathcal{MSET}(\mathcal{B})$ and $\mathrm{B}_0 = 0$, then*

$$\mathrm{B} = \sum_{k \geq 1} \frac{\mu(k)}{k} \log(\mathrm{A}(z^k)),$$

where μ is the number-theoretic Möbius-function, defined as

$$\mu(k) = \begin{cases} 1 & \text{if } k = 1, \\ (-1)^{\ell} & \text{if } k \text{ is the product of } \ell \text{ distinct primes}, \\ 0 & \text{otherwise.} \end{cases}$$

Reducible polynomials.

- Let $I_{r,n}(F) = \{f \in P_{r,n}(F) \colon f \text{ irreducible}\}$,
  $R_{r,n}(F) = P_{r,n}(F) \setminus I_{r,n}(F)$.
- The polynomial 1 is neither reducible nor irreducible.
- It is natural to have $R_{r,0}(F) = \{1\}$ and $I_{r,0}(F) = \varnothing$.
- $\mathcal{P} = \bigcup_{n \geq 0} P_{r,n}(\mathbb{F}_q)$, $\mathcal{I} = \bigcup_{n \geq 0} I_{r,n}(\mathbb{F}_q)$, and $\mathcal{R} = \mathcal{P} \setminus \mathcal{I}$, are combinatorial classes with the total degree as size functions.
- Then,

$$\mathrm{P}_n = \mathrm{P}_{r,n}(\mathbb{F}_q) = \#P_{r,n}(\mathbb{F}_q) = q^{b_{r,n}-1} \frac{1 - q^{-b_{r-1,n}}}{1 - q^{-1}}.$$

- By unique factorization, every element in $\mathcal{P}$ corresponds to an unordered finite sequence of irreducible polynomials, where repetition is allowed. Hence $\mathcal{P}$ is isomorphic to $\mathcal{MSET}(\mathcal{I})$. Then

$$\mathrm{I} = \sum_{k \geq 1} \frac{\mu(k)}{k} \log \mathrm{P}(z^k).$$

Reducible polynomials.

- Simple Maple program to compute exact values.
- Small values of n and r.

```
allpolysGF:=proc(z,N,r) local i: option remember:
    sum('simplify((q^binomial(r+i,r)-q^binomial(r+i-1,r))/
        (q-1))*z^i',i = 0..N):
end:

irreduciblesGF:=proc(z,N,r) local k: option remember:
    convert(taylor((sum('mobius(k)/k*log(allpolysGF(z^k,N,r))',
        k=1..N)), z, N+1), polynom):
end:

reduciblesGF:=proc(z,N,r) option remember:
    allpolysGF(z,N,r)-irreduciblesGF(z,N,r):
end:

reducibles:=proc(n,r)
coeff(sort(expand(reduciblesGF(z,n,r))),z^n):
end:
```

Reducible polynomials.

n	$\#R_{3,n}(\mathbb{F}_q)$
1	0
2	$(q^6+2q^5+3q^4+3q^3+2q^2+q)/2$
3	$(3q^{12}+6q^{11}+9q^{10}+8q^9+6q^8+3q^7-q^6-3q^5-3q^4+q^2+q)/3$
4	$(4q^{22}+8q^{21}+12q^{20}+12q^{19}+14q^{18}+16q^{17}+18q^{16}+16q^{15}+10q^{14}-13q^{12}-20q^{11}-20q^{10}-10q^9-q^8+6q^7+7q^6+4q^5-2q^3-q^2)/4$
5	$(5q^{37}+10q^{36}+15q^{35}+15q^{34}+15q^{33}+15q^{32}+15q^{31}+15q^{30}+15q^{29}+20q^{28}+25q^{27}+30q^{26}+30q^{25}+25q^{24}+15q^{23}-15q^{21}-30q^{20}-45q^{19}-60q^{18}-65q^{17}-55q^{16}-26q^{15}+10q^{14}+40q^{13}+50q^{12}+40q^{11}+19q^{10}-10q^8-10q^7-5q^6-q^5+q^3+q^2+q)/5$
6	$(6q^{58}+12q^{57}+18q^{56}+18q^{55}+18q^{54}+18q^{53}+18q^{52}+18q^{51}+18q^{50}+18q^{49}+18q^{48}+18q^{47}+18q^{46}+18q^{45}+18q^{44}+24q^{43}+30q^{42}+36q^{41}+36q^{40}+30q^{39}+21q^{38}+6q^{37}-3q^{36}-6q^{35}-3q^{34}+3q^{32}-6q^{31}-27q^{30}-60q^{29}-99q^{28}-128q^{27}-141q^{26}-132q^{25}-104q^{24}-60q^{23}-3q^{22}+70q^{21}+144q^{20}+201q^{19}+203q^{18}+147q^{17}+51q^{16}-45q^{15}-102q^{14}-105q^{13}-71q^{12}-27q^{11}+3q^{10}+14q^9+11q^8+5q^7+3q^6+3q^5+2q^4-2q^3-2q^2-q)/6$

n	$\#R_{4,n}(\mathbb{F}_q)$
1	0
2	$(q^8+2q^7+3q^6+4q^5+4q^4+3q^3+2q^2+q)/2$
3	$(3q^{18}+6q^{17}+9q^{16}+12q^{15}+12q^{14}+12q^{13}+11q^{12}+9q^{11}+6q^{10}+2q^9-3q^8-6q^7-7q^6-6q^5-2q^4+q^2+q)/3$
4	$(4q^{38}+8q^{37}+12q^{36}+16q^{35}+16q^{34}+16q^{33}+16q^{32}+16q^{31}+16q^{30}+16q^{29}+18q^{28}+20q^{27}+22q^{26}+24q^{25}+26q^{24}+28q^{23}+26q^{22}+20q^{21}+10q^{20}-4q^{19}-22q^{18}-36q^{17}-45q^{16}-48q^{15}-42q^{14}-34q^{13}-21q^{12}-6q^{11}+8q^{10}+18q^9+20q^8+16q^7+9q^6+2q^5-2q^4-2q^3-q^2)/4$

n	$\#R_{5,n}(\mathbb{F}_q)$
1	0
2	$(q^{10}+2q^9+3q^8+4q^7+5q^6+5q^5+4q^4+3q^3+2q^2+q)/2$
3	$(3q^{25}+6q^{24}+9q^{23}+12q^{22}+15q^{21}+15q^{20}+15q^{19}+15q^{18}+15q^{17}+15q^{16}+14q^{15}+12q^{14}+9q^{13}+5q^{12}-6q^{10}-10q^9-12q^8-12q^7-10q^6-5q^5-2q^4+q^2+q)/3$
4	$(4q^{60}+8q^{59}+12q^{58}+16q^{57}+20q^{56}+20q^{55}+20q^{54}+20q^{53}+20q^{52}+20q^{51}+20q^{50}+20q^{49}+20q^{48}+20q^{47}+20q^{46}+20q^{45}+20q^{44}+20q^{43}+20q^{42}+20q^{41}+22q^{40}+24q^{39}+26q^{38}+28q^{37}+30q^{36}+32q^{35}+34q^{34}+36q^{33}+38q^{32}+40q^{31}+38q^{30}+32q^{29}+22q^{28}+8q^{27}-10q^{26}-32q^{25}-50q^{24}-64q^{23}-74q^{22}-80q^{21}-79q^{20}-78q^{19}-74q^{18}-66q^{17}-53q^{16}-34q^{15}-12q^{14}+10q^{13}+29q^{12}+42q^{11}+45q^{10}+40q^9+30q^8+18q^7+7q^6-2q^4-2q^3-q^2)/4$

Divergent series.

- Analytic approach as in [Flajolet and Sedgewick 2009] cannot be used.
- Move from power series in $\mathbb{Q}[\![z]\!]$ to power series in $\mathbb{Q}(\mathbf{q})[\![z]\!]$, where $\mathbf{q}$ is a symbolic variable representing the field size.
- For $r \geq 2$ and $n \geq 0$ we let

$$\mathsf{P}_n(\mathbf{q}) = \mathsf{P}_{r,n}(\mathbf{q}) = \mathbf{q}^{b_{r,n}-1}\frac{1-\mathbf{q}^{-b_{r-1,n}}}{1-\mathbf{q}^{-1}} \in \mathbb{Z}[\mathbf{q}],$$

- We define the power series $\mathsf{P}, \mathsf{I}, \mathsf{R} \in \mathbb{Q}(\mathbf{q})[\![z]\!]$ by

$$\mathsf{P}(\mathbf{q}, z) = \sum_{n\geq 0} \mathsf{P}_n(\mathbf{q}) z^n,$$

$$\mathsf{I}(\mathbf{q}, z) = \sum_{k\geq 1} \frac{\mu(k)}{k} \log \mathsf{P}(\mathbf{q}, z^k),$$

$$\mathsf{R}(\mathbf{q}, z) = \mathsf{P}(\mathbf{q}, z) - \mathsf{I}(\mathbf{q}, z).$$

Divergent series.

- Then $1 - \mathrm{P}(\mathbf{q}, z^k)$ is an original power series, and $\log \mathrm{P}(\mathbf{q}, z^k)$ and I are well-defined, with $\mathrm{I}(\mathbf{q}, 0) = 0$.
- For $q \in \mathbb{Q}$, the rational functions in $\mathbb{Q}(\mathbf{q})$ without pole at $\mathbf{q} \leftarrow q$ form a ring.
- The evaluation map which substitutes an integer q for $\mathbf{q}$ is a ring homomorphism.
- Since P_n is actually a polynomial in $\mathbf{q}$, evaluating $\mathbf{q} \leftarrow q$ maps $\mathrm{P}(\mathbf{q}, z)$ to $\mathrm{P}(z)$ coefficientwise.
- Furthermore,

$$[z^n]\mathrm{I}(q, z) = \mathrm{I}_n,$$
$$[z^n]\mathrm{R}(q, z) = \mathrm{R}_n.$$

Asymptotic results.

- $O(\mathbf{q}^{-m})$ with $m > 0$ means the existence of some f with degree at most $-m$ that makes the equation valid.
- Results valid for any "fixed" r and n.
- If a term $O(\mathbf{q}^{-m})$ appears, then we may conclude a numerical asymptotic result for growing prime powers q.

Theorem

Let $r \geq 2$ *and* $\rho_{r,n}(\mathbf{q}) = \mathbf{q}^{\binom{r+n-1}{r}+r-1} \frac{1-\mathbf{q}^{-r}}{(1-\mathbf{q}^{-1})^2} \in \mathbb{Q}(\mathbf{q})$.

Then $\mathrm{R}_0 = 1$, $\mathrm{R}_1 = 0$, $\mathrm{R}_2 = \frac{\rho_{r,2}(\mathbf{q})}{2} \cdot (1 - \mathbf{q}^{-r-1})$,

$$\mathrm{R}_3 = \rho_{r,3}(\mathbf{q})\left(1 - \mathbf{q}^{-\binom{r+1}{2}} + \mathbf{q}^{-\binom{r}{2}} \frac{1 - 2\mathbf{q}^{-r} + 2\mathbf{q}^{-2r-1} - \mathbf{q}^{-2r-2}}{3(1-\mathbf{q}^{-1})}\right),$$

$$\mathrm{R}_4 = \rho_{r,4}(\mathbf{q}) \cdot \left(1 + \mathbf{q}^{-\binom{r+1}{3}} \cdot \frac{1 + O(\mathbf{q}^{-r(r-1)/2})}{2(1-\mathbf{q}^{-r})}\right),$$

and for $n \geq 5$ $\mathrm{R}_n = \rho_{r,n}(\mathbf{q}) \cdot \left(1 + \mathbf{q}^{-\binom{r+n-2}{r-1}+r(r+1)/2} \cdot \frac{1+O(\mathbf{q}^{-r(r-1)/2})}{1-\mathbf{q}^{-r}}\right)$.

Combinatorial Approach: Precise error bounds.

- Exponentially decaying in r, n, and $\log_2 q$, when the other two are fixed.

Theorem

Let $q, r \geq 2$ and $\rho_{r,n}$ as before. We have $\#R_{r,0}(\mathbb{F}_q) = 1$, $\#R_{r,1}(\mathbb{F}_q) = 0$, $\#R_{r,2}(\mathbb{F}_q) = \frac{\rho_{r,2}(q)}{2} \cdot (1 - q^{-r-1})$,

$$\begin{aligned}\frac{|\#R_{r,3}(\mathbb{F}_q) - \rho_{r,3}(q)|}{\rho_{r,3}(q)} &= q^{-r(r-1)/2} \frac{1 - 2q^{-r} + 2q^{-2r-1} - q^{-2r-2}}{3(1 - q^{-1})} \\ &\leq q^{-r(r-1)/2},\end{aligned}$$

and for $n \geq 4$

$$\begin{aligned}\frac{|\#R_{r,n}(\mathbb{F}_q) - \rho_{r,n}(q)|}{\rho_{r,n}(q)} &\leq \frac{q^{-\binom{r+n-2}{r-1}+r(r+1)/2}}{(1 - q^{-1})(1 - q^{-r})} \\ &\leq 3q^{-\binom{r+n-2}{r-1}+r(r+1)/2}.\end{aligned}$$

Proportion of reducible polynomials.

Corollary

For $q, r \geq 2$ and $n \geq 5$, we have

$$\frac{1}{4} q^{-\binom{r+n-1}{r-1}+r} \leq \frac{\#R_{r,n}(\mathbb{F}_q)}{\#P_{r,n}(\mathbb{F}_q)} \leq 3q^{-\binom{r+n-1}{r-1}+r}.$$

Corollary

Let $q, r \geq 2$ and $\rho_{r,n}$ as before. We have $\#I_{r,1}(\mathbb{F}_q) = \#P_{r,1}(\mathbb{F}_q)$, $\#I_{r,2}(\mathbb{F}_q) = \#P_{r,2}(\mathbb{F}_q) - \frac{\rho_{r,2}(q)}{2} \cdot (1 - q^{-r-1})$,

$$|\#I_{r,3}(\mathbb{F}_q) - (\#P_{r,3}(\mathbb{F}_q) - \rho_{r,3}(q))| \leq \rho_{r,3}(q) \cdot q^{-(r-1)r/2},$$

and for $n \geq 4$

$$|\#I_{r,n}(\mathbb{F}_q) - (\#P_{r,n}(\mathbb{F}_q) - \rho_{r,n}(q))| \leq \rho_{r,n}(q) \cdot 3q^{-\binom{r+n-2}{r-1}+\binom{r+1}{2}}.$$

Powerful polynomials.

- For an integer $s \geq 2$, a polynomial is called *s-powerful* if it is divisible by the sth power of some nonconstant polynomial, and *s-powerfree* otherwise; it is *squarefree* if $s = 2$.
- Let $Q_{r,n,s}(F) = \{f \in P_{r,n}(F) \colon f \text{ is } s\text{-powerful}\}$,
  $S_{r,n,s}(F) = P_{r,n}(F) \setminus Q_{r,n,s}(F)$.
- Let the combinatorial classes $\mathcal{Q} = \bigcup_{n \geq 0} Q_{r,n,s}$ and $\mathcal{S} = \mathcal{P} \setminus \mathcal{Q}$.
- Any monic polynomial f factors uniquely as $f = g \cdot h^s$ with g monic s-free polynomial and h arbitrary monic. Hence as G.F.

$$\mathrm{P} = \mathrm{S} \cdot \mathrm{P}(z^s), \quad \mathrm{Q} = \mathrm{P} - \mathrm{S}.$$

- Gives simple Maple programs to compute the coefficients of Q.

Powerful polynomials.

- Simple Maple program to compute exact values.
- Small values of n, s and r.

```
spowerfreesGF:=proc(z,N,r,s) local i: option remember:
    convert(taylor(allpolysGF(z,N,r)/allpolysGF(z^s,N,r),
        z,N+1),polynom):
end:

spowerfulsGF:=proc(z,N,r,s) option remember:
    allpolysGF(z,N,r)-spowerfreesGF(z,N,r,s):
end:

spowerfuls:=proc(n,r,s)
    coeff(sort(expand(spowerfulsGF(z,n,r,s))),z^n):
end:
```

Powerful polynomials.

n	$\#Q_{2,n,3}(\mathbb{F}_q)$
0, 1, 2	0
3	q^2+q
4	$q^4+2\,q^3+q^2$
5	$q^7+2\,q^6+2\,q^5+q^4$
6	$q^{11}+2\,q^{10}+2\,q^9+2q^8+q^7+q^5-q^3-q^2$
7	$q^{16}+2\,q^{15}+2\,q^{14}+2\,q^{13}+2\,q^{12}+q^{11}+q^7+q^6-q^5-2\,q^4-q^3$
8	$q^{22}+2\,q^{21}+2\,q^{20}+2\,q^{19}+2\,q^{18}+2\,q^{17}+q^{16}+q^{10}+q^9-2\,q^7-2\,q^6-q^5$
9	$q^{29}+2q^{28}+2\,q^{27}+2\,q^{26}+2\,q^{25}+2\,q^{24}+2\,q^{23}+q^{22}+q^{14}+q^{13}-q^{11}-2\,q^{10}-q^9-q^7-2\,q^6-q^5+q^4+q^3$

n	$\#Q_{3,n,2}(\mathbb{F}_q)$
0, 1	0
2	q^3+q^2+q
3	$q^6+2\,q^5+3\,q^4+2\,q^3+q^2$
4	$q^{12}+2\,q^{11}+3\,q^{10}+4\,q^9+4\,q^8+4\,q^7+2q^6-2\,q^4-2\,q^3-q^2$
5	$q^{22}+2\,q^{21}+3\,q^{20}+3\,q^{19}+3q^{18}+3\,q^{17}+3\,q^{16}+3\,q^{15}+3\,q^{14}+3\,q^{13}+3\,q^{12}+3\,q^{11}+3\,q^{10}+2\,q^9-3\,q^7-5\,q^6-5\,q^5-3\,q^4-q^3$
6	$q^{37}+2\,q^{36}+3\,q^{35}+3\,q^{34}+3q^{33}+3\,q^{32}+3\,q^{31}+3\,q^{30}+3q^{29}+3\,q^{28}+3\,q^{27}+3\,q^{26}+3\,q^{25}+3\,q^{24}+3\,q^{23}+2\,q^{22}+q^{21}+q^{19}+2\,q^{18}+3\,q^{17}+4\,q^{16}+4\,q^{15}+3\,q^{14}+q^{13}-4\,q^{12}-8\,q^{11}-11\,q^{10}-11\,q^9-8\,q^8-3\,q^7+2\,q^6+4\,q^5+3\,q^4+q^3$

n	$\#Q_{3,n,3}(\mathbb{F}_q)$
0, 1, 2	0
3	q^3+q^2+q
4	$q^6+2\,q^5+3\,q^4+2\,q^3+q^2$
5	$q^{12}+2\,q^{11}+3\,q^{10}+3\,q^9+3\,q^8+3\,q^7+2q^6+q^5$
6	$q^{22}+2\,q^{21}+3\,q^{20}+3\,q^{19}+3\,q^{18}+3\,q^{17}+3\,q^{16}+3\,q^{15}+3\,q^{14}+3\,q^{13}+2\,q^{12}+q^{11}+q^9+q^8+q^7-q^5-2q^4-2\,q^3-q^2$
7	$q^{37}+2\,q^{36}+3\,q^{35}+3\,q^{34}+3q^{33}+3\,q^{32}+3\,q^{31}+3\,q^{30}+3q^{29}+3\,q^{28}+3\,q^{27}+3\,q^{26}+3\,q^{25}+3\,q^{24}+3\,q^{23}+2\,q^{22}+q^{21}+q^{12}+2\,q^{11}+3\,q^{10}+2\,q^9-3\,q^7-5\,q^6-5\,q^5-3\,q^4-q^3$

Powerful polynomials.

Theorem

Let $r, s \geq 2$, $n \geq 0$, and

$$\eta_{r,n,s}(\mathbf{q}) = \mathbf{q}^{\binom{r+n-s}{r}+r-1} \frac{(1-\mathbf{q}^{-r})(1-\mathbf{q}^{-\binom{r+n-s-1}{r-1}})}{(1-\mathbf{q}^{-1})^2} \in \mathbb{Q}(\mathbf{q}),$$

$$\delta = \binom{r+n-s}{r} - \binom{r+n-2s}{r} - \frac{r(r+1)}{2}.$$

1. *If $n \geq 2s$, then $\delta \geq r$.*
2.

$$Q_n = \begin{cases} 0 & \text{for } n < s, \\ \eta_{r,n,s}(\mathbf{q}) & \text{for } s \leq n < 2s, \\ \eta_{r,n,s}(\mathbf{q})\left(1 + \mathbf{q}^{-\delta} \cdot \frac{1-\mathbf{q}^{-\binom{n+r-2s-1}{r-1}}}{1-\mathbf{q}^{-\binom{n+r-s-1}{r-1}}} \right. & \\ \quad \left. \cdot \left(\frac{1-\mathbf{q}^{-r(r+1)/2}}{1-\mathbf{q}^{-r}} - \mathbf{q}^{-r(r-1)/2} \frac{1-\mathbf{q}^{-r}}{1-\mathbf{q}^{-1}} \right) \right) & \text{for } 2s \leq n < 3s. \end{cases}$$

Powerful polynomials.

Theorem (cont.)

1. *For $(n,s)=(6,2)$ and $r\geq 2$, we have*

$$\begin{aligned}
Q_6 = \eta_{r,6,2}(\mathbf{q})\Bigg(1+\mathbf{q}^{-\binom{r+3}{4}-r+1}\cdot\Bigg(\mathbf{q}^{-1}\frac{(1-\mathbf{q}^{-1})\left(1-\mathbf{q}^{-\binom{r+2}{3}}\right)}{(1-\mathbf{q}^{-r})\left(1-\mathbf{q}^{-\binom{r+3}{4}}\right)}\\
+\mathbf{q}^{-(r^3-7r+6)/6}\frac{(1-\mathbf{q}^{-r(r+1)/2})^2}{(1-\mathbf{q}^{-r})\left(1-\mathbf{q}^{-\binom{r+3}{4}}\right)}\\
-\mathbf{q}^{-(r^3+3r^2-10r+6)/6}\frac{(1-\mathbf{q}^{-r})(1-\mathbf{q}^{-r(r+1)/2})}{(1-\mathbf{q}^{-1})\left(1-\mathbf{q}^{-\binom{r+3}{4}}\right)}\\
-2\mathbf{q}^{-(r^3+3r^2+4r-6)/6}\frac{1-\mathbf{q}^{-r(r+1)/2}}{1-\mathbf{q}^{-\binom{r+3}{4}}}\\
+\mathbf{q}^{-(r^3+6r^2-7r+6)/6}\frac{(1-\mathbf{q}^{-r})^2}{(1-\mathbf{q}^{-1})\left(1-\mathbf{q}^{-\binom{r+3}{4}}\right)}\Bigg)\Bigg)\\
=\eta_{r,6,2}(\mathbf{q})\left(1+\mathbf{q}^{-\delta+(r-2)(r-1)(r+3)/6}(1+O(\mathbf{q}^{-1}))\right).
\end{aligned}$$

2. *For $n\geq 2s$ and $(n,s)\neq(6,2)$, we have*

$$Q_n=\eta_{r,n,s}(\mathbf{q})\left(1+\mathbf{q}^{-\delta}(1+O(\mathbf{q}^{-1}))\right).$$

More precise asymptotic bounds.

Theorem

1. *For* $(n,s)=(6,2)$, *we have* $\delta = r(r+1)(r^2+9r+2)/24$ *and*

$$|\#Q_{r,6,2}(\mathbb{F}_q) - \eta_{r,6,2}(q)| \leq \eta_{r,6,2}(q)\cdot 2q^{-\delta+(r-2)(r-1)(r+3)/6}.$$

2. *For* $n \geq 3s$ *and* $(n,s)\neq(6,2)$, *we have*

$$|\#Q_{r,n,s}(\mathbb{F}_q) - \eta_{r,n,s}(q)| \leq \eta_{r,n,s}(q)\cdot 6q^{-\delta}.$$

Corollary

For $q,r,s \geq 2$ *and* $n \geq s$, *we have*

$$\frac{1}{2}q^{\binom{r+n-s}{r}+r-1} \leq \#Q_{r,n,s}(\mathbb{F}_q) \leq 10\frac{28}{3}q^{\binom{r+n-s}{r}+r-1},$$

$$\frac{1}{2}q^{-\binom{r+n}{r}+\binom{r+n-s}{r}+r} \leq \frac{\#Q_{r,n,s}(\mathbb{F}_q)}{\#P_{r,n}(\mathbb{F}_q)} \leq 5q^{-\binom{r+n}{r}+\binom{r+n-s}{r}+r},$$

$$\frac{1}{6}q^{-\binom{r+n-1}{r}+\binom{r+n-s}{r}} \leq \frac{\#Q_{r,n,s}(\mathbb{F}_q)}{\#R_{r,n}(\mathbb{F}_q)} \leq 19q^{-\binom{r+n-1}{r}+\binom{r+n-s}{r}}.$$

s-powerfree polynomials.

Corollary

Let $q, r, s \geq 2$, $n \geq 0$, and $\eta_{r,n,s}$ and δ as before. We have

$$\#P_{r,n}(\mathbb{F}_q) - 3\eta_{r,n,s}(q) \leq \#S_{r,n,s}(\mathbb{F}_q) \leq \#P_{r,n}(\mathbb{F}_q),$$

and more precisely

$$\#S_{r,n,s}(\mathbb{F}_q) = \begin{cases} \#P_{r,n}(\mathbb{F}_q) & \text{for } n < s, \\ \#P_{r,n}(\mathbb{F}_q) - \eta_{r,n,s}(q) & \text{for } s \leq n < 2s, \\ \#P_{r,n}(\mathbb{F}_q) - \eta_{r,n,s}(q)\left(1 + q^{-\delta} \cdot \frac{1-q^{-\binom{n+r-2s-1}{r-1}}}{1-q^{-\binom{n+r-s-1}{r-1}}}\right. & \\ \quad \left. \cdot \left(\frac{1-q^{-r(r+1)/2}}{1-q^{-r}} - q^{-r(r-1)/2}\frac{1-q^{-r}}{1-q^{-1}}\right)\right) & \text{for } 2s \leq n < 3s, \end{cases}$$

$$|\#S_{r,6,2}(\mathbb{F}_q) - (\#P_{r,n}(\mathbb{F}_q) - \eta_{r,6,2}(q))| \leq \eta_{r,6,2}(q) \cdot 2q^{-\delta+(r-2)(r-1)(r+3)/6},$$

and for $n \geq 3s$ with $(n, s) \neq (6, 2)$

$$|\#S_{r,n,s}(\mathbb{F}_q) - (\#P_{r,n}(\mathbb{F}_q) - \eta_{r,n,s}(q))| \leq \eta_{r,n,s}(q) \cdot 6q^{-\delta}.$$

Relatively irreducible polynomials.

- A polynomial over F is *absolutely irreducible* if it is irreducible over an algebraic closure of F.
- It is *relatively irreducible* if it is irreducible over F but factors over some extension field of F.

$$A_{r,n}(F) = \{f \in P_{r,n}(F) : f \text{ is absolutely irreducible}\} \subseteq I_{r,n}(F),$$
$$E_{r,n}(F) = I_{r,n}(F) \setminus A_{r,n}(F).$$

- For a field extension $\mathbb{F}_{q^k}$ over $\mathbb{F}_q$, let $G_k = \mathrm{Gal}(\mathbb{F}_{q^k} : \mathbb{F}_q)$. It acts on $\mathbb{F}_{q^k}[x]$ coefficientwise with $k \mid n$ and the "norm" map

$$\varphi_{r,n,k} : P_{r,n/k}(\mathbb{F}_{q^k}) \to P_{r,n}(\mathbb{F}_q),$$
$$g \mapsto \prod_{\sigma \in G_k} g^\sigma,$$

- Since $(\varphi_{r,n,k}(g))^\tau = \varphi_{r,n,k}(g)$ for any $\tau \in G_k$ and therefore $\varphi_{r,n,k}(g) \in P_{r,n}(\mathbb{F}_q)$, this map is well-defined.

Relatively irreducible polynomials.

- Relatively irreducible polynomials in $P_{r,n}(\mathbb{F}_q)$ are the product of all conjugates of an irreducible polynomial g defined over some extension field $\mathbb{F}_{q^k}$.
- If g itself is relatively irreducible over $\mathbb{F}_{q^k}$, then there exists an appropriate multiple j of k and $h \in P_{r,n/j}(\mathbb{F}_{q^j})$ with the same image $\varphi_{r,n,k}(g) = \varphi_{r,n,j}(h)$ in $P_{r,n}(\mathbb{F}_q)$ and the property that h is absolutely irreducible.
- So, every relatively irreducible polynomial is contained in $\varphi_{r,n,k}(A_{r,n/k}(\mathbb{F}_{q^k}))$ for a unique $k > 1$ dividing n. Then

$$A_{r,n}(\mathbb{F}_q) = \varphi_{r,n,1}(A_{r,n}(\mathbb{F}_q)),$$
$$E_{r,n}(\mathbb{F}_q) \subseteq \bigcup_{1<k \mid n} \varphi_{r,n,k}(A_{r,n/k}(\mathbb{F}_{q^k})).$$

Relatively irreducible polynomials.

- Let $A^{+}_{r,n/k}(\mathbb{F}_{q^k}) = A_{r,n/k}(\mathbb{F}_{q^k}) \setminus \bigcup_{s \mid k,\, s \neq k} A_{r,n/k}(\mathbb{F}_{q^s})$ be the set of absolutely irreducible polynomials over $\mathbb{F}_{q^k}$ that are not defined over a proper subfield containing $\mathbb{F}_q$, and

$$I_{r,n,k}(\mathbb{F}_q) = \varphi_{r,n,k}(A^{+}_{r,n/k}(\mathbb{F}_{q^k})).$$

Lemma

1. *We have the disjoint union*

$$I_{r,n}(\mathbb{F}_q) = \dot{\bigcup_{k \mid n}} I_{r,n,k}(\mathbb{F}_q)$$

and more precisely

$$A_{r,n}(\mathbb{F}_q) = I_{r,n,1}(\mathbb{F}_q),$$
$$E_{r,n}(\mathbb{F}_q) = \dot{\bigcup_{1<k \mid n}} I_{r,n,k}(\mathbb{F}_q).$$

2. $$\#I_{r,n,k}(\mathbb{F}_q) = \tfrac{1}{k} \#A^{+}_{r,n/k}(\mathbb{F}_{q^k}).$$

Relatively irreducible polynomials.

- With $\mathsf{I}(\mathbf{q}, z)$ as before, we get the power series $\mathsf{A}, \mathsf{E} \in \mathbb{Q}(\mathbf{q})\,[\![z]\!]$

$$\begin{aligned}
\mathsf{A}_0(\mathbf{q}) &= \mathsf{I}_0(\mathbf{q}) = 0, \\
\mathsf{A}_n(\mathbf{q}) &= \sum_{k \mid n} \frac{1}{k} \sum_{s \mid k} \mu(s) \mathsf{I}_{n/k}(\mathbf{q}^s) \in \mathbb{Z}[\mathbf{q}] \text{ for } n > 0, \\
\mathsf{A}(\mathbf{q}, z) &= \sum_{n \geq 0} \mathsf{A}_n(\mathbf{q}) z^n \in \mathbb{Z}[\mathbf{q}]\,[\![z]\!]\,, \\
\mathsf{E}(\mathbf{q}, z) &= \mathsf{I}(\mathbf{q}, z) - \mathsf{A}(\mathbf{q}, z) \\
&= -\sum_{1 < k \mid n} \frac{1}{k} \sum_{s \mid k} \mu(s) \mathsf{I}_{n/k}(\mathbf{q}^s) \in \mathbb{Z}[\mathbf{q}]\,[\![z]\!]\,.
\end{aligned}$$

- Then

$$\begin{aligned}
\mathsf{A}_n(q) &= \#A_{r,n}(\mathbb{F}_q), \\
\mathsf{E}_n(q) &= \#E_{r,n}(\mathbb{F}_q).
\end{aligned}$$

Relatively irreducible polynomials.

```
absirreds:=proc(n,r) local k,s: option remember:
    add(1/k*add(mobius(s)*subs(q=q^s,coeff(irreduciblesGF(
        z,n/k,r),z^(n/k))),s=divisors(k)),k=divisors(n))
end:

absirredsGF:=proc(z,N,r) local k,s: option remember:
    sum('absirreds(k,r)*z^k',k=1..N)
end:

relirredsGF:=proc(z,N,r) option remember:
    irreduciblesGF(z,N,r)-absirredsGF(z,N,r);
end:

relirreds:=proc(n,r)
    coeff(sort(expand(relirredsGF(z,n,r))),z^n):
end:
```

Relatively irreducible polynomials.

n	$\#E_{2,n}(\mathbb{F}_q)$
1	0
2	$(q^4-q)/2$
3	$(q^6+q^3-q^2-q)/3$
4	$(2\,q^{10}+q^8-2\,q^5-2\,q^4+q^2)/4$
5	$(q^{10}+q^5-q^2-q)/5$
6	$(3\,q^{18}+3\,q^{16}+2\,q^{15}-2\,q^{12}-3\,q^{10}-3\,q^9-3\,q^8+q^6+q^5-q^4-q^3+2\,q^2+q)/6$
7	$(q^{14}+q^7-q^2-q)/7$
8	$(4\,q^{28}+4\,q^{26}+4\,q^{24}-6\,q^{20}-8\,q^{18}-3\,q^{16}-4\,q^{13}+6\,q^{10}+8\,q^9+2\,q^8-4\,q^7-4\,q^6+q^4)/8$

n	$\#E_{3,n}(\mathbb{F}_q)$
1	0
2	$(q^6+q^4-q^3-q)/2$
3	$(q^9+q^6-q^2-q)/3$
4	$(2\,q^{18}+2\,q^{16}+2\,q^{14}+q^{12}-2\,q^9-3q^8-2\,q^7-3\,q^6+2\,q^3+q^2)/4$
5	$(q^{15}+q^{10}+q^5-q^3-q^2-q)/5$
6	$(3\,q^{38}+3\,q^{36}+3\,q^{34}+3\,q^{32}+3\,q^{30}+3\,q^{28}+2\,q^{27}+3\,q^{26}+2\,q^{24}-3\,q^{22}+2\,q^{21}-6\,q^{20}-3\,q^{19}-11\,q^{18}-3\,q^{17}-9\,q^{16}-3q^{15}-6\,q^{14}-3\,q^{13}-q^{12}+3\,q^{11}+9\,q^{10}+4q^9+7\,q^8+q^7-3\,q^6-3\,q^5-2\,q^4+2\,q^3+2\,q^2+q)/6$
7	$(q^{21}+q^{14}+q^7-q^3-q^2-q)/7$

n	$\#E_{4,n}(\mathbb{F}_q)$
1	0
2	$(q^8+q^6-q^3-q)/2$
3	$(q^{12}+q^9+q^6-q^4-q^2-q)/3$
4	$(2\,q^{28}+2\,q^{26}+2\,q^{24}+2\,q^{22}+2q^{20}+2\,q^{18}+q^{16}-2\,q^{14}-2\,q^{13}-3q^{12}-2\,q^{11}-4\,q^{10}-2\,q^9-4\,q^8-q^6+2\,q^5+2\,q^4+2\,q^3+q^2)/4$
5	$(q^{20}+q^{15}+q^{10}+q^5-q^4-q^3-q^2-q)/5$
6	$(3\,q^{68}+3\,q^{66}+3\,q^{64}+3\,q^{62}+3\,q^{60}+3q^{58}+3\,q^{56}+3\,q^{54}+3\,q^{52}+3q^{50}+3\,q^{48}+3\,q^{46}+3\,q^{44}+5\,q^{42}+3\,q^{40}+2\,q^{39}+3\,q^{38}+2\,q^{36}-6\,q^{34}-q^{33}-9\,q^{32}-3\,q^{31}-10\,q^{30}-3\,q^{29}-15\,q^{28}-q^{27}-15\,q^{26}-3\,q^{25}-14\,q^{24}-3\,q^{23}-12\,q^{22}-3\,q^{21}-9\,q^{20}-3\,q^{19}-4\,q^{18}+3\,q^{17}+9\,q^{16}+7\,q^{15}+16\,q^{14}+10\,q^{13}+12\,q^{12}+7\,q^{11}+10\,q^{10}-2\,q^9-q^8-6\,q^7-7\,q^6-4\,q^5+q^4+2\,q^3+2\,q^2+q)/6$

Relatively irreducible polynomials.

- The approach by generating functions gives

Theorem

Let $r, n \geq 2$, let ℓ be the smallest prime divisor of n, and

$$\epsilon_{r,n}(\mathbf{q}) = \frac{\mathbf{q}^{\ell\left(\binom{r+n/\ell}{r}-1\right)}}{\ell(1-\mathbf{q}^{-\ell})} \in \mathbb{Q}(\mathbf{q}),$$

$$\kappa = (\ell-1)\left(\binom{r-1+n/\ell}{r-1} - r\right) + 1.$$

Then the following hold.

1. $\mathsf{E}_1(\mathbf{q}) = 0$.
2. *If n is prime, then*

$$\mathsf{E}_n(\mathbf{q}) = \epsilon_{r,n}(\mathbf{q})(1-\mathbf{q}^{-nr})\left(1 - \mathbf{q}^{-r(n-1)}\frac{(1-\mathbf{q}^{-r})(1-\mathbf{q}^{-n})}{(1-\mathbf{q}^{-1})(1-\mathbf{q}^{-nr})}\right).$$

3. *If n is composite, then $\kappa \geq 2$ and*

$$\mathsf{E}_n(\mathbf{q}) = \epsilon_{r,n}(\mathbf{q})(1 + O(\mathbf{q}^{-\kappa})).$$

Relatively irreducible polynomials.

- The combinatorial approach yields the following result.

Theorem

Let $r, q \geq 2$, and $\epsilon_{r,n}$ and κ as before.

1. $\#E_{r,1}(\mathbb{F}_q) = 0$.
2. *If n is prime, then*

$$\#E_{r,n}(\mathbb{F}_q) = \epsilon_{r,n}(q)(1 - q^{-nr})\left(1 - q^{-r(n-1)}\frac{(1 - q^{-r})(1 - q^{-n})}{(1 - q^{-1})(1 - q^{-nr})}\right),$$

$$0 \leq \epsilon_{r,n}(q) - \#E_{r,n}(\mathbb{F}_q) \leq 3q^{-r(n-1)}.$$

3. *If n is composite, then*

$$|\#E_{r,n}(\mathbb{F}_q) - \epsilon_{r,n}(q)| \leq \epsilon_{r,n}(q) \cdot 3q^{-\kappa}.$$

Relatively irreducible polynomials.

Corollary

Let $q, r, n \geq 2$, and ℓ be the smallest prime divisor of n, then

$$\frac{1}{4\ell} q^{\ell\binom{r+n/\ell}{r}-\ell} \leq \#E_{r,n}(\mathbb{F}_q) \leq \frac{2}{\ell} q^{\ell\binom{l+n/\ell}{r}-\ell},$$

$$\frac{1}{8\ell} q^{-\binom{r+n}{r}+\ell\binom{r+n/\ell}{r}-\ell+1} \leq \frac{\#E_{r,n}(\mathbb{F}_q)}{\#P_{r,n}(\mathbb{F}_q)} \leq \frac{2}{\ell} q^{-\binom{r+n}{r}+\ell\binom{r+n/\ell}{r}-\ell+1},$$

$$\frac{1}{8\ell} q^{-\binom{r+n}{r}+\ell\binom{r+n/\ell}{r}-\ell+1} \leq \frac{\#E_{r,n}(\mathbb{F}_q)}{\#I_{r,n}(\mathbb{F}_q)} \leq \frac{2}{\ell} q^{-\binom{r+n}{r}+\ell\binom{r+n/\ell}{r}-\ell+1}.$$

Corollary

Let $r, q, n \geq 2$ and $\rho_{r,n}(q)$ as in (1). Then

$$\#P_{r,n}(\mathbb{F}_q) - 4\rho_{r,n}(q) \leq \#A_{r,n}(\mathbb{F}_q) \leq \#I_{r,n}(\mathbb{F}_q) \leq \#P_{r,n}(\mathbb{F}_q),$$

where the 4 can be replaced by 3 for $n \geq 3$.