The density of polynomials of degree n over $\mathbb{Z}_p$ having exactly r roots in $\mathbb{Q}_p$

Stevan Gajović (University of Groningen)
Joint work with Manjul Bhargava (Princeton University), John Cremona (University of Warwick), and Tom Fisher (University of Cambridge)

Branching from number theory: p-adics in the sciences,
Max Planck Institute for Mathematics in the Sciences in Leipzig,
03/09/2021

university of groningen

Motivation

- Forthcoming work of M. Bhargava, J. Cremona, T. Fisher:

* "The density of hyperelliptic curves over $\mathbb{Q}$ of genus g that have points everywhere locally"

- Hyperelliptic curves given by (affine equation) $C : y^2 = f(x)$, $f \in \mathbb{Z}[x]$.
- Simpler question - when C has an affine Weierstrass point locally?
- Extend to a fixed number of zeros.
- Related work:

* Buhler, Goldstein, Moews, and Rosenberg - p-adic polynomial splitting

* Caruso; Evans; Kulkarni and Lerario; Shmueli (all indenpendently) - expectations of the number of roots of p-adic polynomials

Magic of $\mathbb{Q}_p$

Theorem (Polynomial Hensel's lemma)

- $f \in \mathbb{Z}_p[x]$.
- *Assume that its reduction modulo* p, $\overline{f}$, *factors over* $\mathbb{F}_p[x]$ *as*
- $\overline{f} = \overline{g}\overline{h}$ *such that*
- $\overline{g}, \overline{h} \in \mathbb{F}_p[x]$ *are coprime polynomials in* $\mathbb{F}_p[x]$, *and* g *is monic.*
- *There exists a factorization* $f = gh$ *where*
- $g, h \in \mathbb{Z}_p[x]$, g *and* h *reduce modulo* p *to* $\overline{g}$ *and* $\overline{h}$, *respectively,*
- g *is monic of degree* $\deg(g) = \deg(\overline{g})$.

Magic of $\mathbb{Q}_p$

Theorem (Polynomial Hensel's lemma)

- $f \in \mathbb{Z}_p[x]$.
- *Assume that its reduction modulo* p, $\overline{f}$, *factors over* $\mathbb{F}_p[x]$ *as*
- $\overline{f} = \overline{g}\overline{h}$ *such that*
- $\overline{g}, \overline{h} \in \mathbb{F}_p[x]$ *are coprime polynomials in* $\mathbb{F}_p[x]$, *and* g *is monic.*
- *There exists a factorization* $f = gh$ *where*
- $g, h \in \mathbb{Z}_p[x]$, g *and* h *reduce modulo* p *to* $\overline{g}$ *and* $\overline{h}$, *respectively,*
- g *is monic of degree* $\deg(g) = \deg(\overline{g})$.

Theorem (Hensel's lemma - simple version)

- $f \in \mathbb{Z}_p[x]$.
- $x_0 \in \mathbb{Z}_p$ *is a simple root of* f *modulo* p, *i.e., that* $f(x_0) \equiv 0 \pmod{p}$ *and* $f'(x_0) \not\equiv 0 \pmod{p}$.
- *There is a unique* $X_0 \in \mathbb{Z}_p$ *such that* $X_0 \equiv x_0 \pmod{p}$ *and* $f(X_0) = 0$.

Haar measure on $\mathbb{Z}_p$ and probability

- $\mathbb{Z}_p$ possesses the normalized Haar measure μ_p ($\mu_p(\mathbb{Z}_p) = 1$).

Haar measure on $\mathbb{Z}_p$ and probability

- $\mathbb{Z}_p$ possesses the normalized Haar measure μ_p ($\mu_p(\mathbb{Z}_p) = 1$).
- For any $k \in \mathbb{F}_p$, denote $D_k = \{x \in \mathbb{Z}_p : x \equiv k \pmod{p}\}$.
- Hence, $\mu_p(D_k) = \frac{1}{p}$, for all $k \in \mathbb{F}_p$
- Similarly, $\mu_p(p^m\mathbb{Z}_p + a) = \mu_p(p^m\mathbb{Z}_p) = \frac{1}{p^m}$, for any $a \in \mathbb{Z}_p$.

Haar measure on $\mathbb{Z}_p$ and probability

- $\mathbb{Z}_p$ possesses the normalized Haar measure μ_p ($\mu_p(\mathbb{Z}_p) = 1$).
- For any $k \in \mathbb{F}_p$, denote $D_k = \{x \in \mathbb{Z}_p : x \equiv k \pmod{p}\}$.
- Hence, $\mu_p(D_k) = \frac{1}{p}$, for all $k \in \mathbb{F}_p$
- Similarly, $\mu_p(p^m\mathbb{Z}_p + a) = \mu_p(p^m\mathbb{Z}_p) = \frac{1}{p^m}$, for any $a \in \mathbb{Z}_p$.
- We extend μ_p to $\mathbb{Z}_p^n$ for any $n \in \mathbb{N}$. Then $\mu_p(\mathbb{Z}_p^n) = 1$.

Haar measure on $\mathbb{Z}_p$ and probability

- $\mathbb{Z}_p$ possesses the normalized Haar measure μ_p ($\mu_p(\mathbb{Z}_p) = 1$).
- For any $k \in \mathbb{F}_p$, denote $D_k = \{x \in \mathbb{Z}_p : x \equiv k \pmod{p}\}$.
- Hence, $\mu_p(D_k) = \frac{1}{p}$, for all $k \in \mathbb{F}_p$
- Similarly, $\mu_p(p^m\mathbb{Z}_p + a) = \mu_p(p^m\mathbb{Z}_p) = \frac{1}{p^m}$, for any $a \in \mathbb{Z}_p$.
- We extend μ_p to $\mathbb{Z}_p^n$ for any $n \in \mathbb{N}$. Then $\mu_p(\mathbb{Z}_p^n) = 1$.
- Let $V \subseteq \mathbb{Z}_p^n$. Then $\int_V d\mu_p = \mu_p(V)$.

Haar measure on $\mathbb{Z}_p$ and probability

- $\mathbb{Z}_p$ possesses the normalized Haar measure μ_p ($\mu_p(\mathbb{Z}_p) = 1$).
- For any $k \in \mathbb{F}_p$, denote $D_k = \{x \in \mathbb{Z}_p : x \equiv k \pmod{p}\}$.
- Hence, $\mu_p(D_k) = \frac{1}{p}$, for all $k \in \mathbb{F}_p$
- Similarly, $\mu_p(p^m\mathbb{Z}_p + a) = \mu_p(p^m\mathbb{Z}_p) = \frac{1}{p^m}$, for any $a \in \mathbb{Z}_p$.
- We extend μ_p to $\mathbb{Z}_p^n$ for any $n \in \mathbb{N}$. Then $\mu_p(\mathbb{Z}_p^n) = 1$.
- Let $V \subseteq \mathbb{Z}_p^n$. Then $\int_V d\mu_p = \mu_p(V)$.
- *The density* of $V \subseteq \mathbb{Z}_p^n$ is $\mu_p(V)$.
- The density of $p^m\mathbb{Z}_p$ inside $\mathbb{Z}_p$ is $\frac{1}{p^m}$. "Probability" that a random element $a \in \mathbb{Z}_p$ is divisible by p^m is $\frac{1}{p^m} = \mu_p(p^m\mathbb{Z}_p)$.
- *The probability* of some event parametrised by $\mathbb{Z}_p^n$ is the density of the subset of $\mathbb{Z}_p^n$ on which this event realises.

Haar measure on $\mathbb{Z}_p$ - polynomial probability

- Let R be a ring.
- $R[x]_n$ = all polynomials in $R[x]$ of degree at most n.
- $R[x]_n^1$ = all monic polynomials in $R[x]$ of degree n.

Haar measure on $\mathbb{Z}_p$ - polynomial probability

- Let R be a ring.
- $R[x]_n =$ all polynomials in $R[x]$ of degree at most n.
- $R[x]_n^1 =$ all monic polynomials in $R[x]$ of degree n.
- $f = a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{Z}_p[x]_n \leftrightarrow (a_n, \ldots, a_1, a_0) \in \mathbb{Z}_p^{n+1}$.
- $f = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{Z}_p[x]_n^1 \leftrightarrow (a_{n-1}, \ldots, a_1, a_0) \in \mathbb{Z}_p^n$.

Haar measure on $\mathbb{Z}_p$ - polynomial probability

- Let R be a ring.
- $R[x]_n =$ all polynomials in $R[x]$ of degree at most n.
- $R[x]_n^1 =$ all monic polynomials in $R[x]$ of degree n.
- $f = a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{Z}_p[x]_n \leftrightarrow (a_n, \ldots, a_1, a_0) \in \mathbb{Z}_p^{n+1}$.
- $f = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{Z}_p[x]_n^1 \leftrightarrow (a_{n-1}, \ldots, a_1, a_0) \in \mathbb{Z}_p^n$.
- Consider monic polynomials of degree n that have property $\mathcal{P}$.
- There is $S \in \mathbb{Z}_p^n$ that corresponds to polynomials with property $\mathcal{P}$.
- The probability of property $\mathcal{P}$ is then $\mu_p(S)$ as a subset of $\mathbb{Z}_p^n$.

Strategy

- Consider a problem to determine the probability that a random monic $f \in \mathbb{Z}_p[x]$ of degree n has at least one root in $\mathbb{Q}_p$.

Strategy

- Consider a problem to determine the probability that a random monic $f \in \mathbb{Z}_p[x]$ of degree n has at least one root in $\mathbb{Q}_p$.
- Divide monic polynomials f of degree n into three disjoint subsets:

  (1) those for which $\overline{f}$ has no roots over $\mathbb{F}_p$;

Strategy

- Consider a problem to determine the probability that a random monic $f \in \mathbb{Z}_p[x]$ of degree n has at least one root in $\mathbb{Q}_p$.
- Divide monic polynomials f of degree n into three disjoint subsets:

  (1) those for which $\overline{f}$ has no roots over $\mathbb{F}_p$;

  (2) those for which $\overline{f}$ has a simple root over $\mathbb{F}_p$;

Strategy

- Consider a problem to determine the probability that a random monic $f \in \mathbb{Z}_p[x]$ of degree n has at least one root in $\mathbb{Q}_p$.
- Divide monic polynomials f of degree n into three disjoint subsets:
  (1) those for which $\overline{f}$ has no roots over $\mathbb{F}_p$;
  (2) those for which $\overline{f}$ has a simple root over $\mathbb{F}_p$;
  (3) those for which $\overline{f}$ has roots over $\mathbb{F}_p$, but no simple roots.

Strategy

- Consider a problem to determine the probability that a random monic $f \in \mathbb{Z}_p[x]$ of degree n has at least one root in $\mathbb{Q}_p$.
- Divide monic polynomials f of degree n into three disjoint subsets:
  (1) those for which $\overline{f}$ has no roots over $\mathbb{F}_p$;
  (2) those for which $\overline{f}$ has a simple root over $\mathbb{F}_p$;
  (3) those for which $\overline{f}$ has roots over $\mathbb{F}_p$, but no simple roots.
- Then
  (1) do not have roots over $\mathbb{Q}_p$;

Strategy

- Consider a problem to determine the probability that a random monic $f \in \mathbb{Z}_p[x]$ of degree n has at least one root in $\mathbb{Q}_p$.
- Divide monic polynomials f of degree n into three disjoint subsets:
  (1) those for which $\overline{f}$ has no roots over $\mathbb{F}_p$;
  (2) those for which $\overline{f}$ has a simple root over $\mathbb{F}_p$;
  (3) those for which $\overline{f}$ has roots over $\mathbb{F}_p$, but no simple roots.
- Then
  (1) do not have roots over $\mathbb{Q}_p$;
  (2) Hensel's lemma $\implies$ have at least one root over $\mathbb{Q}_p$;

Strategy

- Consider a problem to determine the probability that a random monic $f \in \mathbb{Z}_p[x]$ of degree n has at least one root in $\mathbb{Q}_p$.
- Divide monic polynomials f of degree n into three disjoint subsets:
  (1) those for which $\overline{f}$ has no roots over $\mathbb{F}_p$;
  (2) those for which $\overline{f}$ has a simple root over $\mathbb{F}_p$;
  (3) those for which $\overline{f}$ has roots over $\mathbb{F}_p$, but no simple roots.
- Then
  (1) do not have roots over $\mathbb{Q}_p$;
  (2) Hensel's lemma $\implies$ have at least one root over $\mathbb{Q}_p$;
  (3) the hardest case, we do not know the exact answer, needs further investigation (need Hensel's lemma for polynomials).

Strategy

- General strategy is

(1) Consider all possible factorisations (=splitting types) of polynomials f over $\mathbb{F}_p$;

Strategy

- General strategy is

(1) Consider all possible factorisations (=splitting types) of polynomials f over $\mathbb{F}_p$;

(2) Compute probabilities of each splitting type;

Strategy

- General strategy is

(1) Consider all possible factorisations (=splitting types) of polynomials f over $\mathbb{F}_p$;

(2) Compute probabilities of each splitting type;

(3) Compute the probability that f has a root in each splitting type.

Strategy

- General strategy is

(1) Consider all possible factorisations (=splitting types) of polynomials f over $\mathbb{F}_p$;

(2) Compute probabilities of each splitting type;

(3) Compute the probability that f has a root in each splitting type.

(4) Sum the products of last two probabilities over all splitting types of degree n.

Strategy

- General strategy is

(1) Consider all possible factorisations (=splitting types) of polynomials f over $\mathbb{F}_p$;

(2) Compute probabilities of each splitting type;

(3) Compute the probability that f has a root in each splitting type.

(4) Sum the products of last two probabilities over all splitting types of degree n.

- $\alpha_n :=$ the probability that a random monic polynomial of degree n has a root in $\mathbb{Q}_p$ (equivalently in $\mathbb{Z}_p$).
- $\beta_n :=$ the same probability under the condition that $f \equiv x^n \pmod{p}$.
- Goal: As practise, compute α_n, β_n.

Irreducible polynomials over $\mathbb{F}_p$

Theorem

The number of monic irreducible polynomials of degree n in $\mathbb{F}_p[x]$ is equal to ($\mu : \mathbb{N} \to \{0, -1, 1\}$ is the Möbius funciton)

$$N_n := \frac{\sum_{k|n} \mu(k) p^{\frac{n}{k}}}{n}.$$

(*) $N_1 = p$;

(*) $N_q = \frac{p^q - p}{q}$ for q a prime number;

(*) $N_{q^2} = \frac{p^{q^2} - p^q}{q^2}$ for q a prime number;

(*) Important: $N_n = \frac{p^n + o(p^n)}{n}$.

Factorization probabilities

- *Splitting type of degree n* is a tuple $\sigma = (d_1^{e_1}\, d_2^{e_2}\, \cdots\, d_t^{e_t})$ where the d_j and e_j are positive integers satisfying $\sum d_j e_j = n$.

Factorization probabilities

- *Splitting type of degree n* is a tuple $\sigma = (d_1^{e_1}\ d_2^{e_2}\ \cdots\ d_t^{e_t})$ where the d_j and e_j are positive integers satisfying $\sum d_j e_j = n$.
- $\mathcal{S}(n) :=$ the set of all splitting types of degree n.
- Fix $\sigma = (d_1^{e_1}\ d_2^{e_2}\ \ldots\ d_t^{e_t}) \in \mathcal{S}(n)$.

Factorization probabilities

- *Splitting type of degree n* is a tuple $\sigma = (d_1^{e_1}\ d_2^{e_2}\ \cdots\ d_t^{e_t})$ where the d_j and e_j are positive integers satisfying $\sum d_j e_j = n$.
- $\mathcal{S}(n) :=$ the set of all splitting types of degree n.
- Fix $\sigma = (d_1^{e_1}\ d_2^{e_2}\ \ldots\ d_t^{e_t}) \in \mathcal{S}(n)$.
- A monic polynomial f in $\mathbb{F}_p[x]$ of degree n has *splitting type* σ if

(1) f factors as $f(x) = \prod_{j=1}^{t} f_j(x)^{e_j}$,

(2) f_j are distinct irreducible monic polynomials over $\mathbb{F}_p$,

(3) $\deg(f_j) = d_j$, for all $1 \leq j \leq t$.

Factorization probabilities

- *Splitting type of degree n* is a tuple $\sigma = (d_1^{e_1}\ d_2^{e_2}\ \cdots\ d_t^{e_t})$ where the d_j and e_j are positive integers satisfying $\sum d_j e_j = n$.
- $\mathcal{S}(n) :=$ the set of all splitting types of degree n.
- Fix $\sigma = (d_1^{e_1}\ d_2^{e_2}\ \ldots\ d_t^{e_t}) \in \mathcal{S}(n)$.
- A monic polynomial f in $\mathbb{F}_p[x]$ of degree n has *splitting type* σ if

(1) f factors as $f(x) = \prod_{j=1}^{t} f_j(x)^{e_j}$,

(2) f_j are distinct irreducible monic polynomials over $\mathbb{F}_p$,

(3) $\deg(f_j) = d_j$, for all $1 \leq j \leq t$.

Irreducible factorization of f	**$\sigma(f)$=splitting type of f**	**Degree**
$x^2(x+1)(x^2+1)(x^3+2)^4$	$(3^4\ 2\ 1^2\ 1)$	17

- $\lambda(\sigma) =$ the probability that a degree n monic polynomial $f \in \mathbb{F}_p[x]$ has splitting type σ - it is a rational function of p.

Degrees $n = 2$ and $n = 3$ - quickly

- Let $f \in \mathbb{Z}_p[x]$ be a monic polynomial of degree $n = 2$ - blackboard.

Degrees $n = 2$ and $n = 3$ - quickly

- Let $f \in \mathbb{Z}_p[x]$ be a monic polynomial of degree $n = 2$ - blackboard.
- Let $f \in \mathbb{Z}_p[x]$ be a monic polynomial of degree $n = 3$.
- We make the table of possible splitting types of $\overline{f}$ over $\mathbb{F}_p$ and the number of them.

(3)	$N_3 = \frac{p^3-p}{3}$
$(2\,1)$	$N_2 N_1 = \frac{p^3-p^2}{2}$
(1^3)	$N_1 = p$
$(1^2\,1)$	$N_1(N_1-1) = p(p-1)$
$(1\,1\,1)$	$\binom{N_1}{3} = \frac{p(p-1)(p-2)}{6}$

Degrees $n = 2$ and $n = 3$ - quickly

- Let $f \in \mathbb{Z}_p[x]$ be a monic polynomial of degree $n = 2$ - blackboard.
- Let $f \in \mathbb{Z}_p[x]$ be a monic polynomial of degree $n = 3$.
- We make the table of possible splitting types of $\overline{f}$ over $\mathbb{F}_p$ and the number of them.

(3)	$N_3 = \frac{p^3-p}{3}$
$(2\,1)$	$N_2 N_1 = \frac{p^3-p^2}{2}$
(1^3)	$N_1 = p$
$(1^2\,1)$	$N_1(N_1-1) = p(p-1)$
$(1\,1\,1)$	$\binom{N_1}{3} = \frac{p(p-1)(p-2)}{6}$

$$\implies \alpha_3 = \frac{p^3-p^2}{2p^3} + \frac{p(p-1)}{p^3} + \frac{p(p-1)(p-2)}{6p^3} + \frac{p}{p^3}\beta_3.$$

Degrees $n = 2$ and $n = 3$ - quickly

- Let $f \in \mathbb{Z}_p[x]$ be a monic polynomial of degree $n = 2$ - blackboard.
- Let $f \in \mathbb{Z}_p[x]$ be a monic polynomial of degree $n = 3$.
- We make the table of possible splitting types of $\overline{f}$ over $\mathbb{F}_p$ and the number of them.

(3)	$N_3 = \frac{p^3-p}{3}$
$(2\,1)$	$N_2 N_1 = \frac{p^3-p^2}{2}$
(1^3)	$N_1 = p$
$(1^2\,1)$	$N_1(N_1-1) = p(p-1)$
$(1\,1\,1)$	$\binom{N_1}{3} = \frac{p(p-1)(p-2)}{6}$

$$\implies \alpha_3 = \frac{p^3-p^2}{2p^3} + \frac{p(p-1)}{p^3} + \frac{p(p-1)(p-2)}{6p^3} + \frac{p}{p^3}\beta_3.$$

- We want to compute β_3 - blackboard.

Degree $n = 4$

- Table of splitting types of degree 4 with probabilities:

(1)	(4)	$N_4 = \frac{p^4-p^2}{4}$	0
(2)	(3 1)	$N_3 N_1 = \frac{p^4-p^2}{3}$	1
(3)	(2^2)	$N_2 = \frac{p^2-p}{2}$	0
(4)	(2 2)	$\binom{N_2}{2} = \frac{(p^2-p)(p^2-p-2)}{8}$	0
(5)	$(2\,1^2)$	$N_2 N_1 = \frac{p^3-p^2}{2}$	β_2
(6)	(2 1 1)	$N_2\binom{N_1}{2} = \frac{p^2(p-1)^2}{4}$	1
(7)	(1^4)	$N_1 = p$	β_4
(8)	$(1^3\,1)$	$N_1(N_1-1) = p(p-1)$	1
(9)	$(1^2\,1^2)$	$\binom{N_1}{2} = \frac{p(p-1)}{2}$	$1-(1-\beta_2)^2$
(10)	$(1^2\,1\,1)$	$N_1\binom{N_1-1}{2} = \frac{p(p-1)(p-2)}{2}$	1
(11)	(1 1 1 1)	$\binom{N_1}{4} = \frac{p(p-1)(p-2)(p-3)}{24}$	1

Case $n = 4$ - continued

Question

Can we in (5) assume that the polynomial which reduces to a square of a linear polynomial is random?

Question

Can we assume in (9) the same thing? Are these two polynomials "independent"?

Case $n = 4$ - continued

Question

Can we in (5) assume that the polynomial which reduces to a square of a linear polynomial is random?

Question

Can we assume in (9) the same thing? Are these two polynomials "independent"?

Answers

Yes - by Hensel's polynomial lemma!

- We know how to express β_4 in terms of α_1, α_2, and α_4.
- $\Longrightarrow$ Compute α_4 and β_4.

Definitions

- Denote the density of the following subset of polynomials in $\mathbb{Z}_p[x]$ having exactly r $(0 \leq r \leq n)$ roots in $\mathbb{Q}_p$

(1*) for degree n polynomials $f \in \mathbb{Z}_p[x]$ by $\rho^*(n, r)$;

(2*) for monic degree n polynomials $f \in \mathbb{Z}_p[x]$ by $\alpha^*(n, r)$;

(3*) for monic degree n polynomials $f \in \mathbb{Z}_p[x]$ such that $f \equiv x^n \pmod{p}$ by $\beta^*(n, r)$.

Definitions

- Denote the density of the following subset of polynomials in $\mathbb{Z}_p[x]$ having exactly r $(0 \leq r \leq n)$ roots in $\mathbb{Q}_p$

(1*) for degree n polynomials $f \in \mathbb{Z}_p[x]$ by $\rho^*(n, r)$;

(2*) for monic degree n polynomials $f \in \mathbb{Z}_p[x]$ by $\alpha^*(n, r)$;

(3*) for monic degree n polynomials $f \in \mathbb{Z}_p[x]$ such that $f \equiv x^n \pmod{p}$ by $\beta^*(n, r)$.

- Consider, for $0 \leq d \leq n$

$$\rho(n, d) = \sum_{r=0}^{n} \binom{r}{d} \rho^*(n, r).$$

- Recall: $\binom{r}{d}$ = the number of subsets of size d of a set of size r.
- $\implies$ $\rho(n, d)$ = the expected number of sets of size d (d-sets) of $\mathbb{Q}_p$-roots of a random polynomial $f \in \mathbb{Z}_p[x]$ of degree n.

Relations

- Denote the expected number of sets of size d (d-sets) ($0 \leq d \leq n$) of $\mathbb{Q}_p$-roots of

(1) a random polynomial $f \in \mathbb{Z}_p[x]$ of degree n by $\rho(n, d)$;

(2) a random monic polynomial $f \in \mathbb{Z}_p[x]$ of degree n by $\alpha(n, d)$;

(3) a random monic polynomial $f \in \mathbb{Z}_p[x]$ of degree n that reduces to x^n modulo p by $\beta(n, d)$.

Relations

- Denote the expected number of sets of size d (d-sets) ($0 \leq d \leq n$) of $\mathbb{Q}_p$-roots of

(1) a random polynomial $f \in \mathbb{Z}_p[x]$ of degree n by $\rho(n, d)$;

(2) a random monic polynomial $f \in \mathbb{Z}_p[x]$ of degree n by $\alpha(n, d)$;

(3) a random monic polynomial $f \in \mathbb{Z}_p[x]$ of degree n that reduces to x^n modulo p by $\beta(n, d)$.

- There is an inversion formula for $0 \leq r \leq n$

$$\rho^*(n, r) = \sum_{d=0}^{n} (-1)^{d-r} \binom{d}{r} \rho(n, d).$$

- Analogous relations hold for α's and β's.
- If we can compute all values of ρ or ρ^*, we can compute all values of the other one.

Examples - expectations of the number of roots

- Results by Caruso; Evans; Kulkarni and Lerario; Shmueli:

$$\alpha(n,1) = \begin{cases} 1 & \text{if } n = 1, \\ \dfrac{p}{p+1} & \text{if } n \geq 2, \end{cases} \qquad \beta(n,1) = \begin{cases} 1 & \text{if } n = 1, \\ \dfrac{1}{p+1} & \text{if } n \geq 2, \end{cases}$$

and

$$\rho(n,1) = 1 \text{ for all } n \geq 1.$$

Examples - small degrees

- Note $\rho^*(n, n-1) = \alpha^*(n, n-1) = \beta^*(n, n-1) = 0$.
- Buhler et al: $\rho^*(n, n) = \rho(n, n)$ and $\alpha^*(n, n) = \alpha(n, n)$.

Examples - small degrees

- Note $\rho^*(n, n-1) = \alpha^*(n, n-1) = \beta^*(n, n-1) = 0$.
- Buhler et al: $\rho^*(n, n) = \rho(n, n)$ and $\alpha^*(n, n) = \alpha(n, n)$.
- $\rho^*(2, 2) = \frac{1}{2} \implies \rho^*(2, 0) = \frac{1}{2}$.
- $\alpha^*(2, 2) = \frac{1}{2}\,\frac{p}{p+1} \implies \alpha^*(2, 0) = \frac{1}{2}\,\frac{p+2}{p+1}$.

Examples - small degrees

- Note $\rho^*(n, n-1) = \alpha^*(n, n-1) = \beta^*(n, n-1) = 0$.
- Buhler et al: $\rho^*(n, n) = \rho(n, n)$ and $\alpha^*(n, n) = \alpha(n, n)$.
- $\rho^*(2,2) = \frac{1}{2} \implies \rho^*(2,0) = \frac{1}{2}$.
- $\alpha^*(2,2) = \frac{1}{2}\,\frac{p}{p+1} \implies \alpha^*(2,0) = \frac{1}{2}\,\frac{p+2}{p+1}$.
- $\rho^*(3,3) = \gamma$, where $\gamma = \frac{(p^2+1)^2}{6(p^4+p^3+p^2+p+1)}$.
- $\rho^*(3,0) + \rho^*(3,1) + \rho^*(3,3) = 1$.
- $1 = \rho(3,1) = \binom{0}{1}\rho^*(3,0) + \binom{1}{1}\rho^*(3,1) + \binom{3}{1}\rho^*(3,3)$.
- $\implies \rho^*(3,0) = 2\gamma,\ \rho^*(3,1) = 1 - 3\gamma$.

Examples - small degrees

- Note $\rho^*(n, n-1) = \alpha^*(n, n-1) = \beta^*(n, n-1) = 0$.
- Buhler et al: $\rho^*(n, n) = \rho(n, n)$ and $\alpha^*(n, n) = \alpha(n, n)$.
- $\rho^*(2,2) = \frac{1}{2} \implies \rho^*(2,0) = \frac{1}{2}$.
- $\alpha^*(2,2) = \frac{1}{2}\frac{p}{p+1} \implies \alpha^*(2,0) = \frac{1}{2}\frac{p+2}{p+1}$.
- $\rho^*(3,3) = \gamma$, where $\gamma = \frac{(p^2+1)^2}{6(p^4+p^3+p^2+p+1)}$.
- $\rho^*(3,0) + \rho^*(3,1) + \rho^*(3,3) = 1$.
- $1 = \rho(3,1) = \binom{0}{1}\rho^*(3,0) + \binom{1}{1}\rho^*(3,1) + \binom{3}{1}\rho^*(3,3)$.
- $\implies \rho^*(3,0) = 2\gamma$, $\rho^*(3,1) = 1 - 3\gamma$.
- $\alpha^*(3,0) = \frac{1}{p+1} + 2\gamma'$, $\alpha^*(3,1) = \frac{p}{p+1} - 3\gamma'$, $\alpha^*(3,3) = \gamma'$, where
- $\gamma' = \frac{1}{6}\frac{p^5-p^4+p^3}{(p+1)(p^4+p^3+p^2+p+1)}$.

Measure-preserving bijections

Lemma

(*) *Let* $A \subset \mathbb{Z}_p[x]^1_m$, $B \subset \mathbb{Z}_p[x]^1_n$, *and* $AB \subset \mathbb{Z}_p[x]^1_{m+n}$ *or*
(*) *Let* $A \subset \mathbb{Z}_p[x]^1_m$, $B \subset \mathbb{Z}_p[x]_n$, *and* $AB \subset \mathbb{Z}_p[x]_{m+n}$
be measurable subsets such that multiplication induces a bijection

$$A \times B \to AB = \{ab \mid a \in A,\ b \in B\}.$$

If the resultant of a *and* b *satisfies* $\mathrm{Res}(a, b) \in \mathbb{Z}_p^*$ *for all* $a \in A, b \in B$, *then the bijection is measure-preserving.*

Measure-preserving bijections

Lemma

(*) *Let* $A \subset \mathbb{Z}_p[x]^1_m$, $B \subset \mathbb{Z}_p[x]^1_n$, *and* $AB \subset \mathbb{Z}_p[x]^1_{m+n}$ *or*
(*) *Let* $A \subset \mathbb{Z}_p[x]^1_m$, $B \subset \mathbb{Z}_p[x]_n$, *and* $AB \subset \mathbb{Z}_p[x]_{m+n}$
be measurable subsets such that multiplication induces a bijection

$$A \times B \to AB = \{ab \mid a \in A,\ b \in B\}.$$

If the resultant of a *and* b *satisfies* $\mathrm{Res}(a,b) \in \mathbb{Z}_p^*$ *for all* $a \in A, b \in B$, *then the bijection is measure-preserving.*

Proof (sketch-idea).

Change of variables is given by the resultant, which is a unit:

$$\int_{(a,b)\in A\times B} d\mu_p = \int_{ab\in AB} |\mathrm{Res}(a,b)|_p d\mu_p = \int_{ab\in AB} d\mu_p.$$

□

Independence of lifts 1

- For $f \in \mathbb{F}_p[x]_n^1$, we define

(1) $P_f := \{F \in \mathbb{Z}_p[x]_n^1, \overline{F} = f\}$;

(2) $P_f^m := \{F \in \mathbb{Z}_p[x]_m, \overline{F} = f\}$ for $m \geq n$.

Independence of lifts 1

- For $f \in \mathbb{F}_p[x]_n^1$, we define

(1) $P_f := \{F \in \mathbb{Z}_p[x]_n^1, \overline{F} = f\}$;

(2) $P_f^m := \{F \in \mathbb{Z}_p[x]_m, \overline{F} = f\}$ for $m \geq n$.

- Let $f = x^2 + 2$. Then

(1) $P_f := \{x^2 + pax + (2 + pb) : a, b \in \mathbb{Z}_p\}$;

(2) $P_f^4 := \{pax^4 + pbx^3 + (1 + pc)x^2 + pdx + (2 + pe) : a, b, c, d, e \in \mathbb{Z}_p\}$;

Independence of lifts 1

- For $f \in \mathbb{F}_p[x]_n^1$, we define

(1) $P_f := \{F \in \mathbb{Z}_p[x]_n^1, \overline{F} = f\}$;

(2) $P_f^m := \{F \in \mathbb{Z}_p[x]_m, \overline{F} = f\}$ for $m \geq n$.

- Let $f = x^2 + 2$. Then

(1) $P_f := \{x^2 + pax + (2 + pb) : a, b \in \mathbb{Z}_p\}$;

(2) $P_f^4 := \{pax^4 + pbx^3 + (1 + pc)x^2 + pdx + (2 + pe) : a, b, c, d, e \in \mathbb{Z}_p\}$;

Lemma

Suppose that $g, h \in \mathbb{F}_p[x]$ are monic and coprime. Then the multiplication map $P_g \times P_h \to P_{gh}$ is a measure-preserving bijection.

Independence of lifts 1

- For $f \in \mathbb{F}_p[x]_n^1$, we define

(1) $P_f := \{F \in \mathbb{Z}_p[x]_n^1, \overline{F} = f\}$;

(2) $P_f^m := \{F \in \mathbb{Z}_p[x]_m, \overline{F} = f\}$ for $m \geq n$.

- Let $f = x^2 + 2$. Then

(1) $P_f := \{x^2 + pax + (2 + pb) : a, b \in \mathbb{Z}_p\}$;

(2) $P_f^4 := \{pax^4 + pbx^3 + (1 + pc)x^2 + pdx + (2 + pe) : a, b, c, d, e \in \mathbb{Z}_p\}$;

Lemma

Suppose that $g, h \in \mathbb{F}_p[x]$ are monic and coprime. Then the multiplication map $P_g \times P_h \to P_{gh}$ is a measure-preserving bijection.

Proof (sketch-idea).

- Hensel's lemma for polynomials $\implies$ $P_g \times P_h \to P_{gh}$ is a bijection.
- Previous lemma $\implies$ it is measure preserving.

Independence of lifts 1

Corollary

Let $g, h \in \mathbb{F}_p[x]$ be coprime monic polynomials. For $f \in P_{gh}$, let π_1 and π_2 denote the projections of P_{gh} onto P_g and P_h, respectively, under the bijection $P_{gh} \to P_g \times P_h$. Then the number of $\mathbb{Q}_p$-roots of $f \in P_{gh}$ is $X + Y$, where $X, Y : P_{gh} \to \{0, 1, 2, \ldots\}$ are independent random variables distributed on $f \in P_{gh}$ as the number of $\mathbb{Q}_p$-roots of $\pi_1(f) \in P_g$ and $\pi_2(f) \in P_h$, respectively.

- $f = f_1 f_2$, $f \in P_{gh}$, $f_1 \in P_g$, $f_2 \in P_h$.
- Intuition: Count the number of roots f as a sum of numbers of roots of f_1 and f_2, which are independent.

Independence of lifts 2

- Let $m \leq n$, and let $B_{m,n} := \{f \in \mathbb{Z}_p[x]_n : \overline{f} \in \mathbb{F}_p[x]^1_m\}$.

Independence of lifts 2

- Let $m \leq n$, and let $B_{m,n} := \{f \in \mathbb{Z}_p[x]_n : \overline{f} \in \mathbb{F}_p[x]^1_m\}$.
- $B_{2,4} = \{pax^4 + pbx^3 + (1+pc)x^2 + dx + e : a, b, c, d, e \in \mathbb{Z}_p\}$
- Note that $\mathbb{Q}_p$-roots of polynomials in P_1^{n-m} are in $\mathbb{Q}_p \backslash \mathbb{Z}_p$.

Independence of lifts 2

- Let $m \leq n$, and let $B_{m,n} := \{f \in \mathbb{Z}_p[x]_n : \overline{f} \in \mathbb{F}_p[x]_m^1\}$.
- $B_{2,4} = \{pax^4 + pbx^3 + (1+pc)x^2 + dx + e : a, b, c, d, e \in \mathbb{Z}_p\}$
- Note that $\mathbb{Q}_p$-roots of polynomials in P_1^{n-m} are in $\mathbb{Q}_p \backslash \mathbb{Z}_p$.

Lemma

For $n \geq m$, the multiplication map

$$\mathbb{Z}_p[x]_m^1 \times P_1^{n-m} \to B_{m,n}$$

is a measure-preserving bijection.

Independence of lifts 2

Corollary

For $f \in B_{m,n}$, let ψ_1 and ψ_2 denote the projections of $B_{m,n}$ onto $\mathbb{Z}_p[x]_m^1$ and P_1^{n-m}, respectively, under the bijection $B_{m,n} \to \mathbb{Z}_p[x]_m^1 \times P_1^{n-m}$. Let $X, Y : B_{m,n} \to \{0, 1, 2, \ldots\}$ be the random variables giving the numbers of roots of $f \in B_{m,n}$ in $\mathbb{Z}_p$ and in $\mathbb{Q}_p \setminus \mathbb{Z}_p$, respectively. Then X and Y are independent random variables distributed on $f \in B_{m,n}$ as the number of $\mathbb{Q}_p$-roots of $\psi_1(f)(x) \in \mathbb{Z}_p[x]_m^1$ and of $\psi_2(f)^{\mathrm{rev}}(x) := x^{n-m}\psi_2(f)(1/x) \in P_{x^{n-m}}$, respectively.

- $f = pa_n x^n + \cdots + pa_{m+1}x^{m+1} + a_m x^m + \cdots + a_1 x + a_0 = f_1 f_2$,
- $f_1 = x^m + \cdots + b_1 x + b_0$, $f_2 = pc_{n-m}x^{n-m} + \cdots + pc_1 x + 1$.
- $g_2 = x^{n-m} + pc_1 x^{n-m-1} + \cdots + pc_{n-m}$.
- Intuition: Count the number of roots f as a sum of numbers of roots of f_1 and g_2, which are independent.

Conditional expectations

(1) Let $f \in \mathbb{F}_p[x]_n^1$.

- $\alpha(n, d \mid f) =$ the expected number of d-sets of $\mathbb{Q}_p$-roots of a polynomial in $P_f \subset \mathbb{Z}_p[x]_n^1$.
- Note $\beta(n, d) = \alpha(n, d \mid x^n)$.

Conditional expectations

(1) Let $f \in \mathbb{F}_p[x]_n^1$.

- $\alpha(n, d \mid f) =$ the expected number of d-sets of $\mathbb{Q}_p$-roots of a polynomial in $P_f \subset \mathbb{Z}_p[x]_n^1$.
- Note $\beta(n, d) = \alpha(n, d \mid x^n)$.

(2) Let $\sigma \in \mathcal{S}(n)$.

- $\alpha(n, d \mid \sigma) =$ the expected number of d-sets of $\mathbb{Q}_p$-roots of a polynomial in $\mathbb{Z}_p[x]_n^1$ whose mod p splitting type is σ.

Writing the α's in terms of the β's

Lemma

Let $g, h \in \mathbb{F}_p[x]$ be monic and coprime. Then

$$\alpha(\deg(gh), d \mid gh) = \sum_{d_1, d_2 \geq 0, d_1 + d_2 = d} \alpha(\deg(g), d_1 \mid g) \cdot \alpha(\deg(h), d_2 \mid h).$$

If h has no roots in $\mathbb{F}_p$, then

$$\alpha(\deg(gh), d \mid gh) = \alpha(\deg(g), d \mid g).$$

Writing the α's in terms of the β's

Lemma

Let $g, h \in \mathbb{F}_p[x]$ be monic and coprime. Then

$$\alpha(\deg(gh), d \mid gh) = \sum_{d_1, d_2 \geq 0, d_1 + d_2 = d} \alpha(\deg(g), d_1 \mid g) \cdot \alpha(\deg(h), d_2 \mid h).$$

If h has no roots in $\mathbb{F}_p$, then

$$\alpha(\deg(gh), d \mid gh) = \alpha(\deg(g), d \mid g).$$

Proof (sketch-idea).

- Independence of lifts 1 + fact
- Fact: $\binom{X+Y}{d} = \sum_{d_1+d_2=d} \binom{X}{d_1}\binom{Y}{d_2}$ for independent random variables X and Y taking values in $\mathbb{N}_0$.

□

Writing the α's in terms of the β's

Example

$$\alpha(8,2 \mid x^2(x+1)(x^2+3)(x^3+2)) = \alpha(3,2 \mid x^2(x+1)) =$$

$$=\alpha(2,2|x^2)\alpha(1,0|x+1)+\alpha(2,1|x^2)\alpha(1,1|x+1)+\alpha(2,0|x^2)\alpha(1,2|x+1)=$$

$$= \beta(2,2)\beta(1,0) + \beta(2,1)\beta(1,1) + \beta(2,0)\beta(1,2) =$$

$$= \beta(2,2)\cdot 1 + \frac{1}{p+1}\cdot 1 + 1\cdot 0 = \frac{3}{2(p+1)}$$

Writing the α's in terms of the β's

Example

$$\alpha(8,2 \mid x^2(x+1)(x^2+3)(x^3+2)) = \alpha(3,2 \mid x^2(x+1)) =$$

$$=\alpha(2,2|x^2)\alpha(1,0|x+1)+\alpha(2,1|x^2)\alpha(1,1|x+1)+\alpha(2,0|x^2)\alpha(1,2|x+1)=$$

$$= \beta(2,2)\beta(1,0) + \beta(2,1)\beta(1,1) + \beta(2,0)\beta(1,2) =$$

$$= \beta(2,2)\cdot 1 + \frac{1}{p+1}\cdot 1 + 1\cdot 0 = \frac{3}{2(p+1)}$$

Corollary

Let $\sigma = (1^{n_1}\cdots 1^{n_k}\cdots) \in \mathcal{S}(n)$ be a splitting type with exactly $k = m_1(\sigma)$ powers of 1. Then

$$\alpha(n,d \mid \sigma) = \sum_{d_1+\cdots+d_k=d} \prod_{i=1}^{k} \beta(n_i,d_i).$$

More about the ρ values

- *Primitive polynomials* $f \in \mathbb{Z}_p[x]$ are those with $\overline{f} \neq 0$.
- We can restrict to primitive polynomials to compute $\rho(n, d)$.
- Let $f \in \mathbb{Z}_p[x]$ be a primitive polynomial of degree n.
- Define $m = \deg(\overline{f})$ to be *the reduced degree* of f.
- For $0 \leq m \leq n$, the density of primitive polynomials $f \in \mathbb{Z}_p[x]_n$ with reduced degree m is $\frac{p-1}{p^{n+1}-1} p^m$.

More about the ρ values

- *Primitive polynomials* $f \in \mathbb{Z}_p[x]$ are those with $\overline{f} \neq 0$.
- We can restrict to primitive polynomials to compute $\rho(n, d)$.
- Let $f \in \mathbb{Z}_p[x]$ be a primitive polynomial of degree n.
- Define $m = \deg(\overline{f})$ to be *the reduced degree* of f.
- For $0 \leq m \leq n$, the density of primitive polynomials $f \in \mathbb{Z}_p[x]_n$ with reduced degree m is $\frac{p-1}{p^{n+1}-1} p^m$.
- $\rho(n, d, m) =$ the expected number of d-sets of $\mathbb{Q}_p$-roots of f as $f \in \mathbb{Z}_p[x]_n$ runs over polynomials of degree n with reduced degree m.
- Conditioning on the value of $m \implies$

Lemma

$$\rho(n, d) = \frac{p-1}{p^{n+1}-1} \sum_{m=0}^{n} p^m \rho(n, d, m).$$

Further formulas between α's, β's and ρ's

Lemma (ρ's in terms of α's and β's)

We have

$$\rho(n,d,m) = \sum_{d_1+d_2=d} \alpha(m,d_1)\cdot\beta(n-m,d_2). \tag{1}$$

Further formulas between α's, β's and ρ's

Lemma (ρ's in terms of α's and β's)

We have

$$\rho(n,d,m) = \sum_{d_1+d_2=d} \alpha(m,d_1)\cdot\beta(n-m,d_2). \tag{1}$$

Proof (sketch-idea).

- f has reduced degree $m \implies f = cg$, with $c \in \mathbb{Z}_p^*$ and $g \in B_{m,n}$.
- $g = g_1 g_2$, with $(g_1, g_2) \in \mathbb{Z}_p[x]_m^1 \times P_1^{n-m}$.
- Use: Independence of lifts 2 + fact.

□

Further formulas between α's, β's and ρ's

Lemma (ρ's in terms of α's and β's)

We have

$$\rho(n,d,m) = \sum_{d_1+d_2=d} \alpha(m,d_1)\cdot\beta(n-m,d_2). \tag{1}$$

Proof (sketch-idea).

- f has reduced degree $m \implies f = cg$, with $c \in \mathbb{Z}_p^*$ and $g \in B_{m,n}$.
- $g = g_1 g_2$, with $(g_1, g_2) \in \mathbb{Z}_p[x]_m^1 \times P_1^{n-m}$.
- Use: Independence of lifts 2 + fact.

□

Lemma (β's in terms of α's)

Fix d non-negative integer. Then for all $n \geq d$ we have

$$\beta(n,d) = p^{-\binom{n}{2}}\alpha(n,d) + (p-1)\sum_{0\leq s<r<n} p^{-\binom{r+1}{2}}p^s\alpha(s,d).$$

Generating functions

- Define the generating functions:

$$\mathcal{A}_d(t) := (1-t)\sum_{n=0}^{\infty}\alpha(n,d)t^n;$$

$$\mathcal{B}_d(t) := (1-t)\sum_{n=0}^{\infty}\beta(n,d)t^n;$$

$$\mathcal{R}_d(t) := (1-t)(1-pt)\sum_{n=0}^{\infty}(p^n+p^{n-1}+\cdots+1)\rho(n,d)t^n.$$

- Previous relations can be nicely expressing using these generating functions.

Main theorem 1+2

Theorem (BCFG)

We have the following power series identities in two variables t and u:

$$\sum_{d=0}^{\infty} \mathcal{A}_d(pt)u^d = \left(\sum_{d=0}^{\infty} \mathcal{B}_d(t)u^d\right)^p;$$

$$\sum_{d=0}^{\infty} \mathcal{R}_d(t)u^d = \left(\sum_{d=0}^{\infty} \mathcal{A}_d(pt)u^d\right)\left(\sum_{d=0}^{\infty} \mathcal{B}_d(t)u^d\right) = \left(\sum_{d=0}^{\infty} \mathcal{B}_d(t)u^d\right)^{p+1};$$

$$\mathcal{B}_d(t) - t\mathcal{B}_d(t/p) = \Phi\left(\mathcal{A}_d(t) - t\mathcal{A}_d(pt)\right),$$

where $\Phi(\sum_{n\geq 0} c_n t^n) = \sum_{n\geq 0} c_n p^{-\binom{n}{2}} t^n$.

Theorem (BCFG)

- $\alpha(n,d)$, $\beta(n,d)$ *and* $\rho(n,d)$ *are rational functions of* p.
- $\rho(n,d)(p) = \rho(n,d)(1/p)$; $\alpha(n,d)(p) = \beta(n,d)(1/p)$.

Main theorem 3

Theorem (BCFG)

- *$\mathcal{A}_d$, $\mathcal{B}_d$ and $\mathcal{R}_d$ are polynomials of degree at most $2d$.*
- *$\alpha(n,d)$, $\beta(n,d)$, and $\rho(n,d)$ are independent of n provided that n is sufficiently large relative to d.*

Main theorem 3

Theorem (BCFG)

- *$\mathcal{A}_d$, $\mathcal{B}_d$ and $\mathcal{R}_d$ are polynomials of degree at most $2d$.*
- *$\alpha(n,d)$, $\beta(n,d)$, and $\rho(n,d)$ are independent of n provided that n is sufficiently large relative to d.*

Proof - Idea.

- Denote the subset of polynomials in $\mathbb{Z}_p[x]_d^1$ that split completely by $\mathbb{Z}_p[x]_d^{1\,\text{split}}$.
- Consider the multiplication map $\mathbb{Z}_p[x]_d^{1\,\text{split}} \times \mathbb{Z}_p[x]_{n-d}^1 \to \mathbb{Z}_p[x]_n^1$.
- $\alpha(n,d)$ is the p-adic measure of the image of the multiplication map, viewed as a multiset.

$$\implies \alpha(n,d) = \int_{g \in \mathbb{Z}_p[x]_d^{1\,\text{split}}} \int_{h \in \mathbb{Z}_p[x]_{n-d}^1} |\operatorname{Res}(g,h)|_p \, dh \, dg.$$

- The inner integral is independent of $n \geq 2d$.

The density of p-adic polynomials with a root

- $1 - \rho^*(n, 0) =$ the probability that a random polynomial of degree n over $\mathbb{Z}_p$ has at least one root over $\mathbb{Q}_p$.
- $\rho^*(n, 0) = \sum_{d=0}^{n} (-1)^d \rho(n, d)$, likewise for the α's and β's.

The density of p-adic polynomials with a root

- $1-\rho^*(n,0)=$ the probability that a random polynomial of degree n over $\mathbb{Z}_p$ has at least one root over $\mathbb{Q}_p$.
- $\rho^*(n,0)=\sum_{d=0}^{n}(-1)^d\rho(n,d)$, likewise for the α's and β's.
- Then

$$\mathcal{A}^*(t):=(1-t)\sum_{n=0}^{\infty}\alpha^*(n,0)t^n=\sum_{d=0}^{\infty}(-1)^d\mathcal{A}_d(t),$$

$$\mathcal{B}^*(t):=(1-t)\sum_{n=0}^{\infty}\beta^*(n,0)t^n=\sum_{d=0}^{\infty}(-1)^d\mathcal{B}_d(t),$$

$$\mathcal{R}^*(t):=(1-t)(1-pt)\sum_{n=0}^{\infty}\frac{p^{n+1}-1}{p-1}\rho^*(n,0)t^n=\sum_{d=0}^{\infty}(-1)^d\mathcal{R}_d(t).$$

More results

- Our theorem specialises to (by setting $u = -1$)

Theorem

$$\mathcal{A}^*(pt) = \mathcal{B}^*(t)^p,$$

$$\mathcal{R}^*(t) = \mathcal{A}^*(pt)\mathcal{B}^*(t) = \mathcal{B}^*(t)^{p+1},$$

$$\mathcal{B}^*(t) - t\mathcal{B}^*(t/p) = \Phi(\mathcal{A}^*(t) - t\mathcal{B}^*(pt)),$$

where Φ is as before.
The same symmetry in p holds.

More results

- Our theorem specialises to (by setting $u = -1$)

Theorem

$$\mathcal{A}^*(pt) = \mathcal{B}^*(t)^p,$$

$$\mathcal{R}^*(t) = \mathcal{A}^*(pt)\mathcal{B}^*(t) = \mathcal{B}^*(t)^{p+1},$$

$$\mathcal{B}^*(t) - t\mathcal{B}^*(t/p) = \Phi(\mathcal{A}^*(t) - t\mathcal{B}^*(pt)),$$

where Φ is as before.
The same symmetry in p holds.

- Asymptotic results when $p \to \infty$ and $n \to \infty$.

The end

Thank you for your attention!

Question

Any questions?

Asymptotic results when $p \to \infty$

Proposition

(a) Let $0 \leq d \leq n$ be integers. Then

$$\lim_{p\to\infty} \alpha(n,d) = \lim_{p\to\infty} \rho(n,d) = \frac{1}{d!}.$$

(b) Let $0 \leq r \leq n$ be integers. Then

$$\lim_{p\to\infty} \rho^*(n,r) = \lim_{p\to\infty} \alpha^*(n,r) = \sum_{d=0}^{n} (-1)^{d-r} \binom{d}{r} \frac{1}{d!} = \frac{1}{r!} \sum_{d=0}^{n-r} (-1)^d \frac{1}{d!}.$$

Hence, if we also let $n \to \infty$, we obtain

$$\lim_{n\to\infty} \lim_{p\to\infty} \rho^*(n,r) = \lim_{n\to\infty} \lim_{p\to\infty} \alpha^*(n,r) = \frac{1}{r!} e^{-1}.$$