What is the probability that a (sparse) polynomial of degree d over a finite field is irreducible?

Kaloyan Slavov

ETH Zürich

September 8, 2020

Let $d \geq 1$ and let $\mathbb{F}_q$ be a finite field (large q).

Let $d \geq 1$ and let $\mathbb{F}_q$ be a finite field (large q).

Question (Gauss)

What is the probability that a random polynomial

$$T^d + a_{d-1}T^{d-1} + \cdots + a_1 T + a_0 \in \mathbb{F}_q[T]$$

is irreducible?

Let $d \geq 1$ and let $\mathbb{F}_q$ be a finite field (large q).

Question (Gauss)

What is the probability that a random polynomial

$$T^d + a_{d-1}T^{d-1} + \cdots + a_1 T + a_0 \in \mathbb{F}_q[T]$$

is irreducible?

d	total	reducible types	# reducible	Prob - reducible	Prob - irred.
1	q				
2	q^2				
3	q^3				

Let $d \geq 1$ and let $\mathbb{F}_q$ be a finite field (large q).

Question (Gauss)

What is the probability that a random polynomial

$$T^d + a_{d-1}T^{d-1} + \cdots + a_1 T + a_0 \in \mathbb{F}_q[T]$$

is irreducible?

d	total	reducible types	# reducible	Prob - reducible	Prob - irred.
1	q		0	0	1
2	q^2				
3	q^3				

Let $d \geq 1$ and let $\mathbb{F}_q$ be a finite field (large q).

Question (Gauss)

What is the probability that a random polynomial

$$T^d + a_{d-1}T^{d-1} + \cdots + a_1 T + a_0 \in \mathbb{F}_q[T]$$

is irreducible?

d	total	reducible types	# reducible	Prob - reducible	Prob - irred.
1	q		0	0	1
2	q^2	$(T+a)(T+b)$			
3	q^3				

Let $d \geq 1$ and let $\mathbb{F}_q$ be a finite field (large q).

Question (Gauss)

What is the probability that a random polynomial

$$T^d + a_{d-1}T^{d-1} + \cdots + a_1 T + a_0 \in \mathbb{F}_q[T]$$

is irreducible?

d	total	reducible types	# reducible	Prob - reducible	Prob - irred.
1	q		0	0	1
2	q^2	$(T+a)(T+b)$	$\approx \binom{q}{2}$	$\approx \frac{1}{2}$	$\approx \frac{1}{2}$
3	q^3				

Let $d \geq 1$ and let $\mathbb{F}_q$ be a finite field (large q).

Question (Gauss)

What is the probability that a random polynomial

$$T^d + a_{d-1}T^{d-1} + \cdots + a_1 T + a_0 \in \mathbb{F}_q[T]$$

is irreducible?

d	total	reducible types	# reducible	Prob - reducible	Prob - irred.
1	q		0	0	1
2	q^2	$(T+a)(T+b)$	$\approx \binom{q}{2}$	$\approx \frac{1}{2}$	$\approx \frac{1}{2}$
3	q^3	$(T+a)(T+b)(T+c)$ $(T+a)(T^2+bT+c)$			

Let $d \geq 1$ and let $\mathbb{F}_q$ be a finite field (large q).

Question (Gauss)

What is the probability that a random polynomial

$$T^d + a_{d-1}T^{d-1} + \cdots + a_1 T + a_0 \in \mathbb{F}_q[T]$$

is irreducible?

d	total	reducible types	# reducible	Prob - reducible	Prob - irred.
1	q		0	0	1
2	q^2	$(T+a)(T+b)$	$\approx \binom{q}{2}$	$\approx \frac{1}{2}$	$\approx \frac{1}{2}$
3	q^3	$(T+a)(T+b)(T+c)$ $(T+a)(T^2+bT+c)$	$\approx \binom{q}{3} + q.\frac{q^2}{2}$	$\approx \frac{1}{6} + \frac{1}{2} = \frac{2}{3}$	$\approx \frac{1}{3}$

Let $d \geq 1$ and let $\mathbb{F}_q$ be a finite field (large q).

Theorem (Gauss)

The probability that a random polynomial

$$T^d + a_{d-1}T^{d-1} + \cdots + a_1 T + a_0 \in \mathbb{F}_q[T]$$

is irreducible is $\approx 1/d$.

d	total	reducible types	# reducible	Prob - reducible	Prob - irred.
1	q		0	0	1
2	q^2	$(T+a)(T+b)$	$\approx \binom{q}{2}$	$\approx \frac{1}{2}$	$\approx \frac{1}{2}$
3	q^3	$(T+a)(T+b)(T+c)$ $(T+a)(T^2+bT+c)$	$\approx \binom{q}{3} + q.\frac{q^2}{2}$	$\approx \frac{1}{6} + \frac{1}{2} = \frac{2}{3}$	$\approx \frac{1}{3}$

Question

Let $f(T) \in \mathbb{F}_q[T]$ be monic of degree d. Is it true that as $s, b \in \mathbb{F}_q$,

$$\mathrm{Prob}\left(f(T) + sT + b \text{ is irreducible in } \mathbb{F}_q[T]\right) \approx 1/d \ ?$$

Question

Let $f(T) \in \mathbb{F}_q[T]$ be monic of degree d. Is it true that as $s, b \in \mathbb{F}_q$,

$$\operatorname{Prob}\left(f(T) + sT + b \text{ is irreducible in } \mathbb{F}_q[T]\right) \approx 1/d\ ?$$

Usually, yes.

$$\operatorname{Prob}\left(T^5 + T^4 - 2T^3 + sT + b \text{ is irreducible in } \mathbb{F}_{11}[T]\right)$$

Question

Let $f(T) \in \mathbb{F}_q[T]$ be monic of degree d. Is it true that as $s, b \in \mathbb{F}_q$,

$$\mathrm{Prob}\left(f(T) + sT + b \text{ is irreducible in } \mathbb{F}_q[T]\right) \approx 1/d \ ?$$

Usually, yes.

$$\mathrm{Prob}\left(T^5 + T^4 - 2T^3 + sT + b \text{ is irreducible in } \mathbb{F}_{11}[T]\right) = 34/11^2 = 0.202 \approx 0.2 \quad \checkmark$$

Question

Let $f(T) \in \mathbb{F}_q[T]$ be monic of degree d. Is it true that as $s, b \in \mathbb{F}_q$,

$$\mathrm{Prob}\left(f(T) + sT + b \text{ is irreducible in } \mathbb{F}_q[T]\right) \approx 1/d \ ?$$

Usually, yes.

$$\mathrm{Prob}\left(T^5 + T^4 - 2T^3 + sT + b \text{ is irreducible in } \mathbb{F}_{11}[T]\right) = 34/11^2 = 0.202 \approx 0.2 \quad ✓$$

But sometimes, no.

Question

Let $f(T) \in \mathbb{F}_q[T]$ be monic of degree d. Is it true that as $s, b \in \mathbb{F}_q$,

$$\operatorname{Prob}\left(f(T) + sT + b \text{ is irreducible in } \mathbb{F}_q[T]\right) \approx 1/d \text{ ?}$$

Usually, yes.

$$\operatorname{Prob}\left(T^5 + T^4 - 2T^3 + sT + b \text{ is irreducible in } \mathbb{F}_{11}[T]\right) = 34/11^2 = 0.202 \approx 0.2 \quad ✓$$

But sometimes, no.

$$\operatorname{Prob}\left(T^7 + sT + b \text{ is irreducible in } \mathbb{F}_{2^{10}}[T]\right) = 0.29... \not\approx 0.14 \quad ✗$$

Question

Let $f(T) \in \mathbb{F}_q[T]$ be monic of degree d. Is it true that as $s, b \in \mathbb{F}_q$,

$$\mathrm{Prob}\left(f(T) + sT + b \text{ is irreducible in } \mathbb{F}_q[T]\right) \approx 1/d \ ?$$

Usually, yes.

$$\mathrm{Prob}\left(T^5 + T^4 - 2T^3 + sT + b \text{ is irreducible in } \mathbb{F}_{11}[T]\right) = 34/11^2 = 0.202 \approx 0.2 \quad ✓$$

But sometimes, no.

$$\mathrm{Prob}\left(T^7 + sT + b \text{ is irreducible in } \mathbb{F}_{2^{10}}[T]\right) = 0.29... \not\approx 0.14 \quad ✗$$

$$\mathrm{Prob}\left(T^{27} - T^9 + T^3 + sT + b \text{ is irreducible in } \mathbb{F}_{3^{20}}[T]\right) = 0 \not\approx 1/27 \quad ✗$$

Theorem (Bank, Bary–Soroker, Rosenzweig'2015)

Let $f(T) \in \mathbb{F}_q[T]$ *be monic of degree* d. *Then as* $s, b \in \mathbb{F}_q$,

$$\mathrm{Prob}\left(f(T) + sT + b \text{ is irreducible in } \mathbb{F}_q[T]\right) = 1/d + O_d(q^{-1/2}).$$

Theorem (Bank, Bary–Soroker, Rosenzweig'2015)

Let $f(T) \in \mathbb{F}_q[T]$ *be monic of degree* d. *Suppose* $(d(d-1), q) = 1$. *Then as* $s, b \in \mathbb{F}_q$,

$$\mathrm{Prob}\left(f(T) + sT + b \text{ is irreducible in } \mathbb{F}_q[T]\right) = 1/d + O_d(q^{-1/2}).$$

Theorem (Bank, Bary–Soroker, Rosenzweig'2015)

Let $f(T) \in \mathbb{F}_q[T]$ *be monic of degree* d. *Suppose* $(d(d-1), q) = 1$. *Then as* $s, b \in \mathbb{F}_q$,

$$\operatorname{Prob}\Big(f(T) + sT + b \text{ is irreducible in } \mathbb{F}_q[T]\Big) = 1/d + O_d(q^{-1/2}).$$

Proposition (Kurlberg, Rosenzweig; Jarden, Razon)

Let $f(T) \in \mathbb{F}_q[T]$ *be monic of degree* d. *Suppose* $f'' \neq 0$ *and* $(q, d) = 1$.

Theorem (Bank, Bary–Soroker, Rosenzweig'2015)

Let $f(T) \in \mathbb{F}_q[T]$ be monic of degree d. Suppose $(d(d-1), q) = 1$. Then as $s, b \in \mathbb{F}_q$,

$$\mathrm{Prob}\left(f(T) + sT + b \text{ is irreducible in } \mathbb{F}_q[T]\right) = 1/d + O_d(q^{-1/2}).$$

Proposition (Kurlberg, Rosenzweig; Jarden, Razon)

Let $f(T) \in \mathbb{F}_q[T]$ be monic of degree d. Suppose $f'' \neq 0$ and $(q, d) = 1$. Then for all but $O_d(1)$ values of $s \in \mathbb{F}_q$, the polynomial $f(T) + sT$ is a Morse polynomial;

Theorem (Bank, Bary–Soroker, Rosenzweig'2015)

Let $f(T) \in \mathbb{F}_q[T]$ be monic of degree d. Suppose $(d(d-1), q) = 1$. Then as $s, b \in \mathbb{F}_q$,

$$\mathrm{Prob}\left(f(T) + sT + b \text{ is irreducible in } \mathbb{F}_q[T]\right) = 1/d + O_d(q^{-1/2}).$$

Proposition (Kurlberg, Rosenzweig; Jarden, Razon)

Let $f(T) \in \mathbb{F}_q[T]$ be monic of degree d. Suppose $f'' \neq 0$ and $(q, d) = 1$. Then for all but $O_d(1)$ values of $s \in \mathbb{F}_q$, the polynomial $f(T) + sT$ is a Morse polynomial; as $b \in \mathbb{F}_q$,

$$\mathrm{Prob}\left(f(T) + sT + b \text{ is irreducible in } \mathbb{F}_q[T]\right) = 1/d + O_d(q^{-1/2}).$$

Theorem (Bank, Bary–Soroker, Rosenzweig'2015)

Let $f(T) \in \mathbb{F}_q[T]$ be monic of degree d. Suppose $(d(d-1), q) = 1$. Then as $s, b \in \mathbb{F}_q$,

$$\mathrm{Prob}\left(f(T) + sT + b \text{ is irreducible in } \mathbb{F}_q[T]\right) = 1/d + O_d(q^{-1/2}).$$

Proposition (Kurlberg, Rosenzweig; Jarden, Razon)

Let $f(T) \in \mathbb{F}_q[T]$ be monic of degree d. Suppose $f'' \neq 0$ and $(q, d) = 1$. Then for all but $O_d(1)$ values of $s \in \mathbb{F}_q$, the polynomial $f(T) + sT$ is a Morse polynomial; as $b \in \mathbb{F}_q$,

$$\mathrm{Prob}\left(f(T) + sT + b \text{ is irreducible in } \mathbb{F}_q[T]\right) = 1/d + O_d(q^{-1/2}).$$

For $f(T) = \sum a_i T^i$, define $D^2 f = \sum a_i \binom{i}{2} T^{i-2}$ (second Hasse derivative).

For $f \in \mathbb{F}_q[T]$, write $f(x) - f(y) = (x-y)\widetilde{f}(x,y)$ in $\mathbb{F}_q[x,y]$.

For $f \in \mathbb{F}_q[T]$, write $f(x) - f(y) = (x-y)\widetilde{f}(x,y)$ in $\mathbb{F}_q[x,y]$.

Theorem (S'2020)

Let $f(T) \in \mathbb{F}_q[T]$ be monic of degree d. Suppose

Then for all but $d^2 - d - 1$ values of $s \in \mathbb{F}_q$: as $b \in \mathbb{F}_q$,

$$\mathrm{Prob}\left(f(T) + sT + b \text{ is irreducible in } \mathbb{F}_q[T]\right) = 1/d + O_d(q^{-1/2}).$$

For $f \in \mathbb{F}_q[T]$, write $f(x) - f(y) = (x-y)\widetilde{f}(x,y)$ in $\mathbb{F}_q[x,y]$.

Theorem (S'2020)

Let $f(T) \in \mathbb{F}_q[T]$ be monic of degree d. Suppose

Then for all but $d^2 - d - 1$ values of $s \in \mathbb{F}_q$: as $b \in \mathbb{F}_q$,

$$\mathrm{Prob}\left(f(T) + sT + b \text{ is irreducible in } \mathbb{F}_q[T]\right) = 1/d + O_d(q^{-1/2}).$$

Corollary (S'2020)

Let $f(T) \in \mathbb{F}_q[T]$ be a polynomial as above. Then as $s, b \in \mathbb{F}_q$,

$$\mathrm{Prob}\left(f(T) + sT + b \text{ is irreducible in } \mathbb{F}_q[T]\right) = 1/d + O_d(q^{-1/2}).$$

For $f \in \mathbb{F}_q[T]$, write $f(x) - f(y) = (x-y)\widetilde{f}(x,y)$ in $\mathbb{F}_q[x,y]$.

Theorem (S'2020)

Let $f(T) \in \mathbb{F}_q[T]$ *be monic of degree* d. *Suppose* $\deg f' \geq 1$,

Then for all but $d^2 - d - 1$ *values of* $s \in \mathbb{F}_q$: *as* $b \in \mathbb{F}_q$,

$$\mathrm{Prob}\left(f(T) + sT + b \text{ is irreducible in } \mathbb{F}_q[T]\right) = 1/d + O_d(q^{-1/2}).$$

Corollary (S'2020)

Let $f(T) \in \mathbb{F}_q[T]$ *be a polynomial as above. Then as* $s, b \in \mathbb{F}_q$,

$$\mathrm{Prob}\left(f(T) + sT + b \text{ is irreducible in } \mathbb{F}_q[T]\right) = 1/d + O_d(q^{-1/2}).$$

For $f \in \mathbb{F}_q[T]$, write $f(x) - f(y) = (x-y)\widetilde{f}(x,y)$ in $\mathbb{F}_q[x,y]$.

Theorem (S'2020)

Let $f(T) \in \mathbb{F}_q[T]$ be monic of degree d. Suppose $\deg f' \geq 1$, $D^2 f \neq 0$, and

Then for all but $d^2 - d - 1$ values of $s \in \mathbb{F}_q$: as $b \in \mathbb{F}_q$,

$$\mathrm{Prob}\left(f(T) + sT + b \text{ is irreducible in } \mathbb{F}_q[T]\right) = 1/d + O_d(q^{-1/2}).$$

Corollary (S'2020)

Let $f(T) \in \mathbb{F}_q[T]$ be a polynomial as above. Then as $s, b \in \mathbb{F}_q$,

$$\mathrm{Prob}\left(f(T) + sT + b \text{ is irreducible in } \mathbb{F}_q[T]\right) = 1/d + O_d(q^{-1/2}).$$

For $f \in \mathbb{F}_q[T]$, write $f(x) - f(y) = (x-y)\widetilde{f}(x,y)$ in $\mathbb{F}_q[x,y]$.

Theorem (S'2020)

Let $f(T) \in \mathbb{F}_q[T]$ be monic of degree d. Suppose $\deg f' \geq 1$, $D^2 f \neq 0$, and

$$\gcd\left(\widetilde{f}(x,y) - f'(x), \widetilde{f}'(x,y)\right) = (x-y)^t \quad \textit{in} \quad k[x,y], \quad \textit{for some } t \geq 0.$$

Then for all but $d^2 - d - 1$ values of $s \in \mathbb{F}_q$: as $b \in \mathbb{F}_q$,

$$\mathrm{Prob}\left(f(T) + sT + b \text{ is irreducible in } \mathbb{F}_q[T]\right) = 1/d + O_d(q^{-1/2}).$$

Corollary (S'2020)

Let $f(T) \in \mathbb{F}_q[T]$ be a polynomial as above. Then as $s, b \in \mathbb{F}_q$,

$$\mathrm{Prob}\left(f(T) + sT + b \text{ is irreducible in } \mathbb{F}_q[T]\right) = 1/d + O_d(q^{-1/2}).$$

For $f \in \mathbb{F}_q[T]$, write $f(x) - f(y) = (x-y)\widetilde{f}(x,y)$ in $\mathbb{F}_q[x,y]$.

Theorem (S'2020)

Let $f(T) \in \mathbb{F}_q[T]$ be monic of degree d. Suppose $\deg f' \geq 1$, $D^2 f \neq 0$, and

$$\gcd\left(\widetilde{f}(x,y) - f'(x), \widetilde{f}'(x,y)\right) = (x-y)^t \quad \textit{in} \quad k[x,y], \quad \textit{for some } t \geq 0.$$

Then for all but $d^2 - d - 1$ values of $s \in \mathbb{F}_q$: as $b \in \mathbb{F}_q$,

$$\mathrm{Prob}\left(f(T) + sT + b \text{ is irreducible in } \mathbb{F}_q[T]\right) = 1/d + O_d(q^{-1/2}).$$

Corollary (S'2020)

Let $f(T) \in \mathbb{F}_q[T]$ be a polynomial as above. Then as $s, b \in \mathbb{F}_q$,

$$\mathrm{Prob}\left(f(T) + sT + b \text{ is irreducible in } \mathbb{F}_q[T]\right) = 1/d + O_d(q^{-1/2}).$$

E.g. $$\mathrm{Prob}\left(T^{12} + T^3 + sT + b \text{ is irreducible in } \mathbb{F}_{2^n}[T]\right) \approx 1/12.$$

Proof. Let $s \in \mathbb{F}_q$. Consider
$$\begin{aligned} \varphi_s \colon \mathbb{A}^1 &\longrightarrow \mathbb{A}^1 \\ t &\longmapsto -f(t) - st \end{aligned}$$
whose fiber over b is the set of roots of $f(T) + sT + b$.

Proof. Let $s \in \mathbb{F}_q$. Consider

$$\begin{aligned}\varphi_s \colon \mathbb{A}^1 &\longrightarrow \mathbb{A}^1\\ t &\longmapsto -f(t) - st\end{aligned}$$

whose fiber over b is the set of roots of $f(T) + sT + b$.

$$\Downarrow$$

φ_s has geometric monodromy S_d

$\Downarrow$ [Chebotarev]

Proof. Let $s \in \mathbb{F}_q$. Consider
$$\begin{aligned} \varphi_s \colon \mathbb{A}^1 &\longrightarrow \mathbb{A}^1 \\ t &\longmapsto -f(t) - st \end{aligned}$$
whose fiber over b is the set of roots of $f(T) + sT + b$.

$$\Downarrow$$

φ_s has geometric monodromy S_d

$$\Downarrow \text{ [Chebotarev]}$$

$$\frac{\#\{b \in \mathbb{F}_q \mid f(T) + sT + b \text{ is irreducible}\}}{q} = \frac{\#\{\pi \in S_d \mid \pi \text{ is a cycle}\}}{\#S_d} + O(q^{-1/2})$$

Proof. Let $s \in \mathbb{F}_q$. Consider

$$\begin{aligned} \varphi_s \colon \mathbb{A}^1 &\longrightarrow \mathbb{A}^1 \\ t &\longmapsto -f(t) - st \end{aligned}$$

whose fiber over b is the set of roots of $f(T) + sT + b$.

$$\Downarrow$$

φ_s has geometric monodromy S_d

$$\Downarrow \text{ [Chebotarev]}$$

$$\begin{aligned} \frac{\#\{b \in \mathbb{F}_q \mid f(T) + sT + b \text{ is irreducible}\}}{q} &= \frac{\#\{\pi \in S_d \mid \pi \text{ is a cycle}\}}{\#S_d} + O(q^{-1/2}) \\ &= 1/d + O(q^{-1/2}). \end{aligned}$$

Proof. Let $s \in \mathbb{F}_q$. Consider
$$\begin{aligned} \varphi_s \colon \mathbb{A}^1 &\longrightarrow \mathbb{A}^1 \\ t &\longmapsto -f(t) - st \end{aligned}$$
whose fiber over b is the set of roots of $f(T) + sT + b$.

1)
2)

$\Downarrow$ [Ballico, Hefez'1986]

φ_s has geometric monodromy S_d

$\Downarrow$ [Chebotarev]

$$\begin{aligned} \frac{\#\{b \in \mathbb{F}_q \mid f(T) + sT + b \text{ is irreducible}\}}{q} &= \frac{\#\{\pi \in S_d \mid \pi \text{ is a cycle}\}}{\#S_d} + O(q^{-1/2}) \\ &= 1/d + O(q^{-1/2}). \end{aligned}$$

Proof. Let $s \in \mathbb{F}_q$. Consider
$$\begin{aligned} \varphi_s \colon \mathbb{A}^1 &\longrightarrow \mathbb{A}^1 \\ t &\longmapsto -f(t) - st \end{aligned}$$
whose fiber over b is the set of roots of $f(T) + sT + b$.

1) $\exists\, b \in \overline{\mathbb{F}_q}$ such that $f(T) + sT + b = (T-\alpha)^2(T-\beta_1)\ldots(T-\beta_{d-2})$ in $\overline{\mathbb{F}_q}[T]$.
2)

$\Downarrow$ [Ballico, Hefez'1986]

φ_s has geometric monodromy S_d

$\Downarrow$ [Chebotarev]

$$\begin{aligned} \frac{\#\{b \in \mathbb{F}_q \mid f(T) + sT + b \text{ is irreducible}\}}{q} &= \frac{\#\{\pi \in S_d \mid \pi \text{ is a cycle}\}}{\# S_d} + O(q^{-1/2}) \\ &= 1/d + O(q^{-1/2}). \end{aligned}$$

Proof. Let $s \in \mathbb{F}_q$. Consider

$$\begin{aligned} \varphi_s \colon \mathbb{A}^1 &\longrightarrow \mathbb{A}^1 \\ t &\longmapsto -f(t) - st \end{aligned}$$

whose fiber over b is the set of roots of $f(T) + sT + b$.

1) $\exists\, b \in \overline{\mathbb{F}_q}$ such that $f(T) + sT + b = (T-\alpha)^2(T-\beta_1)\ldots(T-\beta_{d-2})$ in $\overline{\mathbb{F}_q}[T]$.
2) $\widetilde{f}(x,y) + s$ is irreducible over $\overline{\mathbb{F}_q}$.

$\Downarrow$ [Ballico, Hefez'1986]

φ_s has geometric monodromy S_d

$\Downarrow$ [Chebotarev]

$$\begin{aligned} \frac{\#\{b \in \mathbb{F}_q \mid f(T) + sT + b \text{ is irreducible}\}}{q} &= \frac{\#\{\pi \in S_d \mid \pi \text{ is a cycle}\}}{\#S_d} + O(q^{-1/2}) \\ &= 1/d + O(q^{-1/2}). \end{aligned}$$

Let k be an algebraically closed field.

Let k be an algebraically closed field.

Theorem (Stein'1989; Lorenzini'1993)

Let $g \in k[x, y]$. Then $g(x, y) + s$ is irreducible for all but $\deg g - 1$ values of s

Let k be an algebraically closed field.

Theorem (Stein'1989; Lorenzini'1993)

Let $g \in k[x, y]$. Then $g(x, y) + s$ is irreducible for all but $\deg g - 1$ values of s

Note: $(x + 2y)^4 + 3(x + 2y)^2 + (x + 2y) + s \in k[x, y]$ always reducible.

Let k be an algebraically closed field.

Theorem (Stein'1989; Lorenzini'1993)

Let $g \in k[x, y]$. Then $g(x, y) + s$ is irreducible for all but $\deg g - 1$ values of s, unless g is of the form $Q(h(x, y))$ with $\deg Q > 1$.

Note: $(x + 2y)^4 + 3(x + 2y)^2 + (x + 2y) + s \in k[x, y]$ always reducible.

Let k be an algebraically closed field.

Theorem (Stein'1989; Lorenzini'1993)

Let $g \in k[x,y]$. Then $g(x,y)+s$ is irreducible for all but $\deg g - 1$ values of s, unless g is of the form $Q(h(x,y))$ with $\deg Q > 1$.

Note: $(x+2y)^4 + 3(x+2y)^2 + (x+2y) + s \in k[x,y]$ always reducible.

Recall $\widetilde{f}(x,y) = (f(x)-f(y))/(x-y)$.

Let k be an algebraically closed field.

Theorem (Stein'1989; Lorenzini'1993)

Let $g \in k[x,y]$. Then $g(x,y)+s$ is irreducible for all but $\deg g - 1$ values of s, unless g is of the form $Q(h(x,y))$ with $\deg Q > 1$.

Note: $(x+2y)^4 + 3(x+2y)^2 + (x+2y) + s \in k[x,y]$ always reducible.

Recall $\widetilde{f}(x,y) = (f(x)-f(y))/(x-y)$.

Lemma (S'2015)

A polynomial $\widetilde{f}(x,y)$ is not of the form $Q(h(x,y))$ with $\deg Q > 1$, unless $\operatorname{char} k = p$ and $f(T) = \sum a_i T^{p^i} + a_0$.

Proposition (Kurlberg, Rosenzweig; Jarden, Razon)

Let $f(T) \in \mathbb{F}_q[T]$ *be monic of degree* d*. Suppose* $f'' \neq 0$ *and* $(q, d) = 1$*. Then ...*

Theorem (S'2020)

Let $f(T) \in \mathbb{F}_q[T]$ *be monic of degree* d*. Suppose* $\deg f' \geq 1$, $D^2 f \neq 0$, *and*

$$\gcd\left(\widetilde{f}(x,y) - f'(x), \widetilde{f'}(x,y)\right) = (x-y)^t \quad \textit{in} \quad k[x,y], \quad \textit{for some } t \geq 0.$$

Then ...

Proposition (Kurlberg, Rosenzweig; Jarden, Razon)

Let $f(T) \in \mathbb{F}_q[T]$ *be monic of degree* d*. Suppose* $f'' \neq 0$ *and* $(q, d) = 1$*. Then ...*

Theorem (S'2020)

Let $f(T) \in \mathbb{F}_q[T]$ *be monic of degree* d*. Suppose* $\deg f' \geq 1$, $D^2 f \neq 0$, *and*

$$\gcd\left(\widetilde{f}(x,y) - f'(x), \widetilde{f'}(x,y)\right) = (x-y)^t \quad \textit{in} \quad k[x,y], \quad \textit{for some } t \geq 0.$$

Then ...

Conjecture

Let $f(T) \in k[T]$*, where* k *is an algebraically closed field. Suppose* $f'' \neq 0$*. Then*

$$\gcd\left(\widetilde{f}(x,y) - f'(x), \widetilde{f'}(x,y)\right) = 1.$$