A proof of Bary-Soroker & Kozma’s irreducibility theorem
Irreducibility of random polynomials study group, Week 5

Robin Visser
Mathematics Institute
University of Warwick

11 February 2022
Let $L$ be a positive integer divisible by at least 4 distinct primes (e.g. $L = 210$). Let

$$f := X^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0$$

be a random polynomial over $\mathbb{Z}$, where $a_0, \ldots, a_{n-1}$ are independent random variables taking values uniformly in $\{1, \ldots, L\}$. Then

$$\mathbb{P}(f \text{ is irreducible}) \to 1 \quad \text{as } n \to \infty$$
Sketch

- Let $f_p$ denote the reduction of $f \mod p$, for any prime $p$ dividing $L$.
Sketch

• Let $f_p$ denote the reduction of $f$ mod $p$, for any prime $p$ dividing $L$.

• Then $f_p$ is a random uniform polynomial over $\mathbb{F}_p$, with $f_p$ being independent for different primes $p|L$ (by Chinese Remainder Theorem).
• Let $f_p$ denote the reduction of $f \mod p$, for any prime $p$ dividing $L$.
• Then $f_p$ is a random uniform polynomial over $\mathbb{F}_p$, with $f_p$ being independent for different primes $p|L$ (by Chinese Remainder Theorem).
• Note that, for any prime $p$, $f_p$ irreducible $\implies f$ irreducible.
Sketch

• Let $f_p$ denote the reduction of $f$ mod $p$, for any prime $p$ dividing $L$.
• Then $f_p$ is a random uniform polynomial over $\mathbb{F}_p$, with $f_p$ being independent for different primes $p|L$ (by Chinese Remainder Theorem).
• Note that, for any prime $p$, $f_p$ irreducible $\implies f$ irreducible.
  • More specifically, if $f_p$ has irreducible factors of degrees $d_1, \ldots, d_r$, then the Galois group of $f$ (over $\mathbb{Q}$) has an element with cycle lengths $d_1, \ldots, d_r$. 

We show that the probability that $f_p$ is reducible is small. Therefore, we hope to show that the probabilities that $f_{p_1}, f_{p_2}, f_{p_3}, f_{p_4}$ are all (compatibly w.r.t. cycle lengths) reducible, for four distinct primes $p_1, \ldots, p_4$ dividing $L$, is very small. We prove this by considering the small and large divisors separately.
Sketch

- Let $f_p$ denote the reduction of $f$ mod $p$, for any prime $p$ dividing $L$.
- Then $f_p$ is a random uniform polynomial over $\mathbb{F}_p$, with $f_p$ being independent for different primes $p|L$ (by Chinese Remainder Theorem).
- Note that, for any prime $p$, $f_p$ irreducible $\implies$ $f$ irreducible.
  - More specifically, if $f_p$ has irreducible factors of degrees $d_1, \ldots, d_r$, then the Galois group of $f$ (over $\mathbb{Q}$) has an element with cycle lengths $d_1, \ldots, d_r$.
- We show that the probability that $f_p$ is reducible is small.
Sketch

• Let $f_p$ denote the reduction of $f$ mod $p$, for any prime $p$ dividing $L$.
• Then $f_p$ is a random uniform polynomial over $\mathbb{F}_p$, with $f_p$ being independent for different primes $p | L$ (by Chinese Remainder Theorem).
• Note that, for any prime $p$, $f_p$ irreducible $\implies f$ irreducible.
  • More specifically, if $f_p$ has irreducible factors of degrees $d_1, \ldots, d_r$, then the Galois group of $f$ (over $\mathbb{Q}$) has an element with cycle lengths $d_1, \ldots, d_r$.
• We show that the probability that $f_p$ is reducible is small.
• Therefore, we hope to show that the probabilities that $f_{p_1}, f_{p_2}, f_{p_3}, f_{p_4}$ are all (compatibly w.r.t. cycle lengths) reducible, for four distinct primes $p_1, \ldots, p_4$ dividing $L$, is very small.
Sketch

• Let $f_p$ denote the reduction of $f$ mod $p$, for any prime $p$ dividing $L$.

• Then $f_p$ is a random uniform polynomial over $\mathbb{F}_p$, with $f_p$ being independent for different primes $p|L$ (by Chinese Remainder Theorem).

• Note that, for any prime $p$, $f_p$ irreducible $\implies f$ irreducible.
  • More specifically, if $f_p$ has irreducible factors of degrees $d_1, \ldots, d_r$, then the Galois group of $f$ (over $\mathbb{Q}$) has an element with cycle lengths $d_1, \ldots, d_r$.

• We show that the probability that $f_p$ is reducible is small.

• Therefore, we hope to show that the probabilities that $f_{p_1}, f_{p_2}, f_{p_3}, f_{p_4}$ are all (compatibly w.r.t. cycle lengths) reducible, for four distinct primes $p_1, \ldots, p_4$ dividing $L$, is very small.

• We prove this by considering the small and large divisors separately.
Proof for 12 primes

Let \( L \) be divisible by 12 distinct primes (e.g. \( L = 7420738134810 \)), and let \( f \) be a random polynomial with i.i.d. uniform random coefficients in \( \{1, \ldots, L\} \).

For 12 distinct primes \( p_1, \ldots, p_{12} \) dividing \( L \), let \( f_{p_i} := f \mod p_i \).

Let \( k < n \). By Meisner [3], the probability that \( f_{p_i} \) has a divisor of degree \( k \) is \( k - \delta + o(1) \) where \( \delta = 1 - \frac{1}{\log \log 2} = 0.086 \ldots \).

By independence, the probability that \( f \) has a divisor of degree \( k \) is

\[
\Pr(\text{f has factor of degree } k) \leq 12 \prod_{i=1}^{12} \Pr(\text{f}_{p_i} \text{ has factor of degree } k) = k - 1 + \delta + o(1) = k - 1.03 + o(1)
\]
Proof for 12 primes

• Let $L$ be divisible by 12 distinct primes (e.g. $L = 7420738134810$), and let $f$ be a random polynomial with i.i.d. uniform random coefficients in $\{1, \ldots, L\}$. 
Proof for 12 primes

• Let $L$ be divisible by 12 distinct primes (e.g. $L = 7420738134810$), and let $f$ be a random polynomial with i.i.d. uniform random coefficients in $\{1, \ldots, L\}$.

• For 12 distinct primes $p_1, \ldots, p_{12}$ dividing $L$, let $f_{p_i} := f \mod p_i$. 
Proof for 12 primes

• Let $L$ be divisible by 12 distinct primes (e.g. $L = 7420738134810$), and let $\mathbf{f}$ be a random polynomial with i.i.d. uniform random coefficients in $\{1, \ldots, L\}$.

• For 12 distinct primes $p_1, \ldots, p_{12}$ dividing $L$, let $\mathbf{f}_{p_i} := \mathbf{f} \mod p_i$.

• Let $k < n$. By Meisner [3], the probability that $\mathbf{f}_{p_i}$ has a divisor of degree $k$ is $k^{-\delta + o(1)}$ where $\delta = 1 - \frac{1+\log \log 2}{\log 2} = 0.086 \ldots$. 
Proof for 12 primes

• Let $L$ be divisible by 12 distinct primes (e.g. $L = 7 420 738 134 810$), and let $f$ be a random polynomial with i.i.d. uniform random coefficients in $\{1, \ldots, L\}$.

• For 12 distinct primes $p_1, \ldots, p_{12}$ dividing $L$, let $f_{p_i} := f \mod p_i$.

• Let $k < n$. By Meisner [3], the probability that $f_{p_i}$ has a divisor of degree $k$ is $k^{-\delta + o(1)}$ where $\delta = 1 - \frac{1 + \log \log 2}{\log 2} = 0.086 \ldots$.

• By independence, the probability that $f$ has a divisor of degree $k$ is

$$\mathbb{P}(f \text{ has factor of degree } k) \leq \prod_{i=1}^{12} \mathbb{P}(f_{p_i} \text{ has factor of degree } k) = k^{-12\delta + o(1)} = k^{-1.03\ldots + o(1)}$$
Proof for 12 primes

- By summing over sufficiently large $k$ (say $k \geq n^{1/10}$), we obtain the bound

\[ \mathbb{P}(\text{f has factor of degree } \geq n^{1/10}) \ll \sum_{k \geq n^{1/10}} k^{-1.03+o(1)} \ll n^{-0.003+o(1)} \]
Proof for 12 primes

• By summing over sufficiently large $k$ (say $k \geq n^{1/10}$), we obtain the bound

$$\mathbb{P}(f \text{ has factor of degree } \geq n^{1/10}) \ll \sum_{k \geq n^{1/10}} k^{-1.03+o(1)} \ll n^{-0.003+o(1)}$$

• Finally, by showing that the small divisors contribute negligibly, this proves that

$$\mathbb{P}(f \text{ reducible}) \to 0 \text{ as } n \to \infty.$$
Small divisors (Lemma 7)

**Lemma (“small divisors are negligible”)**

Let $L \geq 2$ and $f = X^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0$ where as before $a_i$ are i.i.d uniform random variables. Then there exists a $\omega : \mathbb{N} \to \mathbb{N}$ with $\lim_{n \to \infty} \omega(n) = \infty$ such that

$$\mathbb{P}(f \text{ has a divisor of degree } \leq \omega(n)) \to 0 \quad \text{as } n \to \infty$$

Several proofs of this lemma exist:

- $\omega(n) = n/\log n$, Konyagin 1999.
- $\omega(n) = \sqrt{\log n}$, O'Rourke, Wood 2016.
- $\omega(n)$ exists, Kozma, Zeitouni, 2013.
- $\omega(n) = \theta n$, Bary-Soroker, Koukoulopoulos, Kozma, 2020.
Small divisors (Lemma 7)

Lemma ("small divisors are negligible")

Let $L \geq 2$ and $f = X^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0$ where as before $a_i$ are i.i.d uniform random variables. Then there exists a $\omega : \mathbb{N} \to \mathbb{N}$ with $\lim_{n \to \infty} \omega(n) = \infty$ such that

$$\mathbb{P}(f \text{ has a divisor of degree } \leq \omega(n)) \to 0 \quad \text{as } n \to \infty$$

Several proofs of this lemma exist:

- $\omega(n) = n/\log n$, Konyagin 1999.
- $\omega(n) = \sqrt{\log n}$, O’Rourke, Wood 2016.
- $\omega$ exists, Kozma, Zeitouni, 2013.
- $\omega(n) = \theta n$, Bary-Soroker, Koukoulopoulos, Kozma, 2020.
Proof of Lemma 7

Observation 1

Let $L \geq 1$. Then for every $d$, there are only finitely many irreducible polynomials of degree $d$ which can divide a monic polynomial (of arbitrary degree) with coefficients in $\{1, \ldots, L\}$. 
Proof of Lemma 7

Observation 1

Let $L \geq 1$. Then for every $d$, there are only finitely many irreducible polynomials of degree $d$ which can divide a monic polynomial (of arbitrary degree) with coefficients in \{1, \ldots, L\}.

- Let $p(x) := X^d + b_{d-1}X^{d-1} + \cdots + b_1X + b_0 \in \mathbb{Z}[x]$ be such a polynomial which divides some $f$ with coefficients in \{1, \ldots, L\}, and let $z \in \overline{\mathbb{Z}}$ be a root of $p$. 
Proof of Lemma 7

Observation 1
Let $L \geq 1$. Then for every $d$, there are only finitely many irreducible polynomials of degree $d$ which can divide a monic polynomial (of arbitrary degree) with coefficients in $\{1, \ldots, L\}$.

- Let $p(x) := X^d + b_{d-1}X^{d-1} + \cdots + b_1X + b_0 \in \mathbb{Z}[x]$ be such a polynomial which divides some $f$ with coefficients in $\{1, \ldots, L\}$, and let $z \in \overline{\mathbb{Z}}$ be a root of $p$.
- As $z$ divides a polynomial with coefficients in $\{1, \ldots, L\}$, then $|z| \leq L + 1$, otherwise

$$|z|^n > |L + 1|^n > \sum_{i=0}^{n-1} |a_iz^i| \geq |f(z) - z^n|$$
Proof of Lemma 7

Observation 1
Let $L \geq 1$. Then for every $d$, there are only finitely many irreducible polynomials of degree $d$ which can divide a monic polynomial (of arbitrary degree) with coefficients in $\{1, \ldots, L\}$.

- Let $p(x) := X^d + b_{d-1}X^{d-1} + \cdots + b_1X + b_0 \in \mathbb{Z}[x]$ be such a polynomial which divides some $f$ with coefficients in $\{1, \ldots, L\}$, and let $z \in \overline{\mathbb{Z}}$ be a root of $p$.
- As $z$ divides a polynomial with coefficients in $\{1, \ldots, L\}$, then $|z| \leq L + 1$, otherwise

$$|z|^n > |L + 1|^n > \sum_{i=0}^{n-1} |a_i z^i| \geq |f(z) - z^n|$$

- We can similarly derive a contradiction if $|z| < \frac{1}{L+1}$. 
Proof of Lemma 7

- Using the bound $|z_j| \leq L + 1$ for all roots $z_j$ of $p$, we can apply standard relations between the coefficients $b_i$ and the roots $z_i$, we obtain the bound

$$|b_{d-k}| = \left| \sum_{1 \leq i_1 < \cdots < i_k \leq d} \prod_{j=1}^{k} z_{i_j} \right| \leq {d \choose k} (L + 1)^k$$

for each $k = 1, \ldots, d - 1$. 
• Using the bound $|z_j| \leq L + 1$ for all roots $z_j$ of $p$, we can apply standard relations between the coefficients $b_i$ and the roots $z_i$, we obtain the bound

$$|b_{d-k}| = \left| \sum_{1 \leq i_1 < \ldots < i_k \leq d} \prod_{j=1}^{k} z_{i_j} \right| \leq \binom{d}{k} (L + 1)^k$$

for each $k = 1, \ldots, d - 1$.

• Thus, there are only finitely many possibilities for each coefficients $b_i$, and so finitely many possible irreducible polynomials $p(x)$.

(e.g. a rather crude bound is $(2(L + 1))^{d^2}$)
Proof of Lemma 7

Observation 2

Let \( p \) be some fixed irreducible polynomial, and \( f \) as defined in Theorem 1. Then

\[
P(p \text{ divides } f) = O\left(\frac{1}{\sqrt{n}}\right)
\]
Proof of Lemma 7

Observation 2
Let $p$ be some fixed irreducible polynomial, and $f$ as defined in Theorem 1. Then

$$\mathbb{P}(p \text{ divides } f) = O\left(\frac{1}{\sqrt{n}}\right)$$

This essentially follows from the classical Littlewood-Offord bound, a weak form of which states the following:

Littlewood-Offord (1943) (simplified)
Let $n \geq 1$, and let $x_1, \ldots, x_n$ be any non-zero complex numbers. Let $\epsilon_1, \ldots, \epsilon_n$ be i.i.d. uniform random variables in $\{-1, +1\}$. Then the probability that $\epsilon_1 x_1 + \cdots + \epsilon_n x_n = 0$ is $O\left(\frac{1}{\sqrt{n}}\right)$.
Proof of Lemma 7

Observation 2

Let $p$ be some fixed irreducible polynomial, and $f$ as defined in Theorem 1. Then

$$\mathbb{P}(p \text{ divides } f) = O\left(\frac{1}{\sqrt{n}}\right)$$

This essentially follows from the classical Littlewood-Offord bound, a weak form of which states the following:

Littlewood-Offord (1943) (simplified)

Let $n \geq 1$, and let $x_1, \ldots, x_n$ be any non-zero complex numbers. Let $\epsilon_1, \ldots, \epsilon_n$ be i.i.d. uniform random variables in $\{-1, +1\}$. Then the probability that $\epsilon_1 x_1 + \cdots + \epsilon_n x_n = 0$ is $O\left(\frac{1}{\sqrt{n}}\right)$

• More generally, Littlewood-Offord actually obtained a bound for the probability that $\epsilon_1 x_1 + \cdots + \epsilon_n x_n \in I$ for a given bounded set $I$. 

Proof of (weak) Littlewood-Offord

- We may assume wlog that $x_i$ are real and furthermore that $x_i > 0$ for all $i$. 
Proof of (weak) Littlewood-Offord

• We may assume wlog that $x_i$ are real and furthermore that $x_i > 0$ for all $i$.
• Let $\mathcal{A} := \{A \subseteq \{1, \ldots, n\} \mid \sum_{i \in A} x_i - \sum_{j \not\in A} x_j = 0\}$. 
Proof of (weak) Littlewood-Offord

- We may assume wlog that $x_i$ are real and furthermore that $x_i > 0$ for all $i$.
- Let $\mathcal{A} := \{ A \subseteq \{1, \ldots, n\} \mid \sum_{i \in A} x_i - \sum_{j \notin A} x_j = 0 \}$.
- We note that $\mathcal{A}$ is an anti-chain, i.e. for all distinct $A, B \in \mathcal{A}$, $A \not\subseteq B$.
Proof of (weak) Littlewood-Offord

- We may assume wlog that $x_i$ are real and furthermore that $x_i > 0$ for all $i$.
- Let $\mathcal{A} := \{ A \subseteq \{1, \ldots, n\} \mid \sum_{i \in A} x_i - \sum_{j \notin A} x_j = 0\}$.
- We note that $\mathcal{A}$ is an anti-chain, i.e. for all distinct $A, B \in \mathcal{A}$, $A \nsubseteq B$.
- Thus, by Sperner’s lemma, $|\mathcal{A}| \leq \binom{n}{\lfloor n/2 \rfloor}$, which by Stirling, has bound $O\left(\frac{2^n}{\sqrt{n}}\right)$. 

Remark: This is sharp! (at least for arbitrary $x_i \in \mathbb{C}$), as if $x_1 = \cdots = x_n = 1$, then the probability that $\epsilon_1 x_1 + \cdots + \epsilon_n x_n = 0$ is equivalent to the probability that a one-dimensional random walk starting at 0, ends at 0 after $n$ steps. This is $\Theta\left(\frac{n}{\sqrt{n/2}}\right) = \Theta\left(\frac{1}{\sqrt{n}}\right)$. 

Proof of (weak) Littlewood-Offord

- We may assume wlog that $x_i$ are real and furthermore that $x_i > 0$ for all $i$.
- Let $\mathcal{A} := \{ A \subseteq \{1, \ldots, n\} \mid \sum_{i \in A} x_i - \sum_{j \notin A} x_j = 0 \}$.
- We note that $\mathcal{A}$ is an anti-chain, i.e. for all distinct $A, B \in \mathcal{A}$, $A \not\subseteq B$.
- Thus, by Sperner’s lemma, $|\mathcal{A}| \leq \binom{n}{\lfloor n/2 \rfloor}$, which by Stirling, has bound $O\left(\frac{2^n}{\sqrt{n}}\right)$.
- Therefore, the probability that $\epsilon_1 x_1 + \cdots + \epsilon_n x_n = 0$ is $O\left(\frac{1}{\sqrt{n}}\right)$. 

Remark: This is sharp! (at least for arbitrary $x_i \in \mathbb{C}$), as if $x_1 = \cdots = x_n = 1$, then the probability that $\epsilon_1 x_1 + \cdots + \epsilon_n x_n = 0$ is equivalent to the probability that a one-dimensional random walk starting at 0, ends at 0 after $n$ steps. This is $\Theta\left(\frac{n}{n^{1/2}}\right) = \Theta\left(\frac{1}{\sqrt{n}}\right)$.
• We may assume wlog that $x_i$ are real and furthermore that $x_i > 0$ for all $i$.

• Let $\mathcal{A} := \{ A \subseteq \{1, \ldots, n\} \mid \sum_{i \in A} x_i - \sum_{j \notin A} x_j = 0 \}$.

• We note that $\mathcal{A}$ is an anti-chain, i.e. for all distinct $A, B \in \mathcal{A}$, $A \nsubseteq B$.

• Thus, by Sperner’s lemma, $|\mathcal{A}| \leq \binom{n}{\lfloor n/2 \rfloor}$, which by Stirling, has bound $O\left(\frac{2^n}{\sqrt{n}}\right)$.

• Therefore, the probability that $\epsilon_1 x_1 + \cdots + \epsilon_n x_n = 0$ is $O\left(\frac{1}{\sqrt{n}}\right)$.

Remark: This is sharp! (at least for arbitrary $x_i \in \mathbb{C}$), as if $x_1 = \cdots = x_n = 1$, then the probability that $\epsilon_1 x_1 + \cdots + \epsilon_n x_n = 0$ is equivalent to the probability that a one-dimensional random walk starting at 0, ends at 0 after $n$ steps. This is $\Theta\left(\binom{n}{\lfloor n/2 \rfloor}/2^n\right) = \Theta\left(\frac{1}{\sqrt{n}}\right)$. 
Proof of Lemma 7

Back to the original proof:

- Let $p$ be some fixed irreducible polynomial, and let $z \in \mathbb{C}$ be a root of $p$. 

Applying the (generalised) Littlewood-Offord bound with the random variables $a_i$ and $x_i = z_i$. Then we have $P(p \text{ divides } f) = O(1)\sqrt{n}$.

Thus, for any fixed degree $d \geq 1$, we have $P(f \text{ has a divisor of degree } d) \ll (2L + 2)^{d^2} \sqrt{n}^{1/2}$. 

Proof of Lemma 7

Back to the original proof:

• Let $p$ be some fixed irreducible polynomial, and let $z \in \mathbb{C}$ be a root of $p$.

• Applying the (generalised) Littlewood-Offord bound with the random variables $a_i$ and $x_i = z^i$. Then we have

$$
\mathbb{P}(p \text{ divides } f) = \mathbb{P}(z^n + a_{n-1}z^{n-1} + \cdots + a_0 = 0) = O\left(\frac{1}{\sqrt{n}}\right)
$$
Proof of Lemma 7

Back to the original proof:

• Let $p$ be some fixed irreducible polynomial, and let $z \in \mathbb{C}$ be a root of $p$.

• Applying the (generalised) Littlewood-Offord bound with the random variables $\textbf{a}_i$ and $x_i = z^i$. Then we have

$$
\mathbb{P}(p \text{ divides } f) = \mathbb{P}(z^n + a_{n-1}z^{n-1} + \cdots + a_0 = 0) = O\left(\frac{1}{\sqrt{n}}\right)
$$

• Thus, for any fixed degree $d \geq 1$, we have

$$
\mathbb{P}(\text{f has a divisor of degree } d) \ll \frac{(2L + 2)^{d^2}}{\sqrt{n}}
$$
Proof of Lemma 7

• Therefore, for any fixed $W > 0$, we have

$$\mathbb{P}(f \text{ has a divisor of degree } \leq W) \ll \frac{1}{\sqrt{n}} \sum_{d=1}^{W} (2L + 2)^d^2$$

$$\leq \frac{1}{\sqrt{n}} W (2L + 2)^{W^2}$$

which tends to 0 as $n \to \infty$. 
Proof of Lemma 7

• Therefore, for any fixed $W > 0$, we have

$$
P(f \text{ has a divisor of degree } \leq W) \ll \frac{1}{\sqrt{n}} \sum_{d=1}^{W} (2L + 2)^{d^2} \leq \frac{1}{\sqrt{n}} W (2L + 2)^{W^2}$$

which tends to 0 as $n \to \infty$.

• The result also holds if $W$ grows sufficiently slowly (e.g. $\omega(n) = (\log n)^{1/3}$ works).
Large divisors (Lemma 8)

Lemma (Bary-Soroker, Kozma (2017))

Let $\sigma_1, \sigma_2, \sigma_3, \sigma_4$ be 4 independent uniform permutations in $S_n$. For $i \in \{1, \ldots, 4\}$ and $\ell \leq n$ we define $E_{i,\ell}$ as the event that $\ell$ can be written as a sum of lengths of cycles of $\sigma_i$. Then for all $k < n$,

$$
\mathbb{P}
\left(
\bigcup_{\ell=k}^{2k} \bigcap_{i=1}^4 E_{i,\ell}
\right) \leq C k^{-c}
$$

for some effective constant $c, C$ independent of $n$ and $k$.

Furthermore, for an additional parameter $\lambda$,

$$
\mathbb{P}
\left(
\bigcup_{\ell=k}^{2k} \bigcap_{\lambda_1=0}^\lambda \bigcup_{\lambda_4=0}^\lambda \bigcap_{i=1}^4 E_{i,\ell-\lambda_i}
\right) \leq C(\lambda + 1)^4 k^{-c}
$$
Proof of Lemma 8

- Wlog let $k$ be sufficiently large, and let $\lambda < \frac{k}{2}$. Let $0 < \epsilon < \frac{1}{2}$.
Proof of Lemma 8

- Wlog let $k$ be sufficiently large, and let $\lambda < \frac{k}{2}$. Let $0 < \epsilon < \frac{1}{2}$.
- Define $B_{i,k,\epsilon}$ as the event that $\sigma_i$ has at least $(1 + \epsilon) \log k$ cycles whose sizes are less than $k$. 
Proof of Lemma 8

- Wlog let $k$ be sufficiently large, and let $\lambda < \frac{k}{2}$. Let $0 < \epsilon < \frac{1}{2}$.
- Define $B_{i,k,\epsilon}$ as the event that $\sigma_i$ has at least $(1 + \epsilon) \log k$ cycles whose sizes are less than $k$. 
- We shall use the following two facts (maybe proven later?):
  
  (P1) $\mathbb{P}(B_{i,k,\epsilon}) \ll k^{-\epsilon^2/3}$.
  
  (P2) $\mathbb{P}(E_{i,k} \setminus B_{i,k,\epsilon}) \ll k^{\log 2 - 1 + 2\epsilon}$. 
Proof of Lemma 8

• Wlog let $k$ be sufficiently large, and let $\lambda < \frac{k}{2}$. Let $0 < \epsilon < \frac{1}{2}$.
• Define $B_{i,k,\epsilon}$ as the event that $\sigma_i$ has at least $(1 + \epsilon) \log k$ cycles whose sizes are less than $k$.
• We shall use the following two facts (maybe proven later?):
  
  (P1) $\Pr(B_{i,k,\epsilon}) \ll k^{-\epsilon^2/3}$.
  (P2) $\Pr(E_{i,k} \setminus B_{i,k,\epsilon}) \ll k^{\log 2 - 1 + 2\epsilon}$.
• By noting that $B_{i,\ell,\epsilon}$ implies $B_{i,2k,\epsilon/2}$ for sufficiently large $k$ and $\ell \in [k/2, 2k]$, we therefore obtain the bound

\[
\Pr\left( \bigcup_{\ell=k}^{2k} \bigcap_{i=1}^{4} E_{i,\ell} \right) \leq \sum_{i=1}^{2k} \Pr(B_{i,2k,\epsilon/2}) + \sum_{\ell=k}^{2k} \prod_{i=1}^{4} \Pr(E_{i,\ell} \setminus B_{i,\ell,\epsilon})
\]
Proof of Lemma 8

• Applying the bounds (P1) and (P2), this gives us

\[ \mathbb{P}\left( \bigcup_{\ell=k}^{2k} \bigcap_{i=1}^{4} E_{i,\ell} \right) \ll 4k^{-\epsilon^2/12} + k^{1+4(\log 2 - 1 + 2\epsilon)} \]
Proof of Lemma 8

• Applying the bounds (P1) and (P2), this gives us

\[ \mathbb{P}\left( \bigcup_{\ell=k}^{2k} \bigcap_{i=1}^{4} E_{i,\ell} \right) \ll 4k^{-\epsilon^2/12} + k^{1+4(\log 2-1+2\epsilon)} \]

• By letting \( \epsilon \) be small enough (e.g. \( \epsilon = 0.02 \)), we have that \( 1 + 4(\log 2 - 1 + 2\epsilon) < 0 \), and thus the first result holds for

\[ c = \min\left(\frac{\epsilon^2}{12}, -1 - 4(\log 2 - 1 + 2\epsilon)\right) \]
Proof of Lemma 8

The second estimate can be obtained by essentially the same argument:

\[ P := \Pr \left( \bigcup_{\ell=k}^{2k} \bigcup_{\lambda_1=0}^{\lambda} \cdots \bigcup_{\lambda_4=0}^{\lambda} \bigcap_{i=1}^{4} E_{i,\ell-\lambda_i} \right) \leq \]

\[ \leq \sum_{i=1}^{4} \Pr(B_{i,2k,\epsilon/2}) + \sum_{\ell=k}^{2k} \sum_{\lambda_1=0}^{\lambda} \cdots \sum_{\lambda_4=0}^{\lambda} \prod_{i=1}^{4} \Pr(E_{i,\ell-\lambda_i} \setminus B_{i,\ell-\lambda_i,\epsilon}) \]

\[ \ll 4k^{-\epsilon^2/12} + (\lambda + 1)^4 \sum_{\ell=k/2}^{2k} k^4(\log 2 - 1 + 2\epsilon) \]

\[ \ll (\lambda + 1)^4 k^{-c} \]

where as before \( c = \min(\epsilon^2/12, -1 - 4(\log 2 - 1 + 2\epsilon)) \).
Proof of main theorem

Theorem (Bary-Soroker, Kozma (2017))

Let $L$ be a positive integer divisible by at least 4 distinct primes. Let
\[ f = X^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0 \]
where $a_0, \ldots, a_{n-1}$ are i.i.d random variables taking values uniformly in \{1, \ldots, L\}. Then $\mathbb{P}(f \text{ is irreducible}) \to 1$, as $n \to \infty$. 
Proof of main theorem

Theorem (Bary-Soroker, Kozma (2017))

Let $L$ be a positive integer divisible by at least 4 distinct primes. Let

$$f = X^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0$$

where $a_0, \ldots, a_{n-1}$ are i.i.d random variables taking values uniformly in $\{1, \ldots, L\}$. Then $\mathbb{P}(f \text{ is irreducible}) \to 1$, as $n \to \infty$.

- Fix some $k$ sufficiently large. We shall consider divisors of degree $k < \ell < 2k$. 

Proof of main theorem

**Theorem (Bary-Soroker, Kozma (2017))**

Let $L$ be a positive integer divisible by at least 4 distinct primes. Let

$$f = X^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0$$

where $a_0, \ldots, a_{n-1}$ are i.i.d random variables taking values uniformly in $\{1, \ldots, L\}$. Then $P(f$ is irreducible$) \to 1$ as $n \to \infty$.

- Fix some $k$ sufficiently large. We shall consider divisors of degree $k < \ell < 2k$.
- Let $p_1, \ldots, p_4$ be 4 distinct primes dividing $L$, and define $f_{p_i}$ as the reduction of $f$ mod $p_i$. 
Proof of main theorem

Theorem (Bary-Soroker, Kozma (2017))

Let $L$ be a positive integer divisible by at least 4 distinct primes. Let $f = X^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0$ where $a_0, \ldots, a_{n-1}$ are i.i.d random variables taking values uniformly in $\{1, \ldots, L\}$. Then $\mathbb{P}(f \text{ is irreducible}) \to 1$ as $n \to \infty$.

• Fix some $k$ sufficiently large. We shall consider divisors of degree $k < \ell < 2k$.
• Let $p_1, \ldots, p_4$ be 4 distinct primes dividing $L$, and define $f_{p_i}$ as the reduction of $f \mod p_i$.
• For $r = 1, \ldots, 4$, define $X_r$ as the random tuple which takes the value $(m_{1,r}, m_{2,r}, \ldots)$ where $m_{i,r}$ is the number of irreducible factors of $f_{p_r}$ of degree $i$. 
Proof of main theorem

**Theorem (Bary-Soroker, Kozma (2017))**

Let $L$ be a positive integer divisible by at least 4 distinct primes. Let

$$f = X^n + a_{n-1}X^{n-1} + \cdots + a_1 X + a_0$$

where $a_0, \ldots, a_{n-1}$ are i.i.d random variables taking values uniformly in \{1, \ldots, L\}. Then $\mathbb{P}(f \text{ is irreducible}) \to 1$ as $n \to \infty$.

- Fix some $k$ sufficiently large. We shall consider divisors of degree $k < \ell < 2k$.
- Let $p_1, \ldots, p_4$ be 4 distinct primes dividing $L$, and define $f_{p_i}$ as the reduction of $f$ mod $p_i$.
- For $r = 1, \ldots, 4$, define $X_r$ as the random tuple which takes the value $(m_{1,r}, m_{2,r}, \ldots)$ where $m_{i,r}$ is the number of irreducible factors of $f_{p_r}$ of degree $i$.
- Analogously, let $\sigma$ be a random permutation in $S_n$, and define $Y$ as the random tuple $(n_1, n_2, \ldots)$ where $n_i$ is the number of cycles of $\sigma$ of length $i$. 
Proof of main theorem

- Now first, we let $B_k$ be the event that for some $r = 1, \ldots, 4$ and some $i < \log^2 k$ we have $m_{i,r} < \log^2 k$
Proof of main theorem

• Now first, we let $B_k$ be the event that for some $r = 1, \ldots, 4$ and some $i < \log^2 k$ we have $m_{i,r} < \log^2 k$

• We have the bound $\mathbb{P}(B_k) \ll 4 \log^2 k e^{-c \log^2 k}$ (next week), thus $B_k$ occurs negligibly.
Proof of main theorem

• Now first, we let $B_k$ be the event that for some $r = 1, \ldots, 4$ and some $i < \log^2 k$ we have $m_{i,r} < \log^2 k$

• We have the bound $\mathbb{P}(B_k) \ll 4 \log^2 k e^{-c \log^2 k}$ (next week), thus $B_k$ occurs negligibly.

• Let $R_k$ be the event that for some $k \leq \ell < 2k$ and some $\lambda_r < \log^6 k$ we can write

$$\ell - \lambda_r = \sum_{i > \log^2 k} i \ell_{i,r}, \quad \ell_{i,r} \leq m_{i,r}$$

for all $r = 1, \ldots, 4$. 
Proof of main theorem

• Now first, we let $B_k$ be the event that for some $r = 1, \ldots, 4$ and some $i < \log^2 k$ we have $m_{i,r} < \log^2 k$

• We have the bound $\mathbb{P}(B_k) \ll 4 \log^2 k \cdot e^{-c \log^2 k}$ (next week), thus $B_k$ occurs negligibly.

• Let $R_k$ be the event that for some $k \leq \ell < 2^k$ and some $\lambda_r < \log^6 k$ we can write

$$\ell - \lambda_r = \sum_{i > \log^2 k} i \ell_{i,r}, \quad \ell_{i,r} \leq m_{i,r}$$

for all $r = 1, \ldots, 4$.

• Similarly, let $S_k$ be the event that for some $k \leq \ell < 2^k$ and some $\lambda < \log^6 k$ we can write

$$\ell - \lambda = \sum_{i > \log^2 k} i \ell_i, \quad \ell_i \leq n_i.$$
Proof of main theorem

• We now use that $X_r$ and $Y$ have sufficiently similar distributions (next week) which implies $|P(R_k) - P(S_k)| \ll 1/\log^2 k$. 
Proof of main theorem

- We now use that $X_r$ and $Y$ have sufficiently similar distributions (next week) which implies $|\mathbb{P}(R_k) - \mathbb{P}(S_k)| \ll 1/\log^2 k$.
- By Lemma 8, we have $\mathbb{P}(S_k) \ll k^{-c} \log^{24} k$.  

Proof of main theorem

• We now use that $X_r$ and $Y$ have sufficiently similar distributions (next week) which implies $|P(R_k) - P(S_k)| \ll 1/\log^2 k$.

• By Lemma 8, we have $P(S_k) \ll k^{-c} \log^{24} k$.

• This implies $P(R_k) \ll 1/\log^2 k$. 

Proof of main theorem

- We now use that $X_r$ and $Y$ have sufficiently similar distributions (next week) which implies $|\mathbb{P}(R_k) - \mathbb{P}(S_k)| \ll 1/\log^2 k$.
- By Lemma 8, we have $\mathbb{P}(S_k) \ll k^{-c} \log^{24} k$.
- This implies $\mathbb{P}(R_k) \ll 1/\log^2 k$.
- Now, let $Q_k$ be the event that for some $k \leq \ell < 2k$ we can write $\ell = \sum i\ell_{i,r}$ for some $\ell_{i,r} \leq m_{i,r}$, for all $r = 1, \ldots, 4$. 
Proof of main theorem

• We now use that $X_r$ and $Y$ have sufficiently similar distributions (next week) which implies $|\mathbb{P}(R_k) - \mathbb{P}(S_k)| \ll 1/\log^2 k$.

• By Lemma 8, we have $\mathbb{P}(S_k) \ll k^{-c} \log^{24} k$.

• This implies $\mathbb{P}(R_k) \ll 1/\log^2 k$.

• Now, let $Q_k$ be the event that for some $k \leq \ell < 2k$ we can write $\ell = \sum i \ell_{i,r}$ for some $\ell_{i,r} \leq m_{i,r}$, for all $r = 1, \ldots, 4$.

• As $Q_k \setminus B_k$ is contained in the event $R_k$, this implies $\mathbb{P}(Q_k \setminus B_k) \ll 1/\log^2 k$. 
Proof of main theorem

• We now use that $X_r$ and $Y$ have sufficiently similar distributions (next week) which implies $|\mathbb{P}(R_k) - \mathbb{P}(S_k)| \ll 1 / \log^2 k$.

• By Lemma 8, we have $\mathbb{P}(S_k) \ll k^{-c} \log^{24} k$.

• This implies $\mathbb{P}(R_k) \ll 1 / \log^2 k$.

• Now, let $Q_k$ be the event that for some $k \leq \ell < 2k$ we can write $\ell = \sum i \ell_i, r$ for some $\ell_i, r \leq m_i, r$, for all $r = 1, \ldots, 4$.

• As $Q_k \setminus B_k$ is contained in the event $R_k$, this implies $\mathbb{P}(Q_k \setminus B_k) \ll 1 / \log^2 k$.

• Finally, as $B_k$ is negligible, we have $\mathbb{P}(Q_k) \ll 1 / \log^2 k$. 
Proof of main theorem

- We now use that $X_r$ and $Y$ have sufficiently similar distributions (next week) which implies $|\mathbb{P}(R_k) - \mathbb{P}(S_k)| \ll 1/\log^2 k$.
- By Lemma 8, we have $\mathbb{P}(S_k) \ll k^{-c} \log^{24} k$.
- This implies $\mathbb{P}(R_k) \ll 1/\log^2 k$.
- Now, let $Q_k$ be the event that for some $k \leq \ell < 2k$ we can write $\ell = \sum i \ell_{i,r}$ for some $\ell_{i,r} \leq m_{i,r}$, for all $r = 1, \ldots, 4$.
- As $Q_k \setminus B_k$ is contained in the event $R_k$, this implies $\mathbb{P}(Q_k \setminus B_k) \ll 1/\log^2 k$.
- Finally, as $B_k$ is negligible, we have $\mathbb{P}(Q_k) \ll 1/\log^2 k$.

Therefore, $\mathbb{P}(f \text{ has divisor of degree } \in [k, 2k)) \ll \frac{1}{\log^2 k}$
Proof of main theorem

Finally, summing over all possible divisors, this proves

\[
\mathbb{P}(f \text{ reducible}) \leq \mathbb{P}(f \text{ has divisors of degree } \leq \omega(n)) + \sum_{\substack{k=\omega(n) \cdot 2^i \\
i=0,\ldots,\log_2 n}} \mathbb{P}(f \text{ has divisors of degree } \in [k, 2k])
\]

\[
\ll (\text{something small}) + \sum_{\substack{k=\omega(n) \cdot 2^i \\
i=0,\ldots,\log_2 n}} \frac{1}{\log^2 k}
\]

\[
\ll \frac{1}{\log \omega(n)} - \frac{1}{\log \omega(n) + \log n}
\]

\[
\to 0 \quad \text{as } n \to \infty.
\]
Proof of main theorem

Finally, summing over all possible divisors, this proves

\[
\mathbb{P}(f \text{ reducible}) \leq \mathbb{P}(f \text{ has divisors of degree } \leq \omega(n)) \\
+ \sum_{\substack{k=\omega(n) \cdot 2^i \atop i=0,\ldots,\log_2 n}} \mathbb{P}(f \text{ has divisors of degree } \in [k, 2k])
\]

\[
\ll (\text{something small}) + \sum_{\substack{k=\omega(n) \cdot 2^i \atop i=0,\ldots,\log_2 n}} \frac{1}{\log^2 k}
\]

\[
\ll \frac{1}{\log \omega(n)} - \frac{1}{\log \omega(n) + \log n}
\]

\[
\to 0 \quad \text{as } n \to \infty.
\]

E.g. Using Konyagin’s bound for \(\omega(n)\), we have \(\mathbb{P}(f \text{ reducible}) \ll \frac{1}{\log n} \). \qed
Recent developments

Theorem (Bary-Soroker, Koukoulopoulos, Kozma (2020))

Let \( L \geq 35, \) and let \( f = X^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0 \) where \( a_0, \ldots, a_{n-1} \) are i.i.d random variables taking values uniformly in \( \{1, \ldots, L\} \). Then \( \mathbb{P}(f \text{ is irreducible}) \to 1, \) as \( n \to \infty. \)
Recent developments

Theorem (Bary-Soroker, Koukoulopoulos, Kozma (2020))

Let $L \geq 35$, and let $f = X^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0$ where $a_0, \ldots, a_{n-1}$ are i.i.d random variables taking values uniformly in $\{1, \ldots, L\}$. Then $\mathbb{P}(f \text{ is irreducible}) \to 1$, as $n \to \infty$.

- This was proven using a combination of a standard argument for $L \geq 33730$ and a computer-assisted proof for $35 \leq L < 33730$. 
Recent developments

Theorem (Bary-Soroker, Koukoulopoulos, Kozma (2020))

Let $L \geq 35$, and let $f = X^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0$ where $a_0, \ldots, a_{n-1}$ are i.i.d random variables taking values uniformly in $\{1, \ldots, L\}$. Then $\mathbb{P}(f \text{ is irreducible}) \rightarrow 1$, as $n \rightarrow \infty$.

- This was proven using a combination of a standard argument for $L \geq 33,730$ and a computer-assisted proof for $35 \leq L < 33,730$.
- Here, $f_p$ does not have uniformly distributed coefficients mod $p$ nor independence necessarily, and so Bary-Soroker–Koukoulopoulos–Kozma use $p$-adic Fourier Analysis and the large sieve to prove approximate equidistribution modulo 4 primes.
## Recent developments

**Theorem (Bary-Soroker, Koukoulopoulos, Kozma (2020))**

Let $L \geq 35$, and let $f = X^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0$ where $a_0, \ldots, a_{n-1}$ are i.i.d random variables taking values uniformly in $\{1, \ldots, L\}$. Then $\mathbb{P}(f \text{ is irreducible}) \to 1$, as $n \to \infty$.

- This was proven using a combination of a standard argument for $L \geq 33,730$ and a computer-assisted proof for $35 \leq L < 33,730$.

- Here, $f_p$ does not have uniformly distributed coefficients mod $p$ nor independence necessarily, and so Bary-Soroker–Koukoulopoulos–Kozma use $p$-adic Fourier Analysis and the large sieve to prove approximate equidistribution modulo 4 primes.

- Their proofs also work for general measures (under some assumptions), even for non-identically distributed coefficients.
Proof of P1

Let $S_n(k, \ell)$ be the set of $\pi \in S_n$ containing exactly $\ell$ cycles of length at most $k$. We can write

$$n|S_n(k, \ell)| = \sum_{\pi \in S_n(k, \ell)} \sum_{\sigma | \pi, \sigma \text{ a cycle}} |\sigma|$$

By substituting $\pi = \sigma \pi'$ and noting that $\pi'$ has either $\ell - 1$ or $\ell$ cycles of length at most $k$, we get

$$n|S_n(k, \ell)| \leq \sum_{j=1}^{n} \sum_{m=\ell - 1}^{\ell} \sum_{\pi' \in S_{n-j}(k,m)} \sum_{\sigma | S_n, |\sigma|=j} \sum_{\sigma \text{ a cycle}} \frac{n!}{(n-j)!}$$

Now we rearrange this sum according to the cycle type $(c_1, \ldots, c_n)$ of the permutation $\pi'$ and apply the Cauchy formula:
Proof of P1

\[ n |S_n(k, \ell)| \leq n! \sum_{j=1}^{n} \sum_{c_1, \ldots, c_n \geq 0, c_1+2c_2+\cdots+nc_n=n-j, c_1+\cdots+c_k \in \{\ell-1, \ell\}}^{} \frac{1}{\prod_i c_i!i^{c_i}} \]

\[ \leq n! \sum_{c_1, \ldots, c_n \geq 0, c_1+\cdots+c_k \in \{\ell-1, \ell\}}^{} \frac{1}{\prod_i c_i!i^{c_i}} \]

\[ = n! (\frac{h_{k}^{\ell}-1}{(\ell-1)!} + \frac{h_{k}^{\ell}}{\ell!}) \prod_{k<i \leq n} e^{1/i} \]

where the last inequality follows by the multinomial theorem, and where 
\[ h_n = 1 + \frac{1}{2} + \cdots + \frac{1}{n} \] are the harmonic numbers.
Proof of P1

By applying the bound $h_k \leq 1 + \log k$, this proves that

$$\frac{|S_n(k, \ell)|}{n!} \leq \frac{e}{k} \frac{(1 + \log k)^\ell}{\ell!} (1 + \frac{\ell}{1 + \log k})$$

which we note is $O\left(\frac{(1+\log k)^{\ell-1}}{k(\ell-1)!}\right)$ if $\ell \gg \log k$.

Finally, by summing over all $\ell > (1 + \epsilon) \log k$, we obtain

$$\mathbb{P}(B_{i,k,\epsilon}) \leq \sum_{\ell > (1 + \epsilon) \log k} \frac{|S_n(k, \ell)|}{n!} \ll \sum_{\ell > (1 + \epsilon) \log k} \frac{(1 + \log k)^{\ell-1}}{k(\ell-1)!} \ll \frac{(1 + \log k)^{(1 + \epsilon) \log k - 1}}{k((1 + \epsilon) \log k - 1)!} \ll \frac{1}{k} \left(\frac{e}{1 + e}\right)^{(1 + \epsilon) \log k}$$

Finally, by computing a Taylor expansion of $-1 + (1 + \epsilon) \log \left(\frac{e}{(1 + \epsilon)}\right)$, we obtain the above is bounded by $O(k^{-\epsilon^2/3})$ if $\epsilon \leq 1/2$, which completes the proof of P1. \qed
Proof of P2

Fix some $\ell \leq (1 + \epsilon) \log k$ and consider $\pi \in S_n(k, \ell)$.

If $\pi$ fixes some set $X$ with $|X| = k$, then we denote $\pi_1 = \pi|_X$ and $\pi_2 = \pi|_{[n]\setminus X}$ for the induced permutations on $X$ and its complement.

Then $\pi$ has $\ell_1$ cycles of length $\leq k$, and $\pi_2$ has $\ell_2$ cycles of length $\leq k$, where $\ell_1 + \ell_2 = \ell$.

Thus, by P1, the number of such $\pi \in S_n(k, \ell)$ for a given choice of $X$ and $\ell_1, \ell_2$ is

$$\ll \frac{(1 + \log k)^{\ell_1}}{k \ell_1!} \cdot \frac{(1 + \log k)^{\ell_2}}{k \ell_2!} (n - k)!$$

Therefore, the probability that $\pi \in S_n$ has exactly $\ell$ cycles of length at most $k$ is

$$\ll \sum_{\ell_1 + \ell_2 = \ell} \frac{1}{k^2} \frac{(1 + \log k)^{\ell}}{\ell_1! \ell_2!} = \frac{2^\ell (1 + \log k)^{\ell}}{k^2 \ell!}$$
Proof of P2

Therefore, by summing over all $\ell \leq (1 + \epsilon) \log k$, we obtain

$$
\mathbb{P}(E_{i,k} \setminus B_{i,k,\epsilon}) \ll \frac{1}{k^2} \sum_{\ell \leq (1 + \epsilon) \log k} \frac{2^\ell (1 + \log k)^\ell}{\ell!} \\
\ll \frac{1}{k^2} \frac{2^{(1+\epsilon) \log k} (1 + \log k)^{(1+\epsilon) \log k}}{((1 + \epsilon) \log k)!} \\
\ll \frac{1}{k^{1 - \log 2 - 2\epsilon}}
$$

which proves P2.
Irreducibility of random polynomials: general measures

Irreducible polynomials of bounded height

Eberhard, S., Ford, K., Green, B. (2017)
Invariable generation of the symmetric group

Konyagin, S.V. (1999)
On the number of irreducible polynomials with 0,1 coefficients
On Common Roots of Random Bernoulli Polynomials,  

Littlewood, J.E., Offord, A.C. (1943)  
On the number of real roots of a random algebraic equation (III)  

Meisner, P. (2018)  
Erdös’ Multiplication Table Problem for Function Fields and Symmetric Groups.  
Questions?