Sankhyā : The Indian Journal of Statistics.
1976, Volume **38**, Series B, Pt. 2, pp. 144–152.

THE NUMBER OF REAL ROOTS OF RANDOM POLYNOMIALS OF SMALL DEGREE*

By WILLIAM B. FAIRLEY
Kennedy School of Government, Harvard University

SUMMARY. Random polynomials with random coefficients have been studied by a number of authors, including Kac (1943, 1949), who showed that the average number of real roots of polynomials of degree n is asymptotically $(2/\pi)\log n$. The present paper investigates the average number of real roots for polynomials of small degree and coefficients that are 1 or -1 with equal probability. Log-like behavior of the average for small n is shown by finding exact distributions of the numbers of real roots for n between 1 and 10 and by sampling the large but finite populations for n between 10 and 50.

1. Introduction

A random polynomial is a polynomial whose coefficients are given according to some probability distribution. Denote a polynomial by $p(x)$, and let the coefficients be denoted a_i, so that for an n-th degree polynomial :

$$p(x) = a_0+a_1x+a_2x^2+\ldots+a_nx^n. \qquad \ldots \quad (1)$$

The distribution of the number N of real roots of random polynomials has been studied by several authors, and in particular the mean number of real roots, $E_n(N)$, has been studied for several different distributions of the coefficients a_i. An early reference is Bloch and Polya (1932) who showed that $E_n(N) = 0(\sqrt{n})$ when $P[a_i = -1] = P[a_i = 0] = P(a_i = 1] = 1/3$. Littlewood and Offord (1939) gave the upper bound $E_n(N) < 25\,(\log n)^2+12\log n$ for three distributions : (i) $P[a_i = -1] = P[a_i = 1] = 1/2$, (ii) a_i uniform on $[-1, 1]$; and a_i normally distributed. The a_i are independent in each case. Then Kac (1943, 1949) showed that for uniform and normally distributed coefficients the asymptotic value for $E_n(N)$ as the degree n of the polynomial increases to infinity is given by the simple expression

$$E_n(N) \sim (2/\pi)\log n. \qquad \ldots \quad (2)$$

There are remarkably few real roots of random polynomials. Erdos and Offord (1956) showed that this asymptotic formula holds for the case $P[a_i = 1] = P[a_i = -1] = 1/2$. Stevens (1965) and Ibragimov and Maslova (1971) have extended this result to wider classes of distributions within the domain of attraction of the normal.

*This research was facilitated by a grant from the National Science Foundation, GS-2044X, to Harvard University.

2. Finite populations of polynomials

This paper reports on an investigation of the values of $E_n(N)$ for polynomials of small degree and for coefficients that are 1 or -1 with equal probabilities and mutually independent. We call these ± 1 polynomials. As mentioned above, the asymptotic result (2) holds for ± 1 polynomials, and they are particularly amenable to study for small values of n.

The population of all ± 1 polynomials of given degree n is finite, there being 2^{n+1} polynomials corresponding to the 2^{n+1} choices of the sequences of $n+1$ coefficients 1 or -1. For very small values of n the entire exact distributions of the number of real roots N may be obtained, and $E_n(N)$ along with these, simply by calculating the real roots of all the 2^{n+1} polynomials. The calculations are reduced by certain symmetries in the relations between coefficients and roots, spelled out in Section 5 below and simplified by the fact that all of the real roots of these polynomials lie within the real intervals $[-2, -1/2]\ U\ [1/2, 2]$.

Of course as n increases there comes a point where calculating the roots of all 2^{n+1} polynomials becomes too costly. To obtain the exact distribution for $n = 15$ would require calculating the roots of $2^{13} = 8192$ polynomials of degree 15 and for $n = 20$, $2^{18} = 260, 544$ polynomials of degree 20. The present study uses a stratified sample survey design to sample the populations of polynomials for n larger than 10 in order to study $E_n(N)$ as n increases.

3. Exact distributions

For $n = 1, 2, \dots, 10$, figure 1 plots the exact frequency distributions of the numbers of real roots for ± 1 polynomials and degrees $n = 1, 2, \dots, 10$. Table 1 gives the computed values.

TABLE 1. EXACT DISTRIBUTIONS OF NUMBERS OF REAL ROOTS FOR DEGREES $n = 1, 2, \dots, 10$

odd degree				even degree			
degree n	number of real roots	count	frequency	degree n	number of real roots	count	frequency
1	1	4	1.000	2	0	4	.500
					2	4	.500
3	1	12	.750	4	0	12	.375
	3	4	.250		2	20	.625
5	1	44	.688	6	0	32	.250
	3	20	.312		2	96	.750
7	1	164	.641	8	0	116	.227
	3	92	.359		2	380	.742
					4	16	.031
9	1	596	.582	10	0	408	.199
	3	424	.414		2	1512	.738
	5	4	.004		4	128	.063

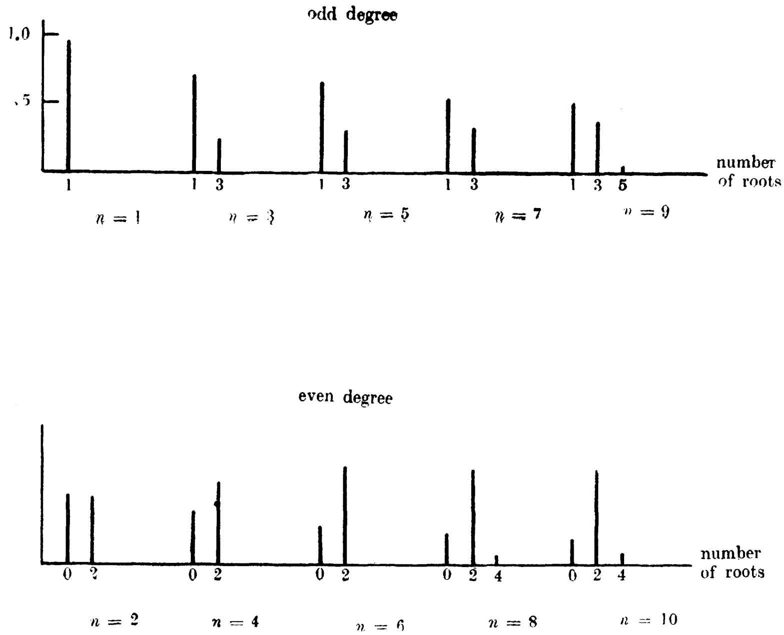

Fig. 1. **Exact Distributions of Numbers of Real Roots For Degrees $n = 1, 2, \ldots, 10$.**

Solutions for the roots were obtained using an algorithm that employs steepest descent to locate approximate roots and then Newton's method to find closer approximations. The method and computer program are described by F. Lilley (1967). The means of the exact distributions of the numbers of real roots are plotted in Figure 2. Treating the cases n even and n odd separately, the plot indicates smooth increases in the means with n.

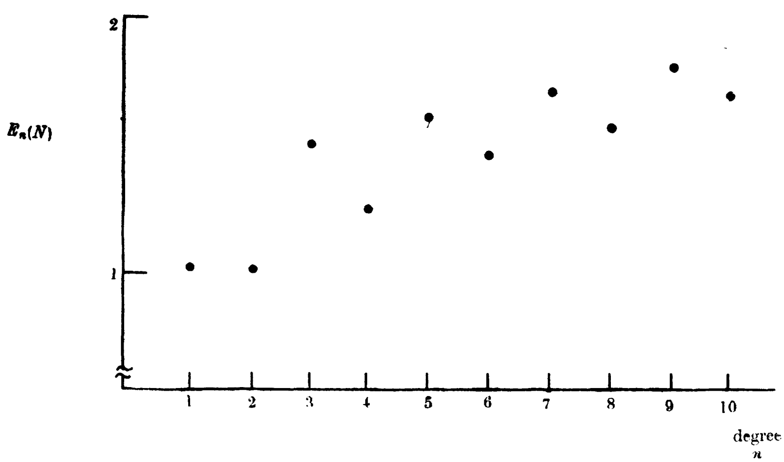

Fig. 2. **Means of Exact Distributions of Numbers of Real Roots.**

4. Sampling experiment for larger n

For values of n larger than 10 a sampling experiment takes advantage of this smoothness by taking only a grid of values of n for n odd and n even. To estimate $E_n(N)$ the population of polynomials for each degree n was sampled. A stratified random sample using proportional allocation was chosen to estimate $E_n(N)$ efficiently. A stratifying variable is suggested by Descartes' rule of signs, which states that an upper bound for the number of positive real roots of a polynomial is the number of changes of sign in the sequence of coefficients. When the coefficients are 1 or -1, $|p(1)|$ is equal to the absolute value of the difference between the number of $+1$'s and the number of -1's which in turn is associated with the number of sign changes and therefore it is conjectured, with the number of positive real roots. The conjecture is verified for degrees $n = 1, 2, \ldots, 10$ by computing N and $|p(1)|$. Since a positive root of $p(x)$ is a negative root of $p(-x)$, $|p(-1)|$ is negatively associated with the number of negative real roots. Now $|p(1)|$ and $|p(-1)|$ are independent for n odd, and for n even they are less and less correlated as n increases, so that the sum $K = |p(1)| + |p(-1)|$ is a random variable that is negatively associated with the number of real roots positive or negative. Therefore K is suggested as a simply computed stratifying variable for sampling ± 1 polynomials.

A sample of $m = 100$ polynomials was taken from the strata defined by values of K for each of 10 populations of polynomials, namely for every eighth value of n between $n = 15$ and $n = 47$, that is, $n = 15, 23, 31, 39, 47$, and between $n = 16$ and $n = 48$, that is, $n = 16, 24, 32, 40, 48$. For polynomials of higher degrees than these the costs and the numerical difficulties of computing roots mount sharply.

Using the results presented in Section 5 on the partitioning of the populations into groups of 4 and of 8 polynomials having the same numbers of roots, it was only necessary to sample a quarter of the 2^{n+1} polynomials of each degree. (For this reason too, the values of K appearing in Table 2 below refer only to sums of the last n—1 coefficients of $p(x)$. See Section 5.)

Table 2 gives the observed mean numbers, $\bar{y}_{nK}$, of real roots for the different strata. The negative association between the values of $\bar{y}_{nK}$ and of K for a given n is apparent. The values of $E_n(N)$ were estimated from the stratum means by the weighted means, $\bar{y}_n$:

$$\bar{y}_n = \sum_K M_K \bar{y}_{nK} / M$$

where M is the population size ($M = (2^{n+1}/4) = 2^{n-1}$).

TABLE 2. STRATUM MEANS, $\bar{y}_{nK}$

	degree n				
K	15	23	31	39	47
2	2.47	2.00	2.47	3.33	3.40
6	1.81	2.20	2.45	2.64	3.40
> 6	1.61				
10		2.43	2.10	3.00	3.00
>10		2.00	2.13		
14				2.55	2.50
>14				2.43	
18					2.20
>18					1.25

	degree n				
K	16	24	32	40	48
2	2.13	2.00	3.00	2.75	2.40
4	2.00	2.44	3.00	2.44	2.57
6	2.17	2.50	2.67	3.29	2.33
8	1.79	2.00	2.35	2.88	2.89
10	2.20	2.00	2.71	2.43	2.50
>10	1.50				
12		2.00	1.67	1.00	2.57
>12		1.20			
14			2.22	2.89	2.20
>14			1.45		
16				2.50	1.50
>16				2.20	2.00

The values of the weighted means, $\bar{y}_n$, and their estimated variances, s_n^2, are given in Table 3. The sample variances in each stratum, s_{nK}^2, were used to compute the variances s_n^2 according to the formula :

$$s_n^2 = \frac{1}{M} \sum_K M_K(M_K - m_K) \frac{s_{nK}}{m_K}.$$

TABLE 3. ESTIMATES OF MEANS AND VARIANCES FROM STRATIFIED SAMPLES

	odd degree			even degree	
degree n	mean $\bar{y}_n$	variance s_n^2	degree n	mean $\bar{y}_n$	vaiance s_n^2
15	1.96	.88	16	2.00	1.36
23	2.22	1.43	24	2.10	1.15
31	2.28	1.32	32	2.40	1.44
39	2.78	1.99	40	2.50	1.39
47	2.86	1.86	48	2.40	1.71

The estimated values, $\bar{y}_n$, are plotted in Figure 3 for n even, $n = 16, 24, 32, 40, 48$. The exact values of $E_n(N)$ for the smaller even degree polynomials, $n = 2, 4, 6, 8, 10$ are also plotted. The asymptotic values $(2/\pi) \log n$ of $E_n(N)$ is also given in Figure 3. The exact and estimated values of $E_n(N)$ reveal a log-like behavior as n increases even for small values of n. For n odd the behavior is similar.

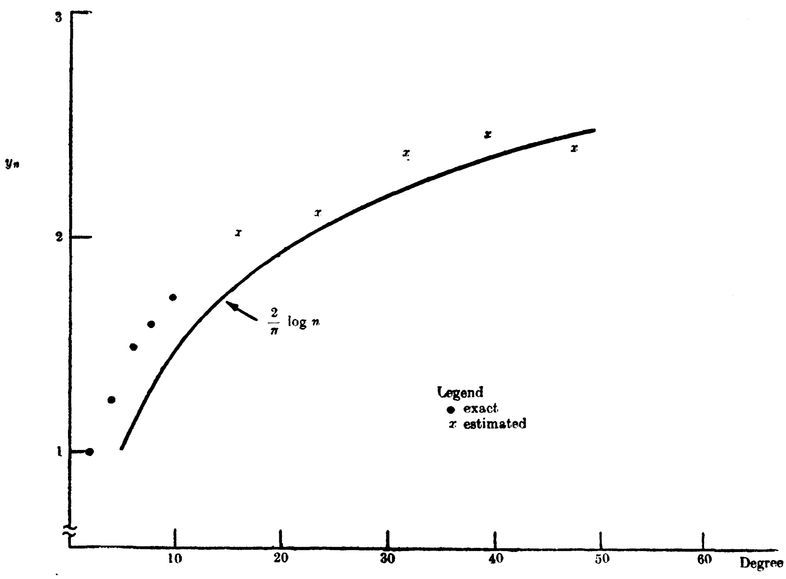

Fig. 3. Mean Numbers of Roots Exact and Estimated n even

5. Partitioning the populations of polynomials

If $p(x)$ has N roots then $-p(x)$ and $p(-x)$ have N roots. If x is a root of $p(x)$ then $1/x$ is a root of the polynomial $\overline{p(x)}$ whose coefficients are those of $p(x)$ in reverse order, so that $\overline{p(x)}$ also has N roots. Various combinations of these three transformations of a given polynomial $p(x)$ lead to still other polynomials having N roots : $-p(-x)$, $\overline{-p(x)}$, $\overline{p(-x)}$, and $\overline{-p(-x)}$. In our application the polynomials have coefficients of 1's and -1's.

Further products of these transformations do not lead to other polynomials in the population. In fact the situation may be conveniently described in algebraic terms as a group of transformations acting on the set S of all sequences of 1's and -1's of length $n+1$. The group T is a set of eight transformations or mappings, $t_0, t_1, \ldots, t_7$, defined on the set S, $t_i : S \to S$, where the group operation is composition of mappings, and, using the polynomial notation $p(x)$ to denote a sequence of $n+1$ 1's and -1's, the t_i are defined by

		n even	*n odd*
$t_0p(x)$	$= p(x)$	identity	same
$t_1p(x)$	$= -p(x)$	changes sign of all coefficients	same
$t_2p(x)$	$= p(-x)$	changes sign of all odd coefficients	same
$t_3p(x)$	$= \overline{p(x)}$	reverses order of coefficients	same
$t_4p(x)$	$= -p(-x)$	changes of sign of even coefficients	same
$t_5p(x)$	$= \overline{-p(x)}$	reverses order and changes all signs	same
$t_6p(x)$	$= \overline{p(-x)}$	reverses order and changes (odd) signs	same (even)
$t_7p(x)$	$= \overline{-p(-x)}$	reverses order and changes (even) signs	same (odd)

Each element of this 8-element group is idempotent, i.e., $t_it_i = t_0$, the identity, for all i, so that each element is its own inverse. The complete multiplication table for the group is; for n even :

	t_0	t_1	t_2	t_3	t_4	t_5	t_6	t_7
t_0	t_0	t_1	t_2	t_3	t_4	t_5	t_6	t_7
t_1		t_0	t_4	t_5	t_2	t_3	t_7	t_6
t_2			t_0	t_6	t_1	t_7	t_3	t_5
t_3				t_0	t_7	t_1	t_2	t_4
t_4					t_0	t_6	t_5	t_3
t_5	symmetric					t_0	t_4	t_2
t_6	by						t_0	t_1
t_7	commutativity							t_0

A population of 2^{n+1} polynomials, the set S, is divided by the action of this group into subsets or orbits such that if $p(x) \in S$ is in an orbit, then $t_ip(x) = q(x)$ is also in the orbit for all $t_i \in T$. All polynomials within a common orbit under T have the same number of real roots.

For n odd and $n > 2$ there are the following cases :

(i) $p(x)$ symmetric, then $p(x) = \overline{p(x)}$, i.e., $t_3 = t_0$ so that also $t_5 = t_1$, $t_6 = t_2$, $t_7 = t_4$ and the orbit of $p(x)$ consists of only 4 polynomials, namely : $p(x)$, $-p(x)$, $p(-x)$, and $-p(-x)$.

(ii) $n/2$ even, odd coefficients of $p(x)$ symmetric while even coefficients are anti-symmetric, then $\overline{p(x)} = -p(-x)$, i.e., $t_3 = t_4$ and the orbit of $p(x)$ consist of 4 polynomials.

(iii) $n/2$ odd, even coefficients of $p(x)$ symmetric while odd coefficients are anti-symmetric, then $p(x) = p(-x)$, i.e., $t_3 = t_2$ and the orbit of $p(x)$ consists of 4 polynomials.

(iv) $p(x)$ asymmetric in all three senses above, then $p(x)$ is in an orbit of 8 polynomials.

Thus a population of 2^{n+1} polynomials consists of orbits of 8 or 4 whose members have the same numbers of real roots. Simple random sampling from the population can be performed more efficiently by simple random sampling of the orbits, provided orbits of 8 are given twice the probability of entering the sample as are orbits of 4. This will be the case if sampling is confined to a list of polynomials whose first two coefficients are identical, fixed at one of (1, 1), (−1, −1), (−1, 1), (1, −1). Suppose for concreteness, (1, 1) is chosen. It may be verified that in the resulting list of $2^{n-1} = 2^{n+1}/4$ polynomials there are two representatives of each orbit of size 8 and one of each orbit of size 4. Stratified random sampling would be carried out on a stratification of this list of 1/4 of the population of polynomials.

As an illustration of the above theory, for $n = 5$ the set S consists of $2^{n+1} = 2^6 = 64$ polynomials with 6 orbits of size 8 and 4 orbits of size 4. The following is a list of the sign sequences of the 64. In parentheses are the numbers of roots of each orbit as determined by numerical solution of the polynomials.

(1)	(1)	(1)	(3)	(3)
−−−−+−	−−−++−	−−−+−−	−−+−−+	−−−−++
++++−+	+++−−+	+++−++	++−++−	++++−−
+−+−−−	+−++−−	+−+++−	+−−−++	+−+−−+
−+−−−−	−++−−−	−−+−−−	+−−+−−	++−−−−
−+−+++	−+−−++	−+−−−+	−+++−−	−+−++−
+−++++	+−−+++	++−+++	−++−++	−−++++
+++−+−	++−−+−	+−−++−	−−+++−	+++−+−
−−−+−+	−−++−+	−+++−+	++−−−+	+−−+−+

(1)	(1)	(1)	(3)	(1)
−−−−−+	−−−−−−	−−−+++	−−+−++	−−++−−
+++++−	++++++	+++−−−	++−+−−	++−−++
+−+−++	+−+−+−	+−++−+	+−−−−+	+−−++−
+−−−−−	−+−+−+	−+−−+−	−++++−	−++−−+
−+−+−−				
−+++++				
−−+−+−				
++−+−+				

Acknowledgement

The author thanks Frederick Mosteller for helpful comments.

References

Bloch, A. and Polya, G. (1932) : On the roots of certain algebraic equations. *Proc. London Math. Soc.*, **II**, **33**, 102-114.

Erdos, P. and Offord, A. (1956) : On the number of real roots of a random algebraic equation. *Proc. London Math. Soc.*, **6**, 139-160.

Ibragimov, I. and Maslova, N. (1971) : On the expected number of real zeros of random polynomials I. Coefficients with zero means. *Theory of Probability and its Applications*, **XVI**, No. 2.

Kac, M. (1943) : On the average number of real roots of a random algebraic equation. *Bulletin American Math. Soc.*, **49**, 314-320.

——— (1949) : On the average number of real roots of a random algebraic equation (II). *Proc. London Math. Soc.*, **50**, 390-408.

Lilley, F. (1967) : *Zeros of a Polynomial.* General electric information series, No. 65SD351.

Littlewood, J. and Offord, A. (1939) : On the number of real roots of a random algebraic equation II. *Proc. Cambridge Phil. Soc.*, **35**, 133-148.

Stevens, D. (1965) : The average number of real zeros of a random polynomial, doctoral dissertation, New York University, Department of Mathematics.

Paper received : February, 1975.