Proc. Camb. Phil. Soc. (1973), **74**, 133
PCPS 74–18
Printed in Great Britain

Probability and the elementary symmetric functions

BY J. DENMEAD SMITH
College of the Resurrection, Mirfield, Yorkshire

(*Received* 2 *November* 1972)

1. *Introduction.* Let p be a prime, and suppose that $x_1, \ldots, x_N$ are independent random variables which take the values $0, 1, \ldots, p-1$ with probabilities $s_0, s_1, \ldots, s_{p-1}$, where $s_0 + \ldots + s_{p-1} = 1$ and $0 < s_k < 1$ for each k. $P_N(n)$ denotes the probability that the elementary symmetric function $\sigma_r(x_1, \ldots, x_N) = \Sigma x_1 \ldots x_r$ of the rth degree in the variables $x_1, \ldots, x_N$ is congruent, modulo p, to a prescribed integer n.

In section 2 it is shown that as $N \to \infty$, $P_N(n)$ tends to a limit $P_\infty(n)$ which is independent of $s_0, s_1, \ldots, s_{p-1}$. Upper and lower bounds for $P_\infty(n)$ are found in section 3, and the limit is determined exactly for certain values of p and r.

Throughout, we use '$m \equiv n$' to denote '$m = n \pmod p$'.

2. *Estimation of* $P_N(n)$. The elementary symmetric functions are generated by the polynomial

$$(1 + x_1 X) \ldots (1 + x_N X) = 1 + \sum_{r=1}^{N} \sigma_r(x_1, \ldots, x_N) X^r$$

in an indeterminate X. Thus if the value of σ_r when m_1 of the integers are 1, m_2 are 2, etc., is denoted by $\sigma_r[m_1, \ldots, m_{p-1}]$,

$$(1 + X)^{m_1} (1 + 2X)^{m_2} \ldots (1 + \overline{p-1} X)^{m_{p-1}} = 1 + \sum_{r=1}^{\infty} \sigma_r[m_1, \ldots, m_{p-1}] X^r, \qquad (2{\cdot}1)$$

where the sum on the right-hand side terminates at $r = m_1 + \ldots + m_{p-1}$.

Now from the binomial theorem,

$$(1 + lX)^p \equiv 1 + l^p X^p \equiv 1 + lX^p$$

so that by induction, if K is a power of p, $(1 + lX)^K \equiv 1 + lX^K$ and therefore

$$1 + \sum_{r=1}^{\infty} \sigma_r[m_1, \ldots, m_l + K, \ldots, m_{p-1}] X^r \equiv (1 + lX^K) \left(1 + \sum_{r=1}^{\infty} \sigma_r[m_1, \ldots, m_l, \ldots, m_{p-1}] X^r \right).$$

It follows, by considering the coefficient of X^r, that if K is the smallest power of p that exceeds r (which we now assume) then $\sigma_r[m_1, \ldots, m_l + K, \ldots, m_{p-1}]$ and

$$\sigma_r[m_1, \ldots, m_l, \ldots, m_{p-1}]$$

are congruent $(\bmod p)$. The set $\mathscr{S}(n)$ of $(p-1)$-tuples $(m_1, \ldots, m_{p-1})$ for which the condition $\sigma_r[m_1, \ldots, m_{p-1}] \equiv n$ holds is therefore periodic in each component, with the same period K.

Now the probability that m_0 of the N integers chosen are 0, m_1 are $1, \ldots, m_{p-1}$ are $p-1$ is the multinomial term

$$\frac{N!}{m_0! \ldots m_{p-1}!} s_0^{m_0} \ldots s_{p-1}^{m_{p-1}},$$

https://doi.org/10.1017/S0305004100047885 Published online by Cambridge University Press

and the value of σ_r is then $\sigma_r[m_1, \ldots, m_{p-1}]$. To calculate the required probability $P_N(n)$ it will be convenient to introduce the characteristic function on $\mathscr{S}(n)$, which is defined by $\chi(m_1, \ldots, m_{p-1}) = 1$ if $\sigma_r[m_1, \ldots, m_{p-1}] \equiv n$ and $\chi(m_1, \ldots, m_{p-1}) = 0$ otherwise. Thus

$$P_N(n) = \Sigma\chi(m_1, \ldots, m_{p-1}) \frac{N!}{m_0! \ldots m_{p-1}!} s_0^{m_0} \ldots s_{p-1}^{m_{p-1}},$$

in which the sum ranges over non-negative integers $m_0, \ldots, m_{p-1}$ satisfying

$$m_0 + \ldots + m_{p-1} = N.$$

We now exploit the periodic property of χ and define a Fourier analysis as follows.

Let ω be a primitive Kth root of unity, for example $\omega = \exp(2\pi i/K)$, and let $[0, K-1]^{p-1}$ denote the $(p-1)$-dimensional lattice cube of $(p-1)$-tuples $(m_1, \ldots, m_{p-1})$, where $0 \leqslant m_k \leqslant K-1$ for each k. If $(l_1, \ldots, l_{p-1}) \in [0, K-1]^{p-1}$,

$$(s_0 + s_1\omega^{l_1} + \ldots + s_{p-1}\omega^{l_{p-1}})^N = \sum_{m_0, \ldots, m_{p-1}} \omega^{l_1 m_1 + \ldots + l_{p-1} m_{p-1}} \frac{N!}{m_0! \ldots m_{p-1}!} s_0^{m_0} \ldots s_{p-1}^{m_{p-1}},$$

where $m_0 + \ldots + m_{p-1} = N$. Thus

$$P_N(n) = \sum_{l_1=0}^{K-1} \ldots \sum_{l_{p-1}=0}^{K-1} a(l_1, \ldots, l_{p-1}) (s_0 + s_1\omega^{l_1} + \ldots + s_{p-1}\omega^{l_{p-1}})^N \tag{2·2}$$

provided

$$\chi(m_1, \ldots, m_{p-1}) = \sum_{l_1=0}^{K-1} \ldots \sum_{l_{p-1}=0}^{K-1} a(l_1, \ldots, l_{p-1}) \omega^{l_1 m_1 + \ldots + l_{p-1} m_{p-1}}. \tag{2·3}$$

Equation (2·3) can be inverted and gives

$$a(l_1, \ldots, l_{p-1}) = \frac{1}{K^{p-1}} \sum_{m_1=0}^{K-1} \ldots \sum_{m_{p-1}=0}^{K-1} \chi(m_1, \ldots, m_{p-1}) \omega^{-(l_1 m_1 + \ldots + l_{p-1} m_{p-1})}. \tag{2·4}$$

Now the expression $\tilde{z} = s_0 + s_1\omega^{l_1} + \ldots + s_{p-1}\omega^{l_{p-1}}$ which occurs in equation (2·2) has $|\tilde{z}| < 1$ unless $l_1 = \ldots = l_{p-1} = 0$. In the other cases $|\tilde{z}|^N$ therefore tends to 0 as $N \to \infty$, and hence

$$\begin{aligned} P_N(n) \to P_\infty(n) &= a(0, \ldots, 0) \\ &= \frac{1}{K^{p-1}} \sum_{m_1=0}^{K-1} \ldots \sum_{m_{p-1}=0}^{K-1} \chi(m_1, \ldots, m_{p-1}), \end{aligned}$$

i.e. $P_\infty(n) = L(n)/K^{p-1}$ where $L(n)$ is the number of elements in the set

$$\mathscr{L}(n) = \mathscr{S}(n) \cap [0, K-1]^{p-1}.$$

We thus have the surprising result that the value of $P_\infty(n)$ does not depend on the magnitudes of $s_0, \ldots, s_{p-1}$ (except in so far as they are non-zero), and it is equal to the probability that $\sigma_r[m_1, \ldots, m_{p-1}] \equiv n$, where $(m_1, \ldots, m_{p-1})$ is a uniformly distributed random vector in $[0, K-1]^{p-1}$.

The 'error' can also be estimated. From equation (2·4), $|a(l_1, \ldots, l_{p-1})| \leqslant L(n)/K^{p-1}$, and with equation (2·2) this gives

$$|P_N(n) - P_\infty(n)| \leqslant \frac{L(n)}{K^{p-1}} \Sigma|s_0 + \ldots + s_{p-1}\omega^{l_{p-1}}|^N, \tag{2·5}$$

where the sum ranges over *non-zero* vectors $(l_1, \ldots, l_{p-1})$ in $[0, K-1]^{p-1}$. Now

$$\tilde{z} = s_0 + s_1\omega^{l_1} + \ldots + s_{p-1}\omega^{l_{p-1}}$$

https://doi.org/10.1017/S0305004100047885 Published online by Cambridge University Press

represents the centroid of a distribution of masses s_0 at 1, s_1 at ω^{l_1}, etc. in the complex plane. If t is the total mass at 1, the remaining masses lie in $\mathrm{Re}\, z \leqslant \cos(2\pi/K)$, $|z| = 1$, and hence $\tilde{z}$ is the centroid of a particle of mass t at 1 and another of mass $1-t$ situated at some point z in $\mathrm{Re}\, z \leqslant \cos(2\pi/K)$, $|z| \leqslant 1$. It is readily seen that $|\tilde{z}|$ is not diminished if z is set equal to $\exp(2\pi i/K)$, and as here

$$\begin{aligned} |\tilde{z}| &\leqslant |t+(1-t)\exp(2\pi i/K)| \\ &= [1-4t(1-t)\sin^2(\pi/K)]^{\frac{1}{2}} \end{aligned}$$

If $s = \inf\{s_0, s_1, \ldots, s_{p-1}\}$,

$$t(1-t)-s(1-s) = (t-s)(1-t-s) \geqslant 0$$

and therefore $|\tilde{z}| \leqslant [1-4s(1-s)\sin^2(\pi/K)]^{\frac{1}{2}}$. Insertion of this in equation (2·5) gives the relation

$$|P_N(n)/P_\infty(n)-1| \leqslant (K^{p-1}-1)[1-4s(1-s)\sin^2(\pi/K)]^{\frac{1}{2}N}.$$

3. *Determination of* $P_\infty(n)$. As shown above, this problem is equivalent to determining $L(n)$, the number of times that $\sigma_r[m_1, \ldots, m_{p-1}]$ is congruent to $n \pmod p$, where $(m_1, \ldots, m_{p-1})$ is a variable lattice-point in the cube $[0, K-1]^{p-1}$. Although this is a counting problem it will be convenient to retain the language of probability, and consider $m_1, \ldots, m_{p-1}$ as random variables, each distributed uniformly in $[0, K-1]$. The results for $P_\infty(n)$ will be obtained by making a transformation of the variables which will now be described.

Let $\mathbf{m} = (m_1, \ldots, m_{p-1})$ be a lattice-vector in $[0, p-1]^{p-1}$, and

$$\boldsymbol{\sigma} = (\sigma_1[\mathbf{m}], \ldots, \sigma_{p-1}[\mathbf{m}])$$

the associated lattice-vector in $[0, p-1]^{p-1}$, defined by

$$(1+X)^{m_1}\ldots(1+\overline{p-1}X)^{m_{p-1}} \equiv 1+\sum_{r=1}^{\infty}\sigma_r[\mathbf{m}]\,X^r.$$

We first show that the mapping $\mathbf{m} \to \boldsymbol{\sigma}[\mathbf{m}]$ is one-to-one.

From Newton's formula,

$$r\sigma_r = \tau_1\sigma_{r-1}-\tau_2\sigma_{r-2}+\ldots+(-)^r\tau_{r-1}\sigma_1-(-)^r\tau_r \quad \text{where} \quad \tau_r = \sum_{l=1}^{p-1} m_l l^r,$$

it follows that $\tau_1, \ldots, \tau_{p-1}$ are determined by $\sigma_1, \ldots, \sigma_{p-1}$ and *vice versa*; hence $\boldsymbol{\sigma}$ and $\boldsymbol{\tau} = (\tau_1, \ldots, \tau_{p-1})$ are in 1-1 correspondence. Also, since the matrix of coefficients $[l^r]$ has a determinant which is non-zero $(\mathrm{mod}\, p)$, the map $\mathbf{m} \to \boldsymbol{\tau}$ is bijective and we therefore conclude that $\boldsymbol{\sigma}$ and $\mathbf{m}$ are in 1-1 correspondence.

Now suppose that $K = p^{\kappa+1}$ where $\kappa \geqslant 0$, and let

$$\mathbf{m} \in [0, K-1]^{p-1}, \quad \boldsymbol{\sigma} \in [0, p-1]^{K-1}$$

where $\boldsymbol{\sigma}$ is defined by equation (2·1). The p-ary representation of m_k is denoted

$$m_k = \sum_{\lambda=0}^{\kappa} m_k^{(\lambda)} p^\lambda$$

where $0 \leqslant m_k^{(\lambda)} \leqslant p-1$, and we write

$$\mathbf{m}^{(\lambda)} = (m_1^{(\lambda)}, \ldots, m_{p-1}^{(\lambda)}) \in [0, p-1]^{p-1}$$

https://doi.org/10.1017/S0305004100047885 Published online by Cambridge University Press

and $\boldsymbol{\sigma}^{(\lambda)} = \boldsymbol{\sigma}[\mathbf{m}^{(\lambda)}] \in [0, p-1]^{p-1}$. Since $(1+kX)^{m_k^{(\lambda)} p^\lambda} \equiv (1+kX^{p^\lambda})^{m_k^{(\lambda)}}$, the following factorization is immediate:

$$1 + \sum_{r=1}^{\infty} \sigma_r[\mathbf{m}] X^r \equiv \left(1 + \sum_{r=1}^{\infty} \sigma_r^{(0)} X^r\right)\left(1 + \sum_{r=1}^{\infty} \sigma_r^{(1)} X^{rp}\right) \ldots \left(1 + \sum_{r=1}^{\infty} \sigma_r^{(\kappa)} X^{rp^\kappa}\right). \quad (3{\cdot}1)$$

The lattice-points $(m_1, \ldots, m_{p-1})$ are in 1-1 correspondence with the vectors $\mathbf{m}^{(0)}, \ldots, \mathbf{m}^{(\kappa)}$, and these are in 1-1 correspondence with the vectors $\boldsymbol{\sigma}^{(0)}, \ldots, \boldsymbol{\sigma}^{(\kappa)}$. Our problem is to determine the probability that σ_r attains the particular value n when $\mathbf{m}$ is a random vector in $[0, K-1]^{p-1}$, and this shows that we may equivalently consider that $\boldsymbol{\sigma}^{(0)}, \ldots, \boldsymbol{\sigma}^{(\kappa)}$ are each random vectors in $[0, p-1]^{p-1}$, defining σ_r according to equation (3·1). Here it is implicit that for $r \geqslant p$, $\sigma_r^{(\lambda)}$ is a function of $\boldsymbol{\sigma}^{(\lambda)}$.

When $r < p$ (i.e. $\kappa = 0$), σ_r is itself a random variable, so that the values $0, 1, \ldots, p-1$ are attained with equal probability and $P_\infty(n) = p^{-1}$ for each n.

For $p \leqslant r = \sum_{\lambda=0}^{\kappa} r_\lambda p^\lambda$ in the p-ary representation, the value of σ_r is

$$\Sigma \sigma_{q_0}^{(0)} \sigma_{q_1}^{(1)} \ldots \sigma_{q_\kappa}^{(\kappa)} \pmod{p}$$

where the sum ranges over all non-negative integers $q_0, q_1, \ldots, q_\kappa$ satisfying

$$r = \sum_{\lambda=0}^{\kappa} q_\lambda p^\lambda$$

and $\sigma_0^{(\lambda)} = 0$ for each λ. Thus, although $0 \leqslant q_\kappa \leqslant r_\kappa$, $q_0, q_1, \ldots, q_{\kappa-1}$ may range outside $q_\lambda \leqslant p-1$ (except in the case $p = 2$) and this is what makes the problem difficult, in general, to solve. However, in certain cases an explicit solution can be provided.

For the simplest case $p = 2$,

$$\sigma_r \equiv \sigma_{r_0}^{(0)} \sigma_{r_1}^{(1)} \ldots \sigma_{r_\kappa}^{(\kappa)}$$

and hence $\sigma_r \not\equiv 0$ (i.e. $\sigma_r \equiv 1$) if and only if $\sigma_{r_0}^{(0)} = \ldots = \sigma_{r_\kappa}^{(\kappa)} = 1$. Now suppose that ν of the digits $r_0, \ldots, r_\kappa$ are non-zero. If $r_\lambda = 0$ then $\sigma_{r_\lambda}^{(\lambda)} = 1$ automatically; otherwise the probability is $\frac{1}{2}$ that $\sigma_{r_\lambda}^{(\lambda)} = 1$. The probability that $\sigma_r \not\equiv 0$ is therefore $2^{-\nu}$, and hence $P_\infty(1) = 2^{-\nu}$.

If $r_0 = \ldots = r_{\kappa-1} = 0$ then

$$\sigma_r \equiv \sigma_{r_\kappa}^{(\kappa)} + \Sigma \sigma_{q_0}^{(0)} \ldots \sigma_{q_\kappa}^{(\kappa)}$$

where the sum ranges over non-negative integers $q_0, \ldots, q_\kappa$ satisfying

$$\sum_{\lambda=0}^{\kappa} q_\lambda p^\lambda = r, \quad q_\kappa < r_\kappa.$$

Since this sum is independent of the random variable $\sigma_{r_\kappa}^{(\kappa)}$, σ_r is equally likely to attain any value. Thus if r is of the form lp^κ where $1 \leqslant l \leqslant p-1$, $P_\infty(n) = p^{-1}$ for each n.

For arbitrary r this may be generalized to an inequality. We shall show, by induction on ν, that if ν of the digits $r_0, \ldots, r_\kappa$ are non-zero, then for every n, $P_\infty(n) \geqslant (p-1)^{\nu-1}/p^\nu$. The case $\nu = 1$ has just been proved.

When $\nu > 1$,

$$\sigma_r = (\Sigma \sigma_{q_0}^{(0)} \ldots \sigma_{q_{\kappa-1}}^{(\kappa-1)}) \sigma_{r_\kappa}^{(\kappa)} + \Sigma \sigma_{t_0}^{(0)} \ldots \sigma_{t_\kappa}^{(\kappa)}$$

where

$$\sum_{\lambda=0}^{\kappa-1} q_\lambda p^\lambda = \sum_{\lambda=0}^{\kappa-1} r_\lambda p^\lambda, \quad \sum_{\lambda=0}^{\kappa} t_\lambda p^\lambda = r$$

https://doi.org/10.1017/S0305004100047885 Published online by Cambridge University Press

and $t_\kappa < r_\kappa$. Hence, if $\Sigma\sigma_{q_0}^{(0)}\ldots\sigma_{q_{\kappa-1}}^{(\kappa-1)} \not\equiv 0$, σ_r is 'controlled' by the random variable $\sigma_{r_\kappa}^{(\kappa)}$. In this case, therefore, when $\sigma_{r_\kappa}^{(\kappa)}$ varies all values of σ_r are attained with equal probability. By the inductive hypothesis, the probability that $\Sigma\sigma_{q_0}^{(0)}\ldots\sigma_{q_{\kappa-1}}^{(\kappa-1)} \not\equiv 0$ is at least $(p-1).(p-1)^{\nu-2}/p^{\nu-1} = (p-1)^{\nu-1}/p^{\nu-1}$, and on dividing by p the required result is obtained.

Also, $P_\infty(n) = 1 - \sum_{m \neq n} P_\infty(m) \leqslant 1-(p-1)^\nu/p^\nu$, and hence

$$\frac{(p-1)^{\nu-1}}{p^\nu} \leqslant P_\infty(n) \leqslant 1-\left(\frac{p-1}{p}\right)^\nu.$$

This completes the proof of the following theorem:

THEOREM 1. *If there are ν non-zero digits in the p-ary representation of r, then*

$$\frac{(p-1)^{\nu-1}}{p^\nu} \leqslant P_\infty(n) \leqslant 1-\left(\frac{p-1}{p}\right)^\nu$$

for each n. In particular, if $\nu = 1$, $P_\infty(n) = p^{-1}$ for each n.

Also, for $p = 2$, $P_\infty(0) = 1-2^{-\nu}$, $P_\infty(1) = 2^{-\nu}$.

The inequality in Theorem 1 can be tightened up if r and $p-1$ are mutually prime. In this case we have $P_\infty(n_1) = P_\infty(n_2)$ if n_1 and n_2 are both non-zero, which gives $P_\infty(0)+(p-1)P_\infty(1) = 1$. From

$$P_\infty(0) \geqslant \frac{(p-1)^{\nu-1}}{p^\nu}$$

an improved upper bound for $P_\infty(1)$ is now obtained:

$$\frac{(p-1)^{\nu-1}}{p^\nu} \leqslant P_\infty(1) \leqslant \frac{1}{p-1} - \frac{(p-1)^{\nu-2}}{p^\nu},$$

although the inequality for $P_\infty(0)$ is not changed.

That $P_\infty(n_1) = P_\infty(n_2)$ if $(r, p-1) = 1$ can be demonstrated as follows. Let G denote the group of $\{1, 2, \ldots, p-1\}$ combining under multiplication mod p, and $G^{(r)}$ the subgroup of the rth powers of G. By Fermat's theorem $G^{(r)} = G^{(s)}$ if $r = s \pmod{(p-1)}$, and since G is cyclic it is easily seen that $G^{(r)} = G$ if and only if r and $p-1$ are mutually prime; in fact by the decomposition theorem for Abelian groups a similar result holds for any finite Abelian group.

Now suppose that $g \in G$, and let the permutation π on G denote the action of g, i.e. $g^{-1}n \equiv \pi(n)$ for each $n \in G$. It is readily verified that, since σ_r is homogeneous of degree r,

$$\sigma_r[m_{\pi(1)}, \ldots, m_{\pi(p-1)}] \equiv g^r\sigma_r[m_1, m_2, \ldots, m_{p-1}].$$

The 1-1 mapping that π induces on $[0, K-1]^{p-1}$ therefore transforms $\mathscr{L}(n_1)$ into $\mathscr{L}(n_2)$, where $n_2 \equiv g^r n_1$, and hence $L(n_2) = L(n_1)$ if n_1 and n_2 belong to the same coset of $G^{(r)}$. In particular, if $(r, p-1) = 1$, $L(n)$ is constant for non-zero n.

We have also been able to evaluate $P_\infty(n)$ in the two cases $r = p+1, p+2$.

THEOREM 2. *Let $\mu = \frac{1}{2}(p+1)$.*

(i) *If $r = p+1$ and $p > 3$,*

$$P_\infty(n) = \begin{cases} \dfrac{1}{p} & \text{for} \quad n = 0 \\ \dfrac{1}{p} \pm \dfrac{1}{p^\mu} & \text{according as } 2n \text{ is a quadratic residue or not, i.e. } (2n)^{\frac{1}{2}(p-1)} \equiv \pm 1. \end{cases}$$

https://doi.org/10.1017/S0305004100047885 Published online by Cambridge University Press

(ii) *If* $r = p+2$ *and* $p > 2$,

$$P_\infty(n) = \begin{cases} \frac{1}{p} + \frac{p-1}{p^\mu} & \text{for} \quad n = 0, \\ \frac{1}{p} - \frac{1}{p^\mu} & \text{otherwise.} \end{cases}$$

Proof. (i) $\sigma_{p+1} \equiv \sigma_1^{(0)}\sigma_1^{(1)} + \sigma_{p+1}^{(0)}$. Thus if $\sigma_1^{(0)} \neq 0$, σ_{p+1} attains all values with equal probability when the remaining variables vary, since σ_{p+1} is obtained from $\sigma_1^{(1)}$ by a linear transformation. However, if $\sigma_1^{(0)} = 0$, then from Newton's formula

$$\sigma_{p+1} \equiv \sigma_{p+1}^{(0)} \equiv -\tau_2^{(0)}\sigma_{p-1}^{(0)} + \tau_3^{(0)}\sigma_{p-2}^{(0)} - \ldots - \tau_{p-1}^{(0)}\sigma_2^{(0)} + 2\sigma_2^{(0)},$$

where we have used the fact that $\tau_p^{(0)} \equiv \tau_1^{(0)} = 0$. When σ_{p+1} is expressed in terms of $\sigma_1^{(0)}, \ldots, \sigma_{p-1}^{(0)}$ the term which involves $\sigma_{p-1}^{(0)}$ is $\sigma_2^{(0)}\sigma_{p-1}^{(0)}$. Thus for $\sigma_1^{(0)} = 0$ and for fixed $\sigma_2^{(0)} \neq 0$, σ_{p+1} takes all values with equal probability.

Now suppose that $\sigma_1^{(0)} = \sigma_2^{(0)} = \ldots = \sigma_k^{(0)} = 0$, where $k < \mu - 1$. The term in σ_{p+1} involving $\sigma_m^{(0)}$ with greatest m is $\sigma_{k+1}^{(0)}\sigma_{p-k}^{(0)}$, in which $m = p-k$. Therefore for fixed $\sigma_{k+1}^{(0)} \neq 0$, σ_{p+1} takes all values with equal probability when the remaining variables are allowed to vary. This process may be carried out for $k = 1, 2, \ldots, \mu-2$, until we have with $\sigma_1^{(0)} = \sigma_2^{(0)} = \ldots = \sigma_{\mu-1}^{(0)} = 0$ that $\sigma_{p+1} = \mu[\sigma_\mu^{(0)}]^2$. The probability that

$$\sigma_1^{(0)} = \ldots = \sigma_{\mu-1}^{(0)} = 0$$

is $1/(p^{\mu-1})$, and if this is the case and the remaining variables vary, the probability that $\sigma_{p+1} \equiv n$ is

$$\begin{cases} 1/p & \text{if} \quad n = 0, \\ 2/p & \text{if} \quad 2n \text{ is a quadratic residue,} \\ 0 & \text{if} \quad 2n \text{ is not a quadratic residue.} \end{cases}$$

Hence

$$P_\infty(n) = \begin{cases} \left(1 - \frac{1}{p^{\mu-1}}\right)\frac{1}{p} + \frac{1}{p^\mu} = \frac{1}{p} & \text{if} \quad n = 0, \\ \left(1 - \frac{1}{p^{\mu-1}}\right)\frac{1}{p} + \frac{2}{p^\mu} = \frac{1}{p} + \frac{1}{p^\mu} & \text{if} \quad 2n \text{ is a } QR, \\ \left(1 - \frac{1}{p^{\mu-1}}\right)\frac{1}{p} = \frac{1}{p} - \frac{1}{p^\mu} & \text{if} \quad 2n \text{ is not a } QR. \end{cases}$$

Euler's criterion states that l, is or is not a QR according as $l^{\frac{1}{2}(p-1)} \equiv \pm 1$.

An exception occurs in the above proof when $p = 3$. In this case, if $\sigma_1^{(0)} = 0$ we have $\sigma_4 = 2[\sigma_2^{(0)}]^2 + 2\sigma_2^{(0)}$. Thus for $\sigma_2^{(0)}$ varying and $\sigma_1^{(0)} = 0$, the probability that σ_4 takes the values 0, 1, 2 are respectively $\frac{2}{3}$, $\frac{1}{3}$, 0 and hence

$$P_\infty(0) = \tfrac{1}{3}.\tfrac{2}{3} + \tfrac{1}{3}.\tfrac{2}{3} = \tfrac{4}{9},$$
$$P_\infty(1) = \tfrac{1}{3}.\tfrac{2}{3} + \tfrac{1}{3}.\tfrac{1}{3} = \tfrac{1}{3},$$
$$P_\infty(2) = \tfrac{1}{3}.\tfrac{2}{3} = \tfrac{2}{9}.$$

(ii) $\sigma_{p+2} \equiv \sigma_2^{(0)}\sigma_1^{(1)} + \sigma_{p+2}^{(0)}$, so that if $\sigma_2^{(0)} \neq 0$ is fixed, σ_{p+2} attains all values with equal probability. Now

$$2\sigma_{p+2}^{(0)} \equiv \tau_1^{(0)}\sigma_{p+1}^{(0)} - \tau_2^{(0)}\sigma_p^{(0)} + \tau_3^{(0)}\sigma_{p-1}^{(0)} - \ldots - \tau_{p-1}^{(0)}\sigma_3^{(0)} + 3\sigma_3^{(0)} \qquad (3{\cdot}2)$$

https://doi.org/10.1017/S0305004100047885 Published online by Cambridge University Press

and
$$\sigma^{(0)}_{p+1} \equiv \tau^{(0)}_1 \sigma^{(0)}_p - \tau^{(0)}_2 \sigma^{(0)}_{p-1} + \ldots - \tau^{(0)}_{p-1} \sigma^{(0)}_2 + 2\sigma^{(0)}_2. \tag{3·3}$$

On taking equation (3·2) $+ \sigma^{(0)}_1 \times$ equation (3·3) both $\sigma^{(0)}_{p+1}$ and $\sigma^{(0)}_p$ are eliminated, and if $\sigma^{(0)}_2 = 0$

$$2\sigma_{p+2} \equiv (\tau^{(0)}_3 - \sigma^{(0)}_1 \tau^{(0)}_2)\, \sigma^{(0)}_{p-1} - (\tau^{(0)}_4 - \sigma^{(0)}_1 \tau^{(0)}_3)\, \sigma^{(0)}_{p-2} + \ldots$$
$$+ (\tau^{(0)}_{p-2} - \sigma^{(0)}_1 \tau^{(0)}_{p-3})\, \sigma^{(0)}_4 - \tau^{(0)}_{p-1} \sigma^{(0)}_3 + 3\sigma^{(0)}_3.$$

The coefficient of $\sigma^{(0)}_{p-1}$ in $2\sigma_{p+2}$ is
$$\tau^{(0)}_3 - \sigma^{(0)}_1 \tau^{(0)}_2 - \sigma^{(0)}_3 = 2\sigma^{(0)}_3$$
and it is therefore non-zero if $\sigma^{(0)}_3 \neq 0$. For $\sigma^{(0)}_2 = 0$ and $\sigma^{(0)}_3 \neq 0$ fixed, σ_{p+2} therefore takes all values with equal probability when the remaining variables $\sigma^{(1)}_1, \sigma^{(0)}_1, \sigma^{(0)}_4, \ldots, \sigma^{(0)}_{p-1}$ are allowed to vary.

Now suppose that $\sigma^{(0)}_2 = \sigma^{(0)}_3 = \ldots = \sigma^{(0)}_{k+1} = 0$, where $k < \mu$. The coefficient of $\sigma^{(0)}_{p-k}$ in $2\sigma_{p+2}$ is
$$(-)^{k+1} [\tau^{(0)}_{k+2} - \sigma^{(0)}_1 \tau^{(0)}_{k+1}] + (p-k)\, \sigma^{(0)}_{k+2}.$$
Also
$$(k+2)\, \sigma^{(0)}_{k+2} = \tau^{(0)}_1 \sigma^{(0)}_{k+1} - \tau^{(0)}_2 \sigma^{(0)}_k + \tau^{(0)}_3 \sigma^{(0)}_{k-1} - \ldots + (-)^k \tau^{(0)}_{k+1} \sigma^{(0)}_1 + (-)^{k+1} \tau^{(0)}_{k+2},$$
so that the coefficient of $\sigma^{(0)}_{p-k}$ in $2\sigma_{p+2}$ is $2\sigma^{(0)}_{k+2}$. Thus $\sigma_{p+2} \equiv \sigma^{(0)}_{k+2} \sigma^{(0)}_{p-k} +$ 'lower suffix terms', and hence if $\sigma^{(0)}_{k+2} \neq 0$, σ_{p+2} is 'controlled' by $\sigma^{(0)}_{p-k}$. This process can be continued until, if $\sigma^{(0)}_2 = \ldots = \sigma^{(0)}_\mu = 0$, we have $\sigma_{p+2} = 0$. The probability that this occurs is $1/(p^{\mu-1})$, in which case σ_r is certain to be zero. In the contrary case σ_r is equally likely to take any value. Therefore

$$P_\infty(n) = \left(1 - \frac{1}{p^{\mu-1}}\right) \frac{1}{p} = \frac{1}{p} - \frac{1}{p^\mu} \quad \text{for} \quad n \neq 0,$$
$$P_\infty(0) = \left(1 - \frac{1}{p^{\mu-1}}\right) \frac{1}{p} + \frac{1}{p^{\mu-1}} = \frac{1}{p} + \frac{p-1}{p^\mu}.$$

4. *Conclusion.* The formulae for σ_r become highly non-linear as r increases, and are difficult to handle even for quite small values of p and r. Thus we have not been able to obtain more general results for $P_\infty(n)$, or to make conjectures on the basis of computed values.

If $\rho_r(x_1, \ldots, x_N)$ is an *arbitrary* symmetric polynomial of degree r, i.e. it can be written as a sum of homogeneous symmetric functions of the type $\Sigma x_1^{\alpha_1} \ldots x_k^{\alpha_k}$ where
$$\alpha_1 + \ldots + \alpha_k \leqslant r,$$
then by the Fundamental Theorem on Symmetric Functions, ρ_r can be written $f(\sigma_1, \ldots, \sigma_r)$ where f is a polynomial which does not depend on N, the number of variables (assuming that $N \geqslant r$). Much of the work thus carries over to ρ_r, in particular the whole of section 2. If $f(\sigma_1, \ldots, \sigma_r)$ is of the form $a\sigma_r + g(\sigma_1, \ldots, \sigma_{r-1})$, where $a \neq 0$, then Theorem 1 goes through (except the result when $p = 2$) and the improved inequality which follows holds when ρ_r is homogeneous and $(r, p-1) = 1$.

Another generalization, where zero probabilities among $s_0, \ldots, s_{p-1}$ are admitted only trivially affects section 2 but section 3 is completely upset because the essential 1-1 mappings no longer exist.

I am grateful to Dr Daykin of Reading University for a helpful conversation.

https://doi.org/10.1017/S0305004100047885 Published online by Cambridge University Press