APPLICATIONS OF COMBINATORIAL FORMULAE TO GENERALIZATIONS OF WILSON'S THEOREM

N. S. MENDELSOHN

Summary. By the use of finite difference operators a series of combinatorial formulae are obtained. Two applications of the formulae are given. First, the following explicit formulae for the number, $f(n)$, of non-isomorphic equivalence relations among n elements are obtained:

$$f(n) = \sum_{k=1}^{n} \sum_{j=0}^{k} (-1)^j \frac{\binom{k}{j} (k-j)^n}{k!} = \sum_{k=1}^{n} \sum_{j=0}^{k} (-1)^j \frac{(k-j)^n}{j!(k-j)!};$$

$$f(n) = \frac{n^n}{n!}\left(\frac{1}{0!}\right) + \frac{(n-1)^n}{(n-1)!}\left(\frac{1}{0!} - \frac{1}{1!}\right) + \frac{(n-2)^n}{(n-2)!}\left(\frac{1}{0!} - \frac{1}{1!} + \frac{1}{2!}\right) + \dots$$

Second, by applying Fermat's theorem (i.e. $x^{p-1} \equiv 1 \bmod p$ for each prime p, which is prime to x) to the combinatorial formulae, we obtain a series of congruences which in a sense are generalizations of Wilson's theorem. The most general formula of this type is the following. Let n and k be arbitrary positive integers such that $k \geq n+1$. There exists a positive integer $N(n, k)$ and a rational number $R(n, k)$, uniquely determined, such that

$$\int_0^1 \frac{dx_n}{x_n} \int_0^{x_n} \frac{dx_{n-1}}{x_{n-1}} \int_0^{x_{n-1}} \frac{dx_{n-2}}{x_{n-2}} \dots \int_0^{x_3} \frac{dx_2}{x_2} \int_0^{x_2} \left\{\frac{(1-x_1)^{p-k} - 1}{x_1}\right\} dx_1 \equiv R(n, k) \bmod p$$

for all primes $p \geqslant N(n, k)$. The number max $(n, 2k-2n-3)$ may be taken for $N(n, k)$. The proof of the theorem contains a method of computing $R(n, k)$. Such computations are not laborious for small n and k. As examples of such computations we quote the following formulae:

$$\int_0^1 \left\{\frac{(1-x)^{p-2} - 1}{x}\right\} dx \equiv -1 \bmod p, \text{ for all primes } p \geqslant 3;$$

$$\int_0^1 \frac{dt}{t} \int_0^t \left\{\frac{(1-x)^{p-3} - 1}{x}\right\} dx \equiv -\tfrac{1}{2} \bmod p, \text{ for all primes } p \geqslant 5.$$

Received September 1, 1948.

The author has also computed explicit formulae for some very general classes of cases of the main formulae. For example, if we denote

$$\int_0^1 \frac{dx_s}{x_s} \int_0^{x_s} \frac{dx_{s-1}}{x_{s-1}} \cdots \int_0^{x_3} \frac{dx_2}{x_2} \int_0^{x_2} \left\{\frac{(1-x_1)^{p-t}-1}{x_1}\right\} dx_1$$

by $I_p\ (s, t)$ we have the following:

$$I_p\ (s, s+1) \equiv -\frac{1}{s!} \bmod p \text{ for all primes } p > s;$$

$$I_p\ (s, s+2) \equiv -\frac{(s+2)}{s!\ 2} \bmod p \text{ for all primes } p > s;$$

$$I_p\ (s, s+3) \equiv -\frac{(s+3)(3s+8)}{s!\ 24} \bmod p \text{ for all } p > \max\ (s, 3);$$

$$I_p\ (s, s+4) \equiv -\frac{(s+4)^2(s+3)}{s!\ 48} \bmod p \text{ for all } p > \max\ (s, 5).$$

The details of the computations are not given in the main body of the paper, but the method used differs in no way from that explained in the paper.

General Remarks. A number of papers have already appeared which deal with the use of finite difference operators for symbolic solutions of combinaatorial problems. We content ourselves with three references [2], [3], and [4] in the bibliography. The operators we will use here are the standard operators E and Δ, defined as $Eu_n = u_{n+1}$ and $\Delta u_n = u_{n+1} - u_n$, with the obvious relation $E = 1 + \Delta$.

Consider a set of "triangular" equations connecting $u_0, u_1, \ldots, u_n$ with $v_0, v_1, \ldots, v_n$ by means of

$$\begin{aligned} v_0 &= c_{00}u_0 \\ v_1 &= c_{10}u_0 + c_{11}u_1 \\ v_2 &= c_{20}u_0 + c_{21}u_1 + c_{22}u_2 \\ &\cdot \\ &\cdot \\ &\cdot \\ v_n &= c_{n0}u_0 + c_{n1}u_1 + c_{n2}u_2 + \ldots + c_{nn}u_n. \end{aligned}$$

If $c_{00}c_{11} \ldots c_{nn} \neq 0$, the equations can be solved for $u_0, u_1, \ldots, u_n$ in terms of $v_0, v_1, \ldots, v_n$ in a unique way. Suppose the solved form of these equations is

$$\begin{aligned} u_0 &= d_{00}v_0 \\ u_1 &= d_{10}v_0 + d_{11}v_1 \\ &\cdot \\ &\cdot \\ &\cdot \\ u_n &= d_{n0}v_0 + d_{n1}v_1 + \ldots + d_{nn}v_n. \end{aligned}$$

https://doi.org/10.4153/CJM-1949-030-4 Published online by Cambridge University Press

It is immediately obvious how the d_{ij} may be obtained from the c_{ij} and conversely. However, we are interested in relating the d_{ij} to the c_{ij} by a symbolic equation. To this end we write both sets of equations as follows:

(1) $$v_n = P_n(E)u_0, \text{ for } n = 0, 1, 2, 3, \ldots$$

(2) $$u_n = Q_n(E)v_0, \text{ for } n = 0, 1, 2, 3, \ldots$$

where $P_n(E) = c_{n0} + c_{n1}E + c_{n2}E^2 + \ldots + c_{nn}E^n$ and $Q_n(E) = d_{n0} + d_{n1}E + d_{n2}E^2 + \ldots + d_{nn}E^n$. To obtain the symbolic equation connecting d_{n0}, d_{n1}, $\ldots$, d_{nn} with c_{ij} we start with (2), $u_n = Q_n(E)v_0$; hence

(3) $$E^n u_0 = d_{n0}v_0 + d_{n1}v_1 + d_{n2}v_2 + \ldots + d_{nn}v_n$$

and using (1) this becomes $E^n u_0 = \{d_{n0} + d_{n1}P_1(E) + d_{n2}P_2(E) + \ldots + d_{nn} P_n(E)\} u_0$. Hence $E^n = Q_n(P)$ symbolically, where it is understood that in computing the right-hand side P^i is to be replaced by $P_i(E)$. In the same way $E^n = P_n(Q)$ where Q^i is to be replaced by $Q_i(E)$. Hence, the relations connecting the d_{ij} with the c_{ij} are compactly expressed by the symbolic equation

(4) $$P_n(Q) = E^n = Q_n(P).$$

The use of this general symbolic equation for the solution of combinatorial problems will be the subject of a subsequent paper. Here we will be concerned only with one particular case. Examples of pairs of polynomials $P_n(E)$ and $Q_n(E)$ which satisfy (4) are:

(a) $P_n(E) = \dfrac{1}{c_n} E^{n-1}\Delta$, and $P_0(E) = \dfrac{1}{c_0}$; $Q_n(E) = c_0 + c_1E + \ldots + c_nE^n$;

(b) $P_n(E) = (kE + r)^n$; $Q_n(E) = \dfrac{1}{k^n}(E - r)^n$;

(c) $P_n(E) = (1 + E)^n$; $Q_n(E) = \Delta^n$ (this is case (b) with $k = r = 1$);

(d) $P_n(E) = E^n - c_nE^{n-1}$; $Q_n(E) = E^n + c_nE^{n-1} + c_nc_{n-1}E^{n-2} + \ldots + c_nc_{n-1}c_{n-2} \ldots c_1$.

The equation to be used from here on is (c). More explicitly (c) is written as follows

$$\text{if}^1\ v_n = (E + 1)^n u_0$$
$$\text{then } u_n = \Delta^n v_0.$$

Applications. We consider first the following subsidiary problem. In how many ways can we place n distinguishable objects in m distinguishable boxes so that each box contains one object at least, the arrangement of the objects in the boxes being irrelevant. Let u_{mn} be the required number. The number of ways of placing the objects in the boxes without restriction is m^n. This can be broken up into the following exclusive cases: (1) no box is empty,

[1]This equation was pointed out to me by I. Kaplansky in 1938 and indirectly, in non-symbolic form, by Dean S. Beatty in 1935. It is implied by some of Poincaré's work. It first appeared explicitly (in non-symbolic form) in [1] which was published in 1938.

(2) one box is empty, (3) two boxes are empty, . . . , $(m + 1)$ all boxes are empty (vacuous). Hence,

$$(5) \qquad m^n = u_{mn} + \binom{m}{1} u_{m-1,n} + \binom{m}{2} u_{m-2,n} + \ldots + \binom{m}{m} u_{0n}.$$

Symbolically, this is written $m^n = (1 + E)^m u_{0n}$. Hence, using (c) we obtain

$$(6) \qquad u_{mn} = \Delta^m 0^n = (E - 1)^m 0^n.$$

Explicitly, this becomes

$$(7) \quad u_{mn} = m^n - \binom{m}{1}(m-1)^n + \binom{m}{2}(m-2)^n + \ldots + (-1)^{m-1}\binom{m}{m-1}.$$

We now apply (6) and (7) to the following problem.

How many non-isomorphic equivalence relationships do there exist among n objects? In combinatorial terms, this requires the determination of the number of ways of placing n distinct objects into any number of boxes, where we do not distinguish the boxes. If $f(n)$ be the required number, then obviously

$$f(n) = \sum_{i=1}^{n} \frac{u_{in}}{i!} + \sum_{i=1}^{n} \frac{\Delta^i 0^n}{i!}.$$

Hence we have

$$(8) \qquad f(n) = \sum_{k=1}^{n} \sum_{j=0}^{k} (-1)^j \binom{k}{j} \frac{(k-j)^n}{k!} = \sum_{k=1}^{n} \sum_{j=0}^{k} (-1)^j \frac{(k-j)^n}{j!(k-j)!}.$$

On inverting the order of summation, we obtain

$$(9) \; f(n) = \frac{n^n}{n!}\left(\frac{1}{0!}\right) + \frac{(n-1)^n}{(n-1)!}\left(\frac{1}{0!} - \frac{1}{1!}\right) + \frac{(n-2)^n}{(n-2)!}\left(\frac{1}{0!} - \frac{1}{1!} + \frac{1}{2!}\right) + \ldots$$

For a second application it is necessary to obtain alternative expressions for $u_{m,n}$. To this end we first note that $u_{mn} = 0$ if $n < m$. If $m = n$, then $u_{mn} = m!$ Applying this to (7) we obtain the well-known formula

$$(10) \quad m! = m^m - \binom{m}{1}(m-1)^m + \binom{m}{2}(m-2)^m + \ldots + (-1)^{m-1}\binom{m}{m-1}.$$

If $n = m + 1$, to evaluate u_{mn} we note that the distribution of objects into boxes is such that two of the objects appear in one of the boxes, the remaining boxes each containing one object. The two objects to appear in one box may be chosen in $\binom{m+1}{2}$ ways, and hence the number of ways of distributing

https://doi.org/10.4153/CJM-1949-030-4 Published online by Cambridge University Press

the objects is $\binom{m+1}{2} m! = \frac{m}{2}(m+1)!$ Applying this to equation (7) we obtain

$$(11)\quad \frac{m}{2}(m+1)! = m^{m+1} - \binom{m}{1}(m-1)^{m+1} + \binom{m}{2}(m-2)^{m+1} + \ldots + (-1)^{m-1}\binom{m}{m-1}.$$

In case $n = m+2$ we can easily show that $u_{m,m+2}$ is given by

$$u_{m,m+2} = \binom{m+2}{3} m! + \frac{1}{2}\binom{m+2}{2}\binom{m}{2} m! = (m+2)!\left\{\frac{m(3m+1)}{24}\right\}.$$

(This comes from considering that the distribution is such that either two of the boxes each contain two objects, the remaining boxes containing one object, or one box contains three objects, the remaining boxes each containing one object.) Applying the above formula to equation (7) we obtain

$$(12)\quad \left\{\frac{m(3m+1)}{24}\right\}(m+2)! = m^{m+2} - \binom{m}{1}(m-1)^{m+2} + \binom{m}{2}(m-2)^{m+2} + \ldots + (-1)^{m-1}\binom{m}{m-1}.$$

In general, we wish to establish the following formula

$$(13)\quad (m+k)!\, P_k(m) = m^{m+k} - \binom{m}{1}(m-1)^{m+k} + \binom{m}{2}(m-2)^{m+k} + \ldots + (-1)^{m-1}\binom{m}{m-1}$$

where $P_k(m)$ is a polynomial in m of degree k with rational coefficients, for each integer k. We already have shown that

$$P_0(m) = 1,\ P_1(m) = \frac{1}{2} m \text{ and } P_2(m) = \frac{m(3m+1)}{24}.$$

Formula (13) is equivalent to the statement that

$$u_{m,m+k} = (m+k)!\, P_k(m).$$

To establish this statement we first note that $u_{m,n}$ satisfies the following recurrence:

$$(14)\qquad u_{mn} = m u_{m,n-1} + m u_{m-1,n-1}.$$

Equation (14) for $n \geq m+2$ follows from the fact that the distribution of the objects into the boxes may be carried out as follows: One of the objects may be placed in any one of the boxes (there are m ways of doing this) and the remaining $(n-1)$ objects may be distributed either amongst all the m boxes so that each box gets at least one object (there are $u_{m,n-1}$ ways of doing this) or they may be distributed amongst the $(m-1)$ boxes not occupied by the first object in such a way that each of these $(m-1)$ boxes gets at least one object (there are $u_{m-1,n-1}$ ways of doing this). Hence equation (14) follows.

If in (14) we replace n by $m+k$ and then put $u_{m,m+k}=(m+k)!\,P_k(m)$, we obtain

$$(m+k)P_k(m)=m\left\{P_{k-1}(m)+P_k(m-1)\right\}. \tag{15}$$

Equation (15) with the initial conditions $P_1(m)=\dfrac{m}{2}$, $P_k(1)=\dfrac{1}{(k+1)!}$ is sufficient to determine $P_k(m)$ for all positive integers k, and for all positive integers m. We proceed to show that $P_k(m)$ is a polynomial in m of degree k with rational coefficients. We will also show that the denominators of these coefficients (when expressed in their lowest terms) contain no prime factors greater than $2k-1$ except for $k=1$. The proof is by induction on k.

Since $P_1(m)=\dfrac{m}{2}$, $P_2(m)=\dfrac{m(3m+1)}{24}$ the theorem is true for $k=1$, $k=2$. Assume that $P_{k-1}(m)=c_{0,k-1}+c_{1,k-1}m+\ldots+c_{k-1,k-1}m^{k-1}$ where each of the $c_{i,k-1}(i=0,1,2,\ldots,k-1)$ is a rational number which when expressed in its lowest terms has a denominator no prime factor of which exceeds $2k-3$. Now put $P_k(m)=c_{0k}+c_{1k}m+c_{2k}m^2+\ldots+c_{kk}m^k$ (assuming that such a form exists). Substituting into (15) we obtain the equation

$$(m+k)\sum_{i=0}^{k}c_{ik}m^i=m\left[\sum_{i=0}^{k-1}c_{i,k-1}m^i+\sum_{i=0}^{k}c_{ik}(m-1)^i\right].$$

In this equation the terms in m^{k+1} on both sides of the equation have identical coefficients. On equating coefficients of m^k we obtain $2kc_{kk}=c_{k-1,k-1}$. This together with $c_{11}=\dfrac{1}{2}$ yields $c_{kk}=\dfrac{1}{2^k k!}$. Now let us assume that $c_{k-r,k}$ has been obtained for $r=0,1,2,\ldots s$. Taking the coefficient of m^{k-s-1} on each side we obtain

$$c_{k-s-2,k}+kc_{k-s-1,k}=c_{k-s-2,k-1}+\left\{c_{k-s-2,k}-\binom{k-s-1}{1}c_{k-s-1,k}+\binom{k-s}{2}c_{k-s,k}+\ldots+(-1)^{k-s-2}\binom{k}{k-s-2}c_{kk}\right\}.$$ Hence we obtain

$$(2k-s-1)c_{k-s-1,k}=c_{k-s-2,k-1}+\left\{\binom{k-s}{2}c_{k-s,k}-\binom{k-s+1}{3}c_{k-s+1,k}+\ldots+(-1)^{k-s-2}\binom{k}{k-s-2}c_{kk}\right\}.$$

Since all the terms on the right have already been computed this yields $c_{k-s-1,k}$. It is obvious that the denominator of $c_{k-s-1,k}$ has no prime factor greater than $2k - 1$. This equation fails to yield the last coefficient c_{0k} but it is easily seen that $c_{0k} = 0$ for $k = 1, 2, 3, \ldots$. If we now put $m = 1$ in (15) and use the fact that $P_k(0) = 0$ (since $c_{0k} = 0$) we obtain $(1 + k)P_k(1) = P_{k-1}(1)$. From this it follows, since $P_1(1) = \frac{1}{2}$, that $P_k(1) = \dfrac{1}{(k+1)!}$. Hence, the initial conditions are satisfied. It is now obvious that if the polynomials $P_k(m)$ which have been determined by the above computation are substituted in equation (15), the equation is identically satisfied. Finally, since our initial conditions uniquely determine $P_k(m)$, the solution just found is the only possible one.

By specializing m in equation (13) and applying Fermat's theorem ($a^{p-1} \equiv 1 \bmod p$, if $(a, p) = 1$ and p is prime) we can get the most general formula we are looking for. However, it will be instructive to start with the more particular formulae (10), (11), (12) to obtain completely explicit solutions for the first few cases.

If in (10) we put $m = p - 1$ where p is a prime we obtain

$$(p-1)! = (p-1)^{p-1} - \binom{p-1}{1}(p-2)^{p-1} + \ldots + (-1)^{p-2}\binom{p-1}{p-2}.$$

Taking congruences mod p and applying Fermat's theorem we obtain

$$\begin{aligned}(p-1)! &\equiv 1 - \binom{p-1}{1} + \binom{p-1}{2} + \ldots + (-1)^{p-2}\binom{p-1}{p-2} \\ &\equiv (1-1)^{p-1} - 1 \equiv -1 \bmod p.\end{aligned}$$

This is, of course, Wilson's theorem, and the method of using formula (10) is well known, but the standard methods of obtaining formula (10) are different from the method employed here and do not generalize to formula (13). We prefer to write Wilson's theorem as follows:

$$(16) \qquad (p - r - 1)! \equiv \frac{(-1)^{r+1}}{r!} \bmod p, \ (r = 0, 1, 2, \ldots p-2).$$

If now in (10) we put $m = p - 2$ where p is an odd prime we obtain

$$(p-2)! = (p-2)^{p-2} - \binom{p-2}{1}(p-3)^{p-2} + \binom{p-2}{2}(p-4)^{p-2} + \ldots + \binom{p-2}{p-3}.$$

Again applying Fermat's theorem to the right side of this equation and formula (16) to the left we obtain

$$1 \equiv \frac{1}{p-2} - \binom{p-1}{1}\frac{1}{p-3} + \binom{p-2}{2}\frac{1}{p-4} + \ldots + \binom{p-2}{p-3} \bmod p.$$

https://doi.org/10.4153/CJM-1949-030-4 Published online by Cambridge University Press

The right-hand side of this congruence is precisely

$$-\int_0^1 \left\{\frac{(1-x)^{p-2}-1}{x}\right\} dx. \quad \text{Hence,} \int_0^1 \left\{\frac{(1-x)^{p-2}-1}{x}\right\} dx \equiv -1 \bmod p$$

for all odd primes p. In the same way if we replace m by $p-3$ in (10) we obtain

$$\int_0^1 \frac{dt}{t} \int_0^t \left\{\frac{(1-x)^{p-3}-1}{x}\right\} dx \equiv -\frac{1}{2} \bmod p \text{ for all primes } p \geq 5.$$

A few other particular cases have been worked out. For example, formula (11) with $m = p-3$ yields

$$\int_0^1 \left\{\frac{(1-x)^{p-3}-1}{x}\right\} dx \equiv -\frac{3}{2} \bmod p \text{ for all primes } p \geq 3.$$

Again formula (12) with $m = p-4$ yields $\int_0^1 \left\{\frac{(1-x)^{p-4}-1}{x}\right\} dx \equiv -\frac{11}{6}$ mod p for all primes $p \geq 5$. If in (13) we put $m = p-k-2$ and then $k = r-2$ we obtain in the same way the more general formula

$$(17) \qquad (-1)^{p-r}P_{r-2}(-r) \equiv \int_0^1 \left\{\frac{(1-x)^{p-r}-1}{x}\right\} dx \bmod p.$$

The left side of this formula is a rational number, which when expressed in its lowest terms, has a denominator with no prime factor greater than $2r-5$. Hence formula (17) is valid at least for all primes p which are greater than $2r-5$. (The case $k = 1$, corresponding to $r = 3$, is an exception.)

We now come to the most general case. In (13) put $m = p-k-r$, obtaining

$$(18) \quad (p-r)!\,P_k(p-k-r) = (p-k-r)^{p-r} - \binom{p-k-r}{1}(p-k-r-1)^{p-r} + \dots + (-1)^{p-k-r-1}\binom{p-k-r}{p-k-r-1}.$$

Taking congruences mod p and using (16) and Fermat's theorem we obtain

$$(19) \quad \frac{(-1)^r}{(r-1)!}P_k(-k-r) \equiv \frac{1}{(p-k-r)^{r-1}} - \binom{p-k-r}{1}\frac{1}{(p-k-r-1)^{r-1}} + \dots + (-1)^{p-k-r-1}\binom{p-k-r}{p-k-r-1}.$$

The right side of this congruence is equal to

$$(-1)^{p-k-r}\int_0^1 \frac{dx_{r-1}}{x_{r-1}} \cdots \int_0^{x_3} \frac{dx_2}{x_2} \int_0^{x_2} \left\{\frac{(1-x_1)^{p-k-r}-1}{x_1}\right\} dx_1.$$

https://doi.org/10.4153/CJM-1949-030-4 Published online by Cambridge University Press

Hence,

$$\frac{(-1)^r}{(r-1)!} P_k(-k-r)$$
$$\equiv (-1)^{p-k-r} \int_0^1 \frac{dx_{r-1}}{x_{r-1}} \cdots \int_0^{x_3} \frac{dx_2}{x_2} \int_0^{x_2} \left\{ \frac{(1-x_1)^{p-k-r}-1}{x_1} \right\} dx_1 \bmod p.$$

If we put $r - 1 = s$ and $(k + r) = t$ in this equation we obtain

(20) $$\frac{(-1)^{s-t}}{s!} P_{t-s-1}(-t)$$
$$\equiv \int_0^1 \frac{dx_s}{x_s} \cdots \int_0^{x_3} \frac{dx_2}{x_2} \int_0^{x_2} \left\{ \frac{(1-x_1)^{p-t}-1}{x_1} \right\} dx_1 \bmod p.$$

If we write this in the form

(21) $$\int_0^1 \frac{dx_s}{x_s} \cdots \int_0^{x_3} \frac{dx_2}{x_2} \int_0^{x_2} \left\{ \frac{(1-x_1)^{p-t}-1}{x_1} \right\} dx_1 \equiv R(s, t) \bmod p$$

we have

$$R(s, t) = \frac{(-1)^{s-t}}{s!} P_{t-s-1}(-t).$$

This equation is valid for every odd prime p greater than the maximum of s and $2t - 2s - 3$. This condition is put on to ensure that $R(s, t)$ will not have denominators divisible by p. It is also necessary to have $t \geq s + 1$ for our expression for $R(s, t)$ to be meaningful.

Our final result may be stated as follows. Let s and t be two positive integers such that $t \geq s + 1$. There exists a rational number $R(s, t)$ such that (21) is valid for all primes $p \geq \max(s, 2t - 2s - 3)$. Also the number $R(s, t)$ is uniquely determined, since, if $T(s, t)$ were another number for which equation (21) is valid for all primes $p \geq$ some number p_0, then $R(s, t) \equiv T(s, t) \bmod p$ for all primes $p \geq$ some integer p_1. Putting $R(s, t) = \frac{a}{b}$ and $T(s, t) = \frac{c}{d}$, we have $ad \equiv bc \bmod p$, for all primes $p \geq \max(p_1, bd)$. Hence $ad = bc$ or $R(s, t) = T(s, t)$.

References

[1] H. Geirenger, *Ann. Math. Statist.*, vol. 9 (1938), 262.

[2] I. Kaplansky, "On a Generalization of the 'Problème des Rencontres'," *Amer. Math. Monthly*, vol. 46 (1939), 159-161.

[3] I. Kaplansky, "Symbolic Solution of Certain Problems in Permutations," *Bull. Amer. Math. Soc.*, vol. 50 (1944), 906-914.

[4] N. S. Mendelsohn, "Symbolic Solution of Card Matching Problems," *Bull. Amer. Math. Soc.*, vol. 52 (1946), 918-924.

University of Manitoba