THE SYMBOLIC COMPUTATION OF FUNCTIONS
OF SEQUENCES OVER FINITE ALPHABETS WITH
GIVEN TRANSITION PROBABILITIES BY
SEQUENCE LENGTH INDEPENDENT ALGORITHMS

by

D. M. Jackson
E. Horowitz

Technical Report
No. 71-100
June 1971

Department of Computer Science
Cornell University
Ithaca, New York 14850
THE SYMBOLIC COMPUTATION OF FUNCTIONS OF SEQUENCES OVER FINITE ALPHABETS WITH GIVEN TRANSITION PROBABILITIES BY SEQUENCE LENGTH INDEPENDENT METHODS

Section

1 Introduction 1
2 The general problem 5
3 Analysis for a class of distance functions 10
4 Recurrence relations and methods of expansion 18
5 Results and Summary 26

Acknowledgements

References

Appendices

I Notation and Convention

II List of basis functions $v_4(n,p)$ for the 3-variable problem with $c(4) \leq 4$
Abstract

A special case of the problem discussed in this paper occurs in connection with non-statistical classification and is introduced from this point of view. The special case concerns the computation of expectations of statistical functions of the "distance" between pairs of fixed length sequences over a binary alphabet with given a priori state transition probabilities. The general problem involves an extension to alphabets of arbitrary order and the comparison of an arbitrary number of fixed length sequences. Given a set of sequences, it is shown that for a large class of functions exact computation may be carried out by an algorithm whose computation time is independent of the length of the sequences. It is further shown that results for all functions of this class may be derived from a small number of basis functions. Two methods for computing basis functions are given. Basis functions for the commonly encountered special case involving pairs of binary sequences are given explicitly.
1. Introduction

The work presented here was motivated by a problem occurring in non-statistical classification. Accordingly, a brief description of the problem is now given.

Non-statistical classification deals with the construction of classifications of populations of objects when an adequate statistical model for the population is not known (Good [1], Nagy [2], Friedman & Rubin [3], Zadeh [4], Cover & Hart [5], Cover [6], inter al.). The objective of classification in this case is to obtain a decomposition of the population which will reveal its structure, and to suggest further models for a more sophisticated treatment of the material. The role of such techniques in applications to taxonomy, for example, is described in detail by Sokal and Sneath [7].

In a typical situation the objects of a population are characterized by a set of vectors whose components specify the value or state of a continuous or discrete attribute. The vectors are of fixed length, the latter being the number of attributes which are measured or observed. A classification algorithm develops classes of objects which are similar to each other and yet well-differentiated from members of other classes. Similarity may be regarded as a distance function on the attribute space.

An acceptable classification must be stable with respect to small changes in the characterizations of the objects since instability of a classification indicates, in the first instance,
that the objects of the population have been inadequately characterized. Thus, we necessarily require that the classification not be grossly affected by occasional errors in the measuring or recording of the states of the attributes in the objects.

The effect of errors in the object characterizations is to introduce an "uncertainty" into the exact computation of the distance between pairs of objects. The estimation of these uncertainties for all pairs of objects of the population is of value in determining the stability of classifications generated by the class of algorithms which utilize a matrix of inter-object distances.

The purpose of this paper is twofold. First, to determine exactly in an analytic form the expectations of statistical functions of the distance between pairs of objects when observations on discrete attributes are susceptible to error independently. This includes the computation of the uncertainties in distance as a special case. Second, to determine, in a form convenient for subsequent numerical computation, explicit expressions for the expectations of statistical functions for the important special case concerning pairs of sequences over the binary alphabet (0,1). Expressions will be derived for arbitrary state transition probabilities so that specialization to a particular case, for example equiprobability of error, is immediate.
The computation of these quantities is generally avoided because of the extreme combinatorial nature of the problem. The problem is particularly acute when the number of attributes is too small to derive sufficiently accurate approximations using the central limit theorem. In this paper it is shown that, for a reasonably broad class of distance functions which includes the Hamming distance function, the computing time for determining expectations of statistical functions of distance can be carried out very fast. More precisely, if the distance function is representable as a multivariate polynomial then the dependence of computation time on the number of attributes is reduced from polynomial to constant. Moreover, each expectation is expressible in terms of a small number of basis functions. Since the latter are multivariate polynomials in the a priori transition probability matrix and the arguments of the distance functions, the determination for different error models or for different pairs of objects is reduced to direct polynomial evaluation. For reference purposes, the algebraic forms of these basis functions are given in Appendix II for the commonly encountered special case involving pairs of fixed length sequences over the binary alphabet. The reductions obtained here are sufficiently substantive to enable these functions to be computed manually with relative ease, whereas previously it was unfeasible to calculate them at all.

The ability to perform by computer complex algebraic manipulations has been important in the development of the work. The SAC-1 system (Horowitz [8]) is designed specifically for
performing a broad class of operations on multivariate polynomials
and rational functions. Although explicit mention of the use
of SAC-1 is not given in the remainder of the paper, it must be
stated that the empirical results obtained with its use have led
to a number of the theorems in Sections 3 and 4.

Section 2 contains a definition of the general problem,
a special case of which is the comparison of pairs of binary
sequences. The computational order of an algorithm for solving
the problem is determined and is found to be polynomial in the
length of the sequences. Section 3 shows that the computational
order of the process is independent of the length of the sequences
for a class of distance functions which includes Hamming distance.
In addition it is shown that a solution of the problem may be
given in terms of the moments and covariances of the error
distribution and that these may be reduced to multivariate
polynomials in the arguments of the distance function and the a
priori state transition probability matrix. Section 4 gives
a number of recurrence relations for reducing the computation
time further. A characterization of the moments and covariance
of arbitrary order is given in terms of the basis functions.
Examples of the application of these recurrence relations are
given in Section 5, together with an explanation of the basis
functions of Appendix II.
2. The General Problem

The general problem may be characterized as follows. Suppose that \( \mathcal{U} \) is a given set of sequences of length \( N \) composed of symbols from an alphabet \( \mathcal{A} \) of order \( k \), and that \( \mathcal{W} \) is an arbitrary subset of \( \mathcal{U} \) of given cardinality \( w \). \( \Lambda = \{ u_i \} \) is a given partition, into \( \lambda \) parts, of the set \( \mathcal{U} \equiv \{ x_i \} \) of all ordered sequences of length \( w \) composed of symbols from \( \mathcal{A} \). \( n = u(W) \) is a vector whose \( i \)-th component gives the number of symbol positions, \( j \), in which the ordered sequence of \( j \)-th symbols, taken one from each of the sequences of \( \mathcal{W} \) in order, belong to \( u_i \). \( f(n) \) is a given real valued function (distance function) of \( n \) and \( \phi \) is a statistical function of \( f \). \( \phi \) is a \( \lambda \) dimensional array, giving the expectations of \( \phi \) for all subsets of \( \mathcal{U} \) of cardinality \( w \), when the symbols of the sequences are susceptible to error independently with given a priori probabilities.

For brevity we shall refer to the construction of \( \phi \) as the \( (w,k,N) \) - problem, since these variables characterize the problem. The \( (w,k,N) \)-problem has \( \lambda \) variables, so when the number of variables is of consequence we shall refer to the \( (w,k,N) \)-problem alternatively as the \( \lambda \)-variable problem.

In practice, the \( (2,2,N) \)-problem, involving the comparison of pairs of binary sequences is the most frequently encountered. The problem arises in a variety of circumstances. Message transmission in discrete noisy channels, matching problem
(Barton [9]) in which the matches may be incorrectly recognized and applications of nonstatistical classification (Jackson [10]) are examples.

To simplify the subsequent analysis, a convention is adopted for abbreviating power products, products of multinomial coefficients and products of summation operators. The convention is summarized in Appendix I.

To examine the combinatorial aspects of the general problem, we begin by considering the matrix $\mathcal{H}$, where $H_{ij} = \text{Prob}(a_i | a_j)$, denoting the given a priori transition probabilities between the symbols $a_i$ and $a_j$ of the alphabet $\mathcal{A}$. If $x^{(p)}$ and $x^{(q)}$ are two arbitrary $w$-tuples of $\mathcal{X}$ whose $i$-th symbols are $x_i^{(p)}$ and $x_i^{(q)}$ respectively, and if $H^{(0)}$ is the transition probability matrix for pairs of $w$-tuples in $\mathcal{X}$ then:

$$H_{pq}^{(0)} = \text{Prob}(x^{(p)} | x^{(q)}) = \prod_{i=1}^{k} \text{Prob}(x_i^{(p)} | x_i^{(q)})$$

(2.1)

Let $H^{(A)}$ be the $\lambda \times \lambda$ transition probability matrix for pairs of parts $u_i, u_j$ of the partition $\Lambda$. Then:

$$H_{ij}^{(A)} = \text{Prob}(u_i | u_j) = \frac{1}{|u_j|} \sum_{(x^{(p)}, x^{(q)}) \in u_i \times u_j} H_{pq}^{(0)}$$

(2.2)

For brevity, the matrix $H^{(A)}$ will be denoted by $P$. $P$ is
column stochastic,

\[ \mathbf{P}(\mathbf{p}) = \mathbf{1} \]  \hspace{1cm} (2.3)

where \( \mathbf{1} \) is the vector with \( \lambda \) components, each of which is equal to one. Since the errors occur independently, it follows that the expectation of \( \phi(f) \) is given by

\[ \phi^*(\mathbf{m}) = \sum_{\{ \mathbf{i}, \mathbf{j} \}} \left[ \frac{\mathbf{n}}{\mathbf{p}} \right] \cdot \mathbf{f}^\mathbf{i} \cdot \psi(\mathbf{m}, \mathbf{n}) \]  \hspace{1cm} (2.4)

where \( \mathbf{i} = \sigma(\mathbf{j}) \) \hspace{1cm} (ii) \hspace{1cm} \psi(\mathbf{m}, \mathbf{n}) = \phi(f(\mathbf{m}), f(\mathbf{n})) \hspace{1cm} \), and \( \text{iii) } \)
\( \mathbf{I} \) is a \( \lambda \times \lambda \) matrix with non-negative integer elements giving the number of transitions from \( u_j \) to \( u_i \). The error matrix is accordingly given by \( \{ \phi^*(\mathbf{m}) | \sigma(\mathbf{n}) = N \} \) and is denoted by \( \phi \). Since the \((w,k,N)\)-problem is a \( \lambda \) variable problem and the matrices \( \mathbf{I} \) are \( \lambda \times \lambda \), then the number of matrices \( \mathbf{I} \) whose elements sum to \( N \) is \( \gamma^{N+\lambda^2-1} \). The computation of \( \phi \) by (2.4) is therefore \( O(N^{\lambda^2-1}) \).

To illustrate the use of a partition \( A \) we shall consider the \((2,2,N)\)-problem with the additional conditions that errors occur equiprobably with probability \( r \), and that the distance function is independent of the order in which the sequences \( A \) and \( B \) are compared. Accordingly, for equiprobability of errors:

\[ \mathbf{H} = \begin{bmatrix} s & r \\ r & s \end{bmatrix} \text{ where } s = 1 - r. \]
Since pairs of binary vectors are involved, the set $\mathcal{H}$ is given by

$$\mathcal{H} \equiv (x_1, x_2, x_3, x_4) \equiv ((0, 0), (0, 1), (1, 0), (1, 1)).$$

The symmetry requirement for the distance functions induces the partition $\Lambda$ on $\mathcal{H}$ given by:

$$\Lambda \equiv (u_1, u_2, u_3) \equiv ((x_1), (x_2, x_3), (x_4))$$

where $\lambda = 3$. It follows from (2.2) that

$$\mathbf{n}(\Lambda) = \begin{bmatrix} s^2 & rs & r^2 \\ 2rs & r^2 + s^2 & 2rs \\ r^2 & rs & s^2 \end{bmatrix}.$$

The time required for computing $\Phi$ for the $(2,2,N)$-problem is therefore $O(N^8)$. For the $(2,k,N)$-problem with a symmetrical distance function, computation time is $O\left(N^4 \frac{k^2 (k+1)^2 - 1}{2}ight)$. This increases exponentially with the order $k$ of the alphabet.

It has already been stated in Section 1 that sufficient reduction for a certain class of distance functions has been achieved by the techniques to be presented here. Indeed the $(2,2,N)$-problem will be reduced to a condition in which it may be solved manually with relative ease.

It has been shown (Jackson & White [11]) for all distance functions that the order of computation may be reduced provided
that each element of $\phi$ is required only to within a prescribed accuracy $\epsilon$. An upper estimate on the order of computation in this case is $N^2k_\epsilon^6$, where $k_\epsilon \ll 2N$ and $k_\epsilon$ is determined from $\epsilon$. Proofs of the convergence of the numerical method for the $(2,2,N)$-problem are given by Jackson & White [12]. Complete recomputation of $\phi$ is, however, necessary if the length $N$, of the sequences, the statistical function $\phi$, the distance function $f$ or the a priori transition probability matrix $H$ are changed. In practice it is commonly necessary to compute $\phi$ for a variety of $N$, $\phi$, $f$ and $H$. In Section 3 it is shown that repetition of the computation for changes in these quantities can be eradicated for a particular class of distance functions. In addition it is shown that the computation time for a single element of $\phi$ is independent of $N$ in this case.
3. **Analysis for a Class of Distance Functions**

Suppose that $\phi$ and $f$ have the property that $\phi(f)$ belong to the class of multivariate polynomials of degree $Q$ in $\lambda$ variables. Accordingly, $\psi(m,n)$ may be expressed in the form:

$$\psi(m,n) = \sum_{i} a_i(n) \cdot \bar{m}^i$$  \hspace{1cm} (3.1)

The values of $a_i(n)$ and the admissible values of $i$ are determinable from the given functions $\phi$ and $f$ by equating coefficients of $\bar{m}^i$. Each of the vectors $\bar{m}$, $m$, $n$ has $\lambda$ components, and $\sigma(\bar{1}) = Q$.

For the $(w,k,N)$-problem, the population $U$ is embedded in the attribute space of dimension $N$. $f$ is a generalized distance function on this space and is defined only at the lattice points since the attributes are discrete. For each ordered set of $w$ points of $U$ there corresponds a single point $n$ in the event space whose dimension is $\lambda - 1$. The mapping of subsets of cardinality $w$ in the attribute space to the lattice points of the event space is many-one. With each lattice point in the event space is associated a conditional probability distribution, $P(m|n)$, giving the probability of the event $m$ conditional on the event $n$.

Since $\phi^*(n) = E(\psi(m,n)|n)$ and $\psi(m,n)$ is a linear combination of the random variables $\bar{m}^i$, then:

$$\phi^*(n) = \sum_{i} a_i(n) \cdot B_i(n,P) \quad \hspace{1cm} (3.2)$$
where $B_{ij}(n,P)$ is identified as the $i$-th covariance, $E(m_i|n)$, of the distribution $P(m|n)$. The remainder of this section is concerned with determining the quantities $B_{ij}(n,P)$ for the $\lambda$ variable case, as multivariate polynomials in $n$ and $P$, and to provide practicable methods for their construction.

**Definition 3.1:** $G_{ij} = P_{ij} \frac{\partial}{\partial P_{ij}}$ where $\frac{\partial}{\partial P_{ij}}$ denotes formal partial differentiation with respect to $P_{ij}$ with the provision that $\{P_{ij}\}$ is treated as a set of independent variables.

The following theorem gives a simple form for $B_{ij}(n,P)$ in terms of the operator $G$. Since the elements of $P$ are treated as independent variables when they appear as operands of $G$, further reduction using the column stochastic property of $P$, namely $P(n) = 1$, is not permissible.

**Theorem 3.1:** If $B_{ij}(n,P)$ is the $i$-th covariance of the distribution $P(m|n)$, where $\sigma(m) = \sigma(n) = N$, then

$$B_{ij}(n,P) = (\sigma(m))^{j} (\sigma(n))^{m} n$$

**Proof:** Since $B_{ij}(n,P)$ is the $i$-th covariance then:

$$B_{ij}(n,P) = \sum_{m} m_{i} \cdot P(m|n)_{\sigma(m)=N}$$

Now from (2.4) the distribution is given by:
\[ P(m|n) = \binom{n}{i} \cdot p^i \text{ where } q(I) = m \text{ and } p(I) = n. \]

Thus, since \( m^i = (q(I))^i \), then substitution into the expression for \( B_A(n,p) \) yields:

\[ B_A(n,p) = \sum_{i=1}^{n} (q(I))^i P(m|n) \quad \text{for } p(I) = n \]

But from Definition 3.1 we have:

\[ q \cdot P(m|n) = I \cdot P(m|n) \]

whence

\[ B_A(n,p) = (q(q))^i \sum_{i=1}^{n} P(m|n) \quad \text{for } p(I) = n \]

\[ = (q(q))^i \cdot (q(p))^n \]

QED

An explicit multivariate polynomial expression for \( B_A(n,p) \) is now derived by utilizing the result of Theorem 3.1 and by applying each term of \( (q(q))^i \) to \( (q(p))^n \). The following lemma is used:

Lemma 3.1: If \( S(n) \) is a Stirling number of the second kind, then the following operator identity holds:
\[(x \frac{d}{dx})^n = \sum_{i=1}^{n} s^{(n)}_i x^i \frac{d^i}{dx^i} \quad n \neq 0.\]

**Proof:** See, for example, Riordan [13].

**Theorem 3.2 (Main theorem):** If \((n)_i = n(n-1)...(n-i+1)\)
(the falling factorial) then

\[B_{\lambda}(n, \mathbb{P}) = \sum_{\gamma} (n)_\gamma \cdot \mathbb{P}^\gamma \cdot C(\gamma, \lambda) \]

where \(\theta(x) = 0 \text{ if } x = 0, \text{ and } 1 \text{ otherwise (\(\theta\) operates component by component in the case of a vector)}\) and

\[C(\gamma, \lambda) = \sum_{\sigma} \left[ \begin{array}{c} 1 \\ \sigma \end{array} \right] s(\gamma) \quad \text{for } \sigma(\gamma) \leq \lambda \]

\[\begin{cases} \alpha(\sigma) = i \\ \alpha(\gamma) > \gamma \end{cases} \]

**Proof:** From Definition 3.1 and Lemma 3.1 we have:

\[G_{jk}^q = \sum_{i=0(q)} s(q)_i p_i \cdot p_j \cdot p_k, \quad C_{jk}^0 = 1.\]

Since the elements of \(\mathbb{P}\) are treated as independent variables when they appear as operands of \(G\) we have:

\[G_{jk}^q(\rho_k(\mathbb{P}))^p = \sum_{i=0(q)} s(q)_i p_i \cdot G_{jk}^q(\rho_k(\mathbb{P}))^{p-i} s(q) \]

\[B_{\lambda}(n, \mathbb{P}) = \sum_{\sigma} \left[ \begin{array}{c} 1 \\ \sigma \end{array} \right] s^{(n)}_\sigma \cdot \mathbb{P}^{\sigma(\mathbb{P})^n}. \]
When the operators of $G$ are assembled with each of the columns of $P$ to which they apply then:

$$B_A(n, P) = \sum \left[ \prod_{n=1}^{\lambda} \prod_{j=1}^{\sigma} \left( a_j^{A_j} \cdot \rho_j(P)^{n_j} \right) \right]_{a(q) = 1}$$

Application of the expansion for $G^q_{jk}$ yields:

$$B_A(n, P) = \sum \left[ \prod_{n=1}^{\lambda} \prod_{j=1}^{\sigma} \left( \frac{a_j}{a_j^n} \cdot \rho_j(P)^{n_j} \cdot \rho_j(Y)^{s_j} \cdot \frac{Y_j}{Y_j^n} \cdot \rho_j(P)^{n_j-P_j} \right) \right]_{a(q) = 1}$$

where $A$, $Y$ and $P$ are conformable matrices. Now, for an arbitrary function $g(x)$ the following identity holds:

$$\prod_{j=1}^{\lambda} \frac{b_j}{b_j} \cdot g(x_j) = \sum_{j=1}^{\lambda} \frac{b_j}{b_j} \cdot \left( \prod_{k=1}^{\lambda} g(x_k) \right)_{x_j = a_j, \ x_j = a_j}$$

Thus:

$$B_A(n, P) = \sum \left[ \prod_{n=1}^{\lambda} \prod_{j=1}^{\sigma} \left( \frac{a_j}{a_j^n} \cdot \rho_j(P)^{n_j} \cdot \rho_j(Y)^{s_j} \cdot \frac{Y_j}{Y_j^n} \cdot \rho_j(P)^{n_j-P_j} \right) \right]_{a(q) = 1}$$

which may be rewritten as

$$B_A(n, P) = \sum \left[ \prod_{n=1}^{\lambda} \prod_{y=1}^{\sigma} \left( \frac{a_j}{a_j^n} \cdot \rho_j(Y)^{s_j} \cdot \frac{Y_j}{Y_j^n} \cdot \rho_j(P)^{n_j-P_j} \right) \right]_{a(q) = 1}$$
Reversal of the order of summation and utilization of the column stochastic property of $P$, the latter step valid since the operator $C$ has been eliminated, yields:

$$B_A(n, P) = \sum_{\theta(A) \leq \sigma(Y) \leq i} (n) \sigma(Y) \cdot P_Y \cdot C(Y, A)$$

where the constants $C(Y, A)$ are defined above.

QED

Remark: It follows from Theorem 3.2 that the computation time for $B_A(n, P)$ is independent of $N$.

The computation time for determining the constants $C(Y, A)$ defined in Theorem 3.2 may be reduced by the simplification given in the following lemma.

Lemma 3.2: For the constants defined in Theorem 3.2 then:

$$C(Y, A) = \left[\frac{\sigma(Y)}{Y}\right]_\sigma \sigma(Y)$$

Proof: From Theorem 3.2 we have:

$$C(Y, A) = \sum_{\sigma \leq Y} \left[\frac{\sigma}{Y}\right]_\sigma \sigma(Y) \quad \text{for} \quad 0(Y) \leq A$$

Since the summations over the rows of $\sigma$ are independent (no column-binding in $\sigma$) then $C(Y, A)$ may be decomposed as follows:
\[ C(\gamma, \lambda) = \prod_{j=1}^{\lambda} C^*(j, \gamma, \lambda) \]

where \( C^*(\sigma, \rho) = \sum_{\sigma(\alpha) = \rho}^{\rho} \frac{\sigma(\alpha)}{\alpha} \) for \( \sigma(\alpha) \leq \rho \)

Now the generating function for Stirling numbers of the second kind, \( S_n^{(m)} \), is:

\[ (e^x - 1)^m = m! \sum_{n=m}^{\infty} S_n^{(m)} \frac{x^n}{n!}, \quad n \geq m \geq 1 \]

Now \( (e^x - 1)^\sigma = \prod_{i=1}^{\lambda} (e^x - 1)^{\alpha_i} \). Expanding both sides of this identity using the generating function, and equation coefficients of \( x^p \), we obtain:

\[ C^*(\sigma, \rho) = \sum_{\sigma(\alpha) = \rho}^{\rho} \frac{\sigma(\alpha)}{\alpha} \]

whence,

\[ C(\gamma, \lambda) = \sum_{\gamma(\alpha) = \lambda}^{\lambda} \frac{\gamma(\alpha)}{\alpha} \]

QED

The following corollary gives a simplified form of \( B_\lambda(n, \rho) \) as a multivariate polynomial in \( n \) and \( \rho \) with constants which may be determined directly by table look-up, rather than by computation. A convenient tabulation
of Stirling Numbers and Multinomial Coefficients is given
by Abramovitz and Segun [14].

**Corollary 3.1:** \( E_A(n, p) = \sum_{\sigma} (n)_{\sigma} (p)^{\sigma} \left[ \frac{\sigma(y)}{y} \right]_{\sigma} \)

**Proof:** Direct from Theorem 3.2 and Lemma 3.2.

An expression for the \( i \)-th moment of the distribution
\( P(m|n) \) can be derived directly by specialization of
Corollary 3.1. Denoting the \( i \)-th moment by
\( M_j^{(i)}(n, p) \) then:

\[
M_j^{(i)}(n, p) = \sum_{\sigma} (n)_{\sigma} \cdot j^{\sigma} \left[ \frac{\sigma(y)}{y} \right]_{\sigma} \left( \frac{\sigma(y)}{\sigma(y)} \right)
\]

Further specialization to the univariate case of a single
variable distributed binomially yields:

\[
m_s = \sum_{x=1}^{s} (n)_{x} p^{x} S_s^{(x)}
\]

which is an expression for the \( s \)-th moment derived by
Riordan [15].
4. Recurrence Relations and Methods of Expansion

A recurrence relation between the $B_1(n,p)$ is now derived with a view to decreasing the computational order of the problem yet further. The following definition is needed:

Definition 4.1:

i) The substitution convention $C(x)$ is defined by
   a) $C(x) : x^1 + (x)_1$; i.e. $(x^1)\big|C(x) = (x)_1$
   b) $C^{-1}(x) : (x)_1 + x^1$

ii) The simultaneous application of conventions $C(x)$ and $C(y)$ is denoted by $C(x,y)$ or $C(z)$ where 
    $z = (x,y)$

iii) The sequential application of conventions $C(x)$ and $C(y)$ from left to right is denoted by $C(x), C(y)$.

iv) Multiplication with respect to substitution convention $C(x)$ is denoted by $\times C(x)$. Let $g_1(x)$ and $g_2(x)$ 
    be two arbitrary functions of $x$. Then
    
    $g_1(x) \times C(x) g_2(x) = \left((g_1(x))\big|C^{-1}(x) \times (g_2(x))\big|C^{-1}(x)\right|C(x)$

v) The well-known pair of inverses (see Riordan [13]):
   
   a) $x^n = \sum_{i=1}^{n} s_1^{(n)}(x)_i$ where $s_1^{(n)}$ are Stirling numbers of the second kind;
   
   b) $(x)_n = \sum_{i=1}^{n} s_1^{(n)} x^i$ where $s_1^{(n)}$ are Stirling numbers of the first kind;
are algebraic devices for manipulating expressions into a form suitable for transformation under one of the conventions $C(x), C^{-1}(x)$.

Theorem 4.1 (Recurrence relations):

1) $B_\frac{1}{2}(m, p) = (p \cdot n) \frac{1}{2} \big| C^{-1}(p \cdot m), C(m)$

2) $B_{\frac{1}{2} + \frac{1}{2}}(n, p) = B_{\frac{1}{2}}(n, p) \times C^{-1}(p \cdot m), C(m)$

Proof: 1) From Corollary 3.1:

$$B_{\frac{1}{2}}(n, p) = \sum_{\{\theta(x) \leq \frac{1}{2} \leq 1\}} \sum_{\{\gamma(x) = 1\}} s(1) \sum_{\{\gamma(x) = 1\}} (n) \frac{1}{2} \bigg| p \gamma(x) \bigg| C(m)$$

Thus, from Definition 4.1(1)(a):

$$B_{\frac{1}{2}}(n, p) = \sum_{\{\theta(x) \leq \frac{1}{2} \leq 1\}} s(1) \sum_{\{\gamma(x) = 1\}} (n) \frac{1}{2} \bigg| p \gamma(x) \bigg| C(m)$$

$$= \sum_{\{\theta(x) \leq \frac{1}{2} \leq 1\}} s(1) (n) \frac{1}{2} \bigg| C^{-1}(p \cdot m), C(m)$$

$$= ((p \cdot n) \frac{1}{2}) \bigg| C^{-1}(p \cdot m), C(m)$$

2) From (i):

$$B_{\frac{1}{2} + \frac{1}{2}}(n, p) = ((p \cdot n) \frac{1}{2} \times (p \cdot n) \frac{1}{2}) \bigg| C^{-1}(p \cdot m), C(m)$$

$$= ((B_{\frac{1}{2}}(n, p)) \bigg| C(p \cdot n), C^{-1}(p \cdot m) \times (B_{\frac{1}{2}}(n, p)) \bigg| C(p \cdot n), C^{-1}(p \cdot m)) \bigg| C^{-1}(p \cdot m), C(m)$$
Thus from Definition 4.1(iv):

\[ B_{A+1}(n, P) = B_A(n, P) \times C^{-1}(P, n), C(n) B_1(n, P) \]

QED

The following theorem provides a means for computing \( B_A(n, P) \) by a set of recurrence relations derivable from Theorem 4.1.

**Theorem 4.2 (Recurrence relations):**

If \( \mathbf{q}^j = (0, 0, \ldots, 0, i_j, 0, \ldots, 0) \) (j-th component nonzero) where \( i_j \) is the j-th component of \( \mathbf{a} \), and if \( \mathbf{1}^j \) is a vector each of whose components is zero except the j-th which is one, then

1) \( B_A(n, P) = \prod_{j=1}^{\lambda} C(n) B_{Q^j}(n, P) \)

2) \( B_{Q^j}(n, P) = \sum_{k=1}^{i_j} s_k (i_j) (B_{1^j}(n, P)) | C(n) \)

**Proof:**

1) Consider the change of variable \( \prod_{q=1}^{\lambda} P^{pq} q = x_p \)

Then from Theorem 4.1(i) we have:
Thus, by repeated application of this result, and from Theorem 4.1(ii), we have

\[ B_{\lambda}(n,p) = \prod_{j=1}^{\lambda} C(n)^{i_j} \]

ii) From Theorem 4.1(i):

\[ B_{\lambda}(n,p) = \sum_{k=0}^{i_j} S_k(x_j)^k \]

It follows from Theorem 4.2 that each \( B_{\lambda}(n,p) \) may be computed from the set of polynomials \( \{ B_{i_j}^k(n,p) \} \); \( k = 1,2,\ldots, i_j \), \( j = 1,2,\ldots, \lambda \). These polynomials are exponentiated multilinear forms. Theorem 4.3 (Permutation theorem) will show that this
set may be reduced to \( B^k_{\Delta}(n, P) \); \( k = 1, 2, \ldots, \max(i_1, i_2, \ldots, i_\lambda) \) by suffix permutation. An example of the use of Theorem 4.2 is given in Section 5.

Another class of recurrence relations between the \( B_{\Delta}(n, P) \)'s may be derived by observing that some of the \( B_{\Delta}(n, P) \)'s may be obtained from others by permutation of suffixes. The results are incorporated into the following theorem.

**Theorem 4.3 (Permutation theorem):**

If \( \pi_\sigma \), \( \pi_\rho \) are row and column suffix permutations, respectively, for integers \( (1, 2, \ldots, \lambda) \) then:

1) \( B_{\pi_\sigma}(n, P) = B_{\Delta}(n, \pi_\sigma^{-1}(P)) \)

2) \( B_{\Delta}(n, P) = B_{\Delta}(\pi_\rho(n), \pi_\rho(P)) \)

**Proof:**

1) From Theorem 4.1(i):

\[
B_{\pi_\sigma}(n, P) = (P \cdot n)^{\pi_\sigma(n)} \begin{vmatrix}
C^{-1}(P \cdot n) \cdot (P) \\
C^{-1}(P \cdot n) \cdot (n)
\end{vmatrix}
= (P \cdot \pi_\sigma^{-1}(n))^{\pi_\sigma(n)} = B_{\pi_\sigma}(n, \pi_\sigma^{-1}(P))
\]

2) From Theorem 4.1(i):

\[
B_{\Delta}(n, P) = (P \cdot n)^{\Delta} \begin{vmatrix}
C^{-1}(P \cdot n) \cdot C(n) \\
C^{-1}(P \cdot n) \cdot C(n)
\end{vmatrix}
= (\pi_\rho(P) \cdot \pi_\rho(n))^{\Delta} = B_{\Delta}(\pi_\rho(n), \pi_\rho(P))
\]

QED
Theorem 4.3 is of importance in the computation of the $\mathcal{B}_1(n,P)$'s as a set of multivariate polynomials in $n$ and $P$.

Part (i) of the theorem has two consequences. First, it gives a rule for deriving $\mathcal{B}_1(n,P)$ from $\mathcal{B}_1(n,P)$ if $\mathcal{A}$ is a permutation of $\mathcal{A}$. Second, it provides a means of generating some of the terms of $\mathcal{B}_1(n,P)$ from other terms of $\mathcal{B}_1(n,P)$.

Part (ii) of the theorem also accomplishes the latter. The results are incorporated into Theorem 4.4 which may be regarded as an algorithm for determining $\mathcal{B}_1(n,P)$.

**Definition 4.2:** A basis function $\mathcal{W}_1(n,P)$ is a multivariate polynomial in $P$ and $n$ defined by:

1) $\mathcal{W}_1(n,P) = \sum_{\sigma(\gamma) = \mathcal{A}} \left[ \frac{\sigma(\gamma)}{\gamma} \right]_{\gamma} (n)_{\rho(\gamma)} \cdot P^\gamma$

   \[ \rho_1(\gamma) > \rho_2(\gamma) > \ldots > \rho_\lambda(\gamma) \]

2) If $\gamma$ and $\gamma'$ satisfy the summation conditions and if $\sigma(\gamma) = \sigma(\gamma')$ where $\gamma' = \pi_\sigma(\gamma)$ or if $\sigma(\gamma) = \sigma(\gamma')$ where $\gamma' = \pi_\rho(\gamma)$ then one of the matrices $\gamma, \gamma'$ is eliminated from the summation.

**Theorem 4.4:** Let $Q_\rho$ be the set of all column suffix permutations $\pi_\rho$, including the identity, for the integers $(1, 2, \ldots, \lambda)$.

Let $Q_\sigma^{(\dagger)}$ be the set of all row suffix permutations $\pi_\sigma$, including the identity, for the integers $(1, 2, \ldots, \lambda)$ with the
property that \( \sigma(\mathbf{i}) = 1 \). If \( i_1 \geq i_2 \geq \ldots \geq i_\lambda \), then

\[
B_{\lambda}(n, P) = \sum_{\mathbf{\sigma}, \mathbf{\rho}} B_{\lambda}(\pi_\mathbf{\sigma}(n), \pi_\mathbf{\rho}^{-1}(P))
\]

where \( B_{\lambda}(n, P) = \)

\[
\sum_{\mathbf{\sigma}, \mathbf{\rho}} \sum_{\lambda \leq \sigma(\mathbf{i}) \leq \lambda} \psi_{\lambda}(n, P)
\]

where \( \psi_{\lambda}(n, P) \) are basis functions, and * denotes summation over algebraically distinct forms.

**Proof:** The theorem follows from Corollary 3.1 and Theorem 4.3.

Theorems 4.3 and 4.4 enable all \( B_{\lambda}(n, P) \) with \( \sigma(\mathbf{i}) \leq Q \) to be computed from the set of basis functions \( \psi_{\lambda}(n, P) \) with \( j \leq i ; \ j_1 \geq j_2 \geq \ldots \geq j_\lambda ; \ i_1 \geq i_2 \geq \ldots \geq i_\lambda \) and \( \sigma(\mathbf{i}) \leq Q \).

The basis functions have the following property which is of importance in the extension to higher values of \( \lambda \).

**Theorem 4.5 (Extension theorem):**

If \( \psi_{\lambda}(n, P) \) is a basis function, then \( \psi_{\lambda}(n, P) \) is independent of \( \lambda \) if \( \lambda \geq \sigma(\mathbf{i}) \).

**Proof:** If \( \lambda \geq \sigma(\mathbf{i}) \), then a vector of length \( \lambda \) can accommodate any set of column sums which sum to a number.
less than or equal to $\lambda$. Addition of a row and column of zeroes to the matrix $\gamma$ (see Definition 4.2) does not affect the basis functions.
5. Results and Summary

The statements of Theorems 4.2 and 4.4 may be incorporated into two algorithms for computing the $B_{\lambda}(n,p)$'s as polynomials in $n$ and $p$. The two methods are illustrated below for the 3-variable problem with $\lambda = (2,1,0)$.

Method 1 (Based on Theorem 4.2):

From Theorem 4.2: $B_{210}(n,p) = B_{200}(n,p) \times C(n) \times B_{010}(n,p)$

Using the change of variable $x_1 = \sum_{j=1}^{3} p_{1j} n_j$ we have:

$B_{200}(n,p) = \left. (x_1^2 + x_1) \right| C(n)$

and

$B_{010}(n,p) = \left. x_2 \right| C(n)$

whence

$B_{210} = \left. (x_1^2 + x_1) x_2 \right| C(n)$

\[ = \left. \left( (P_{11} n_1 + P_{12} n_2 + P_{13} n_3)^2 + (P_{21} n_1 + P_{22} n_2 + P_{23} n_3) \right) \right| C(n) \times C(n_1 n_2 n_3) \]  

(5.1)

which can be expanded straightforwardly. The expansion of the resulting forms may be carried out by a polynomial manipulation system (Horowitz [op.cit.]). It is important to note that the application of $C(n)$ at the final stage implies that the variables $\{x_1\}$ may not be allowed to assume numerical values at the start of the computation, even if $p$ and $n$ are given.
Method 2 (Based on Theorem 4.4):

From Theorem 4.4: \[ B_{210}(n, P) = \sum_{\pi_{\rho} \in Q} (\Psi_{210}(\pi, P) + \Psi_{110}(\pi, P)) \]

The construction of \( \Psi_{210}(n, P) \) involves 4 matrices \( \gamma \), (see definition 4.2):

\[
\begin{array}{ccc}
\gamma & : & (1) \\
\begin{array}{ccc}
2 & . & . \\
1 & . & 1 \\
3 & . & .
\end{array} & \begin{array}{ccc}
2 & . & 2 \\
1 & 1 & 1 \\
1 & 1 & 1 \\
2 & 1 & 1
\end{array} & \begin{array}{ccc}
1 & 1 & 2 \\
1 & . & 1 \\
1 & 1 & 1 \\
1 & . & .
\end{array}
\end{array}
\]

\[
\left[ \sigma(\gamma) \right]_{\sigma} : (1)
\]

The construction of \( \Psi_{110}(n, P) \) involves 2 matrices \( \gamma \) (see definition 4.2):

\[
\begin{array}{ccc}
\gamma & : & (1) \\
\begin{array}{ccc}
1 & . & . \\
1 & . & 1 \\
2 & . & .
\end{array} & \begin{array}{ccc}
1 & . & 1 \\
1 & . & 1 \\
1 & 1 & 1
\end{array}
\end{array}
\]

\[
\left[ \sigma(\gamma) \right]_{\gamma} : (1)
\]
Thus

\[ V_{210}(n, P) = (n_1)^2 P_{11}^2 P_{21} + (n_1)^2 P_{11} P_{21} + 2(n_1)^2 P_{12} P_{12} P_{21} \] (5.2)

\[ + 2(n_1)^2 P_{11}^2 + (n_1)^1 (n_2)^1 P_{12} P_{13} P_{21} \]

\[ V_{110}(n, P) = (n_1)^2 P_{11} P_{21} + (n_1)^1 (n_2)^1 P_{11} P_{22} \]

Each term of these polynomials is generated by one of the matrices. The factorization in (5.2) may be carried out by constructing all matrices with the same column sums, for given row sums.

The expansion of (5.2) to the full form of \( B_{210}(n, P) \) is simpler than the expansion of (5.1) to \( B_{11}(n, P) \) since the former involves only suffix permutation while the latter involves multivariate expansion. However, Method 2 relies on an efficient technique for constructing feasible matrices of the type given in Definition 4.2. The method is of particular value in deriving polynomials for the \( \lambda + 1 \) variable problem from those of the \( \lambda \) variable problem by means of Theorem 4.5 (Extension theorem).

The polynomials given in Appendix II may be used in an important special case of the \((w, k, N)\)-problem, namely that of determining the expectations \( \phi^* \) of statistical functions \( \phi \) of the distance function \( f \) for pairs of binary sequences of fixed length when the digits are susceptible to error with given probability. It has been seen that this is a 3-variable problem. Appendix II contains the basis functions for computing the expectations for all \( i \) with \( \sigma(i) \leq 4 \). Extension to higher \( \sigma(i) \) has not been given for the sake of brevity. The
probability matrix $P$ for the problem is determined from the
given a priori state transition probability matrix by (2.2).
For an arbitrary pair of sequences, it has been proved as a
special case of Theorem 3.2, that the time taken to determine
the expectations of $\phi(f)$ is independent of the length of the
sequences. This has made the computation of these expectations
an entirely feasible proposition.

The basis functions in Appendix II were generated by hand
using Method 2 since only 39 matrices were involved. The main
expression for $B_\lambda(n,P)$, given in Corollary 3.1, was then
implemented with the aid of the SAC-1 system to provide a check
on these results. The time taken to compute and print
$B_\lambda(n,P)$ for the ten different vectors $\lambda$ given in Appendix II
was 57 seconds. This gave the $B_\lambda(n,P)$ as multivariate
polynomials in $n$ and $P$, both for arbitrary $P$ and for $P$
determined under the assumption of equiprobability of error.
The abbreviation obtained by presenting the $B_\lambda(n,P)$ in terms
of the basis functions $\Psi_\lambda(n,P)$ is particularly striking.

The technique used in generating the polynomials of
Appendix II may be used for the general $(w,k,N)$-problem.

In the comparison of Method 1 and Method 2 the former is
the more readily programmable since the method contains little
more than polynomial exponentiation and since languages are
available which permit polynomial manipulation. The SAC-1
system is one such system. However, the data structure representation of polynomials in this system, and others, is such that all variables of a product must appear in each term of that product. The data structure for the product of two sparse polynomials contains a high proportion of zero exponents and zero coefficients. Although the polynomials \( B_j(n, p) \) (See Theorem 4.2(ii)), are not sparse their product (see Theorem 4.2(i)) is since these polynomials involve differing sets of variables. Accordingly, Method 1 is expensive on core storage requirements, particularly as the components of \( \lambda \) increase in value or as \( \lambda \) increases.

Method 2 avoids the core store problems encountered in Method 1 by enabling the construction of \( B_4(n, p) \) to be carried out term by term. This requires only a nominal amount of core storage. This method requires, however, that matrices satisfying Definition 4.2(ii) must be constructed by an efficient algorithm. Although the total time for the computation of the polynomials of Appendix II was exceedingly small since the number of matrices was small, the computing time does become an important issue larger values of \( \lambda \) and for larger values of the components of \( \lambda \). The efficient generation of matrices satisfying the conditions of Definition 4.2(i) and (ii) is being investigated.

Acknowledgements

The authors thank Mr. S. K. Sahni and Mr. J.K. Wong of the Department of Computer Science, Cornell University, for their participation in this work. The work was supported by National Science Foundation Grant GN-27224.
References


8. Eorowitz, E. User notes for the SAC-1 system at Cornell University, Department of Computer Science, Cornell University, Ithaca, New York.


Appendix I

Notation and Conventions

1. Vectors and matrices are underscored by and , respectively.

2. The elements of all vectors and matrices, with the exception of those which are probabilistic, are non-negative integers.

3. It will be assumed throughout the text that the sizes of the vectors and matrices are such that the expressions in which they occur are well defined. Under this assumption, explicit discussion of the sizes of vectors and matrices is largely avoided.

4. Inequalities between vectors operate componentwise; e.g., for , where and have components.

5. Rows and Columns of matrices:
   1) are the th row and th column, respectively, of the matrix .
   2) are row sums of .
   3) are column sums of .

6. Implied Products:
   1) For vectors and matrices
      1) 
      2) 

2) For operators:
\[ \prod_{i=a}^{b} \prod_{p,q}^{pq} \]

3) For multinomials:

1) \[ \prod_{i=M}^{j=1} \left[ \begin{array}{c} i \\ j \end{array} \right] = \frac{i!}{M_j!M_{j2}!...M_{jk}!} \]

\[ \text{where } \left[ \begin{array}{c} i \\ j \end{array} \right] = \frac{i!}{M_j!M_{j2}!...M_{jk}!} \]

2) \[ \prod_{i=M}^{j=1} \left[ \begin{array}{c} i \\ j \end{array} \right] = \frac{i!}{M_{j1}!M_{j2}!...M_{jk}!} \]

\[ \text{where } \left[ \begin{array}{c} i \\ j \end{array} \right] = \frac{i!}{M_{j1}!M_{j2}!...M_{jk}!} \]

4) For Stirling numbers:

1) \[ s_{(i)}^{(j)} = \prod_{k} s_{i_k}^{(j_k)} \]

2) \[ s_{(i)}^{(j)} = \prod_{i,j} s_{i_j}^{(j_i)} \]

5) For falling factorials:

\[ (n)_{(i)} = \prod_{j=1}^{n} (n_j)_{i_j} \]
Appendix II

List of basis functions \( \psi_i(n, P) \) for the 3-variable problem

with \( \sigma(i) \leq 4 \)

a) If \( \phi(f(n), f(m)) = \sum \alpha_i(n) \cdot m^i \) (see (3.1))

then \( E(\phi(f(n), f(m))) = \sum \beta_i(n) \cdot B_i(n, P) \) (see (3.2))

Case 1: \( i_1 \geq i_2 \geq \ldots \geq i_\lambda \).

Then \( B_i(n, P) = \sum \{ \beta_i^{p, q}(n, P) \} \) (see Theorem 4

\( \pi_{e q}, \pi_{e p} \in C_\sigma(\pi_{e q}) \pi_{e p} \in C_\rho(\pi_{e p}) \)

Case 2: For the remaining \( i \)'s, excluded from case 1, we may use:

\( B_{\pi_{e q}}(n, P) = B_{\pi_{e q}}(n, P) \) (see Theorem 4

b) The quantities \( \psi_i(n, P) \) are linear functions of the basis functions as follows: (The arguments of \( \psi_i(n, P) \) are suppressed for brevity)

\[
\begin{align*}
\psi_{100} &= \psi_{100} \\
\psi_{200} &= \psi_{200} + \psi_{100} \\
\psi_{300} &= \psi_{300} + 3\psi_{200} + \psi_{100} \\
\psi_{400} &= \psi_{400} + 6\psi_{300} + 7\psi_{200} + \psi_{100}
\end{align*}
\]
(c) The basis functions $\psi_1(n, p)$ are as follows: (The arguments of $\psi_1(n, p)$ are suppressed for brevity).

\[ \psi_{100} = (n_1)^0_p^1 \]
\[ \psi_{200} = (n_1)^2_p^1 + 2(n_1)(n_2)^1_p^1 \]
\[ \psi_{300} = (n_1)^3_p^1 + 3(n_1)(n_2)^2_p^1 + 6(n_1)(n_2)(n_3)^1_p^1 \]
\[ \psi_{400} = (n_1)^4_p^1 + 4(n_1)(n_2)^3_p^1 + 6(n_1)(n_2)(n_3)^2_p^1 + 12(n_1)(n_2)(n_3)^1_p^1 + 12(n_1)(n_2)(n_3)^1_p^1 \]

\[ \psi_{110} = (n_1)^2_p^1(n_2)^1 \]
\[ \psi_{210} = (n_1)^3_p^1 + (n_2)^2_p^1 \]
\[ \psi_{220} = (n_1)^4_p^1 + 2(n_2)^2_p^1 \]
\[ \psi_{310} = (n_1)^4_p^1(n_2)^1 \]

...
\[ w_{111} = (n_1)^3 p_{11}^1 p_{21}^1 p_{31} + (n_1)^2 (n_2)^1 p_{11}^1 p_{21}^1 p_{32} + (n_1)^1 (n_2)^1 (n_3)^1 p_{11}^1 p_{22}^2 p_{33} \]

\[ w_{211} = (n_1)^4 p_{11}^2 p_{21}^1 p_{31} + (n_1)^3 (n_2)^1 (n_3)^1 (p_{11}^2 p_{21}^1 p_{32} + 2 p_{11}^1 p_{12}^1 p_{21}^1 p_{31}) + (n_1)^2 (n_2)^1 (n_3)^1 (p_{11}^1 p_{22}^1 p_{33} + 2 p_{11}^1 p_{12}^1 p_{21}^1 p_{33} + 2 p_{12}^1 p_{13}^1 p_{21}^1 p_{31}) + (n_1)^1 (n_2)^2 (n_3)^1 (p_{11}^2 p_{22}^2 p_{32} + 2 p_{11}^1 p_{12}^1 p_{21}^1 p_{32}) \]