2005

Multinomial Representation of Majority Logic Coding

John B. Moore  
*Australian National University*

Keng T. Tan  
*Edith Cowan University*

10.1109/ISIT.2005.1523368


© 2005 IEEE. Personal use of this material is permitted. Permission from IEEE must be obtained for all other uses, in any current or future media, including reprinting/republishing this material for advertising or promotional purposes, creating new collective works, for resale or redistribution to servers or lists, or reuse of any copyrighted component of this work in other works.

This Conference Proceeding is posted at Research Online.

https://ro.ecu.edu.au/ecuworks/2757
Multinomial Representation of Majority Logic Coding

John B. Moore
Research School of Info. Sci. & Eng.
Australian National University
Canberra ACT 0200, Australia
Email: john.moore@anu.edu.au

Keng T. Tan
School of Computer and Information Science
Edith Cowan University
Mount Lawley WA 6050, Australia
Email: a.tan@ecu.edu.au

Abstract—Multinomial representations are derived for majority logic operations on bipolar binary data. The coefficients are given simply in terms of the readily computed lower Cholesky factor of Pascal matrices of order $n$ for codes of block length $n$.

I. INTRODUCTION

Majority voting on binary data is the basis of certain nonlinear block coding schemes in communication systems [1], especially in the case where, extremely low power radio wave communications is desired [2]. The majority logic operation is used in both the coding and decoding operations. Because of the nonlinearity of the operation, there is difficulty in predicting system performance, or seeing how to improve system performance. Our view is that a crucial tool in this task is a multinomial representation of the majority logic operation.

A multinomial expansion for majority logic has been partially studied in [3], [4], and the results applied in various communication contexts. General formulas for the first and last coefficients in the expansion are stated, and for bipolar binary vectors of length $n$, it is claimed that the even numbered coefficients are zero for $n$ even, but we know of no sources which give other coefficients.

Here, we give a complete theory for the multinomial representations of majority logic operations on bipolar binary data. The majority logic operation can be a classic $\text{sign}$ function of the sum of the binary data, as studied in the earlier literature known to us. Perhaps more usefully, we also give a theory for what we term here $\text{sign}_+$ functions. These are $\text{sign}$ operations where an output of 0 is replaced by $\pm 1$. The approach extends to other nonlinear functions of the sum of binary data, such as to sigmoidal functions used in artificial neural networks. It also extends to arbitrary nonlinear functions of bipolar binary data vectors that are invariant of the order of the data within the vector.

The coefficients of the multinomial expansion are linear in what we call a generalized Pascal matrix, which can be factored in terms of the lower triangular Cholesky factor, denoted here $P_n$, of a Pascal matrix of order $n$. The ‘new’ results are generalizations of the classical results. It would not be surprising if at least some of the results were known by Pascal, but the motivation for deriving them, or highlighting them, is coming from applications of nonlinear coding for next generation wireless communications.

In Section II, the new results on multinomial expansions of majority logic functions are derived. In Section III, these results are applied to majority logic based nonlinear block coding. Conclusions are drawn in Section VI.

II. THE PASCAL MATRIX AND A MULTINOMIAL EXPANSION

In this section, we introduce background material on classical results in order to set up notation for the main results of the following sections.

Our results concern nonlinear operations on a data $n$-vector $\mathbf{a} = [a_1, a_2, \ldots, a_n]^T$ with $a_i \in \{+1, -1\}$. Now any nonlinear function of $\mathbf{a}$ belongs to a finite discrete set of no more than $2^n$ elements. Indeed, such functions are linear in an indicator $2^n$-vector $\in \{e_1, e_2, \ldots, e_{2n}\}$, where $e_i$ is a zero $2^n$-vector save that the $i^{th}$ element is unity.

Our new results concern nonlinear operations that are invariant of any ordering in the data, such as functions of $\sum_{i=1}^{n} a_i$, $\prod_{i=1}^{n} a_i$, or of $\prod_{i=1}^{n} (1 + a_i)$. In this case, the functions belong to a discrete set of at most $n + 1$ elements.

Our focus is on (nonlinear) majority logic functions involving $\text{sign}$ operations on sums of partial products $a_i$, which map one-to-one to the data vector. The resulting representations are termed multinomial representations.

A. Multinomial representation for majority logic

1) Nonlinear functions and majority logic: Consider the $\text{sign}$ function definition.

$$\text{sign}(x) := \begin{cases} 1 & \text{if } x > 0 \\ 0 & \text{if } x = 0 \\ -1 & \text{if } x < 0 \end{cases} \quad (1)$$

Let us also introduce derivative definitions, denoted $\text{sign}_+$ and $\text{sign}_-$ as

$$\text{sign}_+(x) := \begin{cases} 1 & \text{if } x > 0 \\ \pm 1 & \text{if } x = 0 \\ -1 & \text{if } x < 0 \end{cases} \quad (2)$$

Consider now a set of $n$ bipolar binary digits $\{a_1, a_2, \ldots, a_n\}$, that is where $a_i \in \{+1, -1\}$. The majority logic operation on this $n$-block of data is simply $\text{sign}_+(\sum_{i=1}^{n} a_i)$, where we have used $\text{sign}_+$ to denote either $\text{sign}$, $\text{sign}_+$ or $\text{sign}_-$. The latter two options can be used
if the output of the logic operation is constrained to be also bipolar binary.

2) Multinomial representation: Early literature [3][4], presents a multinomial representation for the majority logic sign operation, which we here also mildly generalize as

\[ \text{sign}_* \left( \sum_{i=1}^{n} a_i \right) = \rho_0 + \rho_1 \sum_{i=1}^{n} a_i + \rho_2 \sum_{i>j} a_i a_j + \cdots + \rho_n \prod_{i=1}^{n} a_i, \] (3)

for suitable selections of coefficients \( \rho := [\rho_0, \rho_1, \ldots, \rho_n] \), which will depend on which of the sign operations is used. The selection of the coefficients and their properties is the study of this paper.

Of course, the expansion of the nonlinear function \( \prod_{i=1}^{n} (1 + a_i) \) has such an expansion as the right hand side of (3) with coefficients \( \rho = [1, 1, \ldots, 1] \). The mapping from the set \( \{a_i\} \) to the set of the sums of products in (3) via the coefficients of the \( \rho_i \) is known to be one to one. The earlier work has given specific formulas for the coefficients \( \rho_0, \rho_1, \ldots, \rho_n \) of (3) in terms of permutation operations \( n! C_i \equiv \frac{n!}{i! (n-i)!} \), at least for the case of the classic sign function. It is also noted in the early work that in this case \( \rho_i = 0 \) for \( n, i \) even, but other coefficients have not been studied to our knowledge.

In our applications of such expansions, it is important to have readily calculated coefficients for all the coefficients \( \rho_i \), and to see relationships between them in order to understand experimentally observed relationships in majority logic coding for communication systems.

In order to proceed, we first review relevant results of the Pascal matrix.

B. The lower Cholesky factor of the Pascal matrix

The well known (second) Pascal matrix, is a lower Cholesky factor of the original (first) Pascal matrix. We will refer to this (second) Pascal matrix simply as the Pascal matrix, and use the notation \( P_n = (p_{i,j}^n) \) for such an \( n \times n \) matrix. Its elements, for \( i, j = 1, 2, \ldots, n \), are defined in terms of the binomial coefficients, so that the \( i, j \) element for \( i \leq j \) is

\[
p_{i,j}^n = \begin{cases} (-1)^{j-i} (-1)^{i-1} C_{j-1} & \text{for } i < j, \\ (-1)^{j-i} (i-1)! (j-i)! & \text{for } i \geq j. \end{cases}
\]

The key property which we exploit subsequently is that \( P_n \) is involutory in that

\[ P_n = P_n^{-1}, \quad P_n P_n = I_n. \] (5)

III. MULTINOMIAL COEFFICIENTS

To lead into the derivations of our main results, consider the polynomials \((s-1)^i\) for \( i = 0, 1, 2, \ldots, n \) for some nonnegative integer \( n \) and scalar \( s \), organized as

\[
\begin{pmatrix}
(s-1)^0 s^0 \\
(s-1)^1 s^{n-1} \\
\vdots \\
(s-1)^n s^0
\end{pmatrix} = P_{n+1}
\]

Now consider the multinomial (3) for all possible polar binary sequences \( \{a_1, a_2, \ldots, a_n\} \). Clearly, the expansion is invariant of the ordering of the \( a_i \), so that there are only \( n+1 \) selections, namely where there are \( k = 0, 1, 2, \ldots, n \) values of \( a_i = 1 \), with correspondingly \( n-k, 0, 1, \ldots, n \) values of \( a_i = -1 \). Indeed the terms involving sums of products of the \( a_i \) in (3) are given, for each \( k = 0, 1, 2, \ldots, n \), as the coefficients of the expansion \((s-1)^k (s+1)^{n-k}\).

A. A generalized Pascal matrix

A useful generalization of (6) is then

\[
\begin{pmatrix}
(s-1)^0 (s+1)^n \\
(s-1)^1 (s+1)^{n-1} \\
\vdots \\
(s-1)^n (s+1)^0
\end{pmatrix} = R_{n+1}
\]

for some readily calculated \((n+1) \times (n+1)\) matrix \( R_{n+1} := (r_{i,j}^{s}) \) consisting of elements \( r_{i,j}^{s} \), and termed here a generalized Pascal matrix. In particular, the \( i \)th row of \( R_{n+1} \) consists of the sums of products of the \( a_i \) in (3), for \( k \) values of \( a_i = 1 \), with correspondingly \( n-k \) values of \( a_i = -1 \), and are the coefficients of the polynomial \((s-1)^k (s+1)^{n-k}\).

For reference, the cases for \( n = 1, 2 \) are spelt out as,

\[
R_2 = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}
\]

\[
R_3 = \begin{bmatrix} 1 & 2 & 1 \\ 1 & 0 & -1 \\ 1 & -2 & 1 \end{bmatrix}
\]

A recursive relationship between the elements of \( R_{k+1} \), and that of \( R_k \), being a generalization of Pascal’s equations, are given for \( k = 2, 3, 4, \ldots, n \), initialized by (8), as

\[
r_{i,j}^{k+1} := \begin{cases} 1, & \text{for } i = 1, 2, \ldots, k+1; \\ r_{i,j}^{k+1} := r_{i,j}^{k} + r_{i,j}^{k-1}, & \text{for } j = 2, 3, \ldots, k+1; \\ r_{k+1,j}^{k+1} := r_{k+1,j}^{k} - r_{k+1,j}^{k-1}, & \text{for } j = 2, 3, \ldots, k+1. \end{cases}
\]

This result is proved in a straightforward manner by induction, and is not spelt out here.

B. Coefficients via the generalized Pascal matrix

As already noted, the multinomial (3), for each possible \( a_1, a_2, \ldots, a_n \) selection, is invariant of the ordering of the \( a_i \), and there are then but \( n+1 \) possible multinomials. These can
then be organized as,

\[
s_n := \begin{bmatrix} \text{sign}_n(n) \\ \text{sign}_n(n-2) \\ \vdots \\ \text{sign}_n(n-n) \end{bmatrix} = R_{n+1} \begin{bmatrix} \rho_0 \\ \rho_1 \\ \vdots \\ \rho_n \end{bmatrix} = R_{n+1} \rho.
\]

(11)

This relationship means that the desired coefficients are the solutions of a linear equation as emphasized in the lemma.

**Lemma 3.1** The multinomial representation of the \( R_n \) function of (3) has coefficients \( \rho \) satisfying the linear equations (11), restated as,

\[
R_{n+1} \rho = s_n,
\]

(12)

where \( R_n \), the generalized Pascal matrix, is defined recursively in (8), and (10).

C. Inverse and decomposition of the generalized Pascal matrix

The nature of the inverse of \( R_{n+1} \) now assumes importance. We next develop our second main result, namely that \( R_n \) has a factorization in terms of the Pascal matrix \( P_n \), and inherits the involutory property to within a scaling. In particular, we claim,

**Lemma 3.2** The generalized Pascal matrix \( R_n \), as defined recursively in (8), and (10), has the scaled involutory property

\[
R_n^2 = 2^{n-1} I_n, \quad R_n^{-1} = 2^{1-n} R_n.
\]

(13)

Proof: This result follows by induction arguments. We work with matrices in lower triangular form. First define \( F_n \) as the matrix \( P_n \) flipped both left to right and top to bottom. In obvious notation, we write,

\[
F_n := \text{flip}(P_n), \quad \text{or } f_{i,j}^n = p_{n-i,n-j}^n.
\]

(14)

Also, define diagonal matrices, in obvious notation, as

\[
D_n := \text{diag}\{2^0, 2^1, 2^2, \ldots, 2^{n-1}\}, \quad S_n := \text{diag}(P_n).
\]

(15)

To proceed with the lemma proof, a decomposition lemma is now stated and proved.

**Lemma 3.3** The generalized Pascal matrix \( R_n \), as defined recursively in (8) and (10), has the decomposition in terms of triangular and diagonal matrices as

\[
R_n = 2^{n-1} S_n F_n D_n^{-1} P_n = P_n D_n F_n S_n.
\]

(16)

Proof: This lemma result follows by induction, which is relatively straightforward because only upper or lower triangular matrices are involved. Our approach is guided by keeping in mind the connection of the matrix elements with polynomial coefficients. Thus an equivalent result to (16) is to post-multiply \( R_n \) by the vector \([s^{n-1}s^{n-2} \ldots s^0] \) and apply both (6) and (7) so that,

\[
\begin{bmatrix}
(s-1)^0(s+1)^{n-1} \\
(s-1)^1(s+1)^{n-2} \\
\vdots \\
(s-1)^{n-1}(s+1)^0
\end{bmatrix} = P_n
\]

\[
\begin{bmatrix}
2^0(s+1)^n \\
2^1(s+1)^{n-1} \\
\vdots \\
(2s)^{n-2}(s+1)^1 \\
(2s)^{n-1}(s-1)^{n-1}
\end{bmatrix} = F_n
\]

These equations are now in a form that they can be verified by straightforward induction arguments. The pattern of the argument becomes clear in passing from \( n = 1 \) to \( n = 2 \), and \( n = 2 \) to \( n = 3 \), so that passing from \( n = 1 \) to \( n = 1 \) is then straightforward. It is necessary to exploit the Pascal equations which are inherent in the Pascal matrix \( P_n \) construction, and suitably adjusted for the ‘flipped’ version \( F_n \). Further details are omitted.

□

Proof: (Continuation of Proof for Lemma III.2) The proof of (13) follows from (16) by substitution and noting in turn that \( S_n, P_n, F_n \) are each readily verified as involutory. Thus,

\[
(R_n)(R_n) = (P_n D_n F_n S_n)(2^{n-1} S_n F_n D_n^{-1} P_n),
\]

\[
= 2^{n-1} P_n D_n F_n D_n^{-1} P_n,
\]

\[
= 2^{n-1} P_n D_n^{-1} P_n,
\]

\[
= 2^{n-1} P_n P_n
\]

\[
= 2^{n-1} I_n.
\]

□

D. Coefficients from columns of the generalized Pascal matrix

The above Lemmas 3.1, 3.2 together give our main result stated as a theorem.

**Theorem 3.1** The multinomial representation of the \( R_n \) function of (3) has coefficients \( \rho \) satisfying the linear equations (11), restated as,

\[
\rho = 2^{1-n} R_{n+1} s_n
\]

(17)

where \( R_n \), the generalized Pascal matrix, is defined recursively in (8), and (10), and satisfies (13) and (16).

This result means that matrix inverses are avoided in calculating coefficients. This becomes significant for large \( n \).

This result for \( \text{sign}_n(s) \) functions generalizes trivially to any nonlinear function \( f(a_1, a_2, \ldots, a_n) \) which is invariant of the ordering of the \( a_i \). The \( s_n \) vector is then replaced by a vector with \( j^{th} \) element \( f(-1, -1, \ldots, 1, 1, 1, \ldots, 1) \), where there are \( j \) elements of the data set being \(-1, \) and \( n-j \) unity elements.

For completeness, we tabulate the coefficients for low \( n \), and point out certain properties which can be established by induction.
Specific relationships between the coefficients are clear from the tables and can be proved by induction arguments, as follows. For Table I, for the $\text{sign}$ operation,

$$\rho_i^{(n)} = 0, \quad \text{for } i = 0, 1, 3, \ldots \text{and all } n,$$

$$\rho_i^{(n)} = \rho_i^{(n-1)}, \quad \text{for all } i \text{ and } n = 3, 5, 7, \ldots,$$

$$\text{sign}(\rho_i^{(n)}) = -1, \quad \text{for all } n \text{ and } i = 3, 7, 11, \ldots,$$

$$\text{sign}(\rho_i^{(n)}) = 1, \quad \text{for all } n \text{ and } i = 1, 5, 9, \ldots, \quad (18)$$

and for Table II, for the $\text{sign}_\pm$ operation,

$$\rho_i^{(n)} = 0, \quad \text{for } i = 0, 2, 4, \ldots,$$

$$\rho_i^{(n)} = \rho_i^{(n-1)}, \quad \text{for } i = 1, 3, 5, \ldots,$$

$$\rho_i^{(n)} = \rho_i^{(n-1)}, \quad \text{for } i = 1, 3, 5, \ldots,$$

$$\text{sign}(\rho_i^{(n)}) = +1, \quad \text{for all } n,$$

$$\text{sign}(\rho_i^{(n)}) = -1, \quad \text{for all } n, \quad (19)$$

There is also symmetry in the coefficients for each odd $n$. Indeed for this case the coefficients for $\text{sign}$ and $\text{sign}_\pm$ are identical (since then $\text{sign}_\pm \equiv \text{sign}$).

We see that Table II can be constructed using these various properties and the entries in Table I. Moreover, all coefficients can be constructed from the subset of Table I, namely the $\rho_i^n$ for $n = 3$, $n = 4$, $n = 5$, $n = 6$, $n = 7$, $n = 8$.

It is readily seen that for $n > 2$, and either coefficient selection, in obvious notation, then $\sum_{i=1}^{n+1} P_{n+1}(n,i)\rho_i^{(n)} = -1$, and $\sum_{i=1}^{n+1} P_{n+1}(n-1,i)\rho_i^{(n-1)} = 0$. There are other products of the rows of $P_n$ and $\rho$ vectors which are also 0 or 1 not spelt out.

The generalized Pascal Matrix is the key to the coefficients. It is worth pointing out that although this matrix is not orthogonal, induction arguments show that all odd rows are orthogonal to all even rows, so that $R_i R_n^*$ has zero $i,j$ entries where $i$ is even and $j$ is odd.

### IV. CONCLUSIONS

Majority logic coding for communication systems has attractive advantages in terms of the simplicity of the decoding. This is achieved at the expense of optimality. The majority logic operations involved are highly nonlinear, so there has been a paucity of theory for developing codes and guaranteeing properties.

A key step in this direction, presented in this paper, has been the generation of an explicit formula for the multinomial representation of the various $\text{sign}_n$ operations involved in majority logic. The formula is readily calculated in terms of binomial coefficients, appearing in a proposed generalized Pascal matrix. A factorization of this matrix, in terms of a lower Cholesky factor of the original Pascal matrix, turns out to simplify the proof and derivation of the coefficients. The results are more complete than hitherto given for the case of $\text{sign}$, and are new for the $\text{sign}_\pm$ case.

### V. ACKNOWLEDGEMENTS

Thanks to GO-CDMA Ltd. of Hong Kong SAR, China, for the use of their intellectual properties in this work.

John’s work is supported in part by the ARC discovery grants A0010582, DP0450539, and in part by the National ICT Australia (NICTA), which is funded by the Australian Government Backing Australia’s Ability Initiative in part through the Australian Research Council.

### REFERENCES


