INTEGERS: ELECTRONIC JOURNAL OF COMBINATORIAL NUMBER THEORY 8 (2008), #A02

A COMBINATORIAL INTERPRETATION OF THE POLY-BERNOULLI NUMBERS AND TWO FERMAT ANALOGUES

Chad Brewbaker
Dept. of Electrical and Computer Engineering, Iowa State University, Ames, IA 50011
crb002@iastate.edu

Received: 6/28/07, Revised: 11/12/07, Accepted: 1/1/08, Published: 1/29/08

Abstract

We show that the number of $(0,1)$-matrices with n rows and k columns uniquely reconstructable from their row and column sums is the poly-Bernoulli number $B_n^{(-k)}$. Combinatorial proofs for both the sieve and closed formulas are presented. In addition, we prove an analogue of Fermat's Little Theorem: For a positive integer n and prime number p we have $B_n^{(-p)} \equiv 2^n \pmod{p}$. Also, an analogue to Fermat's Last Theorem is presented: For all positive integers $\{x, y, z\}$ and $n > 1$ there exist no solution to the equation $B_x^{(-n)} + B_y^{(-n)} = B_z^{(-n)}$.

1. Introduction

Our work concerns the set of binary matrices that can be described uniquely by their row and column sums. In this section we proceed with a historical overview. In section two we present additional terminology, and in the third we present our original work. Before we begin it will be beneficial to use the following terminology throughout the paper.

Definition 1 (Lonesum Matrix). *A Lonesum matrix is a binary matrix that can be uniquely reconstructed from its row and column sums.*

The modern foundations of binary matrix reconstruction can be traced to Ryser [14], Fulkerson ([6], [7], [8], [9]), and Brualdi [4]. Ryser gives the following excellent classification. Before mentioning it let us define a key aspect separately.

Definition 2 (Interchange Operation). *An interchange operation is one of the following: replacing the sub-matrix* $\binom{01}{10}$ *with* $\binom{10}{01}$*, or replacing the sub-matrix* $\binom{10}{01}$ *with* $\binom{01}{10}$*. Note that row and column sum vectors stay unchanged after interchange operations are performed.*

Theorem 1 (Ryser 1957[14]). *Any (0,1)-matrix with row sum vector R and column sum vector S can be transformed into any other (0,1)-matrix with row sum vector R and column sum vector S via interchange operations.*

This gives rise to the notion of a Ryser class [15]:

Definition 3 (Ryser Class). *A Ryser Class is the set of (0,1)-matrices with the same row sum vector, and the same column sum vector.*

Example 1 (Ryser Class). *The Ryser Class of* $\binom{011}{100}$ *is* $\left\{\binom{011}{100}, \binom{101}{010}, \binom{110}{001}\right\}$.

For this work we will be interested in Ryser classes of size one, our Lonesum matrices. By Theorem 1 we can deduce that a (0,1)-matrix will be uniquely determined by its row and column sums if and only if no interchange operation can be performed on the matrix. To ensure that a matrix can be uniquely reconstructable from its row and column sums we need to forbid certain substructure:

Definition 4 (Forbidden Minor). *A forbidden minor is a sub-matrix of the form* $\binom{01}{10}$ *or* $\binom{10}{01}$.

Engineering applications of Lonesum matrices are discussed in [5] and [11]. Also, data compression and recognition algorithms for Lonesum matrices can be found in [18].

2. The Stirling, Bernoulli, and Poly-Bernoulli Numbers

In this section we will define additional terminology needed.

Definition 5 (Stirling Numbers of the Second Kind). *The Stirling numbers of the second kind are the number of ways to partition n elements into k non-empty subsets.*

We denote the Stirling Numbers of the Second Kind by

$$\left\{ {n \atop k} \right\} = \frac{(-1)^k}{k!} \sum_{l=0}^{k} (-1)^l \binom{k}{l} l^n.$$

Definition 6 (Bernoulli Numbers). *The Bernoulli numbers have the formula*

$$B_n = \sum_{m=0}^{n} (-1)^{m+n} \frac{m! \left\{ {n \atop m} \right\}}{m+1}.$$

$\{1,2,3\}\bigcup\{4\}$	$\{1,2,4\}\bigcup\{3\}$
$\{1,3,4\}\bigcup\{2\}$	$\{2,3,4\}\bigcup\{1\}$
$\{1,2\}\bigcup\{3,4\}$	$\{1,3\}\bigcup\{2,4\}$
$\{1,4\}\bigcup\{2,3\}$	

Table 1: $\left\{ {4 \atop 2} \right\} = 7$

$B_0 =$	1	$\emptyset$
$B_1 =$	$\frac{1}{2}$	$\frac{\lvert\{a\}\rvert}{2}$
$B_2 =$	$\frac{1}{6}$	$-\frac{\lvert\{aa\}\rvert}{2} + \frac{\lvert\{ab,ba\}\rvert}{3}$
$B_3 =$	0	$\frac{\lvert\{aaa\}\rvert}{2} - \frac{\lvert\{aab,aba,baa,bab,bba\}\rvert}{3} + \frac{\lvert\{abc,acb,bac,bca,cab,cba\}\rvert}{4}$

Table 2: Combinatorial interpretation of the Bernoulli numbers

Combinatorially the Bernoulli numbers are an inclusion exclusion, where the sum is taken over all words of length n with k distinct letters, and normalized by $k+1$.

We are interested in an extension to the Bernoulli numbers defined by Kaneko [2], [12], [13]. They are in terms of infinite series, and although we will not use this form it is presented for historical context. Kaneko begins with an alternate definition of the Bernoulli numbers as the coefficients B_n in the formula

$$\frac{xe^x}{e^x - 1} = \sum_{n=0}^{\infty} B_n \frac{x^n}{n!},$$

and then modifies the equation to form the poly-Bernoulli numbers.

Definition 7 (Poly-Bernoulli Numbers of Index k). *The poly-Bernoulli numbers of index k, $B_n^{(k)}$, are defined as*

$$\frac{Li_k(1-e^{-x})}{1-e^{-x}} = \sum_{n=0}^{\infty} B_n^{(k)} \frac{x^n}{n!},$$

where $Li_k(z)$ denotes the formal power series $\displaystyle\sum_{m=1}^{\infty} \frac{z^m}{m^k}$.

Kaneko notes that when k is set equal to one it results in the Bernoulli numbers

$$\frac{xe^x}{e^x - 1} = \sum_{n=0}^{\infty} B_n^{(1)} \frac{x^n}{n!}.$$

Kaneko also proves two combinatorial formulas.

Kaneko's Results 1 (Poly-Bernoulli Numbers). *The poly-Bernoulli numbers of negative index satisfy two equivalent formulas:*

$$B_n^{(-k)} = \sum_{m=0}^{n} (-1)^{n+m} m! \left\{ {n \atop m} \right\} (m+1)^k \tag{1}$$

$$B_n^{(-k)} = \sum_{j=0}^{min(n,k)} (j!)^2 \left\{ {n+1 \atop j+1} \right\} \left\{ {k+1 \atop j+1} \right\}. \tag{2}$$

We shall use (1) to prove our combinatorial interpretation of the poly-Bernoulli numbers, and deduce (2) from this interpretation.

3. Original Work

In this section we give two combinatorial bijections between Lonesum matrices and the poly-Bernoulli numbers. In addition we prove two Fermat analogues of the poly-Bernoulli numbers.

3.1. The Sieve Formula

Theorem 2 (Sieve Formula). *The number of distinct $n \times k$ Lonesum matrices is*

$$B_n^{(-k)} = \sum_{m=0}^{n} (-1)^{n+m} m! \left\{ {n \atop m} \right\} (m+1)^k.$$

To simplify the proof we will turn it into a word counting problem.

Definition 8 (Column Alphabet). *A column alphabet is a legal set of columns that can co-exist in a Lonesum (0,1)-matrix.*

Definition 9 (Forbidden Word). *A forbidden word is an ordered list of {0,1} columns that when concatenated contains a forbidden minor.*

For example, the three symbol word $\binom{010}{110}$ is allowed while the three symbol word $\binom{011}{110}$ is forbidden because it contains the forbidden minor $\binom{01}{10}$.

Definition 10 (Symbol Weight). *Symbol weight is the number of 1's in a {0,1} column, which is the column sum.*

Lemma 1 (Symbol Weight). *No two distinct symbols of the same weight occur in an allowable word of our language.*

Proof. If two distinct symbols occur in a given word, then exchanging these columns with each other would not change the row or column sums, which would violate the Lonesum definition. □

By a similar argument, we have the following:

Corollary 1 (Row Weight). *No two distinct rows can have the same weight in an allowable word.*

Lemma 2 (Swap). *Permuting rows or columns does not change membership in the class of Lonesum matrices.*

Proof. Note that the forbidden minors are mirror images. Swapping either the rows or columns of one forbidden minor will give you the other. Thus, any permutation of rows or columns will still yield the same number of forbidden minors. □

Proof of Theorem 2. By Lemma 1 every column alphabet must consist of distinct symbols with a given weight. For convenience we will throw out the all zero and all 1 symbol until later. If we order the symbols of a size $m-1$ alphabet in decreasing order of their weight and view the alphabet as a word every row will sum to an integer between zero and m. Thus, we have m distinct equivalence classes on the row weights. Partitioning the rows into m distinct equivalence classes, and assigning equivalence classes values of a permutation of the integers 0 to m, the number of alphabets is $(m)!\left\{ {n \atop m} \right\}$.

Alphabets containing $m-1$ symbols will be a subset of the alphabets containing m symbols so we must do an inclusion exclusion to avoid over-counting.

Thus, summing over all size $m-1$ alphabets not containing the all 1's symbol or the all zeros symbol, writing all possible length k words over these alphabets along with the all 1's symbol and all zeros symbol, and doing inclusion exclusion to avoid over counting yields the formula

$$\sum_{m=1}^{n} (-1)^{n+m} m! \left\{ {n \atop m} \right\} (m+1)^k.$$

□

3.2. The Closed Formula

Recent work has gone into finding simplified proofs for a closed equation of the poly-Bernoulli numbers [16], [17]. Here we present a combinatorial proof involving Lonesum matrices.

Theorem 3 (Closed Equation).

$$B_n^{(-k)} = \sum_{m=1}^{Min(n,k)} m! \left\{ {n+1 \atop m+1} \right\} m! \left\{ {k+1 \atop m+1} \right\},$$

and more specifically the number of Lonesum $n \times k$ (0,1)-matrices with exactly m distinct nonzero rows is $m!\left\{ {n+1 \atop m+1} \right\} m!\left\{ {k+1 \atop m+1} \right\}$.

We want to show that the number of Lonesum $n \times k$ (0,1)-matrices is given by the right side of the equation, where m is the number of distinct nonzero rows.

Lemma 3 (Distinct Row Placements). *The number of n-row matrices with r given distinct rows is $r!\left\{ {n \atop r} \right\}$.*

Proof. For each row, select one of the given rows for that position. This is equivalent to giving a mapping from an n-set onto an r-set, and we have seen that this number is $r!\left\{ {n \atop r} \right\}$. □

Corollary 2. *The number of n-row matrices with a given set of m distinct nonzero rows and possibly at least one zero row is $m!\left\{ {n+1 \atop m+1} \right\}$.*

Proof. By the preceding lemma, the number with no zero row is $m!\left\{ {n \atop m} \right\}$, while the number with at least one zero row is $(m+1)!\left\{ {n \atop m+1} \right\}$, giving a total count of $m!\left\{ {n \atop m} \right\} + (m+1)!\left\{ {n \atop m+1} \right\} = m!(\left\{ {n \atop m} \right\} + (m+1)\left\{ {n \atop m+1} \right\})$. Since $\left\{ {n \atop m} \right\} + (m+1)!\left\{ {n \atop m+1} \right\} = \left\{ {n+1 \atop m+1} \right\}$ is a fundamental identity for the Stirling numbers, the result is established. □

Lemma 4 (Legal Distinct m-Row Sets). *Given k columns, the number of legal distinct nonzero m-row sets is $m!\left\{ {k+1 \atop m+1} \right\}$.*

Proof. By Corollary 1 we know that rows have to obey a linear order, with row i less than row j when all 1 entries of row i are also contained in row j and row j has more 1 entries than row i. Use this ordering to sort our nonzero row sets from highest weight to lowest weight. Notice that we have m rows and each of them is nonzero. From the existence of a linear order at least one column must have m 1's. Instead of writing out the whole row set we could represent it as a string of k numbers from zero to m representing column sums where at least one of the column sums is m. For example:

$$\begin{matrix} 1 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 0 \end{matrix}$$

could be written as $\{3, 2, 1\}$.

Thus, all row sets can be written as either an onto function from the k-set of columns to the set of integers 1 to m, or as an onto function from the k-set of columns to the set of integers 0 to m in the case we get an all zero column:

$$\begin{matrix} 1 & 1 & 0 \\ 1 & 0 & 0 \end{matrix}$$

Thus, $m!\left\{ {k \atop m} \right\}$ will count the sets without a zero column, and $(m+1)!\left\{ {k \atop m+1} \right\}$ will count row sets with at least one zero column. Thus, the number of legal distinct nonzero m row sets with k columns is $m!\left\{ {k \atop m} \right\} + (m+1)!\left\{ {k \atop m+1} \right\} = m!\left\{ {k+1 \atop m+1} \right\}$. □

Proof of Theorem 3. By the previous two results, the number of Lonesum $n \times k$ matrices with m distinct nonzero rows, with repetitions and zero rows allowed, is $m!\left\{ {n+1 \atop m+1} \right\} m!\left\{ {k+1 \atop m+1} \right\}$.

Since the number of set partitions where the number of partitions is bigger than the set is zero we only need to sum m up to $\min(n,k)$. For the set of all $n \times k$ Lonesum matrices we then get

$$B_n^{(-k)} = \sum_{m=1}^{\min(n,k)} m! \left\{ {n+1 \atop m+1} \right\} m! \left\{ {k+1 \atop m+1} \right\}.$$

□

3.3. An Analogue of Fermat's Little Theorem

We can derive a poly-Bernoulli cohort to Fermat's Little Theorem, which states that for any positive integer a and prime number p,

$$a^p \equiv a \pmod{p}.$$

We will start with the main lemma of [1].

Lemma 5 (ABR 2005). *Let S be a finite set, let p be a prime number, let $f(x) : S \to S$ be a function that has the property $f^p(x) = x$ for any x in S, and let F be the number of fixed points. Then*

$$|S| \equiv |F| \pmod{p}.$$

One could view the function f as a directed graph on elements in S consisting of disjoint length p cycles and loops.

Theorem 4 (Row Ordered Fermat's Little Theorem). *Given a prime number p, and a positive integer n,*

$$B_n^{(-p)} \equiv 2^n \pmod{p}. \tag{3}$$

Proof. Let S be the set of $n \times p$ Lonesum (0,1)-matrices. Let f be the function that rotates the columns of a matrix once to the left. The matrices that are fixed points in this function are those consisting of all one and all zero rows. There are 2^n such matrices, so let $F = 2^n$. From the above lemma $|S| \equiv |F| \pmod{p}$. Substituting for S and F we get $B_n^{(-p)} \equiv 2^n \pmod{p}$. □

3.4. An Analogue of Fermat's Last Theorem

Ernst Kummer in the 1800's attempted to attack Fermat's Last Theorem with the Bernoulli numbers. His approach showed that for a prime number p, if p does not divide $B_{p-2}^{(1)}, ..., B_2^{(1)}$ then p is an exponent satisfying Fermat's last theorem.

There is also a related open problem [10]:

Open Problem 1 (Regular Primes). *A prime p is called regular if it does not divide any of $B_{p-2}^{(1)}, \ldots, B_2^{(1)}$. Prove that there are an infinite number of regular primes.*

The following lemma will be useful in proving our last theorem.

Lemma 6 (Applications).
(i) $B_x^{(-1)} = 2^x$.
(ii) If $x < z$, *then* $B_x^{(-n)} < B_z^{(-n)}$.
(iii) If $x < z$ *and* $y < z$ *and* $n > 1$, *then* $B_x^{(-n)} + B_y^{(-n)} < B_z^{(-n)}$.

Proof. Clearly all column vectors are Lonesum (since a column vector is the column of its row sums), and the number of binary x-tuples is 2^x, which proves (i).

To prove (ii), we can embed the Lonesum $x \times n$ matrices in the $z \times n$ matrices by padding with zero rows or one rows at the bottom. This gives disjoint embeddings.

To prove (iii), embed the $x \times n$ Lonesum matrices in the $z \times n$ Lonesum matrices by padding with zero rows at the bottom, and embed the $y \times n$ Lonesum matrices in the $z \times n$ Lonesum matrices by padding with one rows at the bottom. These embeddings are disjoint, and for any n-tuple not all one or zero, the matrix with this row vector repeated z times is a Lonesum $z \times n$ matrix in neither of the $x \times n$ or $y \times n$ embeddings. □

We can deduce the following theorem.

Theorem 5 (Row Ordered Fermat's Last Theorem).
(i) If $n > 1$, *there are no positive integer solutions to* $B_x^{(-n)} + B_y^{(-n)} = B_z^{(-n)}$.
(ii) If $n = 1$, *the positive integer solutions to* $B_x^{(-n)} + B_y^{(-n)} = B_z^{(-n)}$ *are given by* $x = y = z - 1$.

Proof. Since there are Lonesum matrices of any size, e.g., the zero and one matrices, part (i) follows immediately from parts (ii) and (iii) of the preceding lemma.

If $n = 1$, part (ii) follows immediately from part (i) of the preceding lemma and the fact that if $z > x + 1$ or $z > y + 1$ then there are $z \times 1$ column vectors whose last two entries are 0 and 1, and these will be in neither of the $x \times 1$ or $y \times 1$ embeddings, while if $y = x$ and $z = x + 1$, then z-tuples are obtained from the x-tuples or y-tuples by padding with a 0 or a 1. □

4. Acknowledgements

We would like to thank Daniel and Wendy Ashlock for presenting us the problem of counting Lonesum matrices, and Ryan Martin for his editorial guidance [3]. We would also like to thank the reviewer for recommending part (ii) of Theorem 5 . This work was partially supported by a US Dept. of Education GAANN fellowship.

References

[1] Peter G. Anderson, Arthur T. Benjamin, and Jeremy A. Rouse. Combinatorial proofs of Fermat's, Lucas's, and Wilson's theorems. *American Mathematical Monthly*, 112(3):266–268, 2005.

[2] Tsuneo Arakawa and Masanobu Kaneko. On poly-Bernoulli numbers. *Comment Math. Univ. St. Paul*, 48(2):159–167, 1999.

[3] Chad Brewbaker. Lonesum (0,1) matrices and the poly-Bernoulli numbers of negative index. Master's thesis, Iowa State University, 2005.

[4] Richard A. Brualdi. Matrices of zeros and ones with fixed row and column sums. *Linear Algebra and Its Applications*, 33:159–231, 1980.

[5] Richard A. Brualdi, Volker Mehrmann, and Hans Schnider. Special Issue on Discrete Tomography. *Linear Algebra and Its Applications*, 339, 2001.

[6] Delbert Ray Fulkerson. Traces, term ranks, widths and heights. *IBM Journal of Research and Development*, 4:455–459, 1960.

[7] Delbert Ray Fulkerson. Zero-one matricies with zero trace. *Pacific Journal of Mathematics*, 10(3):831–836, 1960.

[8] Delbert Ray Fulkerson and Herbert John Ryser. Widths and heights of (0,1)-matrices. *Canadian Journal of Mathematics*, 13:239–255, 1961.

[9] Delbert Ray Fulkerson and Herbert John Ryser. Multiplicities and minimal widths for (0,1)-matrices. *Canadian Journal of Mathematics*, 14:498–508, 1962.

[10] Richard K. Guy. *Unsolved Problems in Number Theory 2nd Ed.* Springer-Verlag, New York, 1994.

[11] Gabor T. Herman and Attila Kuba. *Discrete Tomography: Foundations, Algorithms, and Applications*. World Scientific Publishing Co, 1999.

[12] Masanobu Kaneko. Poly-Bernoulli numbers. *Journal de Théorie des Nombres de Bordeaux*, 9:221–228, 1997.

[13] Masanobu Kaneko. Multiple zeta values, poly-Bernoulli numbers, and related zeta functions. *Nagoya Math Journal*, 153:189–201, 1999.

[14] Herbert John Ryser. Combinatorial properties of matrices of zeros and ones. *Canadian Journal of Mathematics*, 9:371–377, 1957.

[15] V.N. Sachkov and V.E. Tarakanov. *Combinatorics of Nonnegative Matrices*. American Mathematical Society, 2002.

[16] Roberto Sánchez-Peregrino. Closed formula for poly-Bernoulli numbers. *Fibonacci Quarterly*, 40(4):362–364, 2002.

[17] Roberto Sánchez-Peregrino. A note on a closed formula for poly-Bernoulli numbers. *American Mathematical Monthly*, 109(8):755–758, 2002.

[18] Jeremy Spinrad. *Efficient Graph Representations*. American Mathematical Society, 2003.