Séminaire Lotharingien de Combinatoire **45** (2001), Article B45d

Binary Moore-Penrose Inverses of Set Inclusion Incidence Matrices

Helmut Krämer
Fachbereich Mathematik der Universität Hamburg
Bundesstraße 55
20146 Hamburg – Germany

Abstract

This note is a supplement to some recent work of R.B. Bapat on Moore-Penrose inverses of set inclusion matrices. Among other things Bapat constructs these inverses (in case of existence) for $H(s,k) \bmod p$, p an arbitrary prime, $0 \leq s \leq k \leq v-s$. Here we restrict ourselves to $p=2$. We give conditions for s,k which are easy to state and which ensure that the Moore-Penrose inverse of $H(s,k) \bmod 2$ equals its transpose. E.g., $H(s,v-s) \bmod 2$ has this property. Furthermore $\operatorname{Ker} H(s,v-s) \bmod 2$ is nonzero if $0<2s<v \leq 3s$ and then there is a decomposition

$$\operatorname{Ker} H(s,v-s) \equiv \sum_{\substack{0 \leq j \leq s-1 \\ 2 \mid \binom{v-s-j}{v-2s}}} \operatorname{Im} H(v-s,v-j) \bmod 2.$$

Also, refinements of this decomposition are given.

1. Let $\mathbb{F}$ be a field. If A is a $m \times n$-matrix with entries in $\mathbb{F}$, then a $n \times m$-matrix G (with entries in $\mathbb{F}$) is called a generalized inverse (g-inverse) of A if

$$AGA = A.$$

A Moore-Penrose inverse of A, denoted by A^{+}, is a $n \times m$-matrix G satisfying the equations

$$AGA = A,\ GAG = G,$$
$$(AG)^T = AG,\ (GA)^T = GA.$$

Note that if A is square and invertible, $G = A^{-1}$ is a Moore-Penrose inverse of A. Thus A^+ (if it exists) can be thought of as a substitute for the inverse of A, even if A is non-square.

- Any real or complex matrix admits a unique Moore-Penrose inverse.

In general, the following theorem gives a necessary and sufficient condition for a matrix to admit a Moore-Penrose inverse over an arbitrary field.

Theorem (R.B. Bapat, K.P.S. Bhaskara, K. Manjunatha, [2])
A $m \times n$-matrix of rank r over an arbitrary field admits a Moore-Penrose inverse if and only if the sum of the squares of the $r \times r$ minors of A is nonzero.

Moore-Penrose inverses were introduced by Penrose for complex matrices with a slight modification replacing in the above four defining equations the transpose of a matrix by its complex-conjugate transpose.

However, the proof that Moore-Penrose inverses are uniquely determined (if they exist) carries over to the definiton given above. For the convenience of the reader we reproduce the proof. So let X, Y two Moore-Penrose inverses of A. Then

$$\begin{aligned} X &= XAX = X(AX)^T = XX^TA^T = XX^T(A^TY^TA^T) \\ &= X(AX)^T(AY)^T = X(AXA)Y = XAY = \\ &= (XA)^T(YAY) = (XA)^T(YA)^TY = (A^TX^TA^T)Y^TY = \\ &= A^TY^TY = (YA)^TY = Y. \end{aligned}$$

Note that all four defining equations have been used in the proof.

Now we recall the definition of set-inclusion incidence matrices. In fact there are two families of incidence matrices. Let s, k, v be in $\mathbb{N}_0$ and $s, k \leq v$. Let $H_v(s,k) = H(s,k)$ denote the integer $(0,1)$-matrix with rows and columns indexed respectively by the s-subsets and k-subsets of a fixed v-set with ij-entry equal to one if and only if the i-th s-subset is contained in the j-th k-subset.

By $\overline{H_v}(s,k) = \overline{H}(s,k)$ we denote the integer $(0,1)$-matrix with rows and columns indexed respectively be the s-subsets and k-subsets of a fixed v-set, with ij-entry equal to one if and only if the i-th s-subset is contained in the complement of the j-th subset.

Here we are mainly concerned with the first family of matrices.

Both $H(s,k)$ and $\overline{H}(s,k)$ may be zero matrices but e.g. both $H(0,k)$ and $\overline{H}(0,k)$ are the $1 \times \binom{v}{k}$ vector of all ones.

There are many relations between $H(s,k)$ and $\overline{H}(s,k)$ (see for example [5], Chapt 15, 8.2) from which we quote only one

- $\overline{H}(s,k) = \sum_i (-1)^i H(i,s)^T H(i,k)$.

If p is any prime number we denote by $H(s,k)_p$, $\overline{H}(s,k)_p$ the matrices obtained by reducing all entries of $H(s,k)$ or $\overline{H}(s,k)$ respectively modulo $p\,\mathbb{Z}$.

Binomial coefficients $\binom{n}{m}$ are also defined if m is negative. We adopt the convention that $\binom{n}{m} = 0$ if $m < 0$ or $n < m$.

2. The problem to give necessary and sufficient conditions which imply the existence of a Moore-Penrose inverse of $H(s,k)_p$, p an arbitrary prime, has been solved very recently:

Theorem (R.B. Bapat [1])
Let $0 \le s \le k \le v - s$, let p be a prime and let

$$\mathcal{N} = \left\{ i : 0 \le i \le s,\ p \nmid \binom{k-i}{s-i} \right\}.$$

Then $H(s,k)_p$ has a Moore-Penrose inverse if and only if $p \nmid \binom{v-i-s}{k-s}$ for all $i \in \mathcal{N}$. Furthermore, the Moore-Penrose inverse, if it exists, is given by

$$H(s,k)_p^+ = \sum_{i,j \in \mathcal{N}} (-1)^i \frac{\binom{v-i-j}{s-i}}{\binom{v-i-s}{k-s}} \overline{H}(i,k)_p^T \, \overline{H}(j,i)_p^T \, H(j,s)_p.$$

Corollary *$H(s,v-s)_p$ admits a Moore-Penrose inverse for all primes p.*

Now Bapat provides an example of an incidence matrix where the Moore-Penrose inverse is just one matrix; take $H_6(2,4)_3$. Here the set $\mathcal{N} = \{2\}$ has minimum cardinality. After making a suitable arrangement of the 2-sets and the 4-sets of the 6-set it is shown that $H_6(2,4)_3^+ = H_6(2,4)_3$.

We give now another example of an incidence matrix where the set $\mathcal{N}$ has maximum cardinality and the Moore-Penrose inverse equals the transpose of the given matrix. Let for a moment p be an arbitrary prime and recall

Wilson's Rank Formula ([8])
Let $0 \le s \le k \le v-s$, let p be a prime and let

$$\mathcal{N} = \left\{ i : 0 \le i \le s,\ p \nmid \binom{k-i}{s-i} \right\}.$$

Then

$$\operatorname{rank} H(s,k)_p = \sum_{i \in \mathcal{N}} \left\{ \binom{v}{i} - \binom{v}{i-1} \right\}.$$

Now we take $k = v-s$. Let s, v be so chosen, that $v > 2s$ and $\mathcal{N} = \{0, 1, \ldots, s\}$. Then the rank-formula yields

$$\operatorname{rank} H(s,v-s)_p = \sum_{i=0}^{s} \left\{ \binom{v}{i} - \binom{v}{i-1} \right\} = \binom{v}{s},$$

so $H(s,v-s)_p$ is nonsingular and therefore

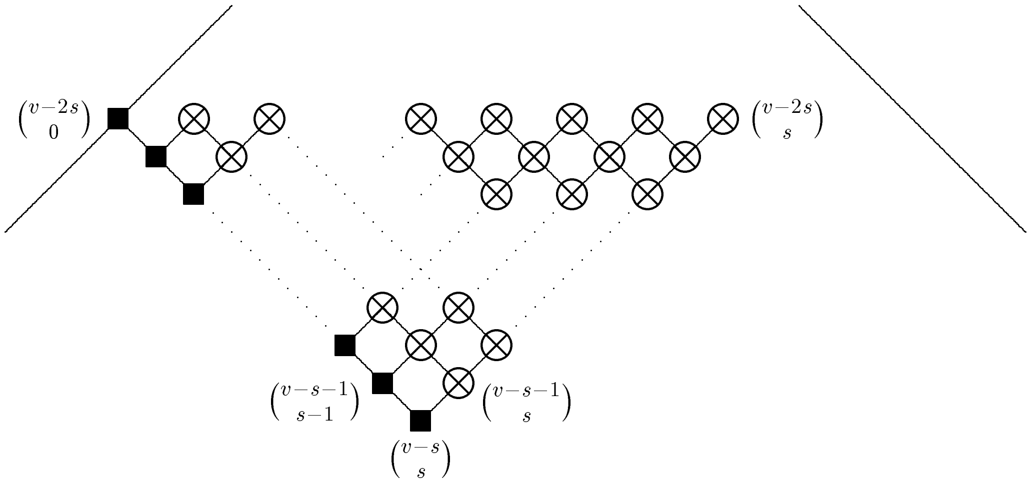
$$H(s,v-s)_p^+ = H(s,v-s)_p^{-1}.$$

Now we take $p = 2$ and claim $H(s,v-s)_2^{-1} = H(s,v-s)_2^T$.

Now $H(s,v-s)^T\, H(s,v-s) = (\alpha\,(L,M))$ with

$$\alpha\,(L,M) = \binom{|L \cap M|}{s}, \quad L, M\ (v-s)\text{-sets}.$$

Now look at Pascal's triangle (more precisely at a part of it).



■ = entry is odd, ⊗ = entry is even.

By moving in the triangle from left to right we obtain

$$2 \mid \binom{v-s-i}{s},\ 1 \leq i \leq s,$$

in particular $v > 3s$.

Therefore

$$H(s, v-s)_2^T\, H(s, v-s)_2 = (\alpha\,(L, M) \bmod 2) = I$$

and the claim is proved; furthermore

$$H(s, v-s)_2^+ = H(s, v-s)_2^T.$$

Note that we can skip the use of Wilson's rank-formula in proving that the Moore-Penrose inverse of $H(s, v-s)_2$ equals its transpose.

3. In the sequel we focus on *binary* Moore-Penrose inverses of incidence matrices $H(s, k)_2$. Our main source of interest is

- Construction of linear binary codes C of the form $C = \operatorname{Ker} H(s,k)_2$ for appropriate s, k.

Definition *Let $0 \le s \le k \le v$. We say that $H(s,k)_2$ admits a special Moore-Penrose inverse, if it admits a Moore-Penrose inverse and this equals $H(s,k)_2^T$.*

We need some elementary number theory. Let p for a moment be an arbitrary prime and let $n \in \mathbb{N}$. If p^α, $\alpha \ge 1$ occurs as a factor in the primary decomposition of n, call α to be the order ($= \operatorname{ord}_p(n)$) of p with respect to n. If $p \nmid n$, define $\operatorname{ord}_p(n) = 0$.

- (Gauß) $\qquad \operatorname{ord}_p(n!) = \sum_{i=1}^{\infty} \left\lfloor \frac{n}{p^i} \right\rfloor.$

- $\operatorname{ord}_p(n!) = \frac{n - Q(n)}{p-1}$. Here $Q(n)$ denotes the sum of the digits in the p-adic expansion of n.
  (See e.g. [6], Chapter I, Exercise 13. This can also easily be proved with help of Gauß' result).

Therefore

- $\operatorname{ord}_p\left(\binom{n}{m}\right) = \frac{Q(m) + Q(n-m) - Q(n)}{p-1}, \; 0 \le m \le n.$

In particular

$$(1)\ldots \qquad \operatorname{ord}_2\left(\binom{n}{m}\right) = Q(m) + Q(n-m) - Q(n), \; 0 \le m \le n.$$

This yields also an "indirect proof" that all "p-adic" functions $Q : \mathbb{N}_0 \to \mathbb{N}_0$ are "subadditive", that is that

$$Q(l+m) \le Q(l) + Q(m); \; m, l \in \mathbb{N}_0,$$

since

$$0 \le \operatorname{ord}_p\left(\binom{l+m}{m}\right) = \frac{Q(m) + Q(l) - Q(m+l)}{p-1}.$$

Theorem 1 *Let $0 \le s < k \le v - s$ and $r \in \mathbb{N}_0$ be such that*

$$2^r \le k - s < 2^{r+1}.$$

Assume

$$v \equiv s + k \bmod 2^{r+1}.$$

Then $H(s,k)_2$ admits a special Moore-Penrose inverse.

Corollary *$H(s, v-s)_2$ admits a special Moore-Penrose inverse.*

Proof: We use the following

Lemma 1 ([5], Chapter 15, 8.4)

Let $0 \le s \le k,\ 0 \le t \le k$. Then

$$H(s,k)\,H(t,k)^T = \sum_i \binom{v-s-t}{v-k-i} H(i,s)^T\, H(i,t).$$

The proof of the lemma uses Vandermonde's identity for binomial coefficients.

Now put in the lemma $s = t$, multiply the identity from the right with $H(s,k)$, use the well-known identity

$$(2)\ldots \qquad H(i,s)\,H(s,l) = \binom{l-i}{s-i} H(i,l), \quad 0 \le i \le s \le l,$$

(see e.g. [5], Chapter 15, 8.1) and obtain

$$(3)\ldots \qquad H(s,k)\,H(s,k)^T\,H(s,k) = \sum_i \binom{v-2s}{v-k-i}\binom{k-i}{s-i} H(i,s)^T\,H(i,k).$$

Now consider the product

$$\binom{v-2s}{v-k-i}\binom{k-i}{s-i}.$$

Denote $q := k - s$. The first factor in the above product is $\binom{v-2s}{q-s+i}$. So we can restrict the above sum (3) to those $i \ge 0$ with $i \ge s - q$. We define a new running index j by

$$i = s - q + j,\ j \ge q - s.$$

Then the above product equals $\binom{v-2s}{j}\binom{2q-j}{q}$ which is zero if $j < 0$ or $j > q$. Therefore

$$(4)\ldots \quad \begin{cases} \quad H(s,k)\, H(s,k)^T\, H(s,k) = \\ \\ \displaystyle\sum_{j=max\{0,q-s\}}^{q} \binom{v-2s}{j}\binom{2q-j}{q} \cdot H(s-q+j,k)^T \cdot H(s-q+j,s). \end{cases}$$

Similarly, by multiplying the identity of the lemma from the left with $H(s,k)^T$ we obtain

$$(4')\ldots \quad \begin{cases} \quad H(s,k)^T\, H(s,k)\, H(s,k)^T = \\ \\ \displaystyle\sum_{j=max\{0,q-s\}}^{q} \binom{v-2s}{j}\binom{2q-j}{q} \cdot H(s-q+j,k)^T \cdot H(s-q+j,s). \end{cases}$$

Claim: $\quad \binom{v-2s}{j}\binom{2q-j}{q}$ is $\begin{cases} \text{odd}, & \text{if } j = q, \\ \text{even}, & \text{if } 0 \le j < q. \end{cases}$

Suppose that the claim has already been proved. Then we reduce equations (4), (4') modulo 2, observe that $H(s,s) = I$ and obtain

$$\begin{aligned} H(s,k)_2\, H(s,k)_2^T\, H(s,k)_2 &= H(s,k)_2, \\ H(s,k)_2^T\, H(s,k)_2\, H(s,k)_2^T &= H(s,k)_2^T. \end{aligned}$$

This already proves that $H(s,k)_2$ admits $H(s,k)_2^T$ as a (special) Moore-Penrose inverse, since the remaining two assertions (which define Moore-Penrose inverses) are trivially satisfied.

Now we prove the claim, first statement. By assumption

$$n : v - s \ge k - s = q \ge 1,$$
$$n \equiv q \bmod 2^{r+1}.$$

Let $n = \lambda \cdot 2^{r+1} + q,\ \lambda \in \mathbb{N}_0,\ q < 2^{r+1}$. Therefore

$$Q(n) = Q(\lambda \cdot 2^{r+1}) + Q(q)$$

and

$$\begin{aligned}\operatorname{ord}_2\left(\binom{v-2s}{q}\right) &= \operatorname{ord}_2\left(\binom{n}{q}\right) = Q(q)+Q(n-q)-Q(n) = \\ &= Q(q)+Q(\lambda\cdot 2^{r+1})-(Q(\lambda\cdot 2^{r+1})+Q(q)) = 0\end{aligned}$$

To prove the second statement of the claim it is sufficient to show:

If for some $j,\ 0 \le j < q,\ \binom{2q-j}{q}$ is odd, then $\binom{n}{j}$ is even.

By assumption

$$(5)\ldots \qquad 0 = \operatorname{ord}_2\left(\binom{2q-j}{q}\right) = Q(q)+Q(q-j)-Q(2q-j).$$

Since $\quad n-j = \lambda\cdot 2^{r+1}+(q-j),\ 1 \le q-j < 2^{r+1}$,

an easy calculation shows

$$\operatorname{ord}_2\left(\binom{n}{j}\right) = Q(j)+Q(q-j)-Q(q).$$

Combine this with Eq (5) and obtain

$$\operatorname{ord}_2\left(\binom{n}{j}\right) = Q(j)+2Q(q-j)-Q(2q-j).$$

Now we use the subadditivity of Q and $Q(2l)=Q(l),\ l\in\mathbb{N}_0$ and obtain

$$\begin{aligned}\operatorname{ord}_2\left(\binom{n}{j}\right) &= Q(j)+(Q(2q-2j)+Q(q-j))-Q(2q-j) \\ &= (Q(j)+Q(2q-2j))+Q(q-j)-Q(2q-j) \\ &\ge Q(2q-j)+Q(q-j)-Q(2q-j) = Q(q-j) > 0.\end{aligned}$$

This proves the claim. □

Remark In the theorem the condition $0 \le s < k \le v-s$ can in some cases (with more work) be weakened. For example take $k = s+1$. Then according to the theorem $H(s,s+1)_2$ admits a special Moore-Penrose inverse provided

$$v \text{ odd },\ s \le \frac{v-1}{2}.$$

However, this is true for v odd and all $s,\ 0 \le s \le v-1$.

4. In this section we come to an application. Let $\mathbb{F}$ be any field. We associate to the integer matrix $H(s,k)$ a linear map $H(s,k)_{\mathbb{F}}$ of $\mathbb{F}$-vectorspaces as follows. Let $C_i,\ 0 \le i \le v$ the $\mathbb{F}$-vectorspace with base $\{\underline{T}\}$, where T runs through all i-subsets of the v-set and let the linear map

$$H(s,k)_{\mathbb{F}} : C_k \to C_s$$

induced by

$$H(s,k)_{\mathbb{F}}\,(\underline{T}) = \sum_{S\subset T}^{|S|=s} \underline{S},\ \ |T| = k.$$

In case $\mathbb{F} = \mathbb{F}_p$ we write again $H(s,k)_{\mathbb{F}} = H(s,k)_p$.

Theorem (A. Bjerhammar [4], R. Penrose [7]) *Let $\mathbb{F}$ be a field and A, G be $m \times n$ resp. $n \times m$ matrices with entries in $\mathbb{F}$ such that $AGA = A$. Then the system of linear equations $Ax = b$ has a solution if and only if*

$$AGb = b$$

in which case the most general solution is

$$x = Gb + (I - GA)y,\ y \textit{ arbitrary.}$$

In particular $\quad \operatorname{Ker} A = \operatorname{Im}(I - GA)$.

Let p be an arbitrary prime and suppose that $H(s,k)_p$ admits a Moore-Penrose inverse. Then

$$(6)\ldots \qquad \operatorname{Ker} H(s,k)_p = \operatorname{Im}(I - H(s,k)_p^+\, H(s,k)_p).$$

On the other side it is straightforward to exhibit a subspace of $\operatorname{Ker} H(s,k)_p$ (regardless whether $H(s,k)_p$ admits a Moore-Penrose inverse or not). According to eq. (2)

$$(7)\ldots \qquad U_{s,k}^p := \sum_{\substack{0\le j\le v-(k+1)\\ p\,|\,\binom{v-s-j}{k-s}}} \operatorname{Im} H(k, v-j)_p$$

is a subspace of $\operatorname{Ker} H(s,k)_p$ (of course, the above sum may be empty). We make the following

Conjecture *Let $0 < s < k < v$, and let p be a prime. Then*

$$\operatorname{Ker} H(s,k)_p = U^p_{s,k}.$$

We give an example where the conjecture is true and take $k = s+1$, $p = 2$. Then $H(s+1, v-j)_2$ is a subspace of $U^2_{s,s+1}$ iff $v-j-s$ is even. But according to eq. (2) then

$$\begin{aligned} H(s+1,s+2)_2 \cdot H(s+2,v-j)_2 &= (v-j-s-1)\cdot 1 \cdot H(s+1,v-j)_2 \\ &= H(s+1,v-j),\ 1 \in \mathbb{F}_2,\ s+2 \le v-j. \end{aligned}$$

Therefore

$$U^2_{s,s+1} \supseteq \operatorname{Im} H(s+1,s+2)_2 \supseteq \operatorname{Im} H(s+2,v-j)_2$$

and $U^2_{s,s+1} = \operatorname{Im} H(s+1,s+2)_2$. It has been remarked in [7], Prop. 7, that $\operatorname{Ker} H(s,s+1)_2 = \operatorname{Im} H(s+1,s+2)_2 \ (= U^2_{s,s+1})$. –

This example also shows that the sum in eq. (7) might be "redundant".

We give a second example which at least gives some evidence that the conjecture might be true.

Let $0 < s < k = v-s$ and p a prime. Then

$$\det H(s,v-s) = \prod_{j=0}^{s-1} \binom{v-s-j}{v-2s}^{\binom{v}{j}-\binom{v}{j-1}}$$

(see [9], Theorem 2 or [7], Corollary 1 to Theorem 1). Then obviously

$$\operatorname{Ker} H(s,v-s)_p \neq (0) \text{ iff } p \mid \det H(s,v-s) \text{ iff } U^p_{s,v-s} \neq (0).–$$

In the sequel we stick to this example in the binary case. First we derive a criterion that ensures that $\operatorname{Ker} H(s,v-s)_2$ is nonzero, making no use of the formula for $\det H(s,v-s)$ just given.

According to the Corollary to Theorem 1 and eq. (6) we have

(8)... $\quad \operatorname{Ker} H(s,v-s)_2 = \operatorname{Im}(I + H(s,v-s)_2^T\, H(s,v-s)_2)$.

Proposition *Let $0 < 2s < v$ and assume that*

$$H(s,v-s)_2 : C_{v-s} \to C_s$$

is an isomorphism. Then $3s < v$. In particular, if $0 < 2s < v \leq 3s$ then $\operatorname{Ker} H(s,v-s)_2$ *is nonzero.*

Proof: By assumption $\operatorname{Ker} H(s,v-s)_2 = (0)$. Then eq. (8) yields

$$I = H(s,v-s)_2^T\, H(s,v-s)_2 = \left(\binom{|L \cap M|}{s} \bmod 2\right).$$

Now if L, M vary through all $(v-s)$-sets, $\binom{|L\cap M|}{s}$ takes all values $\binom{v-s-j}{s} =: \alpha_j$, $0 \leq j \leq s$. Now we have $\alpha_0 > 1$ (and α_0 odd) and α_j even if $0 < j$. This implies $v - 2s > s$. $\square$

At the same time we have proved the

Corollary *Assume that $0 < 2s \leq v$ and that $H(s,v-s)_2$ is nonsingular. Then $H(s,v-s)_2^{-1} = H(s,v-s)_2^T$.*

From now on we assume $0 < 2s < v \leq 3s$. To prove the conjecture for $H(s,v-s)_2$ it is sufficient to show that

(9)... $\quad \operatorname{Im}(I + H(s,v-s)_2^T\, H(s,v-s)_2) \subseteq U^2_{s,v-s} =: U_s$.

We first describe briefly the lines of the proof. Now $\operatorname{Ker} H(s,v-s)_2$ is generated by the elements

$$\sigma_M := \underline{M} + \sum^{|L|=v-s} \binom{|M \cap L|}{s} \cdot 1 \cdot \underline{L},\ \ |M| = v-s,\ 1 \in \mathbb{F}_2.$$

Now we put $v - 2s =: q$, $1 \leq q \leq s$. Furthermore $|L \cap M| = v - s - j$ iff $|L \cup M| = v - s + j$. We define

$$S^M_{v-l} = \sum_{\substack{|L|=v-s \\ |L \cup M| = v-l}} \underline{L},\ \ 0 \leq l \leq s.$$

(Observe that $S^M_{v-s} = \underline{M}$). Then we rewrite the generators σ_M of $\operatorname{Ker} H(s, v-s)_2$:

$$(10)\ldots \qquad \sigma_M = \left(\binom{s+q}{s} \cdot 1 + 1\right) \cdot \underline{M} + \sum_{l=0}^{s-1} \binom{l+q}{s} \cdot 1 \cdot S^M_{v-l},\ 1 \in \mathbb{F}_2.$$

Observe that all σ_M are nonzero.

If X is a subset of the v-set denote by $\complement X$ the complement of X.

Lemma 2 *Let M be a $(v-s)$-subset of the v-set. Then for $0 \le t \le s$ one has*

$$\tau^M_t := \sum_{|T|=t, T \subset \complement M}^{T} H(v-s, v-t)_2\ (\complement T) = \sum_{l=0}^{s} \binom{l}{t} \cdot 1 \cdot S^M_{v-l}.$$

Furthermore if $\binom{v-s-t}{s-t}$ is even then all τ^M_t are contained in $\operatorname{Ker} H(s, v-s)_2$.

Proof: Let L be a $(v-s)$-set and $|L \cup M| = v-l$, $0 \le l \le s$ and $R := \complement(M \cup L)$. Then

$$L \subset \complement T \ \text{ iff } \ \complement R = M \cup L \subset \complement T \ \text{ iff } \ R \supset T.$$

In particular $l \ge t$. So if $l < t$ (this condition is vacuous if $t = 0$) $\underline{L}$ appears with coefficient 0 in all $\binom{s}{t}$ summands of the L.S. of the formula. If $l \ge t$ then $\underline{L}$ appears with coefficient 1 in exactly $\binom{l}{t}$ summands in the L.S. of the formula (we remind the reader of our convention on binomial coefficients).

The last assertion follows from eq. (2). $\square$

Now we will show that all generators σ_M of $\operatorname{Ker} H(s, v-s)_2$ are sums of elements τ^M_t for appropriate t all of which are contained in $\operatorname{Ker} H(s, v-s)_2$, thereby proving eq. (9). At the same time, we obtain more precise assertions on "generating" subspaces of U_s.–

To state the next result we define on $\mathbb{N}_0$ a partial order "$\prec$" as follows. If $j, q \in \mathbb{N}_0$ and

$$j = \sum_{i \ge 0} a_i 2^i,\ q = \sum_{i \ge 0} b_i 2^i$$

are the 2-adic expansions of j resp. q, we define

$$j \prec q \text{ if } a_i \leq b_i \text{ for all } i \geq 0.$$

Then put $\mathcal{M}(q) = \{j : j \in \mathbb{N}_0,\ j \prec q\}$ and $\mathcal{M}(q)^* = \mathcal{M}(q) \setminus \{0\}$.

So, for example for $t \geq 1$

$$\begin{aligned} \mathcal{M}(2^t - 1) &= \{0, 1, 2, \ldots, 2^t - 1\}, \\ \mathcal{M}(2^t) &= \{0, 2^t\}, \\ \mathcal{M}(2^t + 1) &= \{0, 1, 2^t, 2^t + 1\}. \end{aligned}$$

Theorem 2 *Assume* $0 < 2s < v \leq 3s$. *Then* $\operatorname{Ker} H(s, v-s)_2$ *is nonzero and*

$$\operatorname{Ker} H(s, v-s)_2 = \sum_{\substack{0 \leq i \leq s-1 \\ 2 \mid \binom{v-s-i}{v-2s}}} \operatorname{Im} H(v-s, v-i)_2.$$

Moreover it already holds that

$$\operatorname{Ker} H(s, v-s)_2 = \sum_{j \in \mathcal{M}(v-2s)^*} \operatorname{Im} H(v-s, v-s+j)_2.$$

So the theorem states for example that

in case $v - 2s = 2^t - 1,\ t \geq 1$,

$$\operatorname{Ker} H(s, v-s)_2 = \sum_{j=1}^{2^t-1} \operatorname{Im} H(v-s, v-s+j)_2,$$

in case $v - 2s = 2^t,\ t \geq 0$,

$$\operatorname{Ker} H(s, v-s)_2 = \operatorname{Im} H(v-s, v-s+2^t)_2,$$

in case $v - 2s = 2^t + 1,\ t \geq 1$,

$$\operatorname{Ker} H(s, v-s)_2 =$$
$$\operatorname{Im} H(v-s, v-s+1)_2 + \operatorname{Im} H(v-s, v-s+2^t)_2 + \operatorname{Im} H(v-s, v-s+2^t+1)_2. \text{–}$$

Proof of the theorem: We use the notations introduced above.

We apply on the binomial coefficient $\binom{l+q}{s}$, $q = v-2s$, $0 \le l \le s$, q-times the relation $\binom{n}{m} = \binom{n-1}{m} + \binom{n-1}{m-1}$, $n \in \mathbb{N}$, $m \in \mathbb{Z}$. Note that we use the relation even in the trivial cases $m < 0$ or $n \le m$. At each time we cancel binomial coefficients which appear with factor 2. So for example if $q = 2$,

$$\begin{aligned}
\binom{l+2}{s} &= \binom{l+1}{s} + \binom{l+1}{s-1} \\
&= \left(\binom{l}{s} + \binom{l}{s-1}\right) + \left(\binom{l}{s-1} + \binom{l}{s-2}\right) \\
&= \binom{l}{s} + 2\binom{l}{s-1} + \binom{l}{s-2} \equiv \binom{l}{s} + \binom{l}{s-2} \bmod 2.
\end{aligned}$$

So we reach a congruence

$$(11)\ldots \qquad \binom{l+q}{s} \equiv \sum_{i \in \overline{\mathcal{M}}(q)} \binom{l}{s-i} \bmod 2,$$

with a certain subset $\overline{\mathcal{M}}(q)$ of $\{0,1,2,\ldots,q\}$ which contains 0 and q. To determine this subset we consider the $\mathbb{F}_2$-vectorspace

$$V = \mathbb{F}_2^{(\mathbb{Z})} = \{f : \ f : \mathbb{Z} \to \mathbb{F}_2, \ \text{almost all } f(m) = 0, \, m \in \mathbb{Z}\}.$$

Let $\operatorname{Supp} f = \{m : f(m) \neq 0\}$. Define the basis $\{e_m : m \in \mathbb{Z}\}$ of V by

$$e_m(r) = \begin{cases} 1, & r = m, \\ 0, & \text{otherwise.} \end{cases}$$

Finally we define the linear map $\varphi : V \to V$ to be induced by

$$\varphi(e_m) = e_m + e_{m-1}, \ m \in \mathbb{Z}.$$

Now we rewrite eq. (11) as follows:

$$(12)\ldots \qquad \binom{l+q}{s} \equiv \sum_{r \in \operatorname{Supp} \varphi^q(e_s)} \binom{l}{r} \bmod 2.$$

Lemma 3 *If $m \in \mathbb{Z}$ and $q \in \mathbb{N}$, then*

$$\operatorname{Supp} \varphi^q(e_m) = \{m - j : j \in \mathcal{M}(q)\}.$$

Proof: First we prove that the assertion is true if $q = 2^t,\ t \geq 0,$ by induction on t. If $t = 0$, then

$$\operatorname{Supp}\varphi(e_m) = \operatorname{Supp}(e_m + e_{m-1}) = \{m - j : j \in \mathcal{M}(1)\}.$$

Suppose the claim is true for $q = 2^t$. Then

$$\begin{aligned} \varphi^{2^{t+1}}(e_m) &= \varphi^{2^t}(\varphi^{2^t}(e_m) = \varphi^{2^t}(e_m + e_{m-2^t}) \\ &= (e_m + e_{m-2^t}) + (e_{m-2^t} + e_{m-(2^t+2^t)} = e_m + e_{m-2^{t+1}}, \end{aligned}$$

so the claim is true for $q = 2^{t+1}$.

Now we suppose that the assertion is true for all $q \in \mathbb{N}$ and $q \leq 2^t$. Then we show now that the assertion is true for all $q \in \mathbb{N}$ and $q \leq 2^{t+1}$ (this will finish the proof). We may now assume $2^t < q < 2^{t+1}$, so $q = 2^t + u$, $1 \leq u < 2^t$. Then by hypothesis

$$\varphi^q(e_m) = \varphi^u(\varphi^{2^t}(e_m)) = \varphi^u(e_m + e_{m-2^t}) = \sum_{i \in \mathcal{M}(u)} e_{m-i} + \sum_{i \in \mathcal{M}(u)} e_{m-2^t-i}.$$

Since $\mathcal{M}(q) = \mathcal{M}(2^t + u) = \mathcal{M}(u) \cup \{2^t + i : i \in \mathcal{M}(u)\}$ we obtain $\varphi^q(e_m) = \sum_{j \in \mathcal{M}(q)} e_{m-j}$ as claimed. □

We conclude from eq. (12) and the lemma

(13)... $$\binom{l+q}{s} \equiv \sum_{j \in \mathcal{M}(q)} \binom{l}{s-j} \bmod 2. -$$

Now we show that all $\tau^M_{s-j},\ j \in \mathcal{M}(q)^*$ are contained in $\operatorname{Ker} H(s, v-s)_2$. According to Lemma 2 it is sufficient to show that

$$\binom{v - s - (s-j)}{j} = \binom{q+j}{j},\ j \in \mathcal{M}(q)^*$$

are even. But since $j \prec q,\ 1 \leq j$, we have

$$Q(q+j) < Q(q) + Q(j),$$

whence $\operatorname{ord}_2\left(\binom{q+j}{j}\right) > 0$ as claimed.–

Finally we claim that

$$(14)\ldots \qquad \sigma_M = \sum_{j\in\mathcal{M}(q)^*} \tau_{s-j}^M = \sum_{j\in\mathcal{M}(q)^*} \sum_{l=0}^{s} \binom{l}{s-j} \cdot 1 \cdot S_{v-l}^M.$$

In fact the coefficient of $S_{v-s}^M = \underline{M}$ with respect to σ_m is $\binom{s+q}{s} \cdot 1 + 1$ and with respect to the R.S. of eq. (14) is $\sum\limits_{j\in\mathcal{M}(q)^*} \binom{s}{s-j} \cdot 1$. Both coefficients agree by eq. (13).

Furthermore the coefficient of S_{v-l}^M, $0 \leq l < s$ with respect to σ_M is $\binom{l+q}{s} \cdot 1$ (according to eq. (10)) and with respect to the R.S. of eq. (14) is $\sum\limits_{j\in\mathcal{M}(q)^*} \binom{l}{s-j} \cdot 1$ which is $\sum\limits_{j\in\mathcal{M}(q)} \binom{l}{s-j} \cdot 1$ since $l < s$ and $\binom{l}{s} = 0$. Again both coefficients coincide according to eq. (13). This proves eq. (14).

Now we have the following chain of inclusions

$$U_s \subseteq \operatorname{Ker} H(s, v-s)_2 \subseteq \sum_{j\in\mathcal{M}(q)^*} \operatorname{Im} H(v-s, v-s+j)_2 \subseteq U_s.$$

Therefore throughout equality must hold.

This proves the theorem. □

Remark We look at eq. (2) the other way round, that is we keep $H(s,l)$ fixed and let $H(i,s)$ vary, obtaining an inclusion of $\mathbb{F}_p$-vectorspaces.

$$\operatorname{Im} H(s,l)_p \subseteq \bigcap_{\substack{i<s \\ p\mid\binom{l-i}{s-i}}} \operatorname{Ker} H(i,s)_p, \quad p \text{ prime}.$$

Here equality holds. This result (which is of course much more general than ours) has been proved in [3] using Wilson's techniques [9]. That we could dismiss these techniques here is due to the fact that the distribution of even and odd entries in Pascal's triangle is well known. If one is willing to follow the lines used here to prove (parts of) the Conjecture for an arbitrary prime p, an analysis of the distribution of the residue-classes mod p in Pascal's triangle should be made first. We shall return to this topic in a subsequent paper.

References

[1] R.B. Bapat: *Moore-Penrose inverses of set inclusion matrices.* Lin. Alg. and Appl., 318 (2000), 35-44.

[2] R.B. Bapat, K.P.S. Bhaskara, and K. Manjunatha Prasad: *Generalized inverses over integral domains.* Lin. Alg. and Appl., 140 (1990), 181-196.

[3] Th. Bier: *Eine homologische Interpretation gewisser Inzidenzmatrizen* $\bmod p$. Math. Annalen 297 (1993), 289-302.

[4] A. Bjerhammar: *A generalized matrix algebra.* Kungl. Tekn. Högsk. Handl. No. 124 (1968), 32 pp.

[5] C.D. Godsil: Algebraic Combinatorics. New York-London 1993 (Chapman & Hall).

[6] N. Koblitz: p-adic Numbers, p-adic Analysis, and Zeta-Functions. New York-Heidelberg-Berlin, 1977 (Springer).

[7] H. Krämer: *Eigenspace decompositions with respect to symmetrized incidence mappings.* Seminaire Lotharingien de Combinatoire, Art. B41c (1998), 20 pp.
http://www.mat.univie.ac.at/∼slc/

[8] R. Penrose: *A generalized inverse for matrices.* Proc. Cambridge Philos. Soc. 51 (1955), 406-413.

[9] R.M. Wilson: *A diagonal form for the incidence matrices of t-sets vs. k-subsets.* Europ. J. Combinatorics 11 (1990), 609-615.