Theoretical Computer Science 406 (2008) 63–71

Contents lists available at ScienceDirect

Theoretical Computer Science

journal homepage: www.elsevier.com/locate/tcs

On the reconstruction of binary and permutation matrices under (binary) tomographic constraints

S. Brunetti [a], A. Del Lungo [1], P. Gritzmann [b], S. de Vries [c,*]

[a] Dipartimento di Scienze Matematiche e Informatiche 'R. Magari', Università di Siena, Pian dei Mantellin 44, 53100 Siena, Italy

[b] Zentrum Mathematik, Technische Universität München, D-80290 München, Germany

[c] Department of Operations, Faculty of Economics and Business, University of Groningen, P.O. Box 800, 9700 AV Groningen, The Netherlands

ARTICLE INFO

Keywords:
Combinatorics
Discrete tomography
Queens' problem
Bipartite matching
Contingency table
Binary matrix
Permutation
Computational complexity
$\mathbb{NP}$-hardness

ABSTRACT

The paper studies the problem of reconstructing binary matrices constrained by binary tomographic information. We prove new $\mathbb{NP}$-hardness results that sharpen previous complexity results in the realm of discrete tomography but also allow applications to related problems for permutation matrices. Hence our results can be interpreted in terms of other combinatorial problems including the queens' problem.

1. Introduction and main results

For $n \in \mathbb{N}$, let $N = \{1, \ldots, n\}$ and let $\mathcal{B}_n$ be the set of all binary $n \times n$ matrices B regarded as functions $B : N^2 \to \{0, 1\}$. We will then write $B = (\beta_{i,j})_{i,j\in N}$ with $\beta_{i,j} = B(x)$, $x = (i, j)^T$.[2] Ryser [10] studied the problem of characterizing the subsets of $\mathcal{B}_n$ of all such matrices with given row and column sums. Ryser's work can be seen as an anticipation of what was called *discrete tomography* 30 years later; see e.g. [6] and [8]. In view of its relevance to basic algorithmic questions in that field, we are interested in the computational complexity of the question of reconstructing binary matrices with prescribed *binary* marginal sums. Here, not only row and column sums but also diagonal, anti-diagonal or other line sums may be prescribed. More precisely, let $m \in \mathbb{N}$ be the number of marginal sums in different directions, $M = \{1, \ldots, m\}$, and, for every $k \in M$, let the vector $s_k = (\sigma_{k,1}, \sigma_{k,2})^T \in \mathbb{Z}^2 \setminus \{0\}$ specify a direction and let $S_k = \text{lin}\,\{s_k\}$ be the line through the origin spanned by that vector. For each s_k we define an orthogonal vector $t_k = (\sigma_{k,2}, -\sigma_{k,1})^T$. Since t_k is perpendicular to S_k, the set $T_k = \{t_k^T g : g \in N^2\}$ parameterizes all lines parallel to S_k that intersect N^2. One of our basic problems is as follows:

0-1-CONSISTENCY$(S_1, \ldots, S_m)$.

Instance: *$n \in \mathbb{N}$, and for $k \in M$ and $l \in T_k$, $\zeta_{k,l} \in \{0, 1\}$.*

* Corresponding author. Tel.: +31 0 50 363 8617.
E-mail addresses: sara.brunetti@unisi.it (S. Brunetti), gritzman@ma.tum.de (P. Gritzmann), Sven.de.Vries@rug.nl (S. de Vries).

1 To our great grief, our dear friend Alberto Del Lungo passed away before the present paper was finalized.

2 As compared to the standard indexing of matrices we use here the 'affine re-indexing' $(i, j) \leftrightarrow (n + 1 - j, i)$ in order to be able to describe our results in their natural geometric habitat.

0304-3975/$ – see front matter
doi:10.1016/j.tcs.2008.06.014

Task: *Decide, whether there is a* $B \in \mathcal{B}_n$ *such that*

$$\sum_{\substack{i,j \in N \\ i\sigma_{k,2} - j\sigma_{k,1} = l}} \beta_{i,j} = \zeta_{k,l} \quad \text{for } k \in M \text{ and } l \in T_k.$$

A related natural task asks whether a given solution is unique.

0-1-Uniqueness$(S_1, \ldots, S_m)$.

Instance: $n \in \mathbb{N}$, $B \in \mathcal{B}_n$ *such that*

$$\sum_{\substack{i,j \in N \\ i\sigma_{k,2} - j\sigma_{k,1} = l}} \beta_{i,j} \in \{0, 1\} \quad \text{for } k \in M \text{ and } l \in T_k.$$

Task: *Decide, whether there is a* $B' \in \mathcal{B}_n \setminus \{B\}$ *such that*

$$\sum_{\substack{i,j \in N \\ i\sigma_{k,2} - j\sigma_{k,1} = l}} \left(\beta'_{i,j} - \beta_{i,j}\right) = 0 \quad \text{for } k \in M \text{ and } l \in T_k.$$

The case $m = 1$ is, of course, trivial. If $m = 2$ and $s_1 = (1, 0)^T$ and $s_2 = (0, 1)^T$, 0-1-Consistency(S_1, S_2) is also obvious. Given two binary vectors $z_1, z_2 \in \mathbb{R}^n$, we simply ask whether there exists a binary matrix with row sum z_1 and column sum z_2. The answer is affirmative if and only if $\|z_1\|_{(1)} = \|z_2\|_{(1)}$ i.e., the numbers $r = \|z_1\|_{(1)}$ of coefficients 1 in z_1 and z_2 coincide. Actually all such matrices are then permutation matrices expanded by $n - r$ zero rows and columns. The number of different solutions is thus $r!$. Hence, a given solution is unique if and only if $r = 1$. The general case $m = 2$ is also simple. We will show, however, that the transition of 0-1-Consistency$(S_1, \ldots, S_m)$ and 0-1-Uniqueness$(S_1, \ldots, S_m)$ from being trivial to $\mathbb{NP}$-hard takes place 'uniformly' when increasing m from 2 to 3.

Theorem 1. *Let* $m \geq 3$*, and* $s_1, \ldots, s_m \in \mathbb{Z}^2$ *be pairwise linearly independent. Then both* 0-1-Consistency$(S_1, \ldots, S_m)$ *and* 0-1-Uniqueness$(S_1, \ldots, S_m)$ *are* $\mathbb{NP}$*-complete.*

Of course, both problems belong to $\mathbb{NP}$ (with a solution $B \in \mathcal{B}_n$, $B' \in \mathcal{B}_n$ being a certificate, respectively). The proof of the $\mathbb{NP}$-hardness part of Theorem 1 will be given in Section 2.

Let us now outline some additional interpretations of the above (and related) problems; on the one hand, to place them into the perspective of other lines of research in combinatorics, on the other hand to motivate an additional problem that we are also going to address.

The case $m = 4$, $s_1 = (1, 0)^T$, $s_2 = (0, 1)^T$, $s_3 = (1, 1)^T$ and $s_4 = (1, -1)^T$ and $\zeta_{k,l} = 1$ for $k = 1, 2$ and $l \in T_k$ is related to the well-known *queens' problem* on an $n \times n$ chessboard. The question there is whether it is possible to place n queens on the board so that no queen attacks any other. It is well-known that there is at least one solution of the queens' problem for $n = 1$ and $n \geq 4$, [3], but no solution for $n = 2, 3$. Since, naturally, the problem has the symmetries of the chessboard, we do not have uniqueness unless $n = 1$. Hence, the variants of both 0-1-Consistency$(S_1, \ldots, S_4)$ and 0-1-Uniqueness$(S_1, \ldots, S_4)$ where the constraints for $k = 3, 4$ are replaced by the inequalities

$$\sum_{\substack{i,j \in N \\ i\sigma_{k,2} - j\sigma_{k,1} = l}} \beta_{i,j} \leq 1 \quad \text{for } l \in T_k$$

are clear.

If $s_1 = (1, 0)^T$, $s_2 = (0, 1)^T$, $s_3, \ldots, s_m$ are arbitrary, but z_1, z_2 are the all 1's vectors in $\mathbb{R}^n$ we are actually asking for particular permutation matrices. So, with $\mathcal{P}_n$ denoting the subset of $\mathcal{B}_n$ of all permutation matrices we are led to the following problem.

Permutation$(S_3, \ldots, S_m)$.

Instance: $n \in \mathbb{N}$, *and for* $k \in M \setminus \{1, 2\}$ *and* $l \in T_k$, $\zeta_{k,l} \in N \cup \{0\}$.

Task: *Decide, whether there is a permutation* $B \in \mathcal{P}_n$ *such that*

$$\sum_{\substack{i,j \in N \\ i\sigma_{k,2} - j\sigma_{k,1} = l}} \beta_{i,j} = \zeta_{k,l} \quad \text{for } k \in M \setminus \{1, 2\} \text{ and } l \in T_k.$$

We will prove the following result in Section 3.

Theorem 2. *Let* $s_3 = (1, 1)^T$ *or* $s_3 = (-1, 1)^T$*. Then* Permutation(S_3) *is* $\mathbb{NP}$*-complete.*

The theorem shows that checking whether there exists a permutation matrix with prescribed diagonal sums is $\mathbb{NP}$-complete. In terms of a theorem for larger m note that Theorem 1 implies a hardness result for the following problem where in addition to the data and requirements of Permutation$(S_3, \ldots, S_m)$ a permutation submatrix is prescribed already.

PrescribedPermutation($S_3, \dots, S_m$).

Instance: $n \in \mathbb{N}$, *and for* $k \in M \setminus \{1, 2\}$ *and* $l \in T_k$, $\zeta_{k,l} \in N \cup \{0\}$, *sets* $F_1, F_2 \subset N$ *with* $|F_1| = |F_2|$ *a permutation matrix* $P = (\pi_{i,j})_{i \in F_1, j \in F_2}$.

Task: *Decide, whether there is a permutation* $B = (\beta_{i,j})_{i,j \in N} \in \mathcal{P}_n$ *such that*

$$\beta_{i,j} = \pi_{i,j} \quad \text{for } i \in F_1 \text{ and } j \in F_2$$

and

$$\sum_{\substack{i,j \in N \\ i\sigma_{k,2} - j\sigma_{k,1} = l}} \beta_{i,j} = \zeta_{k,l} \quad \text{for } k \in M \setminus \{1, 2\} \text{ and } l \in T_k.$$

In fact, 0-1-Consistency($S_1, \dots, S_m$) may be polynomially transformed to PrescribedPermutation($S_3, \dots, S_m$). If in a given instance of 0-1-Consistency($S_1, \dots, S_m$), $\|z_1\|_{(1)} = \|z_2\|_{(1)} = r$ we may choose and then prescribe any $(n-r) \times (n-r)$ permutation matrix P within the submatrix of the rows and columns specified to 0 in the given instance and then increase the $\zeta_{k,l}$ accordingly. Hence we obtain the following corollary that, when applied to $s_3 = (1, 1)^T$ and $s_4 = (1, -1)^T$, may be seen as being in partial contrast to the results on the queens' problem.

Corollary 3. *Let* $m \geq 3$ *and* $(1, 0)^T$, $(0, 1)^T$ *and* $s_3, \dots, s_m \in \mathbb{Z}^2$ *be linearly independent. Then* PrescribedPermutation($S_3, \dots, S_m$) *is* $\mathbb{NP}$*-complete.*

Naturally, all our results can also be interpreted in terms of contingency tables, (perfect) matchings in bipartite graphs and in terms of representatives of set systems. As to the realm of discrete tomography, both Theorems 1 and 2 strengthen results of [4]. In particular, Theorem 1 shows that for $m \geq 3$ the corresponding hardness result of [4] persists in the 'fully combinatorial' case i.e., when all instances are restricted to those which are binary.

Further note that in the fully binary case the intersection of any solution with any line parallel to any of the given directions $s_1, \dots, s_m$ is empty or a singleton, hence every solution is *convex* in any of the tomographic directions. Also, by considering the 'photographic negative' i.e., by replacing each 0 in a solution by 1 and vice versa, and adjusting the constraints accordingly, we see that the general reconstruction problem (with nonnegative integer constraints) for binary images is also $\mathbb{NP}$-hard for $m \geq 3$ if all solutions are required to be connected with respect to the (so-called p_8-) neighborhood where two points are adjacent if both coordinates differ by at most 1 in absolute value.

The paper is organized as follows. Section 2 gives the proof of Theorem 1, Section 3 contains the proof of Theorem 2 while Section 4 gives some final remarks that place our results into further perspective.

To eliminate a possible source of confusion, let us finally remark that a preprint version of this paper has already been quoted by several authors under the preliminary title 'On the reconstruction of permutation and partition matrices under tomographic constraints'.

2. A passage through higher dimensions

The proof of Theorem 1 builds on a known hardness result for 3-dimensional contingency tables and proceeds in two steps. First we show that for $m \geq 3$ it is $\mathbb{NP}$-hard to decide whether there exists an m-dimensional matrix with given row sums in all m 'index-directions'. Then we develop a projection technique to transform this problem to 0-1-Consistency($S_1, \dots, S_m$). As will be shown the overall reduction is polynomial-time and preserves uniqueness.

2.1. The m-dimensional consistency problem is $\mathbb{NP}$*-complete*

For $n \in \mathbb{N}$ let $\mathcal{B}_n^m$ denote the set of all m-dimensional binary matrices $B = (\beta_x)_{x \in N^m}$ of size n i.e., $B : N^m \to \{0, 1\}$ and $\beta_x = B(x)$. Further, for $k \in N$ set

$$H_k = N^{k-1} \times \{0\} \times N^{m-k}, \qquad L_k = \{0\}^{k-1} \times N \times \{0\}^{m-k}.$$

Then we are dealing with the following problems.

0-1-Consistency$_m$.

Instance: $n \in \mathbb{N}$, *and for* $k \in M$ *and* $y \in H_k$, $\zeta_y \in \{0, 1\}$.

Task: *Decide, whether there exists* $B \in \mathcal{B}_n^m$ *such that*

$$\sum_{x \in y + L_k} \beta_x = \zeta_y \quad \text{for } k \in N \text{ and } y \in H_k.$$

0-1-Uniqueness$_m$ is defined analogously. Note that for $s_1 = (1, 0)^T$ and $s_2 = (0, 1)^T$, 0-1-Consistency(S_1, S_2) coincides with 0-1-Consistency$_2$. Hence, again, the case $m = 2$ is easy. However, Irving & Jerrum [9] showed that both, 0-1-Consistency$_3$ and 0-1-Uniqueness$_3$, are $\mathbb{NP}$-complete. Note that [2] gave a related $\mathbb{NP}$-hardness result, involving, however, in part inequalities rather than equations. We will now give a polynomial-time transformation from 0-1-Consistency$_m$ to 0-1-Consistency$_{m+1}$ that preserves uniqueness.

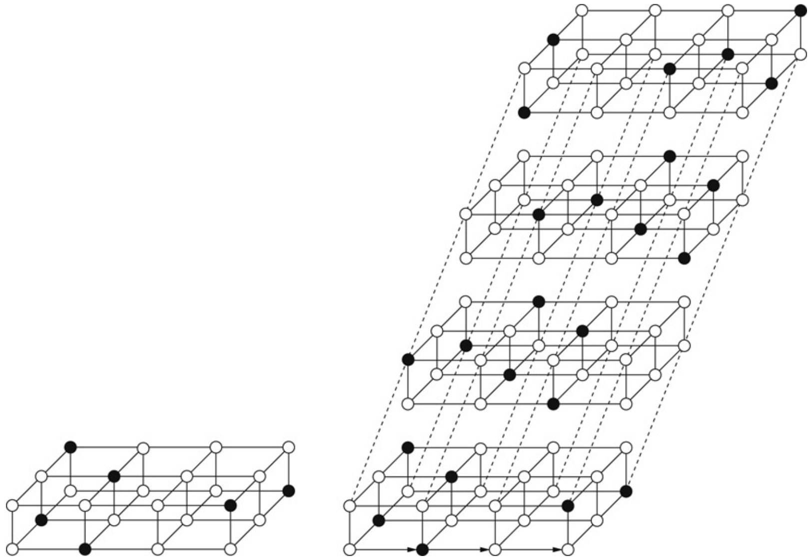

Fig. 1. Transforming 0-1-Consistency$_3$ (left) to 0-1-Consistency$_4$ (right) by cyclic shifts of the planes perpendicular to the e_1-axis. The dashed lines indicate the fourth dimension. Note that on all dashed lines exactly one point is chosen. (For clarity, not all such lines are depicted.)

Theorem 4. *Let $m \geq 3$. Then there is a polynomial-time transformation from* 0-1-Consistency$_m$ *to* 0-1-Consistency$_{m+1}$ *that preserves uniqueness.*

Proof. For $i, d \in \mathbb{N}$ with $i \leq d$ in the following let e_i denote the ith standard unit vector of $\mathbb{R}^d$.

Let an instance $\mathcal{I}_m$ of 0-1-Consistency$_m$ be given, specified by $n \in \mathbb{N}$, and $\zeta_y \in \{0, 1\}$ for $k \in M$ and $y \in H_k$. Further let for $k \in M$

$$C_k = \{y \in H_k : \zeta_y = 1\}, \quad R = \bigcap_{k \in M} C_k + L_k.$$

Then every solution $B \in \mathcal{B}_n^m$ has entries 0 for all components outside of R.

One may be tempted to simply add a 'photographically negative' copy of the given instance as a second layer and set the tomographic constraints in the direction e_{m+1} to 1 on $N^m \times \{0\}$. This is, however, not suitable since the other m sets of tomographic constraints for that second layer would then have values in $\{N - 1, N\}$.

In order to guarantee binary constraints as needed in 0-1-Consistency$_{m+1}$, we will need to resort to a more involved construction. In fact, the construction of an equivalent instance of 0-1-Consistency$_{m+1}$ will be based on stacked images of R that are obtained by permuting the sets $ie_1 + H_1$ for $i \in N$; see Fig. 1. More specifically, let π be a cyclic permutation on N. Note that π induces a bijection $\sigma : N^m \to N^m$ via

$$x = (\xi_1, \ldots, \xi_m)^T \mapsto \sigma(x) = \left(\pi(\xi_1), \xi_2, \xi_3, \ldots, \xi_m\right)^T.$$

The corresponding bijection for the ith iteration π^i will be denoted by σ^i and its inverse by σ^{-i}. Also, N^m will be identified with the subset $N^m \times \{1\}$ of N^{m+1}. Then, for $i \in N$ and $z = (u^T, i)^T \in H_k \times \{i\}$, we set $y = \sigma^{-i+1}(u)$ and

$$\theta_z = \begin{cases} \zeta_u & : \text{ for } k = 1; \\ \zeta_y & : \text{ for } k \in M \setminus \{1\}. \end{cases}$$

For the final direction let

$$K = \bigcup_{i=0}^{n-1} \sigma^i(R), \quad \theta_z = 1 \quad \text{for } z \in K \times \{0\}.$$

Setting all other values θ_z to 0 we obtain an instance $\mathcal{I}_{m+1}$ of 0-1-Consistency$_{m+1}$. Fig. 1 gives an example for $m = 3$. Clearly, the construction is polynomial.

Given a solution $C \in \mathcal{B}_n^{m+1}$ for $\mathcal{I}_{m+1}$, the submatrix of all entries with last index 1 is, of course, a solution B for $\mathcal{I}_m$.

So, let $B = (\beta_x)_{x \in N^m}$ be a solution for $\mathcal{I}_m$, and let $A_m = \{x \in N^m : \beta_x = 1\}$. Now, set

$$A_{m+1} = \left\{(\sigma^{i-1}(x)^T, i)^T : x \in A_m,\ i \in N\right\},$$

and let $C = (\gamma_x)_{x \in N^{m+1}} \in \mathcal{B}_n^{m+1}$ be the matrix with entries 1 precisely for the indices in A_{m+1}. By construction, we have for $k \in M$

$$\sum_{x \in z + L_k \times \{0\}} \gamma_x = \theta_z \quad \text{for each } z \in H_k \times N.$$

Also, since K is the disjoint union of all the sets $\sigma^i(A_m)$ for $i \in N$,

$$\sum_{x \in z+\{0\}^m \times N} \gamma_x = \theta_z \quad \text{for each } z \in N^m \times \{0\}.$$

Finally note that from each of the n submatrices with fixed last index $i \in N$, the whole matrix C can be uniquely reconstructed. Hence C is unique if and only if B has this property. □

As a simple consequence of [9] and Theorem 4 we obtain the following corollary.

Corollary 5. *For $m \geq 3$, 0-1-*Consistency$_m$ *and* 0-1-Uniqueness$_m$ *are $\mathbb{NP}$-complete.*

2.2. *Projecting down to* 0-1-Consistency$(S_1, \ldots, S_m)$

Next we develop a projection technique that allows us to transform 0-1-Consistency$_m$ to 0-1-Consistency$(S_1, \ldots, S_m)$. The decisive issue is, of course, to avoid unwanted intersections of lines parallel to $S_1, \ldots, S_m$ that would mess up the setting. Note that this could easily be done if $s_1, \ldots, s_m$ were part of the input. Then one could choose the directions 'skew enough'. Here, however, $s_1, \ldots, s_m$ are given beforehand and the directions have to be taken as they are. Further note that due to the fact that all tomographic constraints are binary, the reduction techniques of [4] cannot be applied. Hence we need a technically more involved construction. The key arguments are given in Lemma 6.

In the following, we assume that $m \geq 3$, and that $s_1, \ldots, s_m$ are linearly independent. For notational convenience we also assume (without loss of generality) that $s_k = e_k$ for $k = 1, 2$.

Let $\mathcal{I}_m$ be an instance of 0-1-Consistency$_m$, specified by $n \in \mathbb{N}$, and $\zeta_y \in \{0, 1\}$ for $k \in M$ and $y \in H_k$. The idea is to first replace $\mathcal{I}_m$ by a sparser instance and then apply the linear mapping $\varphi : \mathbb{R}^m \to \mathbb{R}^2$ given by $\varphi(e_k) = s_k$ for $k \in M$. Note that, since $s_1 = e_1, s_2 = e_2$, when restricted to $\mathbb{R}^2 \times \{0\}^{m-2}$, the map φ acts as the identity on $\mathbb{R}^2$. Now, set

$$\mu = \max_{i \in M, j \in \{1,2\}} |\sigma_{i,j}|, \qquad \rho = 2\mu^2 n + 1.$$

Further, let $\psi : \mathbb{R}^m \to \mathbb{R}^m$ be the linear map defined by $\psi(e_k) = \rho^{k-1} e_k$ for $k \in M$, let $p = \rho^{m-1} n$, $P = \{1, \ldots, p\}$, and let $\Lambda : \mathcal{B}_n^m \to \mathcal{B}_p^m$ be defined by $B = (\beta_x)_{x \in N^m} \mapsto (\gamma_y)_{y \in P^m}$ with

$$\gamma_y = \begin{cases} \beta_x & \text{if } x \in N^m \text{ and } y = \psi(x); \\ 0 & \text{else.} \end{cases}$$

Clearly, ψ and Λ are injections. Let

$$H'_k = P^{k-1} \times \{0\} \times P^{m-k}, \quad L'_k = \{0\}^{k-1} \times P \times \{0\}^{m-k}.$$

By expanding the given right-hand sides from H_k to H'_k by setting

$$\theta_y = \begin{cases} \zeta_x & \text{if } x \in N^m \text{ and } y = \psi(x); \\ 0 & \text{else,} \end{cases}$$

we obtain an instance $\mathcal{I}'$ of 0-1-Consistency$(S_1, \ldots, S_m)$ equivalent to $\mathcal{I}_m$. In particular, $B \in \mathcal{B}_n^m$ is a solution of $\mathcal{I}_m$ if and only if $\Lambda(B)$ is a solution of $\mathcal{I}'$.

Next we will show that $\varphi(\psi(N^m)) = G$, where

$$G = \bigcap_{k=1}^{m} \bigcup_{y \in \psi(N^m)} \varphi(y) + S_k = \bigcup_{y_1, \ldots, y_m \in \psi(N^m)} \bigcap_{k=1}^{m} \varphi(y_k) + S_k.$$

Note that $G \subset \mathbb{N}^2$.

Lemma 6. *φ is injective on $\psi(N^m)$, $\varphi(\psi(N^m)) = G$, and $\rho^{m-1} = O(n^{m-1})$.*

Proof. The last statement is clear since $\rho^{m-1} = (2n\mu^2 + 1)^{m-1} = O(n^{m-1})$.

Next, we show injectivity of φ on $\psi(N^m)$. So, let $x = (\xi_1, \ldots, \xi_m)^T, x' = (\xi'_1, \ldots, \xi'_m)^T \in N^m$ with $\varphi(\psi(x)) = \varphi(\psi(x'))$. Then

$$\varphi(\psi(x - x')) = \sum_{k=1}^{m} \rho^{k-1}(\xi_k - \xi'_k) s_k = 0,$$

hence

$$\sum_{k=1}^{m} \rho^{k-1}(\xi_k - \xi'_k)\sigma_{ki} = 0 \quad \text{for } i = 1, 2.$$

Since $x, x', s_1, \ldots, s_m$ are integer vectors, ρ is integral, and

$$|(\xi_k - \xi_k')\sigma_{ki}| \le \mu n \le \rho - 1 \quad \text{for } k = 1, \ldots, m \text{ and } i = 1, 2,$$

it follows that

$$(\xi_k - \xi_k')\sigma_{ki} = 0 \quad \text{for } k = 1, \ldots, m \text{ and } i = 1, 2.$$

Since $s_1, \ldots, s_m \neq 0$, we can conclude that $x = x'$.

Finally, we turn to the assertion that $\varphi(\psi(N^m)) = G$. Since quite obviously $\varphi(\psi(N^m)) \subseteq G$, the main part of the proof is to show that $\varphi(\psi(N^m)) \supseteq G$.

Let

$$C = (s_1, \ldots, s_m), \quad a_i^T = t_i^T C.$$

Then

$$\ker(\varphi) = \ker(C), \quad \ker(\varphi) + \mathbb{R}e_i = \{x \in \mathbb{R}^m : a_i^T x = 0\},$$

are of codimensions 2 and 1, respectively.

Now, consider $g \in G$, and let $y_1, \ldots, y_m \in \psi(N^m)$ and $\lambda_1, \ldots, \lambda_m \in \mathbb{R}$ with

$$g = \varphi(y_i) + \lambda_i s_i \quad \text{for } i \in M.$$

In particular, the system

$$\varphi(y) = \varphi(y_i) + \lambda_i s_i \quad \text{for } i \in M$$

is feasible. Hence there is a vector $y \in \mathbb{R}^m$ with

$$y - y_i \in \mathbb{R}e_i + \ker(\varphi) \quad \text{for } i \in M,$$

whence the linear system

$$a_i^T y = a_i^T y_i \quad \text{for } i \in M$$

is feasible. Note that

$$a_1 = (0, -1, t_1^T s_3, \ldots, t_1^T s_m)^T, \quad a_2 = (1, 0, t_2^T s_3, \ldots, t_2^T s_m)^T$$

are linearly independent, and the rank of $(a_1, \ldots, a_m)$ is 2; therefore we have

$$a_i^T = t_i^T s_1 a_2^T - t_i^T s_2 a_1^T \quad \text{for } i \in M.$$

Thus the linear system is feasible, if and only if,

$$t_i^T s_1 a_2^T y_2 - t_i^T s_2 a_1^T y_1 = a_i^T y_i \quad \text{for } i \in M \setminus \{1, 2\},$$

or, equivalently,

$$t_i^T s_1 t_2^T C y_2 - t_i^T s_2 t_1^T C y_1 = t_i^T C y_i \quad \text{for } i \in M \setminus \{1, 2\}.$$

With $y_i = \psi(x_i) = (\rho^0 \xi_{i,1}, \ldots, \rho^{m-1}\xi_{i,m})^T$ the condition reads explicitly

$$\sum_{j \in M} \rho^{j-1}\big(\sigma_{i,2}\sigma_{j,1}(\xi_{2,j} - \xi_{i,j}) - \sigma_{i,1}\sigma_{j,2}(\xi_{1,j} - \xi_{i,j})\big) = 0 \quad \text{for } i \in M \setminus \{1, 2\}.$$

Since

$$\left|\sigma_{i,2}\sigma_{j,1}(\xi_{2,j} - \xi_{i,j}) - \sigma_{i,1}\sigma_{j,2}(\xi_{1,j} - \xi_{i,j})\right| \le 2\mu^2 n = \rho - 1,$$

this is equivalent to

$$\sigma_{i,2}\sigma_{j,1}(\xi_{2,j} - \xi_{i,j}) - \sigma_{i,1}\sigma_{j,2}(\xi_{1,j} - \xi_{i,j}) = 0 \quad \text{for } i \in M \setminus \{1, 2\} \text{ and } j \in M.$$

Note that $\sigma_{i,1}, \sigma_{i,2} \neq 0$ for $i \ge 3$. Hence, for $j = 1$ and $j = 2$ we conclude

$$\xi_{i,1} = \xi_{2,1}, \quad \xi_{i,2} = \xi_{1,2} \quad \text{for all } i \ge 3.$$

Now, let $j \ge 3$. Then, for $i = j$ we obtain

$$\sigma_{j,1}\sigma_{j,2}(\xi_{2,j} - \xi_{1,j}) = 0,$$

thus

$$\xi_{1,j} = \xi_{2,j} \quad \text{for } j \in M \setminus \{1, 2\}.$$

If, on the other hand, $i \neq j$ then

$$\sigma_{i,2}\sigma_{j,1}(\xi_{2,j} - \xi_{i,j}) - \sigma_{i,1}\sigma_{j,2}(\xi_{1,j} - \xi_{i,j}) = (\xi_{i,j} - \xi_{1,j}) \det(s_i, s_j) = 0,$$

hence

$$\xi_{i,j} = \xi_{1,j} \quad \text{for } i, j \in M \setminus \{1, 2\} \text{ and } i \neq j.$$

Summarizing, the vector $x = (\xi_1, \dots, \xi_m)^T \in N^m$ given by

$$\xi_i = \xi_{i,j_0} \quad \text{for } i, j_0 \in M \text{ and } i \neq j_0$$

is well defined, and we see that

$$x_i \in x + \mathbb{R}e_i \quad \text{for } i \in M,$$

i.e., $\varphi\big(\psi(x)\big) = g$.

This completes the proof of the lemma. □

We are now ready to provide the asserted polynomial-time transformation from 0-1-Consistency$_m$ to 0-1-Consistency$(S_1, \dots, S_m)$ and from 0-1-Uniqueness$_m$ to 0-1-Uniqueness$(S_1, \dots, S_m)$.

Theorem 7. *There is a polynomial-time parsimonious transformation from* 0-1-Consistency$_m$ *to* 0-1-Consistency$(S_1, \dots, S_m)$.

Proof. The statement is trivial for $m = 2$; so let $m \geq 3$. Let $\mathcal{I}_m$ be an instance of 0-1-Consistency$_m$, specified as usual by $n \in \mathbb{N}$, and $\zeta_y \in \{0, 1\}$ for $k \in M$ and $y \in H_k$.

Further let $\mu, \rho \in \mathbb{N}$, $\varphi : \mathbb{R}^m \to \mathbb{R}^2$, $\psi : \mathbb{R}^m \to \mathbb{R}^m$ and $G \subset \mathbb{N}^2$ be defined as before.

Note that, as we have seen, every point $g = (\gamma_1, \gamma_2)^T \in G$ is of the form $g = \sum_{i=1}^m \rho^{i-1}\kappa_i s_i$ with $\kappa_i \in N$. Hence we have for $i = 1, 2$

$$1 \leq \gamma_i \leq \rho^{m-1} \sum_{l=1}^{m} \kappa_l \, |\sigma_{l,i}| \leq \rho^{m-1} \cdot m \cdot n \cdot \mu.$$

So, with $q = nm\mu\rho^{m-1}$ and $Q = \{1, \dots, q\}$ we have $G \subset Q^2$. The corresponding instance $\mathcal{I}'$ of 0-1-Consistency$(S_1, \dots, S_m)$ will therefore live on Q^2. With $T_k = \{t_k^T g : g \in Q^2\}$ for $k \in M$ it remains to set $\zeta_{k,l}$ to 0 or 1 for each $k \in M$ and $l \in T_k$. Of course, it suffices to specify those lines parallel to S_k which correspond to a right-hand side $\zeta_{k,l} = 1$. But these are precisely the lines

$$\varphi\big(\psi(x)\big) + S_k \quad \text{for } x \in H_k \text{ and } \zeta_x = 1.$$

It follows from Lemma 6 that $\mathcal{I}_m$ is a yes-instance of 0-1-Consistency$_m$ if and only if $\mathcal{I}'$ is a yes-instance of 0-1-Consistency$(S_1, \dots, S_m)$, and actually that the solutions of $\mathcal{I}$ and $\mathcal{I}'$ are in one-to-one correspondence. □

With Theorems 4 and 7 the $\mathbb{NP}$-hardness of 0-1-Consistency$(S_1, \dots, S_m)$ and 0-1-Uniqueness$(S_1, \dots, S_m)$ for $m \geq 3$ follows now directly from that of 0-1-Consistency$_3$ and 0-1-Uniqueness$_3$. This completes the proof of Theorem 1.

3. Diagonally constrained permutations

In this section we prove Theorem 2 showing the $\mathbb{NP}$-hardness of Permutation(S_3) for $s_3 = (-1, 1)^T$; the statement for $s_3 = (1, 1)^T$ follows by rotation about 90°. So, here we have $T = T_3 = \{i + j : i, j \in N\} = \{2, 3, \dots, 2n\}$. Hence an instance of Permutation(S_3) is specified by $n \in \mathbb{N}$, and numbers $\zeta_2, \zeta_3, \dots, \zeta_{2n} \in N \cup \{0\}$, and the task is to decide, whether there is a permutation $B \in \mathcal{P}_n$ such that

$$\sum_{\substack{i,j \in N \\ i+j=l}} \beta_{i,j} = \zeta_l \quad \text{for } l = 2, 3, \dots, 2n.$$

The hardness will be shown via a reduction from the following restricted version of NumericalMatchingWithTargetSums (NMTS).

RestrictedNumericalMatchingWithTargetSums (RNMTS).

Instance:	$n \in \mathbb{N}$, *and* $\gamma_1, \dots, \gamma_n \in \mathbb{Z}$ *with* $2 \leq \gamma_1 \leq \gamma_2 \leq \cdots \leq \gamma_n \leq 2n$ *and* $\sum_{i=1}^n \gamma_i = n(n+1)$.
Task:	*Decide whether there exist permutations* σ *and* π *on* N *such that* $\sigma(k) + \pi(k) = \gamma_k$ *for* $k \in N$.

RNMTS was shown to be $\mathbb{NP}$-complete by Yu [11]. It is, however, not known whether RNMTS is still $\mathbb{NP}$-hard when the instances are restricted to those with $\gamma_1 < \gamma_2 < \cdots < \gamma_n$; see [5] for more information about NMTS.

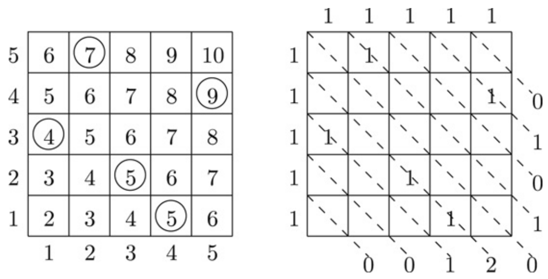

Fig. 2. An example for the transformation.

Let $\mathcal{I} = (n; \gamma_1, \ldots, \gamma_n)$ be an instance of RNMTS. Our transformation is based on the observation that $\mathcal{I}$ can be interpreted in terms of an addition table for the numbers $1, \ldots, n$. More precisely, let $A = (\alpha_{i,j})_{i,j\in N}$ be the $n \times n$ matrix with $\alpha_{i,j} = i + j$ (ordered according to our general convention). Then $\mathcal{I}$ is a yes-instance if and only if for each element γ_k an element $\alpha_{i,j}$ exists with $\alpha_{i,j} = \gamma_k$ such that all chosen entries are in different rows and columns. Hence the positions of these entries form a permutation matrix.

Fig. 2 (left) gives the example $\mathcal{I} = (5; 4, 5, 5, 7, 9)$ with $n = 5$. The selected entries are encircled. The underlying permutation matrix is depicted on the right, and $\sigma = (1, 3, 4, 2, 5)$, $\pi = (3, 2, 1, 5, 4)$. The numbers associated with the diagonals correspond to the numbers of different k for which $\gamma_k = l$ for $l = 2, 3, \ldots, 10$.

So, in general, we obtain an instance $\mathcal{I}'$ of PERMUTATION(S_3) on the same number n by setting

$$\zeta_l = \left|\{k \in N : \gamma_k = l\}\right| \quad \text{for } l = 2, \ldots, 2n.$$

Now, suppose, that $\mathcal{I}$ is a yes-instance and let σ and π be the corresponding permutations. We define the matrix $B = (\beta_{i,j})_{i,j\in N}$ by setting

$$\beta_{\sigma(k),\pi(k)} = 1 \quad \text{for } k \in N$$

and $\beta_{i,j} = 0$ otherwise. Then B is a solution for $\mathcal{I}'$.

Conversely, let $B \in \mathcal{P}_n$ be a solution of $\mathcal{I}'$, and let $\{(i_k, j_k) : k \in N\}$ be the set of index pairs for which $\beta_{i_k,j_k} = 1$ ordered so that $i_k + j_k \leq i_{k+1} + j_{k+1}$ for $k = 1, \ldots, n-1$. Let the permutations σ and π be defined by

$$\sigma(k) = i_k, \quad \pi(k) = j_k \quad \text{for } k \in N.$$

Then, of course, $\sigma(k) + \pi(k) = \gamma_k$.

Note that the transformation is polynomial. This completes the proof of Theorem 2.

4. Final remarks

Our results extend known more 'numerical' hardness results to the purely combinatorial case. One might wonder whether this can be further extended to inverse problems involving higher-dimensional slices of matrices. The following example associated with Radon-transforms will show that this is not the case in general. It is concerned with 3-dimensional matrices with prescribed sums over all three coordinate *planes*.

RADON$_3$.

Instance: $n \in \mathbb{N}$, $\xi_i, \eta_j, \zeta_k \in \mathbb{N}_0$ *for* $i, j, k \in N$.

Task: *Decide whether there is a matrix* $B = (\beta_{i,j,k})_{i,j,k\in N} \in \mathcal{B}_3$ *such that*

$$\sum_{j=1}^{n}\sum_{k=1}^{n} \beta_{i,j,k} = \xi_i \quad \text{for } i \in N$$

$$\sum_{i=1}^{n}\sum_{k=1}^{n} \beta_{i,j,k} = \eta_j \quad \text{for } j \in N$$

$$\sum_{i=1}^{n}\sum_{j=1}^{n} \beta_{i,j,k} = \zeta_k \quad \text{for } k \in N.$$

Of course, this problem can easily been extended to higher dimensions and to sums over other kinds of spaces. As is shown in [1] and [7] RADON$_3$ is $\mathbb{NP}$-complete, and so are higher-dimensional versions thereof.

The fully combinatorial problem 0-1-RADON$_3$, however, that is obtained from RADON$_3$ by restricting the input to $\xi_i, \eta_j, \zeta_k \in \{0, 1\}$ for $i, j, k \in N$ is trivial. In fact, there is a solution if and only if

$$\sum_{i\in N} \xi_i = \sum_{j\in N} \eta_j = \sum_{k\in N} \zeta_k.$$

If this condition is satisfied the task is restricted to those coordinate planes for which the right-hand side is 1. Hence, in the projection to the plane spanned by e_1, e_2 we only need to find a permutation, and a solution to the given instances is obtained by lifting the entries 1 to different heights.

Acknowledgements

The present paper was supported by grant 31-vigoni-dr of the DAAD and grant vigoni-it of the CRUI. We thank the anonymous referees for some helpful remarks.

References

[1] S. Brunetti, A. Del Lungo, Y. Gerard, On the computational complexity of determining three dimensional lattice sets from their three dimensional X-rays, Linear Algebra Appl. 339 (2001) 59–73.
[2] S. Even, A. Itai, A. Shamir, On the complexity of timetable and multicommodity flow problems, SIAM. J. Comput. 5 (1976) 691–703.
[3] B.-J. Falkowski, L. Schmitz, A note on the queen's problem, Inform. Process. Lett. 23 (1986) 39–43.
[4] R.J. Gardner, P. Gritzmann, D. Prangenberg, On the computational complexity of reconstructing lattice sets from their X-rays, Discrete Math. 202 (1999) 45–71.
[5] M.R. Garey, D.S. Johnson, Computers and Intractability: A Guide to the Theory of NP-completeness, Freeman, New York, 1979, 224.
[6] P. Gritzmann, On the reconstruction of finite lattice sets from their X-rays, in: Lecture Notes on Computer Science, vol. 1347, Springer, 1997, pp. 19–32.
[7] P. Gritzmann, S. de Vries, On the algorithmic inversion of the discrete Radon transform, Theoret. Comput. Sci. 281 (2002) 455–469.
[8] G.T. Hermann, A. Kuba (Eds.), Discrete Tomography: Foundations, Algorithms and Applications, Birkhauser Boston, Cambridge, MA, 1999.
[9] R.W. Irving, M.R. Jerrum, Three-dimensional statistical data security problems, SIAM J. Comput. 23 (1994) 170–184.
[10] H. Ryser, Combinatorial Mathematics, The Carus Mathematical Monographs, vol. 14, Math. Assoc. America, 1963.
[11] Wenci Yu, The two-machine flow shop problem with delays and the one-machine total tardiness, Ph.D. Thesis, Eindhoven University of Technology, 1996. http://alexandria.tue.nl/extra3/proefschrift/PRF12A/9602054.pdf.