A PROBABILISTIC APPROACH TO THE DYCHOTOMY PROBLEM

TOMASZ ŁUCZAK AND JAROSLAV NEŠETŘIL

ABSTRACT. Let $\mathcal{R}(n,k)$ denote the random k-ary relation defined on the set $[n] = \{1, 2, \ldots, n\}$. We show that the probability that $([n], \mathcal{R}(n,k))$ is projective tends to one, as either n or k tends to infinity. This result implies that for most relational systems $(B, \underline{R})$ the CSP$(B, \underline{R})$ problem is NP-complete, and confirms a conjecture of Rosenberg [11].

1. INTRODUCTION

Let $\Delta = (\delta_i)_{i \in I}$ be a finite sequence of positive integers. A *relational system of type* Δ is a pair $(A, \underline{R})$, where A is a finite set, $\underline{R} = (R_i)_{i \in I}$, and R_i is a δ_i-ary relation on A, i.e., $R_i \subseteq A^{\delta_i}$, for $i \in I$. If $(A, \underline{R})$, $(A', \underline{R}')$ are relational systems of the same type $\Delta = (\delta_i)_{i \in I}$, then by *homomorphism* from $(A', \underline{R}')$ to $(A'', \underline{R}'')$ we mean a map $f : A' \to A''$ such that for every $i \in I$, we have $(f(x_1), \ldots f(x_{\delta_i})) \in R''_i$ whenever $(x_1, \ldots, x_{\delta_i}) \in R'_i$.

Relational structures and homomorphisms express various decision and counting combinatorial problems such as colouring, satisfiability, and linear algebra problems. Many of them can be reduced to special cases of a general Constraint Satisfaction Problem CSP$(B, \underline{R})$ which, in the language of homomorphisms, can be stated as follows: *given a target relational system* $(B, \underline{R})$ *of type* Δ*, and a relational system* $(A, \underline{R}')$ *of the same type, decide if there exists a homomorphism* $f : A \to B$. A number of such problems have been studied and have known complexity, e.g., when we deal with undirected graphs or the problem is restricted to small sets A (see [3, 6, 12]). However at this moment we are very far from understanding the behaviour

Date: September 26, 2003.

Key words and phrases. CSP, projectivity, random relation.

The first author was partially supported by KBN grant 2 P03A 016 23, the second author by a grant LN00A56 of the Czech Ministry of Education.

of CSP$(B,\underline{R})$ problem even for binary relations $(B,\underline{R})$ (i.e., when relational systems of type $\Delta = (2)$).

One of the basic unsolved questions in this area, which remains widely open even for $\Delta = (2)$, is so called 'dichotomy conjecture' [5], which claims that every CSP$(B,\underline{R})$ problem is either NP-complete or polynomially solvable. In this paper we settle in the affirmative a 'probabilistic version' of this problem.

Theorem 1. *Let $\Delta = (\delta_i)_{i\in I}$ be such that $\max_{i\in I}\delta_i \geq 2$. Then CSP$(B,\underline{R})$ is NP-complete for almost all relational systems $(B,\underline{R})$ of type Δ.*

(Note that for $(B,\underline{R})$ of type $(1,1,\dots,1)$ the problem CSP$(B,\underline{R})$ is trivial.)

The paper is organized as follows. In the following section we formulate the main result of the paper, Theorem 3, which states that most of relational systems are strongly rigid, as conjectured by Rosenberg [11]. We also make the formulation of Theorem 1 precise by introducing a notion of random k-ary relation, and remark that Theorem 1 follows from Theorem 3. Then, we introduce 'reach' relations and show that reachness implies projectivity. Finally, in section 4, we prove Theorem 3.

2. Projective and rigid relational system

Let $(A,\underline{R})$ be a relational system of type $\Delta = (\delta_i)_{i\in I}$. By (A^ℓ, R^ℓ) we denote the relational system of type Δ such that for every $i \in I$

$$\big((a_1^1,\dots,a_\ell^1),\dots,(a_\ell^1,\dots,a_\ell^k)\big) \in R_i^\ell$$

if and only if $(a_j^1,\dots,a_j^k) \in R_i$ for each $j = 1,\dots,\ell$. An *operation* (*polymorphism* in [1, 4, 7, 11]) of a relational system (A,R) is a homomorphism $f : A^\ell \to A$ from (A^ℓ, R^ℓ) to (A,R) for some $\ell \geq 1$. Such an operation is *idempotent* if $f(a,\dots,a) = a$ for every $a \in A$, and it is a *projection* (on the jth coordinate), if there exists j, $1 \leq j \leq \ell$, such that for every $(a_1,\dots,a_\ell) \in A^\ell$ we have $f(a_1,\dots,a_\ell) = a_j$. We say that a system (A,R) is *projective* if for every $\ell \geq 1$ every idempotent operation $f : A^\ell \to A$ is a projection (c.f., [8, 9]). The system $(A,\underline{R})$ is *rigid* if the identity mapping is the only homomorphism from A to A, and *strongly rigid* if it is both projective and rigid. It is easy to see that $(A,\underline{R})$ is strongly rigid if and only if for each $\ell \geq 1$ every operation $f : A^\ell \to A$ is a projection.

The notions of projective and rigid relational systems play an important role in investigations of complexity of CSP$(B,\underline{R})$ problems. In particular, it is known that these problems are hard whenever the system $(B, \underline{R})$ is strongly rigid, i.e., the following result holds (see, for instance, [1, 2, 4, 7]).

Theorem 2. *If a relational system $(B, \underline{R})$ is strongly rigid, then the problem CSP$(B, \underline{R})$ is* NP*-complete.* $\square$

Thus, in order to show Theorem 1, it is enough to verify that most of relational systems are strongly rigid. In order to make this statement precise, let $\mathcal{R}(n,k)$ denote a random k-ary relation defined on a set $[n] = \{1, 2, \dots, n\}$, for which the probability that $(a_1, \dots, a_k) \in \mathcal{R}(n,k)$ is equal to $1/2$ independently for each $(a_1, \dots, a_k)$, where $1 \leq a_r \leq n$ for $r = 1, \dots, k$ and not all a_i's are equal; for $a \in [n]$, we put $(a, a, \dots, a) \notin \mathcal{R}(n,k)$. Let $([n], (\mathcal{R}(\delta_i, n)_{i \in I}))$ denote the random relational system of type $\Delta = (\delta_i)_{i \in I}$. We shall show that the probability that $([n], (\mathcal{R}(\delta_i, n)_{i \in I}))$ is strongly rigid tends to one as either n, or $\max_i \delta_i$ tends to infinity. Note that a relational system $(A, \underline{R})$ is strongly rigid, provided for some $i_0 \in I$, the system (A, R_{i_0}) of type (δ_{i_0}) is strongly rigid (although the converse implication, in general, does not hold). Thus, it is enough to prove our result for 'simple' relational systems which consist of just one k-ary relation.

Theorem 3. *For a fixed $k \geq 2$,*

$$\lim_{n \to \infty} \Pr\big(([n], \mathcal{R}(k,n)) \textit{ is strongly rigid}\big) = 1, \tag{1}$$

while for a given $n \geq 2$,

$$\lim_{k \to \infty} \Pr\big(([n], \mathcal{R}(k,n)) \textit{ is strongly rigid}\big) = 1. \tag{2}$$

The proof of Theorem 3 we postpone until section 4. It is based on an argument which is somewhat similar to that used by the authors in [10] to show that almost every graph (i.e., almost every binary symmetric relation) is strongly rigid.

We also remark that (2) settles in the affirmative a conjecture posed by Rosenberg [11].

3. Reach relational systems

Let R be a k-ary relation on a set A. A system (A, R) is *reach* if there exist elements $z_1, \dots, z_{k-2} \in A$ such that for any four different elements $x_1, x_2, y_1, y_2 \in A$, there is a $w \in A$ such that for $r = 1, 2$, we have

$$(z_1, \dots, z_{k-2}, w, x_r) \in R \text{ but } (z_1, \dots, z_{k-2}, w, y_r) \notin R. \tag{3}$$

We shall show that reachness implies projectivity.

Theorem 4. *Each reach system (A,R) with $|A| \geq 5$ is projective.*

Before we prove Theorem 4 we introduce some more notation. Let $f : A^\ell \to A$ be an idempotent operation from A^ℓ to A. For an ℓ-tuple $(a_1,\dots,a_\ell) \in A^\ell$, we set

$$\Xi(a_1,\dots,a_\ell) = \{a \in A : a = a_i \text{ for some } i = 1,2,\dots,\ell\},$$

by $\xi(a_1,\dots,a_\ell) = |\Xi(a_1,\dots,a_\ell)|$ we denote the number of different coordinates of $(a_1,\dots,a_\ell)$, and set

$$\Lambda_f(a_1,\dots,a_\ell) = \{i : f(a_1,\dots,a_\ell) = a_i\}.$$

Hence, for instance, $\Xi(a,\dots,a) = \{a\}$, $\xi(a,\dots,a) = 1$ and, since f is idempotent, $\Lambda_f(a,\dots,a) = \{1,2,\dots,\ell\}$. Our proof of Theorem 4 is based on the following two claims.

Claim 1. *If (A,R) is reach, then for every idempotent operation $f : A^\ell \to A$, and every $(a_1,\dots,a_\ell) \in A^\ell$,*

$$\Lambda_f(a_1,\dots,a_\ell) \neq \emptyset. \tag{4}$$

Proof. We shall use induction on $\xi(a_1,\dots,a_\ell)$. As we have already observed, the fact that f is idempotent implies that $\Lambda_f(a,\dots,a) = \{1,2,\dots,\ell\}$. Let us suppose that the assertion holds for every $(a_1,\dots,a_\ell)$ with at most m, $1 \leq m \leq \ell - 1$, different coordinates, and let $(b_1,\dots,b_\ell)$ be such that $\Xi(b_1,\dots,b_\ell) = \{c_1,\dots,c_{m+1}\}$ and

$$f(b_1,\dots,b_\ell) = d \notin \{c_1,\dots,c_{m+1}\}.$$

Because R is reach one can choose from A elements e_i, $i = 1,\dots,k-2$, and $\bar{c}_j$, $j = 1,\dots,m$, such that for each $j = 1,\dots,m$, we have

$$(e_1,\dots,e_{k-2},\bar{c}_j,c_j) \in R \quad \text{but} \quad (e_1,\dots,e_{k-2},\bar{c}_j,d) \notin R,$$

and

$$(e_1,\dots,e_{k-2},\bar{c}_m,c_{m+1}) \in R.$$

For $i = 1,2,\dots,\ell$, define

$$\bar{b}_i = \begin{cases} \bar{c}_j & \text{if} \quad b_i = c_j \text{ for some } j = 1,\dots,m, \\ \bar{c}_m & \text{if} \quad b_i = c_{m+1}. \end{cases}$$

Then $\xi(\bar{b}_1,\dots,\bar{b}_\ell) = m$ and so, by the inductional assumption, for some $s_0 = 1,\dots,m$, we have $f(\bar{b}_1,\dots,\bar{b}_\ell) = \bar{c}_{s_0}$. Note however that the k-tuple

$$\big((e_1,\dots,e_1),(e_2,\dots,e_2),\dots,(e_{k-2},\dots,e_{k-2}),(\bar{b}_1,\dots,\bar{b}_\ell),(b_1,\dots,b_\ell)\big)$$

belongs to R^ℓ but its mapped by f into $(e_1,\ldots,e_{k-2},\bar{c}_{s_0},d)$ which, due to the choice of $\bar{c}_{s_0}$, does not belong to R. This contradiction shows that $\Lambda_f(b_1,\ldots,b_\ell)\neq\emptyset$. $\square$

Claim 2. *If (A,R) is reach, then for every idempotent operation $f: A^\ell \to A$, and every pair of ℓ-tuples $(a_1,\ldots,a_\ell)$, $(b_1,\ldots,b_\ell)$, there exists t, $1 \le t \le \ell$, such that*

$$\{a_t,b_t\}\subseteq\{f(a_1,\ldots,a_\ell),f(b_1,\ldots,b_\ell)\}. \tag{5}$$

Proof. Claim 1 implies that $f(a_1,\ldots,a_\ell)=a_{j_1}$, $f(b_1,\ldots,b_\ell)=b_{j_2}$, for some indices j_1, j_2, $1\le j_1,j_2\le\ell$. Since (A,R) is reach one can find elements e_i, $i=1,\ldots,k-2$, and $c_1,\ldots,c_\ell$ such that for each $s=1,\ldots,\ell$,

$$(e_1,\ldots,e_{k-2},c_s,a_s),(e_1,\ldots,e_{k-2},c_s,b_s)\in R \tag{6}$$

but

$$(e_1,\ldots,e_{k-2},c_s,w)\notin R \quad\text{for}\quad w\in\{a_{j_1},b_{j_2}\}\setminus\{a_s,b_s\}. \tag{7}$$

From Claim 1 it follows that $f(c_1,\ldots,c_\ell)=c_t$ for some t, $1\le t\le\ell$. Note also that both k-tuples

$$\big((e_1,\ldots,e_1),\ldots,(e_{k-2},\ldots,e_{k-2}),(c_1,\ldots,c_\ell),(a_1,\ldots,a_\ell)\big)$$

and

$$\big((e_1,\ldots,e_1),\ldots,(e_{k-2},\ldots,e_{k-2}),(c_1,\ldots,c_\ell),(b_1,\ldots,b_\ell)\big)$$

belong to R^ℓ, and so we must have

$$(e_1,\ldots,e_{k-2},c_t,a_{j_1}),(e_1,\ldots,e_{k-2},c_t,b_{j_2})\in R\,.$$

This fact, together with (7), implies that $\{a_t,b_t\}\subseteq\{a_{j_1},b_{j_2}\}$. $\square$

Proof of Theorem 4. Let

$$\hat{A}^\ell=\{(a_1,\ldots,a_\ell)\in A^\ell:\xi(a_1,\ldots,a_\ell)\le 3\}.$$

Let us observe that for some $(a_1,\ldots,a_\ell)\in\hat{A}^\ell$ we have $|\Lambda_f(a_1,\ldots,a_\ell)|=1$. Indeed, take $(a_1,\ldots,a_\ell)\in\hat{A}^\ell$ for which $|\Lambda_f(a_1,\ldots,a_\ell)|$ is minimal. Since, by Claim 1, $|\Lambda_f(a_1,\ldots,a_\ell)|\ge 1$, assume that $j\in\Lambda_f(a_1,\ldots,a_\ell)$. Let $b,b'\in A\setminus\Xi(a_1,\ldots,a_\ell)$ and let

$$c_i=\begin{cases} b & \text{if } i=j\\ b' & \text{if } i\in\Lambda_f(a_1,\ldots,a_\ell)\setminus\{j\},\\ a_j & \text{if } i\notin\Lambda_f(a_1,\ldots,a_\ell).\end{cases}$$

Then $(c_1, \ldots, c_\ell) \in \hat{A}^\ell$, but Claim 2 implies that $\Lambda_f(c_1, \ldots, c_\ell)$ is a proper subset of $\Lambda_f(a_1, \ldots, a_\ell)$. Hence, there is an $(a_1, \ldots, a_\ell) \in A^\ell$ such that $\Lambda_f(a_1, \ldots, a_\ell) = \{t\}$ for some $1 \leq t \leq \ell$.

Let us fix such $(a_1, \ldots, a_\ell)$ and t, pick $b \in A \setminus \Xi(a_1, \ldots, a_\ell)$, and define

$$\bar{a}_i = \begin{cases} b & \text{if } i = t \\ a_i & \text{if } i \neq t. \end{cases}$$

Then, using again Claims 1 and 2, we infer that $\Lambda_f(\bar{a}_1, \ldots, \bar{a}_\ell) = \{t\}$. A similar argument shows that $\Lambda_f(d_1, \ldots, \bar{d}_\ell) = \{t\}$ whenever $(d_1, \ldots, d_\ell)$ belongs to the set $\tilde{A}^\ell \subset \hat{A}^\ell$ which consists of all ℓ-tuples $(d_1, \ldots, d_\ell)$ such that for all $i, j \neq t$ we have $d_i = d_j \neq d_t$.

Now let $(a_1, \ldots, a_\ell)$ be any ℓ-tuple of A^ℓ and suppose that $f(a_1, \ldots, a_\ell) = a_s \neq a_t$, for some s, $1 \leq s \leq \ell$. Consider $(d_1, \ldots, d_\ell) \in \tilde{A}^\ell$ such that

$$d_i = \begin{cases} a_s & \text{if } i = t \\ a_t & \text{if } i \neq s. \end{cases}$$

Then, the pair $(a_1, \ldots, a_\ell)$, $(d_1, \ldots, d_\ell)$ contradicts Claim 2. Consequently, for every $(a_1, \ldots, a_\ell)$ we have $f(a_1, \ldots, a_\ell) = a_t$, and the assertion follows. $\square$

In order to deal with relational systems defined on small sets, we introduce one more definition. Let $2 \leq i \leq k-1$ and (A, R) be a relation system with k-ary relation R. We call (A, R) *i-reach* if (A, R) is reach and there exist elements $z_1, \ldots, z_{k-i-1} \in A$ such that for every two different i-tuples $(x_1, \ldots, x_i)$, $(y_1, \ldots, y_i) \in A^i$, there is a $w \in A$ for which

$$(z_1, \ldots, z_{k-i-1}, w, x_1, \ldots, x_i) \in R \tag{8}$$

but

$$(z_1, \ldots, z_{k-i-1}, w, y_1, \ldots, y_i) \notin R. \tag{9}$$

It turns out that (A, R) is projective also for $|A| \geq 2$ if the assumption of Theorem 4 is slightly strengthened.

Theorem 5. *If (A, R) is 3-reach, then (A, R) is projective.*

The following result which is, in a way, a generalization of Claim 1. can be shown by imitating the proof of Claim 2.

Claim 3. *If (A, R) is i-reach for some $i \geq 2$, then for every set of i ℓ-tuples $(a_1^r, \ldots, a_\ell^r)$, $r = 1, 2, \ldots, i$, we have*

$$\bigcap_{r=1}^{i} \Lambda_f(a_1^r, \ldots, a_\ell^r) \neq \emptyset. \tag{10}$$

Proof. Let us assume that (A, R) is i-reach, and let $(a_1^r, \ldots, a_\ell^r) \in A^\ell$, for $r = 1, \ldots, i$. From Claim 1 it follows that there exist indices j_r, $1 \leq j_r \leq \ell$, such that $\Lambda_f(a_1^r, \ldots, a_\ell^r) = a_{j_r}^r$, for $r = 1, \ldots, i$. Since (A, R) is i-reach one can find elements e_i, $i = 1, \ldots, k-i-1$, and $c_1, \ldots, c_\ell$, such that for each $s = 1, \ldots, \ell$,

$$(e_1, \ldots, e_{k-i-1}, c_s, a_s^1, \ldots, a_s^i) \in R \tag{11}$$

but

$$(e_1, \ldots, e_{k-2}, c_s, a_{j_1}, \ldots, a_{j_i}) \notin R \quad \text{unless} \quad (a_s^1, \ldots, a_s^i) = (a_{j_1}, \ldots, a_{j_i}). \tag{12}$$

Claim 1 implies that $f(c_1, \ldots, c_\ell) = c_t$ for some t, $1 \leq t \leq \ell$. Note that for each $r = 1, 2, \ldots, i$, the k-tuple

$$\big((e_1, \ldots, e_1), \ldots, (e_{k-i-1}, \ldots, e_{k-i-1}), (\bar{c}_1, \ldots, \bar{c}_\ell), \\ (a_1^1, \ldots, a_\ell^1), \ldots, (a_1^i, \ldots, a_\ell^i)\big)$$

belongs to R^ℓ, and so its image under f, equal to $(e_1, \ldots, e_{k-i-1}, c_t, a_{j_1}^1, \ldots, a_{j_i}^i)$, belongs to R. But then (12) implies that $(a_t^1, \ldots, a_t^i) = (a_{j_1}, \ldots, a_{j_i})$, i.e.,

$$t \in \bigcap_{r=1}^{i} \Lambda_f(a_1, \ldots, a_\ell). \qquad \square$$

Proof of Theorem 5. As in the proof of Theorem 4 we show first that for some $(a_1, \ldots, a_\ell) \in A^\ell$ we have $|\Lambda_f(a_1, \ldots, a_\ell)| = 1$.

Indeed, suppose that $|\Lambda_f(a_1, \ldots, a_\ell)| \geq 2$, $j \in \Lambda_f(a_1, \ldots, a_\ell)$, $j \neq j'$, and $b \neq A \setminus \{a_j\}$. Define

$$c_i = \begin{cases} a_i & \text{if } i \neq j, \\ b & \text{if } i = j, \end{cases}$$

and

$$d_i = \begin{cases} a_i & \text{if } i \notin \Lambda_f(a_1, \ldots, a_\ell) \setminus \{j\}, \\ b & \text{if } i \in \Lambda_f(a_1, \ldots, a_\ell) \setminus \{j\}. \end{cases}$$

Then, it is easy to see that

$$\Lambda_f(a_1, \ldots, a_\ell) \cap \Lambda_f(c_1, \ldots, c_\ell) \cap \Lambda_f(d_1, \ldots, d_\ell) = \emptyset,$$

contradicting Claim 3. Thus, for some $(a_1,\dots,a_\ell)\in A^\ell$, we have $\Lambda_f(a_1,\dots,a_\ell)=\{t\}$. Now the assertion follows from Claim 3. $\square$

4. Proof of the main result

Let us start with the following result, which, in fact, gives more than we need.

Lemma 6. *Let $i\ge 2$ be a fixed natural number.*

(i) *For a fixed $k\ge 2$*

$$\lim_{n\to\infty}\Pr\Big(([n],\mathcal{R}(n,k))\ \textit{is } i\textit{-reach}\Big)=1.$$

(ii) *For a fixed $n\ge 2$*

$$\lim_{k\to\infty}\Pr\Big(([n],\mathcal{R}(n,k))\ \textit{is } i\textit{-reach}\Big)=1.$$

Proof. Let $i,k\ge 2$ be fixed and let $z_1,\dots,z_{k-i-1}$ be any given elements of $[n]$, say, $z_r=r$ for $r=1,\dots,k-i-1$. Then, the probability that for given two i-tuples $(x_1,\dots,x_i)$, $(y_1,\dots,y_i)$ for all elements w either (8) or (9) (or (3)) does not hold is bounded from above by $4\cdot 2^{-n}$. Hence the probability that one cannot find a required w, for some of at most n^{2i} possible choices for x's and y's, is smaller than $n^{4i}2^{-n+2}$ and tends to 0 as $n\to\infty$. This proves the first part of the lemma.

In order to show (ii) observe first that there are at most $4n^{4i+1}$ choices for i-tuples $(x_1,\dots,x_i)$, $(y_1,\dots,y_i)$ and $w\in[n]$. The probability that for all these choices and for given $z_1,\dots,z_{k-i-1}$ each of the relations (3), (8), and (9), holds, is bounded from below by $\rho=2^{-4n^{4i+1}}$. But there are $N=n^{k-i-1}$ possible choices for z's and so the number of $(k-i-1)$-tuples $(z_1,\dots,z_{k-i-1})$ for which (3), (8), (9), hold is bounded from below by the random variable Z with binomial distribution $Bi(N,\rho)$. Since $N\to\infty$ as $k\to\infty$ but ρ remains bounded away from 0, with probability tending to 1 as $k\to\infty$, we have $Z>0$. Hence, with probability tending to 1 as $k\to\infty$, there exists a choice of $z_1,\dots,z_{k-i-1}$ for which (3), (8), (9) hold (for all $w\in A$!) and (ii) follows. $\square$

We shall also need to know that the system $([n],\mathcal{R}(n,k))$ typically has no non-trivial endomorphisms.

Lemma 7.

(i) *For a fixed* $k \geq 2$,

$$\lim_{n\to\infty} \Pr\Big(([n], \mathcal{R}(n,k)) \text{ is rigid}\Big) = 1.$$

(ii) *For a fixed* $n \geq 2$,

$$\lim_{k\to\infty} \Pr\Big(([n], \mathcal{R}(n,k)) \text{ is rigid}\Big) = 1.$$

Proof. Let us observe that the probability that for some $m \geq \log^2 n$, and $S_1, S_2 \subseteq [n]$, $|S_1|, |S_2| = m$, $S_1 \cap S_2 = \emptyset$, there exists a bijective homomorphism of $(S_1, \mathcal{R}(n,k)|S_1)$ into $(S_2, \mathcal{R}(n,k)|S_2)$ is bounded from above by

$$\sum_{m\geq \log^2 n} \binom{n}{m}\binom{n}{m} m! \Big(\frac{3}{4}\Big)^{m^k} \leq \sum_{m\geq \log^2 n} \bigg(\frac{e^2n^2}{m^2}\Big(\frac{3}{4}\Big)^{m^{k-1}}\bigg)^m, \qquad (13)$$

since the probability that, given $f : S_1 \to S_2$, and $(a_1, \ldots, a_k) \in S_1^k$, we have $(a_1, \ldots, a_k) \in \mathcal{R}(n,k)$ but $(f(a_1), \ldots, f(a_k)) \notin \mathcal{R}(n,k)$ is equal to $1/4$. Note that for a fixed k and $n \to \infty$, the probability (13) tends to 0. Furthermore, one can easily check, that with probability tending to 1 as $n \to \infty$, each subset S of $[n]$ with at least $2\log n$ vertices contains a k-tuple which belongs to $\mathcal{R}(n,k)$. From the above two facts we infer that, with probability tending to 0 as $n \to \infty$, each homomorphism of $\mathcal{R}(n,k)$ has at least $n - 6\log^3 n$ fixed points. But one can argue as in the proof of Lemma 6 to show that the probability that for each pair of elements $v, w \in [n]$ and each $W \subseteq [n]$, $|W| \leq 6\log^3 n$, there are vertices $z_1, \ldots, z_{k-1} \in [n] \setminus W$ such that $(z_1, \ldots, z_{k-1}, v) \in \mathcal{R}(n,k)$ but $(z_1, \ldots, z_{k-1}, w) \notin \mathcal{R}(n,k)$. Hence, with probability tending to one as $n \to \infty$, for any automorphism of $([n], \mathcal{R}(n,k))$ each point of $[n]$ is mapped to itself and (i) follows.

In order to show (ii) observe that, since with probability tending to 1 as $k \to \infty$ the relation $\mathcal{R}(n,k)$ is non-empty (see Lemma 6), the image of each homomorphism of $([n], \mathcal{R}(n,k))$ contains at least two points. Let us take any non-trivial function $f : [n] \to [n]$ with $|f([n])| \geq 2$, and let $j, j' \in [n]$, be such that $\sigma(j) \neq j, \sigma(j')$. For $r = 1, \ldots, k$, $s = 1, \ldots, k$, let

$$a_r^s = \begin{cases} j & \text{if } \ r \leq s \\ j' & \text{if } \ r < s. \end{cases}$$

Note that all $2k$ k-tuples $(a_1^s, \ldots, a_k^s)$, $(f(a_1^s), \ldots, f(a_k^s))$, $s = 1, \ldots, k$, are different. Furthermore, the probability that for some $s = 1, \ldots, k$, it does not happen that $(a_1^s, \ldots, a_k^s) \in \mathcal{R}(n,k)$ and $(f(a_1^s), \ldots, f(a_k^s)) \notin \mathcal{R}(n,k)$, is $3/4$. Consequently, the probability that for each of at most n^n possible non-trivial mappings $f : [n] \to [n]$ none of the pairs $(a_1^s, \dots, a_k^s)$, $(f(a_1^s), \dots, f(a_k^s))$, $s = 1, \dots, k$, is a 'witness' that f is not a homomorphism is bounded from above by $n^n(3/4)^k$ and tends to 0 when n is fixed and $k \to \infty$. Consequently, if $n \geq 2$ is fixed and $k \to \infty$, the probability that there exists non-trivial endomorphism of $([n], \mathcal{R}(n, k))$ tends to 0. □

Proof of Theorem 3. Theorem 3 follows immediately from Theorems 4 and 5 and Lemmas 6 and 7. □

References

1. M. Bodirsky, J. Nešetřil: Constraint satisfaction problems with countable homogeneous templates, KAM-DIMATIA Series 2003-618. In: Proceedings of Computer Science Logic and the 8th Kurt Gödel Colloquium, August 25-30, 2003, Vienna, Springer Verlag, 2003.
2. V.G. Bodnarčuk, L.A. Kaluzhnin, V.N. Kotov, B.A. Romov, Galois theory for Post algebras I-II (in Russian), *Kibernetika*, **3** (1969), 1-10 and **5** (1969), 1-9. English version: *Cybernetics*, (1969), 243-252 and 531-539.
3. A. Bulatov: A dichotomy theorem for constraints on a three element set. In: FOCS'02, 2002, 649–658.
4. A. Bulatov, A. Krokhin, P.G. Jeavons: The complexity of maximal constraint languages. In: STOC'01, 2001, 667–674.
5. T. Feder, M. Vardi: The computational structure of monotone monadic SNP and constraint satisfaction: a study of through datalog and group theory, SIAM J. Computing, **28** (1998), 57–104.
6. P. Hell, J. Nešetřil: On the complexity of H-coloring, J. Combin. Th. B **48** (1990),92–110.
7. P.G. Jeavons: On the algebraic structure of combinatorial problems, Theor. Comp. Sci. **200** (1998), 185–204.
8. B. Larose, C. Tardif: Strongly rigid graphs and projectivity, Multiple-Valued Logic **7** (2001), 339–361.
9. B. Larose, C. Tardif: Projectivity and independent sets in powers of graphs, J. Graph Theory **40** (2002), no. 3, 162–171.
10. T. Łuczak, J. Nešetřil: A note on projective graphs, J. Graph Theory, to appear.
11. I.G. Rosenberg: Strongly rigid relations, Rocky Mountain Journal of Math. **3** (1973), 631-639.
12. T. Schaefer: The complexity of satisfiability problems. In: STOC'78, 1978, 216–226.

Faculty of Mathematics and Computer Science, Adam Mickiewicz University, 61-614 Poznań, Poland

E-mail address: `<tomasz@amu.edu.pl>`

Department of Applied Mathematics, Institute of Theoretical Computer sciences (ITI), Faculty of Mathematics and Physics, Charles University, Praha, Czech Republic

E-mail address: `<nesetril@kam.ms.mff.cuni.cz>`