Available online at www.sciencedirect.com
SCIENCE DIRECT®
Journal of Combinatorial Theory, Series A 103 (2003) 121–136
Journal of Combinatorial Theory Series A
http://www.elsevier.com/locate/jcta

The Specker–Blatter theorem does not hold for quaternary relations

Eldar Fischer

Faculty of Computer Science, Technion-Israel Institute of Technology, Haifa, Israel

Received 14 July 2002

Abstract

Let $\mathscr{C}$ be a class of relational structures. We denote by $f_{\mathscr{C}}(n)$ the number of structures in $\mathscr{C}$ over the labeled set $\{0, \ldots, n-1\}$. For any $\mathscr{C}$ definable in monadic second-order logic with unary and binary relation symbols only, E. Specker and C. Blatter showed that for every $m \in \mathbb{N}$, the function $f_{\mathscr{C}}$ satisfies a linear recurrence relation modulo m, and hence it is ultimately periodic modulo m. The case of ternary relation symbols, and more generally of arity k symbols for $k \geqslant 3$, was left open.

In this paper we show that for every m there is a class of structures $\mathscr{C}_m$, which is definable even in first-order logic with one quaternary (arity four) relation symbol, such that $f_{\mathscr{C}_m}$ is not ultimately periodic modulo m. This shows that the Specker–Blatter Theorem does not hold for quaternary relations, leaving only the ternary case open.

1. Introduction

1.1. The Specker–Blatter Theorem

Counting all objects of a specified kind belongs to the oldest activities in mathematics. In particular, counting the number of graphs of every order n that satisfy a given property is still a classic undertaking in combinatorial theory, as witnessed in [10,18].

A remarkable theorem due to E. Specker and C. Blatter, first announced in 1981, cf. [2–4,17] states that many of the above counting functions behave in orderly ways despite their apparent complexity. It is unfortunate that this theorem has received

E-mail address: eldar@cs.technion.ac.il.

0097-3165/03/$ - see front matter
doi:10.1016/S0097-3165(03)00075-X

less than the attention it deserves for both the beauty of the result and the ingenuity in its proof.

Let us consider k relation symbols $R_1, \ldots, R_k$, and let $\mathscr{C}$ be a class of labeled relational structures over $R_1, \ldots, R_k$. For every n we denote by $f_{\mathscr{C}}(n)$ the number of such structures over the universe $\{0, \ldots, n-1\}$. For example, a class $\mathscr{C}$ of structures over one binary relation E is a class of directed labeled graphs (possibly with loops but with no completely parallel edges), and in this case $f_{\mathscr{C}}(n)$ counts the number of such graphs with the vertex set $\{0, \ldots, n-1\}$.

Theorem 1 (The Specker–Blatter Theorem). *For a class $\mathscr{C}$ definable in monadic second-order logic with unary and binary relation symbols only, the function $f_{\mathscr{C}}$ satisfies a linear recurrence relation*

$$f_{\mathscr{C}}(n) \equiv \sum_{j=1}^{d} a_j^{(m)} f_{\mathscr{C}}(n-j) \pmod{m}$$

for every $m \in \mathbb{N}$. In particular, all functions $f_{\mathscr{C}}^{(m)} : \mathbb{N} \to \mathbb{Z}_m$ defined by $f_{\mathscr{C}}^{(m)}(n) = f_{\mathscr{C}}(n) \pmod{m}$ are ultimately periodic.

The case of ternary relation symbols, and more generally of arity $k \geqslant 3$ relation symbols, was left open in [4,17]. The question as to whether Theorem 1 holds for these appears in the list of open problems in finite model theory, [13, Problem 3.5].

In this paper we show that Theorem 1 does not hold for quaternary relations, leaving only the ternary case unresolved.

Theorem 2. *For every prime p there is a class of structures $\mathscr{C}_p$ which is definable in first-order logic by a formula ϕ_{Im_p}, with one binary relation symbol E and one quaternary relation symbol R, such that $f_{\mathscr{C}_p}$ is not ultimately periodic modulo p.*

It is indeed sufficient to formulate and prove Theorem 2 for every prime number p, since for an m which is not prime the theorem easily extends by applying it to a p which is a prime divisor of m. In the end of the paper we also specify how to construct a property as above that involves only a single quaternary relation symbol.

In a future article [8] we shall further explore the boundaries of the Specker–Blatter Theorem. For example, it is shown there that for unary relations the recurrence relation holds also over $\mathbb{Z}$, even if we consider linearly ordered labeled structures (while the Specker–Blatter Theorem does not hold over linearly ordered structures for binary relations); other instances for which the Specker–Blatter Theorem holds are also described there.

1.2. Definability and logic

The following is a brief review; for the reader who is unfamiliar with definability in logic we recommend [6].

Let $\bar{R} = \{R_1, \ldots, R_k\}$ be a set of relation symbols, where each R_i is associated with the arity ρ_i. A (relational) $\bar{R}$-*structure* is a tuple $\mathfrak{A} = \langle A, R_1^{\mathfrak{A}}, \ldots, R_k^{\mathfrak{A}} \rangle$ where $R_i^{\mathfrak{A}} \subseteq A^{\rho_i}$ for every $1 \leqslant i \leqslant k$; in the above notation we also say that A is the *universe* of $\mathfrak{A}$. Let $\mathscr{C}$ be a class of relational $\bar{R}$-structures. We denote by $f_{\mathscr{C}}(n)$ the number of structures in $\mathscr{C}$ over the labeled set $[n] = \{0, \ldots, n-1\}$, that is,

$$f_{\mathscr{C}}(n) = |\{(R_1^{\mathfrak{A}} \subseteq [n]^{\rho_1}, \ldots, R_k^{\mathfrak{A}} \subseteq [n]^{\rho_k}) : \langle [n], R_1^{\mathfrak{A}}, \ldots, R_k^{\mathfrak{A}} \rangle \in \mathscr{C}\}|.$$

First Order Logic (FOL) over $\bar{R}$ has the atomic formulas of the type "$R_i(x_1, \ldots, x_{\rho_i})$" and "$x_1 = x_2$", where $x_1, x_2, \ldots$ are any individual variables. The set $\mathrm{FOL}(\bar{R})$ denotes all formulas, composed using atomic formulas, boolean connectives, and quantifiers of the type "$\exists x$" and "$\forall x$", which have no free (nonquantified) variables. For example, the formula stating that a relation E is the edge set of a simple undirected graph is such a formula: $\forall x(\neg E(x,x)) \wedge \forall x \forall y(E(x,y) \to E(y,x))$. The satisfaction relation between an $\bar{R}$-structure $\mathfrak{A}$ and a first order formula ϕ is defined as usual (e.g. $\mathfrak{A} \vDash R_1(x_1, \ldots, x_{\rho_1})$ if $(x_1, \ldots, x_{\rho_1}) \in R_1^{\mathfrak{A}}$, and so on). With a slight abuse of notation we shall sometimes use "R_i" to denote also "$R_i^{\mathfrak{A}}$" when the meaning of the expression is clear from its context.

Monadic Second Order Logic (MSOL) formulas are obtained by allowing additionally for variables $S_1, S_2, \ldots$ which hold sets (unary predicates), atomic formulas of the type "$x_1 \in S_2$", and quantifiers over the set variables; as before $\mathrm{MSOL}(\bar{R})$ denotes all such formulas that have no free variables (of either kind). For example, there exists an MSOL formula stating that a simple graph given by a relation E is 2-colorable: $\exists S(\forall x \forall y(((x \in S \wedge y \in S) \vee (x \notin S \wedge y \notin S)) \to (\neg E(x,y))))$.

A class $\mathscr{C}$ of $\bar{R}$-structures is called FOL-*definable* if there exists $\phi \in \mathrm{FOL}(\bar{R})$ such that for every $\mathfrak{A}$ we have $\mathfrak{A} \in \mathscr{C}$ if and only if $\mathfrak{A} \vDash \phi$. The notion of a class being MSOL-*definable* is similarly defined.

The following are some more examples concerning an $\bar{R}$ which consists of a single binary relation symbol R. The nondefinability statements appearing below can be proven using Ehrenfeucht–Fraïssé Games, see [6].

1. The class ORD of all linear orders. It is $\mathrm{FOL}(R)$-definable, and satisfies $f_{\mathrm{ORD}}(n) = n!$.
2. For the class CONN of simple undirected connected graphs, [10, p. 7] gives

$$f_{\mathrm{CONN}}(n) = 2^{\binom{n}{2}} - \frac{1}{n} \sum_{k=1}^{n-1} k \binom{n}{k} 2^{\binom{n-k}{2}} f_{\mathrm{CONN}}(k).$$

   The class CONN is not $\mathrm{FOL}(R)$-definable, but it is $\mathrm{MSOL}(R)$-definable using a universal quantifier over set variables.
3. Let $m \in \mathbb{N}$ and let EQC_m denote the class of simple undirected graphs which consist of m disjoint cliques of equal size. For example, for $m = 2$ we have $f_{\mathrm{EQC}_2}(2n) = \frac{1}{2}\binom{2n}{2}$ and $f_{\mathrm{EQC}_2}(2n+1) = 0$. The class EQC_m is not $\mathrm{MSOL}(R)$-definable, but it will play a crucial role in the following.

To appreciate the Specker–Blatter Theorem (Theorem 1), one should look at the counting function $f_{\mathscr{R}_r}(n)$ of the class of simple r-regular graphs $\mathscr{R}_r$, which is clearly definable (for every fixed r) in first-order logic. Counting the number of labeled regular graphs is treated completely in [10, Chapter 7], where an explicit formula is given, essentially due to Redfield [16] and rediscovered by Read [14,15]. However, the formula is complicated and does not readily yield the modular recurrence relations. For cubic graphs, the function is explicitly given in [10, p. 175] as $f_{\mathscr{R}_3}(2n+1)=0$ and

$$f_{\mathscr{R}_3}(2n)=\frac{(2n)!}{6^n}\sum_{j,k}\frac{(-1)^j(6k-2j)!6^j}{(3k-j)!(2k-j)!(n-k)!}48^k\sum_i\frac{(-1)^i j!}{(j-2i)!i!}.$$

In [9, Section 9], I. Gessel provides techniques of studying congruences for $f_{\mathscr{R}_r}(n)$, but their application is still quite difficult. A simpler asymptotic formula was found by Bollobas [5]; it has proven to be useful in studying regular random graphs, but by its approximative nature it provides no information with respect to congruences.

1.3. *Outline of the paper*

The proof of Theorem 2 is based on the classes EQC_p (where p is prime) given above. In Section 2 we show that $b_p(n)=f_{\mathrm{EQC}_p}(n)$ is not ultimately periodic modulo p. In Section 3 we construct classes of structures $\mathscr{D}_p$ such that $f_{\mathscr{D}_p}(n)\equiv b_p(n) \pmod p$. These structures however use infinitely many binary relation symbols (actually the number of relations can be made finite but it still depends on n). These structures use an inductive definition of a binary property, with the induction step by itself being in essence FOL-definable. In Section 4 we finally construct classes $\mathscr{C}_p$ that have a one to one and onto correspondence with the classes $\mathscr{D}_p$, and which are FOL-definable. This is done by "unfolding" the inductive definition, using the relations of each stage as "markers" for the relations of the next stage. This process results in quaternary relations. Similar techniques of unfolding inductions are frequently used in descriptive complexity theory, see e.g. [6].

2. Counting modulo p

In the following, we let p be a prime number, and state some lemmas and definitions; in particular, we provide a graph property for which the number of models is not ultimately periodic modulo p, but which is not first-order. Based on it we will construct a first-order property in the following sections.

To help us count modulo p, we make extensive use of the following simple lemma. Similar methods have been extensively used before, at least as early as in the 1872 combinatorial proof of Fermat's congruence theorem by J. Petersen, given in the introduction of [9].

Some notation first: Every permutation $\sigma:[n]\to[n]$ can also act on the family of $\bar{R}$-structures over $[n]$ (for a given fixed $\bar{R}$) in the obvious way, by sending

$\mathfrak{A} = \langle [n], R_1^{\mathfrak{A}}, \ldots, R_k^{\mathfrak{A}} \rangle$ to $\sigma(\mathfrak{A}) = \langle [n], \sigma(R_1^{\mathfrak{A}}), \ldots, \sigma(R_k^{\mathfrak{A}}) \rangle$, where we define $\sigma(R_i^{\mathfrak{A}}) = \{(\sigma(a_1), \ldots, \sigma(a_{\rho_i}))|(a_1, \ldots, a_{\rho_i}) \in R_i^{\mathfrak{A}}\}$. Families of $\bar{R}$-structures definable, e.g. by a set of first- or second-order logic axioms are clearly closed under the action of σ, and, moreover, σ induces a permutation on such families; in fact, the abstraction of a similar observation is the starting point of the theory of combinatorial species (see [1]).

Lemma 3. *Suppose that $\mathscr{F}$ is a family of structures over $[n] = \{0, \ldots, n-1\}$ which is closed under the action of every permutation of $[n]$ (e.g. a family defined by a first-order expression over some language). Let $\sigma : [n] \to [n]$ be a permutation such that $\sigma \neq \mathrm{Id}$ but $\sigma^p = \mathrm{Id}$.*

Let $\mathscr{F}' \subset \mathscr{F}$ be a family of structures such that σ also preserves membership in $\mathscr{F}'$, and which contains all structures that are invariant with respect to σ (that is, $\mathscr{F}'$ contains every $\mathfrak{A} \in \mathscr{F}$ for which $\sigma(\mathfrak{A}) = \mathfrak{A}$). Then $|\mathscr{F}'| \equiv |\mathscr{F}| \pmod p$.

Proof. By the above definitions and discussion, σ induces a permutation over $\mathscr{F}$, which preserves $\mathscr{F}'$. Decomposing this permutation of $\mathscr{F}$ to disjoint orbits, it is not hard to see that every member of $\mathscr{F}$ which is not invariant under σ is in an orbit of size p (using the information that p is prime); in particular $\mathscr{F} - \mathscr{F}'$ is a disjoint union of such orbits, and so its size is divisible by p. □

We denote by $b_p(n)$ the number of graphs with $[n]$ as a set of vertices which are disjoint unions of exactly p same-size cliques, that is, $b_p(n) = f_{\mathrm{EQC}_p}(n)$. We now investigate the congruences of $b_p(n)$ modulo p. Congruence classes of binomial coefficients and related functions have received a lot of attention in the literature, starting with Lucas's famous result [12] (see also [7]). We start with the following lemma.

Lemma 4. *For every $k > 1$, $b_p(pk) \equiv b_p(k) \pmod p$.*

Proof. We define $\sigma : [pk] \to [pk]$ by $\sigma(pi + j) = pi + j + 1$ for $0 \leqslant i < k$ and $0 \leqslant j < p - 1$, and $\sigma(pi + p - 1) = pi$ for $0 \leqslant i < k$ (so σ is composed of k disjoint orbits of size p).

We now use Lemma 3. We first note that all graphs for which any clique contains more than one member, but not all members, of $\{pi, \ldots, pi + p - 1\}$ for some i, are not invariant with respect to σ. We also note that all graphs for which some clique contains all members of $\{pi, \ldots, pi + p - 1\}$, but only one member of $\{pj, \ldots, pj + p - 1\}$ for some other j, are not invariant with respect to σ.

We let $\mathscr{F}'$ be the family of all other graphs which are disjoint unions of p same-size cliques. It is not hard to see that $\mathscr{F}'$ contains two types of graphs—those for which every $\{pi, \ldots, pi + p - 1\}$ is contained in one of the cliques, whose number is $b_p(k)$, and those for which every $\{pi, \ldots, pi + p - 1\}$ contains exactly one member from every clique, whose number $(p!)^{k-1}$ is divisible by p if $k > 1$. □

Consequence 5. *For every n which is not a power of p, we have $b_p(n) \equiv 0 \pmod p$, and for every n which is a power of p we have $b_p(n) \equiv 1 \pmod p$. In particular, $b_p(n)$ is not ultimately periodic modulo p.*

Proof. By induction on n, where the basis is $n = p$ (for which $b_p(n) = 1$) and every n which is not divisible by p (for which $b_p(n) = 0$); the induction step follows from Lemma 4. □

3. Comparing sizes in a modulo-preserving manner

The first intuition with regards to ensuring (with a first order property) that the sizes of p sets $A_0, \ldots, A_{p-1}$ are all equal, is to add a binary relation and state that it is a perfect matching between each pair of these sets. However, the number of ways to construct such matchings for equal size sets is divisible by $|A_0|!$, and so it is zero modulo p for any large enough n. We thus have to formulate a different notion. We start with one that does not ensure that the sets are equal, and later show how to iterate it in a manner that indeed provides a good substitute for the notion of a perfect matching.

Definition 6. A preserving p-matching between $A_0, \ldots, A_{p-1}$ is a set of $\frac{1}{p}\sum_{i=0}^{p-1} |A_i|$ vertex disjoint p-cliques on $\bigcup_{i=0}^{p-1} A_i$, such that every clique is either fully contained in one of $A_0, \ldots, A_{p-1}$, or contains exactly one vertex from each A_i.

Note that for $p = 2$, every perfect matching on $A_0 \cup A_1$ (not necessarily between A_0 and A_1) is a preserving 2-matching. The enumeration of preserving p-matchings modulo p is given by the following.

Lemma 7. *If $|A_0| \equiv \cdots \equiv |A_{p-1}| \pmod p$ then the number of preserving p-matchings is 1 modulo p. Otherwise, there are no preserving p-matchings at all.*

Proof. The proof of the second part (where the $|A_i|$ are not all equivalent modulo p) is simple. The proof of the first part is by induction on $\sum_{i=0}^{p-1} |A_i|$.

The base case is where all $|A_i|$ are equal to some $k < p$. It is clear that in this case a preserving matching consists of k cliques such that each of them contains exactly one vertex from each A_i. Denoting $A_i = \{v_{i,0}, \ldots, v_{i,k-1}\}$, define σ by $\sigma(v_{i,j}) = v_{i+1,j}$ for every $0 \leqslant j \leqslant k-1$ and $0 \leqslant i < p-1$, and $\sigma(v_{p-1,j}) = v_{0,j}$ for every $0 \leqslant j \leqslant k-1$. Since $k < p$, for every clique with vertices $\{v_{0,j_0}, \ldots, v_{p-1,j_{p-1}}\}$ there exist $i \neq i'$ such that $j_i = j_{i'}$; from this it is not hard to show that the matching is not invariant with respect to σ unless for every such clique, $j_i = j_{i''}$ for every i''. Thus there exists only one preserving p-matching which is invariant with respect to σ, and using Lemma 3 the base case is proven.

For the induction step, let i_0 be such that $|A_{i_0}| \geqslant p$, and let $v_0, \ldots, v_{p-1}$ be p vertices in A_{i_0}. In this case we define σ by $\sigma(v_j) = v_{j+1}$ for $0 \leqslant j < p-1$, $\sigma(v_{p-1}) = v_0$, and

$\sigma(u) = u$ for every $u \notin \{v_0, \ldots, v_p - 1\}$. It is clear that the only invariant preserving p-matchings are those for which $\{v_0, \ldots, v_{p-1}\}$ is one of the p-cliques, and using Lemma 3 the induction step follows. □

To fully equate the sizes of the sets $A_0, \ldots, A_{p-1}$, we use the following notion of a matching between the sets.

Definition 8. Given disjoint sets $A_0, \ldots, A_{p-1}$, an *iterative p-matching* between these sets is a sequence of graphs $\{\mathscr{M}_i\}_{i \geqslant 0} = \mathscr{M}_0, \mathscr{M}_1, \ldots$ where each has its own vertex set, satisfying the following.

- If $A_i = \emptyset$ for every i then $\mathscr{M}_0 = \emptyset$.
- Otherwise, $\mathscr{M}_0$ is a preserving p-matching between $A_0, \ldots, A_{p-1}$.
- Defining by A'_i the set of p-cliques of $\mathscr{M}_0$ inside A_i for every i, $\mathscr{M}_1, \mathscr{M}_2, \ldots$ is an iterative p-matching between $A'_0, \ldots, A'_{p-1}$.

The above sequences may look infinite, but it is easy to see that if $A_0, \ldots, A_{p-1}$ are all finite, then the number of nonempty elements in an iterative p-matching is also finite, and moreover, the total number of possible iterative p-matchings over $A_0, \ldots, A_{p-1}$ is finite. We shall also use the following alternative definition of iterative matchings.

Definition 9. Given disjoint sets $A_0, \ldots, A_{p-1}$, a *graphic iterative p-matching* between these sets is a sequence of graphs $\{M_i\}_{i \geqslant 0} = M_0, M_1, \ldots$ which all have $\bigcup_{i=0}^{p-1} A_i$ as a vertex set, satisfying the following.

- Every M_i consists of isolated vertices and vertex disjoint copies of the complete p-partite graph with p color classes of size p^i.
- Each of the p-partite graphs in M_i is either fully contained in one of $A_0, \ldots, A_{p-1}$, or is such that each of its color classes is fully contained in a different A_i; in particular, M_0 is a preserving p-matching between $A_0, \ldots, A_{p-1}$.
- For $i > 0$, each color class of a p-partite graph in M_i consists of all vertices of one of the p-partite graphs in M_{i-1} which are fully contained in one of $A_0, \ldots, A_{p-1}$; moreover, for each of the p-partite graphs of M_{i-1} with the above property there exists a complete p-partite graph in M_i containing its vertices in this manner.

It is not very hard to see that the correspondence defined below is in fact a one to one and onto correspondence between all possible iterative matchings and all possible graphic iterative matchings between $A_0, \ldots, A_{p-1}$.

Definition 10. Given a graphic iterative matching $\{M_i\}_{i \geqslant 0}$ we construct the corresponding iterative matching $\{\mathscr{M}_i\}_{i \geqslant 0}$ as follows.

- $\mathscr{M}_0$ is M_0.
- For every i we let A'_i be the set of p-cliques of M_0 that are fully contained in A_i. We then construct $M'_1, M'_2, \ldots$ by defining M'_j to have an edge between $u \in \bigcup_{i=0}^{p-1} A'_i$

and $v \in \bigcup_{i=0}^{p-1} A'_i$ if and only if M'_j has an edge between the corresponding cliques. It is not hard to see that $M'_1, M'_2, \ldots$ is a graphic iterative p-matching between $A'_0, \ldots, A'_{p-1}$; we then define $\mathscr{M}_1, \mathscr{M}_2, \ldots$ as the iterative matching corresponding to $M_1, M_2, \ldots$ inductively.

Given an iterative matching $\{\mathscr{M}_i\}_{i \geqslant 0}$, we construct the corresponding graphic iterative matching $\{M_i\}_{i \geqslant 0}$ as follows.

- M_0 is $\mathscr{M}_0$.
- We now construct by induction a graphic iterative matching $\{N_i\}_{i \geqslant 1}$ corresponding to $\{\mathscr{M}_i\}_{i \geqslant 1}$. We note that $\{\mathscr{M}_i\}_{i \geqslant 1}$ is an iterative matching over $A'_0, \ldots, A'_{p-1}$, which are sets of p-cliques over members of $A_0, \ldots, A_{p-1}$, and thus the graphs $\{N_i\}_{i \geqslant 1}$ are over the vertex set $A'_0, \ldots, A'_{p-1}$. For every $i \geqslant 1$ we construct M_i from N_i as follows: Every vertex of N_i corresponds to a clique of M_0 which is contained in some A_j. We replace each such vertex by the p vertices of the corresponding clique in M_0, and replace each edge uv of N_i by all possible edges between the vertices that correspond to u and the vertices that correspond to v. We do not put in M_i any additional edges (there may be additional isolated vertices, those of the cliques in M_0 that are not fully contained in some A_j).

It is not hard to see that the second correspondence is the inverse of the first.

Henceforth, we use the term "iterative matchings" for both points of views. We now show how iterative matchings are useful for equating sets in the modulo p setting.

Lemma 11. *If $|A_i|$ are all equal, then the number of iterative p-matchings between $A_0, \ldots, A_{p-1}$ is 1 modulo p. Otherwise, there are no such matchings.*

Proof. The proof is by induction on $\sum_{i=1}^{p-1} |A_i|$. The case where this sum is zero is clear (in this case $A_i = \emptyset$ for every i and indeed there exists exactly one possible iterative p-matching), as well as all cases where the $|A_i|$ are not all equivalent modulo p (in which there is no possibility for constructing even the first preserving p-matching $\mathscr{M}_0$).

In any other case the number of ways to construct $\mathscr{M}_0$ is 1 modulo p by Lemma 7. For each such construction, if we construct the appropriate $A'_0, \ldots, A'_{p-1}$ as per the definition above, it is easy to see that $\sum_{i=1}^{p-1} |A'_i| < \sum_{i=1}^{p-1} |A_i|$, as well as that $|A'_i|$ are all equal if and only if $|A_i|$ are all equal. The latter occurs because when we denote by r the number of cliques in $\mathscr{M}_0$ not fully contained in any of the A_i, we get $|A'_i| = \frac{|A_i| - r}{p}$ for every i.

If $|A_i|$ are all equal, then by the induction hypothesis for every choice of $\mathscr{M}_0$ the number of choices for $\mathscr{M}_1, \mathscr{M}_2, \ldots$ is 1 modulo p, and thus their sum over all choices of $\mathscr{M}_0$ is 1 modulo p. If $|A_i|$ are not all equal, then by the induction hypothesis

there exists no good choice of $\mathcal{M}_1, \mathcal{M}_2, \ldots$ for any choice of $\mathcal{M}_0$, completing the proof. □

We conclude our investigation of iterative matchings with a simple lemma which is not directly related to counting, but is used in the following.

Lemma 12. *For every iterative matching between $A_0, \ldots, A_{p-1}$ (by Lemma 11 we need only consider sets with equal sizes), every vertex in $\bigcup_{i=0}^{p-1} A_i$ is eventually matched (a vertex in A_j is considered eventually matched if it has a neighbor outside of A_i in some M_k, when we consider the graphic version $\{M_i\}_{i\geqslant 0}$ of the iterative matching).*

Proof. In this case it is better to look at $\{\mathcal{M}_i\}_{i\geqslant 0}$ which corresponds to $\{M_i\}_{i\geqslant 0}$, and note that a vertex $v \in A_i$ is eventually matched if and only if it is either contained in a clique of $\mathcal{M}_0$ which is not internal to A_i, or contained in a clique of $\mathcal{M}_0$ which is internal to A_i but which is eventually matched by $\mathcal{M}_1, \mathcal{M}_2, \ldots$; the proof is then completed by an easy induction on $|A_0|$. □

3.1. Iterative matchings and species

Iterative matchings admit a natural description in the framework of the theory of species, initiated by Joyal [11] and detailed in [1]. For the interested reader who is familiar with this theory, we outline how iterative matchings can be described using the theory of species in this small digression from the main topic of the paper. The notation used in the following is taken from [1].

We let $X_0, \ldots, X_{p-1}$ denote variables (or singleton species) for p sorts of points. Let E be the species of (one-sorted) sets, and E_p be the species of sets of cardinality p. Thus, for example, $E(E_p(X))$ is equivalent to the species of (labeled) graphs which are disjoint union of cliques with p vertices, and $E(X \cdot Y)$ is the two-sorted species of bijections between two base sets.

The p-sorted species $\mathrm{PM}(X_0, \ldots, X_{p-1}) = E(X_0 \cdot \ldots \cdot X_{p-1}) \cdot E(E_p(X_0) + \ldots + E_p(X_{p-1}))$ corresponds to that of the preserving p-matchings between p sets, and the recursive definition of iterative matchings translates to the combinatorial functional equation

$$\mathrm{IM}(X_0, \ldots, X_{p-1}) = E(X_0 \cdot \ldots \cdot X_{p-1}) \cdot \mathrm{IM}(E_p(X_0), \ldots, E_p(X_{p-1})).$$

Unfolding the above recursive equation provides us with

$$\mathrm{IM}(X_0, \ldots, X_{p-1}) = \prod_{k\geqslant 0} E(E_p^{(k)}(X_0) \cdot \ldots \cdot E_p^{(k)}(X_{p-1})),$$

where we define by induction $E_p^{(0)}(X) = X$ and $E_p^{(k+1)}(X) = E_p(E_p^{(k)}(X))$. It is not hard to show that this alternate formula for the species corresponds to the graphic definition of iterative matchings (where the term $E(E_p^{(k)}(X_0) \cdot \ldots \cdot E_p^{(k)}(X_{p-1}))$ corresponds to the restriction of the matching to the vertices of the connected components of M_k which are not contained in any A_i).

The results of this section concerning the number of iterative matchings modulo p can also be proven using the tools of the theory of species: The above combinatorial equations lead to a recursive formula for the number of iterative matchings between p sets, which in turn can be shown to have the required properties.

4. Constructing the first-order property

We now construct a first-order property that in essence counts $b_p(n)$ times the number of possible iterative matchings between the p sets of size $\frac{k}{p}$; by Lemma 11 this is equivalent modulo p to $b_p(n)$.

We look at structures $\langle [n], E, R \rangle$ where E is a binary relation and R is a quaternary (arity four) relation. The property will state that E is a union of p vertex-disjoint cliques and that R is a representation (we will prove that it is unique) of an iterative p-matching between the cliques in E. Instead of defining the property all at once we define it as the conjunction of several properties defined below. All the properties are first-order, and whenever proving this part is clear we shall omit all further mention thereof. In the presentation we shall also define and use some relations that can be expressed using first-order expressions over E and R.

Definition 13. Property $\mathrm{Cl}_p(E)$ states that E is a nondirected simple graph which is the disjoint union of exactly p cliques.

In the sequel we denote by $A_0, \ldots, A_{p-1}$ the p cliques. We note however that the labeling of these cliques is arbitrary, and make sure that all the logical constructions below are invariant with respect to permuting the labels $A_0, \ldots, A_{p-1}$; in particular the definition of a preserving p-matching is such a construction (see below).

Definition 14. Property $\mathrm{Edg}_p(R)$ states that if (e_1, e_2, o_1, o_2) is in R then $e_1 \neq e_2$, and also (e_2, e_1, o_1, o_2) and (e_1, e_2, o_2, o_1) and (e_2, e_1, o_2, o_1) are in R. We say in this case that *the edge* (e_1, e_2) *has* (o_1, o_2) *as an origin*. We say that (e_1, e_2) *has an origin* if there exist (o_1, o_2) for which (e_1, e_2, o_1, o_2) is in R. Note that there is the possibility that $o_1 = o_2$.

In the sequel we shall usually refer by the term "edge" to an (e_1, e_2) that has an origin according to R, and only refer indirectly (e.g. by the definition of $A_0, \ldots, A_{p-1}$) to the graph E.

Definition 15. If (e_1, e_2) which has an origin satisfies $(e_1, e_2) \notin E$ (that is, it is an edge between A_i and A_j for some $i \neq j$) then we say that (e_1, e_2) is a *bridge*. Otherwise we say that (e_1, e_2) is *internal* to the clique that contains e_1 and e_2 (which is one of $A_0, \ldots, A_{p-1}$).

We shall use the definition of bridge and internal edges to define the property of R representing an iterative p-matching $\{M_i\}_{i\geqslant 0}$, while distinguishing which edge belongs to which M_i will result from the above definition of an origin. First we deal with M_0.

Definition 16. Property $\text{Base}_p(E, R)$ states the following.

- If (e_1, e_2) has (o, o) as an origin, then for every (o_1, o_2) it has (o_1, o_2) as an origin if and only if $o_1 = o_2$.
- For every o, the set of edges having (o, o) as an origin is a preserving p-matching between $A_0, \ldots, A_{p-1}$.

It is not hard to see that the statement that a graph G is a preserving p-matching (in the second item of the above definition G is the set of edges having (o, o) as an origin) is first-order definable for any fixed p. It is the conjunction of the statement that G is a disjoint union of cliques of size p covering the set of vertices, "for every u_0 there exist $u_1, \ldots, u_{p-1}$ such that $\{u_0, \ldots, u_{p-1}\}$ is a clique of G, and furthermore there exist no two vertices of distance exactly 2 from each other", with the statement that every p-clique in G either contains no bridge edges or contains only bridge edges.

The reason for requiring that an edge has either no origin of the type (o, o) or has all such possible pairs as origins is to ensure that there is only one way to represent M_0 using R.

We shall now require a representation of M_i given a the representation of M_{i-1}. To express the relation between M_i and M_{i-1} in first-order logic, we use the following.

Lemma 17. *Suppose that E and $A_0, \ldots, A_{p-1}$ are as above, and that S is a binary relation that is known to be a graph all of whose connected components are of diameter 1 or 2. Then, the following statement about a graph G is first-order definable*:

- *Denoting by $C_1, \ldots, C_l$ the connected components of S which are not isolated vertices and are fully contained in any one of $A_0, \ldots, A_{p-1}$, G consists of isolated vertices and vertex disjoint copies of complete p-partite graphs, each of which has p members of $\{C_1, \ldots, C_l\}$ as its color classes.*
- *Each of the complete p-partite graphs is either fully contained in one of $A_0, \ldots, A_{p-1}$, or is such that each of its color classes is fully contained in a different A_i.*
- *Each of $C_1, \ldots, C_l$ intersects (and thus forms a color class of) one of the complete p-partite graphs of G.*

Proof. Since all the components of S have diameter at most 2, the statement that u and v belong to the same component of S is first-order definable ("$u = u$, or uv is an edge of S, or there exists w such that uwv is a path in S"). Thus it is also not very hard to formulate in first-order logic the statement that a vertex u is in some C_j (which is equivalent to stating that u is not isolated in S and all vertices of distance

2 or less from u are in the same A_i as u), and the statement that u and v are both in C_j for some $1 \leqslant j \leqslant l$.

The following is a first-order formulation of the statement that G consists of isolated vertices and complete p-partite graphs: "For every vertex u_0, either u_0 is isolated in G, or there exist $u_1, \ldots, u_{p-1}$ such that $\{u_0, \ldots, u_{p-1}\}$ is a clique, there exist no vertex of distance exactly 2 (according to G) from $\{u_0, \ldots, u_{p-1}\}$, every vertex of distance 1 from $\{u_0, \ldots, u_{p-1}\}$ has exactly $p-1$ neighbors in this set, and every two such vertices are adjacent in G if and only if they do not have the same $p-1$ neighbors in $\{u_0, \ldots, u_{p-1}\}$".

To comply with the first and the third items above, we use the conjunction of the above statement about G with the statement that any two vertices are in the same C_j if and only if they have distance exactly 2 in G (note that u belongs to some C_j if and only if there exists some v so that u and v belong to the same C_j).

To further comply with the second item above, we use the conjunction of this with the statement that if uv and vw are edges in G, then either both are fully contained in some A_i or none of them is (using also the information that each of $C_1, \ldots, C_l$ is fully contained in some A_i). □

We now turn back to defining the property that ensures a representation of M_i given that of M_{i-1}. The following definition makes use of the notion of connected components, which is not first-order definable. However, we shall prove later that for any (o_1, o_2) the set of edges having it as an origin forms a disjoint union of isolated vertices and complete p-partite graphs, so in particular all the connected components have diameter at most 2, and thus we can use Lemma 17 for the definition instead. We shall also prove that each such component is either internal to one of $A_0, \ldots, A_{p-1}$, or brings together a component of M_{i-1} from every A_j. This will be proven by induction; the basis $o_1 = o_2$ is relatively easy using the property $\mathrm{Base}_p(E, R)$.

Definition 18. Property $\mathrm{Next}_p(E, R)$ states the following.

- If (e_1, e_2) has (o_1, o_2) with $o_1 \neq o_2$ as an origin, then for every (o_1', o_2') it has (o_1', o_2') as an origin if and only if (o_1, o_2) and (o_1', o_2') have the same origin (i.e. if there exists (r_1, r_2) such that $(o_1, o_2, r_1, r_2) \in R$ and $(o_1', o_2', r_1, r_2) \in R$).
- For every $o_1 \neq o_2$ for which (o_1, o_2) has an origin, we look at the set of connected components of the set of edges having the same origin as (o_1, o_2), apart from those which are isolated vertices and those that are not internal to one of $A_0, \ldots, A_{p-1}$; denote them by $C_1, \ldots, C_l$. We also denote by G the graph resulting from the set of edges having (o_1, o_2) as an origin.
  - G consists of isolated vertices and vertex disjoint copies of complete p-partite graphs, each of which has p members of $C_1, \ldots, C_l$ as its color classes.
  - Each of the complete p-partite graphs in G is either fully contained in one of $A_0, \ldots, A_{p-1}$, or is such that each of its color classes is fully contained in a different A_i.
  - Each of $C_1, \ldots, C_l$ intersects one of the complete p-partite graphs of G.

To finalize the definition of our first-order property, we make sure that vertex pairs incident with bridge edges are "out of the game", to avoid multiplicities in counting that may result from assigning them arbitrary origins. Also in the next definition, the part about being in the same connected component of a graph can be replaced with a first-order expression that works for the case where all the connected components are of diameter at most 2.

Definition 19. Property $\mathrm{Clear}_p(E,R)$ states that for every (o_1,o_2), no edges that are incident with a bridge edge having (o_1,o_2) as an origin may have any origin, except possibly the edges which are internal to the connected components of the graph of edges having (o_1,o_2) as an origin.

We now state and prove the concrete form of Theorem 2.

Theorem 20. *Let* $\mathrm{Im}_p(E,R) = \mathrm{Cl}_p(E) \wedge \mathrm{Edg}_p(R) \wedge \mathrm{Base}_p(E,R) \wedge \mathrm{Next}_p(E,R) \wedge \mathrm{Clear}_p(E,R)$. *Denote by* $f_{\mathrm{Im}_p}(n)$ *the number of structures* $\langle [n], E, R \rangle$ *satisfying* Im_p. *Then* $f_{\mathrm{Im}_p}(n) \equiv b_p(n) \pmod p$, *and so it is not ultimately periodic modulo* p.

To prove it we consider an E which satisfies $\mathrm{Cl}_p(E)$, and define a way to encode an iterative matching between the cliques $A_0, \ldots, A_{p-1}$ of E, as a relation R for which Im_p is satisfied. Then we prove that such encodings are the only instances which satisfy Im_p for any given E.

Definition 21. Suppose that $\{M_i\}_{i \geqslant 0}$ is an iterative matching (we use the graphic definition) between the cliques of E. We define an R which is the *encoding* of $\{M_i\}_{i \geqslant 0}$ as follows.

- Every edge of M_0 is according to R an edge that has every (o,o) and no other pair as an origin.
- For $i>0$, we let every edge of M_i have every edge of M_{i-1} and no other pair as an origin.
- No other combinations of edges with origins exist apart from those constructed above.

The above definition produces from an iterative matching a structure that satisfies Im_p.

Claim 22. *An encoding of an iterative matching satisfies* Im_p. *Moreover, for any two distinct iterative matchings, the corresponding encodings are also distinct.*

Proof. It is clear from the definition above that every encoding of an iterative matching satisfies $\mathrm{Cl}_p(E)$ and $\mathrm{Edg}_p(R)$. Also, $\mathrm{Base}_p(E,R)$ is satisfied since all the edges of the preserving matching M_0 now have every possible (o,o) as an origin, and no other edge has any origin of the type (o,o).

The first item of $\mathrm{Next}_p(E,R)$ is satisfied because in an iterative matching the edges of M_i and M_j are disjoint for every $i \neq j$. Every edge that has an origin of the type

(o_1, o_2) for $o_1 \neq o_2$ belongs to some M_i, and so the set of its origins is exactly the edges of M_{i-1}; those origins share in turn the same nonempty set of their own origins (which is the edge set of M_{i-2} if $i > 1$, or $\{(o, o) | o \in [n]\}$ if $i = 1$), which is disjoint to the set of origins of any edge not in M_{i-1}.

The second item of $\text{Next}_p(E, R)$ (with all its sub-items) now clearly follows from the connection (as per the definition of a graphic iterative matching) between M_i, the set of edges with (o_1, o_2) as an origin, and M_{i-1}, the set of edges having the same origin as that of (o_1, o_2).

Finally, $\text{Clear}_p(E, R)$ is satisfied: If a bridge edge has (o_1, o_2) as an origin then it belongs to M_i for some $i \geqslant 0$, so by the definition of a graphic iterative matching none of its vertices are contained in an edge of M_j for any $j > i$. There may be edges containing any of these vertices in M_j for some $j \leqslant i$, but in this case they are internal to the corresponding connected component of M_j (and are in fact internal to one of its color classes). □

Suppose now that we are given a structure $\langle [n], E, R \rangle$ that satisfies Im_p. To prove that it is an encoding of some iterative matching we first define inductively the graphs $\{M_i\}_{i \geqslant 0}$ and then prove that they form the matching which $\langle [n], E, R \rangle$ encodes.

Definition 23. Given a structure $\langle [n], E, R \rangle$ satisfying Im_p we define a sequence $\{M_i\}_{i \geqslant 0} = M_0, M_1, \ldots$ of graphs on $[n]$ inductively as follows.

- M_0 consists of all the edges having any (o, o) as an origin.
- M_i for $i > 0$ consists of all the edges having any edge from M_{i-1} as an origin.

We now show that the above sequence $\{M_i\}_{i \geqslant 0}$ is indeed an iterative matching, and that $\langle [n], E, R \rangle$ is its encoding.

Lemma 24. *The following holds for the above defined graphs.*

- *Every edge in M_0 has every (o, o) and no other pair as an origin, and every edge in M_i has every edge in M_{i-1} and no other pair as an origin.*
- *There is no edge in $M_i \cap M_j$ for any $i \neq j$.*
- *M_0 is a preserving matching between the p cliques of E.*
- *$\{M_i\}_{i \geqslant 0}$ is an iterative matching between the p cliques of E (in particular, the connected components of each M_i are isolated vertices and complete p-partite graphs).*
- *There are no other edges with origins (according to R) apart from those in $\bigcup_{i \geqslant 0} M_i$.*

Proof. The first two items follow by induction from $\langle [n], E, R \rangle$ satisfying the first item of Base_p and the first item of Next_p: It is clear from Base_p that the conditions concerning M_0 hold, as well as that $M_0 \cap M_j$ is empty for every $j > 0$. Given the induction hypothesis about the origins of $M_0, \ldots, M_{i-1}$ and their edge-disjointness from any M_j, it follows from the first item of Next_p that every edge of M_i has exactly

the edges of M_{i-1} as its origins. The disjointness of M_i and M_j for $j>i$ now follows from the disjointness of M_{i-1} and M_{j-1}, and the disjointness of M_i and M_j for $j<i$ follows directly from the induction hypothesis.

The third item above follows from the second item of Base_p. The fourth item follows by induction from the above together with the second item in Next_p (with all its sub-items), as it fully describes the connection between M_i and M_{i-1} (for $i>0$) in a graphic iterative matching $\{M_i\}_{i\geqslant 0}$.

Finally, the fifth item follows from $\langle [n], E, R\rangle$ satisfying Clear_p: Lemma 12 ensures that every vertex v is contained in a bridge edge in some M_j. It is not hard to see from the definition of an iterative matching that $\bigcup_{i\geqslant 0} M_i$ is a disjoint union of cliques (of possibly varying sizes). Now if a pair of vertices (u,v) is not an edge in $\bigcup_{i\geqslant 0} M_i$, then it is clearly not internal to the connected component of the M_j that contains a bridge edge containing v, so Clear_p (where we let (o_1,o_2) be any origin of this bridge edge) ensures that (u,v) has no origin.

Lemma 24 directly provides the final component required for the proof of Theorem 20.

Consequence 25. For every $\langle [n], E, R\rangle$ satisfying Im_p, the relation R is an encoding of an iterative matching between the p cliques of E.

Proof of Theorem 20. Claim 22 and Consequence 25 imply that the number of structures $\langle [n], E, R\rangle$ equals $b_p(n)$ times the number of possible iterative matchings between p sets of size $\frac{n}{p}$, and by Lemma 11 the latter number is 1 modulo p. □

Finally, we note that it is possible to formulate a property similar to Im_p that uses only a single quaternary relation R, by using "$R(u,u,v,v)$" to represent "$E(u,v)$" and changing the formulation of the property accordingly.

Acknowledgments

I am indebted to J.A. Makowsky, for introducing me to the Specker–Blatter Theorem and its related open questions, and for his various suggestions. I also wish to thank two anonymous referees for their suggestions, and for introducing me to the theory of combinatorial species.

References

[1] F. Bergeron, G. Labelle, P. Leroux, Combinatorial Species and Tree-like Structures, Cambridge University Press, Cambridge, 1998.
[2] C. Blatter, E. Specker, Le nombre de structures finies d'une théorie à caractère fini, Sci. Math. Fonds Nat. Rec. Sci. Bruxelles (1981) 41–44.
[3] C. Blatter, E. Specker, Modular periodicity of combinatorial sequences, Abstracts AMS 4 (1983) 313.

[4] C. Blatter, E. Specker, Recurrence relations for the number of labeled structures on a finite set, in: E. Börger, G. Hasenjaeger, D. Rödding (Eds.), In Logic and Machines: Decision Problems and Complexity, Lecture Notes in Computer Science, Vol. 171, Springer, Berlin, 1984, pp. 43–61.
[5] B. Bollobas, A probabilistic proof of an asymptotic formula of the number of regular labelled graphs, European J. Combin. 1 (1980) 311–316.
[6] H.D. Ebbinghaus, J. Flum, Finite Model Theory, Perspectives in Mathematical Logic, Springer, Berlin, 1995.
[7] N.J. Fine, Binomial coefficients modulo a prime, Amer. Math. Monthly 10 (1947) 589–592.
[8] E. Fischer, J.A. Makowsky, The Specker–Blatter theorem revisited, in preparation.
[9] I. Gessel, Combinatorial proofs of congruences, in: D.M. Jackson, S.A. Vanstone (Eds.), Enumeration and Design, Academic Press, New York, 1984, pp. 157–197.
[10] F. Harary, E. Palmer, Graphical Enumeration, Academic Press, New York, 1973.
[11] A. Joyal, Une théorie combinatoire des séries formelles, Adv. Math. 42 (1981) 1–82.
[12] E. Lucas, Théorie des fonctions numériques simplement périodiques, Amer. J. Math. 1 (1878) 184–240, 289–321.
[13] J.A. Makowsky, Specker's problem, in: E. Grädel, C. Hirsch (Eds.), Problems in Finite Model Theory, THE FMT Homepage, 2000. Last version: June 2000, http://www-mgi.informatik.rwth-aachen.de/FMT/problems.ps
[14] R.C. Read, The enumeration of locally restricted graphs, I, J. London Math. Soc. 34 (1959) 417–436.
[15] R.C. Read, The enumeration of locally restricted graphs, II, J. London Math. Soc. 35 (1960) 344–351.
[16] J.H. Redfield, The theory of group-reduced distributions, Amer. J. Math. 49 (1927) 433–455.
[17] E. Specker, Application of logic and combinatorics to enumeration problems, in: E. Börger (Ed.), Trends in Theoretical Computer Science, Computer Science Press, 1988, pp. 141–169 Reprinted in: Ernst Specker, Selecta, Birkhäuser, Basel, 1990, pp. 324–350.
[18] R.P. Stanley, Enumerative Combinatorics, Cambridge University Press, Cambridge, 1997 (Vol. 1, first appeared in 1986 and Vol. 2, in 1999).