Recurrence relations for the number of labeled structures on a finite set

Chr. Blatter and E. Specker (Zürich)

Introduction

Let C be a class of finite binary structures. An element of C is a finite set S endowed with a binary relation R. C is assumed to be closed under isomorphism. With such a class C a function f_C is associated as follows:

$$f_C(n) := \# \text{ structures on } \{1,2,\ldots,n\} \text{ belonging to } C .$$

We give some examples

(1) Class U of all structures

$$f_U(n) = 2^{n^2}$$

(2) Class G of all graphs

$$f_G(n) = 2^{\binom{n}{2}}$$

(3) Class E of all equivalence relations

$$f_E(n) = B_n \qquad \text{(Bell numbers)}$$

(4) Class $E2$ of all equivalence relations with two classes of same size

$$f_{E2}(2n) = \frac{1}{2}\binom{2n}{n}$$

(5) Class T of all trees

$$f_T(n) = n^{n-2} \qquad \text{(Cayley)}$$

(6) Let A be a nonempty subset of $\mathbb{N}\setminus\{0,1,2\}$. $C(A)$ is the class of all graphs which are n-gons , $n \in A$.

In some of these and many other cases it is well known that f_C satisfies a linear recurrence relation mod m, i.e. there exist integers $k, a_1, \ldots, a_k$ $(1 \leq k)$ such that for all n

$$f_C(n) \equiv \sum_{j=1}^{k} a_j \, f_C(n-j) \mod m$$

[5,6]. [6] contains an extensive list of references.

In the following we give rather general conditions on C for such relations to hold for all m.

Theorem

If C is the class of R-structures defined by a formula of monadic second order logic, then the function f_C satisfies for every m a linear recurrence relation mod m.

Corollary

If C is as in the theorem, then the function $f_C(\text{mod } m)$ is periodic for sufficiently large n.

The proof of the theorem is based on the notion of "class of finite character". A class of R-structures is of finite character iff there exist finitely many R-structures $E_1, \ldots, E_r$ such that the following holds: For every R-structure E there is an i $(1 \leq i \leq r)$ such that for all R-structures S and all x in S:

$$S(E/x) \in C \iff S(E_i/x) \in C ,$$

where $S(E/x)$ is the structure obtained from S by substituting E for x in a natural way. The theorem follows from

Theorem 1

If C is of finite character, then the thesis of the theorem holds.

Theorem 3

If C is as in the hypothesis of the theorem, then C is of finite character.

In the proof of this theorem, Ehrenfeucht-Fraïssé games play an essential role [3,4].

Referring to our examples, the classes introduced in (1), (2), (3) are definable by a formula of first order logic. The class of trees is definable by a formula of monadic second order (but not of first order) logic. In all these cases it is easy to give a direct proof that the character is finite; we shall carry this out for the case of trees. It is equally easy to verify that all the classes $C(A)$ introduced in (6) are of finite character. Since there are uncountably many of these, it follows that not all of them are definable by a formula of monadic second order. The class $E2$ is not of finite character and the function $f_{E2}(\text{mod } 2)$ is not periodic for large n, since the values of $f_{E2}(n)$ is odd iff n is an even power of 2. The class $E2$ is definable by a formula of second order logic.

The generalization to structures of several binary relations is immediate. Ternary relations, however, seem to present additional difficulties. The main results of this paper have been announced (and partly proved) in [1,2].

Modular counting

1. A structure for us is a pair $S := (X,R)$ consisting of a non-empty finite set X, the carrier of S, and a binary relation

$$R : X \times X \to \{0,1\}$$

on X. In keeping with common usage we let S denote the carrier of the structure S as well whenever feasible. The one point reflexive structure we denote by 1.

If $S = (S,R)$ is a structure and

$$E.: x \mapsto (E_x, R_x) \quad (x \in S)$$

is a family or list of structures with disjoint carriers E_x, indexed by the elements x of S, we denote by $S(E.)$ the compound structure on the set $\tilde{S} := \bigcup_{x \in S} E_x$ obtained by substituting the structures E_x into the points $x \in S$. The relation $\tilde{R}$ on $\tilde{S}$ is given by

$$\tilde{R}(e_1,e_2) := \begin{cases} R(x_1,x_2) & (e_i \in E_{x_i}\ ,\ x_1 \neq x_2) \\ R_x(e_1,e_2) & (e_1,e_2 \in E_x\ ,\ e_1 \neq e_2) \\ R(x,x) & (e_1 = e_2 \in E_x)\ . \end{cases}$$

This means: elements of different E_{x_i}'s are related by the rules valid in S whereas within an individual E_x we keep the relation R_x defined there but for the case $\tilde{R}(e,e)$, where (somewhat arbitrarily) the relation on S takes over.

If the family $b \mapsto E_b$ of structures to be substituted is restricted to a subset $B \subset S$, in particular to a single point $b \in S$, one may suppose that the list $b \mapsto E_b$ $(b \in B)$ is continued to all of S by the assignment $E_x := 1$ $(x \notin B)$. The resulting compound structure is denoted by $S(E./B)$ resp. by $S(E/b)$.

The following definition will be essential: A class C of structures, closed under isomorphism, is of <u>finite character</u> if there is a finite basis $\mathfrak{B}$ of structures and for any structure E a basis structure $E^{\S} \in \mathfrak{B}$ such that the following holds:

(§) For arbitrary compound structures $S(E.)$ one has

$$S(E.) \in C \quad \Longleftrightarrow \quad S(E.^{\S}) \in C\ .$$

We may assume $1 \in \mathfrak{B}$. The condition (§) is equivalent to the following:

(§') For arbitrary substitutions at a single point one has

$$S(E/b) \in C \quad \Longleftrightarrow \quad S(E^{\S}/b) \in C\ .$$

As a matter of fact a general compound structure founded on $S = \{b_1,\dots,b_n\}$ is isomorphic to the structure

$$S(E_1/b_1)(E_2/b_2) \ \dots \ (E_n/b_n)$$

obtained by successively substituting at a single point; furthermore the order of the individual substitutions is irrelevant.

In the light of (§') the above definition may be reformulated as follows: Call two structures E, E' C-<u>equivalent</u> and write $E \, \rho^C \, E'$, if for arbitrary substitutions at a single point one has

$$S(E/b) \in C \quad \Longleftrightarrow \quad S(E'/b) \in C \,.$$

Then C is of finite character iff there are only finitely many equivalence classes.

<u>Example.</u> Let T denote the class of trees and consider the set

$\mathfrak{B} :=$ 

of the four structures 1, S_2, S_3, S_4 indicated by our drawing. We will show that $\mathfrak{B}$ is a basis for T.

If $E = 1$ then $E \in \mathfrak{B}$. If an E consisting of $n > 1$ isolated points is substituted at a univalent point b of a tree S, then $S(E/b)$ is a tree; if such an E is substituted at a zero- or multivalent point b of a tree S, then $S(E/b)$ is disconnected or contains a circle, so is not a tree, and finally, if S is not a tree, then $S(E/b)$ is not a tree either. Hence all structures E consisting of more than one isolated points are T-equivalent, in particular T-equivalent to S_2. Now let E contain an edge but still be no tree. Then $S(E/b)$ will contain a triangle, if b is not isolated and will contain a non-tree as a component, if b is isolated. In other words, $S(E/b)$ will never be a tree, so $E \, \rho^T \, S_3$. Finally, if E is a tree on $n \geqslant 2$ points, then $S(E/b)$ will be a tree iff $S = 1$, so $E \, \rho^T \, S_4$.

For a given class C of structures we let $f_C(n)$ denote the number of C-structures on $\{1,2,\dots,n\}$. Since C remains fixed in the sequel we may drop the index C and write f instead of f_C, similarly with other objects attached to C.

Theorem 1

If C is a class of finite character, the function $f \pmod m$ satisfies for every module m a linear recurrence relation.

Corollary

If C is a class of finite character, the function $f \pmod m$ is periodic for sufficiently large n.

The proof of Theorem 1 is by induction on the number of prime divisors of m. In the process we shall actually prove a more general theorem (Theorem 2).

2. For a (possibly empty) set A we consider structures S on the carrier $A \dot{\cup} \{1,2,\ldots,n\}$. A permutation g of A induces a g-image S^g of S through

$$R^g(a,b) := R(g^{-1}(a), g^{-1}(b))$$

where we have tacitly put $g := \mathbb{1}$ on $\{1,2,\ldots,n\}$.

Now let G be a group of permutations of the set A and $\mathbb{A}$ a set of binary relations on A which is invariant under G. We denote by $U(A,G,\mathbb{A};n)$ the set of structures

$$S := (A \dot{\cup} \{1,2,\ldots,n\}, R)$$

with the following properties:

(2.1) $\quad S \in C$,

(2.2) $\quad R/A^2 \in \mathbb{A}$,

(2.3) $\quad g \in G^* := G \setminus \{\mathbb{1}\} \Rightarrow S^g \neq S$.

Theorem 2

If C is of finite character the function

$$n \mapsto |U(A,G,\mathbb{A};n)| \quad \mathrm{mod}(|G| \cdot m)$$

satisfies for every $m \geq 1$ a linear recurrence relation.

Theorem 1 is a special case of Theorem 2, for

$$f(n) = |U(\emptyset, \{\mathbb{I}\}, \emptyset; n)| .$$

3. Assume $m = 1$ and consider the equivalence relation

$$S \sim S' \quad :\iff \quad \exists g \in G \quad : \quad S^g = S'$$

on $U(A,G,\mathfrak{A}; n)$. Because of (2.3) each equivalence class consists of $|G|$ elements, hence

$$|U(A,G,\mathfrak{A}; n)| = 0 \qquad \mathrm{mod}\ |G|$$

for all n .

4. For the induction step we count an even more general set of structures. Let $A,G,\mathfrak{A}$ be as above and kept fixed. Let

$$(R_i', R_i'') \qquad (1 \leq i \leq r := 4^{|A|})$$

be the pairs of unary relations on A and $\vec{B} := (B_1,\ldots,B_r)$ be an r-tuple of disjoint sets, $B := \bigcup_{i=1}^{r} B_i$. We shall consider structures

$$S := (A \,\dot\cup\, B \,\dot\cup\, \{1,\ldots,n\} \ , \ R)$$

and their compound structures $S(E./B)$ for a given list $E. : B \to \mathfrak{B}$ of basis structures. Denote by $V(\vec{B},E.; n)$ the set of such structures S with the following properties:

(4.1) $\quad S(E./B) \in C$,

(4.2) $\quad R/A^2 \in \mathfrak{A}$,

(4.3) $$\left.\begin{aligned} R(a,b) &= R_i'(a) \\ R(b,a) &= R_i''(a) \end{aligned}\right\} \quad (a \in A \ , \ b \in B_i)$$

$$(4.4) \qquad g \in G^* \quad \Rightarrow \quad S^g \neq S \ .$$

We will show that the functions

$$(4.5) \qquad n \mapsto v(\ldots;n) := |V(\ldots;n)| \qquad \mathrm{mod}(|G|\cdot m)$$

satisfy a linear recurrence relation. In doing so we may assume Theorem 2 for proper divisors of m. Let $\mathcal{F}$ be the set of all functions (4.5).

5. Let p be a prime divisor of m and let $\mathcal{F}_o := \{v_j \mid 1 \leqslant j \leqslant s\}$ be the subset of those $v \in \mathcal{F}$ for which

$$|B_i| \leqslant (p-1)|\mathcal{B}| \qquad (1 \leqslant i \leqslant r) \ .$$

Lemma 1

For each $w \in \mathcal{F}$ there are numbers $a_j \in \mathbb{Z}$ and a function $q : \mathbb{N} \to \mathbb{N}$ satisfying a linear recurrence relation, such that

$$w = \sum_{j=1}^{s} a_j v_j + q \qquad \mathrm{mod}(|G|\cdot m) \ .$$

6. We first show that Lemma 1 implies Theorem 2.

Proof

Consider a structure $S \in V(\vec{B},E.;n)$. The last element n of S is in a certain way related to the individual elements of A, i.e., there is a certain i, $1 \leqslant i \leqslant r$, such that

$$R(a,n) = R_i'(a) \ , \quad R(n,a) = R_i''(a) \qquad (a \in A) \ .$$

If one adds the element n to the set B_i and inserts the structure 1 at the proper place into the list $E.$, one obtains objects $\vec{B}^{(i)}$ and $E.^{(i)}$, and S appears as an element of the set $V(\vec{B}^{(i)},E.^{(i)};n-1)$.

We thus have the natural identification

(6.1) $$V(\vec{B},E.;n) = \bigcup_{i=1}^{r} V(\vec{B}^{(i)},E.^{(i)};n-1) .$$

Consider now a fixed $v_k \in \mathcal{F}_o$. Because of (6.1) there are functions $w_i \in \mathcal{F}$ $(1 \leq i \leq r)$ with

$$v_k(n) = \sum_{i=1}^{r} w_i(n-1) ,$$

and by Lemma 1 there are numbers $a_{ij} \in \mathbb{Z}$ and functions p_i satisfying a linear recurrence relation such that

$$w_i = \sum_{j=1}^{s} a_{ij}v_j + p_i \qquad \mathrm{mod}(|G|\cdot m) .$$

Putting $\sum_{i=1}^{r} a_{ij} =: b_{kj}$, $\sum_{i=1}^{r} p_i =: q_k$ we thus have

$$v_k(n) = \sum_{j=1}^{s} b_{kj}v_j(n-1) + q_k(n-1) ,$$

which shows that the $v_k \in \mathcal{F}_o$ indeed satisfy a linear recurrence relation. Since

$$|U(A,G,\mathfrak{A};\cdot)| = v(\emptyset,\emptyset;\cdot) \in \mathcal{F}_o ,$$

Theorem 2 follows.

<u>7.</u> Let A , G , $\mathfrak{A}$, $\vec{B}$, $E.$ be as above.

<u>Lemma 2</u>

If $|B_1| > (p-1)|\mathfrak{B}|$, there are an r-tuple of sets $\vec{B}^*$ and t (to be explained later) corresponding lists $E.^{\S k}$ $(1 \leq k \leq t)$ of structures, furthermore a function q satisfying a linear recurrence relation, such that

(7.1) $$|B_1^*| = |B_1| - (p-1) ,$$

(7.2) $$B_i^* = B_i \qquad (i \neq 1) ,$$

(7.3) $$v(\vec{B},E.;n) = \sum_{k=1}^{t} v(\vec{B}^*,E.^{\S k};n) + q(n) \qquad \mathrm{mod}(|G|\cdot m) .$$

Lemma 1 is a consequence of Lemma 2.

8. Proof of Lemma 2

We may assume

$$B_1 = B_1' \uplus B_1'' , \quad B_1' = \{b_o, b_1, \ldots, b_{p-1}\}$$

with

$$E_{b_\ell} = E_o \qquad (0 \leq \ell \leq p-1) .$$

Consider the cyclic permutation

$$h_o : B_1' \to B_1' , \quad b_\ell \mapsto b_{\ell+1}$$

(the index ℓ taken mod p) which together with G (acting on A) generates a permutation group H of order $|H| = |G| \cdot p$.

The essential step now is to split the set of structures $V := V(\vec{B}, E.; n)$ into two classes according to the effect of h_o :

$$V_1 := \{S \in V | S^{h_o} \neq S\} , \quad V_2 := \{S \in V | S^{h_o} = S\} .$$

9. We first investigate the class V_1 and begin with the following

Lemma 3

If $S \in V_1$, then $S^h \neq S$ for all $h \in H^*$.

Proof

Assume $S^h = S$ for some $h = gh_o^\ell$, $g \in G$. If $\ell = 0$ then $S^g = S$, hence $g = \mathbb{1}$ because of (4.4), thus $h = \mathbb{1}$. This leaves $\ell \neq 0$, hence $h_1 := h_o^\ell \neq \mathbb{1}$. Since p is prime we have $S^{h_1} = S$ as well. From this and $S^{gh_1} = S$ we conclude $g \neq \mathbb{1}$. Again by (4.4) we can find elements

$$c_1, c_2 \in A \uplus B \uplus \{1, 2, \ldots, n\}$$

with $R(c_1, c_2) \neq R(g(c_1), g(c_2))$, and since g affects only the points of A we may assume $c_1 \in A$. On the other hand

$$(9.1) \qquad R(c_1,c_2) = R(gh_1(c_1),gh_1(c_2))$$

$$= R(g(c_1),gh_1(c_2)) \;,$$

which implies $h_1(c_2) \neq c_2$, hence $c_2 \in B_1'$. This and (4.3) allow us to continue (9.1) in the following way:

$$= R(g(c_1),h_1(c_2)) = R(g(c_1),c_2)$$

$$= R(g(c_1),g(c_2)) \;.$$

So we have a contradiction to our assumption on c_1 , c_2 which proves Lemma 3.

10. Put $A' := A \uplus \biguplus_{b\in B} E_b$. When the $S \in V_1$ are restricted to $A \uplus B$ and the E_b are substituted we obtain on A' a set of structures $\mathbb{A}'$. Because of Lemma 3 we may write

$$V_1(\vec{B},E.;n) = U(A',H,\mathbb{A}';n) \;.$$

We now apply Theorem 2 with the module $m' := \frac{m}{p}$ and draw the following conclusion: The function

$$n \mapsto |U(A',H,\mathbb{A}';n)| \qquad \mathrm{mod}(|H|\cdot\tfrac{m}{p})$$

satisfies a linear recurrence relation, and because of $|H| = |G|\cdot p$ this in turn implies that the function

$$q := |V_1(\vec{B},E.;\cdot)| \qquad \mathrm{mod}(|G|\cdot m)$$

satisfies a linear recurrence relation.

11. We now turn to the set V_2 which contains the structures from $V(\vec{B},E.;n)$ invariant under h_o . Put

$$B_1^* := \{b_o\} \uplus B_1'' \;,\; \vec{B}^* := (B_1^*,B_2,\ldots,B_r) \;;$$

denote by $W(\vec{B};n)$ the set of structures

$$S = (A \uplus B \uplus \{1,2,\dots,n\}, R)$$

for which (4.2), (4.3), (4.4) hold (this means that $S(E./B) \in C$ is not required) and by $W_2(\dots)$ the set of those $S \in W(\dots)$ for which $S^{h_o} = S$. Finally let $\mathfrak{V}$ be the set of structures σ_k $(1 \leqslant k \leqslant t)$ on B_1' invariant under h_o (so $t := |\mathfrak{V}|$).

12. Lemma 4

The restrictions

$$\alpha_1(S) := S|A \uplus B^* \uplus \{1,2,\dots,n\}, \quad \alpha_2(S) := S|B_1'$$

define a bijective map

$$\alpha : W_2(\vec{B}; n) \to W(\vec{B}^*; n) \times \mathfrak{V} .$$

Proof

If $g \in G^*$ there is $c_1 \in A$ and c_2 with $R(c_1,c_2) \neq R(g(c_1),g(c_2))$. This already implies $(\alpha_1(S))^g \neq \alpha_1(S)$ in the case $c_2 \notin B_1'$. If $c_2 \in B_1'$ we also have $R(c_1,b_o) \neq R(g(c_1),b_o)$ because of (4.3), hence $(\alpha_1(S))^g \neq \alpha_1(S)$ in this case too. This means that α is a well defined map into the indicated cartesian product.

Assume now $S_1 \neq S_2$ but $\alpha_2(S_1) = \alpha_2(S_2)$. We then can find $c_1 \notin B_1'$ and c_2 with $R_1(c_1,c_2) \neq R_2(c_1,c_2)$. This already implies $\alpha_1(S_1) \neq \alpha_1(S_2)$ in the case $c_2 \notin B_1'$. If $c_2 \in B_1'$ we conclude from $S_i^{h_o} = S_i$ $(i = 1,2)$ that $R_1(c_1,b_o) \neq R_2(c_1,b_o)$, hence $\alpha_1(S_1) \neq \alpha_1(S_2)$ also in this case.

Finally for two given structures

$$\hat{S} \in W(\vec{B}^*; n), \quad \sigma \in \mathfrak{V}$$

consider the structure

$$S = (A \uplus B \uplus \{1,2,\dots,n\}, R) \in W_2(\vec{B}; n)$$

defined by

$$R(c_1,c_2) := \begin{cases} \hat{R}(c_1,c_2) & (c_1,c_2 \notin B_1') \\ R^{\sigma}(c_1,c_2) & (c_1,c_2 \in B_1') \\ \hat{R}(c_1,b_o) & (c_1 \notin B_1',\ c_2 \in B_1') \end{cases} .$$

For this S one has $\alpha(S) = (\hat{S}, \sigma)$, hence Lemma 4 is proven.

13. For each $\sigma_k \in \mathfrak{V}$ we define a list $E_{\cdot}^{k}$ on B^* as follows:

$$E_b^k := \begin{cases} E_b & (b \in B^*,\ b \neq b_o) \\ \\ \sigma_k((E_o,\ldots,E_o)) & (b = b_o) \end{cases} .$$

This means that at the point b_o a compound structure has to be substituted, namely the h_o-invariant structure resulting from substituting E_o at every point of σ_k. To this structure there is an equivalent basis structure $E^{\S} \in \mathfrak{B}$ which allows us to form the definitive list

$$E_b^{\S k} := \begin{cases} E_b & (b \in B^*,\ b \neq b_o) \\ \\ E^{\S} & (b = b_o) \end{cases} .$$

With these notations we have

$$(13.1) \qquad |V_2(\vec{B},E.;n)| = \sum_{k=1}^{t} |V(\vec{B}^*,E_{\cdot}^{\S k};n)|$$

Proof

A structure S belongs to V_2 iff $S \in W_2(\vec{B};n)$ and $S(E./B) \in C$. Now by Lemma 4 the structures $S \in W_2(\vec{B};n)$ correspond bijectively to the pairs of structures from

$$W(\vec{B}^*;n) \times \{\sigma_1,\ldots,\sigma_t\} .$$

Consider such an S and let $\alpha_2(S) = \sigma_k$. Then one has

$$S(E./B) = \alpha_1(S)(E_{\cdot}^{k}/B^*) ,$$

and because of (§) we may write

$$S(E./B) \in C \iff \alpha_1(S)(E.^k/B^*) \in C$$

$$\iff \alpha_1(S)(E.^{\S k}/B^*) \in C$$

$$\iff \alpha_1(S) \in V(\vec{B}^*, E.^{\S k}; n) .$$

From this we conclude that the structure S is counted on the left of (13.1) iff it is counted on the right.

14. Lemma 2 now follows from the conclusion of section 10 and (13.1).

Logic and classes of finite character

We recall the definition of the Ehrenfeucht-Fraïssé game $G_n(S_1,S_2)$ associated to R-structures S_1, S_2 and a natural number n [3,4]: A play of the game $G_n(S_1,S_2)$ consists of a sequence of n moves of the two players I, II. The i^{th} move $(i = 1,\dots,n)$ of player I is the choice of either an element or a subset of one of the structures S_1, S_2; the i^{th} move of player II is the choice of an object of the same type as the choice of I in the i^{th} move but in the other structure. So in the i^{th} move two objects s_i^1, s_i^2 belonging to S_1 resp. S_2 are selected; both are either elements or both subsets. After a particular play of the game there have been chosen two sequences $(s_1^1,\dots,s_n^1)$, $(s_1^2,\dots,s_n^2)$. Player II has won this play iff these sequences are isomorphic, i.e. iff for all i, j $(1 \leqslant i, j \leqslant n)$ the following conditions are satisfied:

(1) If s_i^1, s_j^1 are elements (and therefore also s_i^2, s_j^2):

$$s_i^1 = s_j^1 \text{ iff } s_i^2 = s_j^2 ; \; R(s_i^1,s_j^1) \text{ iff } R(s_i^2,s_j^2) .$$

(2) If s_i^1 is an element (and therefore also s_i^2) and s_j^1 is a

set (and therefore also s_j^2) :

$$s_i^1 \in s_j^1 \text{ iff } s_i^2 \in s_j^2 .$$

The notion of winning strategy for a player is defined in the usual way. Roughly speaking, a strategy tells the player what to do in any situation that might arise during play; the strategy is a winning strategy if the player wins irrespectively of the moves of his opponent. Clearly, if the structures S_1 , S_2 are isomorphic, player II has a winning strategy in the game $G_n(S_1,S_2)$.

The relation defined by "Player II has a winning strategy in the game $G_n(S_1,S_2)$ " will be abbreviated by "$S_1 \ \omega_n \ S_2$ " .

The following two lemmas are known [3,4]:

<u>Lemma 5</u>

For all n , the relation ω_n is an equivalence relation with a finite number of equivalence classes.

<u>Lemma 6</u>

For a formula Φ of monadic second order logic in the predicates R and $=$, there exists a natural number n such that for all R-structures S_1 , S_2 :

If $S_1 \, \omega_n \, S_2$ then $S_1 \models \Phi$ iff $S_2 \models \Phi$.

<u>Remark</u>

A formula of monadic second order logic is a formula in individual variables $x_o,x_1,\ldots$ and in set variables $Y_o,Y_1,\ldots$; prime formulas are of the type $x_1 = x_2$, $R(x_1,x_2)$, $x_1 \in Y_1$; formulas are quantified with respect to individual and set variables. The fact that a formula Φ holds in the structure S is abbreviated by $S \models \Phi$.

<u>Lemma 7</u>

If two R-structures E_1 , E_2 satisfy $E_1 \ \omega_n \ E_2$, then for all

R-structures S and all x in S : $S(E_1/x)\ \omega_n\ S(E_2/x)$.

Proof

Let τ be a winning strategy for player II in the game $G_n(E_1,E_2)$. We may (and will) assume that the choice of the empty set by player I is immediately followed by the choice of the empty set by II. Let S be an R-structure and x an element of S ; we put $S_k = S(E_k/x)$, $k = 1,2$. In order to define a winning strategy for player II in the game $G_n(S_1,S_2)$, a partial play of the game $G_n(E_1,E_2)$ is associated to each partial play of the game $G_n(S_1,S_2)$. A partial play of the game $G_n(S_1,S_2)$ defines two sequences $(s_1^1,\dots,s_i^1)$, $(s_1^2,\dots,s_j^2)$, where $i = j$ or $i = j+1$ according to whether it is I's or II's move; the objects s_h^k are elements or subsets of S_k $(k = 1,2)$, s_h^1 and s_h^2 being of the same type. We define

$$t_h^k = t(s_h^k)$$

as the following object of the structure E_k : If s_h^k is an element of the substructure E_k of S_k , then t_h^k is equal to s_h^k ; if s_h^k is another element of S_k , i.e. an element of $S\setminus\{x\}$, then t_h^k is the empty set. If s_h^k is a subset of S_k , then t_h^k is the restriction of this set to E_k . The strategy σ of player II (which we are going to define) will have the following property:
If II plays according to σ and if a partial play results in the sequences $(s_1^1,\dots,s_i^1)$, $(s_1^2,\dots,s_i^2)$ $(i \leq n)$, then

(1) The pair of sequences is isomorphic.

(2) If s_h^1 is an element of $S\setminus\{x\}$, then $s_h^2 = s_h^1$.

(3) If s_h^1 is an element of E_1 , then s_h^2 is an element of E_2 .

(4) If s_h^1 is a subset of S_1 , then
$s_h^1 \cap (S\setminus\{x\}) = s_h^2 \cap (S\setminus\{x\})$.

(5) If the pair $(t_1^1,\dots,t_i^1)$, $(t_1^2,\dots,t_i^2)$ is the associated pair, then for all j the choice of t_j^2 corresponds to the strategy τ of II $(1 \leq j \leq i)$.

In order to define a winning strategy for player II it suffices to extend a pair

$$(s^1_1,\dots,s^1_i)\ ,\ (s^2_1,\dots,s^2_{i-1}) \text{ — }$$

where the pair

$$(s^1_1,\dots,s^1_{i-1})\ ,\ (s^2_1,\dots,s^2_{i-1})$$

satisfies conditions (1) - (5) — to a pair $(s^1_1,\dots,s^1_i)$, $(s^2_1,\dots,s^2_i)$ satisfying the conditions (1) - (5). This is done as follows:

If s^1_i is an element of $S\setminus\{x\}$, then s^2_i is put equal to s^1_i ; we then have $t^1_i = t^2_i = \emptyset$, satisfying condition (5). Otherwise we consider the associated pair $(t^1_1,\dots,t^1_i)$, $(t^2_1,\dots,t^2_{i-1})$, which corresponds to a partial play of the game $G_n(E_1,E_2)$, played by player II according strategy τ . Therefore, the strategy τ extends this pair to an isomorphic pair $(t^1_1,\dots,t^1_i)$, $(t^2_1,\dots,t^2_i)$. In this case, the object s^2_i is defined as follows: If s^1_i is an element of E_1 , hence equal to t^1_i , s^2_i is put equal to t^2_i , which is then an element of E_2 . If s^1_i is a subset of S_1 , s^2_i is defined as the union of $s^1_i \cap (S\setminus\{x\})$ and t^2_i ; s^1_i being a set, also t^1_i and t^2_i are sets. From these definitions, it follows immediately that the sequences $(s^1_1,\dots,s^1_i)$, $(s^2_1,\dots,s^2_i)$ satisfy conditions (2), (3), (4), (5). It remains to check the isomorphism of the pair. All relations R , $=$, ε being binary, it suffices to investigate the pairs (s^1_h,s^1_j) , (s^2_h,s^2_j) , $1 \leq h$, $j \leq i$. Assume that one of the objects s^1_h , s^1_j - say s^1_h - is an element of $S\setminus\{x\}$; then $s^2_h = s^1_h$. Clearly , if s^1_j is also an element, then $s^1_h = s^1_j$ iff $s^2_h = s^2_j$ and, if s^1_j is a set $s^1_h \in s^1_j$ iff $s^2_h \in s^2_j$. Assume - besides s^1_h being an element of $S\setminus\{x\}$ - that s^1_j is an element; we then have to show

$$R(s^1_h,s^1_j) \quad \text{iff} \quad R(s^2_h,s^2_j)\ .$$

If s^1_j is in $S\setminus\{x\}$, then $s^2_j = s^1_j$ and the equivalence holds trivially. If s^1_j is in E_1 , then $R(s^1_h,s^1_j)$ iff $R^S(s^1_h,x)$; s^2_j being an element of E_2 , we also have $R(s^2_h,s^2_j)$ iff $R^S(s^2_h,x)$ and the equivalence is established because of $s^2_h = s^1_h$.

Assume now that s_h^1 is an element of E_1 ; then $s_h^1 = t_h^1$ and $s_h^2 = t_h^2$, s_h^2 being an element of E_2 . If s_j^1 is an element of E_1 , then - in the case $s_h^1 \neq s_j^1$ -

$$R(s_h^1, s_j^1) \text{ iff } R^{E_1}(t_h^1, t_j^1) .$$

The isomorphism of the pair (t_h^1, t_j^1) , (t_h^2, t_j^2) implies $R^{E_1}(t_h^1, t_j^1)$ iff $R^{E_2}(t_h^2, t_j^2)$. Together with $R(s_h^2, s_j^2)$ iff $R^{E_2}(t_h^2, t_j^2)$ we obtain $R(s_h^1, s_j^1)$ iff $R(s_h^2, s_j^2)$. In the case $s_h^1 = s_j^1$, we also have $s_h^2 = s_j^2$ and therefore $R(s_h^k, s_j^k)$ iff $R^S(x,x)$, $k = 1,2$, yielding the desired result. The case of the equality relation instead of R is trivial.

Assume finally that s_j^1 is a set; then $s_h^1 \in s_j^1$ iff $t_h^1 \in t_j^1$; furthermore $t_h^1 \in t_j^1$ iff $t_h^2 \in t_j^2$ and $t_h^2 \in t_j^2$ iff $s_h^2 \in s_j^2$.

We thus have considered all cases, h and j being symmetric and no relation being defined if s_h^1 and s_j^1 are sets.

<u>Theorem 3</u>

The class of models of a formula of monadic second order logic in the binary predicates R , = is a class of finite character.

<u>Proof</u>

Let Φ be a formula as in the theorem. According to Lemma 6, there exists an integer n such that for all R-structures S_1 , S_2 : $S_1 \,\omega_n\, S_2$ implies $(S_1 \models \Phi \iff S_2 \models \Phi)$. If C is the class of models of Φ , we have

$$(S_1 \models \Phi \iff S_2 \models \Phi) \text{ iff } (S_1 \in C \iff S_2 \in C) ,$$

in other words

$$S_1 \,\omega_n\, S_2 \text{ implies } (S_1 \in C \iff S_2 \in C) .$$

Let E_1 , E_2 be R-structures and assume $E_1 \,\omega_n\, E_2$. Then, by Lemma 7, for all R-structures S : $S(E_1/x) \,\omega_n\, S(E_2/x)$, i.e. $S(E_1/x) \in C \iff S(E_2/x) \in C$.

By the definition of the equivalence relation ρ^C we thus have for all E_1, E_2:

$$E_1 \, \omega_n \, E_2 \Rightarrow E_1 \, \rho^C \, E_2 .$$

ω_n having finitely many classes by Lemma 5, the same holds for ρ^C, proving the theorem.

References

[1] Chr. Blatter et E. Specker, Le nombre de structures finies d'une théorie à caractère fini, Sciences Mathématiques, Fonds National de la Recherche Scientifique, Bruxelles 1981, 41-44

[2] Chr. Blatter and E. Specker, Modular periodicity of combinatorial sequences, Abstracts Am. Math. Soc. 4 (1983), 313

[3] A. Ehrenfeucht, Application of games to some problem of mathematical logic, Bull. Acad. Pol., Cl. III, 5 (1957), 35-37

[4] R. Fraïssé, Sur quelques classifications des systèmes de relations, Publ. Sci. Univ. Alger Ser. A, 1 (1954), 35-182

[5] I.M. Gessel, Combinatorial proofs of congruences, preprint

[6] T.S. Motzkin, Sorting numbers for cylinders and other classification numbers, Proc. of Symposia in pure mathematics 19 (1971), 167-176

Mathematisches Seminar

Eidgenössische Technische Hochschule Zürich

ETH-Zentrum

CH - 8092 Zürich