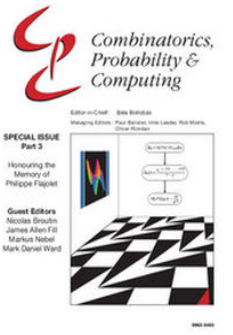

Modular Counting and Substitution of Structures

E. SPECKER

Combinatorics, Probability and Computing / Volume 14 / Issue 1-2 / January 2005, pp 203 - 210
DOI: 10.1017/S0963548304006698, Published online: 15 February 2005

Combinatorics, Probability and Computing (2005) 14, 203–210.
DOI: 10.1017/S0963548304006698 Printed in the United Kingdom

Modular Counting and Substitution of Structures

E. SPECKER,

Eidgenössische Technische Hochschule Zürich,
ETH Zentrum, HG, Rämistrasse 101, CH-8092 Zürich
(e-mail: specker@math.ethz.ch)

Received 30 December 2002; revised 28 June 2003

Dedicated to the memory of Walter Deuber

The aim of this paper is to point to a difference between binary and hyperary structures. The modular counting functions of a class of structures defined by a sentence of second-order monadic logic with equality, based on binary relations, are ultimately periodic. However, this is not the case for sentences based on quaternary relations.

1. Introduction

The aim of this paper is to point to a difference between binary and hyperary structures. (Graphs are binary structures, hypergraphs are hyperary structures, *i.e.*, ternary, quaternary, *etc.*).

All structures considered are finite, and all classes of structures are closed under isomorphism. The counting function of a class **C** counts the number of labelled structures in **C** in a set of n elements. Modular counting functions are counting functions reduced modulo an integer $m \geqslant 2$.

Example. The counting function of the class **B** of equivalence relations is given by the Bell numbers $B(n)$. Modulo 2, it satisfies the recurrence $B(n) = B(n-1) + B(n-2)$; the sequence $B(n)$ mod 2 is therefore periodic. The real number b_m whose m-ary representation is the sequence $B(n)$ mod m is called the *class number* mod m of **B**. For example, b_2 is equal to $5/7$.

The paper consists of three independent parts. In the first part, the following theorem is reviewed.

Theorem 1.1. ([1, 2, 3, 9, 10]) *The modular counting functions of a class* **C** *of structures defined by a sentence of second-order monadic logic with equality* (*cf.*, *e.g.*, [10]), *based on*

binary relations, satisfy a linear recursion relation and are therefore ultimately periodic, i.e., the class numbers of **C** *are rational numbers.*

A proof is sketched for the case of one binary relation and prime moduli.
The second part is devoted to a theorem of Eldar Fischer.

Theorem 1.2. (Eldar Fischer [6]) *For every modulus m there exists a sentence S in the language* $\mathbf{L_1}$ *of first-order logic with equality, based on a quaternary relation, such that the counting function* mod *m of the class of models of S is not ultimately periodic.*

By a slight modification of Fischer's construction, a sentence S is defined in $\mathbf{L_1}$, based on a quaternary relation, such that the following holds. The cardinalities of models of S are powers of 2. On a given set, any two models are isomorphic; their automorphism group is the 2-Sylow subgroup of the symmetric group; the number of labelled structures is odd. The class number mod 2 of the class of these structures is therefore irrational.
The third part concludes the paper with a list of problems.

2. Binary relations

Definition of substitution. For binary structures (A, R), (B, S) on disjoint sets A, B, and an element a in A, a structure (C, T) is defined as follows: C is the union of $A \setminus \{a\}$ and B. On $A \setminus \{a\}$, T coincides with R; on B it coincides with S. If x is an element of $A \setminus \{a\}$ and y an element of B, then $T(x, y)$ equals $R(x, a)$ and $T(y, x)$ equals $R(a, x)$. The structure (C, T) is designated $\mathrm{Sub}(A, R, a, B, S)$; it is called a *substitutional instance* of the two structures.

Definition of C-equivalence. Given a class **C** of binary structures, two binary structures (B, S), (B', S') are **C**-*equivalent* if, for all binary structures (A, R) and all a in A, either both of the structures $\mathrm{Sub}(A, R, a, B, S)$, $\mathrm{Sub}(A, R, a, B', S')$ belong to **C** or neither does.

Definition of finite character. A class **C** is of *finite character* if the number of **C**-equivalence classes is finite. (The number of classes is called the *index of* **C**.)

Example. The class of 3-colourable graphs has index 4. Three of the classes consist of those graphs with chromatic number exactly i, for $i = 1, 2, 3$; the fourth consists of all other binary relations.

Theorem 2.1. *If a class of binary structures is definable by a formula of monadic second order, then it has finite character.*

Theorem 2.2. *If a class of binary structures has finite character, then its modular counting functions are ultimately periodic.*

A proof of Theorem 2.1 will be given on the basis of the Fraïssé–Ehrenfeucht interpretation of monadic second-order logic [4, 5, 8]. Given a number n and two binary

structures $S_i = (V_i, R_i)$ $(i = 1, 2)$ on disjoint sets V_1, V_2, a two-person game $G(n, S_1, S_2)$ is defined as follows. Both players have n half-moves; at each move, players I and II choose alternately either an element or a subset of V_1, V_2. The choices have to satisfy the condition that, at every move, either two elements or two subsets are chosen, one in V_1 and the other in V_2. (As player I chooses first, this rule restricts the moves of player II.) Once a play is over, there are chosen sequences $(a_1, \ldots, a_n)$ and $(b_1, \ldots, b_n)$. Player II wins if and only if these sequences are isomorphic, *i.e.*, if a_i and a_k are elements, then $a_i = a_k$ if and only if $b_i = b_k$, and $R(a_i, a_k)$ if and only if $R'(a_i, a_k)$, while if a_i is an element and a_k a subset, then $a_i \in a_k$ if and only if $b_i \in b_k$.

Definition of *n*-equivalence. The structures S_1, S_2 are *n-equivalent* if player II has a winning strategy in the game $G(n, S_1, S_2)$.

Lemma 2.3. ([5, 8]) *The relation of n-equivalence has finitely many equivalence classes.*

Lemma 2.4. ([5, 8]) *To each sentence S of monadic second order there corresponds an integer n such that the following holds: if two structures A, B are n-equivalent then the sentence S holds in A if and only if it holds in B.*

Theorem 2.5. *If two structures are n-equivalent, so are their substitutional instances.*

Sketch of proof. Let S_i $(i = 1, 2)$ be two n-equivalent binary structures and let S_i' $(i = 1, 2)$ be two substitutional instances in a structure T. A winning strategy in the game $G(n, S_1', S_2')$ for player II is defined on the basis of a winning strategy in the game $G(n, S_1, S_2)$ as follows. If player I has chosen an element in one of the sets S_1, S_2, then player II chooses according to his strategy in the game $G(n, S_1, S_2)$ (taking into account the elements and subsets already chosen in the substructure). If player I has chosen an element outside S_1, then player II chooses the same element. If player I has chosen a subset s, then II applies the following strategy: he represents s as a union of s' and $s \setminus s'$, where $s' = s \cap S_1$, determines corresponding sets and chooses their union.

The following proof of Fermat's theorem is the prototype of the proof of Theorem 2.2. Let the graph G be the cycle with p edges (p prime) coloured by c colours. There are c^p such colourings. In order to determine $c^p \bmod p$, notice that the set of coloured circles obtained by rotating a given circle p times has either 1 or p elements. Therefore $c^p \bmod p$ is equal to the number of colourings which are invariant under rotations. Since the number of such colourings is equal to c, then c^p is equal to $c \pmod p$.

How can this method of counting mod p be generalized to a class $\mathbf{C}$ of structures where counting invariant structures is not easier than counting all structures? Invariant structures being smaller (in a sense to be specified) than general structures, it suffices to generalize the concept of $\mathbf{C}$-structure in such a way that invariant structures are smaller $\mathbf{C}$-structures. This can be done in the case of classes of finite character.

Theorem 2.6. *Let* $\mathbf{C}$ *be a class of binary structures of index m, and let p be a prime number. Then there exist* p^m *functions from* $\mathbb{N}$ *to* $\mathbb{N}$ *such that:*

- *one of these functions is the counting function of the class* $\mathbf{C}$,
- *the functions* mod p *satisfy a linear recursion relation with constant coefficients: they are therefore ultimately periodic.*

Remark. An analogous theorem holds for all moduli, but the following sketch proof does not cover the general case.

Proof. Assume that $\mathbf{C}$ is of index m (equivalence classes: $\mathbf{C}(1),\dots,\mathbf{C}(m)$), and let j be a sequence $(j_1,\dots,j_k)$ with $1 \leqslant j_h \leqslant m$. A structure T on the set $\{1,\dots,n\}$ is a $\mathbf{C}$-j-*structure* if the structure obtained from T by replacing each h, $1 \leqslant h \leqslant k$, by a structure of the class $\mathbf{C}(j_h)$ is a $\mathbf{C}$-structure (*i.e.*, a structure in $\mathbf{C}$). Functions f^j are defined as follows: $f^j(n)$ is the number of $\mathbf{C}$-j-structures on $\{1,\dots,n\}$ (for $k \leqslant n$: otherwise $f^j(n) = 0$). Let J be the set of sequences j such that $j_h \leqslant j_{h+1}$ and $j_h < j_{h+p-1}$ (*i.e.*, at most $p-1$ of the numbers j_h are equal). The length $\ell(j)$ of such a sequence is at most pm, and there are p^m sequences in J.

The set of functions f^j $(j \in J)$ satisfies the requirements of Theorem 2.6.

(1) If e is the empty sequence, then $\mathbf{C}$-e- and $\mathbf{C}$-structures are the same.

(2) The representation of $f^j(n)$ as a linear combination, mod p, of functions with smaller argument is obtained by the following procedure. Setting $l(j) = k$, rotate the elements $k+1,\dots,k+p$ of the set $\{1,\dots,n\}$. Now $f^j(n)$ is equal, mod p, to the number of invariant $\mathbf{C}$-j-structures. Each such invariant structure defines a substructure on the set $\{k+1,\dots,k+p\}$ belonging to some class $\mathbf{C}(h)$. By inserting h in the sequence j at the right place, a sequence j^* is defined (not necessarily being an element of J) and $f^j(n)$ is congruent mod p to the sum (extended over all these j^*) of $f^{j^*}(n-p+1)$. If j^* is not an element of J, j^* contains a constant subsequence of length p. Rotating the corresponding indices and counting only the invariant structures, p substitutions can be replaced by a single substitution. The corresponding lengths are reduced by $p-1$. After at most $m-1$ iterations of this process, sequences of J will be obtained and the cardinalities of the structures will be at least $n-d$, where d depends only on m and p, but not on n. (A possible choice for d is $(m+1)(p-1)$, presumably much too large.) By replacing in each step the counting functions by the corresponding linear combination, f^j is represented mod p as a linear combination of values $f^i(n-k)$ ($i \in J$ and $1 \leqslant k \leqslant d$).

Ultimate periodicity follows immediately as the number of sequences

$$\left(f^{j(1)}(n),\dots,f^{j(t)}(n)\right), \quad J = \{j(1),\dots,j(t)\}$$

is finite. □

3. Fischer's theorem

Theorem 3.1. (Eldar Fischer [6]) *For every modulus m, there exists a first-order sentence* $S(m)$ *in a quaternary relation such that the counting function* mod m *is not ultimately periodic.*

Fischer's sentence $S(2)$ has the following property: the number of models on a set of n elements is odd if and only if n is a power of 2. The following modification of Fischer's proof yields a somewhat sharper theorem for the case $m = 2$.

Let V be a finite set and let c be a symmetric map from $V \times V$ onto an initial segment $(0, \ldots, r)$ of $\mathbb{N}$. With such a pair (V, c) is associated a sequence of graphs G_k $(k = 0, \ldots, r)$: the vertex set of G_k is V, and its edge relation holds if and only if $c(x, y) \leqslant k$. The pair (V, c) may be viewed as a complete graph with edges coloured by the colours $0, \ldots, r$. It is also denoted by (V, r, c).

A pair (V, c) is a cc-*graph* (*completely coloured graph*) of order r if the following conditions are satisfied.

(CC1) The components of the graphs G_k are complete graphs (with a loop at each vertex).
(CC2) The vertex set of G_0 is V; its components are singletons.
(CC3) For $0 \leqslant k \leqslant r$, each component of G_{k+1} is the union of two different components of G_k.

The graph G_{r-1} of a cc-graph (V, c) of order r has exactly two components V_1, V_2. The induced structures (V_1, c), (V_2, c) are cc-graphs of order $r - 1$.

Theorem 3.2.

(1) *The cardinality of a* cc-*graph of order* r *is* 2^r.
(2) *There is exactly one unlabelled* cc-*graph of order* r.
(3) *If* $n = 2^r$, *then there are* $n!/2^{n-1}$ *labelled* cc-*graphs of order* r *on a set of* n *elements. Their automorphism group has* 2^{n-1} *elements.*
(4) $n!/2^{n-1}$ *is odd. The automorphism group of a* cc-*graph is the* 2-*Sylow subgroup* (2SSG) *of the symmetric group.*

Proof. The proofs are by induction on the order r, the case $r = 0$ being obvious.

(1) If the two components of the cc-graph G_r associated with a cc-graph of order $r + 1$ have 2^r elements, then the graph G_{r+1} has 2^{r+1} elements.

(2), (3) A cc-graph $(V, r + 1, c)$ is determined by the splitting of V into the two components and by the induced substructures on these parts, which proves (2). The number of splittings of a set of $2n$ elements into two equal parts is $\frac{1}{2}(2n)!/n!^2$. The product of this number with the square of $n!/2^{n-1}$ is equal to $(2n)!/2^{2n-1}$. The automorphisms of $(V, r + 1, c)$ mapping the two substructures (V_i, r, c) onto themselves form a subgroup of index two. This group is isomorphic to the direct sum of the automorphism groups of (V_i, r, c), $i = 1, 2$. The product $2 \times 2^{n-1} \times 2^{n-1}$ is equal to 2^{2n-1}.

(4) Let $\exp(k)$ be the exponent of 2 in the prime factorization of k. A simple argument shows that $\exp((2n!)) = n + \exp(n!)$, and hence inductively that $\exp(n!) = n - 1$ when n is a power of 2. Since the order of the automorphisms of a cc-graph with n elements is 2^{n-1}, it is the 2SSG of the symmetric group. □

Corollary 3.3. *There are exactly two unlabelled graphs of cardinality* 2^r *whose automorphism group is the* 2-*Sylow subgroup of the symmetric group of order* 2^r.

Sketch of proof. All 2SSGs being conjugate, a 2SSG of the symmetric group of order 2^r is the automorphism group of a (V, r, c). A simple argument shows that the following two graphs on V are the only graphs having the same automorphisms as (V, r, c): the graph G whose edges are the edges which are coloured in (V, r, c) by an odd (alternatively, by an even) colour.

Example. With $r = 3$ and even colours, the graph is the union of two quadrilaterals.

Theorem 3.4. cc-*graphs can be coded as quaternary structures satisfying a first-order condition.*

In other words, we have the following result.

Theorem 3.5. *There exists a first-order sentence S in a quaternary relation R, and a canonical bijection from the set of* cc-*graphs on V to the set of models of S on V.*

Proof. The proof is carried out in three steps.

(S1) A quaternary relation R is associated to a cc-graph.
(S2) First-order sentences satisfied by this relation are formulated.
(S3) It is shown that a relation satisfying these sentences is associated to a cc-graph.

(S1) $R(u_1, u_2, v_1, v_2)$ holds if and only if $c(u_1, u_2) \leqslant c(v_1, v_2)$. If (V, c) and (V', c') are different, so are the associated relations.

(S2) The following relation is first-order definable in terms of R:

$$c(u_1, u_2) + 1 = c(v_1, v_2).$$

It is equivalent to the following formula: not $c(v_1, v_2) \leqslant c(u_1, u_2)$ and, for all x_1, x_2,

$$\text{if } (c(u_1, u_2) \leqslant c(x_1, x_2) \text{ and } c(x_1, x_2) \leqslant c(v_1, v_2)), \text{ then}$$
$$\text{either } c(x_1, x_2) \leqslant c(u_1, u_2) \text{ or } c(v_1, v_2) \leqslant c(x_1, x_2).$$

The following sentences are satisfied by the relation R and expressible in the language of first order.

(2.1) R is symmetric in the first and second as well as in the third and fourth argument. R may therefore be thought of as a binary relation $\leqslant^*$ on the set of unordered pairs of elements of V.
(2.2) $\leqslant^*$ is alternative and transitive, *i.e.*,

$$u \leqslant^* v \text{ or } v \leqslant^* u,$$
$$\text{if } u \leqslant^* v \text{ and } v \leqslant^* w \text{ then } u \leqslant^* w.$$

An alternative and transitive relation will be called a *pseudo-order*.
(2.3) For all x, y, the relation in u, v defined by $c(u, v) \leqslant c(x, y)$ is an equivalence relation.
(2.4) For all u_1, u_2, we have $u_1 = u_2$ if and only if $c(u_1, u_2) \leqslant c(v_1, v_2)$ for all v_1, v_2. (The pairs (u_1, u_1) are minimal elements in the pseudo-order $\leqslant^*$.)

(2.5) Assume $c(x_1, y_1) + 1 = c(x_2, y_2)$, and let eq_i $(i = 1, 2)$ be the equivalence relations corresponding to x_i, y_i. Then, for every s, there exists t such that the following holds: $\mathrm{eq}_2(s, t)$ and not $\mathrm{eq}_1(s, t)$ and, for all u, $\mathrm{eq}_2(s, u)$ if and only if either $\mathrm{eq}_1(s, u)$ or $\mathrm{eq}_1(t, u)$.

(S3) For each quaternary relation R on a set V satisfying conditions (2.1)–(2.5), there exists a number r and a map c from $V \times V$ onto $(0, \ldots, r)$ such that (V, r, c) is a cc-graph and $R(u, v, x, y)$ holds if and only if $c(u, v) \leqslant c(x, y)$.

To see this, note that the relation $R(u, v, x, y)$ defines a pseudo-order $\leqslant^*$ on $V \times V$ satisfying $(u, v) \leqslant^* (v, u)$. There exist, therefore, an integer r and a symmetric map c from $V \times V$ to $\{0, \ldots, r\}$ such that $R(U_1, u_2, v_1, v_2)$ holds if and only if $c(u_1, u_2) \leqslant c(v_1, v_2)$.

CC1, CC2 and CC3 are immediate consequences of (2.3), (2.4) and (2.5). □

4. Problems

(1) Is every ultimately periodic function from $\mathbb{N}$ to $\{0, \ldots, m-1\}$ the counting function mod m of a class of structures definable in $\mathbf{L}_1$ (the language of first-order logic with equality) based on a binary relation?

(2) Does there exist a class definable in $\mathbf{L}_1$ based on a finite number of relations such that no modular counting function is ultimately periodic?

Let $\mathbf{F}(k)$ be the set of counting functions mod 2 of classes definable in $\mathbf{L}_1$ based on a finite set of at most k-ary relations.

(3) Is $\mathbf{F}(k)$ a *proper* subset of $\mathbf{F}(k+1)$?

(4) Define other sets analogous to $\mathbf{F}(k)$ and state problems 5, 6, ... *ad libitum.*

Acknowledgement

I thank Walter Schnyder and the referees for carefully reading the manuscript and suggesting improvements.

References

[1] Blatter, C. and Specker, E. (1981) Le nombre de structures finies à charactère fini. *Sciences Mathématiques, Fonds National de la Recherche Scientifique, Bruxelles*, pp. 41–44.
[2] Blatter, C. and Specker, E. (1983) Modular periodicity of combinatorial sequences. *Abstract Amer. Math. Soc.* **4** 313.
[3] Blatter, C. and Specker, E. (1984) Recurrence relations for the number of labeled structures on a finite set. In *Logic and Machines*, Vol. 171 of *Lecture Notes in Computer Science*, Springer, pp. 43–61.
[4] Ebbinghaus, H. D. and Flum, J. (1995) *Finite Model Theory*, Springer.
[5] Ehrenfeucht, A. (1957) Application of games to some problems of mathematical logic. *Bull. Acad. Pol.* Cl. III, **5** 35–37.
[6] Fischer, E. (2003) The Blatter–Specker theorem does not hold for quaternary relations. *J. Combin. Theory Ser. A* **103** 121–136.
[7] Fischer, E. and Makowsky, J. (2003) The Specker–Blatter theorem revisited: Generating functions for definable classes of structures. In *Proc. 9th COCOON*, pp. 90–101.

[8] Fraïssé, R. (1954) Sur quelques classifications des systèmes de relations. *Publ. Sci. Univ. Alger. Sér. A* 15–182.
[9] Sengpiel, K. (1989) Modulares Zählen. Diplomarbeit im Fach Informatik Universität Erlangen–Nürnberg.
[10] Specker, E. (1988) Applications of logic and combinatorics to enumeration problems. In *Trends in Theoretical Computer Science* (E. Börger, ed.), Computer Science Press, pp. 141–169. Reprinted in E. Specker (1990) *Selecta*, Birkhäuser, pp. 324–350.