THE BULLETIN OF SYMBOLIC LOGIC
Volume 6, Number 1, March 2000

# COUNTEREXAMPLES OF THE 0-1 LAW FOR FRAGMENTS OF EXISTENTIAL SECOND-ORDER LOGIC: AN OVERVIEW

JEAN-MARIE LE BARS

**Abstract.** We propose an original use of techniques from random graph theory to find a Monadic $\Sigma_1^1$ (Minimal Scott without equality) sentence without an asymptotic probability. Our result implies that the 0-1 law fails for the logics $\Sigma_1^1(\mathrm{FO}^2)$ and $\Sigma_1^1$ (Minimal Gödel without equality). Therefore we complete the classification of first-order prefix classes with or without equality, according to the existence of the 0-1 law for the corresponding $\Sigma_1^1$ fragment. In addition, our counterexample can be viewed as a single explanation of the failure of the 0-1 law of all the fragments of existential second-order logic for which the failure is already known.

## §1. Introduction.

**1.1.** 0-1 **laws in logic.** We will concentrate on purely relational vocabularies. Let $\mathcal{R}$ be a vocabulary (i.e., a finite set of relation symbols) and $\mathcal{P}$ be a property on the collection of all finite structures over $\mathcal{R}$. For each natural number $n$, we will denote by $\mu_n(\mathcal{P})$ the fraction of finite models with domain $n$ (which is the set $\{0, \ldots, n-1\}$) for which $\mathcal{P}$ holds. The asymptotic probability of $\mathcal{P}$ denoted by $\mu(\mathcal{P})$ is the limit of $\mu_n(\mathcal{P})$ as $n$ goes to infinity provided this limit exists.

Defining $\mu_n$ in terms of fractions amounts to considering what is known as the uniform probability space where two structures of the same size have the same probability. The following experiment yields a random $n$-elements structure: for any integer $k$, any $S \in \mathcal{R}$ of arity $k$ and any tuple $\overline{\mathbf{a}_k}$ of $k$ elements of $n$, we choose at random (with probability $\frac{1}{2}$) whether the tuple $\overline{\mathbf{a_k}}$ is in the relation $\mathcal{S}$.

A property is called almost surely true (respectively false) when its asymptotic probability is equal to 1 (respectively 0). We say that the 0-1 law holds for a logic, which is a set of formulas, if the asymptotic probability of any property which is expressible in this logic is either 0 or 1. In 1969 Glebskii, Kogan, Liogonki and Talanov [13] and independently Fagin in 1976 [10] showed that the 0-1 law holds for first-order logic.

**1.2. Fragments of $\Sigma_1^1$.** An existential second-order sentence over a vocabulary $\mathcal{R}$ is an expression $\psi$ of the form $\exists \mathcal{S}\ \varphi(\mathcal{R} \cup \mathcal{S})$, where $\mathcal{S}$ is a set of

Received January 25, 1999; revised November 22, 1999.


1079-8986/00/0601-0003/$2.60

relation variables and $\varphi(\mathcal{R} \cup \mathcal{S})$ is a first-order sentence over $\mathcal{R} \cup \mathcal{S}$. Existential second-order logic, denoted by $\Sigma_1^1$, is the set of such expressions. The sentence $\psi$ is said to be *monadic* when $\mathcal{S}$ is a set of *unary* relation variables. Similarly, Monadic $\Sigma_1^1$, the monadic existential second-order logic, denotes the set of such expressions.

Let $\mathcal{L}$ be a set of first-order sentences, which will be called a first-order logic. We denote by $\Sigma_1^1(\mathcal{L})$ the set of existential second-order sentences whose first-order part belongs to $\mathcal{L}$. Monadic $\Sigma_1^1(\mathcal{L})$ is defined similarly.

The focus on $\Sigma_1^1$ dates back to Fagin's work [9] where it was shown that the sets (of mathematical structures) recognizable in NP coincide with those definable by formulas of the logic $\Sigma_1^1$. Since we can express PARITY ("there is an even number of elements"), which has clearly no asymptotic probability, by a $\Sigma_1^1$-sentence, the 0-1 law does not hold for $\Sigma_1^1$. However we may expect to get 0-1 laws by considering fragments of $\Sigma_1^1$.

**1.3. Correspondence between 0-1 law and decidability.** Recall that a sentence is a formula without free variables and that a first-order prefix class is a set of prenex first-order sentences whose quantifier prefix belongs to a regular language over the alphabet $\{\forall, \exists\}$. A logic is called "solvable" if its satisfiability problem is decidable. There are exactly three solvable maximal first-order prefix classes (see Dreben and Goldfarb [6]): *the Ackermann class* ($\exists^*\forall\exists^*$), *the Bernays-Schönfinkel class* ($\exists^*\forall^*$), *the Gödel class* without equality (i.e., $=$ does not occur in the formulas) ($\exists^*\forall\forall\exists^*$ without equality).

The study of 0-1 laws for fragments of second-order logic with respect to the uniform measure on the class of all finite structures over a given relational vocabulary started with a result by Kaufmann and Shelah in 1985 to the effect that the 0-1 law fails for monadic second-order logic.

After this, researchers carried out an in-depth investigation for fragments of existential second-order logic. In 1989, Kolaitis and Vardi began a classification of first-order prefix classes according to the existence of a 0-1 law for the corresponding $\Sigma_1^1$ fragments. They showed that a 0-1 law holds for $\Sigma_1^1$(Bernays-Schönfinfel) [17] and $\Sigma_1^1$(Ackermann) [18]. Since Ackermann and Bernays-Schönfinfel are the only solvable maximal first-order prefix classes with equality, they proposed the following conjecture:

> *A first-order prefix class with equality is solvable if and only if the 0-1 law holds for the corresponding $\Sigma_1^1$ fragment.*

In 1993, Pacholski and Szwast confirmed this correspondence by giving a counterexample to the 0-1 law for $\Sigma_1^1$(Minimal Gödel with equality) ($\Sigma_1^1(\forall\forall\exists$ with equality) [24].

A class of first-order sentences is said to be finitely controllable if every satisfiable sentence of $\mathcal{L}$ is finitely satisfiable. Since the set of first-order valid sentences is recursively enumerable, every finitely controllable class is clearly solvable.

Observing that the three classes mentioned above are also finitely controllable, Kolaitis and Vardi suggested that the real connection is between finite controllability of a first-order logic and the existence of a 0-1 law for the corresponding $\Sigma^1_1$ fragment [19].

However, they conjectured in [18] that the 0-1 law might not hold for the $\Sigma^1_1$ (Gödel class without equality) although this logic is finitely controllable. So, one could possibly not preserve this connection for prefix classes without equality.

Nevertheless, it seems possible to extend this correspondence to other first-order logics. The most natural candidate is $\mathrm{FO}^2$, the set of first-order sentences with at most two variables. It is well-known that $\mathrm{FO}^2$ is finitely controllable and therefore solvable. (See Mortimer's paper [22].) In [12] Flum asked the question whether a 0-1 law holds for $\Sigma^1_1(FO^2)$.

The following properties provide a counterexample of the 0-1 law for the $\Sigma^1_1$ fragments for which the failure is already known.

**§2. How to express PARITY.** It is evident that the property PARITY—there is an even number of elements—has no asymptotic probability. This property is useful for providing a counterexample of the 0-1 law for a logic.

For example, we may encode a unary function $f$ which is a permutation where every element is of order 2 by a binary relation; in other words $f$ satisfies:

(1) $\quad f \circ f(a) = a$ and $f(a) \neq a$, for any element $a$ of the domain.

It is easily seen that such a function is definable in a finite structure if and only if the domain has an even number of elements.

**2.1. $\Sigma^1_1$ ($\forall^3\exists$ with equality).** The $\Sigma^1_1(\forall^3\exists$ with equality)-sentence below expresses that there is a function $f$ which satisfies (1).

$$\exists R\, \forall x \forall y \forall z \exists t\, \Big(Rxt \wedge Rtx \wedge x \neq t \wedge \big((Rxy \wedge Rxz) \rightarrow y = z\big)\Big),$$

where $R$ is a binary relation variable.

**2.2. $\Sigma^1_1$ (Kahr-Moore-Wang with equality).** Recall that the Kahr-Moore-Wang class with equality is the set of sentences of the form

$$\forall x \exists y \forall z\, \varphi(x, y, z),$$

where $\varphi$ is quantifier-free formula which may contain the equality symbol.

$\Sigma^1_1$ (Kahr-Moore-Wang with equality)-sentence below expresses that there is a function $f$ which satisfies (1).

$$\exists R\, \forall x \exists y \forall z\, (Rxy \wedge (Rxz \rightarrow y = z) \wedge (Rxz \iff Rzx) \wedge \neg Rxx),$$

where $R$ is a binary relation variable.

**§3. How to express PARITY Almost Surely.**

**3.1. $\Sigma_1^1$ ($\forall^3\exists$ without equality).** Kolaitis and Vardi proved in [18] that the following $\Sigma_1^1(\forall^3\exists$ without equality)-sentence $\varphi$ over a vocabulary with a binary relation symbol $E$ expresses the property PARITY almost surely:

$$\exists R \exists S\, \forall x \forall y \forall z \exists w\, \Big( Rxw \wedge ((Rxy \wedge Rxz) \rightarrow Syz) \\ \wedge (Rxy \iff Ryx) \wedge \neg Rxx \wedge (Sxy \rightarrow (Exz \iff Eyz))\Big),$$

where $S$ and $R$ are binary relation variables. The proof is easy: assume that the structure satisfies the following axiom of extension:

$$\forall x \forall y (x \neq y \rightarrow \exists z (Exz \wedge \neg Eyz)). \tag{2}$$

Then the formula $\forall x \forall y \forall z (Sxy \rightarrow (Exz \iff Eyz))$ implies the formula

$$\forall x \forall y (Sxy \rightarrow x = y).$$

So one may interpret $S$ as the equality relation and $\varphi$ expresses that $R$ encodes a function $f$ which satisfies (1). We conclude by observing that (2) as any axiom of extension is almost surely true (see for example Fagin's paper [10]).

**3.2. $\Sigma_1^1$ (Kahr-Moore-Wang without equality).** Vedo in [27] used the almost surely true axiom (2) to prove that the $\Sigma_1^1$ (Kahr-Moore-Wang without equality) sentence $\Psi$ below expresses PARITY almost surely.

$$\exists U \exists S\, \forall x \exists y \forall z\, ([Exz \iff Syz] \wedge [Sxz \iff Eyz] \wedge [Ux \iff \neg Uy]),$$

where $U$ and $S$ are respectively unary and binary relation variables and $E$ is a binary relation symbol.

To see this we consider $\Psi'$ the Skolem form of $\Psi$:

$$\exists f \exists U \exists S\, \forall x \forall z\, ([Exz \iff Sf(x)z] \\ \wedge [Sxz \iff Ef(x)z] \wedge [Ux \iff \neg Uf(x)]),$$

It is easily seen that $\Psi$ and $\Psi'$ are logically equivalent. Let $\mathcal{M}$ be a structure over $E$ of domain $M$ which is a model of $\Psi$ and then a model of $\Psi'$. Let $f_M$, $U_M$ and $S_M$ be some interpretations of $f$, $U$ and $S$ for which $\Psi'$ holds in $\mathcal{M}$. Let $a$ and $b$ be any element of $M$. On the one hand, $a \in U_M$ if and only if $f_M(a) \notin U_M$, thus $f_M(a) \neq a$. On the other hand, by interpreting in $z$ by $b$ and $x$ by successively $a$ and $f_M(a)$, we have $(a, b) \in E$ if and only if $(f_M(a), b) \in S_M$ and $(f_M(a), b) \in S_M$ if and only if $(f_M \circ f_M(a), b) \in E$. This implies $(a, b) \in E$ if and only if $(f_M \circ f_M(a), b) \in E$. Clearly $f_M$ satisfies (1) and we conclude as we did in 3.1.

**3.3. The monadic existential second-order logic.** Kaufmann answered in 1987 a question of Kolaitis: the 0-1 law fails for the monadic existential second-order logic (see [15]).

For this he proved that PARITY is almost surely expressible by a sentence in this logic. The main idea consists in extending a linear order firstly defined in a small part of the structure over the full domain *via* monadic existential second-order sentences. So, we get a linear order over the whole structure and a successor function. Then it is very easy to define PARITY by adding just one unary relation variable to colour elements black and white: we choose the colour *black* for the first element, the colour *white* for the successor and so on. We have an even number of elements if and only if the last element is white.

**3.4. The monadic existential second-order logic on undirected graphs.** Observe that the vocabulary involved in Kaufmann's counterexample contains four binary relations; in [21] we established a similar result on undirected graphs. It requires a modification of Kaufmann's result. On an undirected graph, the set of edges cannot encode a linear order over a subset $U$ of the set of vertices; however we show that there are a first-order formula $\varphi(x, y)$ and a monadic existential second-order sentence $\psi$ which expresses that $\varphi(x, y)$ defines a linear order over $U$.

## §4. Another property over cardinality.

**4.1. $\Sigma^1_1$ (Minimal Gödel with equality).** Recall that the Gödel class (respectively Minimal Gödel class) is the set of sentences in prenex form of prefix $\exists^*\forall\forall\exists^*$ (respectively $\forall\forall\exists$).

Gödel proved in 1933 that the satisfiability problem for Gödel sentences without equality is decidable and conjectured that it still holds with equality. Precisely, he claimed that the Gödel class with equality can be shown to contain no infinity axiom and hence is decidable.

Nearly fifty years later—in 1984—Goldfarb showed that the Minimal Gödel with equality is undecidable [14]. In opposition to Gödel's claim, he gave an infinity axiom F (a satisfiable sentence which has no finite model) and by exploiting properties of F, encoded an undecidable problem into this class.

Pacholski and Szwast managed to prove, by modifying Goldfarb's proof, the failure of the 0-1 law for $\Sigma^1_1$(Minimal Gödel with equality).

They exhibited a sentence in this logic—which involved 43 clauses—which expresses that the cardinality $n$ of the domain is of the form $\frac{(m^2+3m+4)}{2}$, for some positive integer $m$.

Clearly such a sentence has no asymptotic probability. Further, Pacholski and Szwast proposed a modification of this sentence—which contains 163 clauses!—whose asymptotic probability exists and is different from 0 and 1.

## §5. Asymptotic probabilities on second-order logic.

**5.1. The monadic second-order logic.** The study of asymptotic probabilities for fragments of second-order logic with respect to uniform measure started with a result by Kaufmann and Shelah in 1985 to the effect that the 0-1 law fails for monadic second-order logic.

Their main result is the following lemma:

LEMMA ([16]). *Suppose that $f$ and $g$ are recursive functions such that $f(n) < g(n)$ for all $n$. Then there is a sentence $\varphi$ of monadic second-order logic and a finite-to-one function $h$ from $\mathbf{N}$ onto $\mathbf{N}$ such that*

$$\lim_{n\to+\infty}\left|\mu_n(\varphi) - \frac{f(h(n))}{g(h(n))}\right| = 0.$$

**5.2. $\mu(\varphi) = q$, for $q$ rational number.** The logics $\mathcal{L}$ below have the following property: for every rational number $q \in ]0, 1[$, there is a $\Sigma_1^1(\mathcal{L})$-sentence $\varphi$ such that $\mu(\varphi) = q$.

- The monadic existential second-order logic on binary structures [15] and even on undirected graphs [21].
- Kahr-Moore-Wang class with equality (see Tendera's article [26]).

**5.3. $\mu(\varphi) = r$, for $r$ recursive real number.** We call a real number $r$ *recursive* if there are two recursive functions $h(m)$ and $g(m)$ such that

$$\lim_{m\to\infty}\frac{h(m)}{g(m)} = r.$$

The logics $\mathcal{L}$ below have the following property: for every recursive real $r \in [0, 1]$, there exists a $\Sigma_1^1(\mathcal{L})$-sentence $\varphi$ such that $\mu(\varphi) = r$.

- Kahr-Moore-Wang class without equality [27].
- Gödel class with equality [23].

Observe that it is an optimal result: if $r$ is the asymptotic probability of a sentence then $r$ is recursive.

## §6. Our results: survey.

The aim of our work is to prove that the 0-1 law does not hold for $\Sigma_1^1(FO^2)$ and $\Sigma_1^1$ (Minimal Gödel without equality).

Our proofs rely on results about random graphs (i.e., undirected graphs) and digraphs (i.e., directed graphs) with respectively constant edge and constant arc probabilities; of particular interest in this paper is the value of *the clique number* in almost all graphs. A clique in a graph $G$ is a subset of vertices which are pairwise joined by an edge and the *clique number* of $G$ is the size of a largest clique. Matula showed that there are almost surely only two possible values for the clique number [25]. These values are approximated by a real function $\delta$ which depends only on the constant edge probability $p$ and the number $n$ of vertices of the graph.

Let $H$ be a digraph and let $U$ be a set of vertices of $H$. $U$ is said to be *stable* (or *independent*) if there is no arc between vertices of $U$. $U$ is said to be *dominating* (or *absorbing*) if from each vertex out of $U$ goes an arc to some vertex of $U$. If $U$ is both *stable* and *dominating*, we call it a kernel of $H$. We let KERNEL denote the set of digraphs having at least one kernel.

We show that we have a relationship between a kernel of a random digraph and a clique of a random graph, provided the probability spaces are well defined.

The property KERNEL is easily expressible by the following Monadic $\Sigma^1_1(FO^2)$ sentence

$$\exists U\ \Big((\forall x \forall y\ ((Ux \wedge Uy) \rightarrow \neg\ Axy)) \wedge\ (\forall x \exists y\ (\neg\ Ux \rightarrow (Uy \wedge Axy)))\Big).$$

This property is known to be NP-complete (see Chvatal [4, 5]).

Fernandez de la Vega proved that the property KERNEL is almost surely true [11]. To be more precise, he gave a sequence $m(n)$ such that there is almost surely a kernel of order $m(n)$ in a digraph with $n$ vertices. This result comes from the frail balance between the two parts of the property KERNEL, stability and dominance. This balance may be broken if the ratio between $|U|$ and the number of vertices not in $U$ is modified.

Taking advantage of this sensitive ratio, we define two digraph properties—$\mathrm{KERNEL}_1$ and $\mathrm{KERNEL}_2$—which are variants of KERNEL and which have no asymptotic probability. On the one hand $\mathrm{KERNEL}_1$ is definable by a Monadic $\Sigma^1_1(FO^2)$ sentence, therefore the 0-1 law does not hold for Monadic $\Sigma^1_1(FO^2)$. On the other hand $\mathrm{KERNEL}_2$ is expressible by a Monadic $\Sigma^1_1$ (Minimal Scott without equality) sentence, i.e., a Monadic $\Sigma^1_1$ sentence where the first-order part is of the form

$$(\forall x \forall y \varphi_1(x, y))\ \wedge\ (\forall x \exists y \varphi_2(x, y)),$$

where $\varphi_1$ and $\varphi_2$ are quantifier-free and equality-free formulas with variables $x$ and $y$. This second result implies that the 0-1 law does not hold for $\Sigma^1_1$ (Minimal Gödel without equality) either.

For both properties we use the same argument to prove that the asymptotic probability is not defined; we construct two infinite sets of natural numbers $A$ and $B$ such that the property is almost surely true (respectively false) if we restrict our study to structures of domain $n \in A$ (respectively $n \in B$).

**§7. Random graphs and clique number.** The study of random graphs began with the fundamental paper by Erdös and Rényi [7]. For more details, we refer the reader to classical textbooks [8, 1, 2].

Following standard usage, an undirected graph will be called simply a graph, a directed graph will be termed a digraph. We denote by $n$ the set $\{0, \dots, n-1\}$, for any positive integer $n$. Let $\mathcal{G}_n$ denote the set of graphs that have $\{0, \dots, n-1\}$ as their set of vertices. Let $p$ be a fixed real such that $0 < p < 1$.

We obtained a random graph $G_n \in \mathcal{G}_n$ by performing the following experiment: for each pair $\{a, b\}$ of distinct vertices of $G_n$, $\{a, b\}$ is an edge of $G_n$ with probability $p$. We will denote by $\mathcal{G}(n, p)$ the probability space obtained in this way.

Let $\mathcal{P}$ be a graph property. We denote by $\mu_n^p(\mathcal{P})$ the probability that a random graph $G_n$ from $\mathcal{G}(n, p)$ satisfies $\mathcal{P}$. The limit of $\mu_n^p(\mathcal{P})$, as $n$ goes to the infinity, is called the asymptotic probability of $\mathcal{P}$ on $\mathcal{G}(n, p)$ and is denoted $\mu^p(\mathcal{P})$, provided this limit exists. We will say that a graph property $\mathcal{P}$ is almost surely true when $\mu^p(\mathcal{P}) = 1$ and almost surely false when $\mu^p(\mathcal{P}) = 0$.

Let $\mathcal{H}_n$ denote the set of digraphs that have $\{0, \dots, n-1\}$ as their set of vertices. We will use similar definitions and notations for $\mathcal{H}(n, p)$, $\mu_n^p(\mathcal{P})$ and $\mu^p(\mathcal{P})$ in the case of digraphs.

Recall that a clique in a graph $G_n$ is a subset of vertices which are pairwise joined by an edge. The *clique number* of $G_n$, denoted by $\omega(G_n)$, is the size of a largest clique of $G_n$.

The two following theorems give nearly the same result in a different form.

THEOREM 7.1 (Matula 1972). *For fixed $p$ and fixed $\varepsilon > 0$, $G_n \in \mathcal{G}(n, p)$ has almost surely its clique number equal to $\lfloor \delta - \varepsilon \rfloor$ or $\lfloor \delta + \varepsilon \rfloor$, where*

$$\delta = 2 \log_{\frac{1}{p}} n - 2 \log_{\frac{1}{p}} \log_{\frac{1}{p}} n + 1 + 2 \log_{\frac{1}{p}} \left( \frac{e}{2} \right). \tag{3}$$

PROOF. See Palmer's book [25] pages 75-80. ⊣

THEOREM 7.2 (Erdös and Bollobás 1974). *Let $p$ be a fixed real such that $0 < p < 1$ and $n$ a positive integer. Let $d = d(n, p)$ denote the greatest integer $r$ such that the expectation of the number of cliques of order $r$ in $G_n \in \mathcal{G}(n, p)$ is greater than or equal to* 1.

*$G_n \in \mathcal{G}(n, p)$ has almost surely its clique number in the set $\{d-1, d, d+1\}$,*

$$\text{i.e.,} \quad \lim_{n \to +\infty} \Pr(\omega(G_n) \in \{d-1, d, d+1\}) = 1.$$

PROOF. See [3] or [1] pages 137-139. ⊣

**7.1. First and second moment methods.** Let $r = r(n)$ be a sequence of positive integers. We define (elementary) random variables $X_{r,U}^{\text{clique}}$, for any subset $U$ of $n$ of cardinality $r$ as follows:

$$X_{r,U}^{\text{clique}} = 1 \text{ if } U \text{ is a clique,} \\ = 0 \text{ otherwise.}$$

We denote by $X_r^{\text{clique}}$ the random variable which equals the number of cliques of order $r$, so we have $X_r^{\text{clique}} = \sum_{U \subset n, |U| = r} X_{r,U}^{\text{clique}}$. This implies

$$E\,[X_r^{\text{clique}}] = \sum_{U \subset n, |U| = r} E\,[X_{r,U}^{\text{clique}}] = \binom{n}{r} \Pr(U_r \text{ is a clique}) = \binom{n}{r}\, p^{\frac{r(r-1)}{2}},$$

where $U_r$ denotes the set $\{0, \dots, r-1\}$.

Thus $d = d(n, p)$ is the greatest integer $r$ such that $\binom{n}{r}\, p^{\frac{r(r-1)}{2}} \geq 1$. If the sequence $r(n)$ satisfies

$$\lim_{n \to +\infty} E[X_r^{\text{clique}}] = 0,$$

by using the first moment method

$$\text{(4)} \qquad \Pr\,(X_r^{\text{clique}} > 0) \leq E\,[X_r^{\text{clique}}]$$

we conclude that we have $\lim_{n \to +\infty} \Pr\,(X_r^{\text{clique}} > 0) = 0$.

If the sequence $r(n)$ satisfies

$$\lim_{n \to +\infty} \frac{E\,[(X_r^{\text{clique}})^2] - E\,[X_r^{\text{clique}}]^2}{E\,[X_r^{\text{clique}}]^2} = 0,$$

by using the second moment method (Chebychev's inequality)

$$\text{(5)} \qquad \Pr\,(X_r^{\text{clique}} = 0) \leq \frac{E\,[(X_r^{\text{clique}})^2] - E\,[X_r^{\text{clique}}]^2}{E\,[X_r^{\text{clique}}]^2},$$

we conclude that we have $\lim_{n \to +\infty} \Pr\,(X_r^{\text{clique}} > 0) = 1$.

Of course, these methods are useful for other properties. In particular, one may use them for the digraph property KERNEL.

Both previous theorems use the first and second moment methods.

## §8. The digraph property KERNEL.

**8.1. Relationship between cliques and stables.** There is an obvious relationship between cliques and stables. To each digraph $H_n = \langle n, A \rangle$ from $\mathcal{H}(n)$ we associate the unique graph from $\mathcal{G}(n)$, denoted by $\overline{H_n}$, such that, for any unordered pair $\{a, b\}$ of distinct vertices, $\{a, b\}$ is an edge of $\overline{H_n}$ if and only if neither $(a, b)$ nor $(b, a)$ is an arc of $H_n$. It is clear that $U$ is a stable of $H_n$ if and only if $U$ is a clique of $\overline{H_n}$. Moreover, if we assume that $p_1$ and $p_2$ are two fixed reals such that

$$0 < p_1, p_2 < 1 \ \text{ and } \ p_1 = (1 - p_2)^2.$$

the probability of $H_n$ in $\mathcal{H}(n, p_2)$ coincides clearly with the probability of $\overline{H_n}$ in $\mathcal{G}(n, p_1)$.

From now on, we denote by $p_1$ and $p_2$ two fixed reals such that $0 < p_1, p_2 < 1$ and $p_1 = (1 - p_2)^2$. We will write $d(n)$ instead of $d(n, p_1)$.

Let $r$ be an integer such that $r \leq n$. As we did for the clique property in the previous section, we define the 0-1 random variables on the subsets $U$ of $n$ of cardinality $r$ for the properties stable, dominating (dom) and kernel ($\mathcal{K}$): $X_{r,U}^{\text{stable}}$, $X_{r,U}^{\text{dom}}$, $X_{r,U}^{\mathcal{K}}$ and the integer random variables $X_r^{\text{stable}}$, $X_r^{\text{dom}}$, $X_r^{\mathcal{K}}$.

It is obvious that $X_{r,U}^{\text{stable}}$ and $X_{r,U}^{\text{dom}}$ are independent random variables, since they involve two disjoint sets of arcs. Furthermore, the properties in concern are monotonic:

Each subset of a stable is also a stable. This implies

$$\Pr\left(\bigcup_{r'\geq r}[X_{r'}^{\text{stable}}>0]\right)=\Pr\left(X_r^{\text{stable}}>0\right). \tag{6}$$

Each superset of a dominating set is also a dominating set. This entails

$$\Pr\left(\bigcup_{r'\leq r}[X_{r'}^{\text{dom}}>0]\right)=\Pr\left(X_r^{\text{dom}}>0\right). \tag{7}$$

THEOREM 8.1 (Fernandez de la Vega [11]). *For any fixed $p$, $H_n \in \mathcal{H}(n,p)$ has almost surely a kernel of order $m(n) = \lceil \beta(n) \rceil$ where $\beta(n)$ is the real defined by*

$$\beta(n)=\log_{\frac{1}{1-p}} n-\log_{\frac{1}{1-p}}\log_{\frac{1}{1-p}} n. \tag{8}$$

As one did for previous theorems, we use first and second moment methods.

It is easily seen that the larger $r$, the smaller the probability that $H_n$ has a stable of order $r$. In the opposite, the larger $r$, the larger the probability that $H_n$ has a dominating set of order $r$.

A careful study brings to the fore a balance between *stability* and *dominance* which implies that there is a very narrow range of possible values for the sequence $m(n)$. This crucial observation is formalized in the following technical proposition:

PROPOSITION 8.1. *Let $m(n)$ the sequence defined as in Theorem* 8.1. *For any fixed $p$, let $H_n \in \mathcal{H}(n,p)$. There exist two positive integers $k_1$ and $k_2$ which depend only on $p$ such that $H_n$ has almost surely no kernel of order $r$, where $m(n)-k_1 < r < m(n)+k_2$.*

Our goal is to define a variant $\mathcal{P}$ of the property KERNEL which has a different ratio between *stability* and *dominance*. The trick consists in considering several binary relation instead of only one.

First, we want that there does not exist any sequence $r(n)$ which satisfies

$$\lim_{n\to+\infty}\Pr\left(X_r^{\mathcal{P}}>0\right)>0. \tag{9}$$

Moreover, we want that Proposition 8.1 still holds for $\mathcal{P}$. Equivalently, there are a sequence $m(n)$ and two positive integers $k_1$ and $k_2$ such that the property $\mathcal{P}$ that the graph has a kernel is equivalent almost surely to the fact that the graph as a "kernel" of order between $m(n)-k_1$ and $m(n)+k_2$. (8.1) makes it obvious that $\mathcal{P}$ will not be almost surely true.

In the section below, we show how to define such a property.

**§9. The variant KERNEL$_1$.** We prove that the property KERNEL has a variant which has no asymptotic probability.

Let $\mathcal{R}$ denote the following vocabulary consisting of binary relation symbols

$$\mathcal{R} = \{R_1, \ldots, R_{16}, S_1^1, \ldots, S_{16}^1, \ldots, S_1^{2^{15}}, \ldots, S_{16}^{2^{15}}\}.$$

We define KERNEL$_1$ on finite structures over the vocabulary $\mathcal{R}$ by modifying the properties *stable* and *dominating*.

**9.1. Definition of KERNEL$_1$.** Let $\mathcal{M}_n$ be an $\mathcal{R}$-structure with domain $n$ and $U$ be a subset of $n$.

$U$ is a *stable* set of $\mathcal{M}_n$ if there is no ordered pair of distinct elements $(a, b)$ of $U \times U$ which belongs to $\bigcup_{i\in\{1,\ldots,16\}} R_i$.

$U$ is a *dominating* set of $\mathcal{M}_n$ if, for any $j \in \{1, \ldots, 2^{15}\}$ and any $c$ of $n \setminus U$, there exists $d_j \in U$ such that $(c, d_j)$ belongs to $\bigcup_{i\in\{1,\ldots,16\}} S_i^j$.

$U$ is a kernel of $\mathcal{M}_n$ if it is both *stable* and *dominating*.

$\mathcal{M}_n$ has the property KERNEL$_1$ if it has at least one kernel.

KERNEL$_1$ is expressible by the Monadic $\Sigma_1^1(FO^2)$ $\mathcal{R}$-sentence below

$$\exists U\Bigg(\bigg(\forall x\forall y\Big(Ux \wedge\ Uy \wedge x \neq y\Big) \to \neg\bigg(\bigvee_{i\in\{1,\ldots,16\}} R_i xy\bigg)\bigg)$$
$$\wedge\bigg(\bigwedge_{j\in\{1,\ldots,2^{15}\}} \forall x\exists y\bigg(\neg\, Ux \to \bigg(Uy \wedge \bigvee_{i\in\{1,\ldots,16\}} S_i^j xy\bigg)\bigg)\bigg)\Bigg).$$

To keep the relationship with the clique number, we put $p_2 = 1 - \left(\frac{1}{2}\right)^{16}$ (because of our new definition of a stable set) and $p_1 = (1 - p_2)^2 = \left(\frac{1}{2}\right)^{32}$.

Then, we study the clique number on the probability space $\mathcal{G}(n, p_1)$.

PROPOSITION 9.1. KERNEL$_1$ *has no asymptotic probability.*

The proof consists in establishing the following lemmas.

LEMMA 9.1. *We will say that an $\mathcal{R}$-structure has the property*

$$\text{KERNEL}_1(\neq d(n))$$

*if it has a kernel of order different from $d(n)$. This property is almost surely false.*

LEMMA 9.2. *We will say that an $\mathcal{R}$-structure has the property*

$$\text{KERNEL}_1(d(n))$$

*if it has a kernel of order $d(n)$.*

*There are two infinite sets of positive integers $\mathcal{A}$ and $\mathcal{B}$ which satisfy the following conditions*:

(i) $\lim\limits_{\substack{n\to+\infty\\ n\in\mathcal{B}}} \mu_n(\text{KERNEL}_1\ (d(n))) = 0.$

(ii) $\lim_{\substack{n\to+\infty \\ n\in\mathcal{A}}} \mu_n(\text{KERNEL}_1\ (d(n))) = 1.$

**9.2. Sketch of proof of Lemma 9.1.** Clearly, Steps 1–4 below imply Lemma 9.1.

Let $d' = d'(n)$ denote the integer $d'(n) = \lfloor \frac{3}{4}\, d(n) \rfloor$, for any positive integer $n$.

*Step* 1. $\lim_{n\to+\infty} \Pr\left(\bigcup_{r\geq d+2} (X_r^{\mathcal{K}_1} > 0)\right) = 0.$

Proof. It is a direct application of Theorem 7.2. ⊣

It means that there is almost surely no stable of $\mathcal{M}_n$ of order $d+2$ (see the relationship between cliques and stables) and so, no such set of order $r \geq d+2$.

*Step* 2. $\lim_{n\to+\infty} \Pr\left(\bigcup_{r\leq d'} (X_r^{\mathcal{K}_1} > 0)\right) = 0.$

*Idea.* We prove that there is almost surely no dominating set of $\mathcal{M}_n$ of order $d'$ and so, no such set of order $r \leq d'$.

*Step* 3. $\lim_{n\to+\infty} \Pr\ (X_{d+1}^{\mathcal{K}_1} > 0)) = 0.$

*Idea.* We prove that $\lim_{n\to+\infty} E\ [X_{d+1}^{\mathcal{K}_1}] = 0$ and we conclude by using the first moment method (4).

*Step* 4. $\lim_{n\to+\infty} \Pr\left(\bigcup_{d'<r\leq d-1} (X_r^{\mathcal{K}_1} > 0)\right) = 0.$

*Idea.* Let $r(n)$ be a sequence such that $d'(n) < r(n) \leq d(n) - 1$.
We show that there exists a constant $K < 0$ such that $E[X_r^{\mathcal{K}_1}] \leq \exp(d'K)$.
It follows $\Pr\ (\bigcup_{d'<r\leq d-1}(X_r^{\mathcal{K}_1} > 0)) < d\ \exp(d'\,K)$.
So, we have $\lim_{n\to+\infty} \Pr\ (\bigcup_{d'<r\leq d-1}(X_r^{\mathcal{K}_1} > 0)) = 0$.

**9.3. Proof of Lemma 9.2.** The following steps establish respectively conditions (i) and (ii) of Lemma 9.2. First we prove that, for any real $\alpha \in [0, 1]$, there is an infinite set of natural numbers $\mathcal{S}^\alpha$ such that

$$\lim_{\substack{n\to+\infty \\ n\in\mathcal{S}^\alpha}} \delta - d = \alpha. \tag{10}$$

*Step* 5. There exists an infinite set of natural numbers $B$ which satisfies

$$\lim_{\substack{n\to+\infty \\ n\in B}} \delta(n) - d(n) = \frac{1 + 6\ln 2}{16\ln 2} \text{ and } \lim_{\substack{n\to+\infty \\ n\in B}} \Pr(X_d^{\mathcal{K}_1} > 0) = 0.$$

PROOF. We restrict our study, in this step, to integers $n$ which belong to $B$. We show that $\lim_{\substack{n\to+\infty \\ n\in B}} E\,[X_d^{\mathcal{K}_1}] = 0$ and we conclude by using the first moment method.

*Step* 6. There exists an infinite set of natural numbers $A$ which satisfies

$$\lim_{\substack{n\to+\infty \\ n\in A}} \delta(n) - d(n) = \frac{1+\ln 2}{16\ln 2} \text{ and } \lim_{\substack{n\to+\infty \\ n\in A}} \Pr(X_d^{\mathcal{K}_1} > 0) = 1.$$

PROOF. We restrict our study, in this step, to integers $n$ which belong to $A$. First we show that $\lim_{\substack{n\to+\infty \\ n\in A}} E\,[X_d^{\mathcal{K}_1}] = +\infty$.

Let us denote by $(S(n))$ the sequence below

$$S(n) = \frac{E[(X_d^{\mathcal{K}_1})^2] - E[X_d^{\mathcal{K}_1}]^2}{E[X_d^{\mathcal{K}_1}]^2}.$$

We choose, for any integer $l \leq d$, two subsets $U_1^l$ and $U_2^l$ of $n$ of cardinality $d$ with exactly $l$ common elements.

Let $\mathcal{P}^{\mathrm{dom}}(d)$ denotes the probability that $U_1^l$ will be a dominating set of the random structure $\mathcal{M}_n$. Of course, it is also the probability that $U_2^l$ will be a dominating set.

Let $\mathcal{P}^{\mathrm{dom}\,2}(d,l)$ denote the probability that $U_1^l$ and $U_2^l$ will be both dominating sets of the random structure $\mathcal{M}_n$.

By using the independence of the random variables $X_{r,U}^{\mathrm{stable}}$ and $X_{r,U}^{\mathrm{dom}}$, we easily obtain the equality

$$S(n) = \sum_{l=0}^{d} a_l - 1,$$

where, for $l = 0 \ldots d$, $a_l$ denotes the term

$$\frac{\binom{n}{d}\binom{d}{l}\binom{n-d}{d-l}\, p_1^{d(d-1)-\frac{l(l-1)}{2}}\, \mathcal{P}^{\mathrm{dom}\,2}(d,l)}{\binom{n}{d}^2 \left(p_1^{\frac{d(d-1)}{2}}\right)^2 \left(\mathcal{P}^{\mathrm{dom}}(d)\right)^2}.$$

First we show that $a_0 = 1+o(1)$ and $a_1 = o(1)$. Then, for any $l \in \{2,\ldots,d\}$, we establish that

$$a_l \leq \exp\left(-\frac{1}{2}d\right),$$

which obviously implies $\lim_{n\to+\infty, n\in A} S(n) = 0$. Finally, we conclude by the second moment method. ⊣

**§10. The variant KERNEL$_2$.** Now, we define KERNEL$_2$, another variant of KERNEL, which has also no asymptotic probability. We get two improvements. Indeed this property doesn't require the equality symbol and involves just one type of arc in the definition of a dominating set. Hence, KERNEL$_2$ will be expressible by a Monadic $\Sigma_1^1$(Minimal Scott without equality) sentence.

Let $\mathcal{R}$ be the set $\{R_1, \ldots, R_{16}\}$ consisting of binary relation symbols and $\mathcal{M}_n$ be a structure with domain a positive integer $n$ over the vocabulary $\mathcal{R}$. We denote by $W(\mathcal{M}_n)$ the set $\{a \in n \setminus (a, a) \notin R_1\}$ and by $V(\mathcal{M}_n)$ the set $\{a \in n \setminus (a, a) \notin \bigcup_{i=1\ldots16} R_i\}$

**10.1. Definition of KERNEL$_2$.** Let $\mathcal{M}_n$ be an $\mathcal{R}$-structure with domain $n$ and $U$ be a subset of $n$.

• $U$ is a *stable* set of $\mathcal{M}_n$ if it is a subset of $V(\mathcal{M}_n)$ and there is no ordered pair of distinct elements $(a, b)$ of $U \times U$ which belongs to $\bigcup_{i\in\{1,\ldots,16\}} R_i$.

• $U$ is a *dominating* set of $\mathcal{M}_n$ if it is a subset of $V(\mathcal{M}_n)$ and, for each $c \in W(\mathcal{M}_n) \setminus U$, there exists $d \in U$ such that $(c, d)$ belongs to $\bigcup_{i=1\ldots16} R_i$.

• $U$ is a kernel of $\mathcal{M}_n$ if it is both *stable* and *dominating*.

$\mathcal{M}_n$ has the property KERNEL$_2$ if it has at least one kernel.

It is easily seen that KERNEL$_2$ is expressible by a $\Sigma_1^1$(Minimal Scott without equality) sentence.

PROPOSITION 10.1. *KERNEL$_2$ has no asymptotic probability.*

The proof requires new technical tools, indeed it is not evident that it is possible to keep for KERNEL$_2$ all the previous results for KERNEL$_1$. One may say that it is necessary to know $w$ and $v$, the respective cardinalities of $W(\mathcal{M}_n)$ and $V(\mathcal{M}_n)$, for any positive integer $n$, otherwise we cannot define properly the random variables. Therefore, we introduce conditional probabilities (see [20] or [21]).

**§11. Conclusion.** Proposition 10.1 implies that the 0-1 law fails for Monadic $\Sigma_1^1$ (Minimal Scott without equality), a very weak fragment of monadic existential second-order logic. Notice that KERNEL$_2$ is a unique counterexample for the failure results of all the logics above. Recall that KERNEL$_2$ is over a vocabulary with sixteen binary relation symbols. It leaves open the question whether the 0-1 law holds for $\Sigma_1^1(FO^2)$ (respectively $\Sigma_1^1$(Minimal Gödel without equality)) over the vocabulary consisting of a single binary relation; we conjecture that a 0-1 law holds for $\Sigma_1^1(FO^2)$ on graphs and digraphs. It is natural to ask whether there is a $\Sigma_1^1(FO^2)$-sentence with an asymptotic probability different from 0 and 1. Contrary to the other counterexamples, KERNEL$_1$ and KERNEL$_2$ give no indication and method to answer this question.

**Acknowledgments.** I would like to thank Etienne Grandjean for his constant help and support. I am also grateful to Nadia Creignou and Philippe Toffin for useful discussions and Thierry Lacoste for his drafting help.

REFERENCES

[1] B. BOLLOBÁS, ***Graph theory, an introduction course***, Springer-Verlag, 1979.

[2] ———, ***Random graphs***, Academic Press, 1985.

[3] B. BOLLOBÁS and P. ERDÖS, *Cliques in random graphs*, ***Mathematical Proceedings of the Cambridge Philosophical Society***, vol. 80 (1976), pp. 419–427.

[4] V. CHVATAL, *On the computational complexity of finding a kernel*, Technical report, Report NO CRM-300, 1973, Universite de Montréal, Centre de Recherches Mathématiques.

[5] N. CREIGNOU, *The class of problems that are linearly equivalent to satisfiability or a uniform method for proving NP-completeness*, ***Theoretical Computer Science***, vol. 145 (1995), pp. 111–145.

[6] D. DREBEN and W. D. GOLDFARB, ***The decision problem: Solvable classes of quantificational formulas***, Addison-Wesley, 1979.

[7] P. ERDÖS and A. RÉNYI, *On the evolution of random graphs*, ***Publ. Math. Inst. Hungar. Acad. Sci.***, vol. 7 (1960), pp. 17–61.

[8] P. ERDÖS and J. SPENCER, ***Probabilistic method in combinatorics***, A Series of Monographs and Textbooks, Academic Press, 1974.

[9] R. FAGIN, *Generalized first-order spectra and polynomial time recognizable sets*, ***Complexity of computations*** (R. Karp, editor), SIAM-AMS Proceedings, vol. 7, American Mathematical Society, Providence, RI, 1974, pp. 43–73.

[10] ———, *Probabilities on finite models*, ***The Journal of Symbolic Logic***, vol. 41 (1976), pp. 50–58.

[11] W. FERNANDEZ DE LA VEGA, *Kernel on random graphs*, ***Discrete Mathematics***, vol. 82 (1990), pp. 213–217.

[12] J. FLUM, *Problems in finite model theory collected in Oberwolfach*, 1994.

[13] Y.V. GLEBSKII, D.I. KOGAN, M. I. LIOGONKI, and V. A. TALANOV, *Range and degree of realizability of formulas in the restricted predicate calculus*, ***Cybernetics***, vol. 5 (1969), pp. 142–154.

[14] W. D. GOLDFARB, *The Gödel class with identity is unsolvable*, ***Bulletin of the American Mathematical Society***, vol. 10(1) (January 1984), pp. 113–115.

[15] M. KAUFMANN, *Counterexample to the* 0-1 *law for existential monadic second-order logic*, Technical report, CLI Internal Note 32, Computational Logic Inc., December 1987, paper available at ftp://ftp.informatik.rwth-aachen.de/pub/FMT/jurek/kaufmann.ps.

[16] M. KAUFMANN and S. SHELAH, *On random models of finite power and monadic logic*, ***Discrete mathematics***, vol. 54 (1985), pp. 285–293.

[17] PH. G. KOLAITIS and M.Y. VARDI, *The decision problem for the probabilities of higher-order properties*, ***Proceedings of the 19th ACM Symposium on Theory of Computing, STOC'87***, 1987, pp. 425–435.

[18] ———, 0-1 *laws and decisions problems for fragments of second-order logic*, ***Information and Computation***, vol. 87 (1990), pp. 302–338.

[19] ———, 0-1 *laws for fragments of second-order logic: an overview*, ***Logic from computer science*** (***Proceedings of Workshop, 1989***) (Y.N. Moschovakis, editor), 1992, pp. 265–286.

[20] J-M. LE BARS, *Fragments of existential second-order logic without* 0-1 *laws*, ***Proceedings of the 13th IEEE Symposium on Logic in Computer Science***, 1998.

[21] ———, *Probabilités asymptotiques et pouvoir d'expression des fragments de la logique du second ordre*, ***Ph.D. thesis***, University of Caen, 1998.

[22] M. Mortimer, *On languages with two variables*, ***Zeischrift für Mathematische Logik und Grundlagen der Mathematik***, vol. 21 (1975), pp. 135–140.

[23] L. Pacholski and W. Szwast, *Asymptotic probabilities of existential second-order Gödel sentences*, ***The Journal of symbolic logic***, vol. 56 (1991), pp. 427–438.

[24] ———, *A counterexample to the* 0-1 *law for the class of existential second-order minimal Gödel sentences with equality*, ***Information and Computation***, vol. 107 (1993), pp. 91–103.

[25] E. M. Palmer, ***Graphical evolution: An introduction to the theory of random graphs***, Wiley, 1985.

[26] L. Tendera, *A note on asymptotic probabilities of existential second-order minimal classes: the last step*, ***Fundamenta Informaticae***, vol. 20 (1994), pp. 277–285.

[27] A. Vedø, *Asymptotic probabilities for second-order existential Kahr-Moore-Wang sentences*, ***The Journal of Symbolic Logic***, vol. 62 (March 1997), pp. 304–319.

INFORMATIQUE, GREYC
UNIVERSITÉ DE CAEN
CAEN, FRANCE
*E-mail*: lebars@info.unicaen.fr