The 0-1 law fails for frame satisfiability of propositional modal logic

Jean-Marie Le Bars
GREYC, University of Caen, France
lebars@info.unicaen.fr

Abstract

The digraph property KERNEL is a very simple and well-known property studied in various areas. We previously defined a variant of this property as a counterexample of 0-1 law for the monadic existential second order logic with at most two first-order variables, over structures with 16 binary relations. Goranko and Kapron have defined two variants in frames which expresses frame satisfiability of propositional modal logic, also expressible in a small fragment of the logic above over structures with only one relation. We propose another variant of KERNEL which provides a counterexample of the 0-1 law for frame satisfiability of propositional modal logic. This refutes a result by Halpern and Kapron which establishes that the 0-1 law holds for this logic. It also strongly refines our previous counterexample.

Keywords: Modal and Temporal Logics, Finite Model Theory, Computational Complexity

1. Introduction

The study of random digraphs began with the fundamental paper by Erdös and Rényi [3] where they studied the asymptotic probability of graph properties in random graphs with constant edge probability and gave applications of probabilistic method in combinatorics. Studies may be conducted for digraphs, we obtain a random digraph $H_n =< V_n, A >$ by performing the following experiment: let $0 < p < 1$ be a fixed real and $V_n = \{0, \dots, n-1\}$ a set of n vertices. For each (ordered) pair (a, b) of distinct vertices of V_n, (a, b) is an arc of H_n (i.e. $(a, b) \in A$) with probability p. We will denote by $\mathcal{H}(n, p)$ the probability space so obtained. It is well known that case $p = \frac{1}{2}$ corresponds to the uniform distribution where two digraphs of $\mathcal{H}(n, p)$ have the same probability. Let $\mathcal{P}$ be a digraph property. We denote by $\mu_n^p(\mathcal{P})$ the probability that a random digraph H_n from $\mathcal{H}(n, p)$ satisfies $\mathcal{P}$. The limit of $\mu_n^p(\mathcal{P})$ as n goes to the infinity, denoted $\mu^p(\mathcal{P})$, is called the asymptotic probability of $\mathcal{P}$ on $\mathcal{H}(n, p)$, provided this limit exists. We will use the notations $\mu_n(\mathcal{P})$ and $\mu(\mathcal{P})$ for the uniform distribution case. We will say that a digraph property $\mathcal{P}$ is *almost surely true* when $\mu^p(\mathcal{P}) = 1$ and *almost surely false* when $\mu^p(\mathcal{P}) = 0$. According to the probability space given by p, we say that a 0-1 law holds in a class of properties $\mathcal{C}$ when each property in $\mathcal{C}$ is either almost surely true or almost surely false. In the whole paper when the probability space is not mentioned it will mean that the uniform distribution is assumed. It is easy to extend these definitions for finite relational structures. Glebskii et al. [7] and independently Fagin [5] first established a fascinating connection between logical definability and asymptotic probabilities for the uniform distribution case: every property expressible in first-order logic is either almost surely true or almost surely false. Besides, Fagin [5] proved the following result called *transfer theorem*: for a fixed relational vocabulary (a set of relational symbols) σ, there is a unique (up to isomorphism) countable structure $\mathcal{A}$ such that for any first-order σ-sentence φ,

$$\mathcal{A} \models \varphi \iff \mu(\varphi) = 1.$$

The research of 0-1 laws for fragments of second-order logic with respect to the uniform distribution on the class of all finite structures over a given relational vocabulary started with a result by Kaufmann and Shelah in 1985 stating that the 0-1 law fails for monadic second-order logic. Subsequently, researchers carried out an in-depth investigation for fragments of existential second-order logic. The focus was on Fagin's Theorem [4] that NP properties are exactly the properties definable in Σ_1^1. In 1989, Kolaitis and Vardi began a classification [10, 11] completed in 1993 by Pacholski and Szwast [15] of the first-order prefix classes with equality according to the existence of a 0-1 law for the corresponding Σ_1^1 fragments (see [12] for a recent survey): *a first-order prefix class with equality is solvable if and only if the 0-1 law holds for the corresponding Σ_1^1 fragment.* In addition, the transfer theorem stated above holds.

Given a directed graph $H = (V, A)$, a kernel of H is a nonempty subset U of V, such that for any a, b in U, (a, b) does not belong to A, *i.e.* U is a stable set, and for any a not in U, there is b in U, such that (a, b) belongs to A, *i.e.* U is a dominating set of vertices in G. H has the property

KERNEL if it has at least one kernel. The property KERNEL has been shown NP-complete by V. Chvàtal [1, 2]. Fernandez de la Vega [6] and Tomescu [16] obtained independently the result that the property KERNEL is almost surely true over random graphs. Our goal is to show that variants of the property KERNEL are of the utmost interest from the point of view of asymptotic probabilities. Before their result, there was no insight that the property was almost surely true. This result comes from a frail balance between *stability* and *dominance*, the two parts of the property KERNEL. Indeed the truth could have been different if the ratio of this two parts have been slightly different. Our idea is to change this ratio in order to break this balance. Kernel properties provide the best counterexamples of 0-1 laws in fragments of Σ_1^1. In [13, 14] we define such a variant –namely KERNEL$_2$– which has no asymptotic probability. We changed the ratio by using several types of arcs. For this, we use a relational vocabulary of 16 binary relations.

So that the 0-1 law fails for two small fragments of Σ_1^1, Mon $\Sigma_1^1(FO^2)$ and Mon Σ_1^1 (Minimal Gödel class without equality). Since FO^2 and Minimal Gödel class without equality are two solvable fragments of first-order logic, one cannot extend to those logics the above correspondence between solvability and 0-1 laws. Besides, observe that KERNEL$_2$ is expressible over structures with 16 binary relations, so we may hope to improve this result.

Modal logic is a natural extension of propositional logic. The standard semantics of modal logic is possible-worlds semantics. A frame $\mathcal{F}$ is an ordered pair (S, R) where S is a set of worlds (or states) and R is a binary relation (called the accessibility relation) on S. A (Kripke) structure $\mathcal{M} = (S, R, \pi)$ based on the frame $\mathcal{F}$ uses a mapping $\pi : S \times \{p_1, p_2 \ldots\} \to \{true, false\}$ which gives the truth value of all the primitive propositions $p_1, p_2 \ldots$. The set of modal formulae is inductively defined (see Section 2.1). Let φ be a modal formula and $\mathcal{M}$ a structure. We define the *structure satisfiability* as follows: φ is satisfiable in $\mathcal{M}$ if there is a state $s \in S$ such that $(\mathcal{M}, s) \models \varphi$.

Let φ be a modal formula and $\mathcal{F} = (S, R)$ be a frame. We define the *frame satisfiability* as follows: φ is satisfiable in $\mathcal{F}$ if there is a structure $\mathcal{M}$ based on $\mathcal{F}$ and a state $s \in S$ such that $(\mathcal{M}, s) \models \varphi$.

It is well known that frame satisfiability of propositional modal logic is expressible in $\Sigma_1^1(\exists x MDL)$, a fragment of Mon$\Sigma_1^1(FO^2)$ over structures with one binary relation.

Halpern and Kapron in [9] stated that the 0-1 law holds for propositional modal logic, both for structure and frame validity (or equivalently for structure and frame satisfiability)[1]. On the one hand, the first result easily follows from the 0-1 law for first-order logic, on the other hand, the proof of the second result in [9] requires a rather complicated combinatorial estimation of probabilities, which unfortunately offers little logical insight as noted in [9].

STRONG KERNEL is the most natural variant of KERNEL over frames. Let $\mathcal{F} =< S, R >$ be a frame, a subset U of the states of S is a *strong kernel* if U is a kernel and U is a set of non-reflexive states, *i.e.* $(s, s) \notin R$, for any $s \in U$. $\mathcal{F}$ has the property STRONG KERNEL if it has at least one strong kernel.

Goranko and Kapron proved in [8] that STRONG KERNEL is expressible in modal logic over almost all finite frames for frame satisfiability by the short modal formula

$$\Box\Box(p \leftrightarrow \neg \Diamond p),$$

where U corresponds to the set of states where p is true.

After numerical tests, they conjectured that the property is almost surely false, but they didn't succeed in computing the asymptotic probability of this property. Nevertheless they compute the asymptotic probability of another variant of KERNEL, namely a DOUBLE KERNEL, and showed that this property is almost surely false. By applying a Kolaitis and Vardi's result [10], they deduce that the transfer theorem fails for frame satisfiability in modal logic.

In this paper, we define another variant of KERNEL, namely MODALKERNEL. A frame $\mathcal{F} =< S, R >$ has the property MODALKERNEL if there are a subset U of S and a state $s_0 \notin U$ such that $U \cup \{s_0\}$ is a stable set of non-reflexive states and $U \cup \{s_0\}$ is a dominating set over the set of states accessible from s_0, *i.e.* the states $s \in S$ such that $(s_0, s) \in R$.

This property is expressible in modal logic over almost all finite frames for frame satisfiability.

Our main result is the proof that MODALKERNEL does not have an asymptotic probability. We give below an idea of the method.

Let $\mathcal{P}$ be the property KERNEL or one of its variant. The main difficulty of computing the asymptotic probability of $\mathcal{P}$ comes from that we do not know *a priori* which are the possible sizes of a kernel. The first step consists in reducing the study into an unique size $m(n)$ which only depends of the number of vertices n.

Let $E[X]$ be the expectation of the number of kernels of size $m(n)$. In each case, we obtain after non trivial computations the two cases below:
i) $\lim_{n\to+\infty} E[X] = 0$ and $\mathcal{P}$ is almost surely false.
ii) $\lim_{n\to+\infty} E[X] = +\infty$ and $\mathcal{P}$ is almost surely true.

However it is possible that $E[X]$ does not have a limit. Furthemore, we may have different limits for some subsequences of natural numbers n. This is the case for our previous counterexamples of 0-1 laws. The proof that MODALKERNEL does not have an asymptotic probability follows the same scheme as those of our previous proofs [13, 14]; we construct two infinite sets of natural numbers, A and B, such that the property is almost surely

[1] Recently Halpern and Kapron showed how our counterexample helped him discover a gap in their proof of 0-1 law for frame validity.

true (resp. false) if we restrict our study to structures of domain $n \in A$ (resp. $n \in B$). It requires several technical computations which need to adapt Fernandez de la Vega [6] and Tomescu [16] results.

This result refutes Halpern and Kapron's 0-1 law for frame satisfiability and provides the smallest so far fragment of the monadic existential second-order logic for which the 0-1 law fails.

1.1. Definition of the property KERNEL

Definition 1 *Let $H =< V, A >$ be a directed graph and U be a subset of V. U is said to be a* **stable set** *if there is no arc between two vertices of U. U is a* **dominating set** *if, for each vertex v out of U, there is a vertex v' in U such that (v, v') is an arc of H. U is a* **kernel** *if it is both a stable and dominating set and H has the digraph property KERNEL if it has at least one kernel.*

From now on, we will denote by V_n the set $\{0, .., n-1\}$, for any natural number n and $\mathcal{H}_n$ the set of digraphs that have V_n as their set of vertices.

1.2. Random variables

Let $\mathcal{P}$ be one of the properties stable set (stable), dominating (dom) and kernel ($\mathcal{K}$) applied to subsets of V. Let $r \in \{1, \ldots, n\}$. We define (elementary) random variables $X^{\mathcal{P}}_{r,\mathcal{P}}$, for any subset U of V_n of cardinality r, $X^{\mathcal{P}}_{r,U} = 1$ if the property $\mathcal{P}$ holds for U and 0 otherwise. We denote by $X^{\mathcal{P}}_r$ the random variable which equals the number of subsets U of order r satisfying property $\mathcal{P}$. With the above definition, it is obvious that random variables $X^{stable}_{r,U}$ and $X^{dom}_{r,U}$ are independent each other, since they involve two disjoint sets of arcs. Furthermore, stability is a monotone decreasing property (over the subgraphs of H), *i.e.* each subset of a stable set is also a stable set, that is to say

$$\Pr\left(\cup_{r' \geq r}[X^{stable}_{r'} > 0]\right) = \Pr\left(X^{stable}_r > 0\right)$$

by stability is monotone increasing property, *i.e.* each superset of a dominating set is also a dominating set, that is to say

$$\Pr\left(\cup_{r' \leq r}[X^{dom}_{r'} > 0]\right) = \Pr\left(X^{dom}_r > 0\right).$$

For the computations, we use the following asymptotic notations: $f(n) = O(g(n))$ iff there are two positive constants c and N such that $|f(n)| \leq c|g(n)|$ for all $n \geq N$, $f(n) = o(g(n))$ iff $lim_{n\to+\infty}|\frac{f(n)}{g(n)}| = 0$ and $f(n) = \Theta(g(n))$ iff there are three positive constants c_1, c_2 and N such that $c_1|g(n)| \leq |f(n)| \leq c_2|g(n)|$, for all $n \geq N$.

1.3. First results

Tomescu and Fernandez de la Vega independently obtained very close results:

Theorem 1 *(Tomescu, [16])*
Let $H_n \in \mathcal{H}(n, \frac{1}{2})$ and $\beta = \log_2 n - \log_2 \log_2 n$. H_n contains almost surely kernels of order k for each natural number in $]\beta - k_1, \beta + k_2[$, where $k_1 \approx 1.43$ and $k_2 \approx 2.11$ and there is almost surely no kernel of order outside this interval. Moreover, the number $K(H_n)$ of kernels of H_n satisfies

$$n^{0.913+o(1)} < K(H_n) < n^{1+o(1)} \; as \; n \to +\infty.$$

Theorem 2 *(Fernandez de la Vega, [6])*
For any fixed p, $H_n \in \mathcal{H}(n, p)$ has almost surely a kernel of order $\lceil\beta\rceil$ for $\beta = \log_b n - \log_b \log_b n$, where $b = \frac{1}{1-p}$.

It is possible to extend these results by the following theorem:

Theorem 3 *Let $p \in]0, 1[$, $H_n \in \mathcal{H}(n, p)$ and $\beta = \log_b n - \log_b \log_b n$. There exist two natural numbers $k_1 = k_1(p)$ and $k_2 = k_2(p)$ which only depend on p so that $I_\beta =]\beta - k_1(p), \beta + k_2(p)[$ satisfies*

(i) *H_n has almost surely no kernel of order outside I_β.*

(ii) *Let k be a natural number in I_β. H_n has almost surely a kernel of order k.*

1.4. Tools: first and second moment methods

Let $r = r(n)$ be a sequence of natural numbers. Let U be a subset of V_n, we denote by K applied to U the property that U is a kernel.

$$E\,[X^K_r] = \sum_{U \subset V_n, |U|=r} E\,[X^K_{r,U}] = \binom{n}{r} \Pr(K(U_r))$$

where $U_r \subset V_n$ denotes the set $\{0, ..., r-1\}$.
On one hand, if the sequence $r(n)$ satisfies $\lim_{n\to+\infty} E[X^K_r] = 0$, by using the first moment method

$$\Pr\,(X^K_r > 0) \leq E\,[X^K_r],$$

we conclude $\lim_{n\to+\infty} \Pr\,(X^K_r > 0) = 0$.
On the other hand, if the sequence $r(n)$ satisfies

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

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

$$\Pr\,(X^K_r = 0) \leq \frac{E\,[(X^K_r)^2] - E\,[X^K_r]^2}{E\,[X^K_r]^2},$$

this implies $\lim_{n\to+\infty} \Pr\,(X^K_r > 0) = 1$.

1.5 Definitions

From now on, we will use the symbol n and p to denote respectively a natural number and a real in $]0,1[$ and b still equals $\frac{1}{1-p}$.
Let $\beta(n)$ denotes $\log_b\ n - \log_b \log_b\ n$, $m(n)$ denotes $\lfloor\beta(n)\rceil$, the closest natural number to $\beta(n)$ and $m'(n)$ be $\lfloor\frac{3}{4}\ m(n)\rfloor$. Let $f(c) = c + 1 + \ln b$ and $g(c) = -e^c + c + 1 + \ln b$ be functions defined from $\mathbb{R}$ into $\mathbb{R}$. An m-sequence r will be a sequence such that $m'(n) \leq r(n) \leq\ 2\ m(n)$, for any $n \in \omega$. We will denote by $c(n, r(n))$ the unique real c which satisfies $n = e^c\ r(n)\ b^{r(n)}$.

1.6. Proof of Theorem 3 (ii)

Let $\mathcal{P}^{stable}(r)$, $\mathcal{P}^{dom}(r,\nu)$ and $\mathcal{P}^{\mathcal{K}}(r))$ be the probabilities that a subset of V_n of order r will be respectively a stable set, a dominating set over a subset of V_n of order ν, and a kernel. It is easily seen that we have

$$\mathcal{P}^{stable}(r) = b^{-r(r-1)} \text{ and } \mathcal{P}^{dom}(r,\nu) = (1-b^{-r})^{\nu}.$$

Since the events "U_r is a stable set" and "U_r is a dominating set" are independent, we have

$$\mathcal{P}^{\mathcal{K}}(r) = b^{-r(r-1)}\ (1-b^{-r})^{n-r}.$$

It follows $E[X_r^{stable}] = \binom{n}{r}\ b^{-r(r-1)}$
and $E[X_r^{dom}] = \binom{n}{r}\ (1-b^{-r})^{n-r}$
Hence $E[X_r^{\mathcal{K}}] = \binom{n}{r}\ b^{-r(r-1)}\ (1-b^{-r})^{n-r}$.
The proof consists in several steps which require the following lemmas:

Lemma 1 *There is almost surely no kernel of order less than or equal to $m'(n)$.*
We will denote respectively by $min(n,p)$ and $Max(n,p)$ the reals $\beta(n) - k_1(p)$ and $\beta(n) + k_2(p)$.

Lemma 2 *There is almost surely no kernel of order $m'(n) < r < min(n,p)$.*

Lemma 3 *There is almost surely no kernel of order strictly greater than $Max(n,p)$.*

1.7. Proof of Lemmas 1, 2 and 3

These lemmas require the sequence of Claims given below:

Claim 1 $r(n) = \beta(n) - \frac{c(n,r(n))}{\ln b} + o(1)$.

By replacing $r(n)$ by $\beta(n)$, it follows $c(n,\beta(n)) = o(1)$.

Claim 2 $|c(n,m(n))| \leq \frac{\ln b}{2} + o(1)$.

Proof. By definition of $m(n)$ it is a simple application of Claim 1. □

Claim 3 *Let r be an m-sequence. Then $\binom{n}{r} = \Theta\big(\frac{n^r\ r^{-r}}{\sqrt{r}}\big)$.*

Claim 4 *The expectation of the number of stable sets of order r satisfies $E\,[X_r^{stable}] = \Theta\big(\frac{e^{rf(c)}}{\sqrt{r}}\big)$.*

Claim 5 *The probability that a subset of V of order r will be a dominating set satisfies $\mathcal{P}^{dom}(r, n-r) = (1 + o(1))\ e^{-r\ e^c}$.*

Claim 6 *The expectation of the number of kernels of order r satisfies $E\,[X_r^{\mathcal{K}}] = \Theta\big(\dfrac{e^{r\ g(c)}}{\sqrt{r}}\big)$.*

Proof. By combining Claims 4 and 5. □

Let $c_n(r) = c(n,r)$, so that the function is defined from $[m'(n), 2m(n)]$ into $\mathbb{R}$. One can check that, for sufficiently large n (i.e. r), the function c_n is strictly increasing.

Claim 7 *Let $r+1$ denote the sequence $r(n)+1$, then $c_n(r+1) = c_n(r) - \ln b + o(1)$.*

Proof. Apply Claim 1. □

Study of g Since $g'(c) = 0$ iff $c = 0$ and g is strictly decreasing for $c > 0$ and strictly increasing for $c < 0$, the maximum of the function is $g(0) = \ln b$. Thus there are only two reals $0 < c_{min} < c_{Max}$, such that $g(c_{min}) = g(c_{Max}) = 0$. Let $Max(n,p)$ and $min(n,p)$ be the sequences of reals defined by $n = e^{c_{min}}\ min\ b^{min}$ and $n = e^{c_{Max}}\ Max\ b^{Max}$. Observe that c_{min} and c_{Max} do not depend upon n, Claim 7 implies that the interval $I_\beta = [min, Max]$ contains a finite number of natural numbers.

Lemma 1 *There is almost surely no kernel of order less than or equal to $m'(n)$.*

Proof. By using Claims 5 and 3, it follows
$\ln \mathcal{P}^{dom}(m') = (n - m')\ \ln(1-b^{-r})$.
It is easy to check that $b^{-r} = n^{-\frac{3}{4}(1+o(1))}$, then $\mathcal{P}^{dom}(m') = e^{-n^{\frac{1}{4}(1+o(1))}}$. Since $\binom{n}{r} = O(n^r)$, $E\,[X_{m'}^{dom}] = e^{-n^{\frac{1}{4}(1+o(1))}}$, and this term clearly tends to 0 as $n \to +\infty$. Then $\mathcal{H}_n$ has almost surely no dominating set of order $m'(n)$, since dominance is preserved by superset this implies that $\mathcal{H}_n$ has almost surely no dominating set (and a fortiori no kernel) of order less or equal to $m'(n)$. □

Lemma 2 *There is almost surely no kernel of order r, where $m'(n) < r < min(n,p)$.*

Proof. By definition of min, there exists a constant $\kappa < 0$, such that $g(c_{\lfloor min \rfloor}) = \kappa$. Since g is strictly increasing in $[c(n,m'), c_{min}]$, $m'(n) < r < min(n,p)$ implies $g(c(n,r)) < \kappa$, then $E[\,X^{\mathcal{K}_r}\,] < e^{r\ \kappa} \leq e^{m\ \kappa}$.

$$\begin{aligned}\Pr\Big(\bigcup_{m'<r<min} (X_r^{\mathcal{K}} > 0)\Big) &\leq \sum_{m'<r<min} E[\,X_r^{\mathcal{K}}\,] \\ &< min\ e^{m\ \kappa}.\end{aligned}$$

Since $min = \Theta(m')$, it follows

$$\lim_{n\to+\infty} \Pr\,(\bigcup_{m'<r<min} (X_r^{\mathcal{K}} > 0)) \;=\; 0. \;\Box$$

Lemma 3 *There is almost surely no kernel of order strictly greater than Max.*

Proof. First, we prove that we have almost surely no stable set (and a fortiori no kernel) of order strictly greater than $k(n) + 1$. Let δ be the following sequence $\delta(n) = \log_b n - \log_b \log_b n + 1 + \frac{1}{\ln b}$. Then $\delta(n) - \beta(n) = 1 + \frac{1}{\ln b}$. Claim 4 implies $\lim_{n\to+\infty} \Pr\,(\cup_{r\geq Max}[X_r^{stable} > 0]) = 0$.

We establish now that there is almost surely no kernel of order $r \in [\lceil\delta(n)\rceil, \lceil Max\rceil]$.

$$\Pr\big(\bigcup_{\lceil Max\rceil \leq r \leq k} (X_r^{\mathcal{K}} > 0)\big) \leq \sum_{\lceil Max\rceil \leq r \leq \lceil\delta(n)\rceil} E[\,X_r^{\mathcal{K}}].$$

Claim 1 and 2 implies that $\lceil\delta(n)\rceil - m(n) < 2 + \ln b$. Then we deduce by Claim 7 that the number of natural numbers in $]Max, \lceil\delta(n)\rceil]$ are finite and only depends of b. By definition of Max, for any $r \in [Max, k]$ $g(c(n,r) < 0$. Hence

$$\Pr\big(\bigcup_{\lceil Max\rceil \leq r \leq k} (X_r^{\mathcal{K}} > 0)\big) \leq \Theta\big(\frac{1}{\sqrt{Max}}\big)$$

and the last term clearly tends to 0 when $n \to +\infty$. $\Box$

1.8. Proof of Theorem 3 (i)

Fernandez de la Vega established in [6] that

$$\lim_{n\to+\infty} E\,[X_m^{\mathcal{K}}] = +\infty.$$

Then, he proved

$$E\,[(X_m^{\mathcal{K}})(X_m^{\mathcal{K}} - 1)] = (1 + o(1))\; E\,[X_m^{\mathcal{K}}]^2.$$

It follows

$$\lim_{n\to+\infty} \frac{E\,[(X_m^{\mathcal{K}})^2] - E\,[X_m^{\mathcal{K}}]^2}{(E\,[X_m^{\mathcal{K}}])^2} = \lim_{n\to+\infty} \frac{1}{E\,[X_m^{\mathcal{K}}]}.$$

By the Second Moment method,

$$\lim_{n\to+\infty} \Pr\,(X_m^{\mathcal{K}} > 0) = 1,$$

i.e. H_n has almost surely a kernel of order m. We adapt his proof and obtain

$$E\,[(X_{m+t}^{\mathcal{K}})(X_{m+t}^{\mathcal{K}} - 1)] = (1 + o(1))\; (E\,[X_{m+t}^{\mathcal{K}}])^2,$$

for any integer t. Since by definition of I_β we have

$$\lim_{n\to+\infty} E\,[X_r^{\mathcal{K}}] = +\infty,$$

for any natural number $r \in I_\beta$, we conclude that H_n has almost surely a kernel of order r.

2. The 0-1 law fails for frame satisfiability of propositional modal logic

2.1. The modal logic of frame satisfiability

The standard semantics for modal logic is possible-worlds semantics. A frame $\mathcal{F}$ is a pair (S, R) where S is a set of worlds (or states) and R is a binary relation (namely the accessibility relation) on S. We will denote by $M = (S, R, \pi)$ a (Kripke) structure, based on the frame $\mathcal{F}$, where π is a mapping $S \times \{p_1, p_2 \ldots\} \to \{true, false\}$ which gives the truth value of all the primitive propositions $p_1, p_2 \ldots$

Let $s \in S$, the truth of a modal formula is inductively defined as follows: $(\mathcal{M}, s) \models p$, for $p \in \{p_1, p_2 \ldots\}$ iff $\pi(s)(p) =$ true, $(\mathcal{M}, s) \models \neg\varphi$ iff $(\mathcal{M}, s) \not\models \varphi$, $(\mathcal{M}, s) \models \varphi \wedge \psi$ iff $(\mathcal{M}, s) \models \varphi$ and $(\mathcal{M}, s) \models \psi$, $(\mathcal{M}, s) \models \Box\varphi$ iff $(\mathcal{M}, t) \models \varphi$, for every state t accessible from s, *i.e.* $(s, t) \in R$. We define $\Diamond$ the dual of $\Box$ by $\Diamond\varphi \equiv \neg\Box\neg\varphi$

Frame satisfiability

Let φ be a modal formula and $\mathcal{F} = (S, R)$ be a frame. We say that φ is satisfiable in $\mathcal{F}$ if there is a structure $\mathcal{M}$ based on $\mathcal{F}$ and a state $s \in S$ such that $(\mathcal{M}, s) \models \varphi$.

Translation into monadic existential second-order logic

There exists a simple translation of propositional modal logic into monadic existential second-order logic. Let $\mathcal{M} = (S, R, \pi)$ be a (Kripke) structure, we associate a first-order structure $\mathcal{U}_{\mathcal{M}} = (S, R, P_1, P_2, \ldots)$ on the relational vocabulary $R, P_1, P_2, \ldots$, where P_i is the unary relation which encodes the set $\{s \in S \setminus \pi(s, p_i) = true\}$. Each modal formula φ is inductively mapped to the formula $\varphi^{f_0}(x)$ with one free variable x, where $p^{f_0} = P(x)$ if p is a primitive proposition, $(\varphi \wedge \psi)^{f_0} = \varphi^{f_0} \wedge \psi^{f_0}$, $(\neg\varphi)^{f_0} = \neg(\varphi^{f_0})$, $(\Box\varphi)^{f_0} = \forall y\; (R(x, y) \to \varphi^{f_0}[x/y])$, where $\varphi^{f_0}[x/y]$ is the result of replacing all free occurrences of x in φ^{f_0} by y. We have the equivalence between satisfiability of φ in $\mathcal{M}$ and satisfiability of φ^{f_0} in the structure $\mathcal{U}_{\mathcal{M}}$. Thus satisfiability of φ in a Kripke frame $\mathcal{F} = (S, R)$ is expressed by the monadic existential second-order formula $\exists\mathbf{P}\;\exists x\;\varphi^{f_0}(x)$, where $\mathbf{P}$ contains the predicate letters for the primitive propositions occurring in φ. We will denote by $\Sigma_1^1(\exists x MDL)$ the set of these formulae.

The property DIAMETER2

A frame $\mathcal{F}$ has the property DIAMETER2 if every point can be reached from any point in exactly 2 R-steps, i.e. if it satisfies the formula

$$\Psi = \forall x\;\forall y\;\exists z\;(Rxz \wedge Rzy).$$

Fagin [5] proved that all the extension axioms are almost surely true; since Ψ is an extension axiom, the property DIAMETER2 holds in almost all frames.

We denote by $\mathbf{A}$ the universal modality defined as follows: let $\mathcal{M}$ be a Kripke structure and φ be any modal formula, $\mathcal{M} \models A\varphi$ is equivalent to $<\mathcal{M}, s> \models \varphi$, for any state s of $\mathcal{M}$. Therefore let $\mathcal{F}$ be a frame which has the property DIAMETER2, $\mathcal{M}$ be a structure based on the frame $\mathcal{F}$ and φ a modal formula, we have $\mathcal{M} \models A\varphi$
if and only if $<\mathcal{M}, s> \models \Box\Box\varphi$, for any state s of $\mathcal{M}$.

We define later what we will name a kernel in a frame and the corresponding property –the frame has a kernel– will be called MODALKERNEL. The theorem below is the main result of the paper:

Theorem 4 *MODALKERNEL has no asymptotic probability for the uniform distribution case.*

2.2 Idea of the proof of Theorem 4

In this section, we consider frames $\mathcal{F}_{2n}$ with an even number of states $2n$. First we prove that we can concentrate our study only on kernels of size $m(n)$. For this, we establish the proposition below

Proposition 1 *$\mathcal{F}_{2n}$ has almost surely no kernel of order different from m.*

Then we study $E[X]$ the expectation of the number of kernels of size $m(n)$. We define A and B, two infinite sets of even natural numbers. In Proposition 2, we show that

$$\lim_{n \to +\infty} E[X] = 0$$

and then the property is almost surely false, when we restrict our study over $n \in B$. In Proposition 3 we prove that

$$\lim_{n \to +\infty} E[X] = +\infty$$

and the property is almost surely true, when we restrict our study over $n \in A$.

2.3 Definition of the property MODALKERNEL

The property MODALKERNEL has been defined to be expressible in the frames which has the property DIAMETER2. We use a distinguished state to refine the ratio between the two parts of the property, *stability* and *dominance*.

Let $\mathcal{F} = (S, R)$ be a Kripke frame. For any subset U of S and a state s_0 of $\mathcal{F}$, S^{s_0} denotes the set of states accessible from s_0, i.e. $\{s \in S/(s_0, s) \in R\}$ and by L the set of non-reflexive states, i.e. $\{s \in S/(s, s) \notin R\}$.

Assume that the property DIAMETER2 holds for $\mathcal{F}$. Let $\mathcal{M} = <\mathcal{F}, \pi>$ be a structure based on $\mathcal{F}$, we will consider the truth value of the primitive propositions q and p. Let U be a subset of S and s_0 be a state of $\mathcal{F}$.

• (U, s_0) is said to be a **strongly stable set** if $s_0 \notin U$ and for every (ordered) pair (a, b) of states of $U \cup \{s_0\}$, $(a, b) \notin R$ (including the case $a = b$).

Assume s_0 is a state where q is true and U be the set of states where p is true. (U, s_0) is a strongly stable set if and only if

$$<\mathcal{M}, s_0> \models q \wedge \neg p \wedge \Box\Box((p \vee q) \to \neg\Diamond(p \vee q)).$$

• (U, s_0) is said to be **dominating**, if for each state a of S^{s_0}, there is a state b of U such that $(a, b) \in R$. Let U be the set of states where p is true. (U, s_0) is dominating if and only if

$$<\mathcal{M}, s_0> \models \Box\Diamond p.$$

(U, s_0) is a kernel of $\mathcal{F}$ if it is both a *strongly stable* and a *dominating set*. $\mathcal{F}$ has the property MODALKERNEL if there exists s_0 and U such that U is a kernel of $<\mathcal{F}, s_0>$. Hence MODALKERNEL holds in $\mathcal{F}$ if and only if there are a state s_0 and a structure $\mathcal{M}$ based on $\mathcal{F}$ such that

$$<\mathcal{M}, s_0> \models q \wedge \neg p \wedge \Box\Box((p \vee q) \to \neg\Diamond(p \vee q)) \wedge \Box\Diamond p.$$

2.4 Results from a Chernoff bound

Let n_L be the cardinality of L. For any state s_0, we denote by n_{s_0} the cardinality of S^{s_0}. From now on, since we consider the uniform distribution case, for any natural number n, $\beta(n)$ will be the real $\log_2 n - \log_2 \log_2 n$. Furthemore $m(n)$ still denote the natural number $\lfloor \beta(n) \rceil$.

Theorem 5 *(Chernoff) Let $S_{n,p}$ be a random variable with binomial distribution with parameters n and p. For any $h > 0$,*

$$\Pr\left(|S_{n,p} - np| \geq h\right) \leq 2\, e^{-2h^2 n}.$$

Claim 8 *i) For any $\varepsilon > 0$, we have almost surely*

$$|n_L - \frac{n}{2}| < n^{\frac{1}{2}+\varepsilon}.$$

ii) For any $\varepsilon > 0$, the property "there exists a state s_0 such that $|n_{s_0} - \frac{n}{2}| \geq n^{\frac{1}{2}+\varepsilon}$" *is almost surely false.*

Proof of Claim 8. It is a direct application of Theorem 5.

Claim 9 *Let α be a fixed real such that $-\frac{1}{2} < \alpha < \frac{1}{2}$. we will denote by n_k^α the sequence $\lfloor k\ b^{k-\alpha} \rceil$. This sequence satisfies $-\ln b\ \alpha \leq c(m(n_k^\alpha), n_k^\alpha) \leq -\ln b\ \alpha + \Theta(\frac{1}{n})$. and*

$$\lim_{k \to +\infty} m(n_k^\alpha) - \beta(n_k^\alpha) = \alpha.$$

Claim 10 *Let α be a fixed real such that $0 < \alpha < 1$ and n_k^α be the natural number $\lceil k\ 2^{k-\alpha} \rceil$. If we restrict our study over random frames of states of cardinality $2\ n_k^\alpha$,*
$m(n_L) = m(n_{s_0}) = m(n_k^\alpha)$, hold almost surely

Proof. Claim 8 implies that *a.s.* $\log_2 n_{s_0} = \log_2 n + o(1)$, then *a.s.* $\beta(n_{s_0}) - \beta(n) = o(1)$ and similarly we have *a.s.* $\beta(n_L) - \beta(n) = o(1)$. Hence $\beta(n_{s_0}) - \beta(n_L) = o(1)$. Claim 9 implies that *a.s.* $m(n_k^\alpha) - \beta(n_k^\alpha) = \alpha + \Theta(\frac{1}{n})$. We deduce that *a.s.* $m(n_k^\alpha) = m(n_{s_0}) = m(n_L)$. Hence for any sequence 2 n_k^α, we may talk about $m(n_{s_0})$ without referring to a precise set S^{s_0}. □

2.5 Random variables

Let $U \subset S_n$ of order r and $s_0 \in S_n \setminus U$, we denote by $X_{r,U}^{MK-stable}$ the random variable defined as follows: $X_{r,U,s_0}^{MK-stable} = 1$ if U is a strongly stable set and 0 otherwise; $X_{r,U,s_0}^{MK-dom} = 1$ if U is dominating over S^{s_0} and 0 otherwise; $X_{r,U,s_0}^{MK} = 1$ if U is a kernel of $< \mathcal{F}_n, s_0 >$ and 0 otherwise. We denote by $X_{r,U}^{MK-stable}$, $X_{r,U}^{MK-dom}$ and $X_{r,U}^{MK}$ respectively the random variables which equal the sum of the elementary random variables $X_{r,U,s_0}^{MK-stable}$, X_{r,U,s_0}^{MK-dom} and X_{r,U,s_0}^{MK} over all of s_0 and by $X_r^{MK-stable}$, X_r^{MK-dom} and X_r^{MK} those which equals the sum of the random variables $X_{r,U}^{MK-stable}$, $X_{r,U}^{MK-dom}$ and $X_{r,U}^{MK}$ over all U. We denote by $\mathcal{P}^{MK}(r, s_0)$ the probability that (U, s_0) will be a kernel, where s_0 is a state of $\mathcal{S}$ and U is a subset of L of cardinality r. Then

$$\mathcal{P}^{MK}(r, s_0) = \mathcal{P}^{stable}(r+1)\ \mathcal{P}^{dom}(r, s_0),$$

$$E[X_r^{MK-stable}] = \binom{n_L}{r} n_L\ \mathcal{P}^{stable}(r+1),$$

$$E[X_r^{MK-dom}] = \binom{n_L}{r} n_L\ \mathcal{P}^{dom}(r, s_0)$$

and

$$E[X_r^{MK}] = \binom{n_L}{r} n_L\ \mathcal{P}^{MK}(r, s_0).$$

Recall that $m'(n)$ be the integer $m'(n) = \lfloor \frac{3}{4}\ m(n) \rfloor$, for any $n \in \omega$. We still denote by $c(n, r(n))$ the unique real c which satisfies $n = e^c\ r(n)\ 2^{r(n)}$. Recall that we consider the uniform distribution case, let $H_n \in \mathcal{H}(n, \frac{1}{2})$. The following claims establish strong correspondence between the properties KERNEL and MODALKERNEL. Claim 8 implies the following lemma:

Claim 11 *Let r be an m-sequence.*

$$E[X_r^{MK-stable}] = (1 + o(1))\big(n\ 2^{-2r}\ E[X_r^{stable}]\big).$$

Claim 11 and Claim 6 imply

$$E[X_r^{MK-stable}] = \Theta\big(n\ \frac{e^{r(f(c)-2\ln 2)}}{\sqrt{r}}\big).$$

Claim 12 *Let r be an m-sequence. All the states s_0 of $\mathcal{S}$ satisfy almost surely*

$$\mathcal{P}^{dom}(r, s_0) = (1 + o(1))\mathcal{P}^{dom}(r, n - r).$$

We deduce by Claim 12

$$\mathcal{P}^{MK}(r, s_0) = (1 + o(1))\ 2^{-2r}\ \mathcal{P}^{stable}(r)\ \mathcal{P}^{dom}(r, n - r)$$

and

$$\begin{aligned} E[X_r^{MK}] &= (1 + o(1))\Big(n\ 2^{-2r} E[X_r^{\mathcal{K}}]\Big) \\ &= \Theta\big(n\ \frac{e^{r\ (g(c)-2\ln 2)}}{\sqrt{r}}\big). \end{aligned}$$

2.6. Kernels of order different from m

Proposition 1 *$\mathcal{F}_{2n}$ has almost surely no kernel of order different from m.*

Let I_β defined in Theorem 3 on digraphs of order n. We have (Theorem 1) $min \approx \beta - 1.43$ and $Max \approx \beta + 2.11$. For this we prove the following lemmas:

Lemma 4 *$\mathcal{F}_{2n}$ has almost surely no kernel of order less than or equal to $m'(n)$.*

Lemma 5 *$\mathcal{F}_{2n}$ has almost surely no kernel of order $m'(n) < r < min(n)$.*

Lemma 6 *$\mathcal{F}_{2n}$ has almost surely no kernel of order strictly greater than $Max(n)$.*

Lemma 7 *$\mathcal{F}_{2n}$ has almost surely no kernel of order $r \in I_\beta \setminus \{m\}$.*

Proof of Lemma 4
As we did in Lemma 1, it is sufficient to prove that we have almost surely no dominating set of order $m'(n)$.

$$E[X_r^{MK-dom}] = \binom{n_L}{r} n_L\ \mathcal{P}^{dom}(r, n_{s_0}).$$

Let r be a sequence such that $r(n) \leq m'(n)$. By Claim 3, $\binom{n_L}{r} = O(n^r)$, and by Claim 12,

$$\mathcal{P}^{dom}(r, n_{s_0}) = (1 + o(1))\mathcal{P}^{dom}(r, n - r) = e^{-n^{\frac{1}{4}(1+o(1))}}.$$

Then we conclude as in proof of Lemma 1. □
Proof of Lemma 6
Let δ be the sequence $\delta(n) = \log_2 n - \log_2 \log_2 n + 1 + \frac{1}{\ln 2}$. Let $k(n) = \lfloor \delta(n) \rfloor$. As we did in the proof of Lemma 3, we prove that we have almost surely no stable set (and a fortiori no kernel) of order strictly greater than $k(n) + 1$.

$$\Pr\Big(\bigcup_{\lceil Max \rceil \leq r \leq k} (X_r^{MK} > 0)\Big) < n_L\ 2^{-2\lceil Max \rceil}\ \Theta\big(\frac{1}{\sqrt{Max}}\big).$$

Since $n_L \ 2^{-2\lceil Max \rceil} = O(1)$, we conclude as in Lemma 3. $\square$

Proof of Lemma 7:
By study of g, we know that the maximum of the function is $\ln 2$ and is reached for $c = 0$. Let $\nu = min(g(-\frac{1}{2}), g(\frac{1}{2}))$, then $\nu < \ln 2$. By definition of $m, g(c(n,r)) < \nu$ and $n = \Theta(r \ 2^r)$, for any sequence $r \in I_\beta \setminus \{m\}$. Furthermore Claim 11 and 12 imply

$$E[X_r^{MK}] = \Theta\big(n \ \frac{e^{r \ (g(c) - 2\ln 2)}}{\sqrt{r}}\big) < \Theta\big(e^{r(\nu - \ln 2)}\big),$$

$$\Pr\big(\bigcup_{r \in I_\beta \setminus \{m\}} X_r^{MK} > 0\big) < (Max - min) \ \Theta\big(e^{Max(\nu - \ln 2)}\big).$$

Since I_β contains a finite number of natural numbers, the last term tends to 0 as $n \to +\infty$. $\square$

2.7. Kernels of order m

We will denote by X, the random variable X_m^{MK}.

Proposition 2 *Let $\alpha \neq 0$ in $]-\frac{1}{2}, \frac{1}{2}[$. We restrict now our study over frames with $2 \ n_k^\alpha$ states, where $n_k^\alpha = \lfloor k \ 2^{k-\alpha} \rceil$. The property MODALKERNEL is almost surely false over these frames.*

Proof. By Claim 9 $-\ln 2 \ \alpha \leq c(m) \leq -\ln 2 \ \alpha + \Theta(\frac{1}{n})$. Then $E\,[X] < 2^{-2m} \ n \ e^{-\lambda m} < \Theta(me^{-\lambda m})$, for some $\lambda > 0$. Hence $\lim_{k \to +\infty, n = 2 \ n_k^\alpha} \ E\,[X] = 0$. Combining Proposition 2 and 1 and applying the first moment method, we deduce that MODALKERNEL is almost surely false over $\mathcal{F}_{2 \ n_k^\alpha}$. $\square$

Proposition 3 *Almost all frames with $2 \ n_k^0$ states have kernel of order m.*

Proposition 3 requires the lemma below

Lemma 8

$$E\,[X(X-1)] = (1 + o(1))(E\,[X])^2.$$

Proof of Proposition 3.
First we establish

$$\lim_{k \to +\infty, n = 2 \ n_k^\alpha} E\,[X] = +\infty.$$

Since $0 \leq c(m) \leq \Theta(\frac{1}{n})$, $g(c(m)) - \ln 2 = o(\frac{1}{m})$.
Hence Claim 11 and 12 imply

$$\begin{aligned} E\,[X] &= \Theta\big(n \ \frac{e^{m \ (g(c) - 2\ln 2)}}{\sqrt{m}}\big) \\ &= \Theta\big(m \ \frac{1}{\sqrt{m}}\big) = \Theta\big(\sqrt{m}\big). \end{aligned}$$

By the second moment method, Lemma 8 implies

$$\Pr\,(X_m^{\mathcal{K}} = 0) < \Theta\big(\frac{1}{\sqrt{m}}\big). \square$$

Proof of Lemma 8
Let s_1 and $s_2 \in L$, we denote by n_{s_1,s_2} the cardinality of $|S^{s_1} \cap S^{s_2}|$. Similarly as in Claim 8, we prove that for any $\varepsilon > 0$, the property *"There exists a pair (s_1, s_2) such that $|n_{s_1,s_2} - \frac{n}{2}| \geq n^{\frac{1}{2}+\varepsilon}$"* is almost surely false. We get the same result by replacing n_{s_1,s_2} by $n_{s_1} \setminus n_{s_1,s_2}$ and $n_{s_2} \setminus n_{s_1,s_2}$. Let U_1 and U_2 two subsets of cardinality m, we denote by l the cardinality of $U_1 \cap U_2$. We will denote by $\mathcal{P}^{dom2}(m, l, s_1, s_2)$ the conditional probability that (U_1, s_1) is a dominating set given the hypothesis that (U_2, s_2) is a dominating set. It follows

$$\begin{aligned} &\Pr\big(X_{m,U_1,s_1}^{MK} = X_{m,U_2,s_2}^{MK} = 1\big) \\ &= \Pr\big(X_{m,U_1,s_1}^{MK} = 1 / X_{m,U_2,s_2}^{MK} = 1\big) \ \Pr\big(X_{m,U_2,s_2}^{MK} = 1\big) \\ &= \frac{\mathcal{P}^{stable}(m)}{\mathcal{P}^{stable}(l)} \mathcal{P}^{dom2}(m, l, s_1, s_2) \mathcal{P}^{MK}(m, s_2). \end{aligned}$$

We consider the following decomposition

$$E\,[X(X-1)] = \mathcal{A} + \mathcal{B} + \mathcal{C},$$

where $\mathcal{A}$, $\mathcal{B}$ and $\mathcal{C}$ are the summations for the cases

$\mathcal{A}$: $U_1 \neq U_2$ and $s_1 \neq s_2$,
$\mathcal{B}$: $U_1 \neq U_2$ and $s_1 = s_2$.
$\mathcal{C}$: $U_1 = U_2$ and $s_1 \neq s_2$.

Lemma 8 is obtained with the following claims:

Claim 13 $\mathcal{A} = (1 + o(1))(E\,[X_m^{MK}])^2$.

Claim 14 $\mathcal{B} = o(E\,[X_m^{\mathcal{K}}])^2)$.

Claim 15 $\mathcal{C} = o(1)$.

3. Conclusion

We denote by ML^r and ML^{as} respectively the modal logic of the countable random frame and the modal logic of almost surely frame validity. Goranko and Kapron [8] gave a sound and complete axiomatization of ML^r and showed that it is not finitely axiomatizable. The negation of DOUBLE KERNEL is expressible by a modal formula in $ML^{as} \setminus ML^r$, so clearly ML^r is strictly included in ML^{as}. They conjecture that all the properties expressible by formulae in $ML^{as} \setminus ML^r$ are precisely similar properties, namely *kernel partitions*.

Acknowledgments

I would like to thank Valentin Goranko for stimulating and useful discussions, I am indebted to him for this work on modal logic. I have also benefited from comments, suggestion and drafting help from Etienne Grandjean, Ioan Tomescu and Wenceslas Fernandez de la Vega and the anonymous referees.

References

[1] V. Chvàtal. On the computational complexity of finding a kernel. Technical report, Report NO CRM-300, univ. de Montréal, 1973. Centre de Recherches Mathématiques.

[2] N. Creignou. *The class of problems that are linearly equivalent to satisfiability or a uniform method for proving NP-completeness.* Theoretical Computer Science 145:111-145, 1995.

[3] P. Erdös and A. Rényi. On the evolution of random graphs. *Pupl. Math. Inst. Hungar. Acad. Sci.*, 7:17–61, 1960.

[4] R. Fagin. Generalized first-order spectra and polynomial time recognizable sets. In R. Karp, editor, *Complexity of Computations*, volume 7 of *SIAM-AMS Proceedings*, pages 43–73, Providence, RI, 1974. American Mathematical Society.

[5] R. Fagin. Probabilities on finite models. *Journal of Symbolic Logic*, 41:50–58, 1976.

[6] W. Fernandez De La Vega. Kernel on random graphs. *Discrete Mathematics*, 82:213–217, 1990.

[7] 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*, 5:142–154, 1969.

[8] V. Goranko and B. Kapron. *The Modal Logic of the Countable Random Frame to appear in Archive for Mathematical Logic.*

[9] J. Y. Halpern and B. M. Kapron *Zero-One Laws for Modal Logic Annals of Pure and Applied Logic*, 69, 1994, 157-195.0

[10] Ph. G. Kolaitis and M.Y. Vardi. 0-1 laws and decisions problems for fragments of second-order logic. *Information and Computation*, 87:302–338, 1990.

[11] Ph. G. Kolaitis and M.Y. Vardi. 0-1 laws for fragments of second-order logic: on overview. In *Logic from computer science (Proc. of Workshop, 1989)*, pages 265–286. Y. N. Moschovakis, 1992.

[12] Ph. G. Kolaitis and M.Y. Vardi. 0-1 laws for Fragments of Existential Second-Order Logic: A Survey. *Mathematical Foundations of Computer Science*, pages 84–98, 2000.

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

[14] J-M. Le Bars. Counterexamples of the 0-1 law for fragments of existential second-order logic: an overview. *Bulletin of Symbolic Logic*, 9:67–82, 2000.

[15] L. Pacholski and W. Szwast. A counterexample to the 0-1 law for the class of existential second-order minimal Gödel sentences with equality. *Information and Computation*, 107:91–103, 1993.

[16] I. Tomescu. Almost all digraphs have a kernel. *Discrete Mathematics*, 84:181-192, 1990.

A. Claims for Theorem 3

A.1. Proof of Claim 1

By definition of c, we have $\log_b n = \log_b e^c + \log_b r + r$. Hence

$$\begin{aligned} r &= \log_b n - \log_b e^c - \log_b r \\ &= (\log_b n - \log_b \log_b n) - \frac{c}{\ln b} + \\ &\quad (\log_b \log_b n - \log_b r) \\ \log_b r &= \log_b \big(\log_b n \, (1 - \frac{\log_b e^c + \log_b r}{\log_b n}), \\ &= \log_b \log_b n - o(1). \end{aligned}$$

It follows $r = \beta - \dfrac{c}{\ln b}$.

A.2. Proof of Claim 3

Let t be the sequence $n, r(n)$ or $n - r(n)$. Stirling's formula implies

$$t! = t^t \, \exp(-t) \sqrt{2\pi t} \, \exp(o(1)).$$

Hence

$$\begin{aligned} n\,! &= \exp(n \ln n - n + \tfrac{1}{2} \ln n + O(1)). \\ r\,! &= \exp(r \ln r - r + \tfrac{1}{2} \ln r + O(1)). \\ (n-r)\,! &= \exp((n-r)\ln(n-r) - (n-r) + \\ &\quad \tfrac{1}{2}\ln(n-r) + O(1)). \end{aligned}$$

$\ln \binom{n}{r} = n \ln n - n + \dfrac{1}{2} \ln n - r \ln r + r - \dfrac{1}{2} \ln r - (n-r)\ln(n-r) + (n-r) - \dfrac{1}{2}\ln(n-r) + O(1) = n \ln n - r \ln r - n \ln n + n\dfrac{r}{n} + r \ln n - r\dfrac{r}{n} - \dfrac{1}{2}\ln r + \dfrac{1}{2}\dfrac{r}{n} + O(1).$

By observing that $r^2 = o(n)$, it follows $\ln(n-r) = \ln n - \frac{r}{n} + o(\frac{r^2}{n^2}) = \ln n - \frac{r}{n} + o(\frac{1}{n})$.

Then $\ln \dbinom{n}{r} = r \ln n - r \ln r + r - \dfrac{1}{2} \ln r + O(1)$.

A.3. Proof of Claim 4

By definition of $c = c(n, r)$, we have

$$\ln n = c + \ln r + r \ln b.$$

By applying Claim 3, it follows:

$$\begin{aligned} \ln \binom{n}{r} &= r\,c + r \ln r + r^2 \ln b - r \ln r + r \\ &\quad - \tfrac{1}{2} \ln r + O(1). \\ &= r\,c + r^2 \ln b + r - \tfrac{1}{2} \ln r + O(1). \\ \ln \mathcal{P}^{stable}(r) &= -r(r-1) \ln b = -r^2 \ln b + r \ln b. \\ E\,[X_r^{stable}] &= \binom{n}{r} \mathcal{P}^{stable}(r) = \Theta\big(\frac{e^{rf(c)}}{\sqrt{r}}\big). \end{aligned}$$

A.4. Proof of Claim 5

$$\begin{aligned} &\ln \mathcal{P}^{dom}(r, n-r) = (n-r) \ln(1 - b^{-r}). \\ &= (e^c \, r \, b^r - r)\,(-b^{-r} + 0(b^{-2r}). \\ &= -e^c \, r + O(e^c \, r \, b^{-r}) + r \, b^{-r} + O(r \, b^{-2r}). \end{aligned}$$

Since $r\ b^{-r} + O(r\ b^{-2r}) = o(1)$, it remains to establish $\lim_{n\to+\infty} e^c\ r\ b^{-r} = 0$. By definition $n = e^c\ r\ b^r$, then $e^c\ r\ b^{-r} = n\ b^{-2r}$. By assumption, $\lfloor \frac{3}{4}\ m(n) \rfloor \le r(n) \le 2m(n)$. Then $\frac{3}{4}(\log_b n - \log_b \log_b n) \le r$ and $\frac{5}{8}\log_b n < r$, for n large enough. It follows $n < b^{\frac{8}{5}r}$ and $n\ b^{-2r} < b^{-\frac{2}{5}r}$, we conclude by observing that the last term tends to 0 when $n \to +\infty$.

$$E\left[X_{m'}^{dom}\right] = \binom{n}{m'}\ (1 - b^{-m'})^{n-m'}.$$

By using Claims 5 and 3, it follows

$$\ln \mathcal{P}^{dom}(m') = (n - m')\ \ln(1 - b^{-r}).$$

It is easy to check that $b^{-r} = n^{-\frac{3}{4}(1+o(1))}$, then

$$\mathcal{P}^{dom}(m') = e^{-n^{\frac{1}{4}(1+o(1))}}.$$

Since $\binom{n}{r} = O(n^r)$, we have

$$E\left[X_{m'}^{dom}\right] = e^{-n^{\frac{1}{4}(1+o(1))}},$$

and this term clearly tends to 0 as $n \to +\infty$. We have almost surely no dominating set of order $m'(n)$, since dominance is preserved by superset, this implies that we have almost surely no dominating set (and a fortiori no kernel) of order less than or equal to $m'(n)$.

B Claims for Theorem 4

B.1. Proof of Claim 9

Since $c(\beta(n_k^\alpha, n_k^\alpha)) = o(1)$, by applying Claim 7, we deduce $-\frac{\ln b}{2} + o(1) < c(m(n_k^\alpha, n_k^\alpha)) < \frac{\ln b}{2} + o(1)$. We have $e^{c(k-1,n_k^\alpha)}\ (k-1)\ b^{k-1} \le (1+o(1))(k-1)\ b^{k-1} < k\ b^{k-\alpha}$. Then $m(n_k^\alpha) = k$ and $n_k^\alpha = e^{c(m(n_k^\alpha,n_k^\alpha))}\ k\ b^k$. By definition of n_k^α, $0 \le n_k^\alpha - k\ b^{k-\alpha} \le 1$. This implies $e^{c(m(n_k^\alpha,n_k^\alpha))} - b^{-\alpha} < o(1)$, i.e. $-\ln b\ \alpha \le c(m(n_k^\alpha), n_k^\alpha \le -\ln b\ \alpha + \Theta(\frac{b^{\alpha-k}}{k})$, we conclude $-\ln b\ \alpha \le c(m(n_k^\alpha), n_k^\alpha) \le -\ln b\ \alpha + \Theta(\frac{1}{n})$. Then $n_k^\alpha = (1+o(1))\ k\ b^{k-\alpha} = (1+o(1))\ (k-\alpha)\ b^{k-\alpha}$. Hence $\beta(n_k^\alpha) = k - \alpha + o(1)$ and $\lim_{k\to+\infty} m(n_k^\alpha) - \beta(n_k^\alpha) = \alpha$.

B.2. Proof of Claim 12

$\mathcal{P}^{dom}(r, s_0) = (1-2^{-r})^{n-r}(1-2^{-r})^{n_{s_0}-n+r}$. Claim 8 implies that $n_{s_0} - n + r < n^{\frac{1}{2}+\varepsilon}$ holds almost surely, for any $\varepsilon > 0$. Hence $(1-2^{-r})^{n_{s_0}-n+r} = 1 + o(1)$.

B.3. Proof of Claim 13

We will denote by $A(m, l, k_1, k_2)$ the probability $\mathcal{P}^{dom2}(m, l, s_1, s_2)$ when we assume that $n_{s_1} = k_1$ and $n_{s_1,s_2} = k_2$. By using Claim 8, we obtain

$$\mathcal{P}^{dom2}(m, l, s_1, s_2) = (1 + o(1))\ A(m, l, n, \frac{n}{2}).$$

Assume that $n_{s_1} = n_{s_2} = 2\ n_{s_1,s_2} = n_L = n$, by the hypothesis U_2 is dominating over S^{s_2}, for each $a \in S^{s_1} \cap S^{s_2}$ there exists $b \in U_2$ such that $(a, b) \in R$; when $b \in U_1 \cap U_2$, the condition "*there exists* $b \in U_1$ *such that* $(a, b) \in R$" is previously checked, hence

$$A(m, l, n, \frac{n}{2}) \le A(m, l, n, n).$$

Combining with the previous result, it follows

$$\mathcal{P}^{dom2}(m, l, s_1, s_2) \le (1 + o(1))A(m, l, n, n).$$

Observe that $\frac{\mathcal{P}^{stable}(m)}{\mathcal{P}^{stable}(l)}\ A(m, l, n, n)$ is equal to the conditional probability that a U_1 is a kernel of H_n given the hypothesis that a U_2 is a kernel of H_n, for any subsets U_1 and U_2 of V_n of cardinality m, such that $|U_1 \cap U_2| = l$. By applying Claim 11 and 12, it follows

$$\begin{aligned}\mathcal{A} &= n_L(n_L-1)\ 2^{-4m}E\left[(X_m^{\mathcal{K}})(X_m^{\mathcal{K}}-1)\right]\\ &= (1+o(1))\ n^2\ 2^{-4m}E\left[(X_m^{\mathcal{K}})(X_m^{\mathcal{K}}-1)\right].\end{aligned}$$

Fernandez de la Vega prove in [6] that

$$E\left[(X_m^{\mathcal{K}})(X_m^{\mathcal{K}}-1)\right] = (1+o(1))(E\left[X_m^{\mathcal{K}}\right])^2.$$

By Claim 12, $E[X] = (1+o(1))\big(n\ 2^{-2m}\ E[X_m^{\mathcal{K}}]\big)$.
It follows $\mathcal{A} = (1+o(1))(E\left[X_m^{MK}\right])^2$.

B.4. Proof of Claim 14

Recall that $n = (1 + o(1))\ m\ 2^m$.

$$\begin{aligned}\mathcal{B} &= n_L\ 2^{-2(2m-l)}\binom{n_L}{m}\binom{m}{l}\binom{n_L-m}{m-l}\\ &\quad \Pr\left(X_{m,U_1,s_1}^{MK} = X_{m,U_2,s_2}^{MK} = 1\right)\\ &\le (1+(o(1))n\ 2^{-2m}\ E\left[(X_m^{\mathcal{K}})(X_m^{\mathcal{K}}-1)\right]\\ &\le (1+o(1))\ m\ 2^{-m}\ E\left[(X_m^{\mathcal{K}})(X_m^{\mathcal{K}}-1)\right]\\ &\le o((E\left[X_m^{\mathcal{K}}\right])^2).\end{aligned}$$

B.5. Proof of Claim 15

$$\begin{aligned}\mathcal{C} &= n_L(n_L-1)2^{-2m}\binom{n_l}{m}\\ &\quad \Pr\left(X_{m,U_1,s_1}^{MK} = X_{m,U_2,s_2}^{MK} = 1\right)\\ &\le (1+o(1))(n)^2\ 2^{-2m}\binom{n_l}{m}\\ &\quad \mathcal{P}^{\mathcal{K}}(m)\ A(m, 0, n_{s_1}, n_{s_1,s_2}).\end{aligned}$$

We know that

$$\mathcal{P}^{dom2}(m, 0, n_{s_1}, n_{s_1,s_2}) = (1+o(1))A(m, 0, n, \frac{n}{2})$$

and it is easily seen that

$$A(m, 0, n, \frac{n}{2}) = \mathcal{P}^{dom}(m, \frac{n}{2})$$

and Claim 5 implies $\mathcal{P}^{dom2}(m, s_0) \le e^{-\frac{m}{2}}$.
Then $\mathcal{C} \le (1+(o(1))m^2\ e^{-\frac{m}{2}}\ E\left[X_m^{\mathcal{K}}\right]$.

Since $E\left[X_m^{\mathcal{K}}\right] = O\big(\sqrt{m}\big)$, it follows $\mathcal{C} = o(1)$.