TASK QUARTERLY 9 No 3, 317–335

PROBABILISTIC VARIANTS OF RÉNYI-ULAM GAME AND MANY-VALUED LOGIC

CLAUDIO MARINI AND FRANCO MONTAGNA

Dipartimento di Scienze Matematiche ed Informatiche,
Università degli Studi di Siena,
Pian dei Mantellini 44, 53100 Siena, Italy
{*marinic, montagna*}*@unisi.it*

(Received 5 January 2005)

Abstract: In this paper we discuss some generalizations of Rényi-Ulam game with lies: some of them are simply probabilistic variants of it, some others differ from it by the presence of more than one number to guess. In the last part of the paper, we also discuss the relationship between such variants and many-valued logic. This paper is just a survey of known results, but in its last part it also contains some plans for future research.

Keywords: Rényi-Ulam game, guessing secrets

1. Introduction

In 1976 Ulam raised the following problem:

> Someone thinks of a number between one and one million (which is just less than 2^{20}). Another person is allowed to ask up to twenty questions, to each of which the first person is supposed to answer only yes or no. Obviously the number can be guessed by asking first: Is the number in the first half-million? and then again reduce the reservoir of numbers in the next question by one-half, and so on. Finally the number is obtained in less than $\log 1\,000\,000$. Now suppose one were allowed to lie once or twice, then how many questions would one need to get the right answer? One clearly needs more than n questions for guessing one of the $2n$ objects because one does not know when the lie was told. This problem is not solved in general.
>
> Stanisław Ulam, "Adventures of a Mathematician"

This problem, also investigated by Rényi in [1], is known as Rényi-Ulam game. In the last years, mathematicians have studied it in deep, *cf.* [2–7]. The problem has two versions, the adaptive one, where Questioner waits for Responder's answer before formulating the next question, and the non adaptive one, where Questioner has to do all questions in advance. The non adaptive version is just the error-correcting coding theory, *cf.* for instance [8]. This problem has a great number of variants. For instance, one may investigate what happens if Responder can lie only if the answer is YES (respectively if the answer is NO). Alternatively, one may investigate the partially

adaptive game where Questioner must ask a group of non-adaptive questions since the beginning, and then another group of questions after Responder answers to the first group of questions. These problems have been investigated in [9, 10].

Other variants of Rényi-Ulam game with lies arise if we either assume that Responder chooses at random whether to lie or not, or if we assume that there are several numbers to guess, and not just one. The first idea (probabilistic Rényi-Ulam game) was developed by Pelc in [5], and will be reviewed in Section 2. Here the problem is to develop a strategy in order to guess the number with probability $\geq q$ (q being a real in $(0,1)$ given by the problem) with a small number of YES-NO questions assuming that Responder lies with fixed probability $0 < p < \frac{1}{2}$. As we will see, the problem has also a continuous variant.

The second idea (*i.e.*, many numbers to guess) incorporates the Group Testing problem (*cf.* [11]) and the Guessing Secrets game (*cf.* [12]). In both cases we have a finite large search space Ω and a subset S of it (the defective set or the secret set), and Questioner has to guess the elements of S (or to know as much as possible about S) by means of questions of the form: *Is your number in* X*?*, where $X \subseteq \Omega$. The difference between the two games is the following: in Group Testing, Responder has to answer YES if at least one defective is in X, whereas in the Guessing Secret game, Responder can choose one secret (not necessarily the same for all questions) and answer truthfully on the ground of it. A common probabilistic variant of both games is the Probabilistic Guessing Secrets. In this game, given a question of the form: *Is your number in* X*?*, Responder chooses at random (with uniform distribution) one of the secrets, and answers truthfully on the ground of it. This game has been introduced in [12], and will be discussed in Section 3.

Game theory is strictly related to logic. For example, proving a formula can be regarded as a game between two players, the prover, who tries to prove the formula, and the opponent, who tries to attack the prover's attempts. However, in this case the games are *ad hoc*, in the sense that they are not interesting in themselves, their interest is based on the fact that they constitute a good semantics for proofs. Rényi-Ulam game with lies is an exception: it is an interesting game with several applications, and at the same time it constitutes a very natural semantics for Łukasiewicz logic, *cf.* [13] or [14], Section 5. This suggests the following problem: for any of the games listed above, try to find a logic of which the game is a semantics. In other words, for G being any of the above mentioned games, try to solve the equation:

$$\frac{\text{Ulam game with lies}}{\text{Łukasiewicz logic}} = \frac{G}{x}.$$

For the moment, we have no satisfactory solution. In Section 4, we sketch an attempt by Hájek and others to treat probability in the context of many-valued logic, transforming probabilistic computations into derivations in propositional many valued logic. In principle, this makes it possible to treat probability, and probabilistic games in particular, by logical means. This fact has a considerable theoretical interest. However, this is not our desideratum: so far, no efficient decision algorithm is known for Hájek's probabilistic logic, therefore, *prima facie* using logic instead of probability seems a complication rather than a simplification. Moreover, finding a logic which is suitable for a treatment of a game is something different from proving that the game

constitutes a semantics for that logic. Still, it is possible that Hájek's approach will prove useful in order to find logical counterparts for all probabilistic games presented in this paper. An important goal for future research would be to find other examples of pairs interesting logic-interesting game such that the game constitutes a semantics for the logic. In the last section we present some ideas which may be helpful in order to reach this goal.

2. Probabilistic variants of Rényi-Ulam game

In this section we review the work by Rivest (*cf.* [2]) and Pelc (*cf.* [5]) concerning some probabilistic variants of Rényi-Ulam game with lies. In these games, Responder can lie with probability p with $0<p<1$, and Questioner has to guess the number with probability $\geq q$, with $0<q<1$. The parameter q is called *the reliability*. In more details, we consider the following games:

(i) The continuous game $G_{p,q}([0,1],\epsilon)$ (a continuous and probabilistic generalization of Rényi-Ulam game). Responder thinks of a number $x\in[0,1]$ unknown to Questioner, who has to find, with probability $\geq q$, a set $A\subset[0,1]$ such that $\|A\|<\epsilon$ (where $\|A\|$ denotes the measure of A), and $x\in A$. He can ask questions of the form $x<a$? ($a\in[0,1]$). As we said, Responder can lie with probability p. The parameter ϵ is called *the accuracy*. We will mainly consider the case where $\epsilon=\frac{1}{n}$, n a positive integer.

(ii) The discrete bounded game $G_{p,q}\{1,\ldots,n\}$ (a more direct probabilistic generalization of Ulam game). Responder thinks of an integer $x\in\{1,\ldots,n\}$ unknown to Questioner, who has to find it with probability $\geq q$ stating queries of the form $x<a$? with $a\in\{1,\ldots,n\}$. (Note that since the unknown number is an integer, the problem does not change if we allow Questioner to ask questions of the form $x<a$? with $a\in[1,n]$).

In order to deal with these games, it is useful to consider first some probability-free versions of them. In these games, a positive integer M and a real number p with $0<p<1$ are given. The assumption that Responder can lie with probability p is replaced by the following assumption: for an initial series of $m\geq M$ answers, the number of errors cannot exceed pm. Moreover, Questioner has to guess the number (or, in the continuous game, some kind of approximation of it) correctly, and not only with probability q. The other rules remain as in the probabilistic games. In more detail:

(i′) The continuous game $G^*_{p,M}([0,1],\epsilon)$ is similar to the game $G_{p,q}([0,1],\epsilon)$, with the differences just mentioned. Once again, we will mainly consider the case $\epsilon=\frac{1}{n}$, n a positive integer.

(ii′) The discrete bounded game $G^*_{p,M}\{1,\ldots,n\}$ is similar to $G_{p,q}\{1,\ldots,n\}$, with the differences just mentioned.

Lemma 1. *Questioner can win each of the games $G^*_{p,M}([0,1],\frac{1}{n})$, $G^*_{p,M}\{1,\ldots,n\}$, for all n and M if and only if $p\neq\frac{1}{2}$.*

Proof. If $p=\frac{1}{2}$, then let k be the unknown number, and let $m\neq k$ be another number (in the continuous game we take m so that the distance between k and m is greater than 2ϵ). Then Responder can refer half of his answers to m and the other half to k.

On the ground of Responder's answers, Questioner cannot know which one among m and k is the right number, *i.e.* he cannot win the game. If $p > \frac{1}{2}$, then we can consider the opposite of Responder's answers, thus we can reduce the problem to the case where $p < \frac{1}{2}$. In this case, there is a rather easy greedy guessing strategy (the idea is: repeat each question many times, until the majority of answers to that specific question exceeds pK, where $K > M$ is the total number of questions). We will see that there is a better strategy whose cost is $\mathcal{O}(\log n)$ (for the game $G^*_{p,M}\{1,\ldots,n\}$ we need $p < \frac{1}{3}$). The proof of this fact, due to Pelc, is presented below. ■

We start from the continuous game $G^*_{p,M}([0,1],\epsilon)$. In the sequel, given two positive integers Q and E, $\epsilon(Q,E)$ denotes the smallest number ϵ such that with Q questions of the form $x < a$? and at most E wrong answers, Questioner can guess, in the worst case, a set A such that $\|A\| < \epsilon$ and $x \in A$. Moreover, $Q_{con}(n,E)$ denotes the minimum number of questions necessary to guess a set A such that $\|A\| < \frac{1}{n}$ and $x \in A$ when Responder is allowed to lie E times at most. Finally, $\left(\binom{n}{m}\right)$ denotes the number of subsets of $\{1,\ldots,n\}$ of cardinality $\leq m$, that is: $\left(\binom{n}{m}\right) = \sum_{i=0}^{m}\binom{n}{i}$.

Theorem 1. *For any two positive integers Q and E, one has: $\epsilon(Q,E) \leq \left(\binom{Q}{E}\right)\cdot 2^{-Q}$.*

Proof. Following [5], we introduce the concept of *state of knowledge* of Questioner after $Q-q$ questions and after the corresponding answers. The idea is the following: for $e \leq E$ we define the set A^e_q of all elements of $[0,1]$ which are coherent with Responder's answers under the assumption that exactly e of them are wrong. A state of knowledge with q questions remaining (hence after $Q-q$ questions and after the corresponding answers) is the $E+1$-tuple $A_q = (A^0_q,\ldots,A^E_q)$. If $q = Q$, that is, if no question has been asked, then there must be 0 lies, so for $e > 0$ one has $A^e_Q = \emptyset$. Moreover, every x is coherent with the assumption that there are no lies, since there is no question. Thus $A^0_Q = [0,1]$. In other words, $A_Q = ([0,1],\emptyset,\ldots,\emptyset)$. Now assume that $A_q = (A^0_q,\ldots,A^E_q)$, and that the next question is: $x < a$?. Let $T = \{x \in [0,1] : x < a\}$, and let $F = [0,1]\setminus T$. If the answer is YES, then $A_{q-1} = ({}^YA^0_{q-1},\ldots,{}^YA^E_{q-1})$ with ${}^YA^0_{q-1} = A_q \cap T$, and ${}^YA^{e+1}_{q-1} = (A^{e+1}_q \cap T)\cup(A^e_q \cap F)$. Similarly if the answer is NO, then $A_{q-1} = {}^NA_{q-1} = ({}^NA^0_{q-1},\ldots,{}^NA^E_{q-1})$ with ${}^NA^0_{q-1} = A_q \cap F$, and ${}^NA^{e+1}_{q-1} = (A^{e+1}_q \cap F)\cup(A^e_q \cap T)$. Clearly we always have $x \in \bigcup_{e=0}^{E} A^e_q$.

Now we define the *weight* $w(q,A_q)$ of a state A_q when there are q questions remaining by:

$$w(q,A_q) = \sum_{e=0}^{E}\left(\binom{q}{E-e}\right)\cdot\|A^e_q\|,$$

where $\|A^e_q\|$ denotes the measure of A^e_q. (This definition is due to Berlekamp [15]). The following lemma can be proved by checking, using the identity:

$$\left(\binom{n+1}{m+1}\right) = \left(\binom{n}{m+1}\right) + \left(\binom{n}{m}\right).$$

Lemma 2. *The weight function is additive, in the sense that $w(q-1,{}^YA_{q-1}) + w(q-1,{}^NA_{q-1}) = w(q,A_q)$.* ■

We continue the proof of Theorem 1. Note that $w(0,A_0) = \sum_{e=0}^{E}\left(\binom{0}{E-e}\right)\|A^e_0\| = \sum_{e=0}^{E}\|A^e_0\|$, because if $i > 0$, then $\binom{0}{i} = 0$. By this observation and by Lemma 2,

the worst case occurs if Responder always chooses the answer which makes the weight bigger, *i.e.* if Responder answers YES if $w(q-1,{}^{Y}A_{q-1}) > w(q-1,{}^{N}A_{q-1})$ and answers NO otherwise. Moreover, the best strategy for Questioner is to ask a question such that $w(q-1,{}^{Y}A_{q-1}) = w(q-1,{}^{N}A_{q-1})$ (in this way, by Lemma 2, $w(q-1,A_{q-1}) = \frac{w(q,A_q)}{2}$). Now consider $w(q-1,{}^{Y}A_{q-1})$ and $w(q-1,{}^{N}A_{q-1})$ as a functions ${}^{Y}w(a,q)$ and ${}^{N}w(a,q)$ of the parameter a occurring in the question: $x<a$?. Clearly for fixed q, ${}^{Y}w(a,q)$ and ${}^{N}w(a,q)$ are continuous, ${}^{Y}w(0,q) < {}^{N}w(0,q)$, and ${}^{N}w(1,q) < {}^{Y}w(1,q)$. By the intermediate value property, there is an a_q such that ${}^{Y}w(a_q) = {}^{N}w(a_q)$. If Questioner, when there are q questions left, asks $x<a_q$?, then $w(q-1,{}^{Y}A_{q-1}) = w(q-1,{}^{N}A_{q-1}) = \frac{w(q,A_q)}{2}$. Thus after Q questions we have:

$$w(0,A_0) = w(Q,A_Q)\cdot 2^{-Q} = \left(\binom{Q}{E}\right)\cdot 2^{-Q}.$$

Let $A = \bigcup_{e=E} A_0^e$. Then $x\in A$, and $\varepsilon \le \|A\| \le \sum_{e=0}^{E}\|A_0^e\| = w(0,A_0) = \left(\binom{Q}{E}\right)\cdot 2^{-Q}$. This completes the proof. ■

From Theorem 1, we obtain:

Corollary 1. *Let Q be the minimum number such that $\left(\binom{Q}{E}\right) \le \frac{1}{n}\cdot 2^{Q}$. Then $Q_{con}(n,E) \le Q$.*

Proof. If $\left(\binom{Q}{E}\right) \le \frac{1}{n}\cdot 2^{Q}$, then by Theorem 1, $\frac{1}{n} \ge \left(\binom{Q}{E}\right)\cdot 2^{-Q} \ge \epsilon(Q,E)$, and the claim follows from the definition of $\epsilon(Q,E)$. ■

We now consider the analogous problem for the discrete case. Now the search space is $\{1,\ldots,n\}$, but replacing k by $\frac{k}{n}$ we obtain an *isomorphic* problem in which all elements in the search space are in $[0,1]$. Thus we can apply the strategy for the continuous case. If E and Q are as in Corollary 1, with Q questions we are able to produce a set A with $\|A\| < \frac{1}{n}$ such that $x\in A$. In general, this may be not sufficient to guess the number. *E.g.*, A might be the union of very small disks $D_1,\ldots,D_n$ such that for $i=1,\ldots,n$, $\frac{i}{n}\in D_i$ and $\sum_{i=1}^{n}\|D_i\| \le \frac{1}{n}$. However, if A is connected, then since $\|A\| < \frac{1}{n}$, A cannot contain more than one element in $\{\frac{1}{n},\frac{2}{n},\ldots,1\}$, and we can guess the number. Hence it is sufficient to prove:

Theorem 2. *Let Q, E, etc. be as in Corollary 1, with $\epsilon = \frac{1}{n}$. Then with $Q+E$ questions we can obtain a state of knowledge such that the union A of its elements is connected. Since $\|A\| < \frac{1}{n}$, $Q+E$ questions are sufficient to guess the number.*

Corollary 2. *If $\left(\binom{Q}{E}\right) \le \frac{1}{n}\cdot 2^{Q}$, then $Q+E \ge Q_{disc}(n,E(n))$.*

In order to solve the problems $G^{*}_{p,M}([0,1],\frac{1}{n})$, $G^{*}_{p,M}\{1,\ldots,n\}$, we have to take into account that the number E of errors is not fixed, in fact it may depend on the number of questions. The main idea in the proof is to show a $\mathcal{O}(\log n)$ function $E(n)$ such that for sufficiently large n, both $Q_{con}(n,E(n))$ and $(Q_{disc}(n,E(n))$ do not exceed $\frac{E(n)}{p}$. If we are able to do this, then while asking $Q = Q_{con}(n,E(n))$ ($Q = Q_{disc}(n,E(n))$, respectively) questions, only $p\cdot Q \le E(n)$ errors can appear. Then if we apply the strategies used in Theorem 1 and 2, respectively, with $E = E(n)$, from the definition

of $Q = Q_{con}(n, E(n))$ ($Q = Q_{disc}(n, E(n))$, respectively), we obtain that $\frac{E(n)}{p}$ questions (hence $\mathcal{O}(\log n)$ questions) are sufficient to win both games.

We start from a numerical lemma, whose proof is left to the reader.

Lemma 3. *Let $E(n)$ be an arbitrary function such that $\lim_{n\to\infty} E(n) = +\infty$ and let $a > 2$. Then there exist positive constants c_1, c_2 and a constant $k > 1$ such that for sufficiently large n*

$$c_2 \cdot \frac{1}{E(n)} k^{E(n)} \leq \frac{2^{aE(n)}}{\left(\binom{aE(n)}{E(n)}\right)} \leq c_1 E(n) \cdot k^{E(n)}.$$

We are ready to prove the desired result about the games $G^*_{p,M}([0,1], \frac{1}{n})$ and $G^*_{p,M}\{1, \ldots, n\}$.

Theorem 3.

(A) *If $p < \frac{1}{2}$, Questioner can win the game $G^*_{p,M}([0,1], \frac{1}{n})$ for any M and n in time $\mathcal{O}(\log n)$.*

(B) *If $p < \frac{1}{3}$, Questioner can win the game $G^*_{p,M}\{1, \ldots, n\}$ for any M and n in time $\mathcal{O}(\log n)$.*

Proof. (A) As said before, it is sufficient to find an $\mathcal{O}(\log n)$ function $E(n)$ such that for sufficiently large n, the number $Q(n)$ of questions necessary to win the game $G^*_{p,M}([0,1], \frac{1}{n})$ satisfies:

$$(\star) \qquad p \cdot Q_{con}(n, E(n)) \leq E(n).$$

Let $E(n) = (2/\log k)(\log n)$, where k is as in Lemma 3. For large n and $a > 2$ we have (by Lemma 3):

$$\frac{2^{aE(n)}}{\left(\binom{aE(n)}{E(n)}\right)} \geq c_2 \frac{\log k}{2 \log n} k^{\frac{2 \log n}{\log k}} = \frac{c_2 \log k}{2} \cdot \frac{n^2}{\log n} \geq n.$$

Putting $a = 2/p$ we have $a > 2$, hence the above inequality gives:

$$2^{E(n)/p} \geq n \left(\binom{E(n)/p}{E(n)}\right).$$

Now let $Q = E(n)/p$. Then $2^Q \geq n \left(\binom{Q}{E(n)}\right)$, and, by Theorem 1, we obtain $Q_{con}(n, E(n)) \leq Q$, therefore $Q_{con}(n, E(n)) \leq E(n)/p$. Thus $E(n)$ satisfies our requirements. ∎

Proof. (B) Once again, it is enough to show an $\mathcal{O}(\log n)$ function $E(n)$ such that for sufficiently large n and $p < \frac{1}{3}$:

$$(\star\star) \qquad p \cdot Q_{disc}(n, E(n)) \leq E(n).$$

Putting $a = (1/p) - 1$, and $E(n) = (2/\log k)(\log n)$, we have $a > 2$. Then arguing as in the proof of (A), we obtain that for large n, $2^{aE(n)} \leq n \cdot \left(\binom{aE(n)}{E(n)}\right)$. Now let $Q' = aE(n)$, and let $Q = E(n)/p$. Then $2^{Q'} \leq n \cdot \left(\binom{Q'}{E(n)}\right)$. Moreover $Q' = (E(n)/p) - E(n) = Q - E(n)$, therefore by Corollary 2, $Q \geq Q_{con}(n, E(n)) + E(n) \geq Q_{disc}(N, E(n))$. Since $Q = E(n)/p$, we conclude that $Q_{disc}(n, E(n)) \leq E(n)/p$, and $(\star\star)$ is proved. ∎

Remark. In [16] the authors, deal with some variants of $G^*_{p,M}\{1,\ldots,n\}$. They consider three versions:

(A) Questioner presents his questions one at a time and Responder must answer them in such a way that at no point has he lied to more than a fraction p of them; namely, every initial segment of a of his answers must contain no more than pa lies.

(B) Questioner presents his questions one at a time, but Responder is required to make sure that at most pq of his q answers are lies.

(C) Responder must submit all his questions simultaneously to Responder, and he is permitted to look them over before choosing a set of at most pq of them to lie to.

Compared with the game $G^*_{p,M}\{1,\ldots,n\}$, the version (A) introduces one more restriction for Responder (hence it is more favorable to Questioner). Moreover, the rules of version (B) are less restrictive for Responder, and the version (C) is some kind of non-adaptive variant of the game. Thus versions (B) and (C) are more favorable to Responder.

The authors prove the following:

Theorem 4.

(A) *Questioner wins with* $\Theta(\log n)$ *questions if* $p<\frac{1}{2}$ *but Responder wins if* $p\geq\frac{1}{2}$.

(B) *Questioner wins with* $\Theta(\log n)$ *questions if* $p<\frac{1}{3}$ *but Responder wins if* $p\geq\frac{1}{3}$.

(C) *Questioner wins with* $\Theta(\log n)$ *questions if* $p<\frac{1}{4}$, *and Responder wins if* $p>\frac{1}{4}$. *Moreover, Quiestioner wins when* $p=\frac{1}{4}$, *but* $\Theta(n)$ *questions are required.*

Theorem 3 has been used by Pelc [5] in order to prove the following:

Theorem 5.

(A) *If* $p<\frac{1}{2}$, *Questioner can win the game* $G_{p,q}([0,1],\frac{1}{n})$ *for any* $q<1$ *and for any* n *in time* $\mathcal{O}(\log n)$.

(B) *If* $p<\frac{1}{3}$, *Questioner can win the game* $G_{p,q}\{1,\ldots,n\}$ *for any* $q<1$ *and for any* n *in time* $\mathcal{O}(\log n)$.

Proof. Let S_k be the number of errors in a series of k answers. Since each time Responder can lie with fixed probability p, S_k is a random variable with a binomial distribution, that is, $P(S_k=i)=\binom{k}{i}p^i(1-p)^{k-i}$. By Chebyshev's inequality (*cf.* [17]), for any $\varepsilon>0$ we have:

$$P\left(\left|\frac{S_k}{k}-p\right|\geq\varepsilon\right)\leq\frac{p(1-p)}{k\varepsilon^2}.$$

Let us consider first the continuous game $G_{p,q}([0,1],\frac{1}{n})$. Let $\varepsilon=(\frac{1}{2}-p)/2$, and let $\overline{p}=p+\varepsilon$. Then $\overline{p}<\frac{1}{2}$ and $|\frac{S_k}{k}-p|<\varepsilon$ implies $S_k\leq\overline{p}k$ which gives:

$$P(S_k\leq\overline{p}k)\geq P\left(\left|\frac{S_k}{k}-p\right|>\varepsilon\right)\geq 1-\frac{16p(1-p)}{k(1-2p)^2}=1-\frac{c}{k}$$

for $c=\frac{16p(1-p)}{(1-2p)^2}$. Thus for $k\geq\frac{c}{1-q}$, the probability of less than $k\overline{p}$ errors over k questions is greater than q. Now let $M=\frac{c}{1-q}$, and let $f(n)$ be an $\mathcal{O}(\log n)$ function

such that Questioner can win the game $G^*_{\overline{p},M}([0,1],\frac{1}{n})$ with $f(n)$ questions. Without loss of generality, we can assume that $f(n)\geq M$, therefore with probability $\geq q$, over $f(n)$ questions at most $\overline{p}f(n)$ can receive a wrong answer. If this happens, then by Theorem 3, Questioner can win the game $G^*_{\overline{p},M}([0,1],\frac{1}{n})$ with $f(n)$ questions, hence, using the same strategy, with probability $\geq q$, he wins the game $G_{p,q}([0,1],\frac{1}{n})$.

The case of the game $G_{p,q}\{1,\ldots,n\}$ is treated similarly: of course in this case we take $\varepsilon=(\frac{1}{3}-p)/2$, and we reduce the game to $G^*_{\overline{p},M}\{1,\ldots,n\}$ instead of $G^*_{\overline{p},M}([0,1],\frac{1}{n})$. The rest of the argument is quite parallel to that used in the case of $G_{p,q}([0,1],\frac{1}{n})$. ∎

Remark. If $\frac{1}{3}\leq p<\frac{1}{2}$, then Questioner has a winning greedy strategy even for the game $G_{p,q}\{1,\ldots,n\}$, but its cost is $\mathcal{O}(\log n^2)$. The greedy strategy is the following: in order to guess the number, we must know all of its bits. These bits are $m\leq\log n+1$. Now for each bit Questioner asks if it is 0, and he repeats each question until he knows the answer with reliability at least $q^{1/m}$. Thus Questioner knows all m bits with reliability at least $(q^{1/m})^m=q$, which means that he wins the games. Now we estimate the number of repetitions for each question. Let this number equal to $k=f(m)$. Let $\varepsilon>0$ be such that $p+\varepsilon<\frac{1}{2}$, and let $\overline{p}=p+\varepsilon$. It is enough to assure that:

$$P(S_k\leq\overline{p}k)\geq q^{1/m}\quad\text{for some}\quad\overline{p}<\frac{1}{2},$$

because the majority answer can be taken with sufficient reliability. Using Chebyshev's inequality with $c=\frac{p(1-p)}{\varepsilon^2}$, it is sufficient to satisfy:

$$(\bullet)\qquad\left(1-\frac{c}{f(m)}\right)^m\geq q$$

for sufficiently large m. Since for any constants c,r

$$\lim_{x\to\infty}\left(1-\frac{c}{rx}\right)^x=\frac{1}{e^{c/r}},$$

it follows that for sufficiently large fixed r we have $\lim_{x\to\infty}(1-c/(rx))^x>q$. Hence taking $f(m)=rm$ for this constant r we can satisfy $(\bullet)$. Thus it suffices to repeat every question $rm\leq r(\log n+1)$ times. Since Questioner needs the correct answer to $m\leq\log n+1$ questions and each one is repeated $rm\leq r(\log n+1)$ times, the above greedy searching algorithm can be carried out in time $\mathcal{O}(\log^2 n)$.

3. The Guessing Secrets game

As said in the introduction, there are variants of Rényi-Ulam game in which Questioner has to guess more than one number. One of these games is Group Testing. This game is suggested by a concrete problem: suppose that we have to find the defectives in a population of N individuals using blood testing. Then instead of testing every person individually, we can test the blood of, say, 100 people all together: if the test is positive, then we spoil one test, but if it is negative, we save 99 tests. The mathematical formalization of the game is the following: a large set Ω (to be though of as the population), known to Questioner and to Responder, is given. Then Questioner must guess a small subset S of Ω (the set of defectives), known only to Responder, on the ground of a number of questions of the form $X\cap S\neq\emptyset$? (to be

thought of as: *is there any defective in X?*), where $X \subseteq \Omega$. Responder must answer truthfully to each question. We do not treat this game here. For more information, the reader may consult [11].

Now we introduce another variant of Rényi-Ulam game, the *Guessing Secret game*. The game is as follows:

- a large set Ω of cardinality N, and a subset S of it of cardinality $n \ll N$, are given. Whilst Ω is known to both players, S is known only to Responder. (S is called *the secrets set* and its elements are called *the secrets*);
- Questioner may ask questions of the form: *Is your number in X?*, where $X \subseteq \Omega$;
- Responder has to answer truthfully, but he can refer to *any* of the elements of S.

Thus *e.g.* if $S = \{3,8\}$ and the question is: *Is your number less than* 12*?*, then the answer must be YES, but if the question is: *Is your number an even number?*, then the answer may be YES on behalf of 8 and NO on behalf of 3. The difference between Group Testing and Guessing Secrets is that in the first case Responder must answer YES if $X \cap S \neq \emptyset$ and NO otherwise, whereas in the second case Responder must answer YES if $S \subseteq X$, NO if $S \cap X = \emptyset$, but if both $X \cap S$ and $(\Omega \setminus X) \cap S$ are non-empty, then the answer may be indifferently YES or NO.

Responder has many adversary strategies which forbid Questioner to guess all of the secrets. Here are two of them:

(1) Responder may always answer on behalf of the same secret. In this way, Questioner has no information about the other secrets;

(2) Let $k \in \Omega \setminus S$ (we call such k *the intruder*). Then according to the rules of the game, Responder can answer YES to the question: *Is your number in X?* iff either X contains at least two secrets or X contains k and at least one secret. Note that if Responder answers YES according to this strategy, then X must contain at least one secret, so the answer YES is legal, on behalf of that secret. Moreover, if Responder answers NO according to the this strategy, then at least one secret is not in X, and Responder may answer NO on behalf of that secret. With this strategy, Questioner can not distinguish the intruder k from the true secrets: if any one of the secrets is replaced by k, Responder's answers remain the same. So he cannot guess any of the secrets.

For $n = 2$, the whole situation can be presented in terms of graph theory (*cf.* [12]): take Ω as the set of nodes, and the possible pairs of secrets as edges of the graph. At the beginning, all pairs are possible, so the situation is represented by the complete graph on N elements. If the question: *Is your number in X?* receives answer YES, then all edges joining two nodes both not in X can be dropped (they cannot constitute the secret set, otherwise the answer would have been NO). If the above question receives answer NO, then we may drop the edges joining nodes both in X. The best we may obtain is an *intersecting graph*, that is one such that any two edges have a node in common. Indeed, if $\{a,b\}$ and $\{c,d\}$ are two edges such that a,b,c,d are pairwise distinct, then by the question: *Is your number in* $\{a,b\}$*?*, we can exclude either $\{a,b\}$ (if the answer is NO) or $\{c,d\}$ (if the answer is YES). On the other hand, if a subgraph G of the complete graph on N nodes is intersecting, then either there is a node which

is common to all edges of G, or G is the complete graph over three elements. In the first case, let a be the node common to all edges. If Responder always answers on behalf of a (according to the adversary strategy (1)), then Questioner cannot learn more about the secrets, *i.e.*, he cannot simplify G. Similarly, if G is the complete graph with 3 nodes, then two of them, say a and b are the secrets, and the third one, say k, is not. Then if Responder plays the strategy (2) with intruder k, Questioner learn more about the secrets, *i.e.*, he cannot simplify G.

An interesting variant of the Guessing Secrets game is *Probabilistic Guessing Secrets*. The only difference with the previous game is that each time Responder chooses his secret at random with uniform distribution, and answers on behalf of that secret. In [18], the authors develop a guessing algorithm, and compute the mean value and the variance of the number of questions necessary to learn all of the secrets (with probability 1, this occurs after finitely many questions).

We first describe a procedure for guessing one of the secrets. After such a secret (call it s) has been guessed, we leave it out of Ω (formally, we ask questions concerning sets X such that $s \notin X$) and we iterate the procedure until we guess all of the secrets.

Algorithm for guessing one of the secrets

At the beginning our search space Σ is Ω.

Questioner divides Σ in two parts Σ_L and Σ_R of the same cardinality, and asks:

QL *Is your number in* Σ_L*?*

QR *Is your number in* Σ_R*?*

He repeats the questions until he gets answer YES.

Then Questioner updates the search space: if question QL receives answer YES, then $\Sigma = \Sigma_L$. If question QR receives answer YES, then $\Sigma = \Sigma_R$.

Questioner repeats the procedure until Σ consists of one element only, call it s. Then this element is a secret.

After a new secret s has been guessed, Questioner repeats the procedure starting from $\Sigma = \Omega \setminus \{s\}$. More generally, after guessing h secrets $s_1, \ldots, s_h$, Questioner restarts the procedure from $\Sigma = \Omega \setminus \{s_1, \ldots, s_h\}$ until he guesses all of the secrets.

The number of questions needed to learn all of the secrets using the above algorithm is a random variable which depends on the secret chosen in each answer. For instance, if none of Σ_L and Σ_R contains all of the secrets, Responder may answer NO all the times, in which case the algorithm never ends. However, this occurs with probability 0. A superficial analysis of the algorithm is the following:

- the expected time of the number of questions needed for a YES answer is $\leq 2n$, where n is the number of secrets;
- after $\lceil \log(N) \rceil$ YES answers (where N is the cardinality of Ω) one more secret has been guessed. So the expected time needed to guess one secret is $\leq 2n \cdot log_2(N)$;
- finally, the expected time needed to guess all of the secrets is bounded by $2n^2 \cdot log_2(N)$.

The paper [18] contains a more careful analysis of the algorithm. There, the following is shown:

Theorem 6. *Suppose that $n \ll N$. Then the number of questions necessary to learn all the secrets is a Gaussian random variable whose expected value is given by $\frac{1}{\log_e(2)} n^2 \log_2(N)$.*

To conclude this section, we outline some possible lines of research about the Guessing Secrets game. The truly ingenious work by Rivest [2] and by Pelc [5] suggests the possibility of a similar approach for the Probabilistic Guessing Secrets problem. For example, it would be interesting to find a variant of the problem for the continuum, as in the case of probabilistic Ulam's game. Moreover, the analysis of Pelc and Rivest allows the authors to conclude that their algorithm is optimal. We would like to prove a similar result for the Probabilistic Guessing Secrets. Our guess is that one cannot improve the bound $\mathcal{O}(n^2 \log N)$. This problem looks very difficult, but we think that it should be possible to export to the case of Probabilistic Guessing Secrets many ideas (like the weight function, the non-probabilistic variants, *etc.*) used for the probabilistic Ulam game.

4. The Ulam game with lies and Łukasiewicz logic

Many-valued logics have been introduced in order to treat vagueness, but they can be used in the treatment of uncertainty in general. The main properties of many-valued logics are:

- many-valued logics are based on their semantics;
- truth values are not just 0 and 1, but more generally elements in $[0,1]$;
- connectives are truth-functional, that is, the truth value of a compound formula is uniquely determined by the truth value of its components;
- the basic connectives are conjunction & and implication $\rightarrow$. Moreover, if $\star$ is the interpretation of conjunction, then implication is interpreted as the residual of $\star$, namely by $x \Rightarrow y = \sup\{z : z \star x \leq y\}$;
- the interpretation $\star$ of & should be a commutative, associative, weakly increasing and continuous binary operation on $[0,1]$ such that $x \star 1 = x$ for every x. Such an operation is called *a continuous t-norm*.

The language of many-valued logic has propositional variables, parentheses, the propositional constant $\perp$ (falsum), and the binary connectives & and $\rightarrow$. Given a continuous t-norm $\star$ and a map e from propositional variables into $[0,1]$, we extend e to a map (still denoted by e by abuse of language and called *evaluation based on* $\star$) defined inductively on all formulas as follows:

$$e(\perp) = 0;$$
$$e(A\&B) = e(A) \star e(B);$$
$$e(A \rightarrow B) = e(A) \Rightarrow e(B) = \sup\{x : x \star e(A) \leq e(B)\}.$$

Given a continuous t-norm $\star$, its logic $L_\star$ is the set of formulas A such that $e(A) = 1$ for every evaluation e based on $\star$. The main continuous t-norms are:

- the Łukasiewicz t-norm $\star_L$, defined by $x \star_L y = \max\{x+y-1, 0\}$;
- the Gödel t-norm $\star_G$, defined by $x \star_G y = \min\{x, y\}$;
- the product t-norm $\star_\pi$, defined by $x \star_\pi y = x \cdot y$ (ordinary product).

The corresponding logics $L_{\star_L}$, $L_{\star_G}$ and $L_{\star_\pi}$ are called Łukasiewicz logic, Gödel logic and product logic, respectively. As observed in [19], Gödel logic was investigated by Gödel in order to prove that intuitionistic logic is not a finitely-valued logic. However, this logic was discussed even earlier by Dummett, *cf.* [20].

All these logics have an Hilbert-style finite axiomatization (*cf.* [19]). Let $\Rightarrow_L$, $\Rightarrow_G$ and $\Rightarrow_\pi$ be the interpretations of $\rightarrow$ in Łukasiewicz logic, in Gödel logic and in product logic respectively. Then:

$$x \Rightarrow_L y = \min\{1-x+y, 1\}; \quad x \Rightarrow_G y = \begin{cases} 1 & \text{if } x \leq y, \\ y & \text{otherwise;} \end{cases} \quad x \Rightarrow_\pi y = \begin{cases} 1 & \text{if } x \leq y, \\ \frac{y}{x} & \text{otherwise.} \end{cases}$$

Negation is defined in terms of implication by $\neg A = A \rightarrow \bot$. It is easily seen that the interpretations $\sim_L$, $\sim_G$ and $\sim_\pi$ of $\neg$ in Łukasiewicz logic, in Gödel logic and in product logic are respectively:

$$\sim x = 1 - x; \quad \sim_G x = \sim_\pi x = \begin{cases} 1 & \text{if } x = 0, \\ 0 & \text{otherwise.} \end{cases}$$

Moreover, $\Rightarrow_L$ can be defined in terms of $\star_L$ and $\sim_L$ by $x \Rightarrow_L y = \sim_L (x \star_L \sim_L y)$. Thus in Łukasiewicz logic one can take conjunction and negation as basic connectives.

A fundamental property of Rényi-Ulam game with lies, discovered by Mundici (*cf.* [13]), is that it constitutes a semantics for Łukasiewicz logic. In order to explain why it is so, let us start from the Ulam game without lies. Let $X = \{1, \ldots, n\}$ be the search space. In absence of questions, any of $1, \ldots, n$ might be the unknown number, so each of $1, \ldots, n$ has possibility degree 1 (there is no reason to exclude it). Now consider a question q_Z of the form: *is the unknown number in Z?*, with $Z \subseteq X$. If the answer a_Z is YES, then all elements in $X \setminus Z$ are excluded (*i.e.*, they get possibility degree 0), whereas the possibility degree of the elements of Z remains 1. The situation is the opposite if the answer is NO. The function which expresses, for every $x \in X$, its possibility degree based on the question q_Z and the answer a_Z is called *state of knowledge* corresponding to q_Z and a_Z and is denoted by $K^{a_Z}_{q_Z}(x)$. Now consider a finite number of questions $q_1 = q_{Z_1}, \ldots, q_n = q_{Z_n}$ and the corresponding answers $a_1, \ldots, a_n$, with $a_i \in \{\text{YES}, \text{NO}\}$. After these questions and answers, we can exclude all numbers which are excluded by *at least* one answer. Thus letting $K_i(x) = K^{a_i}_{q_i}(x)$, the possibility degree of x is 0 if at least one of the $K_i(x)$ is 0, and it is 1 otherwise. Now let Q be the sequence $(q_1, \ldots, q_n)$ of questions, and A be the sequence $(a_1, \ldots, a_n)$ of the corresponding answers. The *state of knowledge* K^A_Q corresponding to the sequences Q and A, *i.e.* the function which expresses, for every $x \in X$, the possibility degree of x after the questions Q and the corresponding answers A is given by $K^A_Q(x) = \min\{K^{a_i}_{q_i}(x) : i = 1, \ldots, n\}$. More generally, given two states of knowledge $K^A_Q(x)$ and $K^{A'}_{Q'}(x)$, we can consider their *conjunction*, *i.e.*, the state of knowledge we obtain by taking as sequence of questions the juxtaposition $Q \circ Q'$ of the sequences Q and Q' and as sequence of answers the juxtaposition $A \circ A'$ of A and A'. Clearly on the ground of $Q \circ Q'$ and of $A \circ A'$ we can exclude both the numbers

which are excluded by Q and A and the numbers which are excluded by Q' and A'. Thus $K^{A\circ A'}_{Q\circ Q'}(x) = \min\{K^A_Q(x), K^{A'}_{Q'}(x)\}$. In other words, the conjunction of states of knowledge is interpreted as the minimum, as in classical logic. This suggests the possibility of analyzing the whole game inside classical logic. As a matter of fact, the analysis of the states of knowledge, which can be treated inside classical logic, gives us a complete description of the situation: in particular, after a sequence Q of questions and the corresponding sequence A of answers, we can guess the number iff $K^A_Q(x) = 0$ for all the elements of X except from one. It is possible to carry this analogy further, showing that not only the Ulam game without lies can be treated inside classical logic, but conversely it constitutes a semantics for such logic. We do not present the argument now, because it can be regarded as an instance of the relationship between the Ulam game with lies and Łukasiewicz logic, which is treated here below.

Now let us turn to the Ulam game with lies. Suppose that Responder can lie k times at most. As in the previous case, we want to represent the possibility degree of every $x \in X$ after a sequence of questions and the corresponding sequence of answers. Once again, the function expressing for every x its possibility degree will be called *state of knowledge*. At the beginning, every $x \in X$ has possibility degree 1. Now consider a question q_Z of the form: *is the unknown number in Z?*. If the answer is YES, then of course the possibility degree of the elements of Z remains 1, but we cannot exclude the elements of $X \setminus Z$, because the answer might be wrong. However, the answer still gives us some information: if the answer is wrong, then Responder spent one of his k lies, and in the sequel he may lie $k-1$ times at most. Thus we cannot exclude the elements of $X \setminus Z$, but at the same time we have to differentiate them from the elements of Z. The idea is to give to such elements an intermediate possibility value. The choice of this value is suggested by the following observation: if we ask $k+1$ times: *is the unknown number in Z?* and we get $k+1$ YES answers, then we may completely exclude the elements of $X \setminus Z$ (because the assumption that the unknown number is in $X \setminus Z$ would imply $k+1$ lies). Summing-up, at the beginning the possibility degree of any $x \in X \setminus Z$ is 1, and after $k+1$ questions: *is the unknown number in Z?* and $k+1$ YES answers, such value is 0. Thus after one question: *is the unknown number in Z?* and one YES answer, it is natural to give the elements of $X \setminus Z$ value $1 - \frac{1}{k+1} = \frac{k}{k+1}$. Needless to say, if the answer to the previous question was NO, then the natural choice is to give the elements of $X \setminus Z$ the value 1 and to the elements of Z the value $\frac{n}{n+1}$. In order to simplify our treatment, let us say that $x \in X$ is *violated* by the question q: *is the unknown number in Z?* and by the answer $a \in \{\text{YES}, \text{NO}\}$ if either $x \in Z$ and $a = \text{NO}$, or $x \in X \setminus Z$ and the answer is YES. Let us denote the set of elements which are violated by q and a by V^a_q. Then our *state of knowledge* after the question q and the answer a can be represented by the function K^a_q defined by:

$$K^a_q(x) = \begin{cases} \frac{k}{k+1} & \text{if } x \in V^a_q, \\ 1 & \text{otherwise.} \end{cases}$$

We now consider the situation after a sequence Q of n questions $q_1, \ldots, q_n$ and the sequence A of the corresponding answers $a_1, \ldots, a_n$. Let for every $x \in X$, $v^A_Q(x)$ denote the number of questions-answers which violate x. Then clearly we can exclude the elements x with $v^A_Q(x) > k$, because the assumption that x is the unknown number

would imply more than k lies. Moreover, it is natural to give to every x with $v_Q^A(x)=0$ possibility degree 1. In other words, the possibility degree of x decreases from 1 to 0 when $v_Q^A(x)$ increases from 0 to $k+1$. Thus it is natural to define the possibility degree of x as $\max\{1-\frac{v_Q^A(x)}{k+1},0\}$. The whole situation is represented by the state of knowledge K_Q^A, *i.e.* the function which associates to every $x\in X$ its possibility degree. According to the observations just made we have $K_Q^A(x)=\max\{1-\frac{v_Q^A(x)}{k+1},0\}$.

As in the case of Ulam game without lies, we now consider the *conjunction* of two states K_Q^A and $K_{A'}^{Q'}$, that is, the state $K_{Q\circ Q'}^{A\circ A'}$. One moment's reflection shows that for all $x\in X$, $v_{Q\circ Q'}^{A\circ A'}(x)=v_Q^A(x)+v_{Q'}^{A'}(x)$, therefore by an easy computation we get:

$$K_{Q\circ Q'}^{A\circ A'}(x)=\max\{1-\frac{v_Q^A(x)+v_{Q'}^{A'}(x)}{k},0\}=\max\{K_Q^A(x)+K_{A'}^{Q'}(x)-1,0\}.$$

This shows that in this case the conjunction of two states of knowledge is not represented by classical conjunction, but instead by Łukasiewicz conjunction. Thus the right logic in which the Ulam game with lies can be analyzed is Łukasiewicz logic. More precisely, if the number k of lies is known, then the right logic is Łukasiewicz logic with truth values $\{0,\frac{1}{k+1},\ldots,\frac{k}{k+1},1\}$, otherwise it is full Łukasiewicz logic.

It can be proved that not only we can represent the Ulam game with lies inside Łukasiewicz logic, but viceversa we can represent Łukasiewicz logic by means of Rényi-Ulam game with lies, associating to every sentence a state of knowledge. To do this, we first introduce the *impossible state* in which every element has possibility degree 0. Whilst the constantly one state (also called *the initial state*) corresponds to absence of knowledge, the impossible state correspond to an inconsistent knowledge.

We can introduce an order between states, defining $K\le K'$ iff for every $x\in X$, $K(x)\le K'(x)$. Thus $K\le K'$ if K contains *more* information than K'. With respect to this order, the *complement* $\overline{K_Q^A}$ of a state K_Q^A is defined to be the maximal state K such that the conjunction of K and K_Q^A is the impossible state. In terms of information, $\overline{K_Q^A}$ represents the minimal information which is incompatible with the information represented by K_Q^A.

Now let us express all formulas of Łukasiewicz logic in terms of negation and &, (thus writing $\neg(A\,\&\neg B)$ for $A\to B$). Define a *n-k-evaluation* to be a function e_n^k mapping formulas of Łukasiewicz logic into states of knowledge in the Ulam game with search space X of cardinality n and k lies such that, $e_n^k(\bot)$ is the impossible state, and for any two formulas A and B, $e_n^k(A\&B)$ is the conjunction of the states $e_n^k(A)$ and $e_n^k(B)$, and $e_n^k(\neg A)$ is the complement of $e_n^k(A)$. Then we have:

Theorem 7. (*cf.* [13]) *For every formula A, one has: A is a theorem of Łukasiewicz logic iff for any two positive integers n and k and for every n-k-evaluation e_n^k, $e_n^k(A)$ is the initial state, i.e., the constantly one function.*

On the light of this beautiful result, one may ask if some other game can be analyzed inside many-valued logic. More than this, one would like to associate to each game a many-valued logic of which the game constitutes a complete semantics. Even if our attempts have been unsuccessful, in the next sections we will describe some steps in this direction.

5. Many-valued logic and probability

In this section we will discuss Hájek's proposal to treat probability inside many-valued logic [19, 21]. It will turn-out that Hájek ideas allow for a logical treatment of probabilistic games.

In principle, many-valued logic and probability logic are very different: the first one is the logic of vagueness, whereas the second one is the logic of uncertainty. For instance, a sentence like: *there is much traffic in the highway*, is vague, and its truth can be measured by an intermediate number, even if we know exactly how many cars are there. So such a sentence belongs to many-valued logic. To the contrary, the sentence: *the democratic party will win the next elections in USA*, is uncertain, but it will become true or false after the elections. The intermediate values are needed to measure the degree of belief, and not the degree of truth. Nevertheless, it is possible to treat probability by means of many-valued logic, using a modality P, to be interpreted as *it is probable that*. In this context, the probability of A becomes the truth value of the sentence $P(A)$: *it is probable that* A. In [19], Hájek introduces a system called $FP(RPL)$ in order to treat simple probability. Then in [22] the authors introduce an extension $FP(\text{Ł}\Pi\frac{1}{2})$ of $FP(RPL)$, in which it is possible also to treat conditional probability (there, the authors assume that the conditioning event has positive probability, but it is possible to extend the system in order to avoid this restriction, *cf.* [21]).

The language of $FP(\text{Ł}\Pi\frac{1}{2})$ contains propositional variables, Łukasiewicz conjunction $\&_L$, Łukasiewicz implication $\rightarrow_L$, product conjunction $\&_\pi$, product implication $\rightarrow_\pi$, the constants $\bot$ and $\frac{1}{2}$, and the modal operator P. Formulas split in two classes, the Boolean formulas, i.e, formulas without occurrence of the operator P and of $\frac{1}{2}$, and modal formulas which are built from $\frac{1}{2}$, and formulas of the form $P(A)$, A a modal formula, closing under the connectives $\&_L$, $\rightarrow_L$, $\&_\pi$ and $\rightarrow_\pi$. An evaluation e of Boolean formulas maps propositional variables into subsets of a ground set X. Then e can be extended to an evaluation (which we still call e, by abuse of language) over all Boolean formulas as follows:

$$e(\bot) = \emptyset;$$
$$e(A \&_L B) = e(A \&_\pi B) = e(A) \cap e(B);$$
$$e(A \rightarrow_L B) = e(A \rightarrow_\pi B) = (X \setminus e(A)) \cup e(B).$$

When dealing with Boolean formulas, the connectives $\&_L$ and $\&_\pi$, as well as $\rightarrow_L$ and $\rightarrow_\pi$, are interpreted in the same way (classical conjunction and classical implication respectively), so in this context we will simply write $\&$ and $\rightarrow$. We will see in a moment that the interpretations of $\&_L$ and $\&_\pi$, as well as the interpretations of $\rightarrow_L$ and $\rightarrow_\pi$ differ when dealing with modal formulas.

In order to extend e to modal formulas, we need a measure μ on the powerset of X. Then e is extended as follows:

$$e(\tfrac{1}{2}) = \tfrac{1}{2};$$
If A is any Boolean formula, then $e(P(A)) = \mu(e(A))$;
$$e(C \&_L D) = e(C) \star_L e(D);$$
$$e(C \&_\pi D) = e(C) \star_\pi e(D);$$

$e(C \to_L D) = e(C) \Rightarrow_L e(D)$;
$e(C \to_\pi D) = e(C) \Rightarrow_\pi e(D)$.

Note that if C is a modal formula, then $e(C)$ is a real number, whereas if A is a Boolean formula, then $e(A)$ is a subset of X. To avoid this asymmetry, let us define, for every evaluation e, a function $v_e(x, A)$ ($x \in X$, A a formula) as follows:

If A is a Boolean formula, then $v_e(x, A) = 1$ if $x \in e(A)$, and $v_e(x, A) = 0$ otherwise.

If A is a modal formula, then $v_e(x, A) = e(A)$.

In this way, the truth value of a formula is always a real number in $[0,1]$, therefore we can also define the truth value of mixed formulas like $A\&_L B$ were A is Boolean and B is modal.

Definition 1. The logic $FP(\text{Ł}\Pi\frac{1}{2})$ is defined to be the set of formulas A such that for every choice of X, μ and e, and for every $x \in X$, one has $v_e(x, A) = 1$.

It is important to observe that $FP(\text{Ł}\Pi\frac{1}{2})$ has a Hilbert-style axiomatization (*cf.* [22]). Thus in principle it is possible to reason about probability inside a system of *propositional* logic. Another important remark is the following: the conditional probability of A given B (A and B Boolean formulas) can be expressed as $P(A \mid B) \stackrel{\text{def}}{=} P(B) \to_\pi P(A\&B)$. Indeed, for every evaluation e such that $e(P(B)) \neq 0$, one has:

$$e(P(B) \to_\pi P(A\&B)) = e(P(B)) \Rightarrow_\pi e(P(A\&B)) = \frac{e(P(A\&B))}{e(P(B))}.$$

If we interpret the probability of any event C as $e(P(C))$, then $\frac{e(P(A\&B))}{e(P(B))}$ is precisely the conditional probability of A given B.

6. Towards a logical interpretation of the probabilistic variants of Rényi-Ulam game

In order to deal with the probabilistic games described above inside many-valued logic, one may add to $FP(\text{Ł}\Pi\frac{1}{2})$ some propositional constants, representing the data of the game (like *e.g.* questions-answers) and the axioms governing their probabilities. For instance, in the case of probabilistic Ulam game, we need:

- constants L_i, whose meaning is *the unknown number is less than i*;
- constants Y_{ik} whose meaning is: *The k^{th} question: "is the unknown number less than i?" has been answered affirmatively.*

Then we need axioms reflecting the rules of the game. First note that every rational number $r \in [0,1]$ can be represented as a sentence using $\frac{1}{2}$, $\bot$, $\&_L$, $\to_L$, $\&_\pi$ and $\to_\pi$. That is, for every rational $r \in [0,1]$, there is a sentence $\overline{r}$ such that for every evaluation e one has $e(\overline{r}) = r$ (*cf.* [23]). Thus, if the probability p of an error is a rational number, then we can express the fact that Responder can lie with probability p by the axioms:

$L_i \to_L (P(Y_{ik}) \leftrightarrow_L \neg_L \overline{p})$, and
$\neg L_i \to_L (P(Y_{ik}) \leftrightarrow_L \overline{p})$

where $\neg_L C$ and $C \leftrightarrow_L D$ stand for $C \rightarrow_L \bot$ and $(C \rightarrow_L D)\&_L(D \rightarrow_L C)$, respectively. Of course, we need other axioms, for instance the axioms saying that for different $k_1,\ldots,k_h$ and for $i \leq n$, the events $Y_{ik_1},\ldots,Y_{ik_h}$ are independent, or that the probability of L_i is $\frac{i-1}{n}$, *etc.* However, it is not too hard to write down axioms which describe the situation completely. Assuming that the confidence parameter q is a rational number, then we can check if some sequence of answers $A_{i_1 1},\ldots A_{i_h h}$, where $A_{i_j j}$ is either $Y_{i_j j}$ (which means that the question: *is the unknown number less that* i_j*?* has been answered affirmatively) or $\neg_L Y_{i_j j}$ (which means that the question *is the unknown number less that* i_j*?* has been answered negatively), is sufficient to detect the unknown number with probability at least q. Indeed, let A be the conjunction of all formulas $A_{i_j j}$. Then we can say that with probability at least q the unknown number is m iff in our system we are able to derive the formula:

$$\overline{q} \rightarrow_L P((L_{m+1}\&\neg_L Lm) \,|\, A),$$

where as usual $P(C \,|\, D)$ is an abbreviation for $P(D) \rightarrow_\pi P(C\&D)$.

As we said in the introduction, the possibility of translating the learning algorithm inside a logical system has some theoretical interest, but has no practical use: the logical formalization is by far harder than the algorithm itself. More than this, we can describe the algorithm inside a logic, but this does not give a semantics for the logic itself.

7. Towards a duality between logics and games

The problem of establishing a duality between logics and games in such a way that the game constitutes a semantics for the logic is a very interesting one. As far as we know, logicians tried to associate to interesting logics some *ad hoc* (hence not interesting in themselves) games, thus giving priority to logics. The link between Łukasiewicz logic and Rényi-Ulam game with lies is an example where an interesting logic is related to an interesting game. We would like to find other examples of connections of this kind.

In this section we outline some general ideas in order to reach this goal. To any of the games illustrated above, we can associate a collection of states of knowledge, representing each the situation of the game after a sequence of questions-answers. The set of states can be partially ordered letting $K \leq K'$ iff the state K is more informative than the state K'. Moreover we can always define the *conjunction* of two states: if K and K' correspond to a sequence Q (Q', respectively) of questions and to a sequence A (A', respectively) of answers, then the conjunction of K and K' should be the state representing the sequence $Q \circ Q'$ of questions and the sequence $A \circ A'$ of answers. This gives an interpretation of conjunction &. The interpretation of implication should be the following: $K \Rightarrow K'$ is the greatest (*i.e.*, the less informative) state S such that the conjunction of S and K is $\leq K'$ (*i.e.*, more informative than K'). Of course, we need to prove that such a greatest state S always exists.

Now we have to look for the appropriate states of knowledge for each game. For instance, in the case of the (non probabilistic) Guessing Secrets game with two secrets, one may represent a state of knowledge as a subgraph of the complete graph with N nodes (the edges of this graph are those which have not been excluded by the

sequence of questions-answers). The intersection of two states of knowledge G_1 and G_2 is the graph with N nodes whose edges are those common to G_1 and G_2. Finally, the implication of two states of knowledge G_1 and G_2 is the graph with N nodes whose edges are those of G_2 plus those of the complement of G_1. Unfortunately, the underlying logic is classical logic. This might be expected, because the conjunction of states is clearly an idempotent operation (*i.e.*, the conjunction of a state K with itself is K), like in classical logic.

The situation of probabilistic Ulam game is more interesting. Along the line of the semantics of Rényi-Ulam game with lies, one is tempted to represent the state of knowledge corresponding to a sequence Q of questions and a sequence A of answers by the function K_Q^A defined, for all $x \in X$, by $K_Q^A(x) = p^h(1-p)^{n-h}$, where n is the total number of questions, and h is the number of questions which violate x. Note that a state of knowledge K allows us to compute for every x, the probability that x is the unknown number given the sequence of questions and the sequence of answers it represents. Indeed, let $R(Q,A)$ denote the event *the sequence of Responder's answers to the sequence of questions Q is A*, and let for all $x \in X$, N_x denote the event *the unknown number is x*. Then $K_Q^A(x)$ as defined above denotes the conditional probability $P(R(Q,A) \mid N_x)$. What we need for a complete representation of the situation is the reverse probability, that is the function $P(N_x \mid R(Q,A))$, which expresses, for every $x \in X$, the probability that the unknown number is x given that the sequence of Responder answers to the sequence of questions Q is A. This probability can be computed by the Bayes formula:

$$(\diamond) \qquad P(N_x \mid R(Q,A)) = \frac{P(R(Q,A) \mid N_x) \cdot P(N_x)}{P(R(Q,A))}.$$

Now $P(N_x) = \frac{1}{n}$, where n is the cardinality of the search space X. As regards to $P(R(Q,A))$, one has:

$$P(R(Q,A)) = \sum_{x \in X} P(N_x) \cdot P(R(Q,A) \mid N_x) = \sum_{x \in X} \frac{1}{n} \cdot K_Q^A(x).$$

Thus the states of knowledge defined in this way contain enough information about Questioner's knowledge.

With this definition, the conjunction of two states K and K' becomes their product, *i.e.*, the function $K \star K'$ defined for every $x \in X$, by $K \star K'(x) = K(x)K'(x)$. This may suggest that the corresponding logic is product logic. However, the role of product implication is not completely clear. For instance, if $K(x) = p$ and $K'(x) = 1-p$, then the product implication $K'(x) \Rightarrow_\pi K(x)$ is equal to $\frac{p}{1-p}$, a number which in general is not a product of factors equal to p or to $1-p$. Thus $K'(x) \Rightarrow_\pi K(x)$ is not a state of knowledge which may occur in the game.

Our plan for future research is to investigate a slight variant of probabilistic Ulam-Rényi game in order to obtain an appropriate game semantics for product logic.

Acknowledgements

We wish to thank the anonymous referee for improving the presentation and the bibliography of the present paper.

References

[1] Rényi A 1976 *Napló az információelméletről*, Gondolat, Budapest; English translation: 1984 *A Diary on Information Theory*, J. Wiley and Sons, New York

[2] Rivest R L, Meyer A R, Kleitman D J, Winklmann K and Spencer J 1980 *J. Comput. System Sci.* **20** 396

[3] Deppe C 2004 *Coding with Feedback and Searching with Lies*, Bolyai Soc. Studies, Springer

[4] Pelc A 2002 *Theoretical Computer Science* **270** 71

[5] Pelc A 1989 *Theoretical Computer Science* **63** 185

[6] Cicalese F, Mundici D and Vaccaro U 2002 *Rota-Metropolis Cubic Logic and Ulam-Renyi Games*, in: *Algebraic Combinatorics and Computer Science: in Memoriam Gian-Carlo Rota*, Springer, pp. 197–244

[7] Hill R 1995 *Searching with Lies, Surveys in Combinatorics*, Cambridge University Press, pp. 41–70

[8] Peterson W W and Weldon E J Jr 1972 *Error-Correcting Codes*, 2nd Edition, MIT Press, Cambridge, Mass

[9] Cicalese F and Mundici D 2000 *Optimal Coding with One Asymmetric Error: Below the Sphere Packing Bound*, COCOON, pp. 159–169

[10] Cicalese F, Mundici D and Vaccaro U 2002 *Theoretical Computer Science* **270** (1-2) 877

[11] Du D Z and Hwang F K 2000 *Combinatorial Group Testing and Its Applications*, World Scientific Pub Co.

[12] Chung F, Graham R and Leighton T 2001 *The Electronic Journal of Combinatorics* **8** ♯R13

[13] Mundici D 1991 *Proc. Int. Congress of the Italian Society for Logic and Philosophy of Science, SILFS*, vol. 2, CLUEB, Bologna, pp. 151–162

[14] Mundici D, Cignoli R and Ottaviano I M L D 2000 *Algebraic Foundations of Many-valued Reasoning*, Trends in Logic Series Studia Logica Library **7**, Kluwer, Dordrecht

[15] Berlekamp E R 1968 *Block Coding for the Binary Symmetric Channel with Noiseless, Delayless Feedback*, in: *Error-Correcting Codes*, Wiley, New York, pp. 61–85

[16] Spencer J and Winkler P 1992 *Combinatorics, Probability and Computing* **1** 81

[17] Durrett R 1991 *Probability: Theory and Examples*, Belmont, CA, Wadsworth

[18] Del Lungo A, Louchard G, Marini C and Montagna F 2005 *J. Algorithms* **55** 142

[19] Hájek P 1998 *Metamathematics of Fuzzy Logic*, Kluwer

[20] Dummett M 1959 *J. Symbo. Log.* **24** 96

[21] Flaminio T and Montagna F 2004 *Proc. of the 10th Int. Conf. IPMU*, Perugia, Italy, pp. 493–499

[22] Esteva F, Godo L and Hájek P, 2000 *Neural Network World* **5/00** 811

[23] Montagna F 2000 *J. of Logic, Language and Information* **9** 91