Probabilistic Distributions on Formal Objects

Sergei Soloviev, IRIT, Toulouse
(Novi Sad, 26.05.16)

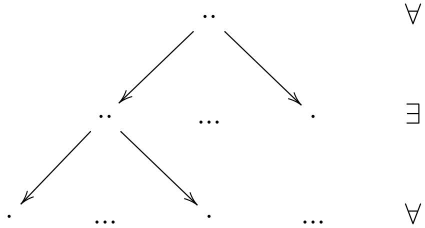
- When we try to define probability distributions on formal objects, it is seldom that we can find a *natural* one (e.g., due to some inherent symmetry).
- If there is no natural probability distribution, how can we expect to study probabilistic properties in an objective way?
- For example, wa may try to consider general properties, that hold for all distributions of a certain class.
- Or we may take into account supplementary information, like purposes of players in a game-theoretic setting.

- My presentation presents very much a work in progress, mostly on game-thereoretic approaches related to logics and formal methods.
- This explains mostly what are our motivations.
- Joint work in progress with participation of: Evgeny Dantsin (Chicago), Vladik Kreinovitch (El Paso), Eric Martin-Dorel and Jan-Georg Smaus (Toulouse)...

Games related to logics.

- Traditional setting: game semantics (but non-traditional point of view).
- Boolean games.
- Possible intersections with type theory.

- First we wanted to explore game semantics in unusual setting.
- Below is the beginning of a game tree for with prefix $\forall x \exists y \forall z$:
-



- Our question: what happens if computational power of players is not the same?
- What is to be understood as computational power?
- There is an obvious answer, but...

- It may take too much time to compute the values.
- Then it is natural to consider probabilistic distributions on x, y, z.... But then, what is a natural probabilistic distribution, say, on natural numbers?
- The problem of complexity may appear even in this case.

I will consider in more detail a concrete case that we studied in connection with so called Boolean games.

- It led us to some interesting questions, like the value of information with respect to winning.
- To express it briefly: consider the game where A wins if the strategy of B is known. But much less may be enough to win than the full information about the strategy of B.

- So before I speak about Boolean games I will tell something about algorithmic games we considered before.
- Before we considered *infinite* games where many of the results of the classical Game Theory do not hold.
- For example, games in extended form where moves of A and B are choices of natural numbers.
- Even if we consider an one-step game of this kind (pure strategy is just a natural number), it will lead to an infinite matrix, and classical *minimax* theorems, theorems about equilibrium in mixed strategies in general do not hold.
- The difference between *constructive* and *non-constructive* also becomes important (Rabin's results of the 50s, Jones results of the 80s).

- Here again the question: what is a “natural” probabilistic distribution on natural numbers arises.
- So we considered the games where the strategy of a player is a recursive function of (discrete) time and (maybe) previous moves.
- For simplicity, let us consider only *prf*.

- The game itself may be “matching game”:
- the players A and B simultaneusly produce two numbers n, n'; if $n = n'$ then A wins the round, else B wins; initially players may have some capital, the loser pays 1 to another player.
- If we put $n > n'$ instead of $n = n'$, we shall obtain a game that I already discussed at this conference, but it does not change much in case of algorithmic strategies.
- The case which interests me is when the capital of A is infinite and the capital of B finite,
- and A can compute some universal function for *prf* while B cannot change its strategy during the game.

- A can win as follows:
- (explanation)
- As it is well known, it is impossible to identify a *prf* using any finite number of its values (neither in the sense of its number nor extensionnally).
- Somewhat, to find the strategy of B the infinite information is needed, but finite information is sufficient to win.

Back to Boolean games

- Back to Boolean games.
- A Boolean game of two players is usually defined as follows.
- There is Boolean formula F of n variables.
- The player A controls k variables and the player B the remaining $n - k$.
- Each has to choose the values of variables (simultaneously or not is a separate question).
- The result of the game is defined by the value of F.

- There is a lot of literature (since 2000).
- By some reason in most of the publications only simultaneous choice of values (without knowledge of the opponent choices) was considered.
- We wanted to do some analysis of Boolean games in their totality based on probabilistic methods.
- That is, we want to consider random-generated F (pay-functions) and estimate the probability of various situations.
- For example: A has winning strategy; B has winning strategy; nobody has.

- More or les naturally, one may consider only DNF or CNF:
- identify F with the set of clauses (Boolean vectors).
- 2^n - set of Boolean vectors of the length n.
- 2^{2^n} - set of Boolean formulas.
- $\Omega = 2^{2^{2^n}}$ - the space of elementary events.
- We may denote $|F|$ the set of boolean vectors corresponding to F.

- Is there any natural probability law?
- There is at least a simple one: each vector belongs to $|F|$ with a fixed probability$p$.
- But there may be other candidates.
- With this simple law the probability of F represented by DNF with m clauses will be $p^m(1-p)^{2^n-m}$.

- Interesting (elementary) consequences.
- The probability of existence of a winning strategy for A

$$= 1 - (1 - p^{2^{n-k}})^{2^k} \quad .$$

- Similarly, for B

$$1 - (1 - q^{2^k})^{2^{n-k}} \quad .$$

- When k and $n - k$ are $\sim n$, $(n \to \infty)$, these probabilities tend to 0.
- The probability that both do not have winning strategies, respectively, tends to 1.

- How to interpret the case when there is no winning strategy neither for A nor for B?
- Order of moves matters!
- Indeed, since A does no have winning strategy, for every strategy of A there exists a strategy for B that B wins.
- So, if A moves first and B knows the moves then B can win.

- Slightly less elementary consequences (with the same probability law).
- What is the value of information w.r.t. winning?
- A knows s bits (choices) of B. How the probability that A has a winning strategy increases?
- It turns out that for small s (with respect to n, k and $n-k$) the probability grows as

$$\sim 2^{(k-1)2^s}$$

- At the moment we are looking, what of this interesting property remains if we consider more general probability laws?
- The question may be formulated like this.
- What properties should have a probability law on F, in other words, on the space

$$2^{2^{2^n}}$$

- to guarantee certain order of growth of the probability of existence of winning strategy?

Dependent types

- Another example that will illustrate another point.
- We may look for some probability law to satisfy some non-probabilistic motivation.
- And then our “subjective” interest may be justified.

1. At “Types” conference I spoke about automorphisms of types in various λ-calculi.
2. Isomorphisms of types are represented by terms that erase to a finite hereditary permutation.
3. Automorphisms are a subclass: the types must be the same, $f : A \to A$.
4. Interest: for example, cryptography (encoding without changing the code).

- In case of types in system *F* or dependent products any finite group may be represented as a group of automorphisms.
- The isomorphisms of a type, and the types isomorphic to it form a groupoid.
- In case of system *F* all isomorphisms may be defined as compositions of permutations (i) of quantified variables and (ii) premises of implication.
- Example.

$$\forall X \forall Y \forall Z.((X \to Y) \to (Y \to Z) \to (Z \to X) \to \forall U.U)$$

and

$$\forall Y \forall Z \forall X.((Y \to Z) \to (Z \to X) \to (X \to Y) \to \forall U.U)$$

- Notice that the types are α-equal, so this is an automorphism.

- What is the proportion of automorphisms among isomorphisms?
- We may use methods of Monte-Carlo.
- It depends, of course, on the type.
- The method of checking for an individual isomorphism (defined via permutations) is simple. The type may be translated into de Bruijn form. Then α-equal types are identical.
- We should define a random sequence of permutations and verify whether the result is an automorphism.

- Interest of random generation:
- generate quickly and automorphism;
- estimate the size of automorphism groups...

Conclusion.