Can Formalism Alone Provide an Answer to the Quest of a Viable Definition of Trust in the WWW Society?*

V. Liagkou[1,3], P. Spirakis[1,3], and Y.C. Stamatiou[2,3]

[1] University of Patras, Department of computer Engineering, 26500,
Rio, Patras, Greece
[2] Mathematics Department, 451 10, Ioannina, Greece
[3] Research and Academic Computer Technology Institute, N. Kazantzaki,
University of Patras, 26500, Rio, Patras, Greece
{liagkou,spirakis}@cti.gr, istamat@cc.uoi.gr

Abstract. Ever since the creation of the first human society, people have understood that the only way of sustaining and improving their societies is to rely on each other for exchanging services. This reliance have traditionally built on developing, among them, *trust*, a vague, intuitive to a large extend and hard to define concept that brought together people who worked towards the progress we all witness around us today. Today's society is, however, becoming increasingly massive, collective, and complex and includes not only people, but huge numbers of machines as well. Thus, trust, being already a difficult concept to define and measure when applied to a few people that form a cooperating group or a set of acquaintances, it is far more difficult to pinpoint when applied to large communities whose members may hardly know each other in person or to interconnected machines employed by these communities. In this paper we attempt to take a pragmatic position with regard to trust definition and measurement. We employ several formalisms, into each of which we define a reasonable notion of trust, and show that inherent weaknesses of these formalisms result in an inability to have a concrete and fully measurable trust concept. We then argue that trust in the modern intertwined WWW society must, necessarily, incorporate to some degree non-formalizable elements, such as common sense and intuition.

Keywords: Trust, formalism, logic.

1 Introduction

Although it is rather straightforward to say that I trust someone with whom I have been long together stating, also, the reason behind my belief (e.g. good previous collaboration, absence of hostile moves etc.), it seems very difficult to come to a

* This work has been partially supported by the ICT Programme of the European Union under contract number ICT-2008-215270 (FRONTS) and by the Open University of Cyprus within the Programme (DYSAT).

A.B. Sideridis and Ch. Z. Patrikakis (Eds.): e-Democracy 2009, LNICST 26, pp. 199–208, 2010.

conclusion as to whether to trust or not when I ``meet'' someone on the WWW or when I encounter a machine which I should use to meet my goals (e.g. a server to make an online transaction or a remote sensor that monitors a critical distant infrastructure). Although in a sufficiently large interconnection pattern like the WWW, all pairs of entities, people and machines, are only a few hops apart and, thus, massiveness of the WWW should not pose a trust problem in principle (e.g. If I do not know you, I most probably know someone else that knows you and may provide a well justified opinion of whether I should trust you or not), there are two major obstacles to the success of this approach: i) trust seems not to possess nice logical properties that aid formal deduction processes like, for instance, the transitivity property, and ii) decisions as to whether I should trust a human or a machine have to take place in an infinitesimal time instance (for instance, when an electronic transaction is pending and needs to be completed soon) and, thus, automation in trust manipulation is a highly desirable property of any formalization of the trust concept.

There is much ongoing research on the development and analysis of new trust management models for complex and dependable computer systems. Blaze *et al.* in [3] proposed the application of automated trust mechanisms in distributed systems. Josang [11] focus on the strong relationship between the notions of trust and security. Moreover a number of schemes for the design of secure information systems have been proposed (see, for example, [5, 10]) which are based on automated trust management protocols. The composition and propagation of trust information between elements of information systems is also of pivotal concern and a number of research works are devoted to them (see [21, 13, 23, 7]). Grandison and Sloman try to see the trust as a belief [17]. Based on a brief analysis they formulate the trust as *a firm belief in the competence of an entity to act dependably, securely and reliably within a specified context.* Moreover they establish the trust as a composition of several different attributes - such as reliability, dependability, honesty, truthfulness, security, competence, and timeliness - which may have to be considered depending on the environment in which trust is being specified. Here we take a different direction, we follow Dimitrakos' (see [15, 16]) definition of trust. We believe that *the trust of a party* A *in a party* B *is the measurable belief of* A *in* B *behaving dependably for a specified period within a specified context in relation to* X . Here we define the trust for a service X as a service requestor A to a service provider B for a service X . Thus, A and B are interlinked with a trust relationship, directed from A to B .

The goal of our paper is not, principally, to propose a certain formalism that allows to express and handle, algorithmically, trust. We rather have a look of several formal frameworks and explore their limitations with regard to their expressive and deductive power in defining and manipulating trust. The main principle behind this approach, is that that unpredictably dynamic, global societies encompassing huge number of elements (either people or machines) are not likely to be amenable to a static viewpoint of trust, no matter how this concept is formalized. The main reason behind this belief is exactly the dynamic nature and massiveness of the modern WWW society. We, thus, believe that trust should be a statistical, asymptotic concept to be studied as a complex relationship *emerging* in the limit as the target system of entities expands and evolves. Thus, our main goal is to study trust within formal frameworks and see how facets of it *emerge* when the involved entities, as well as the interrelationships among them, change in time in unpredictable ways. We present the limitations of these formal approach and discuss possible alternatives.

2 Random Graphs

As we discussed above, the departure point of our work is that dynamic, massive systems like the WWW society of people and machines, are not amenable to a static viewpoint of the trust concept, no matter how this concept is formalized. Thus, our main goal is to define trust as an emerging relationship among entities of the system, that ``appears" when a set of properties hold, asymptotically, almost certainly in random communication structures that model computing systems and the interaction between constituent devices. And one of the most well studied and most intuitively appealing formalism for studying *emergent properties* is the *graph*. This trust metric model can be used to evaluate trust assertions in a distributed information system. Generally, directed graphs can be used to represent and answer the following questions: A trusts B, A trusts C, B trusts D, C trusts D, when trust is assumed to be a binary, directed relationship. In order to evaluate trust between two or more entities, we can assign weights (or believe estimates) to the degree of trust given on the trust relationship. the trust as a numerical value, weighted edges can be introduced in the Strust graph model T. These weights can provide primary data for acquiring a trust value. As long as trust values are just complete definable (e.g. A trusts B and C, no trust statement is expressed to all the other entities), it is quite easy to represent a trust metric in a weighted directed graph and make suitable deductions using, for instance, belief propagation techniques or Bayesian reasoning.

However, things may get complicated if very large community graphs are involved, that evolve in an unpredictable way, such as the WWW society (see [2] for a thorough treatment of threshold phenomena in relation to random graph properties).

3 First and Second Order Logic and Relationships

3.1 First Order Language of Graphs

We are interested in discovering conditions under which a random graph model displays threshold behavior for certain properties that can also be relevant to trust or security issues. In this subsection we will be focused on properties expressible in the *first order language* of graphs. This language can be used to describe some useful (and naturally occurring in applications) properties of random graphs under a certain random graph model using elements of the first order logic.

The alphabet of the first order language of graphs consists of the following (see, e.g., [22]):

- Infinite number of variable symbols, e.g. $z, w, y \ldots$ which represent graph vertices.
- The binary relations ``==" (equality between graph vertices) and ``$:$" (adjacency of graph vertices) which can relate only variable symbols, e.g. ``$x : y$" means that the graph vertices represented by the variable symbols x, y are adjacent.

- Universal, $\exists$, and existential, $\forall$, quantifiers (applied only to *singletons* of variable symbols).
- The Boolean connectives used in propositional logic, i.e. $\vee, \wedge, \neg, \Rightarrow$.

An example of graph property expressible in the first order language of graphs is the existence of a triangle: $\exists x \exists y \exists w (x : y) \wedge (y : w) \wedge (w : x)$. Another property is that the diameter of the graph is at most 2 (can be easily written for any fixed value k instead of 2): $\forall x \forall y [x = y \vee x : y \vee \exists w (x : w \wedge w : y)]$. However, other equally important graph properties, like connectivity, cannot be expressed in this language.

We will now define the important *extension statement* in natural language, although it clearly can be written using the first order language of graphs (see [22] for the details):

Definition 1 (Extension statement $A_{s,t}$). *The extension statement $A_{s,t}$, for given values of s,t, states that for all distinct $x_1, x_2, \ldots, x_s$ and $y_1, y_2, \ldots, y_t$ there exists distinct z adjacent to all x_i s but no y_j.*

The importance of the extension statement $A_{s,t}$ lies in the following Theorem. When applied to the first order language of graphs.

Theorem 1. Let G to be a random graph with n nodes and $A_{s,t}$ to be an extension statement, then if $A_{s,t}$ for all s,t $\lim_{n\to\infty} Pr[G \; has \; A_{s,t}] = 1$, then for every statement A written in the first order language of graphs either $\lim_{n\to\infty} Pr[G \; has \; A] = 0$ or $\lim_{n\to\infty} Pr[G \; has \; A] = 1$.

The connection between threshold properties and first order logic was first noted by Fagin in the seminal paper [6].

3.2 Second Order Language of Graphs

Although the extension statement can be used in order to settle the existence of thresholds for all properties expressible in the first order language of graphs in any random graph model, things change dramatically when properties are considered that are expressed in the *second* order language of graphs. The second order language of graphs is defined exactly as the first order language (see Section 3.1) except that it allows quantification over subsets of graph vertices (predicates) instead of single vertices. An example of such a property follows (see, e.g., [12]).

Definition 2 (Separator). *Let $F = \{F_1, F_2, \ldots, F_m\}$ be a family of subsets of some set X. A separator for F is a pair (S,T) of disjoint subsets of X such that each member of F is disjoint from either S or from T. The size of the separator is* $\min(|S|,|T|)$

In the context of trust, this property may be interpreted as follows. Let us assume that $|F_i| = 2$, modeling an edge of a graph. Thus, the sets F_i model a graph's links between pairs of nodes. With this constraint, the separator property says that in a graph there exist two disjoint sets of nodes S and T such that any set of two adjacent (i.e. communicating) nodes is disjoint from either S or T. In other words, it is not possible to have one node belonging to one of the two disjoint sets S and T and the other node belonging to the other. This might mean that no two communicating nodes are authenticated by two different authentication bodies (the two disjoint sets of nodes). Thus, the two nodes can trust each other more since they are not authenticated by two disjoint (i.e. unrelated) authentication bodies. Each of the two disjoint sets may form, for instance, Certification Authority (CA) providing authentication services.

In order to cast the separator property into the language of graphs, we set X to be a set of vertices and the subsets F_i to be of cardinality 2 so as to represent graph edges. Then the separator property can be written in the framework of the second order language of graphs as follows

$$\exists S \exists T \forall x \forall y [\neg(Sx \wedge Tx) \wedge (Axy \rightarrow \neg(Sx \wedge Ty \vee Sy \wedge Tx)]. \tag{1}$$

Let us define another property:

Definition 3 (Trusted representatives). *A graph G has the trusted representatives property if there exists a set of vertices such that any vertex in the graph is an adjacent with at least one of these vertices.*

A formal definition using second order logic is the following

$$\exists S \forall x \exists y [Axy \wedge Sy]. \tag{2}$$

The extension statement, cannot, unfortunately, be used in order to examine whether (and under which conditions on the random graph model parameters) the separator property or the trusted representatives property is a threshold property since these properties cannot be written in the first order language of graphs.

However, in 1987 Kolaitis and Vardi initiated in [18] a research project in order to characterize fragments of the second order logic that display threshold behavior (i.e. they have a 0-1 law). The interested reader may consult the review paper [19] by the same authors. Without delving into the details, one of the important conclusions reached at by this project is that there are second order fragments that do not have a threshold behavior while other second order fragments do.

Let Σ_1^1 denote the existential second order logic (i.e. formulas contain only existential quantification over second order variables, that is sets). Let FO denote the first order logic formalism and L be any fragment of FO. Then a $\Sigma_1^1(L)$ sentence over a vocabulary R is an expression of the form $\exists S \phi(R, S)$, where S is a set of relation variables and $\phi(R, S)$ is a first order sentence on vocabulary (R, S). In general threshold behavior is not displayed by Σ_1^1 (see [19]). Thus, in order to discover fragments of Σ_1^1 that do have such a behavior, a restriction is imposed on the first order part (i.e. the sentence ϕ written in L) of the sentences considered. This restriction refers to the pattern of quantifiers that appear in the first order sentence ϕ. Some restricted first order logics that have been studied in connection to Σ_1^1 are the following:

1. The *Bernays-Schönfinkel class*, which is the set of all first order sentences with quantifier prefixes of the form $\exists^*\forall^*$ (that is, the existential quantifiers precede the universal quantifiers).
2. The *Ackermann class*, which is defined as the collection of first order sentences of the form $\exists^*\forall\exists^*$ (that is the quantification prefix contains only one universal quantifier.
3. The *Gödel class*, which is defined as the collection of first order sentences of the form $\exists^*\forall\forall\exists^*$ (that is, the prefix contains two consecutive universal quantifiers).

The separator property defined by (1) belongs to the second order fragment Σ_1^1(Gödel) since it contains (in the first order part) two consecutive universal quantifiers. On the other hand, the trusted representatives property defined by (2) belongs to the second order fragment $\Sigma_1^1(Ackermann)$ since it contains a single universal quantifier.

The trusted representatives property can be proved to be a threshold property since the second order logic fragment $\Sigma_1^1(Ackermann)$ has a threshold behavior in general (see [19]). This means that, asymptotically, it holds with either probability 0 or 1 depending on the random graph model parameters. On the other hand, the separator property is not guaranteed to be a threshold property since the Σ_1^1 (Gödel) second order logic fragment does not display a threshold behavior in general (see [19]).

Thus, sentences (properties) that can be written in fragments of second order logic that have a threshold behavior (e.g. $\Sigma_1^1(Ackermann)$) are threshold properties. However, some second order logic fragments allow the construction of sentences that have no limiting probability and, thus, are not 0/1 properties, limiting our ability to assert their long-term validity.

It should be stressed that we do not know (perhaps it is not possible to know) whether all possible trust-related properties can be cast either within the framework of first order logic or second order logic.

4 Probability Theory – Undecidable Probabilities

Theorem 2 [Trachtenbrot-Vaught Theorem [24]]. *There is no decision procedure that separates those first order statements S that hold for some finite graph from those S that hold for no finite graph.*

With regard to random graphs now which, as we show, in conjunction with the first and second order language of graphs, can be used to express, formally, complex relationships that can be related to trust, we have the following result (see [4]):

Theorem 3. *There is no decision procedure that separates those first order statements S that hold almost always for the random graph $G_{n,p}$ from those for which $\neg S$ holds almost always.*

This theorem is targeted to $G_{n,p}$ random graphs, with $p = n^{\alpha}$, α being a rational number between 0 and 1. In summary, for any first order statement A about a finite graph, a first order statement A^* is given that holds almost always in $G_{n,p}$, *if* A holds for some finite graph, while it never holds, if A holds for *no* finite graph. Now, if a formal procedure (algorithm) existed for deciding such statements for the $G_{n,p}$ model, then relationship between A and A^* would allow using the procedure to separate those first order statements A that hold for some finite graph from the statements that hold for no finite graph, contradicting the Trachtenbrot-Vaught Theorem.

More specifically, let us consider the following statement S: There is no isolated vertex in the graph, which can be written as $\forall y \exists z (y : z)$. Let S^* be the corresponding statement, for the random graph $G_{n,p}$ with $p = n^{-2/5}$ (see [4]): $\exists x_1 \exists x_2 \exists x_3 \exists x_4 [\forall y MEM(y; x_1, x_2, x_3, x_4) \Rightarrow \exists z MEM(z; x_1, x_2, x_3, x_4) \wedge ADJ(y, z)]$ with MEM and ADJ the following first order language predicates:

$$MEM(y; x_1, x_2, x_3, x_4) \Leftrightarrow \exists z[(z : x_1) \wedge (z : x_2) \wedge (z : x_3) \wedge (z : x_4) \wedge (z : y)]$$

$$\begin{aligned} ADJ(u, v) \Leftrightarrow & MEM(u; x_1, x_2, x_3, x_4) \wedge \\ & MEM(v; x_1, x_2, x_3, x_4) \wedge \exists t MEM(t; x_1, x_2, u, v). \end{aligned}$$

$$\lim_{n \to \infty} Pr[G_{n,p} \; has \; S^*] = \begin{cases} 0 \; if \;\; S \; holds \; for \; no \; finite \; graph, \\ 1 \; if \;\; S \; holds \; for \; some \; finite \; graph. \end{cases} \tag{3}$$

Then a decision procedure that could differentiate between statements that hold almost always in $G_{n,p}$ and the statements whose negation holds almost always, would provide a decision procedure to differentiate between those statements S that hold for *some* finite graph and those that hold for no finite graph, contradicting the Trachtenbrot-Vaught Theorem.

The morale of this discussion is that it may not even possible to mechanically analyze whether a given state of affairs (e.g. trust assertion) or its negative, within the world of discourse (WWW society), is expected to almost certainly appear. Thus, it may be the case that one may have to observe the target world for sufficiently much time in order to be able to make a safe prediction about the state of affairs that will finally prevail in the limit.

5 The Self-referential Nature of Trust

Finally, in this section, we discuss an important weakness that arises in any formalism, when it is sufficiently powerful to be able to ``talk about itself", i.e. to contain statements about its expressive and deductive power (i.e. derivable statements).

According to the famous incompleteness theorem of Gödel, any formal system powerful enough to encompass the Peano axioms, contains statements for which neither the statement or its negation can be proved using the axioms and deductive rules of the formal system. In other words, there are truths and valid statements that cannot be asserted, using the formalism and its derivation rules alone. Another expression of this ``self-reference" phenomenon, from the point of view of computability theory this time, was given by Alan Turing in 1936 who described a universal computation machine model. In his famous work *On computable numbers, with an application to the Entscheidungsproblem* Turing defined a mathematical model for a device that performs mechanical calculations, later named *Turing machine* after its inventor. This suprisingly minimal, yet maximally powerful, model consisted simply of a infinite tape divided into cells each holding a particular symbol (say 0 or 1), a tape head that can move about the tape reading or writing symbols and, most important, a finite control able to decide on the next thing to do based on the current machine state and the symbol currently under the tape head. The first success of this simple model of algorithmic computation came immediately: Turing proved that no Turing machine and, hence, no algorithm according to *Church's Thesis* exists to decide whether another Turing machine halts when it starts computing with a specified input putting an end to Hilbert's grand program of mechanizing mathematics. The proof, actually, is a computational version of the proof of Gödel, which was cast within the logic calculus formalism. (We would like to urge the interested reader to consult [8] for an excellent account of the developments that paved the way to the rich theories of Computation and Complexity and [9] for a most comprehensive presentation of Computation and Complexity theory as it stands today.)

We can modify the main argument of the two historic results by Gödel and Turing, so as to give a glimpse of the inherent limitations of formalisms with respect to trust definition and manipulation as follows. We recall, that for our purposes trust is a property, a predicate more precisely, that dictates that the involved entities are in a certain state with regard to each other, i.e. the predicate holds.

Let us assume that we have defined a set of trust axioms that we believe are applicable in the situation at hand. For instance, these axioms may include the fact that in our world of discourse trust has the transitivity property, i.e. from $T(x,y)$ and $T(y,z)$ we may deduce $T(x,z)$. We would like to be able to test whether the trust property holds among some other set of entities, by exploiting the axioms and the deduction mechanisms of our formalism. We may recursively enumerate the possible axioms (given trust assertions) of our world of discourse (assumed to be finite) into strings, $w1, w_2, \ldots$. We may also enumerate the possible deduction mechanisms (algorithms) that start from the axioms, apply a set of derivation rules, and then reach a decision with respect to whether a certain trust assertion among entities of our world of discourse is true or not. Then, using an argument similar to Turing's, we may show that no universal trust derivation process may exist that starts from a description of the world of discourse (axioms plus derivation rules) and decides whether a trust assertion follows or not.

6 Discussion

Trust has been one of the cornerstones of the success of modern society in building well-organized groups of people working towards their own wealth as well as that of theirs peers. This traditional notion of trust, however, has two basic characteristics: i) it is based on personal contact, and ii) frequently, it cannot be explained.

Today, it is impossible to have personal information about any entity (either human or a machine offering a service) of the huge and ever expanding WWW society, with which we may want to communicate or perform a transaction. Thus, we would like to rely on rules as well as automated deductive procedures as to whether we should trust an WWW entity or not.

In this paper we have reviewed a number of formalisms with respect to their expressive and deductive power when describing large combinatorial structures, where the structure consists of a number of entities as well as trust assertion among them. We saw that each of the formalisms has some weaknesses in handling trust in complex, large environments containing a huge number of entities that interact unpredictable (almost randomly). Our position is that these observations seem to hint that reliance on formalism alone is not the answer to the problem of defining and manipulating trust. Rather, WWW entities should better focus on including fast heuristics as well as approximations to reality (even accepting trust in some cases axiomatically, e.g. to avoid the incompleteness pitfalls of powerful formal deductive systems). Moreover, it seems that trust will rely, for some time (until we manage to define it alternatively) on what it relied traditionally for the past few centuries: personal experience, public guidance from organizations and governments, creation of awareness groups, and avoiding trusting a WWW entity whenever one is not totally sure about trusting it (educated decisions). Otherwise, formal trust may either be unattainable (e.g. incompleteness results about formalisms) or hard to verify (NP-completeness results from computational complexity).

References

1. Bars, J.-M.L.: Fragments of existential second-order logic without 0-1 laws. In: 13th IEEE Symp. on Logic in Computer Science, pp. 525–536 (1998)
2. Bollobás, B.: Random Graphs, 2nd edn. Cambridge University Press, Cambridge (2001)
3. Blaze, M., Feigenbaum, J., Lacy, J.: Decentralized trust management. In: IEEE Symposium on Security and Privacy, Oakland, CA, USA, pp. 164–173 (1996)
4. Dolan, P.: Undecidable statements and random graphs. Annals of Mathematics and Artificial Intelligence 6, 17–26 (1992)
5. Trachtenbrot, B.: Impossibility of an algorithm for the decision problem on finite classes. Doklady Akad. Nauk. S.S.R. 70, 569–572 (1950)

6. Eschenauer, L., Gligor, V., Baras, J.: On trust establishment in mobile ad-hoc networks. In: Security Protocols Workshop, Cambridge, UK, pp. 47–66 (2002)
7. Fagin, R.: Probabilities on finite models. Symbolic Logic 41, 50–58 (1976)
8. Guha, R., Kumar, R., Raghavan, P., Tomkins, A.: Propagation of trust and distrust. In: International Conference on World Wide Web, pp. 403–412 (2004)
9. van Heijenoort, J.: From Frege to Gödel: A Source Book in Mathematical Logic. Harvard University Press, Cambridge (1967)
10. Herken, R. (ed.): The Universal Turing Machine: A Half-Century Survey. Springer, Heidelberg (1995)
11. Hubaux, J.-P., Buttyan, L., Capkun, S.: The quest for security in mobile ad hoc networks. In: ACM International Symposium on Mobile ad-hoc networking and computing, pp. 146–155 (2001)
12. Josang, A.: The right type of trust for distributed systems. In: New Security Paradigms Workshop, pp. 119–131 (1996)
13. Jukna, S.: Extremal Combinatorics - with Applications in Computer Science. Springer, Heidelberg (2001)
14. Kamvar, S.D., Schlosser, M.T., Garcia-Molina, H.: The eigentrust algorithm for reputation management in p2p networks. In: International Conference on World Wide Web, pp. 640–651 (2003)
15. Cheeseman, P., Kanefsky, B., Taylor, W.M.: Where the really hard problems are. In: Proc. of the International Joint Conference on Artificial Intelligence, pp. 331–337 (1991)
16. Dimitrakos, T., Bicarregui, J.C.: Towards A Framework for Managing Trust in e-Services. In: Proceedings of the 4th International Conference on Electronic Commerce Research, ATSMA, IFIP (November 2001) ISBN 0-9716253-0-1
17. Dimitrakos, T.: System Models, e-Risk and e-Trust. Towards bridging the gap? In: Towards the E-Society: E-Business, E-Commerce, and E-Government (2001)
18. Grandison, T., Sloman, M.: A Survey of Trust in Internet Applications. In: IEEE Communications Surveys and Tutorials (2000)
19. Kolaitis, P., Vardi, M.: The decision problem for the probabilities of higher-order properties. In: 19th ACM Symp. on Theory of Computing, New York, pp. 425–435 (1987)
20. Kolaitis, P., Vardi, M.: 0-1 laws for fragments ofexistential second-order logic: A survey. In: Nielsen, M., Rovan, B. (eds.) MFCS 2000. LNCS, vol. 1893, pp. 84–98. Springer, Heidelberg (2000)
21. Nikoletseas, S., Raptopoulos, C., Spirakis, P.: The existence and efficient construction of large independent sets in general random intersection graphs. In: Díaz, J., Karhumäki, J., Lepistö, A., Sannella, D. (eds.) ICALP 2004. LNCS, vol. 3142, pp. 1029–1040. Springer, Heidelberg (2004)
22. Richardson, M., Agrawal, R., Domingos, P.: Trust management for the semantic web. In: International Semantic Web Conference, pp. 351–368 (2003)
23. Spencer, J.: The strange logic of Random Graphs. Springer, Heidelberg (2001)
24. Theodorakopoulos, G., Baras, J.S.: Trust evaluation in ad-hoc networks. In: ACM Workshop on Wireless security, pp. 1–10 (2004)
25. Trachtenbrot, B.: Impossibility of an algorithm for the decision problem on finite classes. Doklady Akad. Nauk. S.S.R. 70, 569–572 (1950)