University POLITEHNICA of Bucharest

NEW APPROACH OF ENTROPY BOUNDS

Habilitation Thesis - SUMMARY

Pantelimon George Popescu

June 2017, Bucharest, Romania

New Approach of Entropy Bounds
Habilitation Thesis SUMMARY
P.G. Popescu

This work contains some of my research since the completion of my Ph.D., mainly related to Bounds for Shannon Entropy. We start with *Bounds for Kullback-Leibler Divergence*, where the purpose of the paper was to present some new bounds for the relative entropy $D(p||q)$ of two probability distributions and then to apply them to simple entropy and to mutual information. The relative entropy upper bound obtained is a refinement of a bound previously presented into literature.

We continue with *Bounds for Jeffreys-Tsallis and Jensen-Shannon-Tsallis divergences*. Recently, the Jeffreys-Tsallis and Jensen-Shannon-Tsallis divergences were introduced, and for them we established some new inequalities. Our results refine and generalize recent results in Tsallis theory and one of them even responds to an interesting open problem dated since 2011.

Then, in the paper *A new upper bound for Shannon entropy. A novel approach in modeling of Big Data applications*, we took on a Big Data application modeling challenge. Analyzing data type produced, stored and aggregated in Big Data environments is an important challenge in understanding data quality and represents a crucial support for decision making. Big Data application modeling require meta-data modeling, interaction modeling and execution modeling. Entropy, relative entropy and mutual information play important roles in information theory. Our purpose within this paper was to present a new upper bound for the classical Shannon Entropy. The new bound is derived from a refinement of a recent result from the literature, the inequality of S.S. Dragomir (2010). The reasoning is based on splitting the considered interval into the mentioned inequality. The upper bound can be considered in understanding the potential information that each data type may have in a Big Data environment.

In *New inequalities between information measures of network information content*, we refined a classical logarithmic inequality using a discrete case of Bernoulli inequality and then we furthermore refined two information inequalities between information measures for graphs, based on information functionals, presented by Dehmer and Mowshowitz in [32] as Theorems 4.7 and 4.8. The inequalities refer to entropy-based measures of network information content and have a great impact for information processing in complex networks (a sub-area of research in modeling of

complex systems).

Again in the field of networks, we present *A Geometric Programming Solution for the Mutual Interference Model in HetNets*. It is well known that the use of heterogeneous networks and densification strategies will be crucial to handle the wireless cellular traffic increase that is foreseen in the forthcoming years. Hence, the scientific community is putting effort into the proposal and assessment of radio resource management solutions for this type of deployments. For that, an accurate modeling of the underlying resources is mandatory. In this paper, we proposed a mutual-interference model, which enables a precise estimation of the signal-to-interference and noise ratio (SINR), compared with the widespread constant-load alternative. This is of utter relevance, since the SINR has a direct influence on the spectral efficiency and, consequently, on the resources to be allocated. We also propose a transformation of the corresponding resource assignment problem, so that it can be solved using geometric programming techniques. The validity of this transformation is assessed by comparing the corresponding solution with the one that would have been obtained exploiting a heuristic approach (simulated annealing).

We continue with the work *Energy-efficient virtualized clusters*, where we provided the state of the art for the virtualization techniques and means to reduce power consumption when using it. Virtualization allows us to answer all the user's requirements with many-core servers and thus eliminate the *one size does not fit all* issue. The resulting pool of resources is beneficial from an economic as well as environmental point of view. It brings benefits of scale to all logistic elements of the problem: power supply, cooling, floor space. When talking about virtualization and power consumption, one important aspect to be taken into account is the data center's heterogeneity from the hardware architecture point of view (e.g., X86, PowerPC). Mapping virtualized operating systems on hardware nodes in order to minimize power consumption is still an open issue that has been addressed throughout this paper: given a number of physical machines, we tried to map on them the available virtual machines (called virtual machine assignment) in order to have an efficient system when relating to power consumption. We exposed new general bounds for the power consumption of a virtual machine assignment based on Jensen inequality. The lower bound has been previously obtained and used into literature, so here we only rediscover it in a simplified and clearer manner. The upper bound is new and general. Further on, we practically evaluated some discrete cases and we proposed some graphics with the power consumption and its bounds for some particular real cases.

And finally, related to Side Channel Attacks, we presented *Back to Massey: Impressively fast, scalable and tight security evaluation tools*. None of the existing rank estimation algorithms can scale to large cryptographic keys, such as 4096-bit (512 bytes) RSA keys. In this paper, we presented the first solution to estimate the guessing entropy of arbitrarily large keys, based on mathematical bounds, resulting in the fastest and most scalable security evaluation tool to date. Our bounds can be computed within a fraction of a second, with no memory overhead, and provide a margin of only a few bits for a full 128-bit AES key.