Universitatea POLITEHNICA din Bucureşti

Nouă Abordare a Limitelor Entropiei

(NEW APPROACH OF ENTROPY BOUNDS)

Teză Abilitare - REZUMAT

(Habilitation Thesis – SUMMARY)

Pantelimon George Popescu

Iunie 2017, Bucureşti, România

Nouă Abordare a Limitelor Entropiei

Teză Abilitare REZUMAT
P.G. Popescu

Această lucrare conţine o parte din activitatea mea de cercetare ştiinţifică desfăşurată după finalizarea tezei de doctorat, fiind în principal legată de Entropia Shannon.

Vom începe cu articolul *Bounds for Kullback-Leibler Divergence*, unde scopul a fost să prezentăm câteva noi limite pentru entropia relativă $D(p||q)$ a două distribuţii de probabilităţi şi apoi să le aplicăm entropiei simple şi informaţiei mutuale. Limita superioară pe care am obţinut-o pentru entropia relativă este o rafinare a unei limite prezentate anterior în literatură.

Continuăm cu lucrarea *Bounds for Jeffreys-Tsallis and Jensen-Shannon-Tsallis divergences*. De curând au fost introduse divergenţele Jeffreys-Tsallis şi Jensen-Shannon-Tsallis, pentru care am propus noi inegalităţi. Rezultatele noastre rafinează şi generalizează rezultatele recente ale teoriei Tsallis, iar unul dintre ele chiar răspunde unei interesante probleme deschise datând din 2011.

Apoi, în articolul *A new upper bound for Shannon entropy. A novel approach in modeling of Big Data applications*, am abordat una dintre provocarile date de lucrul cu Big Data. Modelarea aplicaţiilor Big Data necesită modelarea meta datelor, a interacţiunilor şi execuţiilor. În această lucrare am prezentat o nouă limită superioară pentru entropia Shannon clasică. Noua limită este derivată dintr-o rafinare a unui rezultat recent în literatură, şi anume inegalitatea lui S.S. Dragomir (2010). Această limită superioară poate fi considerată pentru înţelegerea informaţiei potenţiale pe care o poate avea fiecare tip de date într-un mediu Big Data.

În *New inequalities between information measures of network information content*, am rafinat o inegalitate logatitmică clasică folosind un caz discret al inegalităţii lui Bernoulli, iar apoi am rafinat două inegalităţi informaţionale între măsuri informaţionale pentru grafuri, bazate pe funcţii informaţionale prezentate de Dehmer şi Mowshowitz în [**?**] ca Teoremele 4.7 şi 4.8. Inegalităţile se referă la măsuri ale conţinutului informaţiilor despre reţea bazate pe entropie şi au un mare impact în procesarea informaţiilor în reţelele complexe (un subdomeniu de cercetare în modelarea sistemelor complexe).

Tot in domeniul reţelelor am publicat *A Geometric Programming Solution for*

the Mutual Interference Model in HetNets. Utilizarea reţelelor eterogene şi a strategiilor de densificare va fi crucială pentru managerierea cu succes a creşterii traficului celular wireless ce se prefigurează în anii următori. De aceea, se depune efort ca să avem o modelare precisă a resurselor disponibile. În acest articol am propus un model de interferenţă mutuală care permite o estimare precisă a raportului semnal-interferenţă şi zgomot (SINR), în comparaţie cu mai raspândita alternativă a sarcinii constante. Acesta este extrem de relevant, deoarece SNIR are o influenţă directă asupra eficienţei spectrale, şi astfel asupra resurselor ce vor fi alocate. Propunem de asemenea o transformare a problemei corespondente, de alocare a resurselor, astfel încât aceasta să poată fi rezolvată folosind tehnici de programare geometrică. Validitatea acestei transformări este evaluată prin compararea soluţiei corespondente cu cea care ar fi fost obţinută folosind o abordare euristică.

Continuăm cu lucrarea *Energy-efficient virtualized clusters*, unde am prezentat câteva tehnici de virtualizare de ultimă oră, precum şi metode de a reduce consumul de energie la utilizarea lor. Virtualizarea aduce beneficii de scală tuturor elementelor logistice din ecuaţie: consum energetic, răcire, suprafaţă ocupată. Când discutăm despre virtualizare şi despre consum energetic, un aspect important de luat în considerare este eterogenitatea centrului de date din punctul de vedere al arhitecturii hardware (de ex. X86, PowerPC). Problema mapării sistemelor de operare virtualizate pe nodurile hardware pentru minimizarea consumului energetic a fost adresată de-a lungul întregii lucrări: fiind date un număr de maşini fizice, am încercat să le mapăm (alocăm) pe maşinile virtuale disponibile, astfel încât să obţinem un sistem eficient în privinţa consumului de curent. Am prezentat noi limite generale ale consumului de curent la alocarea unei maşini virtuale pe baza inegalităţii lui Jensen. Limita inferioară a fost obţinuta anterior si folosită în literatură, astfel încât aici doar am redescoperit-o intr-o manieră mai clară şi mai simplificată. Limita superioară este noua şi generală. În continuare am evaluat practic nişte cazuri discrete şi am propus nişte grafice reprezentând consumul energetic şi limitele sale pentru câteva cazuri reale particulare.

În cele din urmă, legat de domeniul atacurilor pe canale laterale (side channel attacks), am prezentat în lucrarea *Back to Massey: Impressively fast, scalable and tight security evaluation tools*. Nici unul dintre algoritmii de estimare a rangului existenţi nu poate fi scalat pentru chei criptografice de dimensiuni mari, precum cheile RSA 4096-bit (512 bytes). În acest articol am prezentat prima soluţie pentru estimarea guessing-entropiei unor chei arbitrare de dimensiuni mari, bazată pe limite matematice. Astfel am obţinut cel mai rapid si mai scalabil instrument de evaluare a securităţii disponibil pană în acest moment. Limitele pot fi calculate într-o fracţiune de secundă, fără încarcarea memoriei, şi oferă o marşă de eroare de doar câţiva biţi pentru o întreagă cheie AES de 128 de biţi.