prof. dr hab. Mirosław Kutyłowski
Wydział Podstawowych Problemów Techniki
Politechnika Wrocławska

Wrocław, 30.12.2018

Recenzja
rozprawy doktorskiej
Pseudoentropy
Macieja Skórskiego

Niniejsza opinia wydana zostaje w związku z uchwałą Rady Wydziału Matematyki, Informatyki i Mechaniki Uniwersytetu Warszawskiego powołującą mnie na recenzenta rozprawy doktorskiej Macieja Skórskiego w przewodzie prowadzonym na Wydziale MIM UW.

Ocena

Po przeanalizowaniu przedłożonych materiałów niniejszym stwierdzam, iż

przedłożona rozprawa doktorska spełnia wymagania

Ustawy o stopniach naukowych i tytule naukowym oraz o stopniach i tytule w zakresie sztuki mimo pewnych zastrzeżeń odnoszących się do strony redakcyjnej, o których mowa w uzasadnieniu poniżej.

Wyniki naukowe stojące za rozprawą są nie tylko znacznie powyżej (bardzo wysokich) wymagań w informatyce w naukach ścisłych w Polsce, ale oczekiwałbym bardzo wysokiej oceny, gdyby przewód był prowadzony na którejkolwiek z najbardziej renomowanych uczelni na świecie.

Uzasadnienie

Zawartość rozprawy i stawiany problem naukowy

Temat pseudoentropii badany przez Autora rozprawy jest niezwykle ciekawy i istotny w kontekście zastosowań teorii informacji w konkretnym kontekście obliczeniowym. Klasyczna teoria informacji nie bierze pod uwagę obserwowalnej zawartości informacji, tzn. takiej, która może być zauważona poprzez wykonanie dostępnych obliczeń. Tak jak wskazuje Autor, badania takie były prowadzone dla pseudolosowości (ze względu na dość oczywisty związek z praktyką obliczeniową). Rozpoznanie sytuacji w analogicznym zakresie dla mierzenia ilości informacji wydaje się bardzo ciekawym i ważnym kierunkiem badań. Ich rezultatem może być nie tylko uporządkowanie pojęć i zrozumienie relacji między nimi, ale przede wszystkim dostarczenie efektywnych narzędzi do rozwiązywania problemów w innych działach informatyki.

Rozprawa składa się z prac opublikowanych na konferencjach o czołowym znaczeniu na świecie: ICALP 2015, TC 2016, ICALP 2017, ITS 2015. Ranga tych publikacji wykracza znacznie poza standardowe oczekiwania jakie możnaby mieć pod kątem wyników przedstawianych jako praca doktorska.

MK

Wkład merytoryczny

Wkład merytoryczny Autora jest syntetycznie opisany na str. 8-10 autoreferatu, w związku z czym ograniczne się do krótkich uwag na temat poszczególnych kierunków badań:

Equivalence of HILL entropy and unpredictability pseudoentropy in high-entropy regimes. Wyniki przedstawione w tym obszarze podejmują temat zastosowań zródła entropii do wyprowadzania pseudolosowych kluczy. Wyniki rzucają światło na rzeczywiste związki pomiędzy *unpredictability entropy* a *HILL entropy* oraz wpływu "kompresji" prowadzonej za pomocą mnożenia przez losowe macierze.

Wyniki te są bardzo pożyteczne (nawet przy uwzględnieniu faktu, że nie wskazują na równoważność w sensie praktycznym). Rezultaty porządkują naszą wiedzę w sensie związków pomiędzy definicjami, same techniki dowodowe oraz pokonanie trudności technicznych mają mniejszą wagę.

Lower bounds for pseudoentropy chain rules and transformations. Autor rozprawy prezentuje granice dolne dla dwóch przypadków: powiązania *HILL pseudoentropy* i *metric pseudoentropy*, oraz utraty *HILL pseudoentropy* w obecności innej zmiennej losowej (tzw. *chain rules*).

Wyniki zamykają badania w tym zakresie – pokazują, że istniejących twierdzeń na ten temat nie da się w ogólności polepszyć. Warto pokreślić, że uzyskanie granic dolnych zazwyczaj wymaga dużo większej dojrzałości badawczej.

Simulating auxiliary information. Przedmiotem tej pracy jest symulowanie dodatkowej informacji Z dla zmiennej losowej (X,Z) poprzez zastąpienie jej poprzez $(X,h(X))$, gdzie h jest możliwie prostą funkcją. Temat z pozoru jest zagadnieniem o charakterze teoretycznym – w istocie silny wynik może pozwolić na eliminację w rozważaniach dodatkowej informacji Z (modelującej np. wyciek informacji z obliczeń kryptograficznych). Z mojego osobistego punktu widzenia ta część rozprawy jest najbardziej fascynująca, bowiem nie tylko zawiera wyniki ciekawe pod względem intelektualnym, ale takie, które mają znane i ważne implikacje w innych obszarach. Uzyskane ulepszenie z ε^{-4} (znane z poprzednich prac) do ε^{-2} jest ulepszeniem o niezwykle istotnych konsekwencjach.

Best generic attacks against pseudoentropy Rozdział ten podejmuje problem źródeł o ograniczonej pseudoentropii. Autorzy wykazują, że dla takiego źródła również *HILL pseudoentropy* jest ograniczona (pod warunkiem eksponencjalnego czasu obliczeń).

Jakkolwiek sam wynik zdaje się potwierdzać naturalne intuicje, to należy podkreślić, że Autor rozprawy wykorzystuje zaawansowany aparat matematyczny.

Geometric characterization Autor przedstawia sformułowania definicji dotyczących *metric pseudoentropy* w języku geometrycznym - co samo w sobie jest zabiegiem czysto językowym. Okazuje się jednak, że prowadzi to do uproszczenia dowodów kilku ważnych wyników.

Przedtawiona praca pokazuje, że Autor rozprawy nie tylko potrafi uzyskiwać trudne wyniki, ale także że potrafi przeprowadzić badania syntetyzujące dotychczasowy stan wiedzy.

Warto podkreślić, że jakkolwiek przedstawione wyniki mieszczą się w ramach jednotematycznego programu badawczego, jednak ich poziom różnorodności pod względem technicznym jest bardzo wysoki.

Na koniec chciałbym podkreślić, że poziom wyników i ich wkład w rozwój informatyki odpowiada raczej poziomowi rozprawy habilitacyjnej niż doktorskiej.

Wiedza kandydata w specjalności naukowej

Bez wątpienia Autor rozprawy jest osobą znakomicie zorientowaną w bieżącym stanie wiedzy na temat pseudoentropii. Jest jednym z ważniejszych autorów na świecie publikujących w tym obszarze badań. Ilustracją tego głębokiego stanu wiedzy jest cykl prac składający się na rozprawę, gdzie poważna część każdej pracy poświęcona jest omówieniem aktualnego stanu wiedzy.

Warto zaznaczyć, że pseudoentropia jest tematem stosunkowo świeżym w teorii informacji uprawianej w informatyce i że relatywnie duży jest udział Autora w rozwój tej działki. Udokumentowane jest to w szczególności pracami publikowanymi na czołowych konferencjach.

Należy również podkreślić, że prace przedstawione jako rozprawa stanowią jedynie część dorobku naukowego Autora rozprawy. Dla przykładu można podać kilka świeżych prac o wysokim poziomie merytorycznym i mogących z powodzeniem wchodzić do zestawu prac składanych jako rozprawa doktorska:

- Maciej Obremski, Maciej Skórski: Inverted Leftover Hash Lemma. ISIT 2018: 1834-1838
- Maciej Skórski: On the complexity of estimating Rènyi divergences. ISIT 2017: 256-260
- Maciej Skórski: Lower Bounds on Key Derivation for Square-Friendly Applications. STACS 2017: 57:1-57:12

Kilka świeżych raportów technicznych świadczy o intensywnej działalności naukowej prowadzonej obecnie przez Autora.

Poprawność wyników i strona redakcyjna

Na rozprawę składa się cykl prac traktujący o pseudoentropii. Prace są częściowo współautorskie, jednak udział Autora rozprawy jest wyraźnie określony. Zgodnie z załączonymi deklaracjami współautorów jest on znaczny. Styl wszystkich prac jest bardzo podobny - niezależnie od tego czy praca jest samodzielna czy ma współautorów. Również ich poziom merytoryczny jest podobny. Tym samym brak jest jakichkolwiek przesłanek pozwalających na kwestionowanie roli Autora rozprawy i jego znacznego udziału w powstaniu przedłożonych wyników.

Autor rozprawy korzysta z możliwości danej przez ustawę i zamiast redagowania odrębnego dzieła przedstawia cykl opublikowanych prac. W tym szczególnym przypadku budzi to jednak zastrzeżenia:

- Wszystkie przedstawione prace mają charakter "extended abstract". Wynika stąd, że każda z nich w zasadzie poświęcona jest zaprezentowaniu wyniku na tle wcześniejszych badań a w niewielkim stopniu poświęcona jest udokumentowaniu szczegółów merytorycznych. Idea publikowania prac w formie "extended abstracts" ma sens - umożliwia szybką wymianę idei, jednak za nimi powinny iść prace zredagowane w sposób bardziej tradycyjny – m.in. z pełną wersją definicji, dowodów twierdzeń, ze wszystkimi szczegółami (również tymi o charakterze rutynowym). Może być to zrealizowane np. w formie raportu w systemie eprint IACR, czy tzw. "journal version". Formułowanie rozprawy doktorskiej było znakomitą okazją do wykonania takiej porządkującej pracy.

- Reguły recenzowania prac zgłaszanych na konferencje takie jak ICALP mówią, że treści znajdujące się w appendixach nie muszą ani być uwzględniane ani oceniane przez recenzentów i komitety programowe. W sytuacji, gdy kluczowe dowody znajdują się właśnie w tych załącznikach do prac a nie w ich głównej części, nie można dać rękojmi, że dowody te zostały wnikliwie sprawdzone przez niezależnych recenzentów.

- Forma prac przedstawionych jako rozprawa doktorska nie umożliwia szybkiej weryfikacji poprawności wyników w zgodzie z wymaganiami czasowymi na złożenie recenzji. W istocie recenzent byłby zmuszony do "uliniowienia" struktury pracy i rozwinięcia szeregu skrótów.

- W wielu przypadkach część główna zawiera zarys ogólnej idei określonego wyniku. Opis taki nie okazuje się zbyt pomocny, gdyż jego zrozumienie może być warunkowane znajomością szczegółów dowodu, który znajduje się w appendixie.

Dla uwiarygodnienia poprawności wyników zawartych w rozprawie dokonałem szczegółowego przeglądu dowodu Tw.1 – jednego z dwóch wyników zawartych w pracy "Condensed Unpredictability". Jakkolwiek dowód (po minimalnych korektach) wydaje się poprawny jednak zaznaczyć trzeba kilka aspektów:

- znaczenie Tw. 1 wydaje się nieco przereklamowane przez autorów: jakkolwiek jest interesujące pod względem intelektualnym osiągnięcie stałego czynnika Δ zamiast logarytmicznego, jednak należy zwrócić uwagę na redukcję wielkości obwodów mogących służyć do rozróżnienia rozkładów z s do $t \approx \frac{s}{2^{2k}}$. Dla interesujących wielkości danych (np. $k = 80$) zmniejszenie rozmiaru 2^{160} razy jest dramatyczne i dużo ważniejsze niż pogorszenie entropii o więcej niż stałą.

- Dowód nie zawiera nowych głębokich idei, jest dość elementarny. Główną trudnością dla czytelnika nie jest stopień zaawansowania dowodu, ale niedopracowane zredagowanie oraz konieczność przyswojenia sobie szeregu definicji. Poniżej zamieszczam listę uwag dotyczących tego dowodu.

MR

Lista szczegółowych uwag redakcyjnych dotyczących dowodu Twierdzenia 1 z pracy "Condensed Unpredictability":

1. str. 33, ostatni akapit: Twierdzenie Hasta nie dotyczy "dekodowania kodów Hadamarda" ale jest eleganckim rozwiązaniem problemu braku odpowiedzi wyroczni (we wcześniejszych pracach dodawano w takim przypadku losowe odpowiedzi). Komentarz przed cytowanym twierdzeniem wprowadza tylko zamieszanie.

2. str. 34: twierdzenie Hasta cytowane jest literalnie. W kontekście pracy Hasta sformułowanie to jest jasne jednak odwoływanie się do pojęcia "kodów Hadamarda" jest zaprzeczeniem zasady brzytwy Occama: wyrocznia w istocie zwraca wartości iloczynu skalarnego x, r dla nieznanego x i zadanego r. Słowa "kod Hadamarda" zostaną użyte tylko raz poza sformułowaniem twierdzenia. Korekcja błędów i inne pokrewne zagadnienia są tu zupełnie nieistotne.

3. str. 34, pierwsze zdanie dowodu: wersja dla $\varepsilon > 0$ nie wynika "bezpośrednio" z definicji pseudoentropii. Miejsce to wymaga pewnego wyjaśnienia.

4. str. 34, nierówność 12: Autor uzasadnia ją słowami "using Markov eq. (10) gives us". Pomijając kwestię żargonowego sformułowania (używać można nierówność Markova a nie samego Andreja Markova), uzasadnienie nierówności (12) wymaga więcej niż nierówności Markova: istotne jest, że w żadnym wypadku prawdopodobieństwo nie przekracza $\frac{1}{2}$.

5. str. 34, zdanie przed nierównością (15): do czego odnosi się słowo "Which"? Nierówność zdaje się wynikać bezpośrednio z (14) i (12).

6. str. 35: "contradicting the right hand-side of (8)": jest dokładnie odwrotnie. Prawa strona (8) została wyprowadzona (co zresztą jest prawidłowym krokiem w dowodzie).

7. notacja: w dowodzie Autor używa notacji $a.b$ dla iloczynu skalarnego wektorów a, b, podczas gdy w treści głównej na stronie 29 mówi o "inner products $A_i = R_i^T X$ for ...". W związku ze zmianą notacji czytelnik w pierwszym momencie powinien założyć, że chodzi w istocie o odmienną operację i poszukiwać jej definicji w pracy. Dopiero analiza dowodu pozwala zorientowanie się, że jest to w istocie pomyłka.

8. notacja: używanie wyrażeń typu R_i^{k+1}, A_i, A^i jest formalnie poprawne, jednak utrudnia czytanie: A_i oznacza pojedynczy element ciągu $A = (A_1, \ldots, A_k)$, A^i oznacza $(A_1, \ldots, A_i)$ zaś A_i^j oznacza $(A_i, \ldots, A_j)$. Dobrą praktyką w zakresie pisania prac o charakterze matematycznym jest stosowanie takiej notacji, by automatycznie czytelnik miał prawidłowe optyczne skojarzenia symboli graficznych z ich znaczeniem. Użycie podobnie wyglądających symboli oznaczających obiekty różnych kategorii jest błędem w sztuce mimo formalnej poprawności.

9. str. 34, nierówność (16): nie wynika ona z samej nierówności Markova.

10. str. 35, definicja (17): definicja jest nieczytelna bo obiekt r^{i-1}, do którego odnosi się pojęcie *good*, nie występuje explicite po prawej stronie. Jest on ukryty w $\hat{A}^{i-1}$. (Drobna literówka: zdanie poprzedzające kończy się kropką.)

11. str. 35, krok 2 dla P_i: obwód A nie może otrzymać x jako inputu, dane te dopiero staramy się wyliczyć – jest to dosyć oczywista pomyłka (x należy po prostu wykreślić), jednak powinna zostać wychwycona przez recenzenta przed opublikowaniem pracy.

12. ten sam krok algorytmu: zdanie "Note that..." sugeruje, że $r^{(i)}$ zostało już gdzieś określone. Nie jest to prawdą. Niestaranne sformułowanie powoduje problemy przy parsowaniu tekstu przez czytelnika: widząc "Invoke ..." a następnie zdanie zaczynające się od "Note that" czytelnik zatrzymuje się próbując zinterpretować wszystkie argumenty wywołania przed przejściem do komentarza następującego po słowach "Note that".

13. str. 35, akapit po specyfikacji $P_i(r_i)$: uzasadnienie "Using (11)" jest błędne. Nierówność (11) nie wystarcza, naprawdę trzeba się odwołać do sposobu generowania odpowiedzi przez A uwzględniającej rzucanie monetą.

14. str. 35, ostatni akapit: w przypadku $c - e$ nie można mówić o równości, zapewniona jest nierówność (co oczywiście wystarcza). Dla czytelności najpierw wypadałoby określić wartość s, a potem przedstawić wyrażenie dla $e + c$.

15. str. 36, wyrażenie opisujące złożoność czasową dla P powinno być wyprowadzone.

W pewnym stopniu przedstawiane w pracach dowody zawierają przeskoki w argumentacji. Niekiedy takie zjawisko można usprawiedliwić faktem narzuconego ograniczenia liczby stron i koniecznością skompresowania tekstu. Nie powinno być jednak regułą, by czytelnik był zmuszony do odtwarzania fragmentów, które nie są oczywiste do odtworzenia w pamięci. Nagminne stosowanie przeskoków (nawet wyłącznie w trywialnych miejscach) powoduje znużenie czytelnika i zaprzestanie weryfikacji po pewnym czasie. Tym samym możliwe jest istnienie fragmentów, których nikt w istocie nie sprawdził. Doświadczenie uczy, że błędy o charakterze matematycznym nieproporcjonalnie często zawarte są we fragmentach kryjących się za zdaniami typu "jak łatwo zauważyć ... ", szczególnie gdy nie występują w początkowych fragmentach pracy. Z tego względu przedstawienie rozprawy w formie zestawu prac mających charakter *extended abstracts* jest co najmniej kontrowersyjne.

Kompozycja prac wchodzących w skład rozprawy jest niestandardowa i niekiedy graniczy z obfuskacją. Dla przykładu opiszmy sytuacje dla pracy "Pseudoentropy: Lower-bounds for Chain rules and Transformations":

- Wstęp na stronach 51-57 w istocie nie jest wstępem ale również przedstawieniem wyników pracy z ogólnymi szkicami idei dowodów. Po wstępie tym pojawia się rozdział "Basic Definitions" na stronach 57-58. Zrozumienie wstępu wymaga jednak uprzedniego zaznajomienia się w rozdziałem "Basic Definitions". Jest to błąd kompozycyjny: wstęp powinien zawierać wyłącznie

odniesienia do pojęć ogólnie znanych w dziedzinie, potem powinny zostać wprowadzone bardziej szczegółowe pojęcia i rozważania dotyczące kwestii szczegółowych.

- Wyniki pracy opisane są na stronach 59 i 60. W przypadku Tw. 1 autorzy przedstawiają krótki *szkic*, w przypadku Tw. 2 odsyłają w zasadzie do appendixów. Wspomniane ogólne szkice nie umożliwiają łatwego odtworzenia dowodów i w ograniczonym stopniu są pomocne dla czytelnika. Tym samym dowód pojedynczego twierdzenia pojawia się w trzech miejscach na różnym poziomie szczegółowości: raz we wstępie, raz w rozdziale trzecim a raz w appendixach (niekoniecznie w jednym kawałku).

Mirosław Kutyłowski