

東北大学大学院情報科学研究科主催

第19回 博士後期課程学生発表会

アブストラクト集

2018年7月13日(金)

東北大学大学院情報科学研究科

2階 大講義室

<第1セッション 13:05～14:25>

小島 匠太郎

「壁反力を利用したクローラロボットの走行制御」

プラント点検等への応用が期待されるクローラロボットには、狭い点検通路で移動する能力が求められる。本研究では、周囲の壁との接触を利用した新たな移動方法の構築を目的とする。発表では、壁から離れる動作中に意図しない方向に移動してしまう“壁デッドロック”問題の回避動作について説明する。加えて、壁を積極的に活用することで、クローラロボットにとって踏破が困難な狭隘な螺旋階段の走行が可能となることについて報告する。

横井 祥

「カーネル法に基づく疎な言語表現のための共起尺度」

ふたつの文の間の関連の強さを自己相互情報量 (PMI) で推定するには長時間の学習が必要となる。本発表では PMI が「相互情報量への文対の貢献度」と捉えられることに対比させ、提案尺度である PHSIC を「HSIC (カーネル法に基づく依存性尺度) への文対の貢献度」で定義する。実験結果として、PHSIC を対話の応答文選択に適用すると PMI よりも約 1000 倍高速に学習できること、また機械翻訳の訓練データのフィルタリングに適用すると翻訳機の性能を保ちながらデータ量を約 3 分の 1 に圧縮できることを示す。

寺岡 諒

「聴覚の空間的注意の情報処理過程に関する研究」

複数の音源が存在する環境下で特定の音を聞き取る際、その音に対して注意を向けることによって、その音の聞き取りが容易になる (カクテルパーティ効果)。この現象に関しては様々な観点から研究がなされているが、どのようなメカニズムによって実現されているのかは明らかではない。そこで本研究では、特に音源位置に対して向けられる注意に着目し、メカニズムを明らかにする。

大澤 弘基

「グラフ彩色遷移問題の一般化に関する研究」

理論計算機科学においてグラフ彩色は重要な研究トピックであり，近年では，複数のグラフ彩色の間の連結性を扱うグラフ彩色遷移問題が盛んに研究されている．この問題は色数が3のときには計算容易であり，色数が4以上のときには計算困難となることが知られており，これ以上の解析はないと考えられていた．本研究では，この問題の一般化を提唱することで，従来の計算複雑性の結果を包含しつつも，より精緻に解析できることを示した．

<第2セッション 14:35～15:55>

八木澤 史子

「児童が情報端末を活用する授業における教師の教授知識に関する研究」

教育の情報化に伴い，学校現場ではICT環境の整備が進み，特に近年多くの自治体で学習者1人に対して1台の情報端末の導入が進んでいる．しかし，児童が情報端末を活用する授業における教師の意思決定やそれに必要な教授知識など教師研究分野の学術的な知見については，十分に明らかにされていない．本研究は，児童が情報端末を活用する授業の観察および質問紙調査によるケーススタディや質的分析を通し，児童が情報端末を活用する授業に必要な教師の教授知識に影響を与える要因を検討するものである．

徐 載 甲

「光学的測定手法に基づく標準マイクロホン特性分析に関する研究」

音響の測定に広く使われる上，音響分野の標準機でもあるマイクロホンの特性を正しく定義するには感度，位相，共振周波数，減衰係数などの多様な因子の測定が必要である．現在，これらの因子を決める方法として多様な方法が適用されているが，方法が複雑である上，同時に測定が不可能である問題があり，音響標準の補給に障壁になっている．本研究では光学的測定手法に基づくマイクロホンの振動幕測定を用いて，これらの因子をより正確で効率よく測定する方法を検討する．

**Daniel Marcell Gongora Flores**

### **Haptic feedback of first-person view videos for enhancing quality of experience and dynamic scene recognition**

Vibrotactile feedback has the potential to augment the entertainment and informative dimensions of visual media with dynamic scenes. First, we propose a vibrotactile rendering method for camera motion in first-person view (FPV) videos that enables viewers to feel the camera movement with both hands. A pilot user study showed favorable effects of our method on viewers' perceived realism and satisfaction when watching FPV videos. Second, we propose using camera vibrations as vibrotactile feedback to support collision detection in fast video playback. A pilot user study showed that camera vibrations delivered to the palm of the dominant hand improved collision detection performance. Furthermore, we observed that without vibrotactile feedback participants are likely to underestimate the number of collisions in a video.

**Ville Yli-Mäyry**

### **Security Evaluation of Low-latency Cryptographic Hardware**

In recent years, the need for low-latency cryptographic ciphers has increased. For this, designs such as PRINCE have been introduced lately to answer the need for ciphers that can perform an encryption operation with very low latency. On the other hand, the hardware security of these implementations has to be considered. Methods in side-channel analysis, that utilize physical characteristics of cryptographic core's implementation to reveal secret information pose a serious security risk to these implementations. This work focuses on the hardware security evaluation of low-latency ciphers. We evaluate different possible side-channel analysis scenarios and methods, and perform a security evaluation on several implementations on FPGA and ASIC.

< 第3セッション 16:05～17:25 >

**李 允成**

#### **「クラウド無線アクセスネットワークにおける省電力化に関する研究」**

近年、モバイルネットワークにおけるデータトラフィック量の増加に伴い、多数の基地局を高密度に配置し集中制御を行うクラウド無線アクセスネットワーク（C-RAN : Cloud Radio Access Network）が導入されている。しかし、C-RAN に設置されている基地局数が莫大であるため、C-RAN の消費電力は膨大である。そこで、基地局の省電力制御及び集中制御部の省電力制御を両方考慮することでC-RAN 全体の消費電力を低減する手法を提案し、その性能を評価する。

岡田 俊太郎

### 「D-Wave マシンによる大規模問題の最適化に向けた埋め込みアルゴリズム」

D-Wave マシンは世界初の商用量子コンピュータであり、最適化問題を高速に処理できると期待されているが、現状の代表的な課題として qubit 数の制約と変数間の相関を表すグラフ構造の制約という 2 つがある。

qubit 数の制約に対しては、既に qbsolv というツールが提供されており、大規模問題の一部の最適化変数を抽出して部分問題を構成し、部分問題の最適化を繰り返し返して全体の解を得る方法が考えられている。

一方で、グラフ構造の制約に対しては任意のグラフ構造をもつ問題をハードウェアグラフに変換するマイナー埋め込みが必要であるが、現在提案されている方法の処理時間は非常に長く、部分問題の繰り返し処理に適していない。

本発表では、部分問題を高速にハードウェアグラフに埋め込むアルゴリズムの検討結果と、これを用いることで qbsolv よりも高精度な解を得られる例を示す。

**Firas Kraiem**

### **On cryptographic assumptions**

It may come as a surprise that we have no certainty that the cryptographic methods we use to protect our important data work as expected. This is because, although nobody knows how to "break" them, nobody has proved that it is impossible, either. How, then, can we gain enough confidence in cryptographic methods to trust them with our secrets? One solution is to take a mathematical problem that has been studied extensively but still has no known solution, and to prove that if someone can "break" our encryption, they can also solve said problem. We look at some such problems.

**Tiago Gama Rodrigues**

### **Realizing 5G and IoT: Various Methods for Lifting Device Limitation in High Scale Scenarios**

The future of network communications is tightly connected to the Internet of Things (IoT) and 5G, which are characterized by massive amounts of devices, all connected, most of which are limited by energy and processing constraints. This doctoral research will aim at developing an IoT support system by tackling different issues with different solutions. Mobile Edge Computing will be used to connect the devices to physically near servers in order to raise their processing capabilities, Power over Fiber will be used to provide enough energy for their functions, and Wireless Mesh Networks can improve the communication of the system. Finally, to deal with the scale and complexity brought by the number of devices, Artificial Intelligence / Machine Learning algorithms will be utilized. The end results will be a high-quality system with cheap and simple devices.

<第4セッション 17:35～18:35>

伊東 桂司

「非原始的な非可換アソシエーションスキームの第2固有行列」

アソシエーションスキームは代数的組合せ論において重要な研究対象のひとつであり、その中でも可換アソシエーションスキームは、その性質の良さからさまざまな応用が研究されている。それに対して、非可換アソシエーションスキームは可換アソシエーションスキームほどよい性質を持っていない。しかし、一部の非原始的な非可換アソシエーションスキームは第2固有行列を決定でき、可換アソシエーションスキームに近いふるまいをすることを紹介する。

河田 真由子

「アリストテレスにおける欲求と行為 一意志概念との対照をもとに」

私たちが通常使用する意志という語が古代ギリシャには無かったことに着目し、意志に相当する諸概念を検討することによって、意志とは何か、その曖昧な定義を問い直すことを目的とする。意志概念の歴史的背景を踏まえながら、アリストテレスのテキストを用い、理性に関わる欲求、自発性、選択の概念を取り上げる。

小舘 俊

「Sleeping Beauty 論文に着目した科学発展過程の解析」

科学を先行する研究の上に積み重なってきた歴史と考えると、それは引用という形で論文にあらわれている。ある典型的な論文の被引用履歴は出版直後にピークを迎えるというものであるが、対して出版直後にはあまり引用されずしばらくしてから急激に引用されるようになる、いわゆる“Sleeping Beauty” と呼ばれる論文も存在する。本研究ではこれに着目し、科学の発展過程について知見を深めることを目的とする。