

博士論文概要 「環境情報からのメッセージ」 情報環境専攻

名前	指導教員	論題	論文要約
赤堀 奈生	野間 淳	Newton polygon と平面曲線の特異点解消による resolution graph の一致性	Newton polygon が一致する多項式において, その多項式の零点集合で定義される特異平面曲線の resolution graph も一致するという仮説を立て, 任意の多項式について成り立つかどうかの研究を行った. Convenient な Newton polygon を持ち, Newton polygon の face が1つのみであり, face が端点の2点でのみ定義される Newton polygon を持つ2つの複素数係数多項式について, それらの零点集合で定義される特異平面曲線の resolution graph が一致することを示した. また, face が複数個ある場合についても, 各 face が端点の2点で定義されるとき同様の結果を得た.

浅川 栄一	白川 真一	Deep Learning を用いた発話テキストに対応するジェスチャの自動生成	本研究では、人型エージェントへの応用を目的とした、発話テキストに対応するジェスチャ生成手法を提案する。提案モデルは、発話テキストを入力として受け取り、出力としてジェスチャを表す2次元関節座標のシークエンスを出力する。ディープラーニングにより学習した提案モデルが生成したジェスチャを評価するために、正解データに対する関節座標の予測精度と分散による評価と生成ジェスチャの定性的な評価を行った。実験の結果から、提案手法によってテキスト情報から自然なジェスチャの生成が可能であることと、生成ジェスチャの質は音声からのジェスチャ生成手法に匹敵することを確認した。
阿部 穰太郎	森 辰則	キュレーションマップ自動生成システムにおける文書組織化の精度向上	キュレーションマップとは、ある文書集合において観点ごとにまとめられたテキストを効率的にユーザに提示する情報複合体である。これを自動生成する手法にて課題となっていた観点分割精度を、文単位化処理、挟み撃ち併合処理、重複文書併合処理を行うことで向上させた。また、キュレーションマップを閲覧するUIを提案し、検索エンジンとの比較実験の結果、多様な情報を詳細に提示できるという点で優れていることがわかった。

安生 英之	藤井 友比呂	日本語における空付加詞読みの可否と述語形態の関係	<p>本研究のテーマは、大人の日本語話者における、付加詞を伴う目的語の省略現象についての分析に関する心理言語学実験である。</p> <p>具体的には、以下の一般化を、実験により検証した。</p> <p>(1) Funakoshi (2016)の一般化</p> <p>他動詞文において、付加詞が省略可能となるのは、目的語が省略されている場合のみである。</p> <p>(2) Hayashi & Fujii (2015)の一般化</p> <p>(1)は、動詞が和語である場合には適用されるが、漢語の場合には適用されない。</p> <p>実験の結果、上記が正しいことが分かった。</p>
安藤 駿	森 辰則	雑談対話における利用者の発話負荷軽減のためのマルチエージェント対話システムの検討	<p>本研究では、2者対話が主流であった従来の雑談対話システムが持つ、互いが積極的に発話しなければ会話が継続できない性質を解決し、利用者の発話負荷を軽減することをめざした。そのために、マルチエージェントによる雑談対話システムを検討し、利用者が積極的に発話しなくても話の輪の中に入っているような実感を得られることをめざした。提案システムにより、利用者の負担感が減少し、満足度の向上に寄与したことが確認できた。</p>

石田 卓也	富井 尚志	エネルギーライフログ DB を用いた EV の動的充放電計画の実証実験	我々は先行研究として、スマートグリッドにおいて日ごとに EV の出発時充電量と充放電のタイミングを動的に変更する「動的充放電計画」を提案した。本研究では、実環境でスマートグリッドを構成し、動的充放電計画の実証実験を行う。グリッドの最小構成単位のマイクロセルとしてオフィス 1 部屋と EV1 台という環境を実装し、実験結果から、シミュレーションと実環境の違いを示した上で、エネルギーバランスの観点から動的充放電計画の有用性を示した。
板垣 亮太	松井 和己	膜を含む臓器の幾何学モデルの微分方程式による自動生成	現在、手術シミュレータの開発が行われている。手術シミュレータ上で患者の臓器モデルを CT 画像から生成する際、膜などの組織は CT から検出されず、自動で生成できない。本研究の目的は膜を含む患者固有臓器モデルの自動生成の手法を提案することである。本研究では膜を含む臓器の形状を場の関数で表した標準モデルを、界面移動を表す方程式を解き患者固有モデルの形状まで変形させることで膜を含む患者固有モデルを自動的に生成させる。

伊藤 俊介	森 辰則	レビューアーの評価基準表現情報に基づくレビューテキストからの不満情報抽出手法の検討	近年 EC サイトが普及し、多くの人が利用している。EC サイトでは過去に記述されたレビューが蓄積され誰でも閲覧することが出来る。レビューには商品の不満情報が存在し、不満情報は EC サイトを利用する人にとって有益な情報である。そのため、本研究では不満情報がどのように現れるかを分析し、レビュー中の不満情報を定義した。この定義を元に、不満情報の抽出手法を検討し、抽出実験を行った。
井上 侑哉	松本 勉	超音波距離計の計測セキュリティに係る研究	ToF 方式超音波距離計は自動車やファクトリーオートメーション等多岐にわたり利用されている。超音波距離計の出力が狂わされる、または動作を停止させるような攻撃を受けると、システムは正常に作動せず、重大な事故につながる危険性が考えられる。そのため ToF 方式超音波距離計の計測セキュリティを高める研究は社会的に意義があるといえる。本稿では ToF 方式超音波距離計の脅威になりうる攻撃および、その攻撃に対するセキュリティ強化策の検討や実証実験を行う。

岩田 脩平	中本 敦浩	内周の大きな平面グラフの improper DP-coloring について	隣接 2 頂点に同じ色を与えることをある程度許す彩色をグラフの improper coloring という. その拡張として improper list coloring, さらにその拡張として improper DP-coloring が知られている. 本研究では, 内周が大きい平面グラフの improper list coloring の先行研究に着目し, それを improper DP-coloring に拡張した結果を得た.
内田 佳介	吉岡 克成	WebUI 情報に着目した広域スキャンによる IoT 機器の発見に関する研究	近年、重要施設の遠隔監視制御を目的とするシステムへの IoT 導入が進んでいる. これらの Web 管理画面に施設名等が明記された上で, 誰もが閲覧可能な状態のまま運用されている事例が報告されている. しかし, 同様の機器がどの程度存在するかは明らかになっておらず, その調査が急務となっている. 本研究では広域スキャンやクラスタリングを用いてこのような機器をインターネット上から半自動的に探索する手法を提案する.

内田 絢斗	白川 真一	ガウス分布を用いた Information Geometric Optimization の有限サンプル解析	本研究では、確率モデルに基づく Black-Box 最適化法のフレームワークである Information Geometric Optimization (IGO) に対し、等方性ガウス分布を適用した場合および分散共分散行列を対角行列に限定したガウス分布を適用した場合について凸二次関数上での振る舞いをそれぞれ理論的に解析する。サンプル数が無限であることを仮定していた先行研究とは異なり、サンプル数が有限の下で解析を行うことで、実際の IGO の振る舞いと一致する理論解析結果を導出する。
-------	-------	--	--

大串 健人	小関 健太	k-tree の domination number について	<p>グラフ G において、G の頂点集合 S が $S \cup N(S) = V(G)$ を満たすとき、S を G の dominating set という。ただし $N(S)$ は S の頂点に隣接する頂点の集合を表す。また G の最小の dominating set の位数を G の domination number という。Campos 氏と Wakabayashi 氏, Tokunaga 氏は、n 頂点の極大外平面グラフ G の domination number が $(n+t)/4$ 以下であると示した。ただし t を G で次数 2 の頂点数とする。本研究ではその結果を 2-tree と呼ばれるグラフへとまず拡張し、それを一般化した k-tree と呼ばれるグラフ G の domination number が $(n+t)/(k+2)$ 以下であることを示した。ただし n を G の頂点数, t を G で次数 k の頂点数とする。</p>
-------	-------	---------------------------------	---

大橋 亮	原下 秀士	Appell-Lauricella 超幾何級数に関連した曲線の微分形式について	代数幾何学や数論において、楕円曲線は重要な研究対象である。本論文では、楕円曲線のある種の一般化である Appell-Lauricella 超幾何級数に付随した曲線について研究を行った。主結果として、容器曲線における正則微分加群の基底を明示的に記述することに成功した。ここで、特異点をもつ曲線上の正則微分形式は Serre により定義されたものである。また、上記曲線を無限遠点のみで特異点解消した曲線についても同様の結果を得ることができた。今後は応用として、いくつかの特殊な場合で上記曲線の超特別性を研究したい。
大矢 康介	森 辰則	世界史用語集の語釈文における見出し語に照応するゼロ代名詞の表層格の推定	本稿では、世界史に関する大学入試論述問題に対して自動要約手法に基づき解答を自動生成する際の知識源の一つとして世界史用語集に注目し、見出し語と語釈部に分かれている文書データから解答となる文章を作成するために、語釈文における見出し語に照応するゼロ代名詞とその表層格を推定する手法を提案する。

大湯 耕大	野間 淳	二重被覆を用いた曲面の特異点解消	$z^n=f(x,y)$ で定義された曲面の n 重被覆を用いた特異点解消に関する先行研究を元に, $n=2$ の場合について blowing up と正規化のみを用いたより簡単な特異点解消の方法をまとめた. その方法を用いて, Du Val Singularity を持つ曲面全てに対して具体的に特異点解消の計算を行い, その計算過程をまとめた. また, この方法によって特異点解消を行なった際に得られる重み付き双対グラフが, 良く知られている Du Val Singularity の重み付き双対グラフと一致することを確かめた.
岡田 凱	白川 真一	階層型強化学習による船舶の着棧制御	海上輸送量の増加に伴う船員不足と人為的要因による事故といった問題に対処するため, 自動操船技術の実現が望まれており, 強化学習などの機械学習技術の応用が期待されている. 本研究では, 階層型強化学習の考え方をを用いることで自動操船技術を構成する着棧制御則の獲得を目指す. 階層型強化学習は, 長期に渡る目標を達成する行動決定規則を獲得することに長けた手法であり, 着棧制御にも適していると考えられる. 数値実験では, 提案手法により得られた制御則を用いることで, 広い範囲からなめらかな軌道で目標位置に接近することが可能であることを示した.

加藤 慎二	長尾 智晴	遺伝的プログラミングにおける 転移学習を用いた汎用的な 精度向上手法	遺伝的プログラミングは様々な問題に適用され、多くの改良手法が提案されている。この遺伝的プログラミングはメタヒューリスティック手法の一つであるため、No Free Lunch に従った精度向上が望ましい。No Free Lunch の定理に従い、知識を利用する手法として転移学習が存在するが、事前問題を設定が困難である。本稿では、多数の事前問題から知識を抽出し、選択する手法を提案する。提案する手法は島モデルを利用して知識抽出と知識選択を行う。この手法の利点は、自動的に知識を利用するため、事前問題の設定が不要であることである。さらに、提案する手法は知識抽出と選択が分かれており、独立したステップが構成されるため、拡張性に優れる。実験によって 70 の回帰問題で検証した結果、提案手法は単純な遺伝的プログラミングよりも、テストデータにて 12.7% 精度が向上した。
-------	-------	------------------------------------	--

川北 隼	西村 尚史	等周不等式の研究	<p>等周不等式とは、長さが一定の縄で囲むことができる面積と縄の長さとの関係を表した昔からよく知られている不等式である。そして、現在までに様々な証明法が発見されている。等周不等式に関する先行研究では平面閉曲線から生まれる新たな図形概念を加えることによって元の不等式を拡張したものがある。本研究では、等周不等式について新規性を獲得することを目的とし、そのために2つの先行研究について着目した。</p>
工藤 大嗣	山田 貴博	支持状態の変化による薄板の分岐解析	<p>薄板の周辺部数カ所を接触状態で支持するような、面内に移動可能な境界条件を考えると、不安定モードが現れる。この不安定モードが現れる現象を本研究では波打ち現象とよぶ。この現象は有機 EL ディスプレイの製造工程で観察され、様々な悪影響を及ぼす。しかしながら、この現象のメカニズムはいまだ解明されていない。本研究は、この現象が薄板の自重による座屈現象であるという仮説のもと、有限要素法を用いた座屈固有値解析を行いそのメカニズムを解明する。</p>

小池 風樹	富井 尚志	EV を用いた再生可能エネルギーのマッチングシミュレーションと実データによる評価	IoT 技術の発達により、再生可能エネルギーの発電ログ、建物の需要電力、および、自動車の走行ログなどのエネルギーに関する記録(エネルギーライフログ) を容易に取得することが可能となった。本研究では、これらのライフログを蓄積するエネルギーライフログ DB を構築し、電気自動車(Electric Vehicle:EV) の充放電による再生可能エネルギーのマッチングシミュレーションを行う。また、EV の補助として据え置き型バッテリーの利用を想定し同様にシミュレーションを行う。評価には実データを用いることで、日ごとや年単位での詳細な分析を可能とした。結果として、負荷平準化のために EV の充給電が貢献することが示された。
小林 正和	岡嶋 克典	車外環境の視認性を考慮した車内インターフェースの評価手法	本研究ではヘッドマウントディスプレイを用いたドライビングシミュレータを作成し、運転時における車内インターフェースと外環境の視認性評価を実施した。実験結果より、車内情報と外環境の視認性の両立という観点から車内インターフェースの安全性について議論する。

合田 明生	田村 直良	格の整合性に着目した小学生作文におけるねじれ文の検出と訂正	小学生の作文添削において、誤文訂正は一つの課題である。ねじれ文は、文法不具合で占める割合が高く問題となっている。そこで本研究では、ねじれ文の検出と訂正を目的とし、小学生作文指導の支援を目指す。ねじれ文を検出したところ、0.86のF値でねじれ文を検出できた。ねじれ文の訂正を行った結果として、元の文だと推測される文が得られた。以上の結果から、小学生作文中のねじれ文検出と訂正という面で、作文添削において重要であると言える。
齊藤 美織	吉岡 克成	セキュリティ通知の連絡先情報の収集に関する研究	サイバー攻撃の脅威の増加に伴い、観測された攻撃について関係者に注意喚起や情報提供を行うセキュリティ通知の重要性が高まっている。一般に、通知先の特定にはWHOIS等のサービスにより提供される情報が用いられるが、一部のサービスでは連絡先情報が頻繁に更新されないなど、通知時に正しい情報が取得できない恐れがある。本研究では、WHOISを含む様々な経路での通知連絡先の収集を提案した。収集した連絡先について、分類および通知実験を行うことにより、通知先として適切であることを示した。

佐保田 和宏	長尾 智晴	歩行型デバイスを用いた VR 空間の感性評価	VR を体験する際、ヘッドマウントディスプレイと呼ばれる装置を用いるのが主流となっている。近年では体験者自身がアクションすることで、VR 空間内を実際に動くような体験ができる装置も開発されている。これらのデバイスは現実感を体験者に与え、高度なシミュレーションが可能である。しかし、シミュレーションの種類が VR 酔い、没入感に与える影響は明らかではない。そこで本研究では歩行型デバイスを用いたシミュレーションを行うことでその有用性や、VR 酔いや没入感の感性評価を行う。
--------	-------	------------------------	---

塩本 龍昇	白川 真一	クラス情報を用いたバイナリハッシュによる類似画像検索の高性能化	バイナリハッシュはデータを2値のハッシュコードへ変換する手法であり、データ量の削減や比較演算の高速化が可能であることから、大規模な類似画像検索へ応用可能である。特に、2値のハッシュコードへの変換関数を機械学習によってデータから獲得する方法が様々提案されている。データのクラス情報が得られる場合、このバイナリハッシュ関数には同じクラスのデータには同じハッシュコードを、別クラスのデータには異なるハッシュコードを割り当てることが望まれる。本研究では、クラス情報に基づいてクラスの代表点を定義し、これを利用した適切なバイナリハッシュ関数を学習するための損失関数を提案する。顔画像データを用いた実験から、提案手法が既存手法よりも高い再現率を獲得できることを示す。
-------	-------	---------------------------------	---

柴山 航	白川 真一	強化学習を用いた VR 空間における効率的なリダイレクションの実現	リダイレクションは人間の錯覚を利用し、狭い現実空間内でも広大な VR 空間を自由歩行していると感じさせる技術である。本研究では強化学習を用いてリダイレクションを効率化する手法を開発する。実験では、既存研究では考慮されていない 2 メートル四方の現実空間や、障害物のある空間での評価を行う。リダイレクションの煩わしさや VR 酔いに繋がるとされる項目について、シミュレータ上では全ての現実空間設定で、また被験者実験では 2 メートル四方の現実空間設定において、既存手法に対して提案手法が高い性能を達成できることを示す。
嶋 宏晃	中本 敦浩	トーラス上の正則グラフの本型埋め込みについて	グラフの埋め込み方に関する問題として、本型埋め込みと呼ばれるものがある。これはグラフの頂点を本の背の部分に配置し、各ページに辺を交差しないように埋め込むときに、必要なページ数の最小値を考える問題である。本研究では、任意のトーラス上の 4 正則四角形分割と 6 正則三角形分割が 4 ページに埋め込めることを証明した。特に 6 正則三角形分割に関しては最善の結果を得ることができた。

白井 和樹	松本 勉	車載ネットワークにおける電 氣的データ改ざんの詳細解析 とセキュリティ強化策	最近の自動車は IT 技術の活用が盛んであり、自動運転技術 などが注目を浴びている。その一方で、自動車がサイバー 攻撃の対象となる危険性が高まっており、自動車の情報セ キュリティ技術の必要性が高まっている。本論文では車載 ネットワークの物理層における攻撃である、電氣的データ 改ざんの脅威を指摘する。また、この攻撃から自動車を保 護する手法についても考察する。
藺部 凧	白崎 実	2つの自由界面を有する液膜 挙動の大規模 CFD 解析	2つの界面を有する薄い液膜を持つ代表例であるシャボン 玉が流入する空気により膨らむ際の挙動について、大規模 CFD（計算流体力学）解析を行った。現象をより体系的に 評価するために、代表的な長さや流速との比率で表す無次 元計算による解析を行った。表面張力の影響の大小によっ て液膜の形状変化は大きく異なった。一方で、粘性力の影 響が大きいほど流入方向とそれに垂直な方向に交互に膨ら む周期が短くなり、各方向の径の大きさの差も小さくなる ことが分かった。

高石 一樹	長尾 智晴	時系列データの将来変動予測における予測根拠の提示	機械学習モデルを用いた時系列データの予測において、予測根拠を提示することは予測結果を意思決定に利用する上で重要である。本論文では、任意の時系列予測モデルに対して、局所近似手法である SHAP とトレンドフィルタを組み合わせるにより、トレンドベースで予測根拠の提示を行う手法を提案する。提案手法では、元の予測モデルに SHAP を適用して得られた寄与度の絶対値を入力値に掛けてからトレンドフィルタを適用することで、寄与度を考慮したトレンドベースの予測根拠提示を行う。実験では海運指数と原油価格予測問題に適用し、実際のトレンドを反映した予測根拠の提示が行われることを確認した。
-------	-------	--------------------------	--

高梨 雄大	長尾 智晴	進化計算法を用いた深層学習モデルの Pruning 最適化	<p>深層学習モデルを計算機リソースが少ない端末で直接利用するためにはモデルの圧縮が必要となるが、高い圧縮率の圧縮下では従来の圧縮手法である Pruning で高い精度を維持することは難しい。本論文では、Pruning で除去するパラメータを GA で最適化する手法を提案する。提案手法では、個体の圧縮率を固定する GA 操作の改変、計算コストを削減するために Fine-tuning 後のテスト精度を予測する Surrogate モデルを利用し、GA で Pruning の最適化した。実験では、CIFAR-10 データセットで学習した CNN に適用し、従来手法よりテスト精度が向上することを確認した。</p>
田村 隆吉	四方 順司	平文が秘密鍵に依存したハイブリッド暗号方式の安全性に関する研究	<p>ハイブリッド暗号を構成する方法として、弱い安全性の暗号から強い安全性の公開鍵暗号や KEM を構成する変換法がいくつか提案されており、その中の HHK 変換は NIST の耐量子暗号の標準化プロジェクトで提案されている構成の中で多く使用されている。一方、秘密鍵に依存した平文の暗号文を攻撃者が得ることができることを考慮した安全性として KDM 安全性が研究されている。本論文では、HHK 変換で提案されている KEM を用いたハイブリッド暗号が KDM 安全性を満たすかについて解析を行った。</p>

大用 拓也	岡嶋 克典	拡張現実感とクロスモーダル効果を用いた味覚の変調とその定量化	まず、拡張現実感を用いて食品の見た目を変えることで塩味を変調することが可能なクロスモーダル効果を定量的に検証した結果、塩味をより強く感じさせることが可能であり、この効果を食塩量に換算した。次に、異なる触覚情報を与えることによるうま味の変調が可能かについて検証し、一部の参加者には効果があったという結果となり、触覚情報を物理量で表し、うま味との関係を定式化した。さらに、食品を異なる種類の食品に見せることで参加者がどのように感じるかを検証した結果、一部の参加者にのみ影響があった。
道用 悠太郎	野間 淳	代数曲線のブローアップのみを用いた特異点解消コンピュータプログラム	特異点および特異点解消の理論は代数幾何学における主要な研究課題の一つであるだけでなく、統計学や情報科学への幅広い応用が期待されている統括的な手法でもある。本研究は、ブローアップのもつ計算の煩雑さを計算機アルゴリズムによって解決し、特異点解消の過程を「方程式の変換」そのものとして扱うことにより、ブローアップによる幾何対象の変化を初学者でも追って理解しやすい形で出力することを目標としている。

<p>永山 翔滋</p>	<p>森 辰則</p>	<p>人狼ゲームをプレイする自律エージェントの戦略に関する検討</p>	<p>本稿では「戦略、戦術を考慮した人狼エージェントの構築」を目指し、研究を行う。 特に人狼の戦術について考察し、その戦術を実現するために人間同士が実際に行った人狼ゲームの対話内容を分析した。 分析すべき観点は幾つかあるが、本研究では人狼の戦術である「ステルス人狼」と「ライン切り」の実現のため、「発話と勝率」、「人狼の連携」、「発話と行動」に着目した。</p>
<p>林 優樹</p>	<p>藤井 友比呂</p>	<p>自然発話コーパスに基づいた幼児日本語における Wh 疑問詞の基底位置に関する研究</p>	<p>本研究では、日本語の親と子の発話において「ナゼ類を含むかそれ以外の Wh 疑問詞を含むか」と「否定辞の有無」の二つを要因とした頻度クロス集計表について統計的分析を行った。その結果、親子の統計量を他の親子と比べたところ、親と子の間で同じような傾向を示すことがわかった。このことから子供が正しい文法を用いているのではなく、親の模倣をしているだけである可能性を示すことができた。</p>

早瀬 太一郎	中本 敦浩	平面グラフの符号付き染色数と剰余染色数について	<p>頂点彩色とは、隣接する頂点が異なる色となるようにグラフ全体を塗り分ける操作のことである。平面グラフの頂点彩色には最大4色が必要であることが知られている。頂点彩色をより一般化した彩色においては必要な色数は多くなる。例えば、平面グラフのリスト彩色においては最大で5色必要な場合があるが、グラフに適切な操作を施す事で色数を4まで減らすことができる。私は、このリスト彩色を更に一般化した彩色で同様の定理を示した。</p>
深野 巧也	富井 尚志	エネルギーライフログDBの再定義とそれを用いたピークシェーピングのための情報提示	<p>我々は先行研究で、エネルギー使用に関するライフログに対して情報検索ができるデータベースシステムであるエネルギーライフログDB(ELLDB)を構築し、その活用事例を積み上げてきた。本稿ではELLDBを需要電力の急激な変動を抑えるピークシェーピングのための情報提示を行えるDBとして再定義した。そして消費電力マネジメントとバッテリーマネジメントによってピークシェーピングが達成されることを示した。</p>

藤田 優一	松井 和己	縫合のモデル化とシミュレーション	<p>医学は物理現象としてはあまり評価されておらず，手術手技の力学的な評価する手法の開発が望まれている。</p> <p>そこで本研究では，縫合について着目し，縫合のモデル化の際に縫合糸と生体軟組織の接触部の摩擦がなく滑りが生じるものと仮定し，縫合について工学的知見から力学的状況を確認することを目的とした縫合のシミュレーションの開発を目指した。また縫合糸を棒要素，生体軟組織をソリッド要素としてモデル化した接触問題として表す手法を提案した。</p>
-------	-------	------------------	--

宗藤 大貴	長尾 智晴	進化計算法を用いた詰将棋の自動創作	<p>人工知能の発展により、様々な論理パズル問題を人間の事前知識なしで解く能力は年々向上している。しかし、パズル問題の創作に関しては、解が一つでないことや生成された問題の評価が難しいことから解答に比べ困難なタスクである。本稿では、パズル問題の中でも、持ち駒があるなどの性質から創作が難しいと考えられる詰将棋を題材とする。エキスパートによる詰将棋創作では、短手数 of 詰将棋や長手数の余詰めのある詰む局面の情報を利用する。この考え方に基づき、進化計算法の 1 つである遺伝的アルゴリズムによって、局面の変換を最適化することで長手数の詰将棋を生成する手法を提案する。実験の結果、最長で 33 手詰めの詰将棋が生成できることが確認できた。</p>
-------	-------	-------------------	---

森下 瞬	吉岡 克成	サイバー攻撃の対象となる機器の実態調査に基づく脅威分析	近年インターネット上で運用されている機器を狙ったサイバー攻撃が増加している。これらのサイバー攻撃の対象となる機器を調査するために、広域スキャン技術が研究開発されている。本研究では、広域スキャンの結果を用いて、実際の機器とハニーポットの応答の差異に基づくハニーポットの運用実態調査と、Telnet 開閉状況と IoT マルウェア感染状況に基づく IoT 機器の運用実態調査を行う。
山岡 哲平	小関 健太	連結 3-正則グラフのハミルトン数	連結なグラフにおいて、全ての頂点を通り始めの頂点に戻る最短の歩道の長さを Hamiltonian number といい、全ての頂点の次数が k のとき k -正則グラフという。辺連結度を仮定した 3-正則グラフの Hamiltonian number の上界は知られているが、辺連結度を仮定しない場合は自明でない上界が知られていなかった。そこで本修士論文では連結 3-正則グラフの Hamiltonian number の研究を行い、その最善の上界を与えた。さらに等号成立のグラフを特徴づけた。

奥秋 陽太	松本 勉	パイプライン型剰余乗算器を用いたペアリング暗号のFPGA実装に関する研究	<p>サイバーフィジカルシステムやクラウドコンピューティングのセキュリティ充実のため高機能暗号への期待が高まっている。暗号化したままデータベース検索が行える検索可能暗号や、複数のメッセージに対する署名検証を一括して行える集約署名は高機能暗号の具体例である。高機能暗号を実現するための主要構成要素は、計算コストの高いペアリング計算であり、パイプライン実装のモンゴメリ乗算器を用いたペアリング計算器により高速な計算が可能となった。本論文では、ペアリング計算器を改良したところ、254bit 素数 BN 曲線上の Optimal Ate ペアリングの計算時間記録を更新し、FPGA ボード VCU118 上では 61.0 μs, ML605 上では 153 μs が達成できたことを示す。</p> <p>高機能暗号実装の高速化に向けては、ペアリング計算の高速実装に加えて、任意のデータを楕円曲線上の点にマッピングする MapToPoint の高速実装も不可欠である。本論文では、複数のメッセージに対する MapToPoint 計算をパイプライン型剰余乗算器を用いて FPGA 上で計算することにより、ソフトウェア実装と比べ集約署名の検証を高速に実装できることを示す。</p>
-------	------	--------------------------------------	--

徐 楚煒	岡嶋 克典	没入型人流シミュレーションを用いた群衆の誘導手法に関する研究	本研究では、エージェントベースシミュレーションを用いて仮想群衆を生成し、群衆の中の一人として実験参加者が仮想空間に入り込み人流の一部となれるシステムを開発した。行動伝染によって、異なる人数の仮想群衆がシナリオを演じることを通して、仮想空間に没入した参加者の視線を意識的に誘導できるかを評価する実験を実施し、よりリアルな人流シミュレーションを可能にする手法とその知覚的効果について検証した。
曹 璐	四方 順司	メモリサイズを改善したアグリゲートメッセージ認証コードの実装と解析	本論文では、既存の追跡機能付きアグリゲートメッセージ認証コード方式を改良、もしくは、拡張するためのいくつかの考察を行う。特に、disjunct 行列を記憶するためのメモリの削減を目的として、テンソル積を利用した disjunct 行列の圧縮手法を提案した。また、有限体上の多項式を利用した disjunct 行列の構成例 (cover-free family) に対して、提案手法を適用した結果を定量的に示した。その結果、アグリゲート処理の時間計算量が増えるものの、従来よりも大幅に disjunct 行列サイズを圧縮できることを示した。

羅 璐	田村直良	サビ情報とニューラルネットワークの組み合わせに基づく中国の POP 歌の歌詞感情分析	ユーザーが好きな音楽を速く検索できるようにするために、中国の音楽ウェブサイトは、様々なトピックで音楽を分類しています。しかし、ネットの音楽リソースがますます多くなる、自動的に曲を分類する必要が有ります。他の音楽コンテンツと比較して、歌詞を利用した曲の感情分類が便利である。中国の流行歌の構造によると、主歌—サビの構造によると、サビは通常 1 曲の感情を表す重要な部分である。本稿では、曲のサビの部分を自己相似行列により抽出し、歌詞に対してサビのベクトルを構成し、サビのベクトルを用いて歌詞の感情的な部分を強調する、これを単語ベクトルおよびニューラルネットと結合して手法を提案する。実験の結果、一般的なニューラルネットの方法に比べ、提案手法 4%—6%の精度向上した。
-----	------	--	---