令和６年度

# 修士論文要旨集

高知大学大学院　総合人間自然科学研究科

理工学専攻 情報科学コース

# 大規模言語モデルを利用した強化学習アルゴリズム

情報科学コース　　片岡　華瑠

強化学習は，エージェントと呼ばれる学習者に，与えられた環境内で試行錯誤を行わせながら，エージェントに最適な行動方策を学習させることを目的とした機械学習の一手法である． 学習を行う過程において環境内の様々な情報（状態）を受取り，あらかじめ設定された報酬と呼ばれるパラメータを長期的に最大化するような行動をエージェントに選択させることで行動を最適化する．

近年，ボードゲームやビデオゲームにおいて人間のプレイヤーに匹敵もしくは凌ぐほどの性能を示すような機械学習の成果が示されている．機械学習における教師あり学習と比較して，強化学習には学習過程の初期にある程度の有効な行動選択を行えるようになるまで膨大な回数の試行錯誤を繰り返す必要が求められる課題がある． この課題に対して，内発的な報酬とよばれる別の形態の報酬を設定することで学習を効率化する手法などが行われている．

一方，大規模言語モデルの発展に伴い，それらを強化学習に取り入れることで学習を効率化する研究も行われている． それらの研究では，大規模言語モデルによる選好に基づいて報酬関数を設計する手法や大規模言語モデルにより直接報酬関数を設計する手法が行われている． しかし，高い性能が示されている大規模言語モデルの行動計画能力を効果的に活用し，強化学習の学習過程を汎用的にアシストできるような手法は多くない．

本研究では，強化学習の学習過程において大規模言語モデルにエージェントの行動選択方策の一部をサポートさせることで，エージェントが短期間で最適な行動を行える手法の実現を目標とした．この手法では，大規模言語モデルの応答速度がネックとなり，従来の強化学習の手法と比べて学習時間が増加することが予想されるため，Random Network Distillation (RND)アルゴリズムを併用して，学習時間増加の抑制を図った．具体的には，RND により状態の新規性を評価し，新規性が高い状態と判断される状態では大規模言語モデルからの提案を多く採用し，新規性の低い状態では従来の強化学習による行動決定を行わせた．これにより，エージェントの学習が不十分な学習過程の初期に報酬を充分に獲得できない状況下でも大規模言語モデルのサポートを活用することで学習進捗を停滞させず効率的に進ませることが期待できる．

実験を行った環境として，ランダムに生成されたステージ内においてエージェントが指定された条件をクリアすることを目的としたビデオゲームを利用した．この環境下において提案手法とそれ以外の手法の比較を行い，学習時間が短縮される場合があることを示した．さらに，標準的な強化学習アルゴリズムと比較し，試行錯誤の回数あたりの学習の進捗状況から，サンプル効率の改善が見られることを確認した．

# 楕円曲線暗号に用いるヒルベルト類多項式の中国剰余定理を利用した計算法の実装

情報科学コース　　中村　佳祐

現代では技術革新により，場所や時間を問わず様々な人とのリアルタイムな通信が可能になっている．通信の安全性は暗号によって支えられており，RSA 暗号や楕円曲線暗号といった公開鍵暗号の存在が大きい．

本研究では楕円曲線暗号で重要な CM 法に着目した．CM 法は楕円曲線暗号に適した曲線を生成する方法であり，ペアリング暗号や同種写像ではより複雑に楕円曲線の構造を制御するために必須となる．本研究室では，2006 年の太田，塩田による研究にてペアリング暗号の一種である Weil 対を用いた暗号系に適した楕円曲線の生成アルゴリズムを提唱した．Weil 対は楕円曲線の $n$ 分点 $E[n]$ に対して定義される写像である．この研究では，CM 法を改良して $E[n] \subseteq E(\mathbb{F}_p)$ を満たす楕円曲線や，より一般に $E[n] \subseteq E(\mathbb{F}_{p^\ell})$ を満たす楕円曲線の生成アルゴリズムが提唱された．2023 年の境野，塩田による研究では同種写像暗号による暗号系の効率の良い構成を提唱した．同種写像暗号は耐量子計算機暗号の一種であり，近年とても注目されている．同種写像暗号では $E[2^m3^n]$ のような小さな素数べきからなる等分点を制御する必要があり，こちらも CM 法が必須となる．CM 法ではヒルベルト類多項式 $H_D(X)$ の根が $j$ 不変量となる楕円曲線を生成する．ヒルベルト類多項式は元来，解析的に定義されている．しかし，その定義通りの構成法では多項式のパラメータである判別式 $D$ の値が大きくなると巨大な桁数の複素数の高精度計算が必要となり，長大な時間がかかることが問題点であった．そこで本研究では，Andrew V. Sutherland により提唱されたアルゴリズムを実装することで，より大きな $D$ に対しても問題なく扱えるヒルベルト類多項式の生成プログラムの作成を目指した．

Sutherland によるアルゴリズムの概略は以下の通りである．判別式が $D$ の 虚 2 次の整数環 $O_D$ に対して，一定の条件を満たす比較的小さな素数 $p$ を必要な個数だけ集める．集めた各 $p$ に対して，準同型環が整数環 $O_D$ となるような $\mathbb{F}_p$ 上の楕円曲線の $j$ 不変量をすべて求めることができる．それらの $j$ 不変量を根にもつ一次式を $\mathbb{F}_p$ 上で掛け合わせることで $H_D(X) \bmod p$ を構成できる．各 $p$ に対して求まった $H_D(X) \bmod p$ の係数に対して，次数ごとに中国剰余アルゴリズムを適用することで $H_D(X)$ を求めることができる．

この手法を評価するため，Python を用いて解析的な構成法と中国剰余アルゴリズムによる構成法を実装した．以下では，解析的な構成法を「解析的な手法」，中国剰余アルゴリズムによる構成法を「CRA による手法」と呼ぶ．ヒルベルト類多項式の計算時間は $D$ の大きさだけでなく，類数の大きさが強く影響している．そこで $D$ の bit 長を固定し，類数を変化させることで 2 方法を比較した．結果，CRA による手法は解析的な手法に比べ約 6 倍ほどの速さで実行できることが確認できた．類数が増大すると，2 手法の差はより開いていく．

加えて，C++と Java による実装も行った．3 言語で実装された CRA による手法に対して同じ判別式で計算を行うことで，言語間の優位性を明らかにした．実験の結果 Java が最も早く，$D$ が 17bit で類数が 138 の場合，Python に比べ約 11 倍ほどの速さで動作することを確認した．

Java の優位性が明らかになったため，Java を用いて CRA による手法の計算時間の大まかな見積もりを算出した．$D$ の bit 長が同じでも類数には大きなバラつきが見られる．そこで，$D$ の bit 長ごとに類数の最大値，最小値，平均値を計算した．その結果，類数が各 bit 長での平均以下であれば，$D$ が 16bit 程度までは十数秒ほどで動作することが多いと確認できた．類数が最小に近ければ，21bit までであれば数十秒で動作した．また大きい bit 長と類数に対しては，約 10 時間で $D$ の bit 長が 21 で類数が 2768 ほどの場合も計算が可能である．$D$ が 22bit の際，類数が最大の場合の計算時間は最小の場合と比べ約 950 倍ほどかかった．この結果から，ランダムにヒルベルト類多項式を生成する場合に類数の制限をかけることの有効性を示した．

# スピーカアレイを用いた視覚障害者への情報提示装置　― 複数スピーカを用いた物理現象提示の検討 ―

情報科学コース　　酒井匡章

視覚障害者が文字や図形などの視覚的情報を得る手段として，触覚や聴覚を用いた代替手段が存在する．文字などの言語化可能な情報に関しては，音声読み上げソフトや点字により情報へのアクセスが比較的緩和されている．また，図形などの言語化が困難な情報は，触図によりその形を視覚障害者へ提示することが可能である． 視覚障害者の教育現場である盲学校では，様々な物理現象や生物の構造などを理解するために触図が用いられている．しかし，触図による表現は万能ではない．触察によって読み取れる情報の量と質は触察能力に依存し，その触察能力自体も多くの訓練時間によって培われるものである．さらに，触図は静的なものであるため，時間によって変化する動的情報を含んだ図形の表現が困難である．

教育において動的情報は，物理現象の概念の理解に欠かせないため，触図とは異なった新たなアプローチで動的情報を含んだグラフィカルな情報を視覚障害者に提示する方法，あるいは，触図と組み合わせることで触図の強みを活かしつつ触図の制約を緩和する方法が必要である．

そこで，本研究室では，音のもつ直感的かつ柔軟性に富んだ特性に着目し，複数のスピーカを用いて音像を移動させることで，触図では表現困難な動的情報の表現をしつつ，即時の認識が可能な情報提示装置“スピーカアレイ”を開発した．

本研究では，センター試験の点訳問題を視覚障害者に解かせた関連研究から視覚障害者が直面する課題を確認し，中等教育で学習する 2 物体の衝突運動の表現をスピーカアレイで行った．先行研究では，ホワイトノイズを用いて動的情報の提示が試みられた．しかし,2 物体の衝突運動をホワイトノイズのみで提示するには，ユーザの負担が大きい．そこで，ホワイトノイズと 770[Hz]を基本周波数とする複合音を 2 物体にみたてて表現することにした．また，本研究は，先行研究で製作されたスピーカアレイではシステムの機能・性能から困難であったため，新たなスピーカアレイを製作した．

初期実験としてある音源が存在する場合，異なる音源の移動が認識できるかの検証を行った．ホワイトノイズと 770[Hz]を基本周波数とする複合音のいずれかを移動させたパターンにおいて，被験者は，ホワイトノイズを移動させた方が移動を分かりやすいと回答した．一方，複合音を移動させる場合，音の途切れを感じるといった意見があった．これは，新たに製作したスピーカアレイのシステムによるものだと考えたため，先行研究の疑問点であったスピーカを切り替える際のクリック音の有無による音の移動感の検証をした．検証結果からクリック音を知覚できる場合，クリック音を印可した方が音移動・音源定位において優位であった． しかし，被験者がクリック音を手がかりとして音移動を認識しているならば，スピーカアレイのメリットである音の提示時間のコントロールが難しくなるため，印可した場合における速度感について検証を今後行う必要がある．

衝突運動の提示実験で，ある被験者は，2 音源の移動はわかったが，衝突に至る前に，音源が離れていると回答した． スピーカアレイのメリットとしてユニットを空間上の任意の位置に配置できるため，衝突運動の追実験として，スピーカの配置間隔によって被験者のもつイメージにより近づけるかを検証した．空間的連続性に考慮した配置・衝突が発生するユニットを密着・衝突の際 2 音源を 1 つのユニットから同時に再生する誇張表現の 3 つのパターンで実験を行った．結果として，ユニットを密着させるパターンが高い評価を得た．

以上の実験よりスピーカアレイによる 2 物体の衝突運動の表現とクリック音の印可に関する知見が得られた．今後の課題として，本研究は水平方向の衝突運動のみに焦点を当てているため，垂直方向に関する検討を行う必要がある．