



研究者名※	中島 徹 NAKASHIMA Toru	学位※	博士(理学)
所属※	理学部 数物情報科学科	職名※	教授
連絡先	nakashima@fc.jwu.ac.jp		
URL			
researchmap※	<a href="https://researchmap.jp/read0132287">https://researchmap.jp/read0132287</a>		
研究分野※	代数学、情報学基礎理論、情報セキュリティ		
研究キーワード※	代数幾何、情報数理、暗号		
共同研究・競争的資金等の研究課題	adelicベクトル束を用いた代数幾何符号の研究(科学研究費・基盤研究C(一般)・研究代表者、2020~2023年)		
社会貢献・産学官連携活動等			
受賞歴			

研究領域	代数幾何、符号理論	(SDGs)
研究テーマ※	adelic幾何を用いた誤り訂正符号の研究	
概要※ (概ね1000字以内) (写真・グラフ等自由)	<p>【研究の背景・目的・内容】 現代の情報通信では、情報の送信の過程で生じた誤りを訂正するために誤り訂正符号の技術が用いられているが、中でも代数幾何の手法を用いて構成される代数幾何符号は高い性能をもつことが知られている。Goppaによる最も初期の代数幾何符号では、有限体上定義された代数曲線と因子を用いて符号を定義していたが、近年になり、高次元の代数多様体上のベクトル束を用いたSavin符号の構成法が提案されるようになった。</p> <p>一方、体上の代数多様体に関して得られた諸結果を算術的多様体と呼ばれる代数体の整数環上のスキームに一般化するArakelov幾何学の研究が近年急速な発展を遂げている。当研究代表者の中島は、代数体と関数体の類似の哲学に基づき、算術的多様体上のエルミートベクトル束を用いたArakelov符号を導入した。しかし、有限体上の符号とArakelov符号の相互関係については研究が進んでいなかった。</p> <p>最近、森脇-Chenによって有限体上の代数多様体と算術的多様体を一般化するadelic曲線の概念が導入された。当研究の目的は、彼らの構築したadelic幾何学の手法を用いることによってSavin符号とArakelov符号を統一するadelic符号を定義して次元や最小距離などのパラメータを決定し、その性能を解明したい。</p> <p>【応用例、研究の展望】 当研究によってadelic幾何学の観点から従来の代数幾何符号を統一的に理解することが可能になり、符号相互の関連が明らかになると思われる。また、従来よりも高い性能を備えた新しいタイプの代数幾何符号を構成することが可能になることが期待される。もしこのような符号の構成に成功すれば、量子コンピュータに於いて必要となる効率の良い量子誤り訂正符号の構成に応用があるのではないかと考えられる。また、adelic符号に基づくMcEliece型の公開鍵暗号の構成への応用も期待される。</p> <p>【研究方法の特色】 従来情報分野の研究に於いて用いられなかったadelic幾何という新しい幾何学を誤り訂正符号に応用し、新しい符号の構成に応用しようという点に当研究の特色があると考えられる。</p>	
本研究関連特許・論文等	<ul style="list-style-type: none"> <li>・Construction of codes from Arakelov geometry, T.Nakashima, Des.Codes and Crypt. 73, 47-54(2014)</li> <li>・AG codes from vector bundles, T.Nakashima, Des.codes and Crypt. 57, 107-115(2010)</li> </ul>	
共同研究・外部機関との連携への期待		