様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

令和　６ 年　 ５ 月 １６ 日現在

機関番号：１２６０８
研究種目：挑戦的研究（萌芽）
研究期間：2019～2023
課題番号：１９Ｋ２２８６５

研究課題名（和文）深層学習モデル間の演算体系確立と大規模分散学習への応用

研究課題名（英文）Towards an Algebra for Distributed Deep Neural Networks

研究代表者
井上　中順（Inoue, Nakamasa）

東京工業大学・情報理工学院・准教授

研究者番号：１０７３３３９７

交付決定額（研究期間全体）：（直接経費）　　5,000,000円

研究成果の概要（和文）：画像や音声の理解を目的とした深層学習技術は、高度な情報化社会において必要不可欠なものとなっている。本研究では、複数のニューラルネットワークが協調的あるいは敵対的に学習する仕組みに関する成果が得られた。主な成果は、Augmented Cyclic Consistency Regularizationと呼ばれる生成的敵対ネットワークの新しい正則化手法、二次の準ニュートン法を用いた敵対的サンプル生成手法、ステップ幅の正則化手法の３つである。これらの有用性を画像および音声の実データで示し、それぞれ国際会議で成果発表をおこなった。

研究成果の学術的意義や社会的意義
本研究の成果は実社会で活用されている画像認識・画像変換、音声認識・音声話者照合システムの高度化に貢献するものである。また、学術的には新たな学習アルゴリズムが情報工学分野、特にパターン認識およびニューラルネットワークの深層学習に貢献するものである。

研究成果の概要（英文）：Deep learning technology for understanding images and audio has become essential in an advanced information society. In this project, results were obtained regarding a mechanism in which multiple neural networks learn cooperatively or adversarially. The main achievements include a new regularization method for generative adversarial networks called Augmented Cyclic Consistency Regularization, an adversarial sample generation method using a second-order Quasi Newton method, and a step size regularization method. The effectiveness of these methods was demonstrated using real image and audio data, and the results were presented at international conferences.

研究分野：パターン認識

キーワード：深層学習

様　式　Ｃ－１９、Ｆ－１９－１（共通）

１．研究開始当初の背景

画像や音声の理解を目的とした深層学習技術は、高度な情報化社会において必要不可欠なものとなっている。研究当初、単一のニューラルネットワークを用いた学習方法が画像や音声のパターン認識に有効であることが知られており、複数のニューラルネットワークが協調的に学習する仕組みは萌芽的であった。

２．研究の目的

本研究の目的は、深層学習で得られるモデル間の演算を可能とする体系の構築である。大量の計算機で独立に学習されたモデルの事後的統合を可能とすることを目指して研究を実施した。最初の２年間で、画像変換に関する識別的ニューラルネットワークと生成的ニューラルネットワークを協調的に学習させる方法に関する成果が得られたため、３年目からは当初の研究計画を修正し、ニューラルネットワーク間の協調性や敵対性に関する研究を中心に実施をおこなった。

３．研究の方法

最初の２年間は画像認識および画像変換に関する畳み込みニューラルネットワークを対象として実験を実施した。具体的には、ImageNet データセットと ResNet, U-Net を用いたニューラルネットワークのパラメータ空間での加減算を試作、また複数のニューラルネットワークを同時に学習する方法と独立に学習する方法に関する実験を実施した。その成果は４－１の通りである。

３年目以降は得られた研究成果をさらに発展させる方針へと軌道修正を行い、音声データへの適用実験として、音声認識および話者照合の実験を実施した。そこで、話者照合に対するメタ学習・敵対的学習・敵対的攻撃性の評価に関する実験結果が優れていることが明らかとなったため、それらの実験を重点的に実施した。得られた成果は４－２と４－３の通りである。

４．研究成果

４－１．Augmented Cyclic Consistency Regularization

近年の生成的敵対ネットワーク（GAN）の進歩により、画像間変換（Image to image translation, I2I）はパターン認識およびコンピュータビジョン分野で大きな注目を集めている。しかし、明示的な教師信号が存在しないため、ペアデータを用いない方法で学習された I2I モデルは、現実的な画像を生成することに失敗することが多く、特に異なる背景やポーズを含む難易度の高いデータセットにおいてその傾向が顕著である。このため、GAN および I2I 変換の応用において安定化は不可欠である。そこで、本研究では、I2I 変換のための新しい正則化手法である Augmented Cyclic Consistency Regularization（ACCR）を提案した。我々の主な着想は、半教師あり学習に由来する一貫性正則化を実サンプル、偽サンプル、再構成サンプル、および拡張サンプルを活用して識別器に適用することである。元の画像と摂動された画像のペアが入力された際に、識別器が類似した予測を出力するように正則化する。我々は、偽サンプルおよび再構成サンプルに対する一貫性正則化が有効である理由を質的に明らかにし、定量的には、我々の手法が一貫性正則化された GAN（CR-GAN）を現実世界の変換において上回り、いくつかの従来手法と比較してその有効性を示した。

この方法は図１に示す通り、２つの生成器と２つの識別器を持つ画像変換モデルを構築し、それらのパラメータ間に相関を持たせる方法である。これは、深層学習モデルを効率的に合算することを目的としたものである。生成器と識別器という異なるニューラルネットワークの出力に一貫性を持たせる正則化を導入することで、学習を安定化させることが可能となることが明らかとなった。具体的には、２つの生成器を G1,G2、２つの識別器を D1,D2 とした時に、G1-G2 出力間、D1-D2 出力間、G1-D2 出力間、G2-D1 出力間の平均二乗誤差が小さくなるような項を学習時に加えることで、画像変換モデルが学習初期の段階から安定化した。表１に示す通り、出力側にのみに一貫性を持たせる従来手法に比べて、画像変換の精度が向上すること、特にノイズや入力の変動に頑健であることが確認された。表は CycleGAN, CR-CycleGAN は従来手法との比較として、MNIST (M), MNIST-M (MM), SVHN (S)という３つの画像データセット間の画像変換精度を示したものである。本研究の成果はパターン認識分野のフラグシップ国際会議である International Conference on Pattern Recognition (ICPR)に採択され、発表をおこなった。

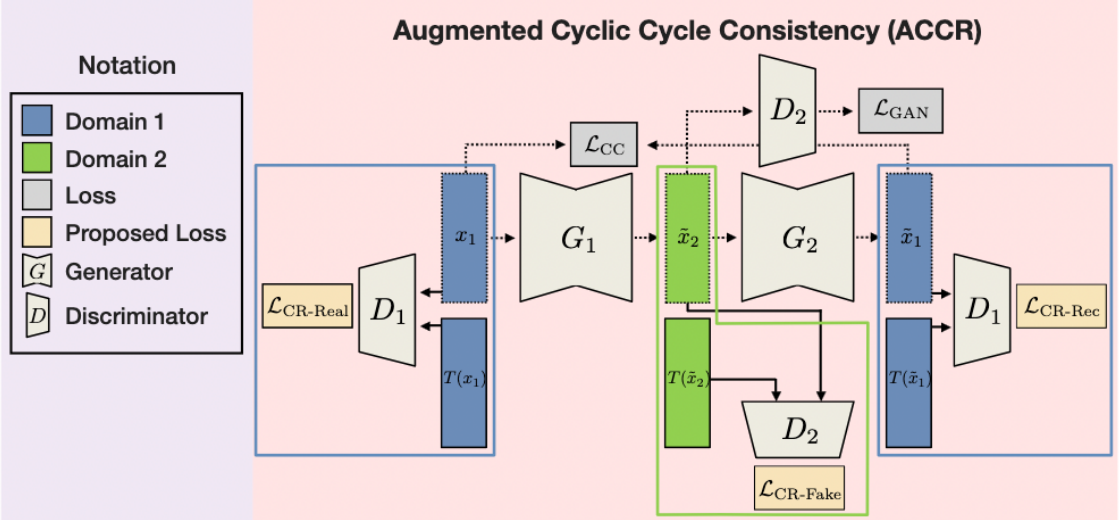

図１．ACCR を用いた学習の構成図

表１．性能の評価

Model	M → MM	MM → M	M → S	S → M
CycleGAN	97.7 ± 0.3	92.2 ± 1.2	47.1 ± 3.1	28.2 ± 0.9
CR-CycleGAN	97.7 ± 0.6	94.3 ± 0.5*	43.7 ± 4.1	29.6 ± 0.7
CR-CycleGAN + CR-Fake (Ours)	97.7 ± 0.3	93.8 ± 0.7*	46.3 ± 4.7	**31.9 ± 3.0***
CR-CycleGAN + CR-Rec (Ours)	97.6 ± 1.2	94.2 ± 1.4*	48.5 ± 3.0	30.5 ± 1.7*
ACCR-CycleGAN (Ours)	**98.0 ± 0.5**	**94.5 ± 0.5***	**51.0 ± 5.2**	**31.9 ± 1.6***

４−２．準ニュートン法を用いた敵対的攻撃法

前述の画像に関する GAN に関する成果を音声分野に応用する研究を進めた結果、話者照合システムに対する敵対的発話の生成に関する成果が得られた。具体的には、二次の準ニュートン法を用いた敵対的発話生成フレームワークを提案した。我々の主なアイデアは、話者照合モデルの性能に大きく関与する敵対的発話を生成する最適化問題を定式化し、それを二次最適化手法で解くことである。まず、一次のガウスニュートン法を用いるアルゴリズムを構築し、その後、二次の準ニュートン法に拡張をおこなった。我々の実験では、大規模データセットである VoxCeleb データセットを用いて提案手法が従来の手法よりも小さい摂動で話者照合システムの出力を逆転させることができた。また、二次最適化手法が小さな摂動を見

つけるのに効果的であることも明らかとした。実験結果は表２に示す通りで頑健性を示す指標 ρ が従来手法の MFCC-ivec Attack よりも顕著に改善され、ガウスニュートン法よりも優位であることが分かる。本成果は国際会議 Asia-Pacific Signal and Information Processing Association Annual Conference (APSIPA ASC)に採択され、発表をおこなった。

表２．話者照合システムに対する頑健性評価

Method	Average		Worst	
	$\bar{\rho}_1$	$\bar{\rho}_2$	$\bar{\bar{\rho}}_1$	$\bar{\bar{\rho}}_2$
MFCC-ivec Attack [7]	9.91	6.94	15.24	10.59
Gauss-Newton Attack	0.27	0.49	2.58	4.80
Quasi-Newton Attack (DFP)	**0.24**	**0.43**	**1.83**	**3.18**
Quasi-Newton Attack (L-BFGS)	**0.24**	**0.43**	1.85	**3.18**

４−３．ステップ幅の正則化方法

前述の話者照合モデルに対する敵対的攻撃で成果が得られたため、この研究をさらに発展させ、話者照合モデルに対する敵対的攻撃の応用において、反復最適化プロセスのステップサイズを自動的に制限するアルゴリズムを提案した。提案のアルゴリズムは、図２のように各反復においてテイラー近似を適用する制限半径 r を持つ部分空間を動的に決定し、投影勾配法を用いて部分空間内の線形問題を解くものである。実験では、i-vectors、SE-ResNet-34、および ECAPATDNN の 3 つの話者照合モデルに対する敵対的攻撃で提案手法の有効性を実証した。その結果、表３に示す通り、提案アルゴリズムによって生成される敵対的摂動の程度が従来の攻撃手法によって生成されるものよりも小さいことが分かった。

本成果は音声信号処理分野で最も著名な国際会議である International Conference on Acoustics, Speech, and Signal Processing (ICASSP)に採択され、発表をおこなった。

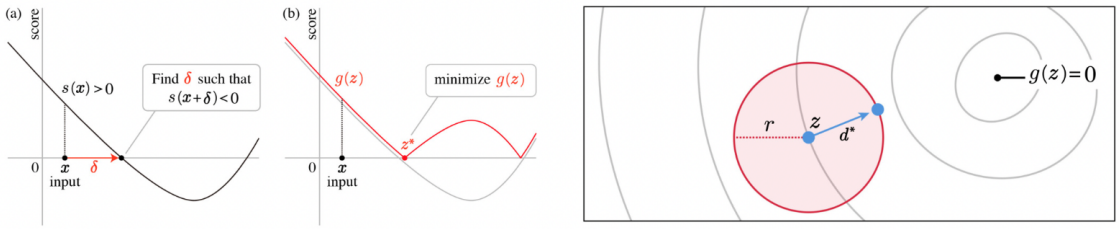

図２．ステップ幅最適化方法の概要

表３．頑健性評価結果

Method	Model	SR	Relative perturbation degree			
			$\bar{\rho}_1$	$\bar{\rho}_2$	$\bar{\bar{\rho}}_1$	$\bar{\bar{\rho}}_2$
Li *et al.*	i-vector	91.32	9.91	6.94	15.24	10.59
	ResNet	67.38	4.81	2.89	37.78	22.61
	ECAPA	71.31	4.81	2.89	37.78	22.61
Ours	i-vector	**100.0**	**0.24**	**0.43**	**1.68**	**2.74**
	ResNet	**100.0**	**0.20**	**0.17**	**2.20**	**1.86**
	ECAPA	**100.0**	**0.22**	**0.20**	**1.88**	**1.65**

５．主な発表論文等

〔雑誌論文〕　計0件

〔学会発表〕　計2件（うち招待講演　0件／うち国際学会　2件）

１．発表者名 Nakamasa Inoue, Keita Goto
２．発表標題 Optimizing Speaker Embeddings using Meta-Training
３．学会等名 APSIPA（国際学会）
４．発表年 2021年

１．発表者名 Keita Goto, Nakamasa Inoue
２．発表標題 Quasi-Newton Adversarial Attacks on Speaker Verification Systems
３．学会等名 APSIPA（国際学会）
４．発表年 2021年

〔図書〕　計0件

〔産業財産権〕

〔その他〕

―

６．研究組織

	氏名 （ローマ字氏名） （研究者番号）	所属研究機関・部局・職 （機関番号）	備考

７．科研費を使用して開催した国際研究集会

〔国際研究集会〕　計0件

８．本研究に関連して実施した国際共同研究の実施状況

共同研究相手国	相手方研究機関