

敵対的訓練を利用したドメイン不変な表現の学習

Learning Domain-Invariant Representations by Adversarial Training

岩澤 有祐^{*1} 矢入 郁子^{*2} 松尾 豊^{*1}
 Yusuke Iwasawa Ikuko Yairi Yutaka Matsuo

^{*1}東京大学工学系研究科 The University of Tokyo
^{*2}上智大学理工学研究科 Sophia University

This paper investigates neural network based model for domain generalization: how to acquire knowledges, which is useful for previously unseen domains, from an arbitrary number of related domains. We propose the use of adversarial training framework to learn domain invariant representations, whilst preserving the functional relationship between input and output variables. The proposed method considers both an adversarial domain classifier and a regular label classifier during training, which allows the model to learn representations that help the classifier to distinguish label but which, at the same time, prevents it from becoming domain-specific representations. This paper provides empirical validations of the efficacy of the proposed method using activity recognition tasks based on data of wearables, which is typical case that requires domain generalization.

1. はじめに

ドメイン汎化 (domain generalization) とは、未知のドメインに対して有用な知識を、任意の数の関連ドメインのデータから獲得するような問題設定のことである [Blanchard 11]. 例えば、ユーザが持ちうるスマートフォンに搭載された加速度センサにより転倒を検知する転倒検知問題を考えてみる. この問題を解く最も単純な方法として、転倒したという事例に関する教師データを付与した上で教師あり学習を行う方法が考えられる. しかし、「転倒した」という事例は珍しく、すべてのユーザから転倒事例を取得することは現実的ではないだろう. この問題を効率的に解くためには、転倒事例が集められないようなユーザ (すなわち未知のドメイン) に対しても有効な分類器を、転倒事例が存在する限られたユーザの訓練事例のみから構築する、即ちドメイン汎化を行う必要がある.

本稿では、ニューラルネットワークと敵対的訓練 (adversarial training) を組み合わせることによりドメイン汎用な表現を学習する方法を提案する. 提案手法は、ドメイン汎用である必要があるラベル分類器 f_y への入力となる特徴量 r を出力する特徴抽出器 f_f を学習する際に、 f_y からラベル y を予想しやすくなるのと同時に、 r からドメイン $d \in \{D_1, D_2, \dots, D_K\}$ を識別しようとする分類器 f_d がドメインを予想できなくなる方向に f_f を学習させるというものである. このように学習時に表現のドメイン依存度を計測し、またその依存度を下げる方向に表現を修正することで、学習される表現 r がドメインによらず類似するようになり、結果としてラベル分類器の出力 f_y の出力もドメインに依存しないものになることが期待される.

本稿では提案手法の有効性を、ドメイン汎化が必要となる典型例である、慣性センサを利用した行動認識におけるユーザ汎化の問題設定において検証する. 具体的には、本稿では下記のとおり2つの検証結果について報告する.

- 提案手法により、学習される特徴量の単純なディープネットと比較してドメイン不変性の高い表現を学習できること.
- よりドメインに不変な特徴量を学習する提案手法により、

未知のドメインに対する汎化性能が改善すること.

2. 関連研究

提案手法のアイデアは、特徴量 r からドメイン d を予想しようとする識別器 f_d を騙すように、特徴抽出器 $f: X \rightarrow R$ を学習させることでドメイン汎用な表現を学習することである. すなわち、提案手法は識別器 f_d がどの程度 r から d を予想できるかを特徴量 r のドメイン不変性の指標へと利用する.

筆者が知るかぎり、敵対的訓練アプローチは Schmidhuber により初めて利用された [Schmidhuber 92]. より近年の研究で、Goodfellow らは敵対的訓練による方法を画像生成タスクに利用し [Goodfellow 14], さまざまな研究による改良がなされている [Denton 15]. 提案手法により近い研究として、Ganin がドメイン適応の文脈で提案した Domain-Adversarial Neural Networks (DANN) [Ganin 14] と Edwards が表現から機微情報を取り除くための手法として開発した Adversarial Learned Fair Representations (ALFR) がある [Edwards 16]. これらはある特徴量が何らかの情報 S (前者はドメイン, 後者は機微情報) に依存しないように学習するという点では提案手法と類似しているが、学習される特徴量のドメイン依存性を低下させることを目的とする本手法とは異なる目的で開発されているものである. また、従来研究はドメインや機微情報 S として2クラスを想定するのに対して、本稿が取り扱うドメイン不変な表現を獲得する問題ではドメインの集合 D は一般に多クラスとなるという点で異なる問題設定を扱っており、より一般的な問題設定における検討を行ったこと、またその問題点の考察を行ったことに本稿の新規性がある.

3. 提案手法

提案手法では、ドメイン汎用な認識モデルを学習するために次のような2つの損失関数の同時最適化問題を解く.

$$L = L_y(X, Y) + \lambda L_d(R, D). \quad (1)$$

ここで、 L_y, L_d は特徴量 R が持つラベル Y に関する情報の大きさおよびユーザ D に関する情報の小ささを表す損失関数

連絡先: 岩澤有祐, 東京大学工学系研究科技術経営戦略学専攻, iwasawa@weblab.t.u-tokyo.ac.jp

であり, λ はその重みである. 以降, この最適化問題を順伝播型ニューラルネットで解く提案手法について説明する.

3.1 提案手法の構造

図 1 に提案手法の概要を示す. 参考までに, 通常の順伝播型ニューラルネットワークを横に並べた. 図中矢印は, 順伝播パスおよび逆伝播パスを意味している. 提案手法は, 通常のニューラルネットワークが持つ 1. 特徴抽出器 $f_f: X \rightarrow R$, 2. 分類器 $f_y: R \rightarrow Y$ に加えて, 3. 敵対的ドメイン分類器 $f_d: R \rightarrow D$ の 3 つのニューラルネットワークにより構成される. ここで, f はそれぞれ任意の構造を持つニューラルネットワークであり, それぞれ $\theta_f, \theta_y, \theta_d$ のパラメータを持つ. 提案手法では, これらの 3 つのニューラルネットワークを利用して L_y および L_d を定量化する.

3.2 $L_y(X, Y)$ の定量化

L_y は, 通常のニューラルネットワークと同様の方法で求める. すなわち, X と Y の間で定義される交差エントロピーを最小化することで求める. 交差エントロピーによる損失関数は, 定式的には次の式ようになる.

$$L_y = -\frac{1}{N} \sum_{n=1}^N \sum_{m=1}^M y_{nm} \log f_y(f_f(x_n)). \quad (2)$$

ここで, N は学習サンプル数, M は分類したいクラスの数, y_{nm} はサンプル n が m 番目のクラスであるかを表す $\{0, 1\}$ の値である. 特徴抽出器および行動分類器は確率変数 X から Y が予想しやすいようにする. すなわち式 2 を最小化するようにパラメータ θ_f および θ_y を修正する.

3.3 $L_d(R, D)$ の定量化

L_d の定量化には敵対的訓練を利用する. 具体的にはまず, 変数 R から D を予想しようとするような敵対的分類器 f_d を考える. これは, f_d を任意の構造のニューラルネットワークとすると, 次の損失関数を最大化することにより実現できる.

$$L_u = \frac{1}{N} \sum_{n=1}^N \sum_{k=1}^K u_{nk} \log f_u(f_f(x_n)). \quad (3)$$

ここで, K は学習に利用できるドメインの数, u_{nk} はサンプル n が k 番目のドメインのサンプルであることを表す $\{0, 1\}$ の値である. ドメイン分類器は, 確率変数 R からドメイン D を予測するように関数 f_d を学習する. これは, 形式的には特徴抽出器 f_f のパラメータである θ_f を固定した上で, 式 3 を最大化するようにパラメータ θ_u を更新することと対応する.

逆に, 特徴抽出器は, 敵対的分類器が確率変数 R からドメイン U を学習できないようにする, これは形式的には, 敵対的ドメイン分類器 f_d のパラメータ θ_u を固定した上で式 3 を最小化するようにパラメータ θ_f を更新することで実現できる. また, 概念的には特徴 R から U を予想するような敵対者を想定した上で, その仮想的な敵対者が情報を抽出できないように f_f を修正することに対応する.

3.4 最適化

まとめると, 提案手法は 1. 特徴抽出器 f_f , 2. 行動分類器 f_y , 3. 敵対的ドメイン分類器 f_d の 3 つの要素から構成され, 最終的な最適化問題は式 4 のようになる.

$$\min_{\theta_f, \theta_y} \max_{\theta_u} [L_y(X, Y; \theta_f, \theta_y) + \lambda L_d(R, U; \theta_f, \theta_u)]. \quad (4)$$

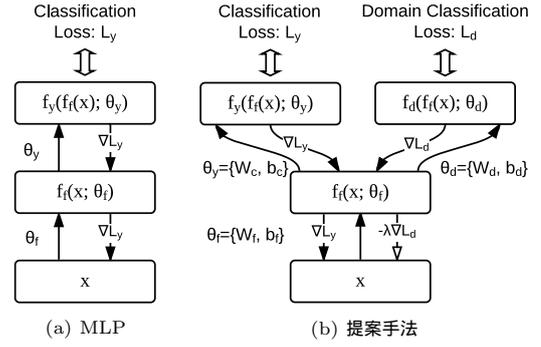


図 1: 提案手法の概要図.

Algorithm 1 提案手法の擬似コード.

Require: dataset $D = \{(x_n, y_n, u_n)\}_{i=1}^N$, parameter λ
Ensure: neural network $\{\theta_f, \theta_y, \theta_u\}$

```

t ← 1
while training() do
  L_u ← eq.3  $\forall (x_n, u_n) \in D$ 
   $\theta_u \leftarrow \theta_u + \frac{\delta L_u}{\delta \theta_u}$ 
  L_y, L_u ← eq.2  $\forall (x_n, y_n) \in D$ , eq.3  $\forall (x_n, u_n) \in D$ 
   $\lambda_t \leftarrow \text{anealing}(\lambda, t)$ 
   $\theta_f, \theta_y \leftarrow \theta_f - \frac{\delta(L_y + \lambda_t L_u)}{\delta \theta_f}, \theta_y - \frac{\delta L_y}{\delta \theta_f}$ 
  t ← t + 1
end while

```

この最適化問題を解くにあたり, ここでは, [Ajakan 14] や [Edwards 16] に従い確率的急降下法 (SGD) による交互最適化を行った. すなわち, 1. L_d を最大化するように θ_u を更新する, 2. L を最小化するように θ_f および θ_y を更新するという手続きを交互に繰り返した.

画像生成の領域に敵対的訓練を利用する場合と比較したドメイン汎化の問題設定の特徴として, 前者が複数のドメイン (画像生成の例では本物画像と偽物画像) を区別出来ないような写像 f_f を得ること自体が目的であるのに対して, 後者はドメイン不変な表現への写像 f_f の学習を通じてより汎用な f_y を得ることが主な目的となる点がある. ここで, ある特徴量がドメインを区別出来ないからといって, 必ずしも良い f_y の構築に貢献するわけではない点には注意が必要である. 例えば, 完全にランダムな写像を与える関数を特徴抽出器として利用すれば得られる特徴量からドメインを区別することは出来ないが, 同時にその特徴量からラベルを予想することも明らかに出来ない. また, 実際実験的にも学習の初期段階にドメインを区別しないように強いると最終的なラベル分類精度が劣化する状況が観測された. このように, 単にドメインを区別出来なくすれば良いだけでなく, 同時にラベルに関する情報は残すように学習を行う必要がある点にドメイン汎化の設定の従来の設定と比較した技術的な難しさがある.

本稿では, この問題に対して λ を小さな値からはじめエポックが進むごとに徐々に大きくする焼きなましヒューリスティックを導入した. パラメータ λ の焼きなましを行うことで, ラベル分類器の学習が進んでいない初期段階でドメイン不変性を過剰に高めようとするのを抑制することができ, 結果として初期フェーズにラベル分類器にとって悪いパラメータ空間に落ちないようにすることができる. 本稿の実験では下記の線形スケジューリング $\lambda_t = (t - \alpha) \cdot \frac{\lambda}{(\beta - \alpha)}$ ($\alpha \leq t < \beta$) を利用しそ

の有効性を検証した．ここで， t はエポック数， $\alpha + 1$ は焼きなましを開始するエポック， β は焼きなましを終了するエポック， λ は最終的なパラメタの設定値を意味している．ただし， $t \leq \alpha$ では $\lambda_t = 0$ であり， $\beta \leq t$ では $\lambda_t = \lambda$ である．

以上をまとめると，提案手法の擬似コードは Algorithm1 に示した通りとなる．

4. 実験・考察

4.1 実験設定

データセットには，最もポピュラーなデータセットの1つである Opportunity を利用した．Opportunity は，朝食をシミュレートしたシナリオにおける日常行動を4人分 (S1-S4) 記録したデータセットである．多数の種類の活動者の身体，物体，および環境に設置されたセンサにより行動を計測しており，合計で72のセンサ，10のモダリティを持つデータである (詳しくは，Sagha らの論文の図1 [Sagha 11] を参照されたい)．結果として，各時刻において113の実数値 (時刻情報は除く) が記録されている．本稿では，提供されている3つの認識タスクのうち Gestures (以降 Opp-G) と Locomotion (以降 Opp-L) による検証を行った．Opp-G は，18クラス^{*1} のより細かな行動を分類するタスクであり，Opp-L は5種類のより大局的なユーザの状態を分類するタスクである．分類問題を解くにあたり，一般に利用されるスライディングウィンドウ方式 (スライド幅30，重なり率0.5) により学習サンプルを生成し，結果として4ユーザ合計で約50,000のサンプルを得た．

図2に実験に利用した提案手法のネットワーク構造を示す．ドメイン分類器を除くと，ネットワーク構造は単純なCNNとなる．層の数やフィルタ数などのハイパーパラメタは同じ Opportunity データセットに対してCNNを適用した [Yang 15] を参考に設計した．ここで，図中 $1 \times K$ は畳み込みサイズ (あるいはプーリングサイズ) を，各層の右下に位置する数値は特徴マップ数あるいはユニット数を意味する．活性化関数は出力層にソフトマックス関数を利用したほかは ReLU を利用し，各畳み込み層および全結合層のあとにはドロップアウトを行った．最適化には Adam [Kingma 15] (学習率は0.0001，その他のパラメタは推奨パラメタ) を利用し150エポック学習させた．

敵対的ドメイン分類器 f_d としては，図中全結合層の出力を入力とする MLP_{800} (800個の中間ユニット数もつ3層ニューラルネットワーク) を利用した． L_d と L_y を重み付けるハイパーパラメタ λ は0.1に設定した．また，焼きなましのパラメタ α および β は開始直後と終了直前の15エポックずつは固定した λ で学習されるように，それぞれ15, 135とした．

提案手法の有効性およびパラメタの重要性を検証のため次の4つの手法を比較した．1) CNN：提案手法において $\lambda=0.0$ とした場合に対応．2) Adv-LR：敵対的ドメイン分類器として， MLP_{800} の代わりにロジスティック回帰を利用したものに対応．3) Adv-MLP：提案手法においてパラメタ λ の焼きなましを行わない場合に対応．4) Adv-MLPA：敵対的ドメイン分類器として MLP_{800} を利用し，かつ焼きなましを行った場合．これらの手法を比較することで，単純なCNNと比較して提案手法によりドメイン汎用性を高められること，また敵対的

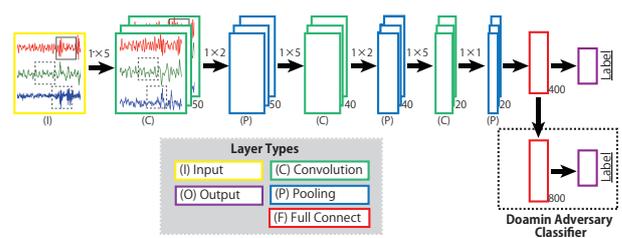


図2: 実験に利用したネットワーク構造.

ドメイン分類器の表現力や焼きなましがドメイン汎化性能に与える影響を検証した．

各手法の評価は次のような Leave-One-Subject-Out 手続き (LOSO) により行った．LOSO は新規ユーザに対する認識精度を検証するためによく利用される方法であり，ここでは1. K 人のうちから1人テストユーザを i を選択する，2. ユーザ i を除く $K-1$ 人のデータの一部を訓練データとして利用しモデルを訓練する (このとき，80%を訓練データとし残り20%は検証データとして利用した)，3. ユーザ i のデータ (以降テストデータ) を利用して評価を行う，という手続きを K 回に渡り繰り返す方法である．このような手続きでは，ユーザ i のデータは各ステップのモデルにおいて訓練に全く利用されないで，学習されたモデルの未知ユーザに対する認識性能を評価することができる．

LOSO の枠組みを利用して，各手法のドメイン汎化性能をテストユーザに対する正解率 ($\frac{1}{N} \sum_{n=1}^N 1(\hat{y}_n = y_n)$) および平均 F 値 ($\frac{1}{|L|} \sum_{l \in L} F^l(\hat{y}, y)$) で評価した．ただし， N は全サンプル数， L は行動クラスの集合， y_n と \hat{y}_n は i 番目のサンプルに対する正解ラベルおよび予測ラベル， $F^l(\hat{y}, y)$ は l 番目のクラスに関する F 値を意味する．正解率は全サンプルを均等に扱うのに対して，平均 F 値は少数クラスのサンプルを重要視した指標であるという点で異なる役割を持つ指標である．また，これに加えて学習された特徴量からドメインをどの程度正確に予想できる分類器を構築できるかを検証した．ドメインをより正確に予想できる場合には得られた特徴量がドメインごとに大きく異なることを意味するため，ドメイン分類精度は高いほどドメイン不変性が低くなる (望ましくない) 指標であると考えられる．なお，ニューラルネットワークを利用した手法については出力層の1つ前の層の出力を特徴量として検証を行った．

4.2 実験結果

表1および表2に，提案手法とベースライン手法の比較結果を示す．表1および表2はそれぞれユーザ汎化性能と表現のドメイン不変性に関する結果に対応している．ただし，ユーザ汎化性能に関する値は大きいほど汎化性能が高く，またドメイン識別性能に関しては低いほど表現のドメイン不変性が高いことを意味することに注意されたい．また，参考値として生データの特徴量とした場合 (Rawdata)，行動認識でよく利用される経験的特徴量を利用した場合 (MV [Yang 15])，行動認識で良い精度を達成することが近年報告されている ECDF [Hammerla 13] を特徴量として利用した場合の結果についても合わせて報告する．なお，これらの3つの特徴量については分類器には K 近傍法を利用した．

結果としてまず，ニューラルネットベースの手法と経験的特徴量を比較すると，いずれもニューラルネットベースの手法を利用した場合に顕著に高いユーザ汎化性能が得られていた．また，CNNと提案手法 Adv-MLPA をユーザ汎化性能の観点で比較すると，提案手法によりどちらのデータセットでもわずか

*1 open door 1, open door 2, close door1, close door 2, open fridge, close fridge, open dishwasher, close dishwasher, open drawer 1, close drawer 1, open drawer 2, close drawer 2, open drawer 3, close drawer 3, clean table, drink cup, toggle switch, and Null

表 1: 提案手法とベースラインのユーザ汎化性能での比較 .

	Opp-G		Opp-L	
	F 値	正解率	F 値	正解率
Rawdata	0.318	0.639	0.558	0.619
MV	0.468	0.698	0.721	0.744
ECDF	0.463	0.714	0.696	0.743
CNN	0.557	0.772	0.794	0.796
Adv-LR	0.547	0.771	0.786	0.790
Adv-MLP	0.551	0.776	0.781	0.794
Adv-MLPA	0.566	0.778	0.804	0.798

表 2: 提案手法とベースラインのドメイン識別性能での比較 .

	Opp-G	Opp-L
Rawdata	0.352	0.352
MV	0.849	0.849
ECDF	0.914	0.914
CNN	0.870	0.903
Adv-LR	0.516	0.579
Adv-MLP	0.480	0.543
Adv-MLPA	0.501	0.550

ながら改善が見られた．具体的には，F 値でそれぞれ 0.01 ポイント，正解率で Opp-G で 0.006 ポイント，Opp-L で 0.002 ポイントの改善が見られた．また，ドメイン不変性の観点で CNN と提案手法を比較すると（表 2），提案手法によりドメイン不変性が CNN と比較して大幅に改善していた．

一方で，CNN と提案手法で焼きなましを行わない場合（Adv-MLP）や敵対的分類器にロジスティック回帰を利用した場合（Adv-LR）を比較すると，ユーザ汎化性能は改善しないかむしろ悪化する場合があった．例えば，CNN と Adv-MLP を比較すると，Opp-G の正解率でほぼ同程度となっていることを除くと Adv-MLP でユーザ汎化性能が僅かに低下していた．ただし，ドメイン不変性の観点（表 2）では Adv-LR や Adv-MLP でも Adv-MLPA と同様に大きな改善が見られた．

5. 考察

表 1 に示したように，提案手法を利用することでわずかながらドメイン汎化性能に改善が見られた．また，表 2 に示したように，単純な CNN で学習された特徴量からドメインを予想する分類器を構築することは容易であった一方で，提案手法により学習された特徴量ではより予想しにくくなっていた．これらの結果から，提案手法はよりドメインを区別することが出来ない，ドメイン不変性の高い特徴量を学習するのに有効であり，また結果としてモデル全体のユーザ汎化性能を高めることにも有効となりうることが示唆された．

一方で本稿で明らかになった提案手法の課題として，1. 単にドメイン不変性を高めるだけでは最終的なラベル分類器の汎用性が高まらない場合がある（例えば Adv-LR や Adv-MLP），2. 改善幅が軽微であるといった点があげられる．1 つめの現象の原因として，ドメイン不変性を高めすぎると入出力関係の一部を棄損してしまい，結果として予測精度が低下してしまう可能性がある．この問題を避けるためには，今回は焼きなましというヒューリスティックを利用することで若干の精度改善が見られたが， λ 自体を最適化したり，スケジューリングを工夫するなどにより更に認識精度を高められる可能性がある．

6. おわりに

本稿では，ドメイン汎用なニューラルネットを構築する方法として，敵対的訓練を利用したドメイン不変な表現の学習方法を提案し，ドメイン汎化が必要な代表的なタスクの 1 つであるウェアラブルセンサによる行動認識の問題設定でその有効性を検証した．今後は，より幅広いデータセットでの検証を行うことで，さらに研究を発展させていきたい．

謝辞

本研究は JSPS 科研費 JP12345678 の助成を受けたものです．

参考文献

- [Ajakan 14] Ajakan, H., Germain, P., Larochelle, H., Laviolette, F., and Marchand, M.: Domain-adversarial neural networks, in *NIPS Workshop on Transfer and Multi-Task Learning: Theory meets Practice* (2014)
- [Blanchard 11] Blanchard, G., Lee, G., and Scott, C.: Generalizing from several related classification tasks to a new unlabeled sample, in *Proc. of NIPS*, pp. 2178–2186 (2011)
- [Denton 15] Denton, E. L., Chintala, S., Fergus, R., et al.: Deep Generative Image Models using a Laplacian Pyramid of Adversarial Networks, in *Proc. of NIPS*, pp. 1486–1494 (2015)
- [Edwards 16] Edwards, H. and Storkey, A.: Censoring Representations with an Adversary, in *Proc. of ICLR* (2016)
- [Ganin 14] Ganin, Y. and Lempitsky, V.: Unsupervised Domain Adaptation by Backpropagation, *arXiv preprint arXiv:1409.7495* (2014)
- [Goodfellow 14] Goodfellow, I., Pouget-Abadie, J., Mirza, M., Xu, B., Warde-Farley, D., Ozair, S., Courville, A., and Bengio, Y.: Generative adversarial nets, in *Proc. of NIPS*, pp. 2672–2680 (2014)
- [Hammerla 13] Hammerla, N. Y., Kirkham, R., Andras, P., and Ploetz, T.: On preserving statistical characteristics of accelerometry data using their empirical cumulative distribution, in *Proc. of International Symposium on Wearable Computers (ISWC)*, pp. 65–68 ACM (2013)
- [Kingma 15] Kingma, D. and Ba, J.: Adam: A method for stochastic optimization, in *Proc. of ICLR* (2015)
- [Sagha 11] Sagha, H., Digumarti, S. T., Millán, J. d. R., Chavarriaga, R., Calatroni, A., Roggen, D., and Tröster, G.: Benchmarking classification techniques using the Opportunity human activity dataset, in *Proc. of INSS*, pp. 36–40 IEEE (2011)
- [Schmidhuber 92] Schmidhuber, J.: Learning factorial codes by predictability minimization, *Neural Computation*, Vol. 4, No. 6, pp. 863–879 (1992)
- [Yang 15] Yang, J. B., Nguyen, M. N., San, P. P., Li, X. L., and Krishnaswamy, S.: Deep Convolutional Neural Networks On Multichannel Time Series For Human Activity Recognition, in *Proc. of IJCAI*, pp. 3995–4001 (2015)