摂動化によってプライバシーを保護した情報推薦方式

望 月 安 菜[†1]　菊 池 浩 明[†1]

プライバシーを保護したまま，摂動化したデータから再構築を行う新しい情報推薦方式を提案する．提案方式は，摂動化により一定確率で評価値をランダマイズすることでプライバシーを保護する．また，ベイズ推定による再構築によって，アイテム間類似度をオリジナルデータへ近似させることが出来，情報推薦の精度が向上することを示す．

A Privacy-Preserving Recommendation Method using Perturbation

Anna MOCHIZUKI[†1] and Hiroaki KIKUCHI[†1]

This paper proposes a new privacy-preserving recommendation method using randomized scheme. A privacy of rating value is preserved since random perturbation prevents private rating value from being identified. While, the accuracy of recommendation is improved by Bayse estimation of similarity matrix of items.

1. はじめに

近年，オンラインショップ Amazon.com に代表される情報推薦が盛んである．ここでは，ユーザの過去の購入履歴，閲覧履歴から情報推薦を行っている．また，ニュースサイトにおけるニュース記事の推薦も盛んである．このような情報推薦の主流は，複数のユーザによって複数のアイテムが評価付けされているデータベースにおいて，他のユーザの値を基に評価されていないアイテムの評価値を予測する協調フィルタリング (Collaborative Filtering) である．

しかし，これらの情報推薦には，不正なサービス事業者によるプライバシー漏洩の課題がある．そこで，プライバシーを守るために，準同型性を満たした公開鍵暗号を使った個人情報を秘匿する研究がある[4]．しかし，暗号は，プライバシー保護は出来るが，大きな計算コストがかかる．そこで，本研究では，個人のプライバシーを保護しながら，暗号化をせずにユーザに応じた情報推薦を行うことを目的とする．

提案方式は，摂動化と呼ばれるランダマイズアルゴリズムと協調フィルタリングからなる．既存研究として，Agrawal ら[1] の研究が挙げられる．彼らは，データマイニング時に人工的に加えたノイズの影響をベイズ推定によって取り除き，決定木学習を実現している．本研究では，彼ら同様，摂動化したデータを用いて，ベイズ推定によってノイズを除去するが，決定木学習の代わりに協調フィルタリングを適用する点に特徴がある．情報提供者の持つ情報にノイズを加える．このデータの解析を行った後に，ノイズ除去の処理を施し，解析結果を同定する．同定する過程を再構築という．

摂動化を使用したこれら手法は，暗号化と比較し計算コストが小さい．また暗号化に比べ実装が容易である．しかし，暗号化がほぼ厳密に正しい結果を得ることに対して，摂動化の学習結果は近似解である．安全性の保証観点からは，暗号化の方が厳密である．

本研究では，摂動化を実行するプログラムを実装した．主な成果としては，以下の通りである．(1) 既存研究によって提案されていたいくつかの有用な摂動化の性質を明らかにした．(2) 新たな方式として摂動化協調フィルタリング法を提案した．(3) 摂動化協調フィルタリング法を使用し，公開データベースを使用し実験を行い，精度や性能を評価した．

表 1　プライバシー保護協調フィルタリング方式の比較

	H.Polat and W.Du[3]	提案方式
ランダマイズ	加法摂動化	ランダマイズドレスポンス
安全性	×（PCA）	○
協調フィルタリング	容易	（目標）

2. 準　　備

2.1 関連研究

H. Polat ら[3] は，加法摂動化による協調フィルタリング方式を提案している．彼らの研

†1 東海大学大学院　工学研究科　情報理工学研究
Course of Information Science and Engineering, Graduate School of Engineering, Tokai university
259-1292 神奈川県平塚市北金目四丁目１番１号
cream_18_puff,kikn@cs.dm.u-tokai.ac.jp

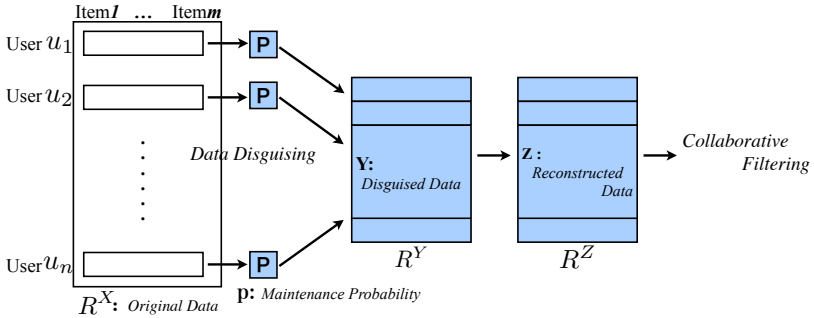

図 1　プライバシー保護した協調フィルタリングの全体構造

究では，オリジナルデータ X に一様分布の乱数 R を加えた $Y = X + R$ について，平均値 $\sum_i Y_i = \sum_i X_i + \sum_i R_i \approx \sum_i X_i$ であることを仮定したナイーブな推薦方式である．従って，Y を，主成分分析 (PCA) することで加えた乱数ノイズを取り除くことが出来ることが指摘されており[2)]，その安全性は低い．

そこで，本研究では，単純な PCA による解析が困難なランダマイズドレスポンス方式を用いて，摂動化を行う．安全性は向上するが,3) の様な単純な協調フィルタリングでは精度が期待できない．以上の関係を表 1 に整理する．

2.2　摂動化と再構築法

再構築問題 (Reconstruction Problem) とは，摂動化された $Y_1 = X_1 + R_1$，確率変数 Y から，真の値 X の確率分布を見積もる問題である．R. Agrawal and R. Srikant[1)] によって最初に発表された摂動化アルゴリズムである．秘匿したい情報に意図的にランダムノイズを乗せて，格納されたデータのプライバシーを保護する．

例えば，年齢が $x = 20$ 代であるという個人情報をそのまま渡す代わりに，一様分布（またはガウス分布）の乱数 r を加え，$y = x + r = 30$ の様に歪んだ値 y を登録する．30 という属性値を持った顧客がいても，本当に 30 代なのか乱数で 40 代から歪まされたのか，第三者には区別がつかない．

暗号化による方法と異なり，時間のかかる暗号化はなく，計算も各パーティで独立に計算できる．通信効率も計算効率も高い．大規模なデータベースにおいても適用可能である．

2.2.1　摂　動　化

簡単な数値例を用いて再構築アルゴリズムの原理を示す．確率変数 A が表 2 の分布に従って与えられているとする．

表 2　真の確率分布 $P(A)$

a	0	1	2	3
$P(A = a)$	0.1	0.3	0.1	0.5

ここで，A の分布を秘匿する為に，表 8 の条件付確率 $P(B|A)$ に従って，A の値を変化（摂動化）させた結果を B とおく．

表 3　条件付確率 $P(B|A)$, 維持確率 $p = 0.4$

$B \backslash A$	0	1	2	3
0	0.4	0.2	0.2	0.2
1	0.2	0.4	0.2	0.2
2	0.2	0.2	0.4	0.2
3	0.2	0.2	0.2	0.4

ここで，維持確率 $p = 0.4$ は，A を変化させない確率の大きさであり，変化させるときは一様な確率で分布させることにする．こうして摂動化した結果を表 4 で示す．オリジナルの分布では $A = 3$ が最頻度で生じていたのに対して，値の差が小さくなりどの値も同じくらい確からしい．

表 4　摂動化した確率分布 $P(B)$

b	0	1	2	3
$P(B = b)$	0.22	0.26	0.22	0.3

2.2.2 再構築アルゴリズム

再構築アルゴリズムは，この $P(B|A)$ と摂動化後の確率分布 $P(B)$ だけを与えて，オリジナルの分布 $P(A)$ を近似することを目的とする．初期値を $P^0(A) = P(B)$ で与える．事後確率の i 番目の近似値は，

$$P^i(A|B) = \frac{P(B|A)P(A)}{P(B)} = \frac{P(B|A)P^{i-1}(A)}{\sum_{a\in A} P(B|A=a)P^{i-1}(A=a)}$$
$$= \frac{P(B|A)P(A)}{P(B|A=0)P^{i-1}(A=0) + \cdots + P(B|A=3)P^{i-1}(A=3)}$$

と近似され，この値を用いて A の事後確率の第一近似値は

$$P^1(A) = \sum_{b\in B} P^0(A|B=b)P(B=b)$$

で与えられる．こうして，逐次的に近似を繰り返し，$P^{i+1}(A) = P^i(A)$ と収束した分布を再構築された P^* とする．この数値例の場合の第二近似値までの結果を表 5 で示す．徐々に真の分布へ近づいていることが分かる．

表 5 再構築された確率分布の第一近似 $P^1(A)$ と第二近似 $P^2(A)$

a	0	1	2	3
$P^1(A=a)$	0.22	0.26	0.22	0.31
$P^2(A=a)$	0.21	0.26	0.21	0.33

2.3 アイテムベース協調フィルタリング

協調フィルタリングは，ユーザ間あるいはアイテム間の類似度に基づき，未知のアイテムに対する評価値を予測するアルゴリズムである．ユーザ間の類似度から評価値を予測するユーザベース方式と，アイテム間の類似度を計算し，評価値を予測するアイテムベース方式がある．ここでは，アイテム間類似度を使用する．

ユーザ u のアイテム i についての評価値を $r_{u,i} \in V$ と表す．ユーザ数 n，アイテム数 m の評価値行列を R とする．例えば，表 6 は，$n = 4$，$m = 5$ の例である．ここで，$*$ の評価値を

$$r_{u,i} = \frac{\sum_j^m s_{j,i} r_{u,j}}{\sum_j |\, s_{j,i} \,|} \tag{1}$$

で予測する (アイテム間の平均に差がないことを仮定して，正規化を省略している)．ここでは，$s_{i,i}$ は，アイテム i と j 間の類似度であり，本稿ではコサイン尺度により

$$s_{j,i} = \frac{\sum_{k=1}^n r_{k,i} r_{k,j}}{\sqrt{r_{1,i}^2 + \cdots + r_{n,i}^2}\sqrt{r_{1,j}^2 + \cdots + r_{n,j}^2}} \tag{2}$$

と定める．

表 6 Original Data (R^X)

	i_1	i_2	i_3	i_4	i_5
u_1	2	2	3	1	
u_2	1	3	2		3
u_3	2		3	3	2
u_4	3	2	$*$	2	2

表 7 Disguised Data (R^Y)

	i_1	i_2	i_3	i_4	i_5
u_1	2	3	1	1	
u_2	1	1	2		1
u_3	1		3	3	
u_4	3	2	$*$	2	3

3. 提 案 方 式

3.1 アイデア

評価値行列 R^X を真のデータ X とみなし，維持確率 p についてランダマイズドレスポンスによって摂動化を行い，偽データ行列 R^Y を作成する．この偽データ R^Y と p についてベイズ推定を行い，真のデータ X の再構築を行う．分布 Y から真の分布 X は予測できても，摂動化された行列 R^Y から，真の行列 R^X を求めることはできない．そこで，再構築の過程で求められた条件付き確率 $P(X|Y)$ を用いて，R^Y からアイテム間類似度の期待値を求めて，推薦アルゴリズムに適用する．

3.2 提案方式 – 期待値による協調フィルタリング

提案の全体構造を図 1 に示す．各ユーザは，自分の評価値を決められた確率で摂動化 (ランダマイズ) して集計サーバに送り，集めた R^Y を公開する．

真の評価値 $r_{u,i}$ と維持確率 p について，摂動化 y を

$$y = P(y) = \begin{cases} r_{u,i} & w/p = p \\ v \in V - \{r_{u,j}\} & \text{otherwise} \end{cases} \tag{3}$$

と定める．例えば，表 6 の行列 R^X を維持確率 $p = 0.4$ で摂動化した行列を表 7 の R^Y とする．

次に，R^Y と p から定まる条件付き確率 $P(Y|X)$ に真の評価値 X についての予測値 Z と条件付き確率 $P^*(X|Y)$ を求める．

表 8 条件付確率 $P(Y|X)$, 維持確率 $p = 0.4$

$Y \backslash X$	0	1	2	3
0	0.37	0.18	0.23	0.22
1	0.19	0.36	0.23	0.22
2	0.18	0.17	0.44	0.21
3	0.18	0.17	0.22	0.43

最後に，次のアルゴリズム CF-E により，任意のアイテムに対する評価値を予測する．

Algorothm 期待値を用いた協調フィルタリング (CF-E)

Input:摂動化評価値行列 R^Y,$P(X|Y)$

Output:推薦値 $r^E_{u,i}$

Step 1 異なるアイテム間の 2 つの摂動化評価値 Y_1,Y_2 が与えられた時，それらの積を取る確率変数を $W(= Y_1 \cdot Y_2)$ とする．W の確率分布は

$$P(W|Y_1, Y_2) = \sum_{W=\alpha\beta} P(X = \alpha|Y_1) \cdot P(X = \beta|Y_2)$$

で求められる．

Step 2 積 W の期待値を求める．すなわち

$$E[W|Y_1, Y_2] = \sum_{\gamma \in V_2} P(W = \gamma|Y_1, Y_2)$$

ここで，V_2 は 2 つの V の要素からなる集合とする．$V = \{1, \ldots, v\}$ の時,$V_2 = \{1, \ldots, v^2\}$.

Step 3 摂動化行列 R^Y が与えられた条件の下で, アイテム i と j 間の類似度 $s^E_{i,j}$ の期待値を式 (2) のコサイン尺度で

$$s^E_{i,j} = E[S_{i,j}|R^Y] = \frac{E[\sum_u^n r^X_{u,i} \cdot r^X_{u,j}|R^Y]}{E[\sqrt{\sum_u (r^X_{u,i})^2}\sqrt{\sum_u (r^X_{u,j})^2}]} = \frac{\sum_u^n E[W|Y_1 = r^Y_{u,i}, Y_2 = r^Y_{u,j}]}{\sqrt{\sum_u (r^Y_{u,i})^2}\sqrt{\sum_u (r^Y_{u,j})^2}}$$

により求める．ここで，分母は R^X におけるノルムを R^Y で近似している．分子は step 2 の期待値で与えられる．

Step 4 式 (1) により期待類似度 s^E によるユーザ u のアイテム i の予測値は,

$$r^E_{u,i} = \frac{\sum_j^m S^E_{i,j} \cdot r^X_{u,j}}{\sum_j^m S^E_{i,j}}$$

で与えられる．

表 9 各評価値の積 W の期待値 $E[W|Y_1, Y_2]$

$Y_2 \backslash Y_1$	0	1	2	3	sum
0	1.69	1.92	2.18	2.47	8.26
1	1.92	2.19	2.49	2.81	9.41
2	2.18	2.49	2.82	3.19	10.68
3	2.47	2.81	3.19	3.16	11.63

表 10 類似度の期待値 $E[S_{i,j}|R^Y]$

	i_1	i_2	i_3	i_4	i_5
i_1	–	0.60	0.46	0.66	0.54
i_2	0.60	–	0.46	0.65	0.56
i_3	0.46	0.46	–	0.50	0.44
i_4	0.66	0.65	0.50	–	0.62
i_5	0.54	0.56	0.44	0.62	–

3.3 数 値 例

本実験では，表 6 のオリジナルデータ R^X を評価行列に，維持確率 $p = 0.4$ で摂動化した偽データ R^Y を表 7 とする，ユーザ数 $n = 4$，アイテム数 $m = 5$，評価値 $V = \{1, 2, 3\}$ とする．また，未評価のものを $r_{i,u} = 0$ とする．

各評価値の分布による再構築を行った結果を図 3 に示す．真の R^X の分布と $p = 0.4$ の維持確率により摂動化を行った偽データの分布 Y を示す．ベイズ推定を利用し，50 回再構

築を行った結果 Z を示す．50 回行った再構築によって十分な精度で近似出来ることが分かる．再構築回数を増やしていくことで，更に近似する．

アルゴリズム CF-E により推薦を行う．摂動化された R^Y の 2 つの評価値が $Y_1 = 2$,$Y_2 = 3$ と観測された時，その積 W の確率分布を図 2 に示す．$W = 0$(未評価) が最大，$W = 6 = 2 \cdot 3$ がその次に高い確率を持つ．

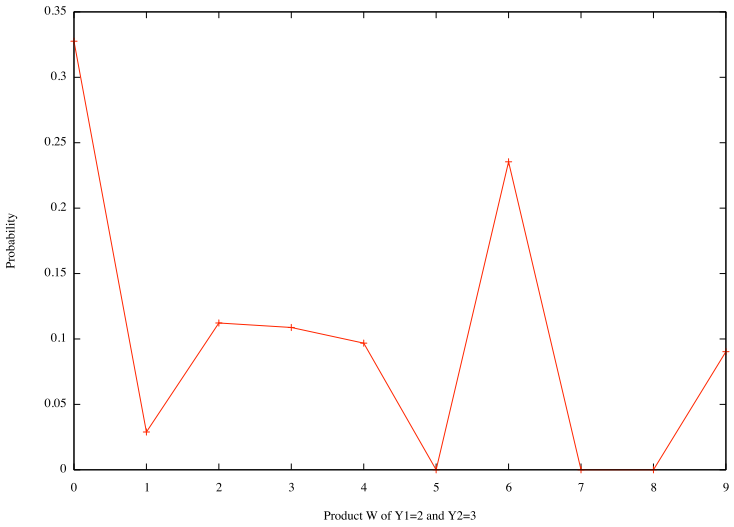

図 2　$Y_1 = 2$,$Y_2 = 3$ が与えられた時の積 $W(= Y_1 \cdot Y_2)$ の評価値の分布　$P(W|Y_1 = 2, Y_2 = 3)$

これらを平均すると，$E[W|Y_1 = 2, Y_2 = 3] = 3.19$ であった．単純な R^Y の積 $2 \cdot 3 = 6$ よりも小さな値で見積もられる．

以上を全ての $Y_1 = 0, 1, 2, 3$, $Y_2 = 0, 1, 2, 3$ の組み合わせについて求めた結果を表 9 に示す．Step 3 により，求めたアイテム間の類似度の期待値 $s^E = E[S|Y_1, Y_2]$ を表 10 に示す．

オリジナルデータ R^X，偽データ R^Y，再構築データについて，それぞれの求めた類似度の分布 $P(W|Y_1 = 2, Y_2 = 3)$ を図 4 に示す．オリジナルデータ X を基準としてみると，偽データ Y がオリジナルデータに近似している事を示している．

オリジナルデータ X を協調フィルタリングした予測値を基準とし，摂動化偽データ Y，再構築データ Z にそれぞれ協調フィルタリングを適用して推薦した値の分布を図 5 に示す．

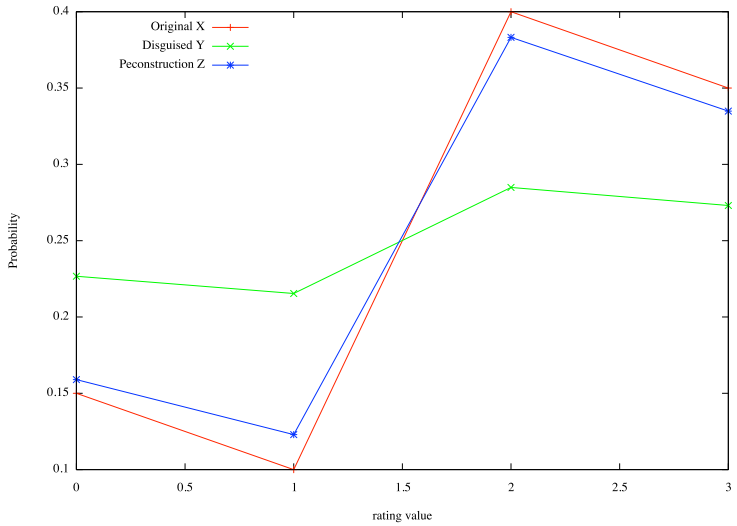

図 3　再構築された評価値の分布

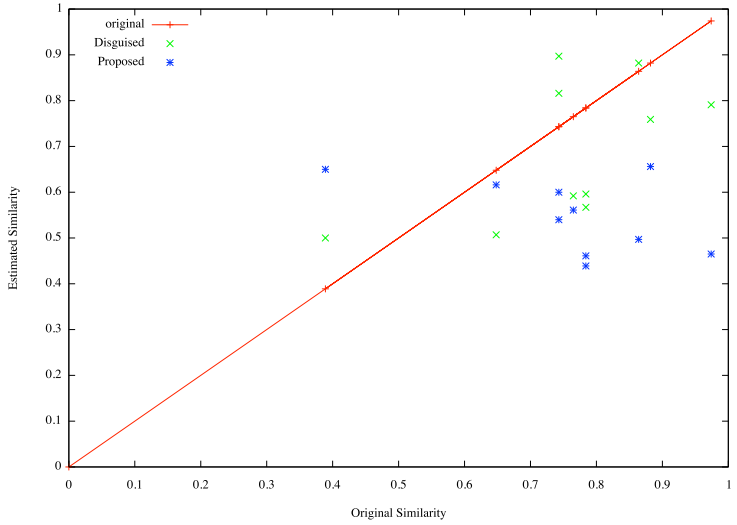

図 4　予測類似度の分布 (S^X, S^Y, S^E)

提案手法である再構築を行ったデータがオリジナルデータの推薦結果に近似していることが分かる．

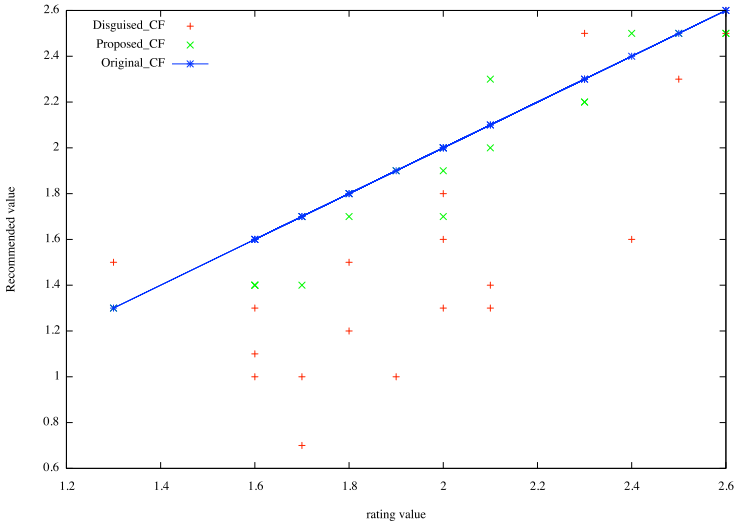

図 5 協調フィルタリングによる推薦値の分布 (r^X, r^Y, r^E)

オリジナルデータ，偽データ，期待値を利用したデータで協調フィルタリングを行い予測した値の MAE(Mean Absolute Error) と標準偏差によって比較を行ったものを表 11 に示す．$MAE^E = \sum_{u,i} |r^X_{u,i} - r^E_{u,i}|$ と定める．摂動化したデータにナイーブに CF を適用したのもは，$MAE^Y = \sum_{u,i} |r^X_{u,i} - r^Y_{u,i}|$ である．偽データより期待値を利用した再構築データの方が誤差が少ない．

表 11 Mean Absolute Error

	MAE	標準偏差
Original	0.968	1.171
Disguised	1.033	1.204
Proposed	1.009	1.228

3.4 考　　察

図 5 より協調フィルタリングを行った際，再構築データはオリジナルデータに近付いていることが分かる．また，表 11 より，偽データより再構築データの方が誤差が少ないが，その差は有意ではない．オリジナルの推薦値の誤差が大きいことから，用いた評価行列が人工的で歪んでいた可能性がある．提案方式では，未評価値の扱いが十分ではなく，それが誤差の要因のひとつと考えられる．

4. おわりに

プライバシーを保護したまま，摂動化したデータから再構築を行う新しい情報推薦方式を提案した．提案方式は，摂動化により一定確率で評価値をランダマイズされたデータが出来るためプライバシーは保護される．また，再構築によって，ベイズ推定によりアイテム間類似度をオリジナルデータへ近似させることが出来るので，情報推薦の精度が向上することを示した．

参 考 文 献

1) R. Agrawal and R. Srikant, “Privacy-Preserving Data Mining”, ACM SIGMOD 2000, pp. 439-450, 2000.
2) Z. Huang, W. Du and B. Chen, “Deriving Private Information from Randomized Data”, ACM SIGMOD 2005, pp. 37-48, 2005.
3) H. Polat and W. Du, “Privacy-Preserving Collaborative Filtering using Randomized Perturbation Techniques”, ICDM 2003, pp. 1-15, 2003.
4) 青木良樹, 菊池浩明, “擬準同型性を満たす類似度による分散協調フィルタリングプロトコル”, SCIS 2011, pp. 1-6, 2011.
5) 麻生英樹, 小野智弘, 本村陽一, 黒川茂莉, 櫻井彰人, “協調フィルタリングと属性ベースフィルタリングの統合について”, 信学技報 NC 2006, pp. 55-59, 2006.