

# Use Fewer Instances of the Letter "i": Toward Writing Style Anonymization

Andrew W.E. McDonald, Sadia Afroz, Aylin Caliskan,

Ariel Stolerman, and Rachel Greenstadt

PSAL, Drexel University

http://psal.cs.drexel.edu

# How do you change your writing style?

#### Stylometry:

Authorship-attribution based on linguistic properties found in text

#### Stylometry:

- Authorship-attribution based on linguistic properties found in text
- Stylometric methods can achieve high accuracy across a high number of authors
  - Writeprints: > 90% accuracy for 100 authors (Abbasi and Chen, 2008)
  - Scaling stylometry up to 100,000 authors (Narayanan et al., 2012)

#### Stylometry:

- Authorship-attribution based on linguistic properties found in text
- Stylometric methods can achieve high accuracy across a high number of authors
  - Writeprints: > 90% accuracy for 100 authors (Abbasi and Chen, 2008)
  - Scaling stylometry up to 100,000 authors (Narayanan et al., 2012)
- Accuracy and precision of stylometry are increasing

Increasingly easier to determine the author of a text

- Increasingly easier to determine the author of a text
- Harder to express ideas / opinions without taking ownership

- Increasingly easier to determine the author of a text
- Harder to express ideas / opinions without taking ownership
- Can be a threat to security and privacy

# Stylometry: A Threat to Security and Privacy

- Physical
  - Restrictive/oppressive regimes

# Stylometry: A Threat to Security and Privacy

- Physical
  - Restrictive/oppressive regimes
- Job
  - Talking against abusive boss

# Stylometry: A Threat to Security and Privacy

- Physical
  - Restrictive/oppressive regimes
- Job
  - Talking against abusive boss
- Generally, your writing style could give you away regardless of other precautions taken
  - Tor, VPN, changed MAC address, etc...

#### Purely Hypothetical?‡

- Previous examples are purely hypothetical. What about a real example?
- From Inside WikiLeaks by Daniel Domscheit-Berg:
  - "I nudged Julian with my foot. We exchanged glances and started giggling. If someone had run WikiLeaks documents through such a program, he would have discovered that the same two people were behind all the various press releases, document summaries, and correspondence issued by the project. The official number of volunteers we had was also, to put it mildly, grotesquely exaggerated."

 Okay, so it's necessary to change your writing style to stay anonymous...  Okay, so it's necessary to change your writing style to stay anonymous...

Why do we need a tool to do this?

Machine translation

- Machine translation
  - Either does too little:
    - They passed through the city at noon of the day following.

- Machine translation
  - Either does too little:
    - They passed through the city at noon of the day following.
    - → German → Japanese →

- Machine translation
  - Either does too little:
    - They passed through the city at noon of the day following.
    - → German → Japanese →
    - They passed the city at noon the following day.

- Machine translation
  - Either does too little:
    - They passed through the city at noon of the day following.
    - → German → Japanese →
    - They passed the city at noon the following day.
  - Or does too much:
    - Just remember that the things you put into your head are there forever, he said.

- Machine translation
  - Either does too little:
    - They passed through the city at noon of the day following.
    - → German → Japanese →
    - They passed the city at noon the following day.
  - Or does too much:
    - Just remember that the things you put into your head are there forever, he said.
    - → German → Japanese →

- Machine translation
  - Either does too little:
    - They passed through the city at noon of the day following.
    - → German → Japanese →
    - They passed the city at noon the following day.
  - Or does too much:
    - Just remember that the things you put into your head are there forever, he said.
    - → German → Japanese →
    - You are dead, that there always is set, please do not forget what he said.

- Machine translation
- Imitation of an author

- Machine translation
- Imitation of an author
  - In a small study with 10 participants, not one managed to imitate Cormac McCarthy's writing well enough to fool our Writeprints feature set (not even 10% change in classification)

- Machine translation
- Imitation of an author
  - In a small study with 10 participants, not one managed to imitate Cormac McCarthy's writing well enough to fool our Writeprints feature set (not even 10% change in classification)
  - Even if this is managed, it is hard to sustain (e.g.
     "A Gay Girl in Damascus" Afroz and Greenstadt, 2012)

- Machine translation
- Imitation of an author
- Simply obfuscating your writing

- Machine translation
- Imitation of an author
- Simply obfuscating your writing
  - Brennan and Greenstadt (2009) showed that this can be done while writing the text (not for preexisting writing)

- Machine translation
- Imitation of an author
- Simply obfuscating your writing
  - Brennan and Greenstadt (2009) showed that this can be done while writing the text (not for preexisting writing)
  - However, the quality of the texts produced was far from scholarly

- Machine translation
- Imitation of an author
- Simply obfuscating your writing
  - Brennan and Greenstadt (2009) showed that this can be done while writing the text (not for preexisting writing)
  - However, the quality of the texts produced was far from scholarly
  - No way to "know" if you are doing the right thing

- Machine translation
- Imitation of an author
- Simply obfuscating your writing

#### Anonymouth



 Java based program that uses JStylo and machine learning techniques to attempt to aid users in severing stylometric ties between themselves and a document they authored

#### The Goals

 An efficient, usable, and effective tool to allow people to express their thoughts anonymously

#### The Goals

- An efficient, usable, and effective tool to allow people to express their thoughts anonymously
- Make clear that stylometry can be fooled, and therefore it cannot be relied upon absolutely

#### The Goals

- An efficient, usable, and effective tool to allow people to express their thoughts anonymously
- Make clear that stylometry can be fooled, and therefore it cannot be relied upon absolutely
- A tool that provides a usable interface between the outcomes from machine learning analytics and a user

#### **Key Contributions**

- JStylo-Anonymouth framework
  - Authorship attribution
  - Identifies changes required for document anonymization relative to a corpus
  - Assists the user making necessary changes accordingly

#### **Key Contributions**

- JStylo-Anonymouth framework
  - Authorship attribution
  - Identifies changes required for document anonymization relative to a corpus
  - Assists the user making necessary changes accordingly
- User study showed that Anonymouth is effective in determining what needs to be changed to achieve anonymization
  - But has trouble telling the user how to make the changes

Author A has a document D to anonymize

- Author A has a document D to anonymize
  - P: set of labeled documents written by A

- Author A has a document D to anonymize
  - P: set of labeled documents written by A
  - O: set of labeled documents written by N other authors ("blend-in" corpus)

- Author A has a document D to anonymize
  - P: set of labeled documents written by A
  - O: set of labeled documents written by N other authors ("blend-in" corpus)
  - F: set of linguistic features to extract

- Author A has a document D to anonymize
  - P: set of labeled documents written by A
  - O: set of labeled documents written by N other authors ("blend-in" corpus)
  - F: set of linguistic features to extract
  - C: classifier trained on  $P \cup O$

- Author A has a document D to anonymize
  - P: set of labeled documents written by A
  - O: set of labeled documents written by N other authors ("blend-in" corpus)
  - -F: set of linguistic features to extract
  - C: classifier trained on  $P \cup O$
- Goal: create D' from D where the extracted features from F are sufficiently changed such that:

$$\Pr[C(D') = A] \le \frac{1}{N+1}$$

### Framework

- JStylo
  - authorship attribution
- Anonymouth
  - authorship anonymization

## **JStylo**

- Standalone platform for authorship attribution
- Underlying feature extraction and authorship attribution engine of Anonymouth
- NLP for feature extraction
- Supervised machine learning:
  - Trains on documents of known candidate authors
  - Tests anonymous documents to attribute authorship
- Phases:
  - Problem set definition
  - Feature extraction
  - Classifiers selection
  - Analysis
- Powered by JGAAP, Weka

#### 1. Problem Definition

#### 2. Feature Selection

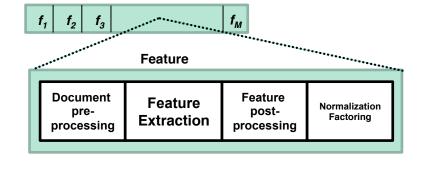
#### 3. Classifiers Selection

 $c_L$ 

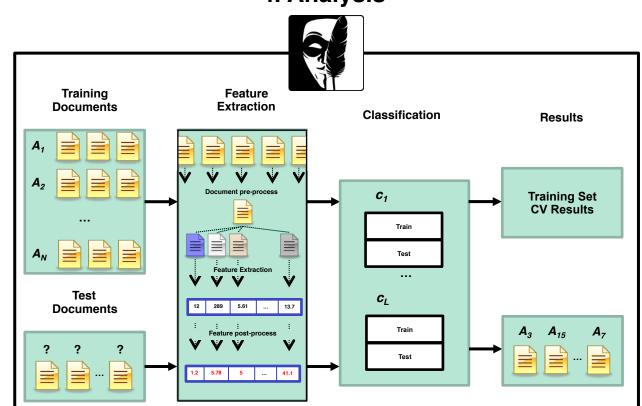
 $c_2 | c_3 |$ 



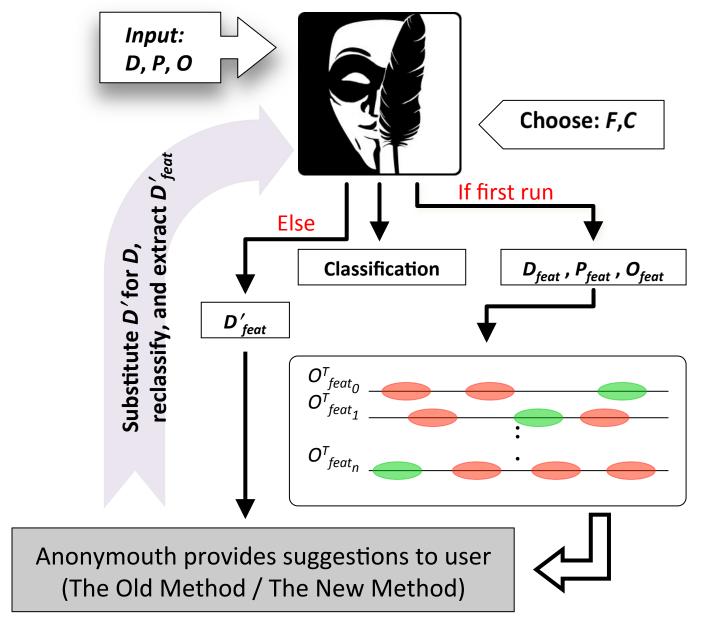








### General Design of Anonymouth

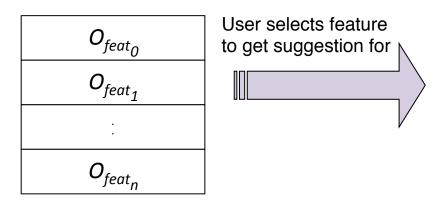


### Anonymouth's Clusters (updated display)

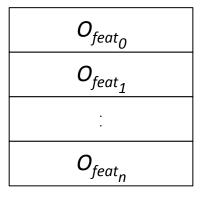


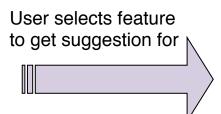
The green circles comprise the target cluster group, T. The red circles are the author's confidence interval for each feature, and the black dot on each plot is the present value of that feature in the author's document to anonymize

## First Try: The Old Method



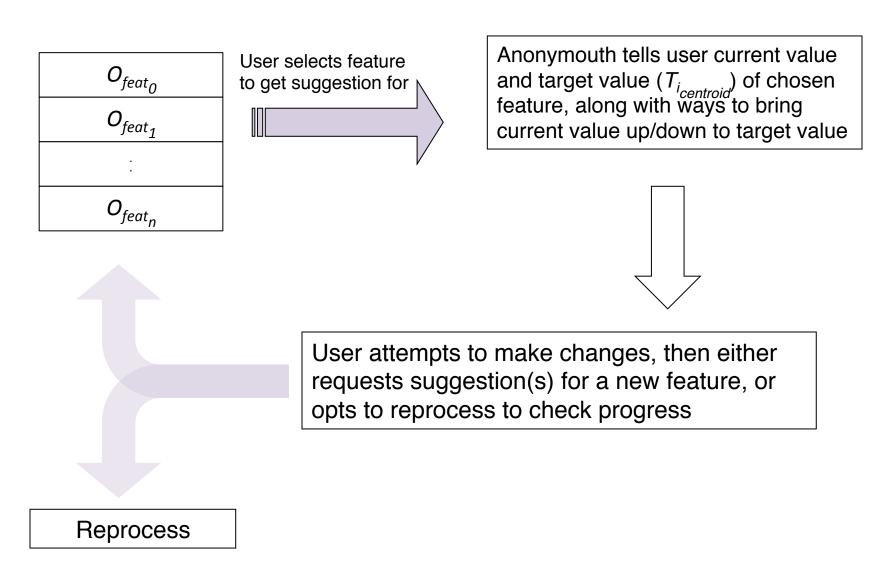
### First Try: The Old Method





Anonymouth tells user current value and target value ( $T_{i_{centroid}}$ ) of chosen feature, along with ways to bring current value up/down to target value

### First Try: The Old Method



 When people are able to do what is asked of them, they are able to anonymize their writing

- When people are able to do what is asked of them, they are able to anonymize their writing
- 8/10 participants were able to anonymize their writing with respect to JStylo's Basic-9 feature set

- When people are able to do what is asked of them, they are able to anonymize their writing
- 8/10 participants were able to anonymize their writing with respect to JStylo's Basic-9 feature set
- 7/10 were able to achieve a classification less than or equal to random chance

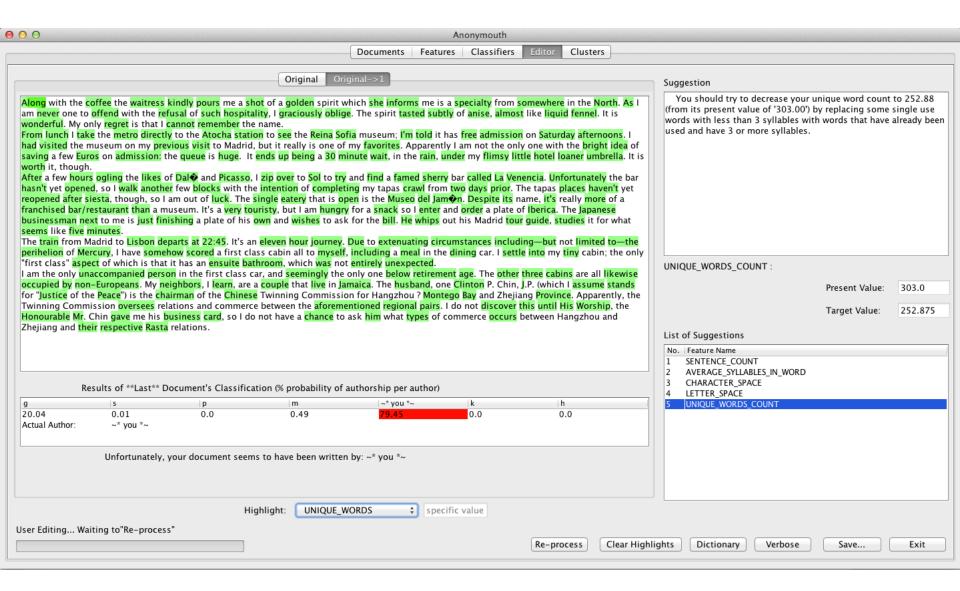
- When people are able to do what is asked of them, they are able to anonymize their writing
- 8/10 participants were able to anonymize their writing with respect to JStylo's Basic-9 feature set
- 7/10 were able to achieve a classification less than or equal to random chance
- But, no users were able to anonymize their writing using JStylo's Writeprints feature set

 However, changing ≈14% (≈100) of the features Anonymouth indicated, 8/10 user's documents were classified as having been written by a different author with 95% probability (Jstylo's Writeprints feature set)

- However, changing ≈14% (≈100) of the features Anonymouth indicated, 8/10 user's documents were classified as having been written by a different author with 95% probability (Jstylo's Writeprints feature set)
- Revealed that initial approach needed revision

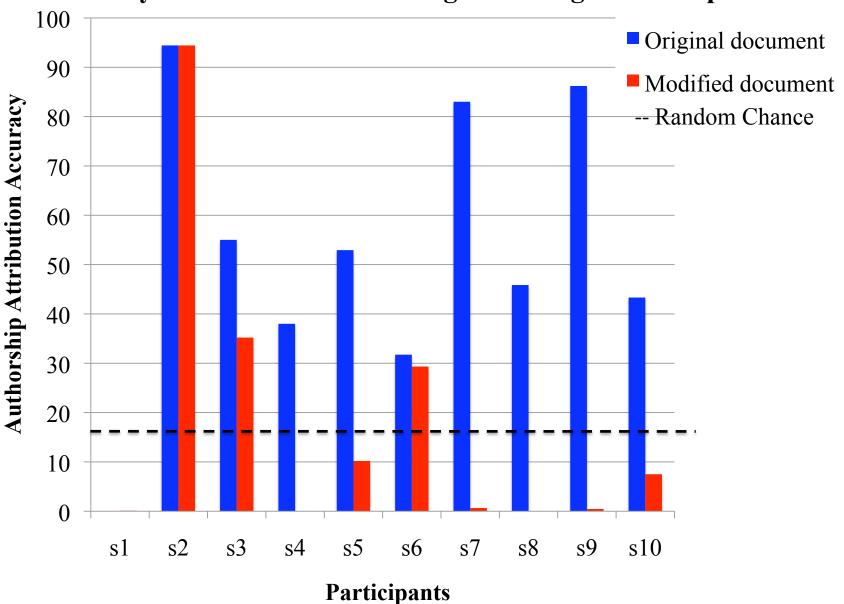
- However, changing ≈14% (≈100) of the features Anonymouth indicated, 8/10 user's documents were classified as having been written by a different author with 95% probability (Jstylo's Writeprints feature set)
- Revealed that initial approach needed revision
- Conclusion: Anonymouth was unusable, but core methodology sound
- Also, asking users to select cluster groups is problematic

#### Editor - Basic-9 Feature Set

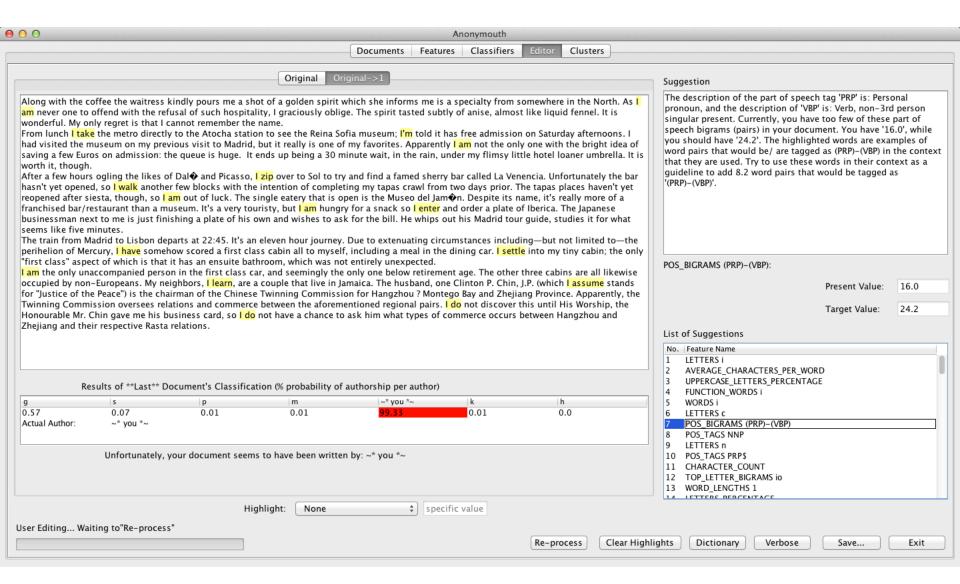


#### **Basic-9 Feature Set Results**

Anonymization in terms of original background corpus



### Editor – Writeprints Feature Set



### Next Steps: The New Method

- Need to present user with more feasible task
- Tweak / change cluster ordering algorithms to eliminate the need for user to select a cluster group
- Present document sentence by sentence, rather than all at once
- Ask to change words rather than specific features
- Allow user to shuffle and remove words to gain a different perspective / help user to see each sentence from a different perspective
- Find "best" synonyms for words
- (Possibly) analyze point of view (1<sup>st</sup>, 2<sup>nd</sup>, 3<sup>rd</sup> person), tense, and verb conjugation habits

**Extract POS tags using Stanford POS Tagger, wrap** each "word" in an object which keeps track of how many features from  $O_{feat}$  were found in that word.

Reprocess

changes to current sentence When user is satisfied with

User requests next sentence or opts to reprocess

For each word compute:

Anonymity Index = 
$$\sum_{i=0}^{n} \left( \frac{a_i}{T} \right) \times \left( g_i \right) \times \left( p_i \right)$$

Where:  $a_i$  = appearances of feature i in word; T = total features found in word;  $g_i$  = Information Gain of feature i; and  $p_i$  = percent change needed of feature i

> **Negative** Anonymity Index Anonymity Index

**Positive** 



Words to remove

Words to add

User may choose to "shuffle" sentence, with or without stripping "words to remove", which randomly reorganizes remaining words in sentence edit box

Present sentence to user with lists of words to add and to remove

### **Going Forward**

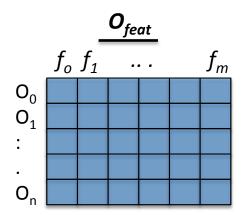
- Clustering is unreliable
- Usability:
  - What information should be given to the user?
  - What is the best way to get the user to make the changes needed to the document?
  - Testing our new method

### Questions?

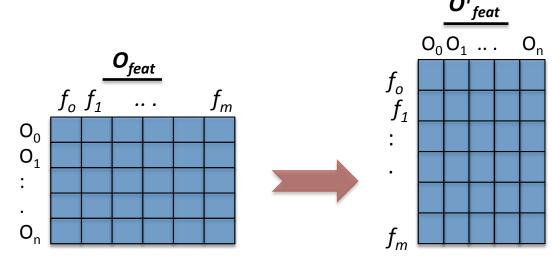
- Contact information:
  - Andrew McDonald
    - awm32@cs.drexel.edu
  - Sadia Afroz
    - sa499@cs.drexel.edu
  - Aylin Caliskan
    - ac993@cs.drexel.edu
  - Ariel Stolerman
    - ams573@cs.drexel.edu
  - Rachel Greenstadt
    - greenie@cs.drexel.edu
- Drexel PSAL website (to download JStylo and Anonymouth):
  - https://psal.cs.drexel.edu/index.php/JStylo-Anonymouth

- User inputs three sets of documents
  - **D**, **P**, and **O**
- He chooses
  - A feature set, F,
  - A classifier, C
- JStylo extracts features from D, P, and O, creating  $D_{feat}$ ,  $P_{feat}$ , and  $O_{feat}$ , respectively, and delivers a classification of document D among  $P \cup O$
- Anonymouth individually clusters the values of a single feature for all documents represented by  ${m O}^{\rm T}_{feat}$

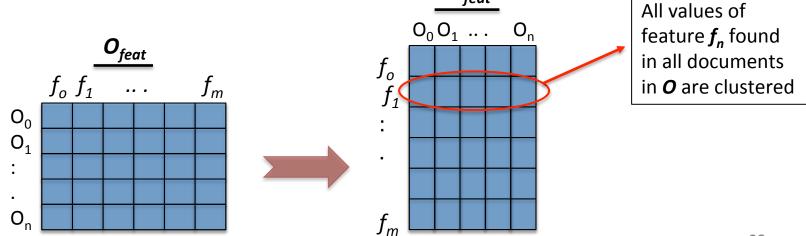
- User inputs three sets of documents
  - **D**, **P**, and **O**
- He chooses
  - A feature set, F,
  - A classifier, C
- JStylo extracts features from D, P, and O, creating  $D_{feat}$ ,  $P_{feat}$ , and  $O_{feat}$ , respectively, and delivers a classification of document D among  $P \cup O$
- Anonymouth individually clusters the values of a single feature for all documents represented by  ${m O}^{\tau}_{feat}$

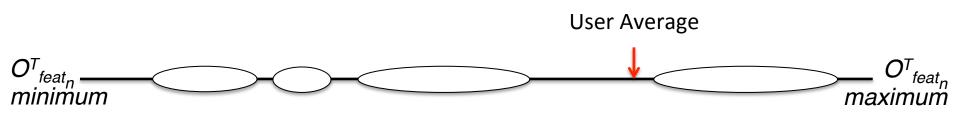


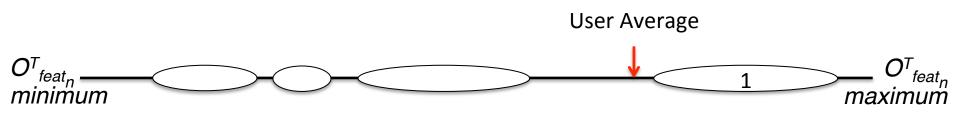
- User inputs three sets of documents
  - **D**, **P**, and **O**
- He chooses
  - A feature set, F,
  - A classifier, C
- JStylo extracts features from D, P, and O, creating  $D_{feat}$ ,  $P_{feat}$ , and  $O_{feat}$ , respectively, and delivers a classification of document D among  $P \cup O$
- Anonymouth individually clusters the values of a single feature for all documents represented by  $O_{feat}^{T}$

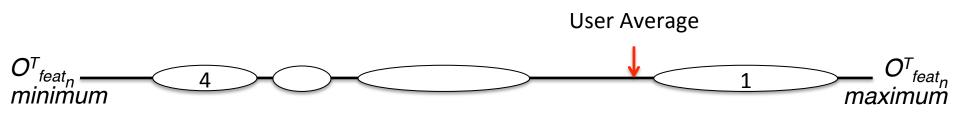


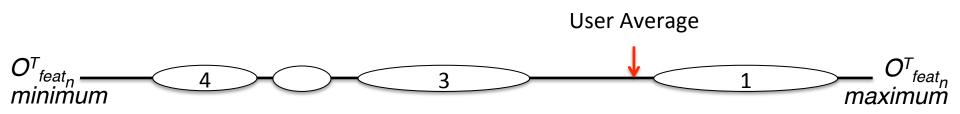
- User inputs three sets of documents
  - **D**, **P**, and **O**
- He chooses
  - A feature set, F,
  - A classifier, C
- JStylo extracts features from D, P, and O, creating  $D_{feat}$ ,  $P_{feat}$ , and  $O_{feat}$ , respectively, and delivers a classification of document D among  $P \cup O$
- Anonymouth individually clusters the values of a single feature for all documents represented by  $O_{feat}^{T}$

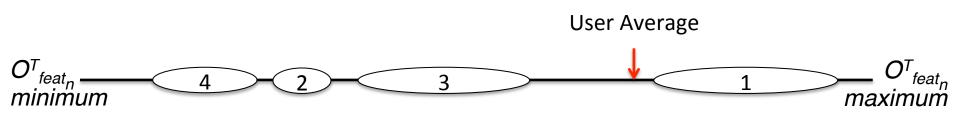


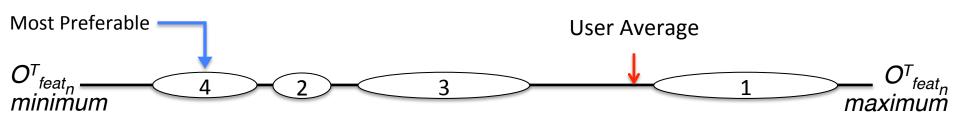


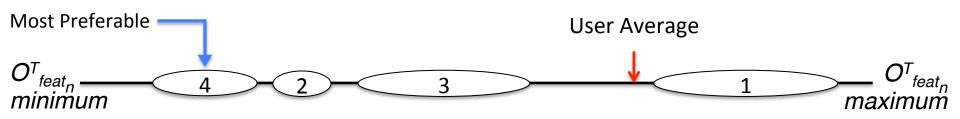




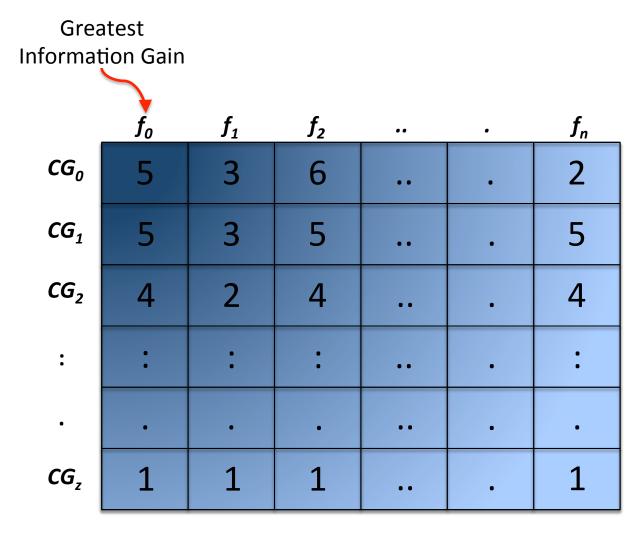


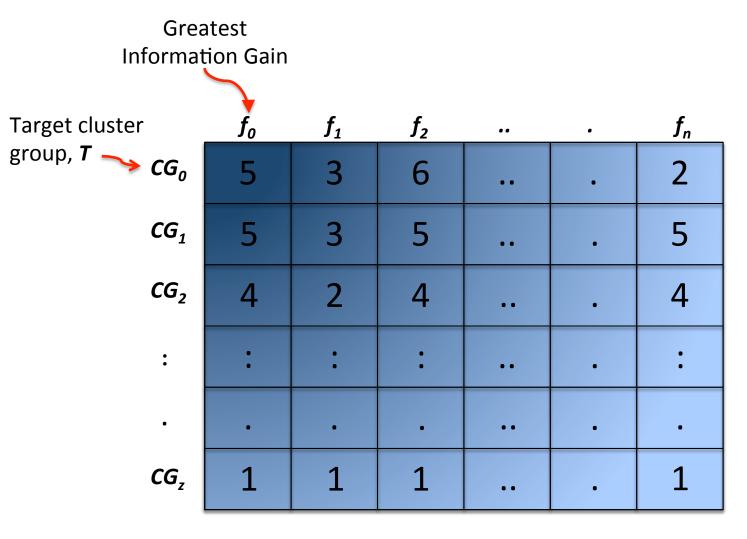




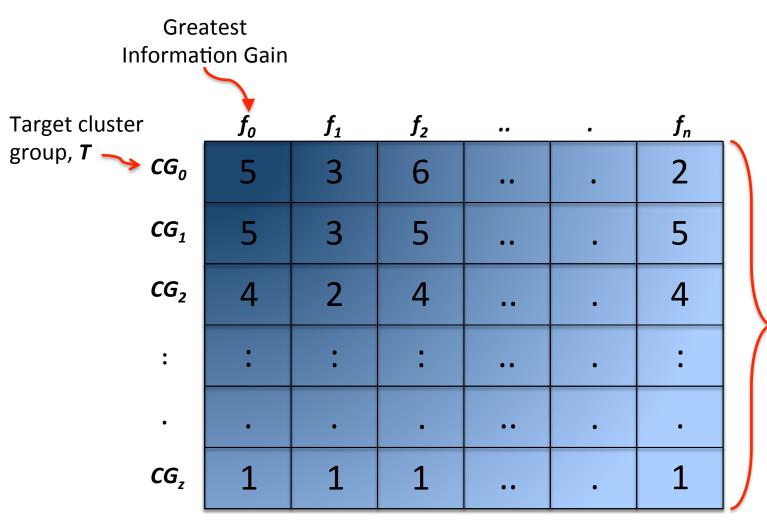


- Once all features have been clustered and ordered, cluster groups are assembled
  - Each cluster group represents at least one document





Gre	Least Information Gain						
Informa	***		n Gam				
Target cluster	$f_0$	$f_1$	$f_2$	••		$f_n$	
group, $T \longrightarrow CG_0$	5	3	6	••	•	2	
CG <sub>1</sub>	5	3	5	••	•	5	
CG <sub>2</sub>	4	2	4	• •	•	4	
:	:	:	•	••	•	:	
Least preferred cluster	•	•	•	••	•	•	
group $\sim$ $CG_z$	1	1	1	••		1	



Each cluster group's clusters must each contain one feature from at least a single document in *O* 

Greatest Information Gain			<b>T</b> contains preferable most impo			
Target cluster	$f_0$	$f_{\scriptscriptstyle 1}$	$f_2$	••	•	$f_n$
group, $T \longrightarrow CG_0$	5	3	6		•	2
CG <sub>1</sub>	5	3	5	••	•	5
CG <sub>2</sub>	4	2	4	••	•	4
:	••	•	:	••	•	•
		٠		••	•	•
CG <sub>z</sub>	1	1	1	••	•	1

respective features

