



# Mining Text Patterns over Fake and Real Tweets

Jose A. Diaz-Garcia<sup>1</sup>(✉) , Carlos Fernandez-Basso<sup>1</sup> , M. Dolores Ruiz<sup>2</sup> ,  
and Maria J. Martin-Bautista<sup>1</sup> 

<sup>1</sup> Department of Computer Science and A.I., University of Granada, Granada, Spain  
joseangeldiazg@ugr.es, {cjferba,mbautis}@decsai.ugr.es

<sup>2</sup> Department of Statistics and O.R., University of Granada, Granada, Spain  
mariloruiz@ugr.es

**Abstract.** With the exponential growth of users and user-generated content present on online social networks, fake news and its detection have become a major problem. Through these, smear campaigns can be generated, aimed for example at trying to change the political orientation of some people. Twitter has become one of the main spreaders of fake news in the network. Therefore, in this paper, we present a solution based on Text Mining that tries to find which text patterns are related to tweets that refer to fake news and which patterns in the tweets are related to true news. To test and validate the results, the system faces a pre-labelled dataset of fake and real tweets during the U.S. presidential election in 2016. In terms of results interesting patterns are obtained that relate the size and subtle changes of the real news to create fake news. Finally, different ways to visualize the results are provided.

**Keywords:** Association rules · Social media mining · Fake news · Text Mining · Twitter

## 1 Introduction

With the rise of social networks and the ease with which users can generate content, publish it and share it around the world, it was only a matter of time before accounts and people would appear to generate and share fake news. These fake news can be a real problem as it usually includes content that can go viral and be taken as true by a large number of people. In this way, political orientations, confidence in products and services, etc. can be conditioned. The textual nature of these news, has made it perfectly approachable by Data Mining techniques such as Text Mining, a sub area of Data Mining that tries to obtain relevant information from unstructured texts.

Because of the potential of these techniques in similar problems, in this paper we address the analysis of tweets that deal with fake content and real content by

using text mining by means of association rules. With this, we intend to prove that through these techniques relevant information can be obtained that can be used for the detection of patterns related to fake news. The contribution to the state of the art of paper is twofold:

- A reusable workflow that can get patterns on fake and real news, that can be the input of a posterior classification algorithm in order to discern between both types of news.
- A comprehensive analysis of patterns related to fake and real news during the 2016 US presidential election campaign.

In order to test and validate the system a tweet dataset has been used in which the tweets have been previously labelled as fake and real. The dataset [4] corresponds to tweets from the 2016 presidential elections in the United States. On this dataset, very interesting conclusions and patterns have been drawn, such as the tendency of fake news to slightly change real news to make it appear real. Different visualization methods are also offered to allow a better analysis of the patterns obtained.

The paper is structured as follows: Sect. 2 reviews some of the related theoretical concepts that allow to understand the following sections. Section 3 describes the related work. Section 4 explains the methodology followed. Finally Sect. 5 includes the experimentation carried out. The paper concludes with an analysis of the proposed approach and the future lines that this work opens.

## 2 Preliminar Concepts

In this section we will see the theoretical background of the Data Mining techniques that will be mentioned throughout the paper and that were used for the experimental development.

### 2.1 Association Rules

Association rules belong to the Data Mining field and have been used and studied for a long time. One of the first references to them dates back to 1993 [1]. They are used to obtain relevant knowledge from large transactional databases. A transactional database could be for example, a shopping basket database, where the items would be the products, or a text database, as in our case, where the items are the words. In a more formal way, let  $t = \{A, B, C\}$  be a transaction of three items ( $A$ ,  $B$  and  $C$ ), and any combination of them forms an itemset. Examples of different itemsets are  $\{A, B, C\}$ ,  $\{A, B\}$ ,  $\{B, C\}$ ,  $\{A, C\}$ ,  $\{A\}$ ,  $\{A\}$ ,  $\{B\}$  and  $\{C\}$ . According to this, an association rule would be represented in the form  $X \rightarrow Y$  where  $X$  is an itemset that represents the antecedent and  $Y$  an itemset called consequent. As a result, we can conclude that consequent items have a co-occurrence relationship with antecedent items. Therefore, association rules can be used as a method of extracting hidden relationships between items or

elements within transactional databases, data warehouses or other types of data storage from which it is interesting to extract information to help in decision-making processes. The classical way of measuring the goodness of association rules regarding a given problem is with two measures: support and confidence. To these metrics, new metrics have been added over time, among which the certainty factor [5] stands out, which we have used in our experimental process and we will define together with the support and confidence in the following lines.

- Support of an itemset. It is represented as  $supp(X)$ , and is the proportion of transactions containing item  $X$  out of the total amount of transactions of the dataset ( $D$ ). The equation to define the support of an itemset is:

$$supp(X) = \frac{|t \in D : X \subseteq t|}{|D|} \tag{1}$$

- Support of an association rule. It is represented as  $supp(X \rightarrow Y)$ , is the total amount of transactions containing both items  $X$  and  $Y$ , as defined in the following equation:

$$supp(X \rightarrow Y) = supp(X \cup Y) \tag{2}$$

- Confidence of an association rule. It is represented as  $conf(X \rightarrow Y)$  and represents the proportion of transactions containing item  $X$  which also contains  $Y$ . The equation is:

$$conf(X \rightarrow Y) = \frac{supp(X \cup Y)}{supp(X)} \tag{3}$$

- Certainty factor. It is used to represent uncertainty in rule-based expert systems. It has been shown to be one of the best models for measuring the fit of rules. Represented as  $CF(X \rightarrow Y)$ , a positive  $CF$  measures the decrease of probability that  $Y$  is not in a transaction when  $X$  appears. If we have a negative  $CF$ , the interpretation will be analogous. It can be represented mathematically as follows:

$$CF(X \rightarrow Y) = \begin{cases} \frac{conf(X \rightarrow Y) - supp(Y)}{1 - supp(Y)} & \text{if } conf(X \rightarrow Y) > supp(Y) \\ \frac{conf(X \rightarrow Y) - supp(Y)}{supp(Y)} & \text{if } conf(X \rightarrow Y) < supp(Y) \\ 0 & \text{otherwise} \end{cases} \tag{4}$$

The most widespread approach to obtain association rules is based on two stages using the downward-closure property. The first of these stages is the generation of frequent itemsets. To be considered frequent the itemset have to exceed the minimum support threshold. In the second stage the association rules are

obtained using the minimum confidence threshold. In our approach, we will employ the certainty factor to extract more accurate association rules due to the goo properties of this assessment measure (see for instance [9]). Within this category we find the majority of the algorithms for obtaining association rules, such as Apriori, proposed by Agrawal and Srikant [2] and FP-Growth proposed by Han et al. [10]. Although these are the most widespread approaches, there are other frequent itemset extraction techniques such as vertical mining or pattern growth.

### 2.2 Association Rules and Text Mining

Since association rules demonstrated their great potential to obtain hidden co-occurrence relationships within transactional databases, they have been increasingly applied in different fields. One of the fields is Text Mining [14]. In this field, text entities (paragraphs, tweets, ...) are handled as a transaction in which each of the words is an item. In this way, we can obtain relationships and metrics about co-occurrences in large text databases. Technically, we could define a text transaction as:

**Definition 1.** *Text transaction: Let  $W$  be a set of words (items in our context). A text transaction is defined as a subset of words, i.e. a word will be present or not in a transaction.*

In a text database, in which each tweet is a transaction, it will be composed of each of the terms that appear in that tweet once the cleaning processes have been carried out. So the items will be the words. The structure will be stored in a matrix of terms in which the terms that appear will be labelled with 1 and those that are not present as 0. For example for the transactional database  $D = \{t1, t2\}$  being  $t1 = (just, like, emails, requested, congress)$  and  $t2 = (just, anyone, knows, use, delete, keys)$  the representation of text transactions would be as we can see in Table 1.

**Table 1.** Example of a database with two textual transactions.

Transaction\Item	Anyone	Congress	Delete	Emails	Just	Keys	Knows	Like	Requested	Use
t1	0	1	0	1	1	0	0	1	1	0
t2	1	0	1	0	1	1	1	0	0	1

## 3 Related Work

In this section, we will see in perspective the use of Data Mining techniques applied in the field of fake news. This is a thriving area within Data Mining and more specifically Text Mining, in which there are more and more related articles published.

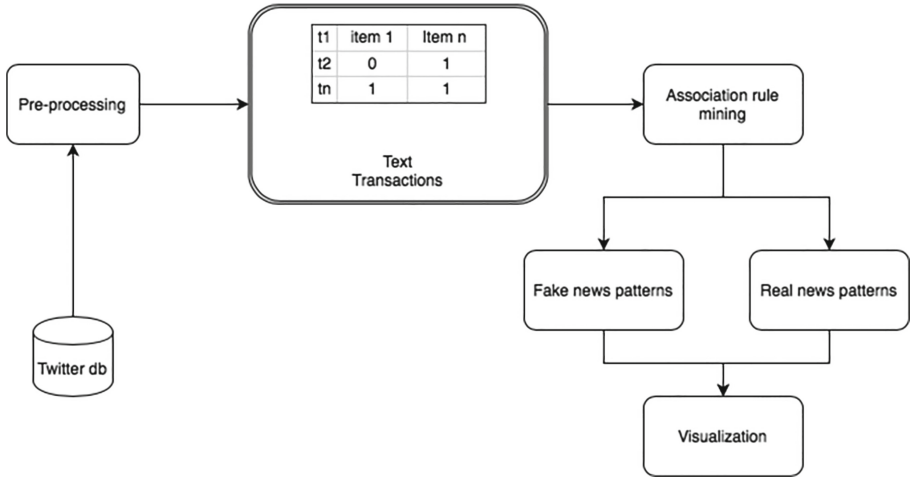
Within the field of text analysis or Natural Language Processing for the detection of fake news, solutions based on Machine Learning and concretely classification problems stand out. This is corroborated in the paper [7], where the authors make a complete review of the approaches to address the problem of analysing fakes news and clearly highlight the problems of classification either by traditional techniques or by deep learning. According to the traditional techniques we find works like [17], in which Ozbay and Alatas, apply 23 different classification algorithms over a set previously labelled fake news coming from the political scene. With this same approach we find the paper [8] in which, the authors apply again a battery of different classification methods that go from the traditional decision trees to the neural networks, all of them with great results. If we look at the branch of deep learning, we also find some works [13, 15, 16] in which the authors try to train neural network models to classify texts in fake news or real. If we look at other Machine Learning methods, another interesting work that focuses on selecting which features are interesting to classify fake news is the paper [18]. On the other hand, we also find solutions based on linear regression as presented by Luca Alfaro et al. in the paper [3]. These works, despite being at the dawn of their development, work quite well but are difficult to generalize to other domains in which they have not been trained.

Because of this, within the aspect of textual entities based on fake news, another series of studies appear that try to address the problem from the descriptive and unsupervised perspective of Text Mining. A very interesting work in this sense, because it combines NLP metrics with a rule-based system is [11], in which in a very descriptive way a solution is provided that is based on the combination of a rule-based system with metrics such as the length of the title, the % of stop-words or the proper names. In the same line there is the proposal in [6] in which authors try to improve the behaviour of a random forest classifier using Text Mining metrics like bigrams, or word frequencies. Finally, in this more descriptive aspect that combines classification and NLP or Text Mining techniques, we also find the social network analysis aspect [12], where the authors classify fake or real news in twitter according to network topologies, information dissemination and especially patterns in retweets.

As far as we know, this is the first work that applies association rules in the field of fakes news. By using this technique we will try to find out which patterns are related to fake news within our domain and try to generalize to possible general patterns related to fake news in other domains of the political field. Due to the impossibility of confronting the system against a similar one, we will carry out in the next sections a descriptive study of the obtained rules.

## 4 Our Proposal

In this section we will depict the procedure followed in our proposal. For that we will detail the pre-processing carried out on the data. We will also look at the pattern mining process on the textual transactions. For a better understanding we can look at Fig. 1. In it we can see how the first part of the process passes



**Fig. 1.** Process flow for association rule extraction in Twitter transactions

through pre-processing the data, then the textual transactions are obtained, the association rules are applied and results are obtained for fake and real news.

Through this processing flow, we offer a system that discovers patterns on fake and real news that can set the basis of new interesting input values for a latter system to, for instance, obtain and classify new coming patterns into real or fake news. In this first approach the system is able to obtain, in a very friendly and interpretable way for the user, which patterns or rules can be related to fake and/or real news.

#### 4.1 Pre-processing

The data obtained from Twitter are often very noisy so it is necessary a pre-processing step before working with them. The techniques used have been:

- Language detection. We are only interested in English tweets.
- Removal of links, removal of punctuation marks, non-alphanumeric characters, and missing values (empty tweets).
- Removal of numbers.
- Removal of additional white spaces.
- Elimination of empty words in English. We have eliminated empty English words, such as articles, pronouns and prepositions. Empty words from the problem domain have been also added, such as, the word via or rt, which can be considered empty since in Twitter it is common to use this word to reference some account from which information is extracted.
- Hashtags representing readable and interpretable terms are taken as normal words, and longer words which do not represent an analysable entity are eliminated.

- Retweets are removed.
- Content transformation to lower case letters.

At this point, we have a set of clean tweets on which we can apply the association rules mining techniques.

## 4.2 Mining Text Patterns

The first step in working with association rules and pattern mining in text is to obtain the text entities. To achieve this, the typical text mining corpus of tweets used so far has to be transformed into a transactional database. This structure requires a lot of memory since it is a very scattered matrix, taking into account that each item will be a word and each transaction will be a tweet. To create the transactions, the tweets have been transformed into text transactions as we saw in Sect. 2.2. We have used a binary version in which if an item appears in a transaction it is internally denoted with a 1, and if it does not appear in that transaction the matrix will have a 0.

The association rule extraction algorithm described in [1] has been used for the results. For this purpose, the parameters of minimum support threshold of 0.005 and minimum certainty factor of 0.7 have been chosen. For experimentation, we have varied the support value from 0.05 to 0.001, with fixed values of confidence and certainty factor.

## 5 Experimentation

In this section we will go into detail on the experimental process. We will study the dataset, the results obtained according to the input thresholds for the Apriori algorithm and finally the visualization methods used to interpret the operation of the system.

### 5.1 Dataset

In order to compare patterns from fake news and on the other from real news we have divided the dataset [4] into two datasets depending on whether they are labelled as fake news or not.

After this, we have two datasets, which will be analysed together but being able to know which patterns correspond to each one. The fake news dataset is composed of 1370 transactions (tweets), on the other hand, the real news dataset is composed of 5195 transactions.

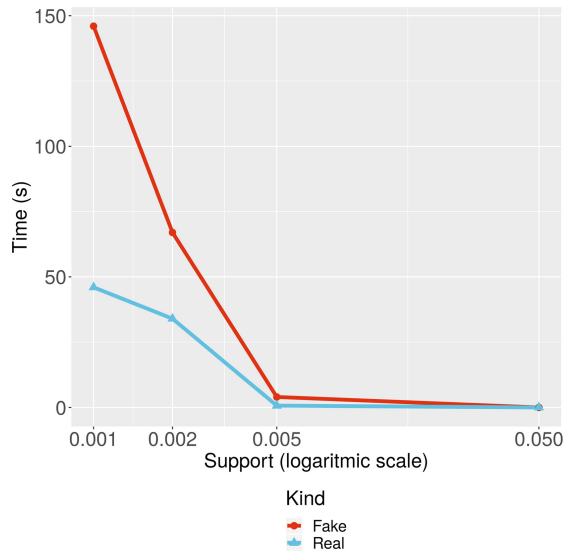
### 5.2 Results

The experimentation has been carried out with different values of supports aiming to obtain interesting patterns within the two sets of data. It is possible to

observe in Fig. 2 how the execution time is greater as the support decreases, due to the large set of items that we find with these support values.

In the Fig. 3 we can see the number of rules generated for the different support values. According to the comparison of both graphs we could draw a correlation between this graph and the previous runtime graph. As for the volume of rules generated and also the time in generating them (that as we have seen offers a graph of equal tendency), it is necessary to emphasize as the dataset fake offers more time and rules, in spite of having less transactions something that comes offered by the variability of the items inside this dataset.

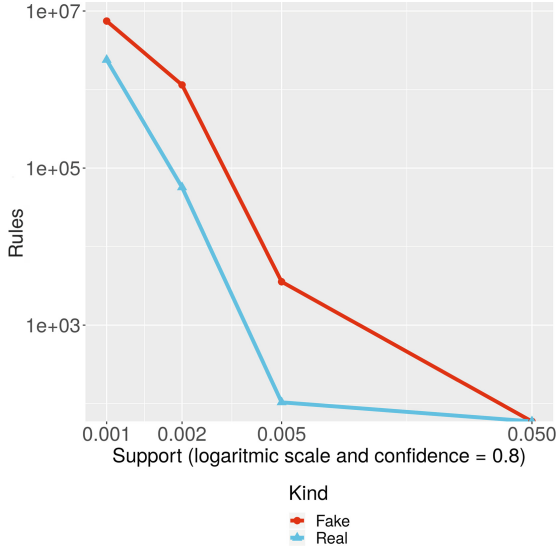
Moreover, in the Figures we see how the AprioriTID algorithm has an exponential increase in the number of rules and execution time when it is executed with low support values or with more transactions. This would rule out in versions based on Big Data, where the volume of input data increases and support must be lowered.



**Fig. 2.** Execution time of the experiments with different supports

This variability and an interpretation of the obtained patterns can be seen attending to the Table 2 where we have the strongest rules of both datasets. If we pay attention to its interpretation, it is curious how for both datasets we can find very similar rules but with some differences. This may be due to the fact that fake news are usually generated with real news to which some small element is changed. This is something that the rules of association discover for example in the rules  $\{sexism, won\} \rightarrow \{electionnight, hate\}$  for fake news and the rule  $\{sexism, won\} \rightarrow \{electionnight\}$  for real news. We can also observe how the tendency is to discover more items in the rules corresponding to fake news, probably caused by these sensationalist adornments that are usually charged to fake news.





**Fig. 3.** Number of rules of the experiments with different supports

**Table 2.** Example of rules obtained in the experiments

Antecedent	Consequent	Supp	Conf	Dataset
Electionnight, won, hate	Sexism	0.0075	0.909	Fake
Sexism, won	Electionnight; hate	0.0075	0.9	Fake
Didn't, trump, won, electionnight, sexism, win, racism	Hate	0.06	1	Fake
Sexism, won	Electionnight	0.0051	0.97	Real
Projects	Foxnews	0.005	1	Real

### 5.3 Visualization

A system that is easily interpretable must have visualization methods so we have focused part of the work on obtaining and interpreting interesting and friendly graphics on the fake and real news. We can observe the results obtained through the graphics of the Figures. In Fig. 4 we can see the rules obtained for the fake news, where we can appreciate that the resulting rules associate in great quantity of occasions to trump with sexist, winning or racist. But some of them are interesting because they indicate the opposite, like the rule that relates *racist*, *trump*, *didn't* and *sexist*.

On the other hand, in Fig. 5 we can see the rules obtained for the real news. Here we can see how fewer rules are obtained for experimentation and that the terms that appear in them encompass media such as *fox, news, usa* or *winning*. Studying the terms that appear in both examples we can see *racist* that in this case is associated with *fox* and *donald*.

Finally, a graph has been generated, which can be seen in Fig. 6, with the results of the fake news filtering the 80 rules with a higher certainty factor. It



Fig. 4. Example of rules in fake news



Fig. 5. Example of rules in real news

can be seen that there are three groups of terms, one with very interconnected negative terms and another with very frequent terms due to the subject matter.



Fig. 6. Example of rules in fake news

## 6 Conclusions and Future Work

In conclusion, we can see how the application of Data Mining on this kind of data allows us to extract hidden patterns. These patterns allow us to know better the terms more used in each type of news according to if it is false or real in addition to the interrelations between them.

Data mining techniques and, in particular, association rules have also been corroborated as techniques that can provide relevant and user-friendly information in Text Mining domains such as this.

In future works we will extend this technique in order to classify new tweets using the information provided after the application of association rule mining. Another application would be the use of the extracted patterns in order to create a knowledge base that can be applied in real time data.

**Acknowledgement.** This research paper is part of the COPKIT project, which has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 786687. Finally the project is also partially supported by the Spanish Ministry of Education, Culture and Sport (FPU18/00150) and the program of research initiation for master students of the University of Granada.

## References

1. Agrawal, R., Imieliński, T., Swami, A.: Mining association rules between sets of items in large databases. In: ACM SIGMOD Record, vol. 22, pp. 207–216. ACM (1993)
2. Agrawal, R., Srikant, R., et al.: Fast algorithms for mining association rules. In: Proceedings of 20th International Conference on Very Large Data Bases, VLDB, vol. 1215, pp. 487–499 (1994)
3. de Alfaro, L., et al.: Identifying fake news from Twitter sharing data: a large-scale study. coRR abs 1902.07207 (2019)
4. Amador Diaz Lopez, J., Oehmichen, A., Molina-Solana, M.: Fakenews on 2016 US elections viral tweets (November 2016–March 2017), November 2017. <https://doi.org/10.5281/zenodo.1048826>
5. Berzal, F., Blanco, I., Sánchez, D., Vila, M.A.: Measuring the accuracy and interest of association rules: a new framework. *Intell. Data Anal.* **6**(3), 221–235 (2002)
6. Bharadwaj, P., Shao, Z.: Fake news detection with semantic features and text mining. *Int. J. Nat. Lang. Comput. (IJNLC)* **8** (2019)
7. Bondielli, A., Marcelloni, F.: A survey on fake news and rumour detection techniques. *Inf. Sci.* **497**, 38–55 (2019)
8. Cordeiro, P.R.D., Pinheiro, V., Moreira, R., Carvalho, C., Freire, L.: What is real or fake?-Machine learning approaches for rumor verification using stance classification. In: IEEE/WIC/ACM International Conference on Web Intelligence, pp. 429–432 (2019)
9. Delgado, M., Ruiz, M.D., Sanchez, D.: New approaches for discovering exception and anomalous rules. *Int. J. Uncertainty Fuzziness Knowl.-Based Syst.* **19**(02), 361–399 (2011)
10. Han, J., Pei, J., Yin, Y.: Mining frequent patterns without candidate generation. In: ACM SIGMOD Record, vol. 29, pp. 1–12. ACM (2000)
11. Ibrishimova, M.D., Li, K.F.: A machine learning approach to fake news detection using knowledge verification and natural language processing. In: Barolli, L., Nishino, H., Miwa, H. (eds.) *Advances in Intelligent Networking and Collaborative Systems*, vol. 1035, pp. 223–234. Springer, Cham (2020). [https://doi.org/10.1007/978-3-030-29035-1\\_22](https://doi.org/10.1007/978-3-030-29035-1_22)
12. Jang, Y., Park, C.H., Seo, Y.S.: Fake news analysis modeling using quote retweet. *Electronics* **8**(12), 1377 (2019)
13. Kaliyar, R.K.: Fake news detection using a deep neural network. In: 2018 4th International Conference on Computing Communication and Automation (ICCCA), pp. 1–7. IEEE (2018)
14. Martin-Bautista, M., Sánchez, D., Serrano, J., Vila, M.: Text mining using fuzzy association rules. In: Loia, V., Nikraves, M., Zadeh, L.A. (eds.) *Fuzzy Logic and the Internet*, vol. 137, pp. 173–189. Springer, Heidelberg (2004). [https://doi.org/10.1007/978-3-540-39988-9\\_9](https://doi.org/10.1007/978-3-540-39988-9_9)
15. Molina-Solana, M., Amador Diaz Lopez, J., Gomez, J.: Deep learning for fake news classification. In: I Workshop in Deep Learning, 2018 Conference Spanish Association of Artificial Intelligence, pp. 1197–1201 (2018)

16. Monti, F., Frasca, F., Eynard, D., Mannion, D., Bronstein, M.M.: Fake news detection on social media using geometric deep learning. arXiv preprint [arXiv:1902.06673](https://arxiv.org/abs/1902.06673) (2019)
17. Ozbay, F.A., Alatas, B.: Fake news detection within online social media using supervised artificial intelligence algorithms. *Phys. A* **540**, 123174 (2020)
18. Reis, J.C., Correia, A., Murai, F., Veloso, A., Benevenuto, F., Cambria, E.: Supervised learning for fake news detection. *IEEE Intell. Syst.* **34**(2), 76–81 (2019)