Chapter 5
Brute Force Search Method for Cyberbullying Detection

ABSTRACT

In this chapter, the authors present a method for automatic detection of malicious internet contents, based on a combinatorial approach resembling brute force search algorithms, with application to language classification. The method automatically extracts sophisticated patterns from sentences and applies them in classification. The experiments performed on actual cyberbullying data showed advantage of this method to previous methods, including the one described in Chapter 4. Pros and cons of this method when compared to previous ones are also discussed in this chapter.

INTRODUCTION

Brute-force search algorithms, also known as exhaustive search algorithms, are a general group of algorithms applying combinatorial approach to problem solving. In particular, such algorithms firstly generate all possible answers to a problem, and then test the answer for its success. Combinatorial algorithms are especially useful in tasks where it is difficult to estimate a probable answer to narrow the scope of search. Therefore they have been traditionally used in password breaking and data decryption (Narayanan & Shmatikov, 2005; Paar, Pelzl & Preneel, 2010).

DOI: 10.4018/978-1-5225-5249-9.ch005

Copyright © 2019, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.

However, due to their minimal requirements when it comes to initial knowledge base, combinatorial algorithms have been also useful in Natural Language Processing, for example, in dependency parsing (Covington, 2001), stemming (Mishra & Prakash, 2012), or specific and novel tasks, such as extraction and analysis of emoticons (Ptaszynski et al., 2010).

However, brute-force approach often faces the problem of exponential and rapid growth of function values during combinatorial manipulations. This phenomenon is known as combinatorial explosion (Krippendorff, 1986). Since this phenomenon often results in very long processing time, combinatorial approaches have been often disregarded. We assumed however, that combinatorial explosion can be handled on modern hardware to the extent needed in our research. Moreover, optimizing the combinatorial approach algorithm specifically to problem requirements should shorten the processing time making it advantageous in the task of processing harmful language.

The method proposed in this chapter is original in following regards. As was pointed out by previous research (Ptaszynski et al., 2010), language used in cyberbullying messages is often deceptive and messy, and it is difficult to grasp a simple set of features to detect it. Therefore, to create a flexible model of cyberbullying, we applied a novel automatic feature extraction procedure. In research on machine learning, or applying any kind of machine learning to solve real world problems, one can use one of two approaches to feature extraction, namely, either automatic feature extraction (later called bottom-up approach) or select some custom predefined features (later called top-down approach, e.g., hand-crafting a lexicon of characteristic terms, etc.). The latter, although sometimes providing satisfying results, requires deep knowledge of the problem beforehand, meaning that the researchers need to figure out valid features themselves, which is inefficient.

In grand majority of NLP research, also in cyberbullying detection, applying the bottom-up approach, the features extracted automatically are typically based on separate words (as in e.g., bag-of-words) (Ptaszynski et al., 2010). Although instead of simple words one can use in text classification parts-of-speech or concepts (Sahlgren & Cöster, 2004), the sophistication of extracted pattern still does not exceed one token. A smaller number of research applies ngrams (usually unigrams to tetragrams of words or letters) (Damashek, 1995; Ponte & Croft, 1998; Siu & Ostendorf, 2000).

Recently, researchers have started to apply slightly more generalized version of ngrams, namely, skip-grams (Guthrie et al., 2006), which allow one controlled "skip", or a gap of a controlled distance. This however is still far from the definition of a pattern proposed here, namely, allowing any number

46 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage: www.igi-global.com/chapter/brute-force-search-method-for-cyberbullying-detection/217353

Related Content

The Use of Telepsychology in Clinical Practice: Benefits, Effectiveness, and Issues to Consider
Nicole Godineand Jeffrey E. Barnett (2013). *International Journal of Cyber Behavior, Psychology and Learning (pp. 70-83).*
www.irma-international.org/article/the-use-of-telepsychology-in-clinical-practice/102458

Exploring the Relationship between Facebook and Self-Esteem among Turkish University Students
Sevinç Mersinand Ali Aclar (2015). *International Journal of Cyber Behavior, Psychology and Learning (pp. 62-72).*
www.irma-international.org/article/exploring-the-relationship-between-facebook-and-self-esteem-among-turkish-university-students/145794

The Direct and Indirect Effects of Computer Uses on Student Success in Math
Sunha Kim, Mido Chang, Namok Choi, Jeehyun Parkand Heejung Kim (2016). *International Journal of Cyber Behavior, Psychology and Learning (pp. 48-64).*
www.irma-international.org/article/the-direct-and-indirect-effects-of-computer-uses-on-student-success-in-math/160697

Social Interaction Process Analysis of Bengalis' on Orkut®
Anupam Das (2010). *Handbook of Research on Discourse Behavior and Digital Communication: Language Structures and Social Interaction (pp. 66-87).*
www.irma-international.org/chapter/social-interaction-process-analysis-bengalis/42772

Online Friendship
Lijun Tang (2012). *Encyclopedia of Cyber Behavior (pp. 412-421).*
www.irma-international.org/chapter/online-friendship/64772