《报告名称》标题
子标题

Feb 21, 2020

Professor: *CP*

GentleCP

1. 一级标题

1.1 二级标题

1.1.1 三级标题

2. 项目列表

2.1 无序列表

默认带有原点

- hello, how are you?
- 你好，我是 cp

修改原点为其他

- hello, how are you?
* 你好，我是 cp

消除原点

2.2 有序列表

1. 默认 1
2. 默认 2
3. 默认 3

利用无序手动更改为有序, 并进行缩进

(1) 手动有序 1

(2) 手动有序 2

(3) 手动有序 3

与上间距

step 1 手动有序 1

step 2 手动有序 2

step 3 手动有序 3

更多间距调整内容参考latex 列表间距修改

3. 公式

3.1 无编号公式

多行公式

$$\begin{aligned} n^2+n+1 = & \\ & \leq n^2+n^2+n^2 \\ & = 3n^2 \\ & \leq c\cdot 2n^3 \end{aligned}$$

行内公式

后面是个公式 $f(n)=n^2+n+1$, $g(n)=2n^3$

3.2 带编号公式

$$\begin{aligned} z_o &= \sigma(W_o * (x_t, h_{t-1})) \\ z_f &= \sigma(W_f * (x_t, h_{t-1})) \\ z_i &= \sigma(W_i * (x_t, h_{t-1})) \\ z &= \tanh(W * (x_t, h_{t-1})) \end{aligned} \tag{1}$$

4. 代码

```
1
2 # 这是注释
3 def test():
4   pass
```

5. 图片

图 1: LSTM 基本结构单元

6. 表格

算法

Algorithm 1 Reliable Negative Instances Selection

Input: Positive Instance Set P, Unlabeled Instance Set U , Sample Ratio s.

Output: Reliable Negative Instance Set RN.

$setRN = \emptyset$
Sample s of the instances from P as S
Set $P_s = P - S$ with label 1, $U_s = U \cup S$ with label -1
Train a classifier g with P_s and U_s
Classify instances in U using g, output the class-conditional-probability
Select a threshold θ according to the class-conditional-probability of instances in S
for $d \in U$ do **do**
    if $Pr(1|d) \leq \theta, RN = RN \cup d$ **then**
    end if
end for
Output RN

表格 1

方法	特点	优点	缺点
有监督学习	对数据进行标注，通过有监督学习的方式来检测恶意 URL	更强的泛化能力	现实生活中很难获得精准的标注数据。在更多时候，我们可能只得到一小部分恶意 URL 和大量未标记的 URL 样本，缺乏足够可靠的负例样本
无监督学习	不需要对数据进行标注	无需标注的数据即可进行训练	已知恶意 URL 的标注信息就难以充分利用，可能无法达到令人满意的识别能力

表格 2

姓名	学号	性别
Steve Jobs	001	Male
Bill Gates	002	Female

表格 3 带编号

表 1: 表格哈哈哈哈

	$x \mod 5 = 0$	$x \mod 5 = 1$	$x \mod 5 = 2$	$x \mod 5 = 3$	$x \mod 5 = 4$
$x0$	0	2	4	1	3
$x1$	1	3	0	2	4

更多表格样式参考：表格样式

7. 参考文献

参考文献：[1]

参考文献

[1] KDD Cup. Available on: http://kdd. ics. uci. edu/databases/kddcup99/kddcup99. html, 2007.

[2] Mahbod Tavallaee, Ebrahim Bagheri, Wei Lu, and Ali A Ghorbani. A detailed analysis of the kdd cup 99 data set. pages 1–6, 2009.

[3] Daniel S Berman, Anna L Buczak, Jeffrey S Chavis, and Cherita L Corbett. A survey of deep learning methods for cyber security. *Information*, 10(4):122, 2019.

[4] Shmuel I Becher and Uri Benoliel. Law in books and law in action: The readability of privacy policies and the gdpr. *CONSUMER LAW & ECONOMICS, Klaus Mathis & Avishalom Tor, eds., Springer (forthcoming, 2019)*, 2019.

[5] Yajin Zhou and Xuxian Jiang. Dissecting android malware: Characterization and evolution. pages 95–109, 2012.

[6] Alex Krizhevsky, Ilya Sutskever, and Geoffrey E Hinton. Imagenet classification with deep convolutional neural networks. pages 1097–1105, 2012.

[7] Felix A Gers, Jürgen Schmidhuber, and Fred Cummins. Learning to forget: Continual prediction with lstm. 1999.

[8] Ian Goodfellow, Jean Pouget-Abadie, Mehdi Mirza, Bing Xu, David Warde-Farley, Sherjil Ozair, Aaron Courville, and Yoshua Bengio. Generative adversarial nets. pages 2672–2680, 2014.

[9] Wei Wang, Ming Zhu, Xuewen Zeng, Xiaozhou Ye, and Yiqiang Sheng. Malware traffic classification using convolutional neural network for representation learning. pages 712–717, 2017.

[10] Yann LeCun, LD Jackel, Léon Bottou, Corinna Cortes, John S Denker, Harris Drucker, Isabelle Guyon, Urs A Muller, Eduard Sackinger, Patrice Simard, et al. Learning algorithms for classification: A comparison on handwritten digit recognition. *Neural networks: the statistical mechanics perspective*, 261:276, 1995.

[11] Pablo Torres, Carlos Catania, Sebastian Garcia, and Carlos Garcia Garino. An analysis of recurrent neural networks for botnet detection behavior. pages 1–6, 2016.

[12] Jonathan Woodbridge, Hyrum S Anderson, Anjum Ahuja, and Daniel Grant. Predicting domain generation algorithms with long short-term memory networks. *arXiv preprint arXiv:1611.00791*, 2016.

[13] Hieu Mac, Duc Tran, Van Tong, Linh Giang Nguyen, and Hai Anh Tran. Dga botnet detection using supervised learning methods. pages 211–218, 2017.