Statistical hypotheses (true positive, false negative etc...) and errors types

Franck Jeannot

Montréal, Canada, Juillet 2018, S544, v1.1

Abstract

A review of the confusing terms true positive, true negative, false positive, false negative and associated Type I and Type II errors used in several fields like cybersecurity and machine-learning.

Keywords: Statistical Hypotheses, Type I error (False positive), Type II error (False negative), null hypothesis significance testing (NHST)

1. Statistical Hypotheses and errors types matrix

Table of error types		Condition. Null Hypothesis is ...	
		TRUE (condition absent)	**FALSE (condition present)**
Decision about null Hypothesis (test outcome)	**(negative test result)**	**True Negative**	**Type II error False Negative**
	Reject (positive test result)	**Type I error False positive**	**True positive**

FIGURE *(1): Synthesis of the statistical outcomes and corresponding error types*

2. Introduction

The basic thing to remember is that the "positive/negative" part relates to the **test results** while the "true/false" is the **link from the test results to the real input and answers to the question if the decision was correct**.

3. Type I and Type II errors

« *A type I error is to falsely infer the existence of something that is not there, while a type II error is to falsely infer the absence of something that is* ».[1] A type I error occurs when the null hypothesis (H_0) is true, but is rejected. It is asserting something that is absent, a false hit. A type I error may be likened to a so-called false positive (a result that indicates that a given condition is present when it actually is not present). A type II error occurs when the null hypothesis is false, but erroneously fails to be rejected. It is failing to assert what is present, a miss.

4. Examples

4.1. Malware

- A **true positive** is recognized if real malware was detected as malware.
- A **false positive** occurs if the test of malware was positive, i.e., detected malware, but the real file is NOT a malware. That is, the (positive) test result was false.
- A **true negative** is the correct situation in which "no malware" was detected as "no malware".
- A **false negative** is something like a "Missed SPAM" in which malware came in but was not recognized as that.[2]

DNH : Decision about Null hypothesis

Table of error types		Condition (Null Hypothesis is . . .)	
		TRUE (condition Absent)	FALSE (condition present)
DNH	(negative test result)	**true negative** is the correct situation in which "no malware" was detected as "no malware".	**Type II error** **false negative** is something like a "Missed SPAM" in which malware came in but was not recognized as that
	Reject as malware (positive test result)	**Type I error** **false positive** detected malware, but the real file is NOT a malware	**true positive** is recognized if real malware was detected as malware

1. https://en.wikipedia.org/wiki/Type_I_and_type_II_errors
2. https://blog.webernetz.net/at-a-glance-false-positive-etc/

4.2. Spam

— A true positive : a spam email was correctly identified as spam
— A true negative : a legitimate email was not identified as spam
— A false positive : a legitimate email was wrongly identified as spam
— A false negative : a spam email was identified as spam (spam got through) [3]

4.3. Pregnancy

— A true positive : a person we told is pregnant that really was.
— A true negative : a person we told is not pregnant, and really wasn't.
— A false negative : a person we told is not pregnant, though they really were.
— A false positive : a person we told is pregnant, though they weren't.

4.4. IDS and IPS

— A true positive occurs when an IDS or IPS correctly identifies malicious traffic as malicious. For instanc, a true positive occurs when a virus or an attack is identified and the action is taken.
— A true negative occurs when an IDS or IPS correctly identifies harmless traffic as harmless. For example, a true negative occurs when an administrator correctly enters a pasword or when HTTP traffic is sent to a web server.
— A false negative occurs when an IDS or IPS does not identify malicious traffic that enters the network.
— A false positive occurs when an IDS or IPS identifies nonmalicious traffic as malicious. [4]

5. Sensitivity and specificity

Sensitivity and **specificity** are statistical measures of the performance of a binary classification test. [5]

6. Confusion matrix

A specific table layout that allows visualization of the performance of an algorithm that uses **sensitivity** and **specificity**. [6]

3. https://www.cyren.com/blog/articles/the-micro-guide-to-spam-terminology-false-positives-false-negatives-and-true-stuff-1219
4. Ref Syngress CISSP Study guide, 3rd ed, chap. 8, IDS and IPS Event types, pp 363-364
5. https://en.wikipedia.org/wiki/Sensitivity_and_specificity
6. https://en.wikipedia.org/wiki/Confusion_matrix

7. Alerting and Risk Vs Quality

The quality of an alert process is improved by reducing false positives. The risk of an alert process is decreased by reducing false negatives.[7]

8. History and etymology

Perezgonzalez, Jose D, in 2015, described [1] the **history** and also **controversy**[8] of the *null hypothesis significance testing* (**NHST**). The discussions in the 1928-1935 period between, Jerzy NEYMAN [2] (1894–1981), Egon PEARSON [3] (1895–1980) and British statistician Sir Ronald Aylmer FISHER (1890–1962) are the main sources of the H_0 notation usage and of the terms **errors of type I**, **errors of type II** (Neyman-Pearson) and ***null hypothesis*** term.

Références

[1] J. D. Perezgonzalez, Fisher, neyman-pearson or nhst ? a tutorial for teaching data testing, Frontiers in Psychology 6 (2015) 223. doi:10.3389/fpsyg.2015.00223.
URL https://www.frontiersin.org/articles/10.3389/fpsyg.2015.00223/full

[2] J. Neyman, E. S. Pearson, The testing of statistical hypotheses in relation to probabilities a priori 29 (1933) 492 – 510.

[3] E. Pearson, J. Neyman, On the problem of two samples, Imprimerie de l'université, 1930.
URL https://books.google.ca/books?id=J0ZIAQAAIAAJ

7. https://www.arcriskandcompliance.com/the-science-behind-false-positive-tuning-2/

8. https://www.phil.vt.edu/dmayo/personal_website/Neyman-1956.pdf