

Varianzanalyse

Cooler Untertitel, den wir uns noch ausdenken

Henri Neumann & Robert Feldhans

15. Dezember 2016

Experimentelle Psychologie für Nichtpsychologen

1. Henri
2. Robert
3. Historische Einordnung
4. Malware und ihre Hauptverteilwege
5. Antiviren-Programme
6. Wirksame Maßnahmen gegen Viren

Henri

Definition

Verfahren, welches die Wirkung einer (oder mehrerer) UV auf eine (oder mehrerer) AV untersucht.

- testet Unterschiede zw. Mittelwerten auf Signifikanz
- Einsatz bei mehr als 2 Stichproben

- Zielvariable: abhängige Variable(AV)
- Faktor: unabhängige Variable(UV)
- Faktorstufen: Ausprägungen/Kategorien eines Faktors
- Effekt: Wirkung eines Faktors auf die AV
- Interaktionseffekt: kombinierte Wirkung zweier Faktoren auf die AV

Abgrenzung anhand von Anzahl abhängige Variablen und Faktoren

Zahl der AVn	Zahl der UVn	Bezeichnung
1	1	Einfaktorielle VA
1	2	Zweifaktorielle VA
1	3	Dreifaktorielle VA
	usw.	
≥ 2	≥ 1	Multivariate VA
≥ 1	≥ 2	Kovrianzanalyse

- Fehlerkomponenten sind normalverteilt
- Fehlervarianzen homogen in den Faktorstufen
- Messwerte bzw. Faktorstufen sind unabhängig voneinander

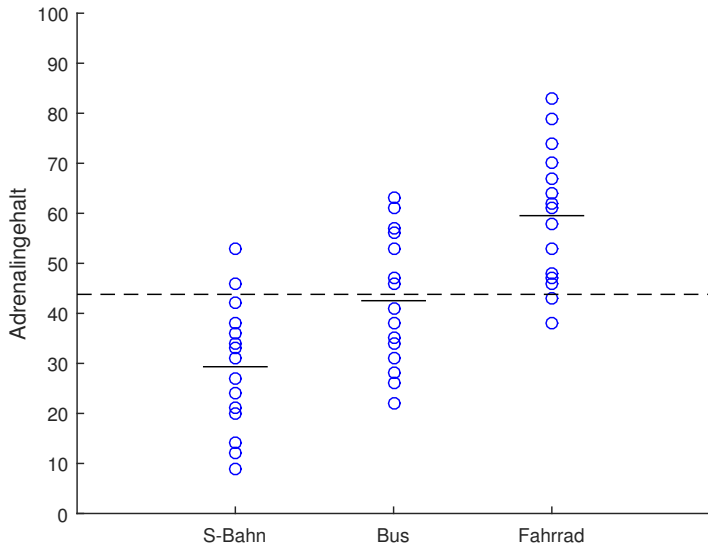
Prinzip der Varianzanalyse

Die gesamte Varianz der AV wird aufgeteilt in:

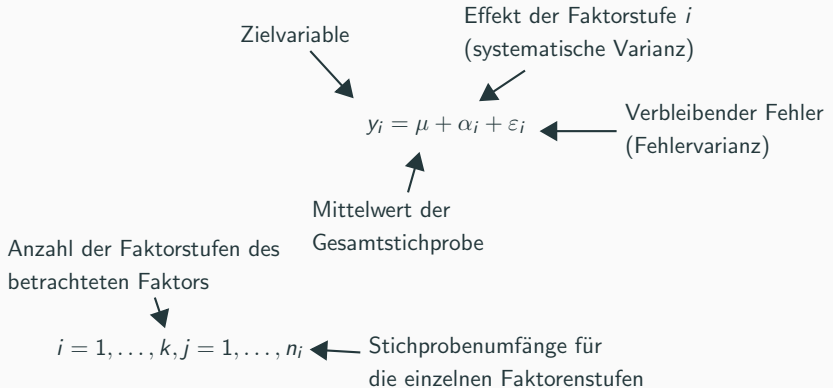
- Varianz *zwischen* Gruppen:
Abweichung der Gruppenmittelwerte vom Gesamtmittelwert
= systematische Varianz
- Varianz *innerhalb* von Gruppen:
Abweichung einzelner Messwerte vom Gruppenmittelwert
= unsystematische Varianz, Fehlervarianz

⇒ anschließend Vergleich der Varianzschätzungen

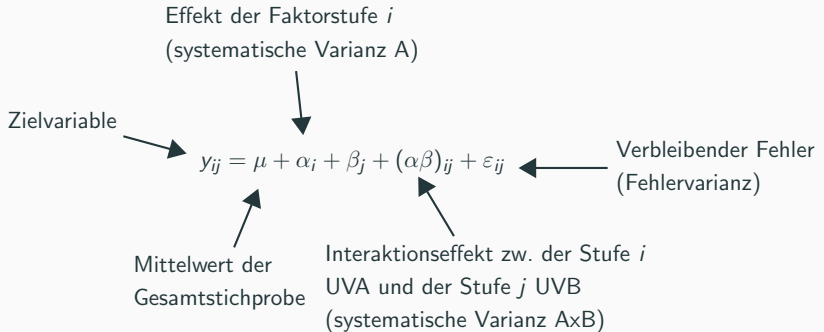
Prinzip der Varianzanalyse



Allgemeines Modell der einfaktoriellen Varianzanalyse



Allgemeines Modell der zweifaktoriellen Varianzanalyse



einfaktoriell

- Nullhypothese:

Alle Mittelwerte sind gleich oder alle Effekte α_i sind Null.

Formal: $H_0 : \mu_1 = \mu_2 = \dots = \mu_k$ oder $\sum \alpha_i^2 = 0$

- Alternativhypothese:

Nicht alle Mittelwerte sind gleich oder mindestens ein Effekt α_i ist ungleich Null.

Formal: $H_1 : \sum (\mu_k - \mu)^2 > 0$ oder $\sum \alpha_i^2 > 0$

zweifaktoriell

Für jeden Faktor wird eine Nullhypothese überprüft(über alle Bedingungen des anderen Faktors):

- Faktor A:

Alle Zeilenmittelwerte sind gleich oder alle Effekte α_i sind Null.

Formal: $H_0 : \mu_{1\cdot} = \mu_{2\cdot} = \dots = \mu_{k\cdot}$ oder $\sum \alpha_i^2 = 0$

- Faktor B:

Alle Spaltenmittelwerte sind gleich oder alle Effekte β_j sind Null.

Formal: $H_0 : \mu_{\cdot 1} = \mu_{\cdot 2} = \dots = \mu_{\cdot n}$ oder $\sum \beta_j^2 = 0$

Zweifaktorielle VA

		UV B				Zeilenmittel
		B_1	B_2	\dots	A_n	HE A
UV A	A_1	μ_{11}	μ_{12}	\dots	μ_{1n}	$\mu_{1\cdot}$ $= \mu + \alpha_1$
	A_2	μ_{21}	\dots	\dots	\dots	$\mu_{2\cdot}$ $= \mu + \alpha_2$
	\dots	\dots	\dots	\dots	\dots	$\mu_{i\cdot}$ $= \mu + \alpha_i$
	A_k	μ_{k1}	\dots	\dots	μ_{kn}	$\mu_{k\cdot}$ $= \mu + \alpha_k$
Spalten- mittel	HE B	$\mu_{\cdot 1}$ $= \mu + \beta_1$	$\mu_{\cdot 2}$ $= \mu + \beta_2$	$\mu_{\cdot j}$ $= \mu + \beta_i$	$\mu_{\cdot n}$ $= \mu + \beta_n$	μ

Robert

Historische Einordnung

Beginn des Schlangenöls

- aus Mythologie des Wilden Westens
- von Wunderheilern eingesetzt
- Heilmittel für Gebrechen aller Art



- versprochenes Wundermittel
- unübersichtliche Bereiche, oft in Technik
- wenig Wirkung
- Heutige Anwendungen oft in Kryptografie und Antiviren-Software

Malware und ihre Hauptverteilwege

Malware

Software, welche schädliche Funktionen ausführen

- Viren
- Würmer
- Trojanische Pferde
- Ransomware
- ...
- **nicht:** fehlerhafte Software

Verschiedene Malware

Virus

Schadprogramm, welches sich verbreitet, in dem es sich in andere Software einschleust. Durch das Kopieren dieser wird der Virus passiv verbreitet (und dabei oft nur lokal)

Wurm

Schadprogramm, welches sich aktiv ausbreitet, in dem es Sicherheitsprobleme ausnutzt. Für Nutzer kaum unterschiedlich zu Viren

Trojanisches Pferd

Schadprogramm, welches sich als nützliche Anwendung tarnt und ohne Wissen des Anwenders (auch) schädliche Funktionen ausführt

Anzahl Malware

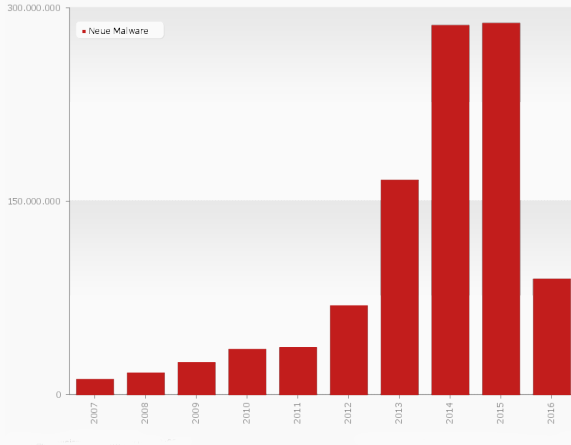


Abbildung 1: Registrierung neuer Schadprogramme in den letzten 10 Jahren. Quelle: avtest

- E-Mail-Dateianhänge
- Drive-by-Downloads
- Datenträger
- Netzwerke

Problem

Viele Statistiken zu Malware und ihren Verteilwegen werden von Antiviren-Software-Firmen angeboten

- wenige **unabhängige** Quellen
- Quantität schwer einzuschätzen
- nur bekannte Probleme aufgelistet

Antiviren-Programme

Wie schützen wir uns vor Viren?

Wir installieren ein Antiviren-Programm!

Zahlen zu AV-Installationen

- AVG Antivirus Free (32 & 64 bit) 22.3M
- avast Free Antivirus 19.4M
- Ad-Aware Free Antivirus 9.2M

jeweils in Millionen Downloads bei Chip (Windows)

Virtualisierung

Idee: Wir tun nur so, als würden wir verdächtigen Code laufen lassen, überwachen tatsächlich seine Verhaltensweise

Firewall

Idee: Ein- und ausgehende Kommunikation überwachen, um Kommunikation von Malware zu verhindern/ Malware zu finden

Problem

Sobald die Kommunikation verschlüsselt abläuft, wird die Überwachung beliebig kompliziert

Antiviren-Browser

Idee: Wir halten den Nutzer davon ab, schädliche Dateien herunterzuladen, indem wir einen Browser bereitstellen, der gefährliche Websites u.Ä. blockiert

Wirksame Maßnahmen gegen Viren

„We cant write secure software. Why are people suprised that we also can not write secure security software?“

Fragen?

Quellen I

- blog.fefe.de
- sherpablog.marketingsherpa.com/wp-content/uploads/2016/02/Snake-Oil-Cures-All.jpeg
- itwissen.info/definition/lexikon/ (diverse Definitionen)
- de.wikipedia.org/wiki/Schadprogramm
- av-test.org/de/statistiken/malware/
- netmarketshare.com/operating-system-market-share.aspx?qprid=10&qpcustomd=0
- bsi.bund.de/DE/Publikationen/Lageberichte/bsi-lageberichte.html
- Chip.de (diverse AV-Downloadseiten)
- bugs.chromium.org/p/project-zero/issues/detail?id=769
- de.urbandictionary.com/define.php?term=Startkeylogger

Quellen II

- bugs.chromium.org/p/project-zero/issues/detail?id=564&redir=1
- news.softpedia.com/news/avast-safezone-browser-lets-attackers-access-your-filesystem-499990.shtml
- imgur.com/Smwnzx3
- www.heise.de/security/meldung/Authentifikation-von-McAfees-Enterprise-Security-Manager-loechrig-3036068.html
- www.heise.de/security/meldung/Symantec-Endpoint-Protection-Gefaehrlicher-Sicherheitsluecken-Cocktail-2768461.html
- thehackernews.com/2015/07/bitdefender-hacked.html?m=1
- www.heise.de/mac-and-i/meldung/Apple-Anti-Viren-Apps-fuer-iOS-irrefuehrend-2581916.html
- www.heise.de/security/meldung/Antiviren-Software-und-Apples-Schutzmechanismen-fuer-Mac-OS-X-nutzlos-2620049.html