Statische Analyse

- Was ist es?
- Warum nutzt man sie?
- Wo wird sie (nicht) eingesetzt?

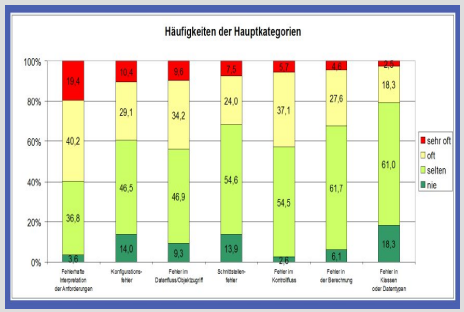
- **Jens-D. Doll**
- **Context IT**
- **www.cococo.de**

fehlerfreie Software

- ✓ Programm
  (Datenfluß, Kontrollfluß, Berechnung)
- ✓ Umgebung
  (Konfiguration, Schnittstellen, Klassen)
- ✓ Anforderungen

}

GI-Umfrage
(7 von 7 Kategorien)



automatisch erkennbare Softwarefehler

✓ Programm

(Datenfluß, Kontrollfluß, Berechnung)

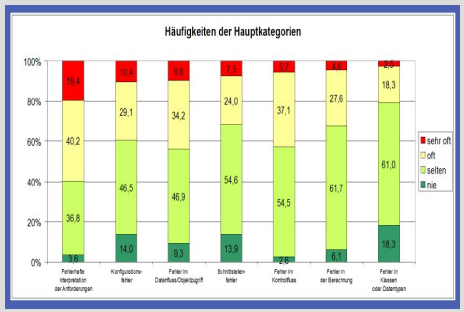
? Umgebung

(Konfiguration, Schnittstellen, Klassen)

Anforderung

}

GI-Umfrage
(3 von 7 Kategorien)



Hauptursachen für technische Fehler

Arithmetik/Algebra	Überlauf, Nulldivision	nicht behebbar
Wertebereiche	Indizes, Tabellen Felder	
Initialisierungen	Variablen, Pointer	
Grenzen	Speicher, Zeit	
.....		

Allgemeinere Ursache Definitionslücke

Diskrepanzen

i) zwischen syntaktisch und semantisch korrekten

ii) zwischen semantisch und operational möglichen

iii) wegen mehrdeutiger Formulierungsmöglichkeiten

Theorie formaler Sprachen

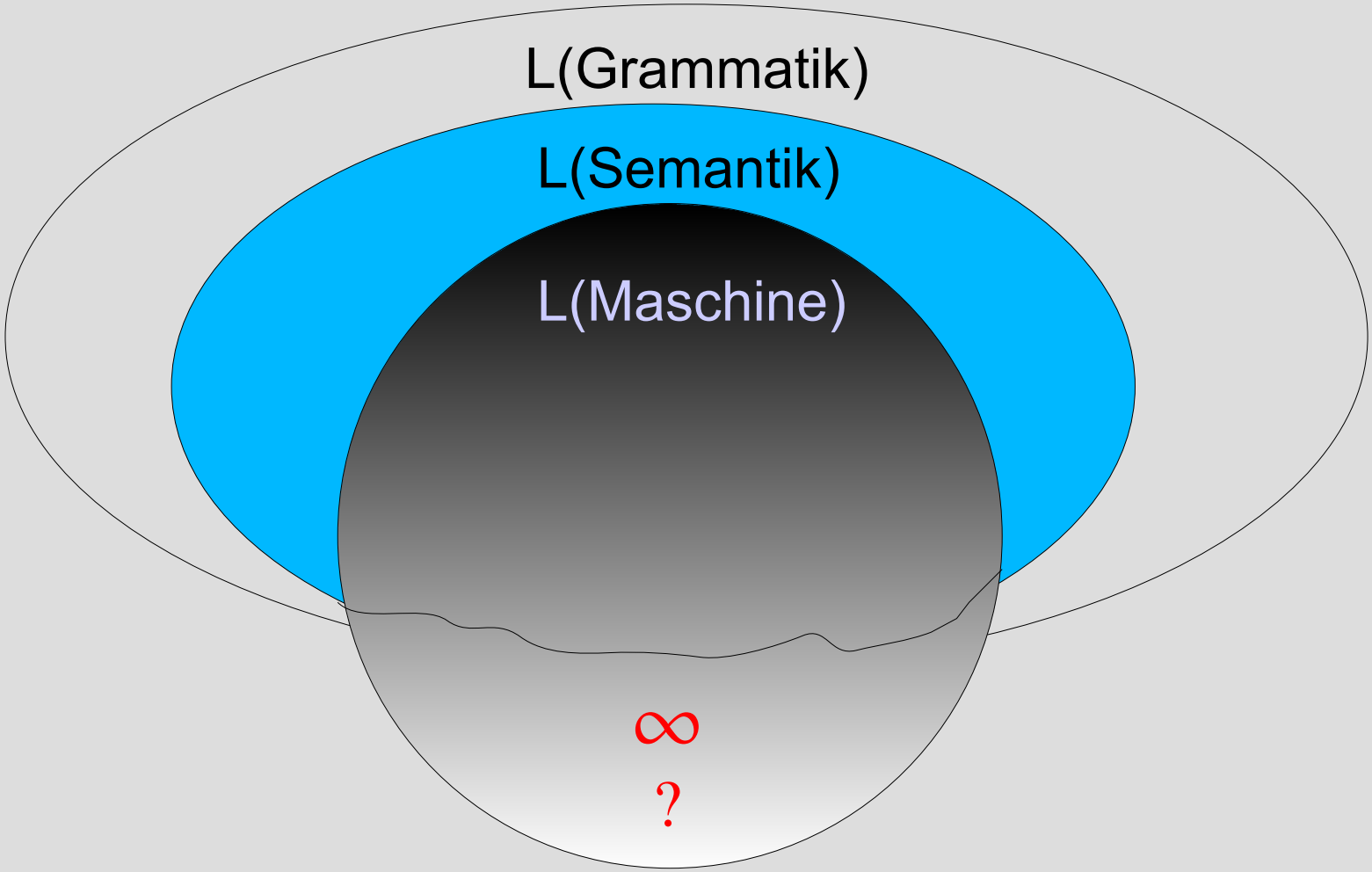
L(Grammatik) $\supseteq$ L(Programmiersprache)

L(Semantik) ist nicht reduziert/minimal

=> Programmiersprachen sind nicht hinreichend definiert!

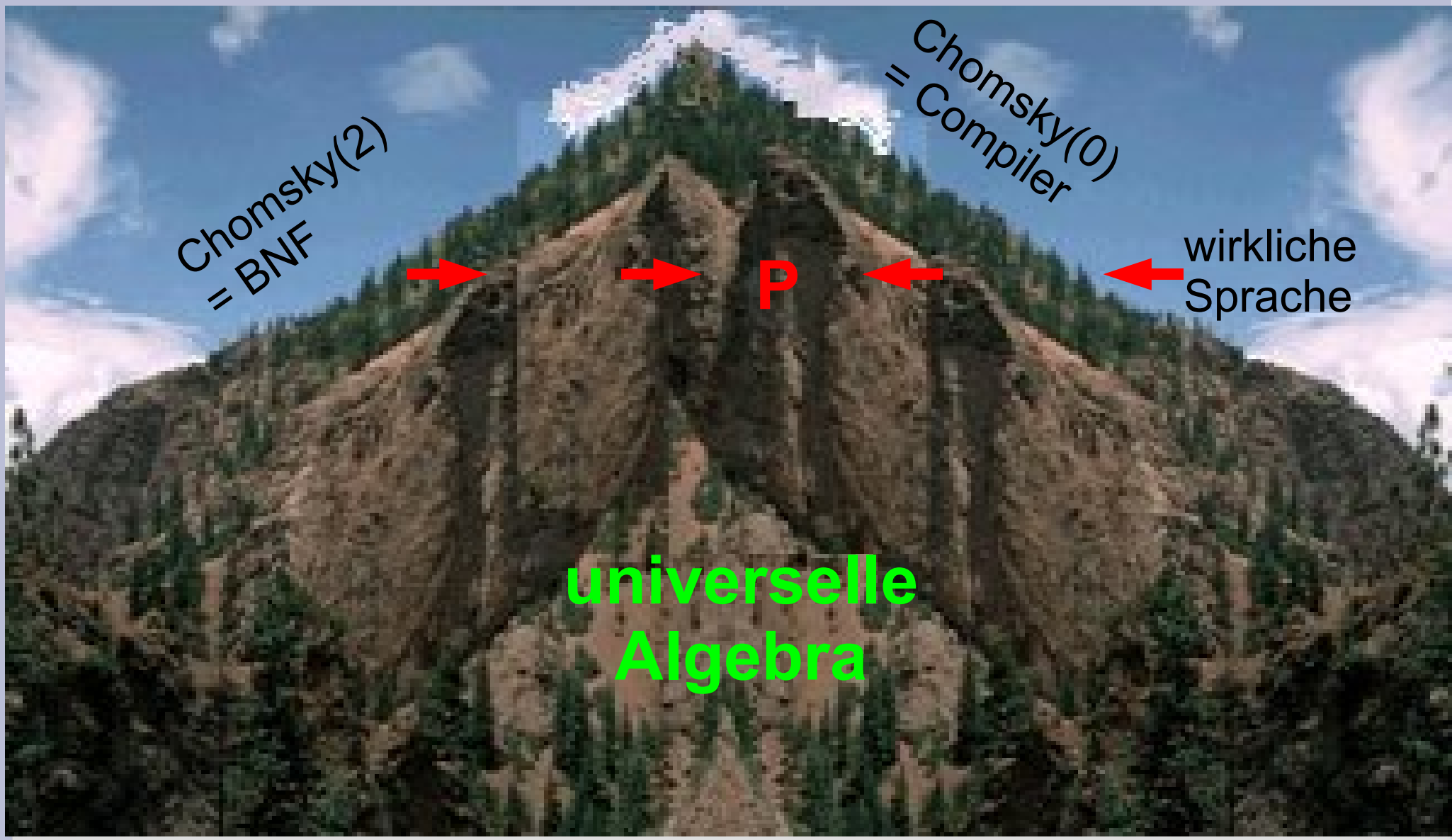
(MISRA-C, SPARK für ADA, normierte Progr., ...)

Sprachbeziehungen

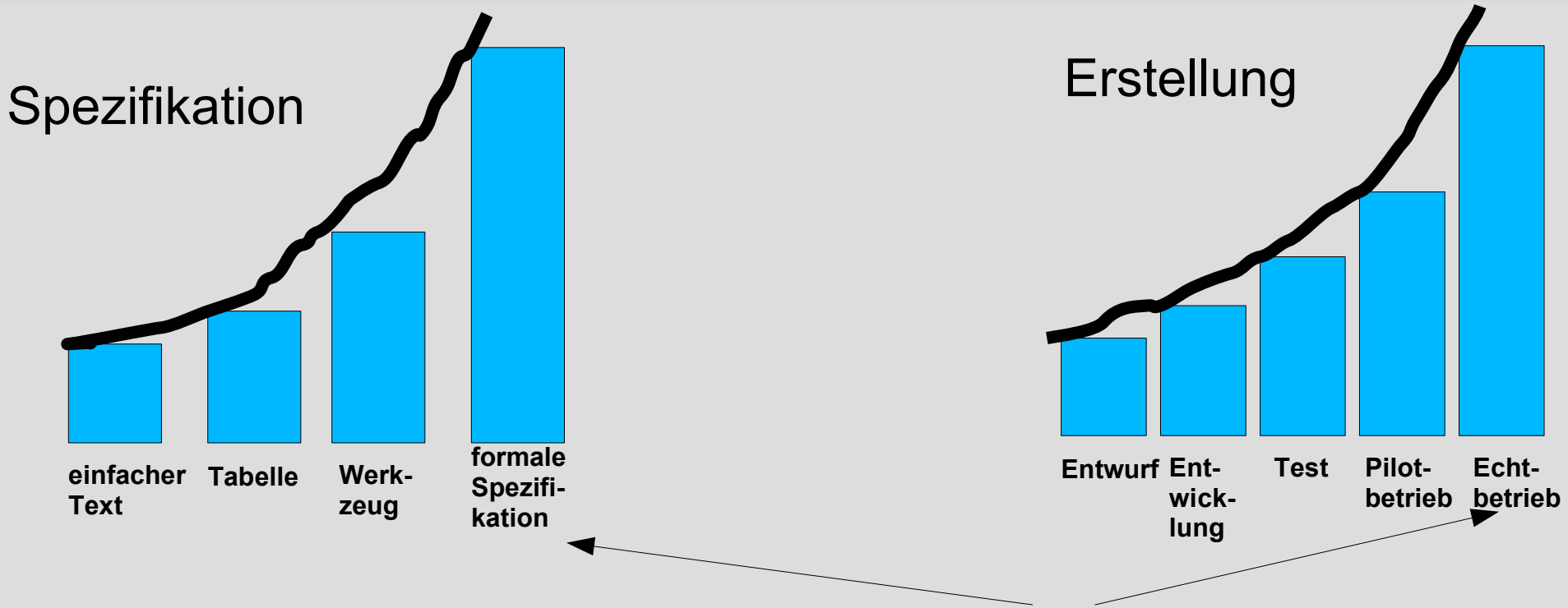


ein Beispiel,syntaktisch,semantisch und operational

ergänzende Sprachdefinition



Ökonomie



spart man am richtigen Ende?

A) jedes Auto muß zum TÜV,
B) ISO9000 betrifft nur die Prozesse

A ∧ B => Es fehlt ein **Software-TÜV**!

Klassifikation der Verfahren

- dynamische Verfahren
  (Valgrind, Debugger, ...)
- Style Checker
  (Lint, Misra ...)
- Ähnlichkeitsanalyse
  (Bauhaus, Simian,...)
- semidefinite Verfahren
  (PolySpace, Coverity, Klockwork, ...)
- definite Verfahren
  (Columbo)

Statische Analyse

erkennbar

- Undefinierte Variablen
- Arithmetik (X/0 etc.)
- Adress- und Indexfehler
- Wertebereich überschritten
- ungenutzter Code/Profiling
- Dateifehler (Open, Eof, ...)
- Terminierung (teilweise)
- unnütze Variablen
- SQL-/Code-/Data-Injection
- Input-Validation
- Clones
- Stilfehler, eigene Regeln
- ...

nicht erkennbar

- Datei nicht vorhanden
- Server nicht gestartet
- Bibliothek nicht vorhanden
- Versionskonflikt
- ...

Einsatzgebiete

ja

- in sicherheitskritischen Bereichen (KKW, ...)
- in kostspieligen Projekten (Auto-, Flugzeugindustrie)
- dort, wo Werkzeuge vorhanden sind (Großunternehmen)
- in Open Source Projekten (Ubuntu, ..)

nein

- in Kleinbetrieben
- im Klimarechenzentrum (warum nicht?)
- ...

einige Produkte

Werkzeug	Sprache	Kosten	Maße	Style-Check	Methode	Fehl-alarme	Lauf-zeit	Land
Polyspace www.polyspace.com/	C, C++	>20.000$	+		abstrakte Interpreta-tion		hoch	F
Lint www.gimpel.com	C, C++	~ 500$	+	+				US
Coverity www.coverity.com/	C, C++	~10.000$	+			20,00%		US
Klocwork www.klocwork.com/	C, C++	~10.000$	+					US
LDRA www.ldra.com/	COBOL, C++, uvm	?	+		CFA, DFA, MISRA			UK
PMD www.sourceforge.com/	JAVA		+					
Compiler www.borland.com	C++, JAVA	<2000$	-					US
viele andere ... www.testingfaqs.org/				+				

Klassifikation der Verfahren

	verifizierend	falsifizierend
Zustands - raum	∞	abstrakte Interpretation Hoare-Kalkül
Funktio - nenraum	Verisoft	Columbo®

Zusammenfassung

Statische Analyse ist

- ökonomisch
- ergänzende Sprachdefinition
- teilweise unerforscht
- eine Entlastung für Tester
- ein Schritt zu fehlerfreier Software

und nun ....

Vielen Dank
Für Ihre
Aufmerksamkeit