Verlässliche Echtzeitsysteme

Übungen zur Vorlesung

Abstrakte Interpretation & Verifikation

Florian Schmaus, Simon Schuster

Friedrich-Alexander-Universität Erlangen-Nürnberg
Lehrstuhl Informatik 4 (Verteilte Systeme und Betriebssysteme)
https://www4.cs.fau.de

25. Juni 2018

Erinnerung: Evaluation der Lehrveranstaltung

- TANs werden in der Übung verteilt
- $\geq 60\,\%$ Rückläuferquote $\rightsquigarrow$ Belohnung: **Semesterabschlussgrillen**
- Termin der Evaluation **30.06.2018**

Überblick

Überblick

Astrée [1]

- Ziel: Nachweis der Abwesenheit von Laufzeitfehlern
- Findet *alle* potentiellen Laufzeitfehler
- Leider auch *falsch-positive*
  ⇝ wegen **Gödelschem Unvollständigkeitstheorem** (1931)
  „Jedes hinreichend mächtige formale System ist entweder widersprüchlich oder unvollständig.“

Programm ist korrekt, wenn

- Astrée keine Alarme meldet
- Oder für alle Alarme nachgewiesen, dass falsch-positiv

Astrée weist nach

- Überschreitung von Array-Grenzen
- Ganzzahldivision durch Null
- Ungültige Dereferenzierung, arithmetische Überläufe
- Ungültige Gleitkommaoperationen
- Unerreichbarer Code
- Lesezugriff auf nicht initialisierte Variabeln
- Verletzung benutzerdefinierter Zusicherungen
  ⇝ `assert()`

Einschränkungen

- Rekursion prinzipiell erlaubt, wird aber nicht analysiert
  ⇝ für Rekursionsergebnis werden keine Einschränkungen ermittelt
- Auswertungsreihenfolge in C nicht vollständig spezifiziert
  ⇝ *eine* bestimmte Ordnung wird angenommen
  - stimmt nicht notwendigerweise mit Compiler überein
  - optionale Warnung durch Astrée
- Funktionen der Standard-C-Bibliothek werden nicht erkannt
  ⇝ mitgelieferte Stubs nutzen
- Dynamischer Speicher nicht erlaubt
  ⇝ kein `malloc()`
  - keine Einschränkung im sicherheitskritischen Echtzeitbereich

Semantik

Astrée nimmt an, dass folgende semantische Regeln gelten:

1. Der C99-Standard
2. Implementierungsabhängiges Verhalten
   - Größe von Datentypen
   - Gleitkommastandard
   - ...
3. Benutzerdefinierte Einschränkungen
   - z. B. ob statische Variablen mit 0 initialisiert werden
4. Außerdem *benutzerspezifizierte Zusicherungen*
   ⇝ und da wird es interessant ☺

Benutzerdefinierte Zusicherungen

`__ASTREE_known_fact((B))`

- Anlyzer nimmt an, dass B gegenben ist
- Analyzer warnt, falls B *nie wahr werden kann*
- `__ASTREE_known_range((V, [a; b]))` ⇝ Wertebereich

`assert((B))`/`__ASTREE_assert((B))`

- Analyzer erzeugt Alarm, falls B *nicht immer wahr ist*
- B kann nicht von der Form `e1 ? e2 : e3` sein
- `__ASTREE_global_assert(())` ⇝ gesamtes Programm

- B muss seiteneffektfrei sein
- *Doppelte Klammerung ist wichtig!*

Beispiel

```
1  #include <astree.h> // Astree-Makros ggf. abschalten
2
3  float filter(Alpha_State *s, float val) {
4    __ASTREE_known_fact((val == val)); // known_fact(!isnan(val))
5    __ASTREE_known_fact((-10.0f < val && val < 10.0f));
6    __ASTREE_known_fact((s->val == s->val));
7    __ASTREE_known_fact((FLT_MIN < s->val
8                         && s->val < FLT_MAX));
9    __ASTREE_assert((0.0f < s->alpha));
10   __ASTREE_assert((s->alpha < 1.0f));
11
12   float residual = val - s->val;
13   s->val = s->val + s->alpha * residual;
14
15   __ASTREE_assert((s->val == s->val));
16   // ...
17   return s->val;
18 }
19
```

Stubs

`__ASTREE_modify((V1, ..., Vn))`

- Zeigt an, dass Variablen `V1` bis `Vn` unbekannten Wert haben

⇝ Braucht man um Stubs zu bauen

- Beispiel: Emulation von Sensoren

Beispiel

```
1  #ifdef __ASTREE__
2  __ASTREE_modify((x; full_range));
3  __ASTREE_known_fact((x >= 0));
4  #else
5  // ... Implementierung
6  #endif
7
```

Schleifen ausrollen

- Astrée versucht Aufwand zu vermeiden
- Schleifen/Verzweigungen werden nicht ausgerollt
- Konsequenz:

Beispiel

```
1  unsigned int i = 0;
2  unsigned int j = 20;
3  while (j > 0) { --j; ++i; }
4
```

- Astrée kann nicht zeigen, daß die Schleife terminiert (☞ Satz von Rice, 1953)

⇝ Annahme für weitere Analyse: `i` läuft über

Lösung:

```
1  __ASTREE_unroll((30))
2  while (j > 0) { --j; ++i; }
3
```

Verzweigungen

- Dito bei Verzweigungen
- Astrée betrachtet normalerweise nur den schlimmsten Zweig
- ⇝ Pessimistisches Ergebnis
- Lösung: Analyse vorübergehend aufspalten:

Verzweigungsanalyse

```
__ASTREE_partition_control
if (...) { ... }
else { ... }
...
__ASTREE_partition_merge(());
```

- Auch für Schleifen, `switch` und Funktionsaufrufe
- ⇝ Blick ins Handbuch: es gibt noch weitere Tricks

Synchrone Programme

- Viele Echtzeitsysteme endlosschleifenbasiert ☹
- ⇝ Astrée modelliert dies

`__ASTREE_max_clock((N))`

beschränkt Schleifendurchläufe

`__ASTREE_wait_for_clock(())`

wartet auf nächsten Tick

```
__ASTREE_max_clock((10)); // sonst evt. keine Schleifeninvariante
void main(void) {
  while (1) {
    // 1. 'volatile'-Werte lesen
    // 2. Zustand und Ausgabe berechnen
    // 3. Ausgabe schreiben
    __ASTREE_wait_for_clock(()); // auf naechsten Clock-Tick warten
  }
}
```

Asynchrone Programme

- Astrée modelliert auch asynchrone Ausführung von Aufgaben
- Keine Annahmen über Scheduler oder Prioritäten
- `automatic-shared-variables` muss auf `yes` stehen

```
int x, y;
volatile int s;

void t1(void) {
  x = 1; s = 1; x = 0;
}

void t2(void) {
  if (s > 0) {
    y = -1;
  } else {
    y = 1;
  }
}

void main(void) {
  x = y; // synchroner Teil
  __ASTREE_asynchronous_loop((t1(), t2()));
}
```

volatile

`__ASTREE_volatile_input((V))`

- Zeigt an, dass `V` sich jederzeit ändern kann
- ⇝ Modelliert Eingabe von außen

`__ASTREE_volatile_input((Vp, r))`

- p ist Pfad in der Variablen,
  z. B. `V.a[3-4].b` ⇝ Variable `V`, Arrayelemente `a[3]` und `a[4]`, Struct-Element `b`
  - `[i]` ⇝ Element `i`
  - `[i-j]` ⇝ Elemente `i` bis `j`
  - `[]` ⇝ alle Elemente
- r schränkt Wertebereich ein `[i, j]` ⇝ von `i` bis `j`

Analyse untersuchen

`__ASTREE_analysis_log(())`

- Gibt Zustand der Analyse an dieser Stelle aus

`__ASTREE_log_vars((V1, ..., Vn))`

- Zeigt Zustand der Analyse in Bezug auf einzelne Variabeln an

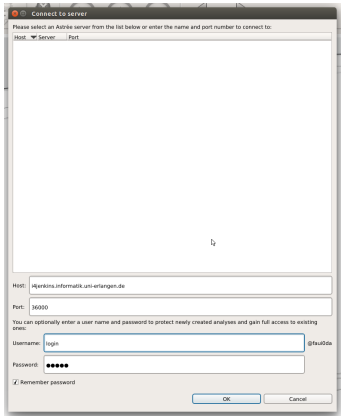
`__ASTREE_print(("text"))`

- Gibt Text aus

Astrée verwenden

- Astrée im CIP:
  `% /proj/i4ezs/tools/astree_c/bin/astreec`
- Anmeldung mit Benutzername und Passwort
  ⇝ Passwort wird bei der ersten Anmeldung festgelegt
- Dokumentation
  - HTML: `/proj/i4ezs/tools/astree_c/share/astree_c/share/html/index.html`
  - PDF: `/proj/i4ezs/tools/astree_c/help/astreec_QuickStart.pdf`

Anmelden

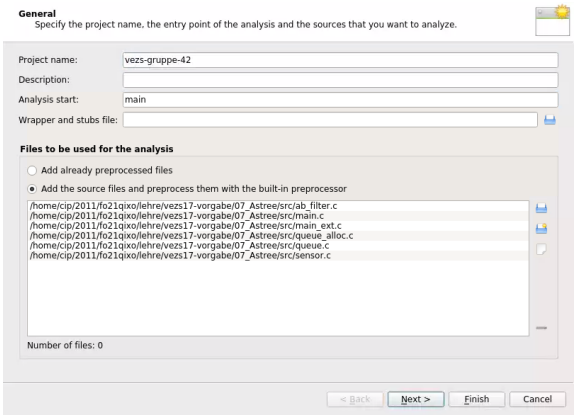


Host i4jenkins.cs.fau.de

Port 36000

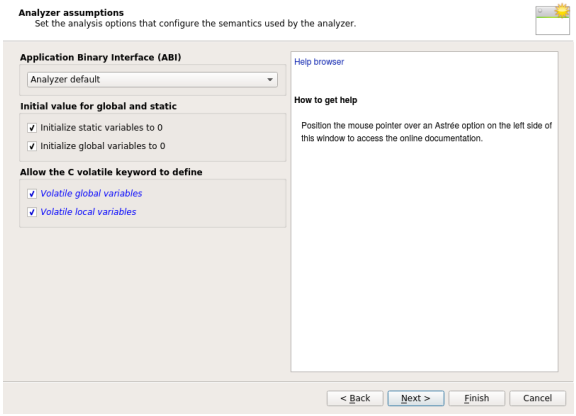
Kein Benutzername/Passwort notwendig.

Projekt anlegen



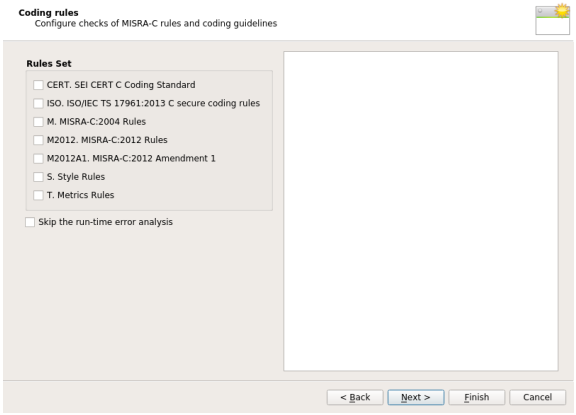
- Quelldateien zum Projekt hinzufügen

Analysen konfigurieren I

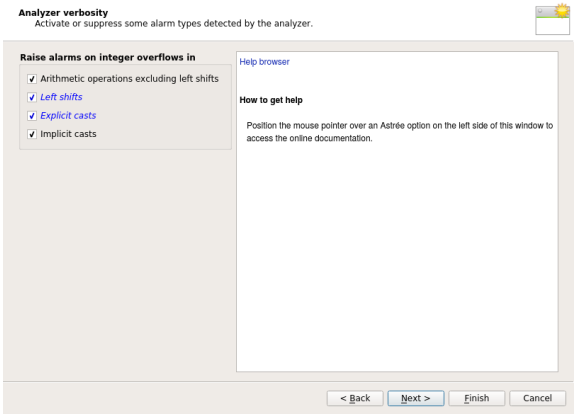


- *Volatile global variables*
- *Volatile local variables*

Analysen konfigurieren II

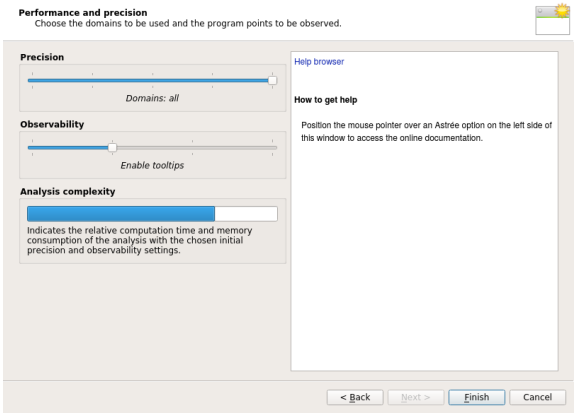


Analysen konfigurieren III

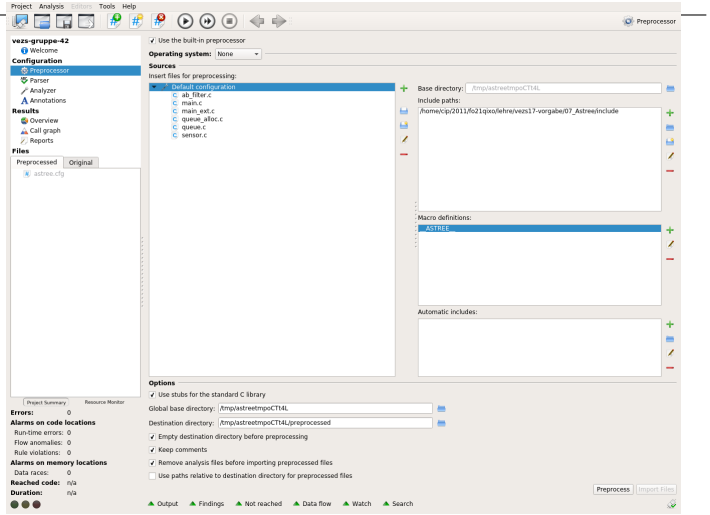


- *Left shift*
- *Explicit casts*

Analysen konfigurieren IV

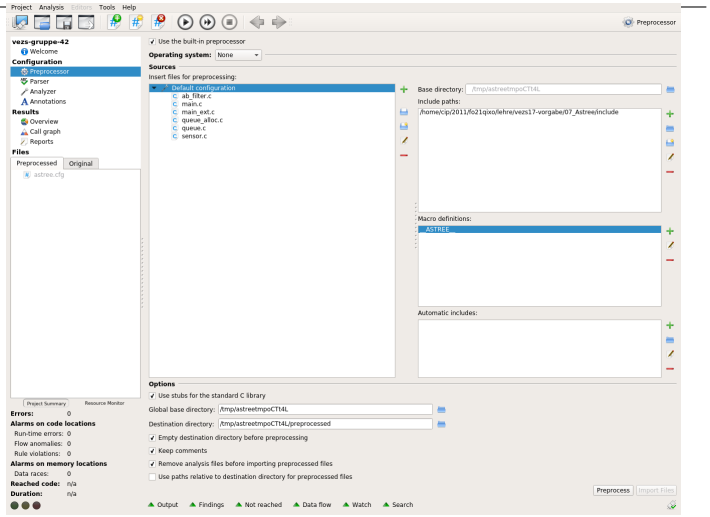


Libc Stubs



- Libc soll nicht mit analysiert werden:
  Use stubs for the standard C library
  ☞ Stubs für libc verwenden

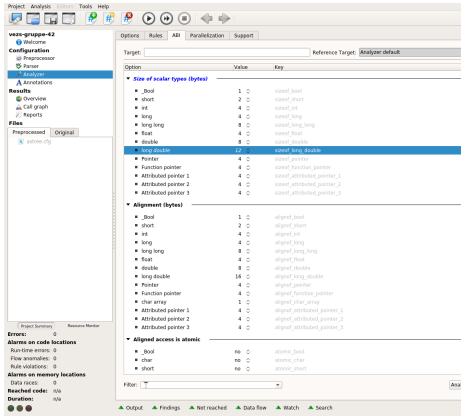
Präprozessoreinstellungen



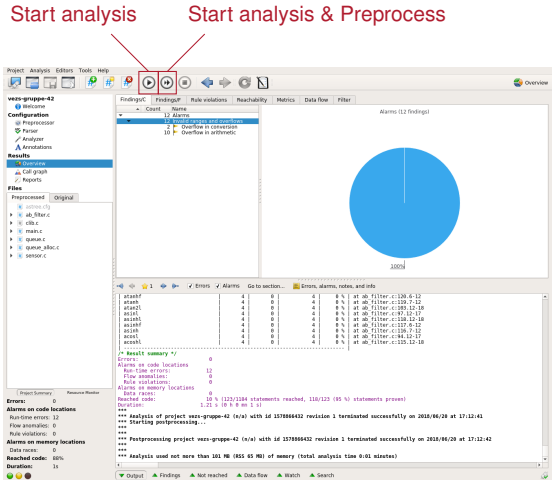
- Include-Pfade festlegen
- __ASTREE__ definieren

ABI

- ABI festlegen



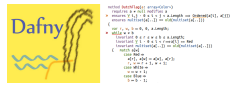
Analyse starten



Überblick

Programme zur Softwareverifikation

- Astrée
- SeaHorn
- Frama-C
- VeriFast
- Dafny
- Coq
- Isabelle/HOL
- Agda
- Idris
- ...



Beispiel: Maximumsfunktion

P : wahr

S :
```
int maximum(int a,int b) {
    int result = INT_MIN;

    if(a > b)
      result = a;
    else
      result = b;

    return INT_MAX;
  }
```

Q : result $\geq a \wedge$ result $\geq b \wedge$ (result $==$ a $\vee$ result $==$ b)

```
const INT_MIN := −2147483648;
const INT_MAX :=  2147483647;

method maximum(a: int, b: int)
       returns (max: int)
  ensures max ≥ a;
  ensures max ≥ b;
  ensures max = a ∨ max = b;
  requires INT_MIN ≤ a ≤ INT_MAX;
  requires INT_MIN ≤ b ≤ INT_MAX;
{
  var result := INT_MIN;
  if (a > b) {
    result := a;
  } else {
    result := b;
  }
  return INT_MAX;
}
```


Beispiel: Maximum in Liste finden

P : $a \neq$ NULL $\wedge$ length > 0

S :
```
int findMax(int *a, size_t length) {
    int max = a[0];
    for (size_t i = 0; i < length; i++) {
      if (a[i] > max) {
        max = a[i];
      }
    }

    return max;
  }
```

Q : $\forall k.k \geq 0 \wedge k <$ length $\Rightarrow$ a[k] $\leq$ result
$\exists k.k \geq 0 \wedge k <$ length $\Rightarrow$ a[k] $==$ result

```
method FindMax(a : array?<int>) returns (MaxValue: int)
  requires a ≠ null;
  requires a.Length > 0;
  ensures ∀ k • k ≥ 0 ∧ k < a.Length ⟹ a[k] ≤ MaxValue;
  ensures ∃ k • k ≥ 0 ∧ k < a.Length ⟹ old(a[k]) = MaxValue;
{
  var max  := a[0];
  var idx  := 0;

  var i := 1;

  while (i < a.Length)
    invariant ∀ k • k ≥ 0 ∧ k < i ∧ k < a.Length ⟹ a[k] ≤ max;
    invariant idx ≥ 0 ∧ idx < i ∧ idx < a.Length;
    invariant a[idx] = max;
    invariant ∃ k • k ≥ 0 ∧ k < i ∧ k < a.Length ⟹ a[k] = max;
  {
    if (max ≤ a[i])
    {
      max := a[i];
      idx := i;
    }
    i := i + 1;
  }

  return max;
}
```

Überblick

Aufgabenstellung

- Sensorstubs implementieren
- Implementierung eines Ringpuffers zur Verwaltung der Sensorwerte
- System erstellen:
  - Sensoren und Filter initialisieren
  - Sensorwerte abrufen
  - Sensorwerte filtern
- Abwesenheit von Laufzeitfehlern nachweisen
  ⇝ Astrée
- Numerische Stabilität des Filters nachweisen
  ⇝ Astrée

Ringpuffer – Implementierung

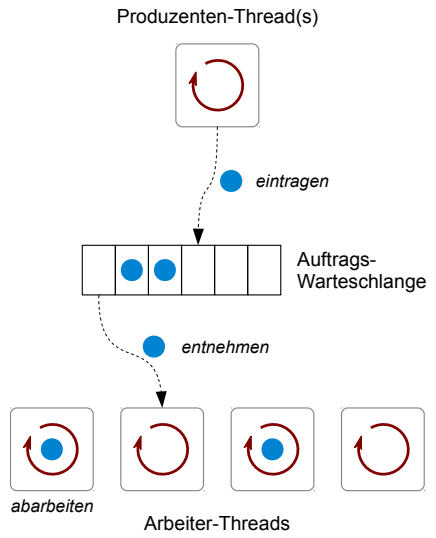
- Beispiel für dynamisch angelegten Ringpuffer

```
1 struct BndBuf{
2   int* buf; // array of <size>
3   int size;
4   int read_pos;
5   int write_pos;
6 };
```

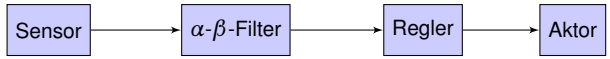
- „Füllstandsanzeige”: Speichern von
  - Belegten Plätzen
  - Verfügbaren Plätzen
- Mögliche Signalisierung falls
  - Plätze frei wurden
  - Plätze belegt wurde

Ringpuffer – Anwendungsszenario

- Verwaltung einer begrenzten Anzahl an Ressourcen
- Beispiel: Thread-Pool
- Feste Menge von Arbeiter-Threads:
  - laufen endlos
  - erhalten Aufträge zur Abarbeitung
- Verteilen der Aufträge mittels zentraler, synchronisierter Warteschlange (z. B. Ringpuffer)
- Vorteil: kein ständiges Erzeugen + Zerstören von Threads für Aufträge

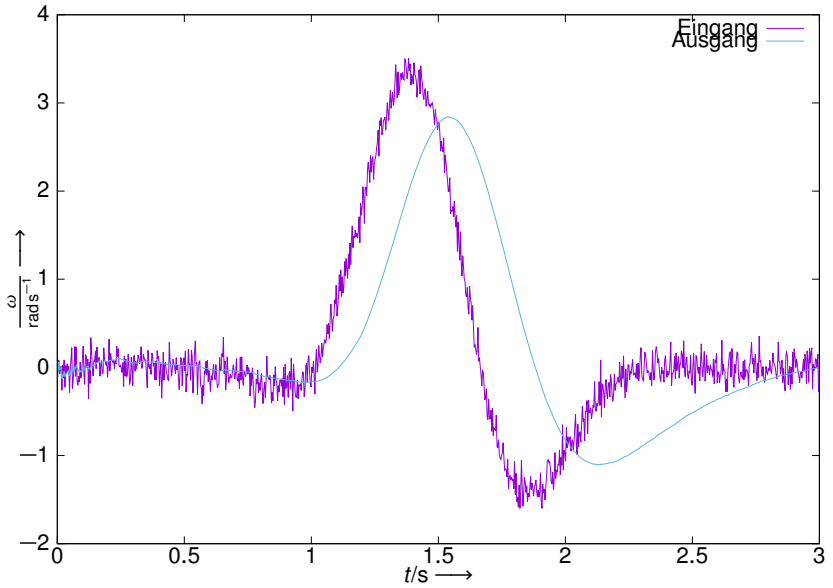


α-β-Filter [3]



- Rauschunterdrückungsfilter
- Geeignet zur Schätzung von physikalischen Größen
  - mit Ableitung $\neq 0$
  - z. B. Position eines Flugzeugs, Lagewinkel ...
  - im I4Copter
    - liefern Sensoren häufiger Werte als diese später verarbeitet werden
    - $\rightsquigarrow$ α-β-Filter für *Ratenwandlung* verwendet
    - $\rightsquigarrow$ nutzt gewonnene Information vollständig

Beispiel α-β-Filterung



Filteralgorithmus

- Wird für jeden Messwert ausgeführt
- $y[\kappa]$: Eingabewert für Abtastschritt κ
- $\hat{x}[\kappa]$: Schätzung der Messgröße zum Abtastschritt κ
- T Abtastintervall, α, β Filterparameter
- Initialisierung: z. B. $\hat{x}[0] = \hat{\dot{x}}[0] = 0$

$$r[\kappa] = y[\kappa] - \hat{x}[\kappa - 1] \qquad \rightsquigarrow \text{Schätzfehler} \qquad (1)$$

$$\hat{x}[\kappa] = \hat{x}[\kappa - 1] + \frac{\beta}{T} \cdot r[\kappa] \qquad \rightsquigarrow \text{1. Ableitung} \qquad (2)$$

$$\hat{x}[\kappa] = \hat{x}[\kappa - 1] + T \cdot \hat{\dot{x}}[\kappa] + \alpha \cdot r[\kappa] \qquad \rightsquigarrow \text{Schätzwert} \qquad (3)$$

- Sinnvolle Werte für α und β?
  - Literatur beschreibt viele Verfahren $\rightsquigarrow$ hier beispielhaft nur eines [5, 4]

Filterparameter

T Abtastintervall
$\rightsquigarrow$ in welchem Zeitabstand gemessen wird

σ_w^2 Prozessvarianz
$\rightsquigarrow$ wie lebhaft der gemessene Prozess ist

σ_v^2 Rauschvarianz
$\rightsquigarrow$ wie verrauscht das Signal ist

$$\lambda = \frac{\sigma_w T^2}{\sigma_v} \qquad \rightsquigarrow \text{Tracking Index} \qquad (4)$$

$$\theta = \frac{4 + \lambda - \sqrt{8\lambda + \lambda^2}}{4} \qquad \rightsquigarrow \text{Dämpfungsparameter} \qquad (5)$$

$$\alpha = 1 - \theta^2 \qquad \rightsquigarrow \text{Gewicht für Wert} \qquad (6)$$

$$\beta = 2(2 - \alpha) - 4\sqrt{1 - \alpha} \qquad \rightsquigarrow \text{Gewicht für Ableitung} \qquad (7)$$

Initialisierungsphase

- Zu Beginn hat das Filter keinen gültigen Zustand
- ⇝ Einschwingphase, in der das Filter „lernt“
- n startet bei 1 und wächst in jeder Runde um 1

$$\alpha_n = \frac{2(2n+1)}{(n+2)(n+1)} \tag{8}$$

$$\beta_n = \frac{6}{(n+2)(n+1)} \tag{9}$$

- Einschwingphase endet, wenn $\alpha_n < \alpha$
- Wird der Filterzustand im Betrieb ungültig, wird eine neue Einschwingphase eingeleitet

Korrektheitsbedingung

- Filter ist nur dann korrekt, wenn es auch *stabil* ist
- ⇝ für wertbegrenzte Eingabe erfolgt wertbegrenzte Ausgabe [6]
- ⇝ für Eingabe 0 geht der Filterausgang asymptotisch gegen 0
- α-β-Filter stabil, wenn gilt

$$0 < \alpha \leq 1 \tag{10}$$

$$0 < \beta \leq 2 \tag{11}$$

$$0 < 4 - 2\alpha - \beta \tag{12}$$

- Außerdem: laut [2] Rauschunterdrückung nur dann, wenn

$$0 < \beta < 1 \tag{13}$$

- Stabilität muss auch in der Initialisierungsphase gegeben sein!

Sinnvolle Wertebereiche

- Erfahrungen mit dem I4Copter haben gezeigt, dass sich die Parameter in folgenden Bereichen bewegen:

Abtastintervall $T \in (0 \ldots 1]$
Prozessvarianz $\sigma_w^2 \in [0.5 \ldots 30.0]$
Rauschvarianz $\sigma_v^2 \in \left[10^{-3} \ldots 10^{-1}\right]$
Wert $y[\kappa] \in [-10 \ldots 10]$

⇝ Korrektheit mindestens für diese Wertebereiche zeigen!

Literatur I

AbsInt Angewandte Informatik GmbH.
The Static Analyzer Astrée, April 2012.

C. Frank Asquith.
Weight selection in first-order linear filters.
Technical report, Army Intertial Guidance and Control Laboratory Center, Redstone Arsenal, Alabama, 1969.

Eli Brookner.
Tracking and Kalman Filtering Made Easy.
Wiley-Interscience, 1st edition, 4 1998.

E. Gray, J. and W. Murray.
A derivation of an analytic expression for the tracking index for the alpha-beta-gamma filter.
IEEE Trans. on Aerospace and Electronic Systems, 29:1064–1065, 1993.

Paul R. Kalata.
The tracking index: A generalized parameter for α-β and α-β-γ target trackers.
IEEE *Transactions on Aerospace and Electronic Systems*, AES-20(2):174–181, mar 1984.

Richard G. Lyons.
Understanding Digital Signal Processing.
Prentice Hall, 3rd edition, 11 2010.