

Title: Meixner: ZUE_DS (11.12.2013)
Date: Wed Dec 11 17:03:55 CET 2013
Duration: 84:33 min
Pages: 33

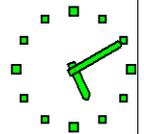
Zentralübung zur Vorlesung Diskrete Strukturen (Prof. Esparza)

Dr. Werner Meixner

Fakultät für Informatik
TU München

<http://www14.in.tum.de/lehre/2013WS/ds/uebung/>

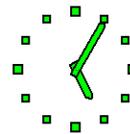
11. Dezember 2013



ZÜ IX

Übersicht:

1. **Übungsbetrieb:** Fragen, Probleme?
2. **Thema:** Wachstumshierarchie von Funktionen
Hierarchie und Sätze
Beispiele
3. **Vorbereitung** auf zirkuläres Rechnen
Zirkuläre Operationen
Rechnen modulo m
3-D Darstellung der mod-Operation
4. **Hin.Ti's** zu HA von Blatt 9



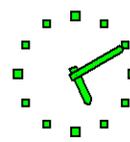
1. Fragen, Anregungen?

Aktuelle Fragen?





2. Thema: Wachstumshierarchie von Funktionen



2.1 Hierarchie und Sätze

Das asymptotische Wachstum von Funktionen $f, g : \mathbb{N} \rightarrow \mathbb{R}$ für $n \rightarrow \infty$ kann durch Einordnung in eine quasilineare Wachstumshierarchie von Funktionen untersucht werden.

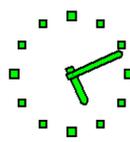
Es stehen die folgenden Relationen zur Verfügung:

- 1 $f \in o(|g|)$, oder $g \in \omega(|f|)$, oder $f \prec g$,
- 2 $f \in \mathcal{O}(|g|)$, oder $g \in \Omega(|f|)$,
- 3 $f \in \Theta(|g|)$, oder $f \asymp g$
- 4 $f \sim g$, d. h. $\lim_{n \rightarrow \infty} \left| \frac{f(n)}{g(n)} \right| = 1$.

Bemerkung: Beträge dienen hier dazu, die Forderung der Nichtnegativität von Funktionen zu erfüllen, auf die die Landau-Symbole angewandt werden können.



2. Thema: Wachstumshierarchie von Funktionen



2.1 Hierarchie und Sätze

Das asymptotische Wachstum von Funktionen $f, g : \mathbb{N} \rightarrow \mathbb{R}$ für $n \rightarrow \infty$ kann durch Einordnung in eine quasilineare Wachstumshierarchie von Funktionen untersucht werden.

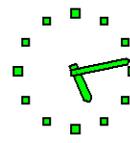
Es stehen die folgenden Relationen zur Verfügung:

- 1 $f \in o(|g|)$, oder $g \in \omega(|f|)$, oder $f \prec g$,
- 2 $f \in \mathcal{O}(|g|)$, oder $g \in \Omega(|f|)$,
- 3 $f \in \Theta(|g|)$, oder $f \asymp g$
- 4 $f \sim g$, d. h. $\lim_{n \rightarrow \infty} \left| \frac{f(n)}{g(n)} \right| = 1$.

Bemerkung: Beträge dienen hier dazu, die Forderung der Nichtnegativität von Funktionen zu erfüllen, auf die die Landau-Symbole angewandt werden können.



2. Thema: Wachstumshierarchie von Funktionen



2.1 Hierarchie und Sätze

Das asymptotische Wachstum von Funktionen $f, g : \mathbb{N} \rightarrow \mathbb{R}$ für $n \rightarrow \infty$ kann durch Einordnung in eine quasilineare Wachstumshierarchie von Funktionen untersucht werden.

Es stehen die folgenden Relationen zur Verfügung:

- 1 $f \in o(|g|)$, oder $g \in \omega(|f|)$, oder $f \prec g$,
- 2 $f \in \mathcal{O}(|g|)$, oder $g \in \Omega(|f|)$,
- 3 $f \in \Theta(|g|)$, oder $f \asymp g$
- 4 $f \sim g$, d. h. $\lim_{n \rightarrow \infty} \left| \frac{f(n)}{g(n)} \right| = 1$.

Bemerkung: Beträge dienen hier dazu, die Forderung der Nichtnegativität von Funktionen zu erfüllen, auf die die Landau-Symbole angewandt werden können.



Nützlich ist die folgende Auswahl aus dieser Hierarchie.

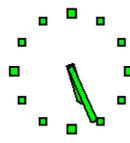
Für alle $k \in \mathbb{N}$, $\epsilon, c \in \mathbb{R}^+$ mit $0 < \epsilon < 1 < c$ gilt

$$0 \prec 1 \prec \log \log n \prec \log n \prec \log^k n \prec e^{\sqrt{\log n}} \prec n^\epsilon \prec n \prec n \log n \prec n^c \prec (\log n)^{\log n} \prec n^{\log n} \prec c^n \prec n! \prec n^n \prec e^{c^n} \prec \dots$$

Man beachte die Beziehungen für asymptotische Gleichheit:

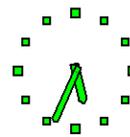
$$n! \sim \sqrt{2\pi n} \left(\frac{n}{e}\right)^n, \quad (\text{Stirling})$$

$$\ln n! \sim n \ln n.$$





Nützlich ist die folgende Auswahl aus dieser Hierarchie.
Für alle $k \in \mathbb{N}$, $\epsilon, c \in \mathbb{R}^+$ mit $0 < \epsilon < 1 < c$ gilt



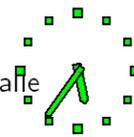
$$\begin{aligned} 0 &\prec 1 \prec \log \log n \prec \log n \prec \log^k n \prec e^{\sqrt{\log n}} \prec n^\epsilon \prec \\ &\prec n \prec n \log n \prec n^c \prec (\log n)^{\log n} \prec n^{\log n} \prec \\ &\prec c^n \prec n! \prec n^n \prec c^{c^n} \prec \dots \end{aligned}$$

Man beachte die Beziehungen für asymptotische Gleichheit:

$$\begin{aligned} n! &\sim \sqrt{2\pi n} \left(\frac{n}{e}\right)^n, & (\text{Stirling}) \\ \ln n! &\sim n \ln n. \end{aligned}$$



Die folgenden Sätze über die o.g. Relationen sind leicht zu beweisen, und sie sind nützlich, weil Sie es gestatten, nahezu alle Aufgaben über den Vergleich von Wachstum algebraisch zu beweisen.



Satz 1:

- ① $\alpha \in \mathbb{R}^+ \implies \alpha \cdot f \asymp f.$
- ② $0 \prec f \wedge 1 \prec g \implies f \prec f \cdot g.$ (folgt aus (3))
- ③ $0 \prec h \wedge f \prec g \implies f \cdot h \prec g \cdot h.$
- ④ $h \prec f \implies f + h \sim f.$
- ⑤ $1 \prec f \prec g \implies e^{|f(n)|} \prec e^{|g(n)|}$ für alle $n.$

Für die angegebenen Funktionen der o.g. Auswahl gilt:

- ⑥ $1 \prec f \prec g \implies 0 \prec \frac{1}{g} \prec \frac{1}{f} \prec 1.$

Es gelten einige weitere einfache Eigenschaften.



Die folgenden Sätze über die o.g. Relationen sind leicht zu beweisen, und sie sind nützlich, weil Sie es gestatten, nahezu alle Aufgaben über den Vergleich von Wachstum algebraisch zu beweisen.



Satz 1:

- ① $\alpha \in \mathbb{R}^+ \implies \alpha \cdot f \asymp f.$
- ② $0 \prec f \wedge 1 \prec g \implies f \prec f \cdot g.$ (folgt aus (3))
- ③ $0 \prec h \wedge f \prec g \implies f \cdot h \prec g \cdot h.$
- ④ $h \prec f \implies f + h \sim f.$
- ⑤ $1 \prec f \prec g \implies e^{|f(n)|} \prec e^{|g(n)|}$ für alle $n.$

Für die angegebenen Funktionen der o.g. Auswahl gilt:

- ⑥ $1 \prec f \prec g \implies 0 \prec \frac{1}{g} \prec \frac{1}{f} \prec 1.$

Es gelten einige weitere einfache Eigenschaften.



Die algebraische Behandlung von Wachstumshierarchien stammt von Godfrey Harold Hardy (G.H. Hardy).



Er führte die Klasse der sogenannten logarithmisch-exponentiellen Funktionen ein.

Alle in der Praxis auftretenden Wachstumsfunktionen sind logarithmisch-exponentiell.

Es ist deshalb eine gute Idee, sich eine geeignete Wachstumshierarchie bereitzuhalten.

2.2 Beispiele

Beispiel 1:

$$n^2 + n \log n \sim n^2:$$

Da $n \log n \prec n^2$, folgt die Behauptung mit Satz 1.4.

Beispiel 2:

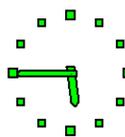
$$n^3 + n \log n \sim n^3:$$

$n^2 \log n \prec n^3$ folgt aus Satz 1.3, der Rest folgt wieder mit Satz 1.4.

Beispiel 3:

$$n^3 \sim n^3 \log n:$$

Es gilt $1 \prec \log n$. Dann folgt die Behauptung mit Satz 1.2.



13zue09.pdf - Adobe Acrobat Professional

File Edit View Document Comments Forms Tools Advanced Window Help

25 / 107 152% Find

2.2 Beispiele

Beispiel 1:

$$n^2 + n \log n \sim n^2:$$

Da $n \log n \prec n^2$, folgt die Behauptung mit Satz 1.4.

Beispiel 2:

$$n^3 + n \log n \sim n^3:$$

$n^2 \log n \prec n^3$ folgt aus Satz 1.3, der Rest folgt wieder mit Satz 1.4.

Beispiel 3:

$$n^3 \sim n^3 \log n:$$

Es gilt $1 \prec \log n$. Dann folgt die Behauptung mit Satz 1.2.

TUM ZÜ DS ©Dr. Werner Meixner 7/30 LEA

13zue09.pdf - Adobe Acrobat Professional

File Edit View Document Comments Forms Tools Advanced Window Help

29 / 107 152% Find

2.2 Beispiele

Beispiel 1:

$$n^2 + n \log n \sim n^2:$$

Da $n \log n \prec n^2$, folgt die Behauptung mit Satz 1.4.

Beispiel 2:

$$n^3 + n \log n \sim n^3:$$

$\therefore n^2 \log n \prec n^3$ folgt aus Satz 1.3, der Rest folgt wieder mit Satz 1.4.

Beispiel 3:

$$n^3 \sim n^3 \log n:$$

Es gilt $1 \prec \log n$. Dann folgt die Behauptung mit Satz 1.2.

TUM ZÜ DS ©Dr. Werner Meixner 2.2 Beispiele 7/30 LEA

13zue09.pdf - Adobe Acrobat Professional

File Edit View Document Comments Forms Tools Advanced Window Help

29 / 107 152% Find

Wie wirken sich unterschiedliche Basen von Logarithmen aus?

Beispiel 4:

$$\log_a \log_b n^k \prec \log_a n:$$
$$\begin{aligned} \log_a \log_b n^k &= \log_a k + \log_a \log_b n \\ &\sim \log_a \log_b n \\ &= \log_a \left(\frac{\log_a n}{\log_a b} \right) \\ &= \log_a \log_a n - \log_a \log_a b \\ &\sim \log_a \log_a n \\ &\prec \log_a n \\ &\prec \log_a n. \end{aligned}$$

$\therefore \log_a \log_b n^k \prec \log_a n$.

TUM ZÜ DS ©Dr. Werner Meixner 8/30 LEA

13zue09.pdf - Adobe Acrobat Professional

File Edit View Document Comments Forms Tools Advanced Window Help

34 / 107 152%

Find

Beispiel 5:

$$n^{\log n} \prec 2^{n \log n}$$

Wir logarithmieren beide Seiten (nicht die Relation!) mit \ln .
Dann gilt für beide Seiten wegen Satz 1.3

$$(\log n) \cdot (\ln n) \prec (n \log n) \cdot \ln 2.$$

Mit Satz 1.5 folgt die Behauptung.

+

TUM ZÜ DS ©Dr. Werner Meixner 9/30 LEA

13zue09.pdf - Adobe Acrobat Professional

File Edit View Document Comments Forms Tools Advanced Window Help

39 / 107 152%

Find

Wir beweisen eine Beziehung der Auswahl aus der Hierarchie.

Beispiel 6:

$$\log^k n \prec e^{\sqrt{\log n}} \prec n^\epsilon$$

Durch Substitution von $\log^k n$ für n in $1 \prec \ln n \prec n^{\frac{1}{2k}}$ folgt

$$1 \prec \ln \log^k n \prec \sqrt{\log n}.$$

Außerdem folgt aus $\sqrt{n} \prec \frac{e}{\log e} n$ durch Substitution von $\log n$ für n die Beziehung $\sqrt{\log n} \prec \epsilon \ln n$.

Mit Satz 1.5 folgt die Behauptung.

+

TUM ZÜ DS ©Dr. Werner Meixner 10/30 LEA

13zue09.pdf - Adobe Acrobat Professional

File Edit View Document Comments Forms Tools Advanced Window Help

45 / 107 152%

Find

Beispiel 7:

Das letzte Beispiel zeigt die alternative Problemlösung mit Rückgriff auf die Definitionen.

- Man zeige: $(\log n^2)^2 \in o(2^{\ln n})$.

\log ohne Angabe der Basis bedeutet, dass die Formel für alle zulässigen Basen zu beweisen ist.

+

TUM ZÜ DS ©Dr. Werner Meixner 11/30 LEA

13zue09.pdf - Adobe Acrobat Professional

File Edit View Document Comments Forms Tools Advanced Window Help

49 / 107 152%

Find

Lösung:

Es ist zu zeigen:

$$\forall \epsilon > 0 \exists n_0 \in \mathbb{N} \forall n \geq n_0 [(\log n^2)^2 < \epsilon \cdot 2^{\ln n}].$$

Sei b eine beliebige zulässige Basis.

Wir lösen die Formel schrittweise auf.

+

TUM ZÜ DS ©Dr. Werner Meixner 12/30 LEA

13zue09.pdf - Adobe Acrobat Professional

File Edit View Document Comments Forms Tools Advanced Window Help

52 / 107 152%

Sei c eine beliebige reelle Zahl mit $c > 0$.
 Nun konstruieren wir ein natürliche Zahl n_c , so dass gilt

$$\forall n \geq n_c [(\log n^2)^2 < c \cdot 2^{\ln n}].$$

Umformung:

$$(\log_b n^2)^2 = \frac{4}{(\ln b)^2} \cdot (\ln n)^2 < c \cdot 2^{\ln n}.$$

Wir bezeichnen $\ln n$ mit x ,
 d.h. wir setzen $x = \ln n$,
 und wir setzen $k = \frac{4}{(\ln b)^2}$.

TUM ZÜ DS ©Dr. Werner Meixner 13/30 LEA

13zue09.pdf - Adobe Acrobat Professional

File Edit View Document Comments Forms Tools Advanced Window Help

51 / 107 152%

Lösung:

Es ist zu zeigen:

$$\forall c > 0 \exists n_c \in \mathbb{N} \forall n \geq n_c [(\log n^2)^2 < c \cdot 2^{\ln n}].$$

Sei b eine beliebige zulässige Basis.
 Wir lösen die Formel schrittweise auf.

⋄

TUM ZÜ DS ©Dr. Werner Meixner 2.2 Beispiele 12/30 LEA

13zue09.pdf - Adobe Acrobat Professional

File Edit View Document Comments Forms Tools Advanced Window Help

52 / 107 152%

Sei c eine beliebige reelle Zahl mit $c > 0$.
 Nun konstruieren wir ein natürliche Zahl n_c , so dass gilt

$$\forall n \geq n_c [(\log n^2)^2 < c \cdot 2^{\ln n}].$$

Umformung:

$$(\log_b n^2)^2 = \frac{4}{(\ln b)^2} \cdot (\ln n)^2 < c \cdot 2^{\ln n}.$$

Wir bezeichnen $\ln n$ mit x ,
 d.h. wir setzen $x = \ln n$,
 und wir setzen $k = \frac{4}{(\ln b)^2}$.

TUM ZÜ DS ©Dr. Werner Meixner 13/30 LEA

13zue09.pdf - Adobe Acrobat Professional

File Edit View Document Comments Forms Tools Advanced Window Help

51 / 107 152%

Sei c eine beliebige reelle Zahl mit $c > 0$.
 Nun konstruieren wir ein natürliche Zahl n_c , so dass gilt

$$\forall n \geq n_c [(\log n^2)^2 < c \cdot 2^{\ln n}].$$

Umformung:

$$(\log_b n^2)^2 = \frac{4}{(\ln b)^2} \cdot (\ln n)^2 < c \cdot 2^{\ln n}.$$

Wir bezeichnen $\ln n$ mit x ,
 d.h. wir setzen $x = \ln n$,
 und wir setzen $k = \frac{4}{(\ln b)^2}$.

TUM ZÜ DS ©Dr. Werner Meixner 13/30 LEA

13zue09.pdf - Adobe Acrobat Professional

File Edit View Document Comments Forms Tools Advanced Window Help

54 / 107 152%

Nun benutzen wir die Ungleichung $x^3 < 2^x$ für $x \geq 10$.
 Die Ungleichung folgt leicht aus $3 \ln x < x \ln 2$ für $x \geq 10$.
 Dann gilt für $x \geq 10$ und $\frac{k}{x} \leq c$

$$k \cdot x^2 = \frac{k}{x} \cdot x^3 < c \cdot 2^x.$$

Nun setzen wir $x_c = \max\{10, \frac{k}{c}\}$ und $n_c = \lceil e^{x_c} \rceil$
 und erhalten für alle $n \geq n_c$ die gewünschte Ungleichung.

+

TUM ZÜ DS ©Dr. Werner Meixner 14/30 LEA

13zue09.pdf - Adobe Acrobat Professional

File Edit View Document Comments Forms Tools Advanced Window Help

58 / 107 152%

3. Vorbereitung auf zirkuläres Rechnen

3.1 Zirkuläre Operationen

Beispiel:
 Operation (+1) auf $\{0, 1, 2, 3\}$:

$$\begin{aligned} 0 + 1 &= 1, \\ 1 + 1 &= 2, \\ 2 + 1 &= 3, \\ 3 + 1 &= 0, \\ 0 + 1 &= 1, \\ 1 + 1 &= 2, \\ 2 + 1 &= 3, \\ 3 + 1 &= 0, \\ \dots &\dots \text{USW.} \end{aligned}$$

+

TUM ZÜ DS ©Dr. Werner Meixner 15/30 LEA

13zue09.pdf - Adobe Acrobat Professional

File Edit View Document Comments Forms Tools Advanced Window Help

64 / 107 152%

Bemerkung:
 Wesentliche Teile der Algebra werden von zirkulären Operationen beherrscht, beispielsweise in Form der Potenzierung a^m , falls $a^m = 1$ gilt.

$$1, a, a^2, a^3, a^4, \dots, a^{m-1}, a^m = 1, a, a^2, \dots$$

Zirkuläres Rechnen ist eine Rechnungsart, die über die Schulmathematik hinausgeht.

+

TUM ZÜ DS ©Dr. Werner Meixner 16/30 LEA

13zue09.pdf - Adobe Acrobat Professional

File Edit View Document Comments Forms Tools Advanced Window Help

68 / 107 152%

Rechnen modulo m

Ganze Zahlen $a, b \in \mathbb{Z}$ nennt man kongruent modulo m , mit $m \in \mathbb{N}$, i. Z.

$$a \equiv b \pmod{m},$$

falls sich a und b um ein ganzzahliges Vielfaches von m unterscheiden, d. h.,
 falls es ein $k \in \mathbb{Z}$ gibt, so dass gilt

$$a = b + k \cdot m.$$

Man schreibt auch $a \equiv_m b$ für $a \equiv b \pmod{m}$.
 \equiv_m ist eine Äquivalenzrelation über \mathbb{Z} ,
 ja sogar eine „Kongruenzrelation“.

+

TUM ZÜ DS ©Dr. Werner Meixner 17/30 LEA

13zue09.pdf - Adobe Acrobat Professional

File Edit View Document Comments Forms Tools Advanced Window Help

73 / 107 152%

Davon abgeleitet ist die Definition der Operation $\text{mod} : \mathbb{Z} \times \mathbb{N} \rightarrow \mathbb{Z}$:

$$b = a \text{ mod } m \iff a \equiv b \pmod{m} \text{ und } 0 \leq b < m.$$

Für jedes m ist $\text{mod } m$ eine unäre Operation über \mathbb{Z} .
 $a \text{ mod } m$ heißt Rest der natürlichen Division von a durch m .

Achtung: Wir werden in der nächsten Zentralübung ein Quiz für zirkuläres Rechnen veranstalten. Lernen Sie also die folgende Abschnitte.

TUM ZÜ DS 18/30 ©Dr. Werner Meixner LEA

13zue09.pdf - Adobe Acrobat Professional

File Edit View Document Comments Forms Tools Advanced Window Help

80 / 107 152%

3.2 Rechnen modulo m

Teil 1:

Zeigen Sie für alle $a, b \in \mathbb{Z}$ und $m \in \mathbb{N}$:

$$a \equiv a \text{ mod } m \pmod{m}, \quad (1)$$

$$(a + b) \text{ mod } m = [(a \text{ mod } m) + (b \text{ mod } m)] \text{ mod } m, \quad (2)$$

$$(a \cdot b) \text{ mod } m = [(a \text{ mod } m) \cdot (b \text{ mod } m)] \text{ mod } m. \quad (3)$$

⋮

TUM ZÜ DS 19/30 ©Dr. Werner Meixner 3.2 Rechnen modulo m LEA

13zue09.pdf - Adobe Acrobat Professional

File Edit View Document Comments Forms Tools Advanced Window Help

81 / 107 152%

1 Zu beweisen ist: $a \equiv a \text{ mod } m \pmod{m}$

Lösung:

Die Kongruenz modulo m ist definiert durch

$$x \equiv y \pmod{m} \iff (\exists k \in \mathbb{Z}) [x = y + k \cdot m].$$

Nach Definition von $(a \text{ mod } m)$ gilt für ein bestimmtes $k \in \mathbb{Z}$

$$a \text{ mod } m = a + k \cdot m, \quad \text{d. h.} \quad a = a \text{ mod } m + k \cdot m,$$

mithin:

$$a \equiv a \text{ mod } m \pmod{m}.$$

TUM ZÜ DS 20/30 ©Dr. Werner Meixner LEA

13zue09.pdf - Adobe Acrobat Professional

File Edit View Document Comments Forms Tools Advanced Window Help

92 / 107 152%

Teil 2:

In enger Beziehung zur mod -Operation steht die **ganzzahlige Division** $a \text{ div } m$ zweier Zahlen $a \in \mathbb{Z}, m \in \mathbb{N}$.
 Es gilt

$$a = (a \text{ div } m) \cdot m + (a \text{ mod } m).$$

Berechnen Sie:

(i) $5 \text{ div } 4$, (ii) $(-5) \text{ div } 4$, (iii) $(-x) \text{ div } 1$.

⋮

TUM ZÜ DS 24/30 ©Dr. Werner Meixner 3.2 Rechnen modulo m LEA

13zue09.pdf - Adobe Acrobat Professional

File Edit View Document Comments Forms Tools Advanced Window Help

97 / 107 152% Find

(ii) $(-5) \operatorname{div} 4$:

Seien $a = -5$ und $m = 4$.

Dann gilt

$$\begin{aligned} ((-5) \operatorname{div} 4) \cdot 4 &= -5 - ((-5) \bmod 4) \\ &= -5 - ((-5 + 8) \bmod 4) \\ &= -5 - 3 = -8. \end{aligned}$$

Es folgt $(-5) \operatorname{div} 4 = -2$.

+

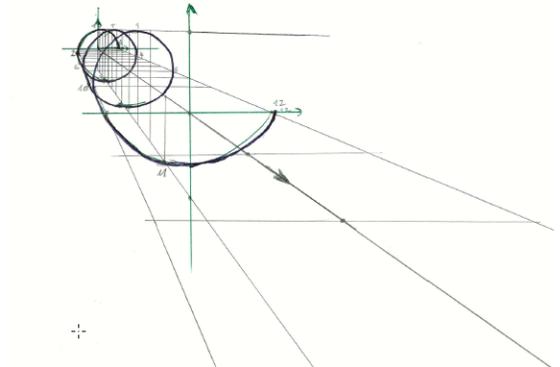
TUM ZÜ DS ©Dr. Werner Meixner 26/30 LEA

13zue09.pdf - Adobe Acrobat Professional

File Edit View Document Comments Forms Tools Advanced Window Help

106 / 107 152% Find

Darstellung:



+

TUM ZÜ DS 3.3 3-D Darstellung der mod-Operation ©Dr. Werner Meixner 29/30 LEA