# 10 Verschlüsselung von Formeln durch natürliche Zahlen

Sei $\sigma(L) = (S, +, \cdot, 0, <)$. Wir ordnen nach folgendem Schema den benutzten Symbolen Zahlen, d.h. ihre Symbolnummer zu.

$$\begin{aligned}
&\mathrm{SN}(v_i) = 2i\\
&\mathrm{SN}(S) = 3\\
&\mathrm{SN}(+) = 5\\
&\mathrm{SN}(\cdot) = 7\\
&\mathrm{SN}(0) = 9\\
&\mathrm{SN}(<) = 11\\
&\mathrm{SN}(=) = 13\\
&\mathrm{SN}(\neg) = 15\\
&\mathrm{SN}(\rightarrow) = 17\\
&\mathrm{SN}(\forall) = 19
\end{aligned}$$

Wir nutzen für die folgenden sehr formalen Dinge die klammernfreie Schreibweise der Formeln und Terme. Auf die Eindeutigkeit dieser Darstellung wurde hingewiesen. Wir schreiben z.B. $+t_1t_2$ statt $t_1 + t_2$, $\rightarrow \varphi_1\varphi_2$ statt $(\varphi_1 \rightarrow \varphi_2)$.

Jedem Term $t$ und jeder Formel $\varphi$ kann nun eindeutig eine Zahl $\ulcorner t \urcorner$ bzw. $\ulcorner \varphi \urcorner$ zugeordnet werden, die den induktiven Formelaufbau verschlüsselt. Für jede Zahl kann man effektiv feststellen, ob sie einen Term oder eine Formel verschlüsselt. Dieser Term bzw. diese Formel kann dann auch effektiv gewonnen werden.

**Definition** der Gödelzahl $\ulcorner t \urcorner$ für den Term $t$:

$$\begin{aligned} \ulcorner 0 \urcorner &= \langle \mathrm{SN}(0) \rangle \\ \ulcorner v_i \urcorner &= \langle \mathrm{SN}(v_i) \rangle \end{aligned}$$

Als Folgennummern der Länge 1 von allen anderen $\ulcorner$Termen$\urcorner$ und den $\ulcorner$Formeln$\urcorner$ unterscheidbar.

Wenn $f$ $n$-stelliges Funktionssymbol und $t_1, \ldots, t_n$ Terme

$$\ulcorner f t_1 \ldots t_n \urcorner = \langle \mathrm{SN}(f), \ulcorner t_1 \urcorner, \ldots, \ulcorner t_n \urcorner \rangle.$$

Wir haben nur die Fälle $n = 1, 2$ für die gewählte Signatur.

**Definition** der Gödelzahl $\ulcorner \varphi \urcorner$ für die Formeln $\varphi$:

$$\begin{aligned} \ulcorner = t_1 t_2 \urcorner &= \langle \mathrm{SN}(=), \ulcorner t_1 \urcorner, \ulcorner t_2 \urcorner \rangle, \\ \ulcorner < t_1 t_2 \urcorner &= \langle \mathrm{SN}(<), \ulcorner t_1 \urcorner, \ulcorner t_2 \urcorner \rangle, \\ \ulcorner \neg \varphi \urcorner &= \langle \mathrm{SN}(\neg), \ulcorner \varphi \urcorner \rangle \\ \ulcorner \to \varphi \psi \urcorner &= \langle \mathrm{SN}(\to), \ulcorner \varphi \urcorner, \ulcorner \psi \urcorner \rangle \\ \ulcorner \forall\, v_i \varphi \urcorner &= \langle \mathrm{SN}(\forall), \ulcorner v_i \urcorner, \ulcorner \varphi \urcorner \rangle. \end{aligned}$$

**Definition** $\mathrm{Thm}_\Sigma = \{ \ulcorner \varphi \urcorner : \Sigma \vdash \varphi, \varphi \text{ Formel} \}$.

$\Sigma$ ist entscheidbar, wenn $\mathrm{Thm}_\Sigma$ rekursiv ist. Sonst heißt $\Sigma$ unentscheidbar.

$\Sigma$ ist genau dann entscheidbar, wenn die Theorie $\mathrm{Abl}(\Sigma)$ entscheidbar ist.

Wir zeigen jetzt, daß viele Mengen von Zahlen, die wichtige Mengen und Funktionen der Syntax verschlüsseln, rekursiv sind. Wir arbeiten mit der fixierten Sprache $L$.

a) $\mathrm{Vble}(a) \leftrightarrow a = \langle (a)_0 \rangle \wedge \exists\, y_{y \leq a}((a)_0 = 2y)$. Dann $\mathrm{Vble}(a)$ gdw $a = \ulcorner v_i \urcorner$ Vble ist rekursiv.

b) $\mathrm{Term}(a) \leftrightarrow 0 = 0$, wenn $a = \langle \mathrm{SN}(0) \rangle$
$\leftrightarrow \mathrm{Term}((a)_1)$, wenn $a = \langle \mathrm{SN}(S), (a)_1 \rangle$
$\leftrightarrow \mathrm{Term}((a)_1) \wedge \mathrm{Term}((a)_2)$,
wenn $a = \langle \mathrm{SN}(+), (a)_1, (a)_2 \rangle \vee a = \langle \mathrm{SN}(\cdot), (a)_1, (a)_2 \rangle$
$\leftrightarrow \mathrm{Vble}(a)$, sonst.

Term (a) trifft genau dann zu, wenn $a = \ulcorner t \urcorner$ für einen Term $t$. Die Definition ist induktiv mit Fallunterscheidungen. Also ist Term (a) rekursiv.

c) $\mathrm{AFor}(a) \leftrightarrow a = \langle (a)_0, (a)_1, (a)_2 \rangle \wedge ((a)_0 = \mathrm{SN}(=) \vee (a)_0 = \mathrm{SN}(<))$
$\wedge \mathrm{Term}((a)_1) \wedge \mathrm{Term}((a)_2)$

Gehen von klammernfreien Darstellungen $= t_1 t_2$ und $< t_1 t_2$ aus. $\mathrm{AFor}(a)$ ist rekursiv.

d) $\mathrm{For}(a) \leftrightarrow \mathrm{For}((a)_1)$, wenn $a = \langle \mathrm{SN}(\neg), (a)_1 \rangle$
$\leftrightarrow \mathrm{For}((a)_1) \wedge \mathrm{For}((a)_2)$, wenn $a = \langle \mathrm{SN}(\rightarrow), (a)_1, (a)_2 \rangle$
$\leftrightarrow \mathrm{Vble}((a)_1) \wedge \mathrm{For}((a)_2)$, wenn $a = \langle \mathrm{SN}(\forall), (a)_1, (a)_2 \rangle$
$\leftrightarrow \mathrm{AFor}(a)$, sonst.

Es gilt $\mathrm{For}(a)$ genau dann, wenn $a = \ulcorner \varphi \urcorner$ für eine Formel $\varphi$. $\mathrm{For}(a)$ ist wieder rekursiv.

e) Wir definieren $\mathrm{Sub}(a,b,c)$, so daß diese Funktion für $a = \ulcorner\varphi\urcorner$ (bzw. $a = \ulcorner t\urcorner$), $b = \ulcorner x\urcorner$ und $c = \ulcorner u\urcorner$ die Gödelzahl der Formel (bzw. des Terms) annimmt, die (den) man erhält, wenn jedes freie Vorkommen von $x$ durch $u$ ersetzt wird. Auf Variablenkollisionen wird erst einmal keine Rücksicht genommen. Analoges gelte für Terme.

$\mathrm{Sub}(a,b,c) = c$, wenn $\mathrm{Vble}(a) \wedge a = b$
$= \langle (a)_0, \mathrm{Sub}((a)_1, b, c)\rangle$, wenn $a = \langle (a)_0, (a)_1\rangle$
$= \langle (a)_0, \mathrm{Sub}((a)_1), b, c), \mathrm{Sub}((a)_2), b, c)\rangle$,
wenn $a = \langle (a)_0, (a)_1, (a)_2\rangle \wedge (a)_0 \neq \mathrm{SN}(\forall)$
$= \langle (a)_0, (a)_1, \mathrm{Sub}((a)_2, b, c)\rangle$,
wenn $a = \langle \mathrm{SN}(\forall), (a)_1, (a)_2\rangle \wedge (a)_1 \neq b$
$= a$, sonst.

$\mathrm{Sub}(a,b,c)$ ist wieder rekursiv. Es hängt von der vorgegebenen Signatur ab, wie auch die beiden folgenden Definitionen.

f) Falls $a = \ulcorner\varphi\urcorner$ oder $\ulcorner t\urcorner$ und $b = \ulcorner x\urcorner$, so soll $\mathrm{Fr}(a,b)$ sagen, daß $x$ frei in $\varphi$ bzw. $t$ vorkommt.
$\mathrm{Fr}(a,b) \leftrightarrow a = b$, wenn $\mathrm{Vble}(a)$
$\leftrightarrow \mathrm{Fr}((a)_1, b)$, wenn $a = \langle (a)_0, (a)_1\rangle$
$\leftrightarrow \mathrm{Fr}((a)_1, b) \vee \mathrm{Fr}((a)_2, b)$, wenn $a = \langle (a)_0, (a)_1, (a)_2\rangle \wedge$
$(a)_0 \neq \mathrm{SN}(\forall)$
$\leftrightarrow \mathrm{Fr}((a)_2, b) \wedge (a)_1 \neq b$ sonst.
Fr ist wieder rekursiv.

g) Subtl($\ulcorner\varphi\urcorner, \ulcorner x\urcorner, \ulcorner u\urcorner$) soll sagen, daß $\varphi^{u/x}$ vorgenommen werden darf, d.h. daß es keine Variablenkollisionen gibt. Weiterhin gilt immer Subtl($\ulcorner t\urcorner, \ulcorner x\urcorner, \ulcorner u\urcorner$) für Terme $t$ und $u$.

$\text{Subtl}(a,b,c) \leftrightarrow \text{Subtl}((a)_1, b, c)$, wenn $a = \langle (a)_0, (a)_1\rangle$

$\leftrightarrow \text{Subtl}((a)_1, b, c) \wedge \text{Subtl}((a)_2, b, c)$,

wenn $a = \langle (a)_0, (a)_1, (a)_2\rangle \wedge (a)_0 \neq \text{SN}(\forall)$

$\leftrightarrow \text{Subtl}((a)_2, b, c) \wedge (\neg\text{Fr}((a)_2, b) \vee \neg\text{Fr}(c, (a)_1)$,

wenn $a = \langle \text{SN}(\forall), (a)_1, (a)_2\rangle \wedge (a)_1 \neq b$

$\leftrightarrow 0 = 0$ sonst.

Subtl ist wieder rekursiv.

Gegeben sei eine Menge $\Sigma$ von $L$-Aussagen. Sei $NLAx_\Sigma = \{\ulcorner\varphi\urcorner : \varphi \in \Sigma\}$. Ziel ist es ein Prädikat $\text{Pr}_\Sigma(a,b)$ zu definieren, so daß:

i) $P_{r_\Sigma}(a,b)$ gilt genau dann, wenn $a = \ulcorner\varphi\urcorner$ für eine Formel $\varphi$ und $b = \langle \ulcorner\varphi_0\urcorner, \ldots, \ulcorner\varphi_{n-1}\urcorner\rangle$ für einen $\Sigma$-Beweis $\varphi_0, \ldots, \varphi_{n-1}$ für $\varphi$.

ii) Wenn $NLAx_\Sigma$ rekursiv ist, dann ist auch $Pr_\Sigma$ rekursiv.

h) Definieren $AAx(a)$, so daß $AAx(a)$ gdw $a = \ulcorner\chi\urcorner$, wobei $\chi$ aussagenlogisches Axiom. In klammernfreier Darstellung sind dies:

$\rightarrow \varphi \rightarrow \psi\varphi$

$\rightarrow\rightarrow \varphi \rightarrow \psi\theta \rightarrow\rightarrow \varphi\psi \rightarrow \varphi\theta$

$\rightarrow\rightarrow \neg\psi\neg\varphi \rightarrow\rightarrow \neg\psi\varphi\psi$

$AAx(a) \leftrightarrow \exists\, x_{x<a} \exists\, y_{y<a}(\text{For}(x) \wedge \text{For}(y)$

$\wedge a = \langle \text{SN}(\rightarrow), x, \langle \text{SN}(\rightarrow), y, x\rangle\rangle)$

$\vee \ldots\ldots$

$\vee \ldots\ldots$

$AAx$ ist rekursiv.

i) $QAx(a)$ für Quantorenaxiome. Diese sind:
$\forall x(\varphi \to \psi) \to (\varphi \to \forall x\psi)$, falls $x$ nicht frei in $\varphi$,
d.h. klammernfrei $\to \forall x \to \varphi\psi \to \varphi\forall x\psi$.
$\forall x\varphi \to \varphi^{t/x}$ falls Subtl($\ulcorner\varphi\urcorner, \ulcorner x\urcorner, \ulcorner t\urcorner$) d.h. klammernfrei $\to$ $\forall x\varphi\varphi^{t/x}$.
$QAx(a) \leftrightarrow \exists x_{x<a} \exists y_{y<a} \exists v_{v<a}$ [For$(x) \wedge$ For$(y) \wedge$ Vble$(v) \wedge$
$a = \langle \mathrm{SN}(\to), (a)_1, (a)_2\rangle \wedge$
$((\neg \mathrm{Fr}(x,v) \wedge (a)_1 = \langle \mathrm{SN}(\forall), v, \langle \mathrm{SN}(\to), x, y\rangle\rangle$
$\wedge (a)_2 = \langle \mathrm{SN}(\to), x, \langle \mathrm{SN}(\forall), v, y\rangle\rangle)$ } 1. Axiom
$\vee \exists t_{t<a}(\mathrm{Term}(t) \wedge \mathrm{Subtl}(x,v,t) \wedge \mathrm{Sub}(x,v,t) = y$
$\wedge (a)_1 = \langle \mathrm{SN}(\forall), v, x\rangle \wedge (a)_2 = y))]$ } 2. Axiom

$QAx$ ist rekursiv und trifft genau auf die Verschlüsselungen der Quantorenaxiome zu.

j) Ähnlich definiert man nun ein rekursives Prädikat $IAx$, so daß $IAx$ genau auf die $\ulcorner\varphi\urcorner$, wobei $\varphi$ Identitätsaxiom, zutrifft.

Für die Ableitungsregeln definieren wir die beiden folgenden rekursiven Prädikate:

k) $MP(a,b,c) \leftrightarrow b = \langle \mathrm{SN}(\to), c, a\rangle$
und

l) $G(a,b) \leftrightarrow \exists v_{v<a}(\mathrm{Vble}(v) \wedge a = \langle \mathrm{SN}(\forall), v, b\rangle)$

m) Sei

$$Ax_\Sigma(a) \leftrightarrow AAx(a) \vee QAx(a) \vee IAx(a) \vee NLAx_\Sigma(a).$$

Es gilt $Ax_\Sigma(a)$ genau dann, wenn $a = \ulcorner\varphi\urcorner$, wobei $\varphi$ $\Sigma$-Axiom. $Ax_\Sigma$ ist genau dann rekursiv, wenn $NLAx_\Sigma$ rekursiv ist.

n) $\mathrm{Prf}_\Sigma(a) \leftrightarrow \mathrm{Seq}(a) \wedge \mathrm{lh}(a) \neq 0 \wedge \forall\, i_{i<\mathrm{lh}(a)}(Ax_\Sigma((a)_i)$
$\vee \exists\, j_{j<i} \exists\, k_{k<i}(MP((a)_i,(a)_j,(a)_k) \vee G((a)_i,(a)_j)))$

$\mathrm{Prf}_\Sigma$ verschlüsselt $\Sigma$-Beweise und ist rekursiv, wenn $NLAx_\Sigma$ rekursiv ist.

o) $\mathrm{Pr}_\Sigma(a,b) \leftrightarrow \mathrm{Prf}_\Sigma(b) \wedge a = (b)_{\mathrm{lh}(b) \dot{-} 1}$ sagt dann, daß $b$ ein $\Sigma$-Beweis für $a$ ist. Wenn $NLAx_\Sigma$ rekursiv ist, so ist auch $\mathrm{Pr}_\Sigma(a,b)$ rekursiv.

Nun gilt $\mathrm{Thm}_\Sigma(a)$ gdw. $\exists\, x \mathrm{Pr}_\Sigma(a,x)$.

**Theorem 10.1** *Wenn $\Sigma$ rekursiv ist (d.h. $NLAx_\Sigma$), dann ist $\mathrm{Pr}_\Sigma$ rekursiv und $\mathrm{Thm}_\Sigma$ ist rekursiv aufzählbar.*