Motivation: Algebraische Analyse von Blockchiffren

Blockchiffren:

- Eine **Blockchiffre** berechnet eine Abbildung
$$F : \{0,1\}^n \times \{0,1\}^m \to \{0,1\}^m \text{ mit } (k,x) \mapsto y.$$
- Für alle $k \in \{0,1\}^n$ ist $F_k := F(k,\cdot)$ eine Permutation auf $\{0,1\}^m$.
- Blockchiffren sind das wichtigste Konstrukt der Kryptographie.

Angriff auf Blockchiffren

Gegeben: $x, y = F_k(x)$
Gesucht: $k = k_1 \dots k_n \in \{0,1\}^n$

Algebraische Modellierung:

- Betrachtes i-tes Ausgabebit von F_k
$$f_i := F_k^{(i)} : \{0,1\}^m \to \{0,1\} \text{ mit } x \mapsto y_i.$$
- Schreibe $f_1, \dots, f_m$ als Polynome in $k_1, \dots, k_n$ über $\mathbb{F}_2$.

Affine Varietät

Definition Affine Varietät

Seien $f_1, \ldots, f_m \in \mathbb{F}[x_1, \ldots, x_n]$ für einen Körper $\mathbb{F}$. Wir bezeichnen

$$\mathbf{V}(f_1, \ldots, f_m) = \{(a_1, \ldots, a_n) \in \mathbb{F}^n \mid f_i(a_1, \ldots, a_n) = 0 \text{ für } i = 1, \ldots, m\}$$

als die durch $f_1, \ldots, f_m$ definierte *affine Varietät*.

Anmerkungen:

- $\mathbf{V}(f_1, \ldots, f_m)$ ist die gemeinsame Nullstellenmenge von $f_1, \ldots, f_m$.
- Für Beispiele verwenden wir oft den Körper $\mathbb{F} = \mathbb{R}$, für die Kryptographie $\mathbb{F} = \mathbb{F}_p$.

Beispiele:

- $\mathbf{V}(x^2 + y^2 - 1)$ ist in $\mathbb{R}^2$ der Einheitskreis mit Mittelpunkt $\mathbf{0}$.
- $\mathbf{V}(x^2 + y^2 - z^2)$ liefert im $\mathbb{R}^3$ einen Doppelkegel.
- $\mathbf{V}(y - x^2, z - x^3)$ liefert als Schnitt zweier Flächen eine Kurve.
- $\mathbf{V}(xz, yz)$ ist die Vereinigung der (x, y)-Ebene mit der z-Achse.

Spezialfall Lineare Varietät

Definition Lineare Varietät

Sei $A \in \mathbb{F}^{m \times n}$ und $\mathbf{b} \in \mathbb{F}^m$. Dann definieren die Lösungen $\mathbf{V} = \{\mathbf{x} \in \mathbb{F}^n \mid A\mathbf{x} = \mathbf{b}\}$ eine *lineare Varietät*.

Anmerkungen:

- Sei $\text{rang}(A) = r$. Dann besitzt $\mathbf{V}$ Dimension $n - r$. D.h. $\dim(\mathbf{V})$ wird von der Anzahl linear unabhängiger Gleichungen bestimmt.

Ziele:

1. **Lösbarkeit:**
   Gilt $\mathbf{V}(f_1, \ldots, f_m) \neq \emptyset$, d.h. ist $f_1 = \ldots = f_m = 0$ lösbar?
2. **Endlichkeit:**
   Ist $\mathbf{V}(f_1, \ldots, f_m)$ endlich? Können wir alle Lösungen bestimmen?

Abgeschlossenheit unter Vereinigung und Schnitt

Satz Abgeschlossenheit unter Vereinigung und Schnitt

Seien V, W affine Varietäten. Dann sind auch $V \cap W$ und $V \cup W$ affine Varietäten.

Beweis:

- Seien $V = \mathbf{V}(f_1, \ldots, f_m)$ und $W = \mathbf{V}(g_1, \ldots, g_\ell)$. Sei $\mathbf{x} \in V \cap W$.
- Dann verschwindet $\mathbf{x}$ sowohl auf $f_1, \ldots, f_m$ als auch auf $g_1, \ldots, g_\ell$.
- Damit verschwindet $\mathbf{x}$ auf $f_1, \ldots, f_m, g_1, \ldots, g_\ell$, d.h.
$$V \cap W = \mathbf{V}(f_1, \ldots, f_m, g_1, \ldots, g_\ell).$$
- Wir zeigen weiterhin: $V \cup W = \mathbf{V}(f_i g_j \mid i = 1, \ldots, m, j = 1, \ldots, \ell)$.
- $V \cup W \subseteq \mathbf{V}(f_i g_j)$: Sei $\mathbf{x} \in V \cup W$, oBda $\mathbf{x} \in V$.
- Dann verschwindet $\mathbf{x}$ auf allen f_i und damit auf allen $f_i g_j$.
- $\mathbf{V}(f_i g_j) \subseteq V \cup W$: Sei $\mathbf{x} \in \mathbf{V}(f_i g_j)$.
- Falls $\mathbf{x} \in V$, gilt $\mathbf{x} \in V \cup W$. Sonst folgt $f_{i'}(\mathbf{x}) \neq 0$ für ein $i' \in [m]$.
- Andererseits verschwindet $\mathbf{x}$ auf allen $f_{i'} g_j$.
- Damit verschwindet $\mathbf{x}$ auf allen g_j. D.h. es gilt $\mathbf{x} \in W$.

Ideal

Definition Ideal

Eine Menge $I \subseteq \mathbb{F}[x_1, \ldots, x_n]$ heißt *Ideal* falls Folgendes gilt.

1. $0 \in I$.
2. Falls $f, g \in I$, dann ist $f + g \in I$.
3. Für $f \in I$ und $h \in \mathbb{F}[x_1, \ldots, x_n]$ gilt $hf \in I$.

Definition Polynomideal

Seien $f_1, \ldots, f_m \in \mathbb{F}[x_1, \ldots, x_n]$. Dann bezeichnen wir mit

$$\langle f_1, \ldots, f_m \rangle = \left\{ \sum_{i=1}^{m} h_i f_i \mid h_i \in \mathbb{F}[x_1, \ldots, x_n] \right\}$$

das *von* $f_1, \ldots, f_m$ *generierte Polynomideal*.

Anmerkung: $I = \langle f_1, \ldots, f_m \rangle$ ist ein Ideal.

- Sei $I = \langle f_1, \ldots, f_m \rangle$. $0 \in I$ wegen $0 = \sum_i 0 \cdot f_i$.
- Seien $f = \sum_i p_i f_i$, $g = \sum q_i f_i \in I$ und $h \in \mathbb{F}[x_1, \ldots, x_n]$. Dann gilt
$$f + g = \sum_i (p_i + q_i) f_i \in I \quad \text{und} \quad hf = \sum_i (hp_i) f_i \in I.$$

Varietäten und Ideale

Definition Basis eines Ideals

Ein Ideal I heißt *endlich erzeugt mit Basis* $f_1, \ldots, f_m \in \mathbb{F}[x_1, \ldots, x_n]$, falls $I = \langle f_1, \ldots, f_m \rangle$.

Satz Varietäten hängen nur vom Ideal ab

Seien $f_1, \ldots, f_m$ und $g_1, \ldots, g_\ell$ Basen eines Ideals I. Dann gilt

$$\mathbf{V}(f_1, \ldots, f_m) = \mathbf{V}(g_1, \ldots, g_\ell).$$

Beweis:

- Zeigen $\mathbf{V}(f_1, \ldots, f_m) \subseteq \mathbf{V}(g_1, \ldots, g_\ell)$. Umkehrung folgt analog.
- Sei $\mathbf{x} \in \mathbf{V}(f_1, \ldots, f_m)$. D.h. $f_i(\mathbf{x}) = 0$ für alle $i = 1, \ldots, m$.
- Da die f_i eine Basis von I bilden, können wir jedes g_j schreiben als $g_j = \sum_{i=1}^{m} h_i f_i$ für $j = 1, \ldots, \ell$.
- Damit gilt $g_j(\mathbf{x}) = \sum_i h_i(\mathbf{x}) \cdot f_i(\mathbf{x}) = 0$. D.h. $x \in \mathbf{V}(g_1, \ldots, g_\ell)$.

Bsp: Es gilt $\langle 2x^2 + 3y^2 - 11, x^2 - y^2 - 3 \rangle = \langle x^2 - 4, y^2 - 1 \rangle$ (Übung), d.h. $\mathbf{V}(2x^2 + 3y^2 - 11, x^2 - y^2 - 3) = \mathbf{V}(x^2 - 4, y^2 - 1) = \{(\pm 2, \pm 1)\}$.

Das Ideal einer Varietät

Frage: Welche Polynome verschwinden auf $\mathbf{V}(f_1, \ldots, f_m)$?

Definition Ideal einer Varietät

Sei V eine affine Varietät. Dann ist das Ideal von V definiert als

$$\mathbf{I}(V) = \{f \in \mathbb{F}[x_1, \ldots, x_n] \mid f(\mathbf{x}) = 0 \text{ für alle } x \in V\}.$$

Satz $\mathbf{I}(V)$ ist ein Ideal

Sei V eine affine Varietät. Dann ist $\mathbf{I}(V)$ ein Ideal.

Beweis:

- $0 \in \mathbf{I}(V)$, da das Nullpolynom auf allen Punkten verschwindet.
- Seien $f, g \in \mathbf{I}(V)$ und $h \in \mathbb{F}[x_1, \ldots, x_n]$. Für alle $\mathbf{x} \in V$ folgt
$$\underbrace{f(\mathbf{x})}_{=0} + \underbrace{g(\mathbf{x})}_{=0} = 0 \text{ und } h(\mathbf{x}) \cdot \underbrace{f(\mathbf{x})}_{=0} = 0.$$
- Damit gilt $f + g \in \mathbf{I}(V)$ und $hf \in \mathbf{I}(V)$.

Beispiel: Ideal einer Varietät

Bsp Ideal einer Varietät

$\mathbf{I}(\{(0,0)\}) = \langle x, y \rangle \subseteq \mathbb{F}[x,y]$.

Beweis:

- $\langle x, y \rangle \subseteq \mathbf{I}(\{(0,0)\})$: Sei $f \in \langle x, y \rangle$. Dann gilt
$$f(x,y) = h_1(x,y) \cdot x + h_2(x,y) \cdot y.$$
- Damit ist $f(0,0) = 0$ und es folgt $f \in \mathbf{I}(\{(0,0)\})$.
- $\mathbf{I}(\{(0,0)\}) \subseteq \langle x, y \rangle$: Sei $f \in \mathbf{I}(\{(0,0)\})$. Dann gilt
$$f(x,y) = \sum_{i,j} a_{ij} x^i y^j \text{ mit } f(0,0) = 0.$$
- Es folgt $a_{00} = 0$ und damit
$$f(x,y) = \left(\sum_{i,j,i>0} a_{ij} x^{i-1} y^j\right) \cdot x + \left(\sum_{j>0} a_{0j} y^{j-1}\right) \cdot y \in \langle x, y \rangle.$$

Polynome $\rightarrow$ Varietät $\rightarrow$ Ideal

Frage: Gilt $\langle f_1, \ldots, f_m \rangle = \mathbf{I}(\mathbf{V}(f_1, \ldots, f_m))$? Antwort: Leider nicht.

Satz

Es gilt $\langle f_1, \ldots, f_m \rangle \subset \mathbf{I}(\mathbf{V}(f_1, \ldots, f_m))$, aber i. Allg. keine Gleichheit.

Beweis:

- Sei $f \in \langle f_1, \ldots, f_m \rangle$, d.h. $f = \sum_{i=1}^{m} h_i f_i$ für Polynome h_i.
- Die Polynome $f_1, \ldots, f_m$ verschwinden auf allen $\mathbf{x} \in \mathbf{V}(f_1, \ldots, f_m)$.
- Damit gilt $f(\mathbf{x}) = 0$ für $\mathbf{x} \in \mathbf{V}(f_1, \ldots, f_m)$, d.h. $f \in \mathbf{I}(\mathbf{V}(f_1, \ldots, f_m))$.
- **Gegenbeispiel** für Gleichheit: $\mathbf{I}(\mathbf{V}(x^2, y^2)) \not\subseteq \langle x^2, y^2 \rangle$.
- Die Gleichungen $x^2 = y^2 = 0$ implizieren $\mathbf{V}(x^2, y^2) = \{(0, 0)\}$.
- Aus dem Beispiel zuvor folgt $\mathbf{I}(\mathbf{V}(x^2, y^2)) = \mathbf{I}(\{(0, 0)\}) = \langle x, y \rangle$.
- Es gilt aber $\langle x, y \rangle \not\subseteq \langle x^2, y^2 \rangle$, da z.B. x nicht in der Form $h_1 \cdot x^2 + h_2 \cdot y^2$ dargestellt werden kann.

Ideale definieren Varietäten

Definition Varietät eines Ideals $\mathbf{V}(I)$

Sei $I \subseteq \mathbb{F}[x_1, \ldots, x_n]$ ein Ideal. Wir definieren

$$\mathbf{V}(I) = \{(a_1, \ldots, a_n) \in \mathbb{F}^n \mid f(a_1, \ldots, a_n) = 0 \text{ für alle } f \in I\}.$$

Satz Varietät eines Ideals $\mathbf{V}(I)$

$\mathbf{V}(I)$ ist eine Varietät. Insbesondere gilt für $I = \langle f_1, \ldots, f_m \rangle$, dass

$$\mathbf{V}(I) = \mathbf{V}(f_1, \ldots, f_m).$$

Beweis:

- $\mathbf{V}(I) \subseteq \mathbf{V}(f_1, \ldots, f_m)$: Sei $(a_1, \ldots, a_n) \in \mathbf{V}(I)$. Dann gilt $f(a_1, \ldots, a_n) = 0$ für alle $f \in I$, d.h. insbesondere für $f_1, \ldots, f_m \in I$.
- $\mathbf{V}(f_1, \ldots, f_m) \subseteq \mathbf{V}(I)$: Sei $(a_1, \ldots, a_n) \in \mathbf{V}(f_1, \ldots, f_m)$ und $f \in I$.
- Wir schreiben $f = \sum_i h_i f_i$ und damit gilt

$$f(a_1, \ldots, a_n) = \sum_{i=1}^{m} h_i(a_1, \ldots, a_n) \cdot \underbrace{f_i(a_1, \ldots, a_n)}_{0} = 0.$$

Beziehung zwischen Varietäten und ihren Idealen

Satz

Seien $V, W \subseteq \mathbb{F}^n$ affine Varietäten. Dann gilt

1. $V \subseteq W$ gdw $\mathbf{I}(W) \subseteq \mathbf{I}(V)$.
2. $V = W$ gdw $\mathbf{I}(V) = \mathbf{I}(W)$.

Beweis:

- $\Rightarrow$: Sei $V \subseteq W$ und $f \in \mathbf{I}(W)$.
- Dann verschwindet f auf allen $\mathbf{x} \in W$ und damit auf allen $\mathbf{x} \in V$.
- Damit folgt $f \in \mathbf{I}(V)$.
- $\Leftarrow$: Sei $\mathbf{I}(W) \subseteq \mathbf{I}(V)$.
- Sei die affine Varietät W definiert durch die Polynome $f_1, \ldots, f_m$.
- Dann gilt $f_1, \ldots, f_m \in \mathbf{I}(W) \subseteq \mathbf{I}(V)$.
- D.h. $f_1, \ldots, f_m$ verschwinden insbesondere auf den Punkten aus V.
- Da W aus *allen* gemeinsamen Nst. der f_i besteht, folgt $V \subseteq W$.
- 2 folgt aus 1: $V = W$ gilt gdw $V \subseteq W$ und $W \subseteq V$ gdw $V = W$.

Interessante Probleme

Ziel: Löse die folgenden Probleme algorithmisch.

1. **Basisdarstellung:**
   Stelle jedes Ideal I mittels einer endlichen Basis $\langle f_1, \ldots, f_m \rangle$ dar.
2. **Idealzugehörigkeit:**
   Entscheide, ob f im Ideal $\langle f_1, \ldots, f_m \rangle$ liegt.
3. **Lösbarkeit von polynomiellen Gleichungssystemen:**
   Bestimme alle gemeinsamen Lösungen von

$$\left| \begin{array}{ccc} f_1 & = & 0 \\ & \vdots & \\ f_m & = & 0 \end{array} \right| .$$