RUHR
UNIVERSITÄT
BOCHUM

RUB

Lehrstuhl für Kryptologie und IT-Sicherheit
Prof. Dr. Alexander May
Gottfried Herold, Philipp Wagner

Hausübungen zur Vorlesung

Kryptanalyse

WS 2012/2013

Blatt 11 / 9. Januar 2013 / Abgabe bis spätestens 15. Januar 2013, 10 Uhr in dem Kasten auf NA 02

AUFGABE 1 (4 Punkte)**:**
Sei $\mathbb{F}$ beliebiger Körper. Zeigen Sie die Gleichheit folgender affiner Varietäten:

$$\langle X^2 + X + Y, XY \rangle = \langle Y^2, X^3Y, X^3 + X^2, X^3 - X - Y \rangle \subset \mathbb{F}^2$$

AUFGABE 2 (4 Punkte)**:**
Gegeben Sei eine Subset-Sum Instanz $a_1, \ldots, a_n, S$. Geben Sie Erzeuger $f_1, \ldots, f_s$ für ein Ideal $I = \langle f_1, \ldots, f_s \rangle \subset \mathbb{F}[X_1, \ldots, X_m]$ an, so dass die Punkte der zugehörigen affinen Varietät $V(I)$ exakt mit den Lösungen der Subset-Sum Instanz korrespondieren. Dabei sollen die f_i effizient (d.h. in Polynomzeit) aus den a_i, S berechenbar sein sowie aus jedem einzelnen Punkt $\vec{x} \in V(I)$ soll sich effizient eine Lösung des Subset-Sum Problems ermitteln lassen (Sie müssen diese Algorithmen nicht angeben, falls sie offensichtlich sind). Den Körper $\mathbb{F}$ dürfen Sie dabei selbst wählen.

AUFGABE 3 (6 Punkte)**:**
Beschreiben Sie alle möglichen Stellungen des in Abbildung 1 dargestellten Roboters durch ein System von Polynomgleichungen. Dabei seien die Punkte $(0, 0)$ und (x, y) um 360° drehbare Gelenke und (a, b) der Schreibkopf. Die Länge der Gelenke ist jeweils 1. Zeigen Sie formal, dass der Schreibkopf in der Lage ist alle Punkte auf dem Kreuz $\{(0, y) \mid y \in [-2, 2]\} \cup \{(x, 0) \mid x \in [-2, 2]\}$ zu erreichen. Welche Punkte kann der Schreibkopf erreichen (dies muss nicht formal bewiesen werden)?

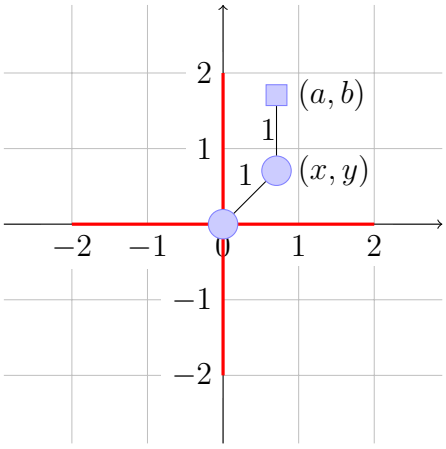

Abbildung 1: Roboter mit 2 Gelenken

AUFGABE 4 (6 Punkte)**:**
Zeigen Sie, dass die Kreisscheibe $D = \{(x, y) \in \mathbb{R}^2 \mid x^2 + y^2 \leq 2^2\}$ mit Radius 2 *keine* affine Varietät ist.
Hinweis: Nehmen Sie an, dass $D = V(I)$ wäre und betrachten sie den Schnitt von D mit einer Koordinatenachse. Überlegen Sie sich, dass dieser Schnitt dann $V(I') \subset \mathbb{R}$ ist, wobei I' aus I hervorgeht, indem man eine Variable auf 0 setzt. Insbesondere ist $I' \subset \mathbb{R}[X]$ ein Polynomideal in nur einer Variablen.