Bisher haben wir die Boolesche Kodierung betrachtet:
$x=0$ entspricht "Falsch" und $x=1$ entspricht "Wahr".

Über Körpern der Charakteristik $\neq 2$ (d.h. $1 \neq -1$)
eignet sich auch folgende Fourier-Repräsentation.

$y = -1$ entspricht "Wahr" und

$y = 1$ entspricht "Falsch".

Um Lösungen in $\{-1, 1\}$ zu erzwingen verwenden wir die Axiome $y^2 = 1$ (anstatt $x^2 = x$).

Die entsprechende Multilinearisierung ist dann

$$ML^{\text{Fourier}}\left(\sum_j a_j \prod_{i \in I_j} y_i^{d_i}\right) := \sum_j a_j \prod_{i \in I_j} y_i^{d_i \bmod 2}$$

Bsp.: $ML^{\text{Fourier}}(y_1^3 y_2^4 y_3) = y_1 y_3$

Es ist nicht schwer zu sehen, dass Satz 4.4, Lemma 4.5, Lemma 4.6, Satz 4.7 analog für Polynome $\{f_1, \dots, f_m\} \cup \{y_1^2 - 1, \dots, y_n^2 - 1\}$ in Fourier-Repräsentation gelten.

Das folgende Lemma gilt ebenfalls sowohl über der Booleschen als auch über der Fourier-Kodierung:

Lemma 4.8

Seien $f_1, \dots, f_m$ Binome der Form $f_s = \prod_{i \in I_s} y_i + a_s \prod_{j \in J_s} y_j$ mit $a_s \in \{-1, 1\}$ über einem Körper der Charakteristik $\neq 2$.

Wenn $f_1, \dots, f_m$ eine Grad-d Widerlegung im ML^{Fourier}-Polynomkalkül besitzen, dann besitzen sie eine Grad-d Widerlegung in der jedes Polynom die Form $\prod_{i \in I} y_i + a \cdot \prod_{j \in J} y_j$ für $a \in \{-1, 0, 1\}$ besitzt.

Beweis: Betrachte die Widerlegung, die von $\text{BASIS}_d^{\text{Fourier}}(f_1, \dots, f_m)$ gefunden wird und normiere stets den Leitkoeffizienten

(statt $\frac{f \quad g}{af + bg}$ verwende $\frac{f \qquad g}{\frac{1}{LK(af+bg)} \cdot a \cdot f + \frac{1}{LK(af+bg)} \cdot b \cdot g}$).

$\square$

$\Rightarrow$ Damit gilt auch: Jede Anwendung der $\frac{f \quad g}{af + bg}$-Regel hat die Form $\frac{f \quad g}{cf - cg}$ für $c \in \{-1, 1\}$ und $LT(f) = LT(g)$.

4.5. Untere Schranken für den Polynomkalkül

Ziel: Wir wollen beweisen, dass der Polynomkalkül über allen Körpern der Charakteristik $\neq 2$ nicht p-beschränkt ist.

Bemerkung: Es gibt auch unerfüllbare Klauselmengen, die über keinem Körper polynomielle Widerlegungen im Polynomkalkül besitzen.

Wir betrachten ein lineares Gleichungssystem über $\mathbb{F}_2$, in dem jede Gleichung höchstens k Variablen enthält.

$$L = \left\{ \sum_{i \in I_j} x_i = a_j \;\middle|\; 1 \leq j \leq m,\ |I_j| \leq k,\ a_j \in \{0,1\} \right\}$$

Kodiert als Klauselmenge:

$$F_L = \left\{ C_j \;\middle|\; \mathrm{var}(C_j) = I_j,\ \text{die Anzahl negativer Literale in } C_j \pmod 2 \text{ ist } 1-a_j \right\}$$

Kodiert als Binome in Fourier-Repräsentation über $\mathbb{F}$ ($\mathrm{char}\,\mathbb{F} \neq 2$):

$$P_L^{\text{Fourier}} = \left\{ \prod_{i \in I_j} Y_i - (-1)^{a_j} \;\middle|\; 1 \leq j \leq m \right\}$$

Wir wollen zeigen, dass $P_L^{\text{Fourier}} \cup \{y_i^2 - 1 \mid 1 \le i \le m\}$ keine Widerlegung vom Grad $o(n)$ besitzt.

(Für geeignete Systeme L.)

Dazu betrachten wir den folgenden Hilfskalkül:

Der <u>Gauß-Kalkül</u> operiert auf linearen Gleichungen über $\mathbb{F}_2$.

Einzige Regel: $$\frac{l_1 = 0 \quad l_2 = 0}{l_1 + l_2 = 0}.$$

Eine Widerlegung im Gaußkalkül ist eine Ableitung von $1 = 0$.

Die <u>Weite</u> einer Widerlegung ist die maximale Anzahl der Variablen in einer Zeile.

Lemma 4.9

Ein lineares Gleichungssystem L über $\mathbb{F}_2$ mit Variablen $x_1, \dots, x_n$ ist unerfüllbar genau dann, wenn L eine Widerlegung der Weite $\le n$ im Gauß-Kalkül besitzt.

<u>Beweis:</u> "$\Leftarrow$" einfach.

"$\Rightarrow$" Folgt aus dem Gaußschen Eliminationsverfahren. $\square$

Lemma 4.10

Wenn $P_L^{Fourier} \cup \{Y_i^2 - 1\}$ eine Ableitung im Polynomkalkül vom Grad d besitzt, dann hat L eine Gauß-Kalkül-Widerlegung der Weite $\leq 2d$.

Beweis:

Nach Lemma 4.5 (Fourier-Variante) und Lemma 4.8 sei Γ eine Widerlegung im $M(Fourier)$-Polynomkalkül vom Grad d mit der Eigenschaft, dass jede Zeile die Form $g = \prod_{i \in I} Y_i + a \cdot \prod_{j \in J} Y_j$ für $a \in \{-1, 0, 1\}$ hat.

Sei $Lin(g) := \begin{cases} 1, & \text{falls } a = 0 \\ \sum_{i \in I \Delta J} x_i, & \text{falls } a = -1 \\ \sum_{i \in I \Delta J} x_i + 1, & \text{falls } a = 1 \end{cases}$

- Für $f_i \in P_L^{Fourier}$ ist $Lin(f_i) = l_i$ die entsprechende Gleichung $l_i = 0$ in L.
- Für alle $g \in \Gamma$ $Lin(g) = Lin(Y_i \cdot g)$

Für alle Anwendungen der Regel

$$\frac{f \quad g}{cf - cg} \quad \text{mit} \quad c \in \{-1, 1\}, \; LT(f) = LT(g)$$

(Siehe Bemerkung auf S. 4-19) gilt:

$$Lin(cf - cg) = Lin(f) + Lin(g).$$

$$f = \prod_{i \in I} y_i + a \prod_{j \in J} y_j \qquad g = \prod_{i \in I} y_i + a' \prod_{j \in J'} y_j$$

$$Lin(f) = \sum_{i \in I \Delta J} y_i + 6 \qquad Lin(g) = \sum_{i \in I \Delta J'} y_i + \delta'$$

o.B.d.A. $J \subseteq J'$

$$Lin(cf - cg) = Lin\left(\prod_{i \in J} y_i - \frac{a'}{a} \prod_{j \in J'} y_j \right) = \sum_{i \in J \Delta J'} y_i + \delta''$$

1. $\sum_{i \in J \Delta J'} y_i = \sum_{i \in I \Delta J} y_i + \sum_{i \in I \Delta J'} y_i$ ✓

2. $\delta'' = \delta + \delta'$ $\Rightarrow$ Fallunterscheidung.

□ (Lemma 4.10)