Zur Erinnerung $L = \{ l_t = 0 \mid 1 \le t \le m \}$ mit $l_t = \left(\sum_{i \in I_t} x_i \right) + a_t$ mit $|I_t| \le k$ ist ein lineares Gleichungssystem über $\mathbb{F}_2$ und F_L die entsprechende Klauselmenge (s. S. 4-20).

Fourier-Kodierung der Klauselmenge F_L:

$$P_{F_L}^{Fourier} = \left\{ \prod_{i \in I} \frac{1 - Y_i}{2} \cdot \prod_{j \in J} \frac{1 + Y_j}{2} \;\middle|\; \bigvee_{i \in I} x_i \vee \bigvee_{j \in J} \overline{x}_j \in F_L \right\}$$

$$= \left\{ \prod_{i \in I_t \setminus J} \frac{1 - Y_i}{2} \cdot \prod_{j \in J} \frac{1 + Y_j}{2} \;\middle|\; 1 \le t \le m, \; J \subseteq I_t, \; |J| \bmod 2 = 1 - a_t \right\}$$

Boolesche Kodierung der Klauselmenge F_L:

$$P_{F_L} = \left\{ \prod_{i \in I_t \setminus J} (1 - x_i) \cdot \prod_{j \in J} x_j \;\middle|\; 1 \le t \le m, \; J \subseteq I_t, \; |J| \bmod 2 = 1 - a_t \right\}$$

Darstellung von L als Binome über Fourier-Basis:

$$P_L^{Fourier} = \left\{ \prod_{i \in I_t} Y_i - (-1)^{a_t} \;\middle|\; 1 \le t \le m \right\}$$

Lemma 4.11.

Wenn $P_{F_L} \cup \{x_i^2 - x_i \mid 1 \le i \le n\}$ eine Widerlegung vom Grad d im Polynomkalkül besitzt, dann hat $P_{F_L}^{Fourier} \cup \{Y_i^2 - 1 \mid 1 \le i \le n\}$ eine Widerlegung vom Grad d.

Beweis: Folgt aus Aufgabe 2, Blatt 4.

Lemma 4.12

Alle Polynome $f \in P_{F_L}^{Fourier}$ haben eine Ableitung vom Grad $\le k+1$ aus $P_L^{Fourier} \cup \{Y_i^2 - 1 \mid 1 \le i \le n\}$.

Beweis: Lösung (Blatt 5).

Lemma 4.13

Wenn $P_{F_L} \cup \{x_i^2 - x_i \mid 1 \le i \le n\}$ eine Grad-d Widerlegung über einem Körper $\mathbb{F}$ der Charakteristik $\neq 2$ im Polynomkalkül besitzt, dann hat L eine Gauß-kalkül Widerlegung der Weite $\le 2 \cdot \max(d, k+1)$.

Beweis: Folgt direkt aus Lemma 4.10, 4.11, 4.12. □

Aus Lemma 4.13 folgt: Um eine $\Omega(n)$ untere Schranke an den Grad im Polynomkalkül für $P_{\mathbb{F}_2}$ zu zeigen, genügt es eine $\Omega(n)$ untere Schranke an die Weite im Gauß-Kalkül für L zu zeigen.
Das gilt allerdings nur für Körper der Charakteristik $\neq 2$, wie der nächste Satz zeigt.

Satz 4.14

$P_{\mathbb{F}_2} \cup \{x_i^2 - x_i \mid 1 \leq i \leq n\}$ hat eine Polynomkalkül-Widerlegung von Grad $\leq k+1$ über $\mathbb{F}_2$.

Beweis:
1. Zeige, dass alle $l \in L$ eine Ableitung vom Grad $\leq k+1$ aus $P_{\mathbb{F}_2} \cup \{x_i^2 - x_i \mid 1 \leq i \leq n\}$ besitzen.
2. Finde anschließend eine Gauß-Kalkül Widerlegung ($\hat{=}$ Grad 1 Polynomkalkül über $\mathbb{F}_2$) von L. □

(Details: Übung)

4.6 Untere Schranken im Gauß-Kalkül

Ziel des Abschnitts ist der Beweis des folgenden Satzes.

Satz 4.15

Es gibt ein unerfüllbares kn. Gleichungssystem L über $\mathbb{F}_2$ mit n Variablen und $k=3$ Variablen pro Gleichung für das jede Widerlegung im Gauß-Kalkül Weite $\Omega(n)$ hat.

Definition Ein (nicht notwendigerweise bipartiter) Graph $H=(V,E)$ ist ein (Δ, s, c)-Expander, falls $|N(V')| \geq c \cdot |V'|$ für alle $V' \subseteq V$ mit $|V'| \leq s$ und $|N(v)| \leq \Delta$ für alle $v \in V$.

Lemma 4.16

Für $\Delta \geq 3$ und $c < \Delta - 2$ gibt es ein $\alpha(\Delta, c) > 0$, sodass es für alle geraden n ein $(\Delta, \alpha \cdot n, c)$-Expander mit n Knoten gibt.

Beweis:

- Wähle bipartiten $\frac{n}{2} \times \frac{n}{2}$ $(\Delta, \alpha' \frac{n}{2}, c')$ - Expander $G = (U_1 \cup U_2, E)$ wie im Beweis von Lemma 2.31a für $c' = c+1$.
- Wir hatten gezeigt: Für alle $U_1' \subseteq U_1$ mit $|U_1'| \leq \alpha' \frac{n}{2}$ gilt $|N(U_1')| \geq c' \cdot |U_1'|$.
- Wegen Symmetrie der Konstruktion (zur Erinnerung: wir wählten Δ perfekte Matchings) gilt auch $N(U_2') \geq c' \cdot |U_2'|$ für alle $U_2' \subseteq U_2$ mit $|U_2'| \leq \alpha' \frac{n}{2}$.
- G hat die gewünschte Eigenschaft:
  Sei $V' \subseteq V(G) = U_1 \cup U_2$ mit $|V'| \leq \alpha' \frac{n}{2}$
  und $V_1' := V' \cap U_1$, $V_2' := V' \cap U_2$.

$$N(V') = N(V_1') \setminus V_2' \cup N(V_2') \setminus V_1'$$

$$\geq c'|V_1'| - (|V'| - |V_1'|) + c' \cdot (|V'| - |V_1'|) - |V_1'|$$

$$= (c'-1)|V'| = c \cdot |V'|. \qquad \square$$

Für ein Graphen $H=(V,E)$ und eine Abbildung $\sigma: V \to \{0,1\}$ sei $L_{H,\sigma}$ das folgende lineare Gleichungssystem über $\mathbb{F}_2$:

$$L_{H,\sigma} := \{ l_v = 0 \mid v \in V \} \text{ mit}$$

$$l_v := \left(\sum_{w \in N(v)} x_{\{v,w\}} \right) + \sigma(v) .$$

Lemma 4.17

a) Wenn $\sum_{v \in V} \sigma(v) \equiv 1 \pmod 2$, dann ist $L_{H,\sigma}$ unerfüllbar.

b) Wenn $\sum_{v \in V} \sigma(v) \equiv 0 \pmod 2$ und G ist zusammenhängend, dann ist $L_{H,\sigma}$ erfüllbar.

Beweis: zu a): Summiere alle $l_v = 0$ und erhalte $1 = 0$.

zu b) Induktion über $|\{v \in V \mid \sigma(v) = 1\}| =: q$.

$q=0$: trivial (setze alle Variable auf 0).

$q \rightsquigarrow q+2$: Wähle zwei Knoten v, w mit $\sigma(v) = \sigma(w) = 1$.

Sei $\tilde{\sigma}(u) := \begin{cases} \sigma(u), & \text{falls } u \notin \{v,w\} \\ 0, & \text{falls } u \in \{v,w\} \end{cases}$ und $\tilde{a}$ erfüllende

Belegung für $L_{H,\tilde{\sigma}}$ nach IA.

Beweis von Lemma 4.17 (cont.)

Da G zusammenhängend, wähle Pfad p zwischen v und v in H.

Sei $\alpha(x_{\{u,u'\}}) := \begin{cases} \tilde{\alpha}(x_{\{u,u'\}}), & \text{falls } \{u,u'\} \notin p \\ 1 - \tilde{\alpha}(x_{\{u,u'\}}), & \text{falls } \{u,u'\} \in p \end{cases}$.

$\Rightarrow \alpha$ ist erfüllende Belegung für $L_{H,\sigma}$. $\square$

Im Folgenden sei $H = (V,E)$ ein $(3, \gamma n, \frac{1}{2})$-Expander und $\sigma : V \to \{0,1\}$ beliebig mit $\sum_{v \in V} \sigma(v) \equiv 1 \pmod 2$.
(Existiert nach Lemma 4.16).

Lemma 4.18

a) $L_{H,\sigma}$ ist unerfüllbar.

b) Alle $L' \subseteq L_{H,\sigma}$ mit $|L'| \leq \alpha n$ sind erfüllbar.

Beweis von Lemma 4.18

a) folgt aus Lemma 4.17 a)

Für b) sei $V' \subseteq V$ mit $L' = \{l_v = 0 \mid v \in V'\} \subseteq L$.

Sei $H[V']$ der induzierte Subgraph auf der Knotenmenge V'. Seien $V''_1, \dots, V''_\ell$ Zusammenhangskomponenten von $H[V']$. L' ist erfüllbar $\Leftrightarrow$ alle $L''_s := \{l_v = 0 \mid v \in V''_s\}$ sind erfüllbar. Sei also $V''_s \subseteq V'$ eine Zshg.skomponente von $H[V']$. $\Rightarrow N_H(V''_s) \subseteq V \setminus V'$ und $N_H(V''_s) \neq \emptyset$.

Sei $\hat{v} \in N(V''_s)$ und $\hat{w} \in V''$ mit $\{\hat{v}, \hat{w}\} \in E$.

- Falls $\sum_{u \in V''_s} \sigma(u) \equiv 0 \pmod 2$ ist $L_{H[V''_s],\sigma}$ nach Lemma 4.17 a) erfüllbar. Mit $\alpha(u) = 0$ für alle $u \in N_H(V''_s)$ ist dann auch L''_s erfüllbar.
- Falls $\sum_{u \in V''_s} \sigma(u) \equiv 1 \pmod 2$ ist $L_{H[V''_s],\tilde{\sigma}}$ mit

$$\tilde{\sigma}(u) := \begin{cases} \sigma(u), & \text{falls } u \neq \hat{v} \\ 1 - \sigma(u), & \text{falls } u = \hat{v} \end{cases}$$

erfüllbar nach Lemma 4.17 b)

Sei $\tilde{\alpha}$ die erfüllende Belegung, dann ist α mit

$$\alpha(x_{\{u,u'\}}) := \begin{cases} \tilde{\alpha}(x_{\{u,u'\}}), & u,u' \in V' \\ 1, & u = \hat{v}, u' = \hat{w} \\ 0, & \text{sonst} \end{cases}$$

erfüllende Belegung für L'. □

Satz 4.19

Jede Widerlegung von $L_{H,0}$ im Gauß-Kalkül hat Weite $\geq \frac{1}{4}\gamma_n$.

<Die Beweisstrategie ist ähnlich zu Lemma 2.28.>

Beweis

$L_{V'} := \{L_v \mid v \in V'\}$

Für eine lineare Gleichung $l = 0$ sei

$$\mu(l) := \min\{|V'| \mid V' \subseteq V,\ L_{V'} \models l\}$$

es gilt:

f.a. $\alpha : \{x_1, \dots, x_n\} \to \{0,1\}$ gilt $\alpha(l') = 0$ f.a. $l' \in L_{V'}$ impliziert $\alpha(l) = 0$.

(a) $\mu(L_v) = 1$ für alle $v \in V$.

(b) $\mu(l_1 + l_2) \leq \mu(l_1) + \mu(l_2)$ für alle l_1, l_2.

(da $L_{V_1} \models l_1$ und $L_{V_2} \models l_2$ impliziert $L_{V_1 \cup V_2} \models l_1 + l_2$)

(c) $\mu(1) > \gamma_n$

(nach Lemma 4.18 b) gilt $L_{V'} \not\models 1$ für alle $|V'| \leq \alpha n$)

$\Rightarrow$ In einer Gauß-Widerlegung von $L_{H,0}$ gibt es eine Gleichung $l = 0$ mit $\frac{\gamma_n}{2} \leq \mu(l) \leq \gamma_n$.

Beweis von Satz 4.19 (cont.)

Sei $V' \subseteq V$ minimal mit $L_{V'} \neq l$.

$\Rightarrow |V'| \leq \gamma n$ und $|N(V')| \geq \frac{1}{2}|V'| \geq \frac{1}{4}\gamma n$.

Behauptung: für alle $\{u,v\} \in E$ mit $u \in N(V')$, $v \in V'$ ist $x_{\{u,v\}}$ Variable in l.

Beweis: Angenommen $x_{\{\hat{u},\hat{v}\}}$ kommt nicht in l vor.

Wegen Minimalität gilt: $L_{V' \setminus \{\hat{v}\}} \neq l$.

Sei α Belegung mit $\alpha(l_v) = 0$ für alle $v \in V' \setminus \{\hat{v}\}$

und $\alpha(l) = 1$.

Wähle $\alpha(x_{\{\hat{u},\hat{v}\}})$ so, dass $\alpha(l_{\hat{v}}) = 0$.

(Das geht, da $x_{\{\hat{u},\hat{v}\}}$ weder in $L_{V' \setminus \{\hat{v}\}}$ noch in l vorkommt.)

$\Rightarrow \alpha(l_v) = 0$ für alle $v \in V'$ und

damit $L_{V'} \neq l$. $\lightning$

□

Beweis von Satz 4.15:

Folgt direkt aus Satz 4.19.

4.7 Die Größe von Beweisen im Polynomkalkül

In diesem Abschnitt zeigen wir, dass der Polynomkalkül nicht p-beschränkt ist (über Körpern der Charakteristik $\neq 2$). Das Gleiche gilt dann auch für die Varianten ML-Polynomkalkül, ML$^{\text{Fasin}}$-Polynomkalkül, PCR. Dazu nutzen wir die Grad-Lücke (Lemma 4.13 und Satz 4.15) und den folgenden Satz.

Satz 4.20

Sei P eine Menge von Polynomen vom Grad $\leq k$, (aus $\mathbb{F}[x_1, \dots, x_n]$) die keine 0/1-Lösung über einem Körper $\mathbb{F}$ besitzen und sei d der kleinste Grad einer Widerlegung von $P \cup \{x_i^2 - x_i \mid 1 \leq i \leq n\}$ im Polynomkalkül.

Dann hat jede Widerlegung von $P \cup \{x_i^2 - x_i \mid 1 \leq i \leq n\}$ die Größe $2^{\Omega\left(\frac{(d-k)^2}{n}\right)}$.

Der Beweis ist analog zu Satz 2.24.

Für eine Menge P von Polynomen in $\mathbb{F}[X_1,\dots,X_n]$ und $p \in \mathbb{F}[X_1,\dots,X_n]$ sei $P \vdash^d p$, falls es eine Ableitung von p aus $P \cup \{X_i^2 - X_i \mid 1 \le i \le n\}$ von Grad $\le d$ im Polynomkalkül gibt.

Lemma 4.21

Seien $f_1, f_2, \dots, f_m, g, g' \in \mathbb{F}[X_1,\dots,X_n]$ Polynome vom Grad $\le d$, $x \in \{X_1,\dots,X_n\}$.

1a) $\{f_1,\dots,f_m, x\} \vdash^d 1 \Rightarrow \{f_1,\dots,f_m\} \vdash^{d+1} 1-x$

1b) $\{f_1,\dots,f_m, 1-x\} \vdash^d 1 \Rightarrow \{f_1,\dots,f_m\} \vdash^{d+1} x$

2a) $\{f, x\} \vdash^d f|_{x=0}$

2b) $\{f, 1-x\} \vdash^d f|_{x=1}$

3a) $\{f_1|_{x=0},\dots,f_m|_{x=0}\} \vdash^d 1$ und $\{f_1|_{x=1},\dots,f_m|_{x=1}\} \vdash^{d+1} 1$
$\Rightarrow \{f_1,\dots,f_m\} \vdash^{d+1} 1$

3b) $\{f_1|_{x=1},\dots,f_m|_{x=1}\} \vdash^d 1$ und $\{f_1|_{x=0},\dots,f_m|_{x=0}\} \vdash^{d+1} 1$
$\Rightarrow \{f_1,\dots,f_m\} \vdash^{d+1} 1$

Sei $\deg(P \vdash f) := \min\{d \mid P \vdash_d f\}$.

(falls f aus P ableitbar).

Beweis von Satz 4.20

Sei $a_n := \frac{1}{1 - \frac{\tilde{d}}{n}}$ für ein festes $\tilde{d}$.

Für eine Polynomkalkül-Widerlegung Γ sei

$T_\Gamma := \{t \mid t \text{ ist Term in } f,\ f \in \Gamma,\ \deg(t) \geq \tilde{d}\}$

die Menge aller großen Terme in der Widerlegung Γ.

Induktiv über b und n:

$(*)$ $|T_\Gamma| < a_n^b \Rightarrow \deg(P \vdash 1) \leq \tilde{d} + b + k$.

(Induktionsanfang $b=0$, $n=1$ trivial)

Sei x Variable, die in $\geq \frac{\hat{d} \cdot |T_\Gamma|}{n}$ Klauseln aus T_Γ vorkommt.

$\Rightarrow P|_{x=0}$ hat $\leq \left(1 - \frac{\hat{d}}{n}\right)|T_\Gamma| < a_n^{(b-1)}$ Terme

der von Grad $\geq \tilde{d}$

$\overset{IA(b)}{\Rightarrow} \deg(P|_{x=0} \vdash 1) \leq \tilde{d} + b - 1 + k$ (1)

Außerdem (Induktion nach n):

$$\deg(P|_{x=1} + 1) \leq \tilde{d} + b + k \qquad (2)$$

Aus ⊛ + (2) und Lemma 4.21 3a) folgt:

$\deg(P+1) \leq \tilde{d} + b + k$. Damit ist ⊛ bewiesen.

Mit $\tilde{d} := \lceil \sqrt{n \cdot \ln(\|\Gamma\|)} \rceil$ gilt dann

$$\|\Gamma\| = e^{\frac{\sqrt{n \ln(4\|\Gamma\|)}^2}{n}}$$

$$\leq e^{\frac{\tilde{d}^2}{n}} \leq \left(\frac{1}{1 - \frac{\tilde{d}}{n}}\right)^{\tilde{d}} = a_n^{\tilde{d}}$$

$$\Rightarrow |\Gamma_n| < a_n^{\tilde{d}}$$

$$\overset{⊛}{\Rightarrow} \deg(P+1) \leq 2\tilde{d} + k \leq \sqrt{4n \cdot \ln(\|P\|)} + k$$

$$\Rightarrow \|\Gamma\| \geq e^{\frac{(\deg(P+1) - k)^2}{4n}} \qquad \square \text{ Satz 4.20}$$