Deterministische Kommunikation

Das Kommunikationsproblem

Alice und **Bob** möchten die Funktion $\mathbf{f} : \mathbf{X} \times \mathbf{Y} \rightarrow \mathbf{Z}$ durch den *Austausch binärer Nachrichten mit minimaler Gesamtlänge berechnen.*

Ihr Wissen ist allerdings beschränkt:

- **Alice** erhält die Eingabe $\mathbf{x} \in \mathbf{X}$,
- **Bob** die Eingabe $\mathbf{y} \in \mathbf{Y}$.
- Kein Spieler kennt die Eingabe des Anderen.

Beide Spieler haben unbeschränkte Rechenkraft.

Kommunikationsprotokolle

Ein Protokoll steuert den Ablauf der Kommunikation.

- Der Protokollbaum von $\mathcal{P}$ ist ein beschrifteter binärer Baum.
  - Jeder innere Knoten **v** ist mit dem verantwortlichen Spieler, also entweder mit **Alice** oder **Bob** beschriftet.
  - Ist ein innerer Knoten **v** mit **Alice** (bzw. **Bob**) beschriftet, dann wird auch eine Funktion $\mathbf{A_v} : \mathbf{X} \to \{\mathbf{0}, \mathbf{1}\}$ (bzw. $\mathbf{B_v} : \mathbf{Y} \to \{\mathbf{0}, \mathbf{1}\}$) angegeben. Jede Nachricht eines Spielers hängt von der Eingabe und allen bisher ausgetauschten Bits ab.
- Der Verlauf der Kommunikation.
  - Wenn die Wurzel mit **Alice** (bzw. **Bob**) beschriftet ist, beginnt **Alice** (bzw. **Bob**) die Berechnung.
  - Hat die Berechnung den Knoten **v** erreicht und ist **v** mit **Alice** (bzw. **Bob**) beschriftet, dann wird die Berechnung genau dann im linken Kind von **v** fortgesetzt, wenn $\mathbf{A_v}(\mathbf{x}) = \mathbf{0}$ (bzw. $\mathbf{B_v}(\mathbf{y}) = \mathbf{0}$).
  - Hat die Berechnung für Eingabe $\mathbf{x} \in \mathbf{X}$ und $\mathbf{y} \in \mathbf{Y}$ ein Blatt **b** erreicht, dann ist **z** die Ausgabe von $\mathcal{P}$ für Eingabe $(\mathbf{x}, \mathbf{y})$ falls **b** mit **z** beschriftet ist.

Ein Beispiel

Für $\mathbf{x} \in \mathbf{X} = \{\mathbf{0}, \mathbf{1}\}^{\mathbf{n}}$ und $\mathbf{i} \in \mathbf{Y} = \{\mathbf{1}, \ldots, \mathbf{n}\}$ ist die Funktion

$$\mathrm{bit}_{\mathbf{n}}(\mathbf{x}, \mathbf{i}) = \mathbf{x}_{\mathbf{i}}$$

zu berechnen.

- Wenn **Bob** die Kommunikation beginnt, dann

  gelingt eine Berechnung mit $\lceil \log_2 \mathbf{n} \rceil$ *Bits,*

  wenn **Bob** seine Eingabe vollständig kommuniziert.
  - Wenn $n = 2^k$, dann besteht das Protokoll aus einem vollständigen binären Baum der Tiefe k: Sämtliche inneren Knoten sind mit **Bob** beschriftet, während Blätter mit **Alice** beschriftet sind.
  - Setze $B_v(i) =$ das $t + 1$ste Bit von i für Knoten der Tiefe $t < k$.
  - Wird Blatt b erreicht, dann kennt **Alice** den Wert i und gibt x_i aus.
- Wenn nur **Alice** Nachrichten verschicken darf, dann muss(!?) sie ihre Eingabe x vollständig kommunizieren:

  $\mathbf{n}$ *Bits sind hinreichend(!) und notwendig(?).*

Deterministische Kommunikationskomplexität

Die Funktion $\mathbf{f} : \mathbf{X} \times \mathbf{Y} \to \mathbf{Z}$ sei gegeben.

(a) Ein Protokoll $\mathcal{P}$ für $\mathbf{f}$ berechnet Ausgabe $\mathbf{f}(\mathbf{x}, \mathbf{y})$ für jede Eingabe $\mathbf{x} \in \mathbf{X}$, $\mathbf{y} \in \mathbf{Y}$. $\mathcal{P}$ **kommuniziert s Bits**, wenn sein Protokollbaum die Tiefe $\mathbf{s}$ hat.

(b) Die **deterministische Kommunikationskomplexität** von f ist

$$\mathbf{D}(\mathbf{f}) = \min\{\mathbf{s} \mid \text{es gibt ein Protokoll für } f\text{, das } s \text{ Bits austauscht}\}.$$

(c) Wenn nur **Alice** Nachrichten verschicken darf, dann sprechen wir von einem einseitigen **A → B Protokoll** und definieren

$$\mathbf{D}^{\mathbf{A}\to\mathbf{B}}(\mathbf{f}) = \min\{s \mid \text{es gibt ein einseitiges } A \to B \text{ Protokoll für } f\text{, das } s \text{ Bits austauscht}\}.$$

$\mathbf{D}^{\mathbf{B}\to\mathbf{A}}$ wird analog definiert.

Das Zusammenhangsproblem

Das Zusammenhangsproblem für ungerichtete Graphen G mit $\mathbf{n}$ Knoten:

- Wir nehmen an, dass G durch seine Adjazenzmatrix spezifiziert wird, wobei eine Hälfte aller Eingaben an **Alice** und die andere Hälfte an **Bob** vergeben wird.
- **Alice** und **Bob** kommunizieren, um einen Spannbaum

  zum Beispiel mit Hilfe der Tiefensuche

  zu berechnen.

$\mathbf{O}(\mathbf{n} \log_2 \mathbf{n})$ Bits reichen aus.

Einseitige Kommunikation

Die Kommunikationsmatrix

Die Funktion $f : X \times Y \to Z$ sei gegeben. Die Kommunikationsmatrix M_f von f besitzt genau eine Zeile für jede Eingabe $x \in X$ und genau eine Spalte für jede Eingabe $y \in Y$. Wir setzen

$$M_f[x, y] = f(x, y).$$

Eine Charakterisierung von $\mathbf{D}^{\mathbf{A}\to\mathbf{B}}(\mathbf{f})$

- Es genügt, wenn Alice mitteilt, zu welcher der α verschiedenen Zeilen ihre Eingabe gehört und deshalb ist $D^{A\to B}(f) \leqslant \lceil \log_2 \alpha \rceil$.
- Warum muss $D^{A\to B}(f) \geqslant \lceil \log_2 \alpha \rceil$ gelten?

Satz: Die Funktion $f : X \times Y \to Z$ sei gegeben. Wenn die Kommunikationsmatrix M_f α verschiedene Zeilen hat, dann folgt

$$\mathbf{D}^{\mathbf{A}\to\mathbf{B}}(\mathbf{f}) = \lceil \log_2 \alpha \rceil.$$

$\mathrm{bit}_n(x, i) = x_i$

- Wie sieht die Kommunikationsmatrix von $\mathbf{bit_n}$ aus?
  - Wenn wir Spalten lexikographisch aufsteigend (gemäß ihrer jeweiligen Eingabe) anordnen, stimmt die Zeile von Eingabe x mit x überein.
  - Die Kommunikationsmatrix hat 2^n Zeilen und n Spalten:

$$D^{A\to B}(\mathrm{bit}_n) = n \;\text{ und }\; D^{B\to A}(\mathrm{bit}_n) = \lceil \log_2 n \rceil.$$

- Also kann es einen exponentiellen Unterschied zwischen einseitigen und mehrseitigen Protokollen geben; ein größerer Unterschied ist aber nicht möglich:

Die Funktion $f : X \times Y \to Z$ sei gegeben. Zeige:

$$D(f) \leqslant D^{A\to B}(f) \leqslant 2^{D(f)}.$$

Es gelte $X^* \subseteq X$ und $Y^* \subseteq Y$.

- Die Teilmatrix $M_f(X^*, Y^*)$ von M_f besteht aus allen Zeilen zu Eingaben in X^* und aus allen Spalten zu Eingaben in Y^*.
- Sei $b \in \{0, 1\}$. Wir sagen, dass eine Teilmatrix **b-chromatisch** ist, wenn alle Einträge der Teilmatrix den Wert b besitzen. Eine b-chromatische Teilmatrix heißt auch **monochromatisch**.

- Angenommen, **Alice** beginnt die Berechnung: Ihre Nachrichten zerlegen die Kommunikationsmatrix in Teilmatrizen $\mathbf{X_i} \times \mathbf{Y}$.
- **Bob** zerlegt jede Teilmatrix $\mathbf{X_i} \times \mathbf{Y}$ in Teilmatrizen $\mathbf{X_i} \times \mathbf{Y_j}$.
- Wenn **Alice** (bzw. **Bob**) die Ausgabe bestimmt, dann besitzt jede Teilmatrix der Zerlegung nur monochromatische Zeilen (Spalten).

Zweiseitige Kommunikation (2/2)

Nachrichten entsprechen Teilmatrizen und Teilmatrizen zerlegen die Kommunikationsmatrix.

Sei $\mathcal{P}$ ein deterministisches Protokoll für eine Boolesche Funktion $\mathbf{f} : \mathbf{A} \times \mathbf{B} \rightarrow \{\mathbf{0}, \mathbf{1}\}$ und $\mathcal{P}$ tausche höchstens $\mathbf{k}$ Bits aus.

- Wenn **Alice** die Ausgabe bestimmt, dann definiert $\mathcal{P}$ eine Zerlegung von M_f in höchstens $\mathbf{2^k}$ Teilmatrizen mit monochromatischen Zeilen.
- Bestimmt **Bob** die Ausgabe, dann definiert $\mathcal{P}$ eine Zerlegung von $\mathbf{M_f}$ in Teilmatrizen mit monochromatischen Spalten.

Die Methode der größten monochromatischen Teilmatrix

Die Methode der größten monochromatischen Teilmatrix

Die Funktion $\mathbf{f} : \mathbf{X} \times \mathbf{Y} \to \{\mathbf{0}, \mathbf{1}\}$ und das Bit $\mathbf{b} \in \{\mathbf{0}, \mathbf{1}\}$ seien gegeben.

- Für eine Menge $\mathbf{F} \subseteq \mathbf{f}^{-1}(\mathbf{b})$ von Eingaben mit Wert $\mathbf{b} \in \{\mathbf{0}, \mathbf{1}\}$ definiere

$$\mathrm{Max}_{b,F}(M_f) \quad = \quad \text{die maximale Anzahl von Einträgen aus } F, \text{ die von einer } b\text{-chromatischen Teilmatrix von } M_f \text{ überdeckt werden.}$$

- $\mathrm{Max}_{\mathbf{b}}(\mathbf{M_f}) = \max_{\mathbf{F} \subseteq \mathbf{f}^{-1}(\mathbf{b})} \left\lceil \log_{\mathbf{2}} \frac{|\mathbf{F}|}{\mathrm{Max}_{\mathbf{b},\mathbf{F}}(\mathbf{M_f})} \right\rceil$.

- Bestimme eine schwierige Menge F von Einträgen in M_f mit Wert b.
- Alle Einträge in F müssen überdeckt werden.
- Eine b-chromatische Nachricht überdeckt $\leqslant \mathrm{Max}_{\mathbf{b}}(\mathbf{M_f})$ Einträge in F.

Für die Funktion $f : X \times Y \to \{0, 1\}$ und das Bit $b \in \{0, 1\}$ gilt

$$\mathbf{D}(\mathbf{f}) \geqslant \max\{\mathrm{Max}_{\mathbf{0}}(\mathbf{M_f}), \mathrm{Max}_{\mathbf{1}}(\mathbf{M_f})\}.$$

Das Gleichheitsproblem EQ_n

Im *Gleichheitsproblem* EQ_n ist festzustellen, ob $\mathbf{x}, \mathbf{y} \in \mathbf{X} = \mathbf{Y} = \{\mathbf{0}, \mathbf{1}\}^{\mathbf{n}}$ identisch ($\mathrm{EQ}_n(x, y) = 1$) oder verschieden ($\mathrm{EQ}_n(x, y) = 0$) sind.

- Die Kommunikationsmatrix von EQ_n ist die Einheitsmatrix.
- Wähle die Diagonale aus: Setze $\mathbf{F} = \{(\mathbf{x}, \mathbf{x}) \mid \mathbf{x} \in \{\mathbf{0}, \mathbf{1}\}^{\mathbf{n}}\}$.
  - Eine 1-chromatische Teilmatrix kann nur aus einem einzigen Eintrag bestehen:
    $$\mathbf{D}(\mathrm{EQ}_{\mathbf{n}}) \geqslant \mathrm{Max}_{\mathbf{1}}(\mathbf{M}_{\mathrm{EQ}_{\mathbf{n}}}) \geqslant \lceil \log_{\mathbf{2}} \frac{\mathbf{2}^{\mathbf{n}}}{\mathbf{1}} \rceil = \mathbf{n}.$$
  - Aber n Bits sind auch ausreichend und
    $$\mathbf{D}(\mathrm{EQ}_{\mathbf{n}}) = \mathbf{n}$$
    ist die exakte Kommunikationskomplexität des Gleichheitsproblems.

Das Vergleichsproblem

Im *Vergleichsproblem* COMP_n ist festzustellen,
ob $\mathbf{x} \in \mathbf{X} = \{\mathbf{0}, \mathbf{1}\}^{\mathbf{n}}$ lexikographisch kleiner oder gleich $\mathbf{y} \in \mathbf{Y} = \{\mathbf{0}, \mathbf{1}\}^{\mathbf{n}}$ ist ($\text{COMP}_n(x, y) = 1$) oder nicht ($\text{COMP}_n(x, y) = 0$).

- Die Kommunikationsmatrix von COMP_n ist eine obere Dreiecksmatrix.
- Sowohl $\mathbf{F} = \mathbf{f}^{-1}(\mathbf{0})$ wie auch $\mathbf{F} = \mathbf{f}^{-1}(\mathbf{1})$ sind schlechte Wahlen: Es gibt riesige 0-chromatische und 1-chromatische Teilmatrizen.
- Stattdessen wähle die Diagonale und setze $\mathbf{F} = \{(\mathbf{x}, \mathbf{x}) \mid \mathbf{x} \in \{\mathbf{0}, \mathbf{1}\}^{\mathbf{n}}\}$.
- Wie im Gleichheitsproblem ist

$$\mathbf{D}(\mathrm{COMP}_{\mathbf{n}}) \geqslant \mathrm{Max}_{\mathbf{1}}(\mathbf{M}_{\mathrm{COMP}_{\mathbf{n}}}) \geqslant \lceil \log_{\mathbf{2}} \frac{\mathbf{2}^{\mathbf{n}}}{\mathbf{1}} \rceil = \mathbf{n}$$

und die exakte Kommunikationskomplexität ist $\mathbf{D}(\mathrm{COMP}_{\mathbf{n}}) = \mathbf{n}$.

Das innere Produkt

$$\langle \mathbf{x}, \mathbf{y} \rangle_{\mathbf{2,n}} := \sum_{\mathbf{i=1}}^{\mathbf{n}} \mathbf{x_i} \cdot \mathbf{y_i} \bmod \mathbf{2}$$

ist für $\mathbf{x}, \mathbf{y} \in \mathbf{X} = \mathbf{Y}\{\mathbf{0}, \mathbf{1}\}^{\mathbf{n}}$ zu berechnen.

- Wir wählen $F = f^{-1}(0)$ und bestimmen die Größe einer größten 0-chromatischen Teilmatrix M.
- $\mathbf{z_1}, \ldots, \mathbf{z_r}$ und $\mathbf{s_1}, \ldots, \mathbf{s_t}$ seien die den Zeilen, bzw den Spalten von M entsprechenden Eingaben. Dann gilt $\langle \mathbf{z_i}, \mathbf{s_j} \rangle_{\mathbf{2,n}} = \mathbf{0}$.
- Sei V_Z der von $z_1, \ldots, z_r$ aufgespannte Vektorraum und V_S der von $s_1, \ldots, s_t$ aufgespannte Vektorraum. Für $\mathbf{z} \in \mathbf{V_Z}, \mathbf{s} \in \mathbf{V_S}$ gilt

$$\begin{aligned} \langle z, s \rangle_{2,n} &= \langle \sum_{i=1}^{r} \alpha_i \cdot z_i, \sum_{i=1}^{t} \beta_j \cdot s_j \rangle_{2,n} = \sum_{i=1}^{r} \alpha_i \cdot \langle z_i, \sum_{j=1}^{t} \beta_j \cdot s_j \rangle_{2,n} \\ &= \sum_{i=1}^{r} \sum_{j=1}^{t} \alpha_i \beta_j \cdot \underbrace{\langle z_i, s_j \rangle_{2,n}}_{=0} = 0. \end{aligned}$$

Das innere Produkt (2/2)

Der Vektorraum $\mathbf{V_Z} = \langle \mathbf{z_1}, \ldots, \mathbf{z_r} \rangle$ steht senkrecht auf dem Vektorraum $\mathbf{V_S} = \langle \mathbf{s_1}, \ldots, \mathbf{s_t} \rangle$.

- Als Konsequenz
$$\dim(\mathbf{V_Z}) + \dim(\mathbf{V_S}) \leqslant \mathbf{n}.$$
- Der Vektorraum V_Z hat $\mathbf{2}^{\dim(\mathbf{V_Z})}$ Elemente und V_S hat $\mathbf{2}^{\dim(\mathbf{V_S})}$ Elemente und deshalb
$$|\mathbf{V_Z}| \cdot |\mathbf{V_S}| = \mathbf{2}^{\dim(\mathbf{V_Z}) + \dim(\mathbf{V_S})} \leqslant \mathbf{2^n}.$$
- Eine 0-chromatische Teilmatrix überdeckt höchstens 2^n Einträge.

Die Kommunikationsmatrix hat $(2^n - 1)2^{n-1} + 2^n = 2^{2n-1} + 2^{n-1}$ 0-Einträge: Mindestens n Bits sind notwendig, aber n Bits sind auch ausreichend $\Rightarrow$
$$\mathbf{D}(\langle , \rangle_{\mathbf{2,n}}) = \mathbf{n}.$$

Die Platz-Komplexität der Palindomsprache

Sei **P** die Palindromsprache über dem Alphabet $\{0, 1\}$.
Dann gehört **P** zu DL, aber **P** gehört nicht zu $\mathrm{DSPACE}(\mathbf{s})$ für $\mathbf{s} = \mathbf{o}(\log_2 \mathbf{n})$.

- Wir wissen bereits, dass **P** zu DL gehört.
- Sei **M** eine I-O Turingmaschine, die **P** mit Speicherplatz $s(n)$ akzeptiert.
- Wir simulieren **M** durch ein Kommunikationsmodell:
  - **Alice** erhält den Präfix der ersten $n/2$ Bits,
    Bob den Suffix der letzten $n/2$ Bits.
  - Jedesmal, wenn der Lesekopf die Position $n/2 + 1$, von links kommend, besucht, schickt **Alice** den Zustand, den Speicherinhalt und die Position des Lese/Schreibkopfes an **Bob**.
  - **Bob** verhält sich ähnlich, wenn der Lesekopf, von rechts kommend, die Position $n/2$ besucht.
- **Alice** und **Bob** müssen mindestens n Bits austauschen $\Rightarrow$
- Der Lesekopf muss die Position $n/2$ mindestens $\Omega(\frac{n}{s(n)})$ mal besuchen.

Ohne in eine Schleife zu geraten, gelingt dies nur für $s = \Omega(\log_2 n)$.

Fooling-Sets

Fooling-Sets (1/2)

Die Funktion $\mathbf{f} : \mathbf{X} \times \mathbf{Y} \to \{\mathbf{0}, \mathbf{1}\}$ sei gegeben. Eine Menge

$$\mathbf{F} = \{(\mathbf{x_1}, \mathbf{y_1}), (\mathbf{x_2}, \mathbf{y_2}), \ldots, (\mathbf{x_k}, \mathbf{y_k})\} \subseteq \mathbf{X} \times \mathbf{Y}$$

mit $\mathbf{f}(\mathbf{x_1}, \mathbf{y_1}) = \cdots = \mathbf{f}(\mathbf{x_k}, \mathbf{y_k}) = \mathbf{b}$ heißt **Fooling-Set für f**, wenn für alle $1 \leqslant i \neq j \leqslant k$

- $x_i \neq x_j$ und $y_i \neq y_j$ (höchstens ein Element in F pro Zeile oder Spalte),
- $f(x_i, y_j) \neq b$ oder $f(x_j, y_i) \neq b$.

Eine monochromatische Teilmatrix überdeckt höchstens einen Eintrag in **F**.

Wenn **F** ein **Fooling-Set für f** ist, dann gilt

$$\mathbf{D}(\mathbf{f}) \geqslant \lceil \log_2 |\mathbf{F}| \rceil.$$

- Fooling-Sets sind ein Spezialfall der Methode der größten monochromatischen Teilmatrix.
  - Im Gleichheitsproblem ($\mathbf{x} \stackrel{?}{=} \mathbf{y}$) und im Vergleichsproblem ($\mathbf{x} \stackrel{?}{\leqslant} \mathbf{y}$) ist die Diagonale der Kommunikationsmatrix ein Fooling Set.
  - Im Disjunktheitsproblem $\mathbf{DISJ_n}$ ist für Inzidenzvektoren $\mathbf{x}, \mathbf{y} \in \{\mathbf{0}, \mathbf{1}\}^{\mathbf{n}}$ zweier Teilmengen $\mathrm{set}(x), \mathrm{set}(y) \subseteq \{1, \ldots, n\}$ zu entscheiden, ob $\mathbf{DISJ_n}(x, y) = 1$ ($\mathrm{set}(x) \cap \mathrm{set}(y) \neq \emptyset$) oder $\mathbf{DISJ_n}(x, y) = 0$ (sonst).

    Übungsaufgabe: DISJ_n besitzt ein Fooling-Set der Größe 2^n.
- Fooling-Sets sind leicht anwendbar, aber nur wenige Probleme besitzen große Fooling-Sets.
  - Wir zeigen später, dass das **innere Produkt** $\langle , \rangle_{\mathbf{2,n}}$ **modulo zwei** nur Fooling Sets der Größe $(n+1)^2$ besitzt.
  - Übungsaufgabe: Eine **zufällige Funktion** $f : \{0, 1\}^{2n} \to \{0, 1\}$ hat nur Fooling-Sets der Größe $O(n)$.

Die Rangmethode

Die Rangmethode (1/2)

Wenn K ein Körper ist, dann ist **$\mathbf{Rang_K(M)}$** der Rang der Matrix M über dem Körper K.

Die Funktion $\mathbf{f} : \mathbf{X} \times \mathbf{Y} \to \{\mathbf{0}, \mathbf{1}\}$ sei gegeben.

(a) Für jeden Körper K gilt

$$\mathbf{D}(\mathbf{f}) \geqslant \lceil \log_2 \mathrm{Rang}_{\mathbf{K}}(\mathbf{M_f}) \rceil.$$

(b) Es gilt $\mathbf{D}^{\mathbf{A} \to \mathbf{B}}(\mathbf{f}) \leqslant \mathrm{Rang}_{\mathbb{Z}_2}(\mathbf{M_f})$.

(a) Ein deterministisches Protokoll $\mathcal{P}$ für $\mathbf{f}$ kommuniziere s Bits.
- $\mathcal{P}$ zerlegt die Kommunikationsmatrix in höchstens 2^s Teilmatrizen T mit nur monochromatischen Zeilen oder nur monochromatischen Spalten.
- $\mathcal{P}$ zerlegt die Kommunikationsmatrix in $\leqslant 2^s$ Teilmatrizen T vom Rang 1.

(b) Es gelte $\mathrm{Rang}_{\mathbb{Z}_2}(\mathbf{M_f}) = R$.
- **Alice** und **Bob** einigen sich auf R unabhängige Zeilen $z_1, \ldots, z_R$.
- **Alice** kommuniziert die Linearkombination α aus $x = \oplus_{i=1}^{R} \alpha_i z_i$ für Eingabe x.
- **Bob** kann x jetzt rekonstruieren und bestimmt $f(x, y)$.

Die Rangmethode (2/2)

Die Funktion $\mathbf{f} : \mathbf{X} \times \mathbf{Y} \to \{\mathbf{0}, \mathbf{1}\}$ sei gegeben.

- Wir zeigen später: Wenn F ein Fooling-Set für $\mathbf{f}$ ist, dann folgt

$$\sqrt{|\mathbf{F}|} - \mathbf{1} \leqslant \mathrm{Rang}_{\mathbf{K}}(\mathbf{M_f}).$$

  - Die Rangmethode liefert also immer „fast“ mindestens so gute Resultate wie die (allerdings einfacher anzuwendende) Methode der Fooling-Sets.
- Betrachte das **innere Produkt $\langle , \rangle_{\mathbf{2},\mathbf{n}}$ modulo zwei**.
  - Es ist $\mathrm{Rang}_{\mathbb{Z}_2}(\langle , \rangle_{2,n}) = n$.
    - Bei ungeschickter Wahl des Grundkörpers kann die Rangmethode „versagen“.
  - Es gibt nur Fooling-Sets der Größe $(n+1)^2$, obwohl $\mathrm{Rang}_{\mathbb{Q}}(\langle , \rangle_{2,n}) = 2^n - 1$.
    - Die Rangmethode kann exponentiell bessere untere Schranken als die Methode der Fooling-Sets liefern.

Die Rang-Vermutung

Gibt es $\varepsilon > 0$, so dass

$$D(f) = \Omega(\log_2(\mathrm{Rang}_{\mathbb{Q}}(f)))^{\varepsilon}$$

für jede Boolesche Funktion f gilt?

Nichtdeterministische Kommunikation

Nichtdeterministische Kommunikation

$\mathbf{f} : \mathbf{X} \times \mathbf{Y} \to \{\mathbf{0}, \mathbf{1}\}$ sei gegeben.

- Ein **nichtdeterministisches Protokoll $\mathcal{N}$ für f**
  - besitzt für jede Eingabe (x, y) mit $f(x, y) = 1$ eine „akzeptierende“ Berechnung, also eine Berechnung mit Ausgabe 1.
  - Alle Berechnungen für Eingaben (x, y) mit $f(x, y) = 0$ enden mit Ausgabe 0.
- $\mathcal{N}$ **kommuniziert höchstens s Bits**, wenn jede Berechnung auf jeder Eingabe höchstens s Bits kommuniziert.

Es ist

$$N(f) = \min\{s \mid \text{es gibt ein nichtdeterministisches Protokoll für } f, \text{ das höchstens } s \text{ Bits kommuniziert.}\}$$

Definiere $N^{A \to B}(f)$ und $N^{B \to A}(f)$ wie im Fall der deterministischen Kommunikation für einseitige Protokolle.

Einseitige Kommunikation

Für jede Funktion **f** gilt

$$\mathbf{N}(\mathbf{f}) = \mathbf{N}^{\mathbf{A}\to\mathbf{B}}(\mathbf{f}).$$

- Wir simulieren ein beliebiges nichtdeterministisches Protokoll $\mathcal{P}$ durch ein einseitiges nichtdeterministisches Protokoll.
  - **Alice** rät einen vollständigen Dialog, der mit ihrer Eingabe konsistent ist und kommuniziert den geratenen Dialog in einer einzigen Nachricht N.
  - **Bob** bricht N in die Einzelnachrichten $N_1, \ldots, N_k$ der jeweiligen Spieler auf und überprüft die Korrektheit des Dialogs von seiner Perspektive.
  - Geht die Überprüfung positiv aus, akzeptiert oder verwirft **Bob** wie von Protokoll $\mathcal{P}$ vorgeschrieben.
- Die Kommunikation des einseitigen Protokolls steigt nicht an.

Ungleichheit

Betrachten das Komplement $\overline{\mathrm{EQ}_n}$ des Gleichheitsproblems:

$$\overline{\mathrm{EQ}_n}(x_1, \ldots, x_n, y_1, \ldots, y_n) = \begin{cases} 1 & x_i \neq y_i \text{ für mindestens eine Position } i, \\ 0 & \text{sonst.} \end{cases}$$

- Da $F = \{(x, x) \mid x \in \{0, 1\}^n\}$ ein Fooling-Set der Größe 2^n für $\overline{\mathrm{EQ}_n}$ ist, folgt $D(\overline{\mathrm{EQ}_n}) = n$ für die deterministische Kommunikationskomplexität.
- Wie groß ist die nichtdeterministische Kommunikationskomplexität von $\overline{\mathrm{EQ}_n}$?
  - **Alice** rät eine Bitposition $i \in \{1, \ldots, n\}$ und kommuniziert die Binärdarstellung von $i - 1$ sowie das Bit x_i.
  - **Bob** akzeptiert genau dann, wenn sein i-tes Bit y_i von x_i verschieden ist.

$\mathbf{N(\overline{\mathrm{EQ}_n}) \leqslant \lceil \log_2 n \rceil + 1}$, aber $\mathbf{D(\overline{\mathrm{EQ}_n}) = n}$.

Kommunikationsspiele

Kommunikationsspiele

Das Kommunikationsspiel **Spiel**$(\mathbf{f})$ für die Funktion $\mathbf{f} : \{\mathbf{0}, \mathbf{1}\}^{\mathbf{n}} \to \{\mathbf{0}, \mathbf{1}\}$.

- **Alice** erhält eine Eingabe x mit $\mathbf{f}(\mathbf{x}) = \mathbf{1}$ und
  Bob eine Eingabe y mit $\mathbf{f}(\mathbf{y}) = \mathbf{0}$.
- Beide Spieler kommunizieren, um sich auf (irgend)eine Position i mit $x_i \neq y_i$ zu einigen. (Eine solche Position muss existieren, denn $x \neq y$ gilt.)
  - Die berechnete Position muss beiden Spielern bekannt sein.
  - Die minimale Anzahl kommunizierter Bits bezeichnen wir mit
    $$\mathbf{C}(\mathrm{Spiel}(\mathbf{f})).$$
- Wir betrachten nur deterministische Protokolle.
  - Nichtdeterministische Protokolle sind zu mächtig, da stets $\lceil \log_2 n \rceil$ Bits ausreichen.

Die Tiefe von Schaltkreisen (1/3)

Die Funktion $\mathbf{f} : \{\mathbf{0}, \mathbf{1}\}^{\mathbf{n}} \to \{\mathbf{0}, \mathbf{1}\}$ sei gegeben. Dann gilt

$$\mathbf{C}(\text{Spiel}(\mathbf{f})) = \text{DEPTH}(\mathbf{f}).$$

Schaltkreis S berechne f in Tiefe t (S habe Negationsgatter nur an den Quellen). Konstruiere, durch Induktion über t, ein Protokoll für $\text{Spiel}(f)$, das $\leqslant t$ Bits austauscht.

- $t = 0$. Es ist entweder $f(z) = z_i$ oder $f(z) = \neg z_i \;\Rightarrow\;$ Ohne zu kommunizieren können sich **Alice** und **Bob** auf die Position i einigen.
- Induktionsschritt:
  - Annahme: Das Ausgabegatter f von S ist ein UND-Gatter mit $\mathbf{f} = \mathbf{f_0} \wedge \mathbf{f_1}$.
    - Nach Induktionsannahme ist $\mathbf{C}(\text{Spiel}(\mathbf{f_0})), \mathbf{C}(\text{Spiel}(\mathbf{f_1})) \leqslant \mathbf{t} - \mathbf{1}$.
    - **Alice** hat Eingabe $\mathbf{x}$ mit $\mathbf{f}(\mathbf{x}) = \mathbf{1}$ und **Bob** hat Eingabe $\mathbf{y}$ mit $\mathbf{f}(\mathbf{y}) = \mathbf{0}$: Es ist $f_0(y) = 0$ oder $f_1(y) = 0$, während natürlich $f_0(x) = f_1(x) = 1$ gilt.
    - **Bob** beginnt die Kommunikation und sendet das Bit b für das $f_b(y) = 0$ gilt.
    - **Alice** und **Bob** wissen, dass $f_b(x) = 1$ und $f_b(y) = 0$ gilt: Nach Induktionsannahme gilt $\mathbf{C}(\text{Spiel}(\mathbf{f_b})) \leqslant \mathbf{t} - \mathbf{1}$, und wir haben $\mathbf{C}(\text{Spiel}(\mathbf{f})) \leqslant \mathbf{t}$ nachgewiesen. ✓
  - Annahme: Das Ausgabegatter f von S ist ein ODER-Gatter mit $\mathbf{f} = \mathbf{f_0} \vee \mathbf{f_1}$.
    - **Alice** übernimmt die Initiative und kommuniziert das Bit b mit $f_b(x) = 1$. Beide wissen jetzt $f_b(x) = 1$ und $f_b(y) = 0$: Wende Induktion auf f_b an. ✓

Die Tiefe von Schaltkreisen (2/3)

- **Wir wissen**: $\mathbf{C}(\mathrm{Spiel}(\mathbf{f})) \leqslant \mathrm{DEPTH}(\mathbf{f})$.
- **Das Spiel für A und B**: Für disjunkte Teilmengen $A, B \subseteq \{0, 1\}^n$ erhält **Alice** $x \in A$ und **Bob** $y \in B$. Beide bestimmen eine Position i mit $x_i \neq y_i$.

  Wir zeigen: Wenn t Bits im Spiel für A und B reichen, dann gibt es einen Schaltkreis S der Tiefe $\leqslant t$ mit $S(x) = 1$ für $x \in A$ und $S(y) = 0$ für $y \in B$.

Wir konstruieren den Schaltkreis S durch Induktion über t.

$\mathbf{t = 0}$. Für die Antwort i –ohne jegliche Kommunikation– ist ($x_i = 1$ und $y_i = 0$) oder ($x_i = 0$ und $y_i = 1$) für alle $x \in A, y \in B$:   Wähle $S = x_i$ oder $S = \neg x_i$.

- Annahme: **Alice** beginnt die Kommunikation.
  - Für jedes x aus der Teilmenge $A_0 \subseteq A$ möge Alice das Bit 0 und für jedes x aus der Teilmenge $A_1 \subseteq A$ das Bit 1 senden.
  - Wende die Induktionsannahme auf A_0 und B wie auch auf A_1 und B an.
    - Schaltkreise S_0 und S_1 der Tiefe $\leqslant t - 1$ trennen A_0 und B, bzw. A_1 und B.
    - Es ist $S_b(x) = 1$ und $S_b(y) = 0$ für alle $x \in A_b$ und $y \in B$.
    - Der Schaltkreis $S = S_0 \vee S_1$ (mit Tiefe $\leqslant t$) trennt $A = A_0 \cup A_1$ und B.
- Annahme: **Bob** beginnt die Kommunikation. Was ist zu tun?

Die Tiefe von Schaltkreisen (3/3)

- Für Boolesche Funktionen $f \in \mathrm{NP}$ sind nur untere Schranken der Form
$$\mathrm{DEPTH}(f) = \Omega(\log_2 n)$$
bekannt.
- Die Angabe besserer unterer Schranken für das Kommunikationsspiel wäre eine Revolution.
  - Die Charakterisierung der Tiefe von Schaltkreisen durch die Kommunikation ist ein wichtiger konzeptioneller Beitrag.
  - Der Zusammenhang zur Tiefe ist aber zu eng: Mit heutigen Methoden kann das Kommunikationsspiel nicht erfolgreich analysiert werden.
- War's dann schon alles?
  - Natürlich nicht, denn wir werden die Tiefe **monotoner Schaltkreise** erfolgreich analysieren können.
  - Für allgemeine Schaltkreise erhalten wir die untere Schranke $\geqslant 2\log_2 n$ für das Kommunikationsspiel und damit für die Tiefe von Schaltkreisen.