Über die Multiparty-Kommunikationskomplexität regulärer Sprachen

Pavel Pudlak
Mathematical Institute, Academy of Sciences of the Czech Republic
e-mail: pudlak@math.cas.cz

Klaus Reinhardt
Institut für Informatik, University of Tübingen
e-mail: reinhard@informatik.uni-tuebingen.de

und

Pascal Tesson und Denis Thérien
School of Computer Science, McGill University
e-mail: {ptesso, denis}@cs.mcgill.ca

KURZFASSUNG

Gemäss dem algebraischen Ansatz von [4] untersuchen wir die Kommunikationskomplexität aperiodischer Monoide im Multiparty-model von Chandra, Furst und Lipton. Wir stellen eine Vermutung vor, die die aperiodischen Monoide, die beschränkte Kommunikationskomplexität haben, charakterisieren würde und zeigen verschiedene Ergebnisse in dieser Richtung.

1. Einleitung

1.1. Kommunikationskomplexität

Wir betrachten Kommunikationsspiele mit k-Spielern (siehe [2]), bei denen n Eingabevariablen in k Mengen $[n] = X_1 \dot{\cup} \ldots \dot{\cup} X_k$ unterteilt sind, wobei der Spieler P_i Zugang zu allen Variablen ausser denen in X_i hat.

Seien A und B endliche Mengen. Ziel der Spieler ist es, gemeinsam eine Funktion $f : A^n \to B$ zu berechnen, wobei es ihnen erlaubt ist, Bits nach einem bestimmten Protokoll an eine Tafel zu schreiben, die für jeden Spieler sichtbar ist. Das Protokoll terminiert, wenn jeder Spieler den Wert von f kennt. Die *Kosten* eines Protokolles für f sind definiert durch die maximale Anzahl von Bits, die von den Spielern für eine Eingabe bei der schlechtesten Art der Verteilung zu kommunizieren ist. Die k-Spieler *Kommunikationskomplexität* $C^{(k)}(f)$ von f sind die Kosten des billigsten k-Spieler-protokolls, das f berechnet. Aus der Definition folgt unmittelbar $C^{(k)}(f) \geq C^{(k')}(f)$ für $k < k'$ und $C^{(k)}(f) \leq \frac{n}{k} + 1$.

1.2. Algebra

Für zwei endliche Monoide [1] M und N gelte $M \prec N$, falls M das homomorphe Bild eines Untermonoides von N ist. Eine Sprache $L \subseteq X^*$ wird durch M erkannt, wenn ein Morphismus $\phi : X^* \to M$ existiert mit $L = \phi^{-1}(F)$ für eine Teilmenge $F \subseteq M$. Eine Sprache L ist regulär, wenn sie durch ein endliches M erkannt werden kann.

[1] Assoziative Halbgruppen mit neutralem Element, siehe [1], [3]

Für eine reguläre Sprache $L \subseteq X^*$ und ein Wort x definieren wir die Menge $Y_x = \{(u, v) : uxv \in L\}$. Durch $x \sim_L y$ genau dann wenn $Y_x = Y_y$ erhalten wir eine Kongruenz mit endlichem Index. Das syntaktische Monoid $X^*/\sim_L$ von L bezeichnen wir als $M(L)$. Dieses Monoid $M(L)$ erkennt L und für alle N, die ebenfalls L erkennen, gilt $M(L) \prec N$.

Die k-Spieler Kommunikationskomplexität $C^{(k)}(M)$ von M ist die maximale Komplexität einer regulären Sprache, die von M erkannt werden kann. Es wurde in [4] gezeigt, dass dies bis auf einen konstanten Faktor der Komplexität, ein Produkt von Elementen in M auszuwerten, entspricht. Ferner gilt $C^{(k)}(M) = \Theta(C^{(k)}(L))$ für alle L mit $M(L) = M$ vorausgesetzt L hat einen neutralen Buchstaben.

DA ist die Menge der Monoide mit $(xyz)^t y (xyz)^t = (xyz)^t$, für ein $t \geq 0$. **DA** hat viele nützliche Charakterisierungen und steht im Zentrum vieler Ergebnisse über Komplexitätsfragen über aperiodische Monoide. Insbesondere benützen wir die Eigenschaft, dass ein aperiodisches Monoid M genau dann ausserhalb von **DA** liegt, wenn es entweder von BA_2, dem syntaktischen Monoid der regulären Sprache $(ab)^*$, oder von U, dem syntaktischen Monoid von A^*aaA^* geteilt wird.

Sei A ein endliches Alphabet und, für $t \in \mathbb{N}$ und $x \in A^*$ sei $\alpha_t(x)$ die Anzahl der Vorkommen jedes Buchstaben von A im Wort x bis zum Schwellenwert t. Wir definieren induktiv über k eine Familie von Äquivalenzrelationen $\approx_{k,t}$ auf A^* für $k, t \in \mathbb{N}$. Es gilt $x \approx_{0,t} y$ für alle $x, y \in A^*$ und alle t. Rekursiv definieren wir $x \approx_{k,t} y$ genau dann wenn

1. $x \approx_{k-1,t} y$
2. $\alpha_t(x) = \alpha_t(y)$
3. Für alle $x = x_0 a x_1$ und $y = y_0 a y_1$ mit $|x_0|_a = |y_0|_a \leq t$, gilt $x_0 \approx_{k-1,t} y_0$ und $x_1 \approx_{k-1,t} y_1$
4. Für alle $x = x_0 a x_1$ und $y = y_0 a y_1$ mit $|x_1|_a = |y_1|_a \leq t$, gilt $x_0 \approx_{k-1,t} y_0$ und $x_1 \approx_{k-1,t} y_1$

Für alle k, t ist das endliche Monoid $A^*/\approx_{k,t}$ aperiodisch für alle k, t und liefert eine Parametrisierung von **DA**:

Lemma *Sei $M = A^*/\gamma$, mit $|A| = n$ so ist $M \in$ **DA** ganau dann wenn $\approx_{k,t} \subseteq \gamma$ für ein Paar k, t.*

Es sei $\mathbf{W_k}$ die Menge der Monoide $M = A^*/\gamma$ mit $\approx_{k,t} \subseteq \gamma$ für ein t.

2. Einige Schranken der Multiparty-Kommunikationskomplexität von Monoiden

Es wurde in [4] gezeigt, dass eine Gruppe G genau dann konstante k-Spieler Kommunikationskomplexität ($k \geq 2$) hat wenn sie nilpotent der Klasse $(k-1)$ ist, andernfalls hat sie lineare Komplexität.

Vermutung: Ein aperiodisches Monoid M hat konstante k-Spieler Kommunikationskomplexität genau dann wenn es zu $\mathbf{W_{k-1}}$ gehört.

Die "wenn"-Richtung können wir durch Konstruktion eines Protokolles zeigen, bei welchem die Spieler feststellen, welche Spieler die ersten bzw. letzten t a's haben und und jeweils rekursiv mit einem Spieler weniger die Relation $\approx_{k-1,t}$ prüfen. Ein Zählen (bis t) ist bereits mit zwei Spielern möglich.

In der umgekehrten Richtung haben wir nur Teilergebnisse. Wir zeigen zunächst, dass ein Monoid, das nicht zu $\bigcup_k \mathbf{W_k} = \mathbf{DA}$ gehört, keine konstante k-Spieler Kommunikationskomplexität für irgend ein k besitzt, was ein offenes Problem in [4] löst. Nach obiger Bemerkung genügt es, untere Schranken für BA_2 und für U zu zeigen.

Theorem *$C^{(k)}(BA_2)$ is nicht konstant für jedes k.*

Es gilt $C^{(k)}(U) \in \omega(\log n)$ laut [4]. Die Vermutung in [4] dass alle aperiodischen Monoide, die nicht zu $\mathbf{DA}$ gehören, lineare Kommunikationskomplexität hätten, widerlegen wir wie folgt:

Theorem *Die Sprache $(ab)^*$ kann durch 4 Spieler mit $O(\sqrt{n}\log(n))$ Kommunikationsbits und durch 5 Spieler mit $O(\log(n))$ Kommunikationsbits erkannt werden.*

2.1. Der 3-Spieler-Fall

Unsere Vermutung ist trivial für $k = 1$. Für $k = 2$, wissen wir aus [4, 5] dass aperiodische Monoide genau dann konstante 2-Kommunikationskomplexität besitzen, wenn sie kommutativ sind, was der Definition von $\mathbf{W_1}$ entspricht. Wir können die Vermutung auch für $k = 3$ zeigen.

Lemma *Ein Monoid M gehört zu $\mathbf{W_2}$ genau dann wenn ein t existiert so dass für alle $x, y, z \in M$ sowohl $x^{t+1} = x^t$ als auch $x^t y x^t z x^t = x^t y z x^t$ gilt.*

Sei $f : \{0,1\}^n \times \{0,1\}^{\log n} \times \{0,1\}^{\log n} \to \{0,1\}$ definiert durch $f(\alpha, \beta, \gamma) = 1$ genau dann wenn $\beta < \gamma$ und in dem n-Bit Wort α die Bits $\alpha_\beta, \alpha_{\beta+1}, \ldots, \alpha_\gamma$ alle gleich 0 sind.

Theorem $C^{(3)}(f) = \omega(1)$

Folgerung: Ein aperiodisches Monoid M hat konstante 3-Spieler Kommunikationskomplexität genau dann wenn es zu $\mathbf{W_2}$ gehört.

Vermutungung: Für alle k gilt: Die reguläre Sprache $A^*a_1A^*a_2 \ldots A^*a_kA^*$, mit $A = \{a_1, \ldots, a_k\}$ hat nicht-konstante k-Spieler ommunikationskomplexität.

Literatur

[1] S. Eilenberg. *Automata, Languages and Machines*, volume B. Academic Press, 1976.

[2] E. Kushilevitz and N. Nisan. *Communication Complexity.* Cambridge University Press, 1997.

[3] J.-E. Pin. *Varieties of formal languages.* North Oxford Academic Publishers Ltd, London, 1986.

[4] J.-F. Raymond, P. Tesson, and D. Thérien. An algebraic approach to communication complexity. *Lecture Notes in Computer Science*, 1443:29–40, 1998.

[5] M. Szegedy. Functions with bounded symmetric communication complexity, programs over commutative monoids, and ACC. *J. Comput. Syst. Sci.*, 47(3):405–423, 1993.