Characterization of circuit size in terms of PLS problems and communication complexity

Rocio Xicohténcatl Reza

Recall: Karchmer-Wigderson game

- Let U, V, I be finite sets, and $R \subseteq U \times V \times I$ be a ternary relation such that:

$$\forall u \in U \; \forall v \in V \; \exists i \in I \; \big((u, v, i) \in R\big)$$

- KW-protocol: a finite binary tree T that represents the exchange bits of information

- The communication complexity of R (CC(R)) is the minimum height of a KW-protocol tree that computes R

Local search problems

- Definition

A *local search problem* L consist of a set $F_L(x) \subseteq \boldsymbol{N}$ of solutions for every instance $x \in \boldsymbol{N}$, an integer-valued *cost function* $c_L(s, x)$ and a *neighborhood function* $N_L(s, x)$ such that:

i) $0 \in F_L(x);$

ii) $\forall s \in F_L(x), N_L(s, x) \in F_L(x);$

iii) $\forall s \in F_L(x),$ if $N_L(s, x) \neq s \ then \ c_L(s, x) < c_L(N_L(s, x))$

- Definition

A *local optimum* for the problem L on x is an s such that:

$$\mathrm{s} \in F_L(x)$$

and

$$N_L(s, x) = s$$

Polynomial Local Search problems

- Definition

A local search problem L is *polynomial*

i) if the binary predicate s $\in F_L(x)$ and the functions $c_L(s,x)$, $N_L(s,x)$ are polynomially time computable

ii) there exists a polynomial $p_L(n)$ such that

$$\forall s \in F_L(x)\ |s| \leq p_L(|x|)$$

- Considering a Karchmer-Wigderson game

- Local search problems whose instances x are (enconding s of) pairs (u, v); $u \in U, v \in V$

For any problem $L = < F_L, c_L, N_L >$

- Let $C(F_L, c_L)$ be the communication complexity of computing simultaneously the predicate s $\in F_L(u, v)$ and the function $c_L(s, u, v)$ in the model when the first player gets (s, u), and the second gets (s, v)

s is in the public domain and C(N_L) is defined similarly

- Definition

The *size* of L is:

$$\left|\bigcup_{\substack{u\in U\\ v\in V}} F_L(u,v)\right| \cdot 2^{2C(F_L,c_L)+C(N_L)}$$

- Definition

We say that R *reduces* to L if there exists a polynomial function $p\colon \boldsymbol{N} \ \rightarrow I$ such that for any $(u, v) \in U \times V$ and any local optimum s for L on (u, v), we have $\left(u, v, p(s)\right) \in R$

We define *size(R)* as

$$\min\{size(L) | \, R \ reduces \ to \ L\}$$

Theorem

a) *For every partial Boolean function* f, $size(R_f) = \theta(S(f))$

b) *For every monotone partial Boolean function* f,

$$size(R_f^{mon}) = \theta(S_{mon}(f))$$

Proof

Let:

- f be a partial Boolean function in n variables
- $t \rightleftharpoons S(f)$
- C be a size-t circuit computing f

Proof

- Denote $f^{-1}(0)\ by\ U$ and $f^{-1}(1)\ by\ V$
- We aim to reduce R_f to a local search problem L of size $O(t)$.
- Assume $t \geq n - 1$
- Arrange nodes $w_1, \dots, w_t$ of C such that a wire go from w_μ to w_ν only when $\mu < \nu$, and f_ν is the function computed at w_ν
- Encode nodes $w_1, \dots, w_t$ by integers $n_1, \dots, n_t$ so that $n_t = 0$ and $\{1, \dots, n\} \cap \{n_1, \dots, n_t\} = \emptyset$

Proof

We construct L as follows:

$$F_L(u,v) \rightleftharpoons \left\{i \,\middle|\, 1 \le i \le n \;\&\; u_i \ne v_i\right\} \cup \left\{n_\nu \,\middle|\, 1 \le \nu \le t \;\& f_\nu(u) = 0 \;\&\; f_\nu(v) = 1\right\}$$

$$c_L(i,u,v) \rightleftharpoons 0 \text{ for } 1 \le i \le n$$

$$N_L(i,u,v) \rightleftharpoons i \text{ for } 1 \le i \le n$$

$$c_L(n_\nu,u,v) \rightleftharpoons \nu \text{ for } 1 \le \nu \le t$$

Proof

$$N_L(n_\nu, u, v) \rightleftharpoons 0 \qquad \text{if } n_\nu \notin F_L(u, v)$$

Otherwise, i.e. $f_\nu(u) = 0,\ f_\nu(v) = 1$

we choose one of the two sons of w_ν for which this property is preserved

If this son is a computational node w_μ

$$N_L(n_\nu, u, v) \rightleftharpoons n_\mu$$

If this son is a leaf x_i^ϵ

$$N_L(n_\nu, u, v) \rightleftharpoons i$$

Proof

Then it is easy to see that R_f $reduces\ to\ L$

And $C(F_L, c_L) \leq 2$ and $C(N_L) \leq 3$

Hence,

$$size(L) \leq O(n+t)$$

And $t \geq n-1$

$$size(L) \leq O(t)$$

For another non-trivial direction:

- Assume that R_L reduces via a function p to a local search problem L

Let

$$h_0 \rightleftharpoons 2^{C(F_L, c_L)}$$

$$h_1 \rightleftharpoons 2^{C(N_L)}$$

- For every fixed $s \in \bigcup_{\substack{u \in U \\ v \in V}} F_L(u, v)$

We have:

$$P_s \text{ for computing } s \in F_L(u, v)$$
$$c_L(s, u, v) \text{ with at most } h_0 \text{ different histories}$$

- h_0 defines a partition of $U \times V$:

$$U_{s,1} \times V_{s,1}; \dots; U_{s,h_0} \times V_{s,h_0}$$

Such that F_L, c_L are fully determined on $U_{s,i} \times V_{s,i}$

That is, for some predicates $\alpha_s \subseteq [h_0]$ and some η_s: $[h_0] \rightarrow \boldsymbol{N}$, for all $i \in [h_0]$ and for all $(u, v) \in U_{s,i} \times V_{s,i}$:

$$s \in F_L(u, v) \text{ iff } i \in \alpha_s$$

$$c_L(s, u, v) = \eta_s(i)$$

"*good*" rectangle $U_{s,i} \times V_{s,i}$

$$i \in \alpha_s$$

Cost of rectangle $U_{s,i} \times V_{s,i}$

$$\eta_s(i)$$

We order good rectangles, so their costs are non-decreasing:

$$U^1 \times V^1; \dots; U^{H_0} \times V^{H_0}$$

Where $H_0 \leq \left| \bigcup_{\substack{u \in U \\ v \in V}} F_L(u, v) \right| \cdot h_0$

- Construct by induction on $\nu \leq H_0$ a circuit C_ν:

For every $\mu \leq \nu$ there exists a node ω_μ of C_ν computing f_μ such that:

$$f_\mu|_{U^\mu} \equiv 0, \qquad f_\mu|_{V^\mu} \equiv 1$$

Assume we already have $C_{\nu-1}$,

C_ν will be obtained by adding at most $h_0 h_1$ new nodes for computing f_ν with required properties from $f_1, \dots, f_{\nu-1}$

- Let

$$U^{\nu} \times V^{\nu} = U_{s,i} \times V_{s,i}$$

Consider the protocol P_s^* of complexity at most $C(F_L, c_L) + C(N_L)$

We run the optimal protocol for computing $N_L(s, u, v)$

$$s' \rightleftharpoons N_L(s, u, v)$$

Then we run $P_{s'}$

- $y_1, \dots, y_H$ for those histories of P_s^* which correspond to at least one instance $(u, v) \in U_{s,i} \times V_{s,i}$

- For every $u \in U_{s,i}$ let $\bar{u}$ be the assignment on $\{0,1\}^H$

$\bar{u}_h = 0$ if there exists $v \in V_{s,i}$ such that P_s^* develops according to h
$\bar{u}_h = 1$ otherwise

$\bar{v}_h = 1$ iff there exists $u \in U_{s,i}$ such that P_s^* develops according to h

- So for every pair $(u, v) \in U_{s,i} \times V_{s,i}$ we have

$$\bar{u}_h = 0\,,\, \bar{v}_h = 1$$

Hence, the partial Boolean function

$$\hat{f}_v(y_1, \dots, y_H) = 0 \text{ on } \{\bar{u}_h | u \in U_{s,i}\}$$
$$\hat{f}_v(y_1, \dots, y_H) = 1 \text{ on } \{\bar{v}_h | v \in V_{s,i}\}$$
$$\text{undefined elsewhere}$$

is *monotone* and the protocol P_s^* finds a solution to $R_{\hat{f}_v}^{mon}$

- (Recall) Let

$$U^{\nu} \times V^{\nu} = U_{s,i} \times V_{s,i}$$

Consider the protocol P_s^* of complexity at most $C(F_L, c_L) + C(N_L)$

We run the optimal protocol for computing $N_L(s, u, v)$

$$s' \rightleftharpoons N_L(s, u, v)$$

Then we run $P_{s'}$

- By proposition (from KW game):

  $For\ every\ (partial)\ monotone\ Boolean\ function\ f,$
  $C\left(R_f^{mon}\right) = D_{mon}(f)$

$$D_{mon}\left(\hat{f}_\nu\right) \leq C(F_L, c_L) + C(N_L)$$

And the same bound holds for some total monotone extension $\bar{f}_\nu$

Note that this implies:

$$S_{mon}\left(\bar{f}_\nu\right) \leq h_0 h_1$$

- Consider a particular h of P_s^*
- Let (s', j) be the corresponding subprotocol $P_{s'}$

- By LS definition, ii)

$$\forall s \in F_L(x), N_L(s,x) \in F_L(x)$$

Rectangle $U_{s,i} \times V_{s,i}$ is good

- By part iii)

$$\forall s \in F_L(x), \text{if } N_L(s,x) \neq s \; then \; c_L(s,x) < c_L(N_L(s,x))$$

either $s' = s$ or $c(U_{s',j} \times V_{s',j}) < c(U_{s,i} \times V_{s,i})$

- If $s' = s$

- s is a local optimum for L on every $(u, v) \in U_{s,i} \times V_{s,i}$
- Since R_f reduces to L, this means that $u_{p(s)} \neq v_{p(s)}$
- Implying actually that $u_{p(s)} = \epsilon, v_{p(s)} = (\neg\epsilon)$

  for some fixed $\epsilon \in \{0,1\}$
- Let $y'_h \rightleftharpoons x_{p(s)}^{(\neg\epsilon)}$

- If $cost\ of\ (U_{s',j} \times V_{s',j}) < cost\ of\ (U_{s,i} \times V_{s,i})$

$$U_{s',j} \times V_{s',j} = U^{\mu} \times V^{\mu}$$

- For some $\mu \leq \nu$
- Let $y'_h \rightleftharpoons f_{\mu}$

- Finally

- Let $f_\nu \rightleftharpoons \bar{f}_\nu(y'_h, \dots, y_H)$
- f_ν can be computed by appending at most $h_0 h_1$ nodes to $C_{\nu-1}$
- Since $\bar{f}_\nu$ is monotone and for every $u \in U^\nu$

$$\bar{f}_\nu(\bar{u}_1, \dots, \bar{u}_H) = 0$$

To check $f_\nu(u) = 0$, we only need to check, for any h

$$y'_h(u) \leq \bar{u}_h$$

To check $f_\nu(u) = 0$, we only need to check, for any h

$$y'_h(u) \leq \bar{u}_h$$

Note that if $\bar{u}_h = 0$, then for some $v \in V^\nu$ the computation on (u, v) proceeds along h

Due to our choice of y'_h, implies $y'_h(u) = 0$

By dual argument, $f_\nu(v) = 1$, for all $v \in V^\nu$

This completes the construction of C_ν

- Now

$$C_{H_0} \text{has size at most } H_0 h_0 h_1$$

- By LS problem definition i), all rectangles $U_{0,i} \times V_{0,i}$ are good
- Thus, adding at most h_0 new nodes to C_{H_0} we compute f by a circuit of size $O\big(size(L)\big)$

Sources

- A.A.Razborov, Unprovability of lower bounds on the circuit size in certain fragments of bounded arithmetic, Izvestiya RAN., 59(1) (1995), 201-224.