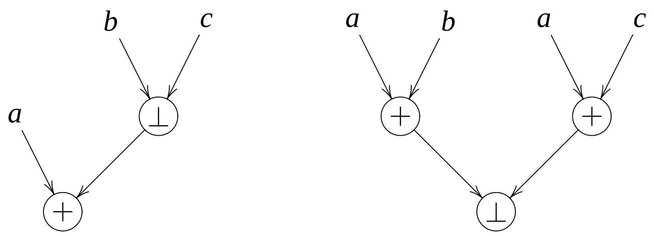

Figure 1: Application the distributivity axiom (1) from the left to the right means "moving" the $+$-gate upwards (to the inputs).

Boolean Function Complexity ADDITIONAL TOPIC

An $\Omega(n^3)$ lower bound for matrix product over semiring $(+,\min)$

S. Jukna April 21, 2012

In the *all pairs shortest path* problem (APSP problem) we are given a weighting of a complete directed graph on n vertices, and want to compute the weights of a shortest paths between all pairs of vertices. It is known (see [1, pp. 204–206] that the complexity (number of arithmetic operations) of this problem is of the same order of magnitude as the complexity of computing the product of two matrices over the semiring $(+,\min)$.

In this latter problem, we have two $n\times n$ matrices $A=(a_{ij})$ and $X=(x_{ij})$. The goal is to compute their "product" $M=AX$ where $M=(m_{ij})$ is an $n\times n$ matrix with

$$m_{ij}=\min\{a_{i1}+x_{1j},a_{i2}+x_{2j},\dots,a_{in}+x_{nj}\}\,.$$

It is clear that n^3 additions are always enough to compute M. On the other hand, Kerr (1970) showed that n^3 additions are also necessary. Since this important lower bound is not well known, we reproduce its proof.

Theorem (Kerr [2])**.** *At least n^3 $+$-gates are necessary to compute M.*

Proof. Take a minimal circuit computing M. This circuit has n^2 output gates y_{ij}. Inputs are $2n^2$ variables a_{ij} and x_{ij}. It will be convenient to denote the min-operation by:

$$x\perp y:=\min(x,y)\,.$$

A *formal polynomial* is an expression of the form $S_1\perp S_2\perp\cdots\perp S_t$ where each S_i is a sum of variables. Let E_{ij} be an expression computed at the output gate y_{ij}. Using the distributivity axiom

$$a+(b\perp c)=(a+b)\perp(a+c) \tag{1}$$

(from the left to the right) this expression can be transformed to a formal polynomial E^*_{ij}. Note that, for all settings of input variables, the expressions E_{ij} and E^*_{ij} output the same value.

The argument is roughly the following. Having an expression E_{ij} computed at the output gate y_{ij}, we transform it into an equivalent formal polynomial E^*_{ij}. Then we show that this formal polynomial must have some special form (using the fact that its values must be the same as those of M_{ij} on *all* inputs). Then we ask: how the original expression E_{ij} must have had look to get E^*_{ij} of this special form? We argue that E_{ij} must have had been the minimum of expressions of the form

$$A_{ikj} = (a_{ik} \perp F) + (x_{kj} \perp G) \tag{2}$$

where F and G are some expressions. Finally we argue that different triples (i,k,j) must have different expressions A_{ikj}. This means that the $+$-gates where the A_{ikj} are computed must be different.

Claim 1. The formal polynomial E^*_{ij} has a form

$$(a_{i1}+x_{1j}) \perp \cdots \perp (a_{in}+x_{nj}) \perp (a_{i1}+x_{1j}+F_1) \perp \cdots \perp (a_{in}+x_{nj}+F_p)$$

where each F_i is some expression. In other words, each of the terms in E^*_{ij} must contain the sum of one of the pairs of variables a_{ik} and x_{kj}, and each term $(a_{ik}+x_{kj})$ must be present in E^*_{ij}.

Proof. Suppose that some term $(\alpha+\cdots+\gamma)$ which does not contain any subterm $a_{ik}+x_{kj}$ is present in E^*_{ij}. Then setting $\alpha = \ldots = \gamma = 0$ and setting all the other variables to 1 leads to contradictory conclusion that $E_{ij} = 0$ and $M_{ij} \geq 1$ (because then $a_{ik} = 1$ or $x_{kj} = 1$).

Now assume that some sum $a_{ik}+x_{kj}$ does not appear as a term in E^*_{ij}. Setting $a_{ik} = x_{kj} = 0$ and all other variables to 1 leads to the conclusion that $M_{ij} = 0$ while $E_{ij} \geq 1$. □

Let us now examine how the terms $(a_{ik}+x_{kj})$ in E^*_{ij} could have been derived from the expression E_{ij} by application of distributivity axiom (1) from the left to the right. When going from E^*_{ij} to E_{ij} we apply this axiom from the right to the left.

Any term which can be combined with $(a_{ik}+x_{kj})$ must contain either a_{ik} or x_{kj} to provide the common factor, and the result after reducing them to a single term must be either $a_{ik}+(x_{kj} \perp F)$ or $(a_{ik} \perp G)+x_{kj}$, where F, G again represent any expressions. No matter how many times this reduction process is repeated, the resulting term must be of the form (2). We can therefore conclude that E_{ij} must have the following form: $E_{ij} = A_{i1j} \perp A_{i2j} \perp \cdots \perp A_{inj}$, where each A_{ikj} is an addition $A_{ikj} = (a_{ik} \perp F)+(x_{kj} \perp G)$. Thus, we have n^3 additions, and it remains to show that all they must be distinct.

Assume for the sake of contradiction that $A_{ikj} \equiv A_{uvw}$ (that is, coincide as functions). For this to happen A_{ikj} must have a form like $(a_{ik} \perp \alpha \perp F)+(x_{kj} \perp G)$, where α is a *single* variable other than a_{ik} or x_{kj}. Set $a_{ik} = x_{kj} = 1$, $\alpha = 0$, and set the rest of variables to 2. Then $M_{ij} = 1+1 = 2$ but $E_{ij} = 1$, which is a contradiction. □

References

[1] A. Aho, J. Hopcroft, and J. Ullman, *The Design and Analysis of Computer Algorithms*, Addison-Wesley, Reading, MA, 1974.

[2] L. R. Kerr, The effect of algebraic structure on the computation complexity of matrix multiplications, PhD Thesis, Cornell Univ., Ithaca, N.Y., 1970.