

ACC电路深度压缩新算法

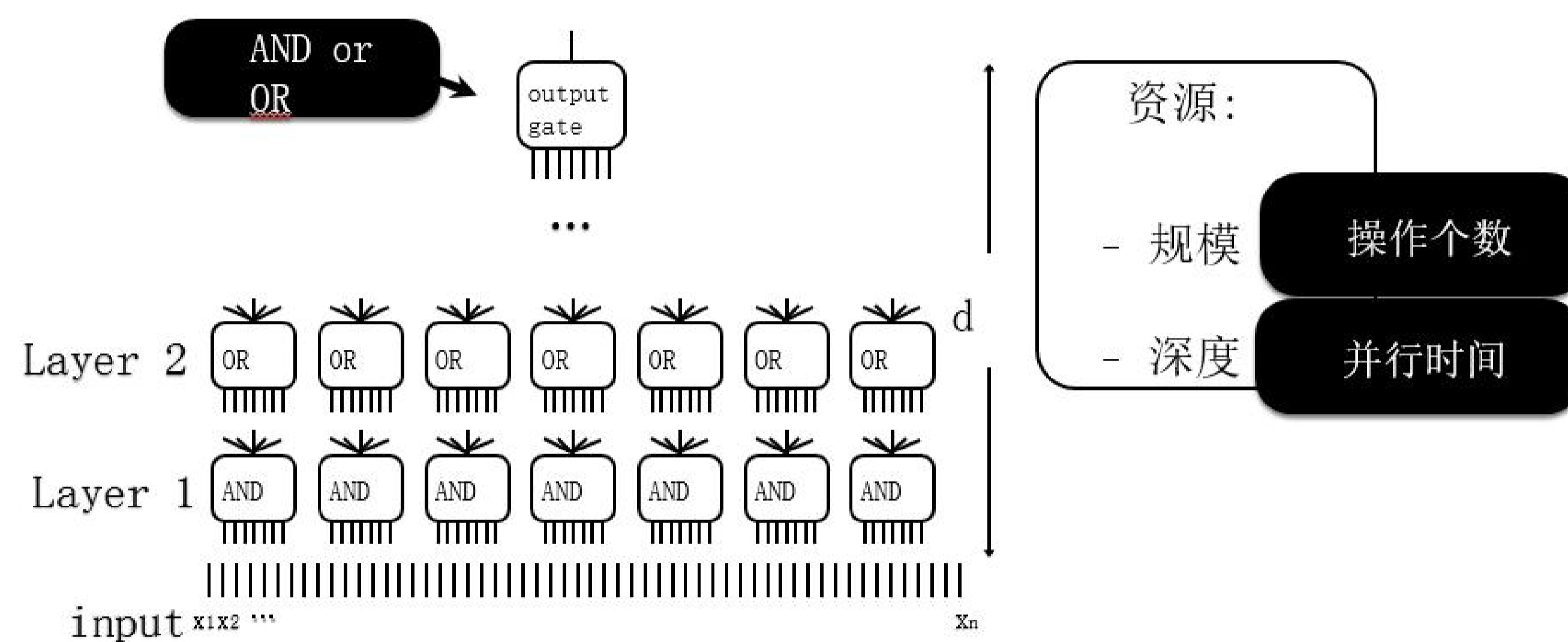
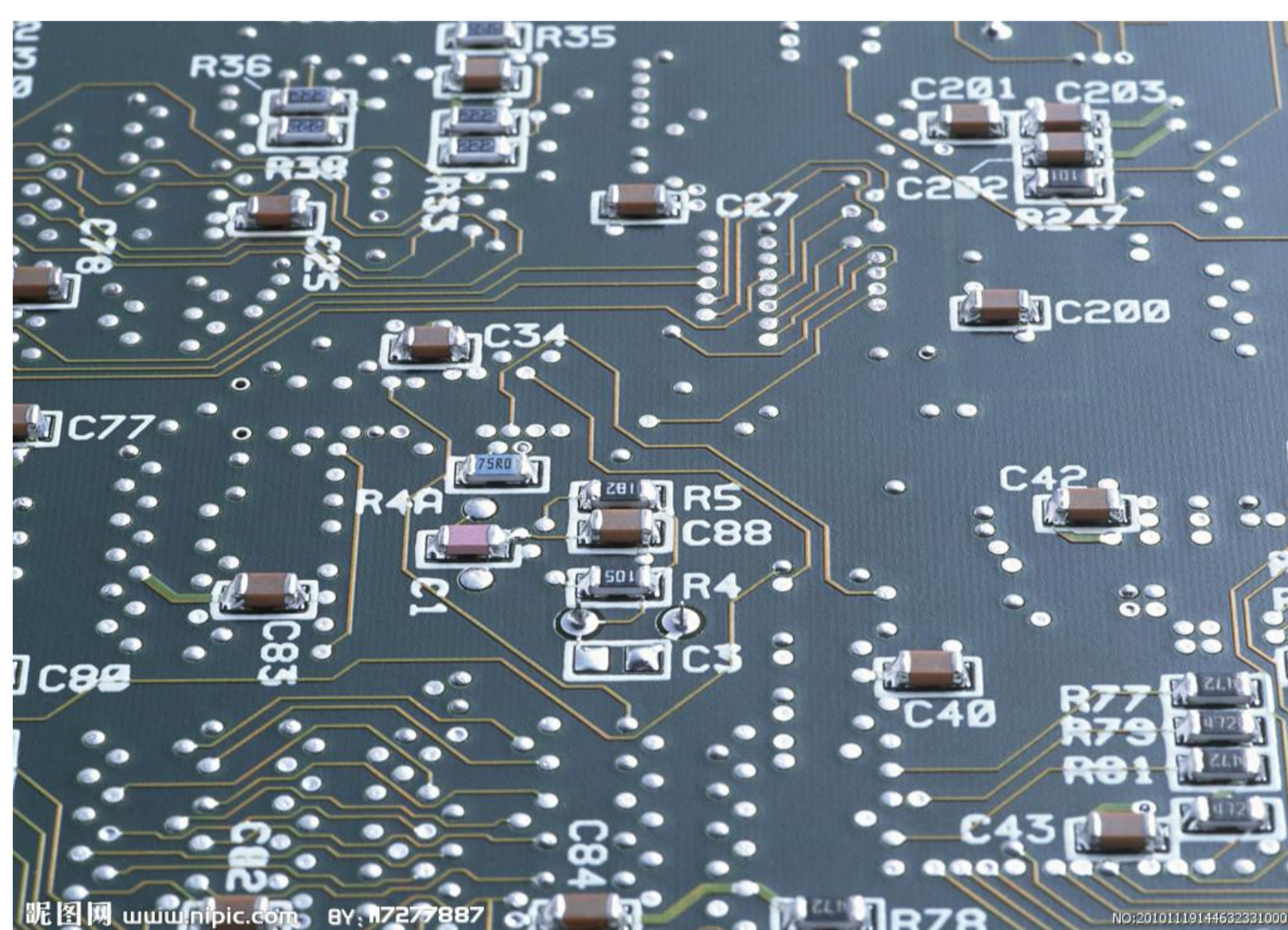
陈世腾 Periklis A. Papakonstantinou

Depth reduction for composites, FOCS 2016, invited by
SICOMP special issue for FOCS 2016

陈世腾 (chenst@ios.ac.cn)

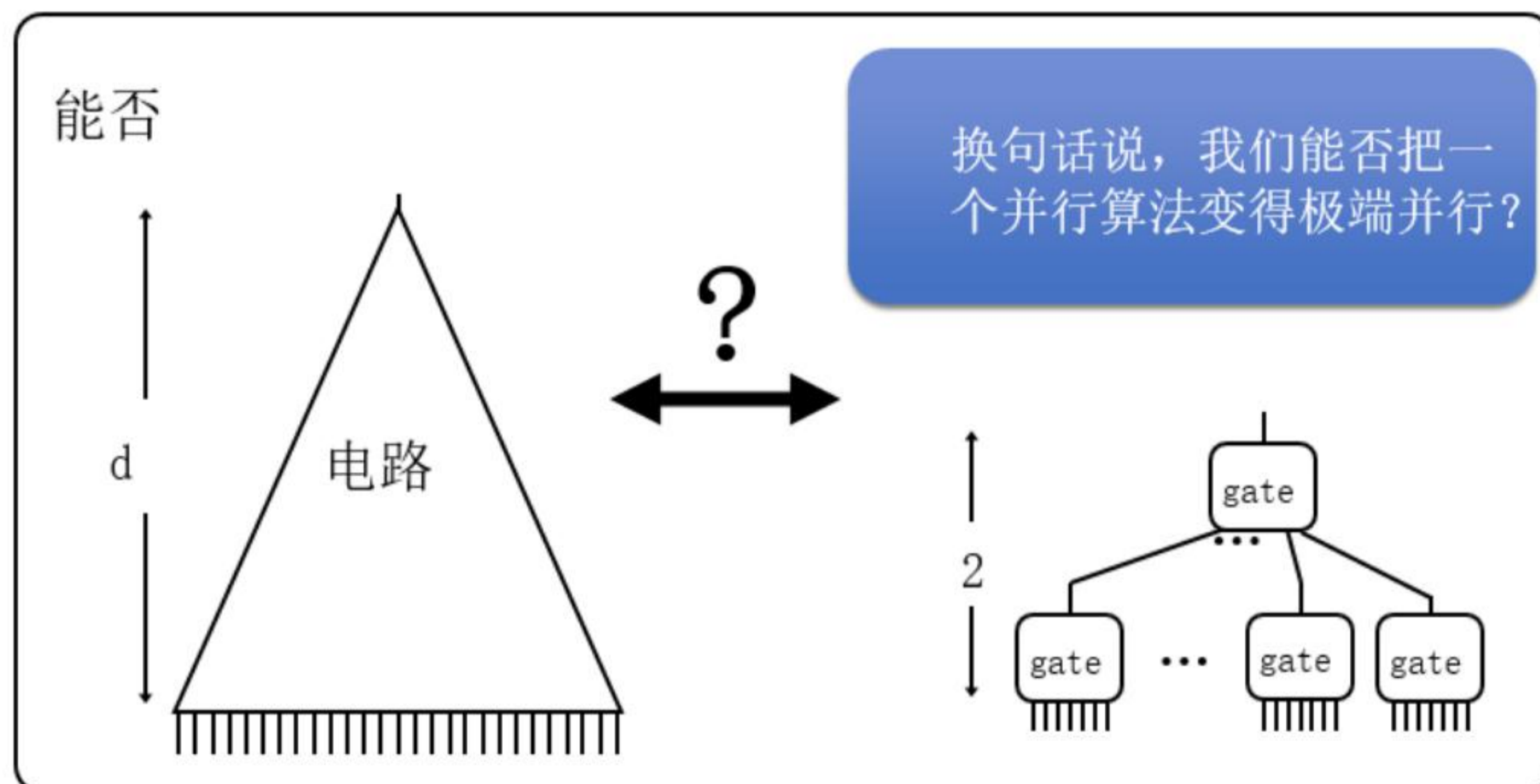
问题背景

布尔电路是从计算机的重要组成部分：数字逻辑电路中抽象出来的计算模型。电路复杂性研究的是给定的计算问题所需要的电路资源，这些资源一般包括电路的规模和电路的深度两方面。Alexander Razborov在1990年获得奈望林纳奖 (Nevanlinna Prize)，获奖成果是提出了用多项式近似布尔电路的方法，即任意常数深度的AND-OR-NOT逻辑电路都可用一个两层的XOR-AND电路近似，这就是理论计算机科学界著名的布尔电路深度压缩。



问题描述

能否将由AND OR NOT MOD m 构成的深度 d 的电路 (ACC(m)) 压缩到2层，并且不让电路规模扩大太多？这里MOD m 是判断输入的1的个数能否被 m 整除的门， m 也被称为电路的除数。



theorem [Allender-Hertrampf' 89]:

for every ACC(p) there is depth 2 circuit:
SYM-AND
of size $2^{O(d \log n)}$

素数的结果

深度压缩

指数差距

theorem [Beigel-Tarui' 91 & Yao' 90]:
for every ACC(m) there is depth 2 circuit:
SYM-AND
of size $2^{O(d \log n)^2}$

合数的结果

Open Problem:
能否缩小差距?

取得成果

对上述open problem的一个肯定的回答，完全移除了带有素数除数的电路和合数除数电路的电路深度压缩的指数级别差距，设计了一个构造性的电路深度压缩算法，利用该算法证明了新的电路复杂性下界。

作者	除数	压缩规模
Razborov, Smolensky, Allender, Hertrampf	素数	$2^{\log n^{O(d)}}$
Yao, Beigel, Tarui	合数	$2^{\log n^2 O(d)}$
我们	合数	$2^{\log n^{O(d)}}$

成果应用

并行化加速

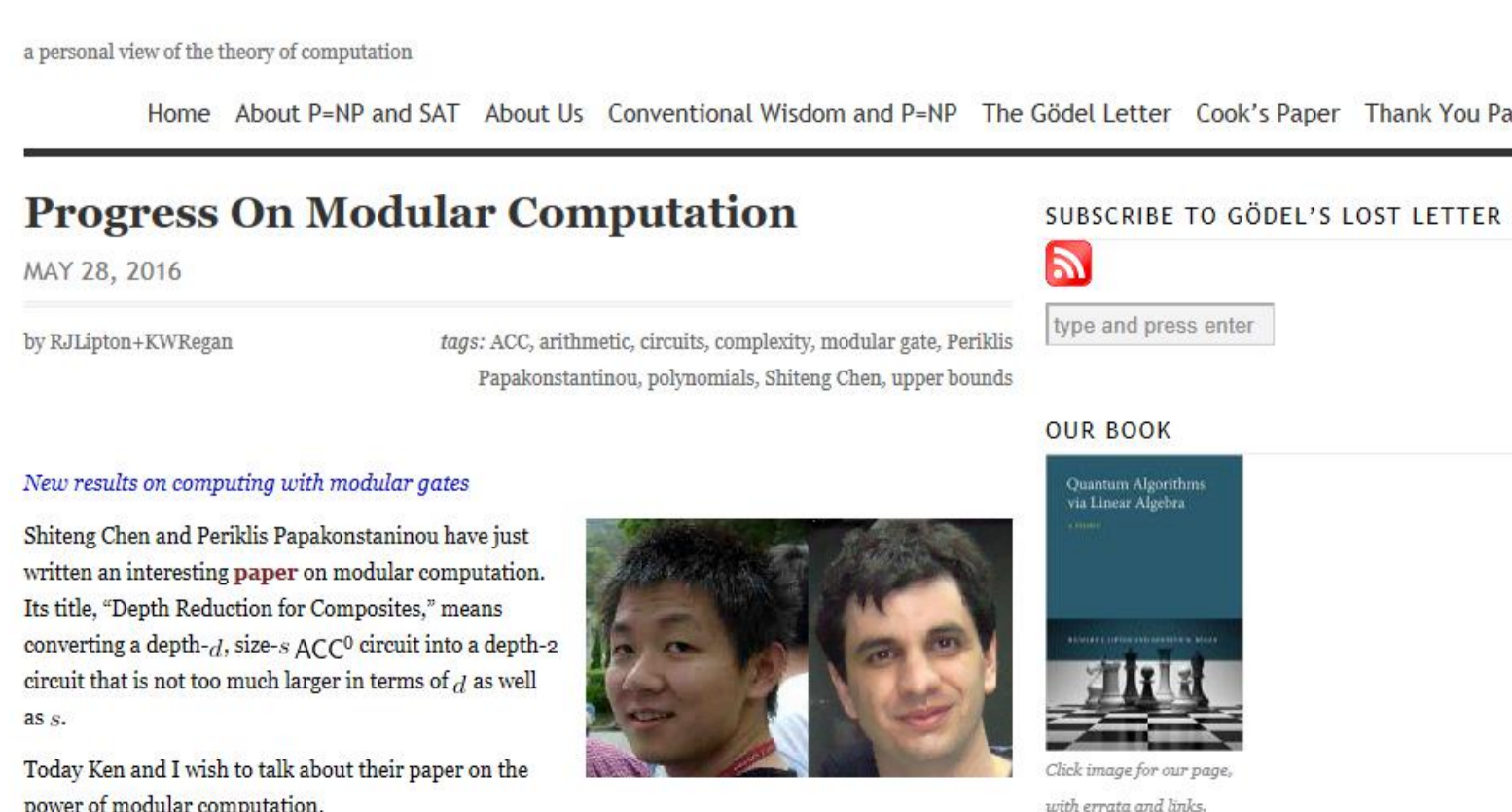
Circuit-SAT算法

NEXP问题的电路复杂性下界
NEXP问题的交互式压缩下界

....

同行评价

Gödel's Lost Letter and P=NP



★Chen and Papakonstantinou (CP) increase our understanding of modular gates by proving a general theorem about the power of low depth circuits with modular gates. This theorem is an exponential improvement over previous results when the depth is regarded as a parameter rather than constant. Their work also connects with the famous work of Ryan Williams on the relation between NEXP and ACC

—blog of Richard Lipton