计算复杂性理论

傅育熙

2023 年 12 月 4 日

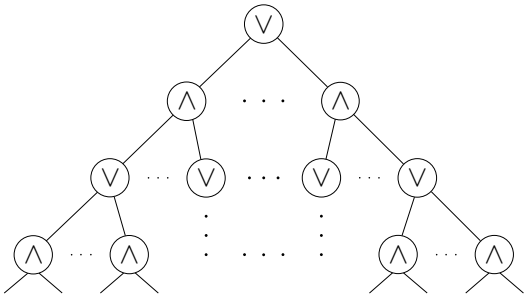
0.1 Hästad Switching Lemma

具有常数高度的电路族可能是唯一一类我们能有信心地说我们完全理解的电路族。在 $\mathbf{NC}^0$ 中的电路族有简单的刻画，也很容易看出包含关系 $\mathbf{NC}^0 \subseteq \mathbf{AC}^0$ 是严格的，见练习**??**。我们希望证明包含关系 $\mathbf{AC}^0 \subseteq \mathbf{NC}^1$ 也是严格的。例**??**中定义的奇偶函数在 $\mathbf{NC}^1$ 中，但直观上没有常数高度的电路族判定，还有很多这样的例子。上世纪八十年代，这个问题被解决了。弗斯特、萨克斯、西普塞 [89] 和阿杰泰 [8] 证明了奇偶函数 $\oplus$ 不在 $\mathbf{AC}^0$ 里。他们的证明使用了随机限制技术 [225]，证明了常数高度的计算奇偶函数的电路的大小有下界 $n^{\Omega(\log n)}$，这个下界大于任何多项式。姚期智沿用了该技术，将下界提高到了约为 $2^{n^{1/(4d)}}$，其中 d 为电路族高度 [254]。哈斯塔德简化了姚的证明并证明了很强的对换引理[108]，利用此引理，哈斯塔德给出了几乎是最优的下界 $2^{n^{1/d}}$。概率方法之外，斯摩伦斯基用代数方法证明了对换引理 [215]，拉兹博罗夫给出了一个用计数方法的简单证明 [187]。我们将介绍的就是拉兹博罗夫的证明。

Furst
Saxe
Sipser

Håstad
Switching Lemma
Smolensky
Razborov

上述所有证明的一个基本思路是利用分配律将一个高度是 $d+1$ 的交替电路（见下图）转换成高度是 d 的交替电路。图1中的上图是交换后的电路，图1中



的下图是将交换后得到的电路的第二层和第三层合并后得到的交替电路。这个简单思路的问题是转换后的交替电路可能变得太大。交替引理给出了一个证明：如果为电路的足够多的输入随机地选取一组输入，会大概率地得到一个交换后门电路个数得到控制的交替电路，这是因为若一个语句（项）中的一个字取 1（0）值，该语句（项）就消失了，一个语句（项）中的一个字取 0（1）值，该字就消失了。用归纳法我们最终得到一个两层电路。两层电路就是析取范式或合取范式，对这个电路的一部分输入确定了一组特定输入后电路的输

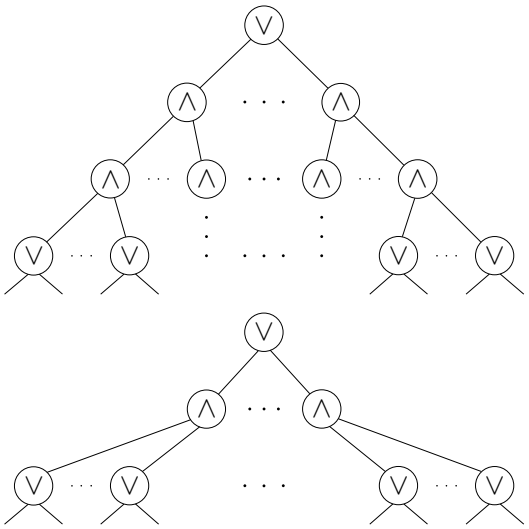


图 1　AC 电路的与或门交换

出值就确定了。这就引起矛盾，因为奇偶函数只有在所有输入值确定后输出才能确定。下面我们就解释如何兑现这一想法。

设 $X = \{x_1, \ldots, x_n\}$。若函数 $\rho : X \to X \cup \{0, 1\}$ 满足：对任意 $x \in X$ 有 $\rho(x) \in \{x, 0, 1\}$，称 ρ 为对 X 中变量的限制。若 $\rho(x) = x$，说明对变量 x 没有限制。称集合 $\{x \mid \rho(x) \neq x\}$ 为 ρ 的支集。一个限制是对 X 中部分变量的赋值，比如 $\rho = [x_1 \leftarrow 0, x_3 \leftarrow 1, x_8 \leftarrow 0]$ 将 x_1 赋值为 0，将 x_3 赋值为 1，将 x_8 赋值为 0，而对其它变量不赋值。一个限制也可看成是一个字的集合，如 $\rho = \{\overline{x_1}, x_3, \overline{x_8}\}$，也可理解成一个合取式，如 $\rho = \overline{x_1} \wedge x_3 \wedge \overline{x_8}$。

restriction

support

对于定义在 X 上的布尔函数 f，f_ρ 是定义在 $\{x \mid x \in X \wedge \rho(x) = x\}$ 上的布尔函数 $f(\rho(x_1), \ldots, \rho(x_n))$。在下面的证明中，我们需要随机地选取限制。设 $0 < n - u \leq u < n$。一个对 $X = \{x_1, \ldots, x_n\}$ 的 u-大小的随机限制 ρ 定义如下：随机地选一个大小为 u 的 X 的子集，对每个被选出的 x，通过投硬币决定其值，即

$$\rho(x) \quad = \quad \begin{cases} 1, & 1/2 \text{ 概率}, \\ 0, & 1/2 \text{ 概率}。 \end{cases}$$

对未被选出的变量 x，定义 $\rho(x) = x$. 用 R^u 表示所有对 u 个变量赋值的限

制。显然

$$|R^u| \quad = \quad \binom{n}{u} 2^u 。$$

在定义**??**中，我们引入了极小项的概念。一个 n-元布尔函数 f 可以有多个长度不等的极小项，我们用符号 $\min(f)$ 表示长度最大的极小项的长度。

引理 0.1. *设 f 为 n-元布尔函数，若 $\min(f) \leq s$，则 f 可表示为 s-析取范式。*

证明. 可以用等式 (**??**) 将 $f(x)$ 写成析取范式 $\bigvee_{f(\alpha)=1} x_\alpha$。设 f 有一个极小项 x_β。一定存在满足 $\beta \subseteq \alpha$ 的 α。使 x_β 为假的真值指派，一定使 x_α 为假，此时 $\bigvee_{f(\alpha')=1}^{\alpha' \neq \alpha} x_{\alpha'}$ 和 $f(x)$ 等价。另一方面，因为 x_β 是极小项，使 x_β 为真的真值指派，一定使 $f(x)$ 为真。结合这两方面的蕴含，得

$$f(x) \Leftrightarrow x_\beta \vee \bigvee_{f(\alpha')=1}^{\alpha' \neq \alpha} x_{\alpha'} 。$$

用归纳法即得引理结论。事实上，f 可表示成所有极小项的析取。 □

若 f 为 s-析取范式，当然有 $\min(f_\rho) \leq s$，结合引理0.1，可知集合

$$\mathrm{Bad}_f(u,s) = \{\rho \in R^u \mid \min(f_\rho) > s\}$$

就是所有使得 f_ρ 不可表示为 s-析取范式的限制 ρ。将引理0.1中的极小项换成极大项，析取范式换成合取范式，结论同样成立。拉兹博罗夫的证明方法基于下述关键引理 [187]。

引理 0.2 (拉兹博罗夫引理)**.** *若 f 是 t-合取范式，则 $|\mathrm{Bad}_f(u,s)| \leq |R^{u+s}| \cdot (4t)^s$。*

证明. 拉兹博罗夫的证明思路出奇地简单：构造从 $\mathrm{Bad}_f(u,s)$ 到 $R^{u+s} \times S$ 的编码函数 $\mathfrak{e}$ 和相应的解码函数，其中 $|S| \leq (4t)^s$。固定字的一个排序，并由此定义 f 中语句的一个序。设 $\rho \in \mathrm{Bad}_f(u,s)$，即 f_ρ 有一个长度 $s' > s$ 的极小项 τ'。去掉 τ' 中任意 $s'-s$ 个字，得到项 τ，即 τ 对这 $s'-s$ 个字不做限制。关于 f_ρ 有几点说明：

- f 中的有些语句消失了（因为取值为 1）；
- f 中的有些语句中的字消失了（因为该字的取值为 0）；

- f_ρ 不可能有语句取值为 0（因为 f_ρ 有极小项）；
- $f_{\rho\tau}$ 不可能是常量（因为 τ' 是 f_ρ 的极小项并且 τ' 的定义域严格包含 τ 的定义域）。

本证明中，我们用 $Lit(\_)$ 表示对象中字的集合，用 $Var(\_)$ 表示对象中变量的集合。设 f 为合取范式，ρ 为对 $Var(f)$ 中变量的限制。设 C_1 为第一个满足条件 $Lit(C_1)\cap Lit(\tau)\neq\emptyset$ 的 f 中的语句。用 τ_1 表示 $Var(C_1)\cap Var(\tau)$，显然 C_1 在限制 τ_1 下取值为 1。用 $\alpha_1\in\{0,1\}^t$ 表示定义在 $Var(C_1)$ 上的集合 τ_1 的特征函数，即若 C_1 的第 i 个变量在 $Var(\tau_1)$ 中，则 $\alpha_1(0^{i-1}10^{t-i})=1$，否则 $\alpha_1(0^{i-1}10^{t-i})=0$。若将 τ_1 中的那些在 $Lit(C_1)\cap Lit(\tau_1)$ 里的字取反，得到唯一的限制 $\overline{\tau_1}$。易见，在限制 $\overline{\tau_1}$ 下 C_1 不再取值 1。将 ρ 换成 $\rho\tau_1$，将 τ 换成 $\tau\setminus\tau_1$，然后重复上述操作，得到 τ_2、$\overline{\tau_2}$、α_2。用归纳法可得 $\tau_3,\tau_3,\ldots,\tau_m$、$\overline{\tau_3},\overline{\tau_4},\ldots,\overline{\tau_m}$、$\alpha_3,\alpha_4,\ldots,\alpha_m$，这里 $m\leq s$ 并且 $\tau=\tau_1\tau_2\ldots\tau_m$。我们需要一些额外的信息指明 $\tau_1,\tau_2,\ldots,\tau_m$ 和 $\overline{\tau_1},\overline{\tau_2},\ldots,\overline{\tau_m}$ 的区别。设向量 $\beta\in\{0,1\}^s$ 指明对 τ 的支集中的变量赋值和 $\overline{\tau}=\overline{\tau_1\tau_2}\ldots\overline{\tau_m}$ 对该变量的赋值是否一致，即若 x 是 $\overline{\tau}$ 中的第 i 个变量，则 $\beta(0^{i-1}10^{t-i})=1$ 当仅当 $\tau(x)=\overline{\tau}(x)$，且 $\beta(0^{i-1}10^{t-i})=0$ 当仅当 $\tau(x)\neq\overline{\tau}(x)$。编码 $\mathfrak{e}$ 的定义如下：

$$\mathfrak{e}(\rho)\ \stackrel{\text{def}}{=}\ \langle\rho\overline{\tau_1\tau_2}\ldots\overline{\tau_m},\alpha_1,\alpha_2,\ldots,\alpha_m,\beta\rangle。$$

限制 $\overline{\tau_1}$ 有如下性质：τ 中的字都不出现在 C_1 之前的那些语句中，否者与 C_1 的定义矛盾；若 τ 中的一个字的否定出现在 C_1 之前的一个语句中，该语句取值 1。由这些性质可知，C_1 是第一个满足如下条件的语句：在限制 $\overline{\tau}$ 下的值不是 1，且对于特征函数 α_1 定义域中的第 i 个字（比如 $\overline{x}$），若 $\alpha_1(x)=1$，则 $\overline{x}$ 在限制 $\overline{\tau}$ 下取假。在 C_1 之前的任何一个取值非 1 的语句中的任何一个字（比如 $\overline{y}$），若 $\overline{y}$ 是该语句中的第 i 个字且 $\alpha_1(0^{i-1}10^{t-i})=1$，则 y 未被 $\overline{\tau}$ 限制。因此，从 f 和 $\rho\overline{\tau}$ 我们可以唯一锁定 C_1。从 C_1 和 α_1 可以恢复 $\overline{\tau_1}$，从 β 和 $\overline{\tau_1}$ 可以恢复 τ_1，并由此得到 $\rho\tau_1\overline{\tau_2}\ldots\overline{\tau_m}$。用归纳法最终得到 $\rho\tau_1\tau_2\ldots\tau_m$ 以及 ρ。因此从 $\mathfrak{e}(\rho)$ 可将 ρ 恢复出来，故 $\mathfrak{e}$ 是单射。

最后，我们估算一下 $\mathfrak{e}(\rho)$ 的值域的大小。首先，$\rho\overline{\tau_1\tau_2}\ldots\overline{\tau_m}\in R^{u+s}$，所以这类可能的限制个数不超过 $|R^{u+s}|$。其次，设 α_i 含有 k_i 个 1，则 $k_i\geq 1$，并且 $k_1+\ldots+k_m=s$。串 $(\alpha_1,\alpha_2,\ldots,\alpha_m)\in\{0,1\}^{mt}$ 的个数不超过 $\prod_{i\in[m]}\binom{t}{k_i}\leq$

$\prod_{i\in[m]} t^{k_i} = t^s$。满足 $k_1 + \ldots + k_m = s$ 的正整数向量 $(k_1, \ldots, k_m)$ 的个数不超过 $\binom{s-1}{m-1} \le 2^s$（见例??）。分量 $\beta \in \{0,1\}^s$ 的个数不超过 2^s，所以 $\mathfrak{e}$ 的值域大小不超过 $|R^{u+s}|\cdot(4t)^s$。 □

拉兹博罗夫引理特别引人注目的一点是其给出的上界不依赖于输入长度，用此特点能比较容易地推出哈斯塔德对换引理。

引理 0.3 (哈斯塔德对换引理)**.** *设 f 为含有 n 个输入变量的 t-合取范式，设 $p < 1/(9t)$。ρ 是大小为 $u = (1-p)n$ 的随机限制。则有*

$$\Pr_{\rho\in_{\mathrm{R}} R^u}[f_\rho \text{不可表示为 } s\text{-析取范式}] \le (9pt)^s。$$

证明. 根据引理0.1，概率值 $\Pr_{\rho\in_{\mathrm{R}} R^u}[f_\rho$不可表示为 s-析取范式$]$ 就是 $\frac{\mathrm{Bad}_f(u,s)}{|R^u|}$。从拉兹博罗夫引理0.2、引理 Razborov-Lemma 和条件 $p < 1/(9t)$ 可得推导：

$$\frac{\mathrm{Bad}_f(u,s)}{|R^u|} \le \frac{\binom{n}{u+s}2^{u+s}(4t)^s}{\binom{n}{u}2^u} \le \left(\frac{n-u}{u}\right)^s (8t)^s \le \left(\frac{p}{1-p}\right)^s (8t)^s \le (9pt)^s。$$

上述第二个不等式之所以成立是因为：

$$\binom{n}{u+s}\Big/\binom{n}{u} = \frac{u!}{(u+s)!}\cdot\frac{(n-u)!}{(n-u-s)!} \le \frac{1}{u^s}\cdot(n-u)^s,$$

最后一个不等式成立是因为

$$1-p > 1-\frac{1}{9t} \ge 1-\frac{1}{9} = \frac{8}{9}。$$

定理得证。 □

哈斯塔德原文 [108] 中的证明用的是条件概率推导，得到了一个更紧的上界 $(5pt)^s$。必须指出的是，上述给出的拉兹博罗夫引理和哈斯塔德对换引理针对的是合取范式，对析取范式相应的结论也成立。接下来我们解释如何从交换引理推出常数高度的计算奇偶函数电路族的指数复杂性下界 [108]。

定理 0.1 (奇偶函数的电路复杂性)**.** *计算 n-元奇偶函数的高度为 $d+1$ 的电路族需 $2^{\Omega(n^{1/d})}$ 个门。*

证明. 给定一个高度是 $d+1$ 的计算 n-元奇偶函数的大小为 $S(n)$ 的电路，我们将利用哈斯塔德对换引理把该电路转换成一个高度是 2 的电路。不失一般性，假定电路的最底层为或门。我们首先将此电路视为一个高度是 $d+2$、最底层为扇入为 1 的与门的交替电路。之所以这样做是因为我们想把电路转换成一个最底层门的扇入数为 $s = 2\log S(n)$ 的电路。取 $p = 1/18$、$t = 1$ 和 $u = (1-p)n$，根据哈斯塔德对换引理，对于大小为 u 的随机限制，每个或门不能表示成一个 s-合取范式的概率不超过 $(9pt)^S(n) = \frac{1}{S(n)^2}$，存在一个或门不能表示成一个 s-合取范式的概率不超过 $\frac{1}{S(n)}$。因此一定存在一个限制，在该限制下，将最下面两层进行交换后，最底层的每个门的扇入为 $s = 2\log S(n)$，并且新电路有 $pn = \frac{n}{18}$ 个输入变量。交换后的电路有 $d+2$ 层，将倒数第二层的与门和倒数第三层的与门合为一层，得到一个 $d+1$ 层的电路。重复上述构造，设 $t = s = 2\log S(n)$、$q = 1/18k$ 和 $v = (1-q)\frac{n}{18}$。在一个 v-大小的随机限制下，倒数第二层的每个与门不能表示成一个 s-析取范式的概率不到 $(9qt)^S(n) = \frac{1}{S(n)^2}$。用同样的推理，我们得知一定存在一个限制，在该限制下，倒数第二层的每个与门可表示成一个 s-析取范式。将得到的新的电路的倒数第二层的或门和倒数第三层的或门合并，得到一个高度是 d 的，最底层与门的扇入数为 $S(n)$，输入变量不超过 $\frac{n}{18}\cdot\frac{1}{18\cdot S(n)} = \frac{n}{18^2 S(n)}$ 的交替电路。

重复上面的操作，最终我们得到一个两层的交替电路，该电路的最底层门的扇入数不超过 $s = 2\log S(n)$，输入变量数不超过 $\frac{n}{18\cdot(18\cdot S(n))^{d-1}} = \frac{n}{O((\log S(n))^{d-1})}$。将此电路中的 $S(n)$ 个变量取特定值后电路的输出为常量（当电路为合取范式时为 0，析取范式时为 1）。因此将原始给定电路的

$$n - \frac{n}{O((\log S(n))^{d-1})} + 2\log S(n)$$

个输入变量取特定值后电路的输出为常量。但 n-元奇偶函数只有在所有 n 个输入确定后才输出常量，因此

$$n \le n - \frac{n}{O((\log S(n))^{d-1})} + 2\log S(n)。$$

由上述不等式即可推得 $S(n) = 2^{\Omega(n^{1/d})}$。 □

定理0.1说，一个解决奇偶函数的常数高度的电路族的大小是指数的，由此得到我们想要的否定结论。

推论 0.1. 奇偶函数不在 $\mathbf{AC}^0$ 中。

threshold function

利用此结论，我们可以通过归约证明其它一些布尔函数不在 $\mathbf{AC}^0$ 中，比如 n-元阈值函数Th_k^n。当 n 个输入中有至少 k 个输入为 1 时，函数 Th_k^n 值为 1，否则值为 0。对任意奇数 $k \in [n]$，容易从计算 Th_k^n 的电路构造计算 $Th_k^n \wedge \neg(Th_{k+1}^n)$ 的电路，此电路可判定输入中是否准确地有 k 个输入为 1。显然，实现下述布尔函数

$$\bigvee_{k\in[n]}^{k\text{为奇数}} \left(Th_k^n \wedge \neg(Th_{k+1}^n)\right)$$

的电路计算奇偶函数。如果阈值函数在 $\mathbf{AC}^0$ 中，奇偶函数就在 $\mathbf{AC}^0$ 中，矛盾。因此阈值函数不在 $\mathbf{AC}^0$ 中。

majority function

另一个著名的在 $\mathbf{NC}^1$ 中但不在 $\mathbf{AC}^0$ 中的函数是多数票函数Maj_n，若 n 个输入中值为 1 的输入个数至少是 $n/2$，函数 Maj_n 输出 1，否则输出 0。我们将证明留给读者。

参 考 文 献

[1] S. Aaronson. Is "P vs NP" formally independent? Bulletin of EATCS, 109-136, 2003.

[2] S. Aaronson. NP-Complete Problems and Physical Reality. ACM SIGACT News, 30-52, 2005.

[3] S. Aaronson and A. Wigderson. Algebrization: A New Barrier in Complexity Theory. ACM Transactions on Computation Theory, 2009.

[4] S. Abramsky. The Lazy Lambda Calculus. In D. Turner, editor, Declarative Programming, Addison-Wesley, 65-116, 1988.

[5] L. Adleman. Two Theorems on Random Polynomial Time. FOCS, 1978.

[6] L. Adleman and M. Huang. Recognizing Primes in Random Polynomial Time. Proceedings of the 19th Annual ACM Symposium on Theory of Computing, 1987, New York, New York, USA. ACM, 1987.

[7] M. Agrawal, N. Kayal and N. Saxena. PRIMES is in P, Annals of Mathematics, 160 (2): 781-793, 2004.

[8] M. Ajtai. Σ_1^1-formula on finite structures, Annals Pure Applied Logic 24, 1–48, 1983.

[9] D. Aldous. On the Markov Chain Simulaiton Method for Uniform Combinatorial Distribution and Simulated Annealling. Probability in the Engineering and Informational Sciences, **1**:33-46, 1987.

[10] R. Aleliunas, R. Karp, R. Lipton, L. Lovász and C. Rackoff. Random walks, universal traversal sequences, and the complexity of maze problems. In 20th Annual Symposium on Foundations of Computer Science (San Juan, Puerto Rico, 1979), 218–223. IEEE, New York, 1979.

[11] N. Alon. Eigenvalues and Expanders. Combinatorica, vol. 6, 83-96, 1986.

[12] N. Alon. Eigenvalues and Expanders. Combinatorica, vol. 6, 207-219, 1986.

[13] N. Alon and V. Milman. λ_1, Isoperimetric Inequalities for Graphs, and Superconcentrators. J. Comb. Theory, 1985.

[14] N. Alon and F. Chung. Explicit construction of linear sized tolerant networks, Discrete Math., 72:15–19, 1989.

[15] N. Alon and J. Spencer. The Probabilistic Method. John Wiley and Sons, 2008.

[16] D. Angluin. On counting problems and the polynomial hierarchy. Theoretical Computer Science, **12**:161-173, 1980.

[17] S. Arora and B. Barak. Computational Complexity: A Modern Approach. Cambridge University Press, 2009.

[18] S. Arora and S. Safra. Probabilistic checking of proofs: A new characterization of NP. J. ACM, 45(1):70–122, 1998. Prelim version FOCS ' 92.

[19] S. Arora, C. Lund, R. Motwani, M. Sudan and M. Szegedy. Proof Verification and the Hardness of Approximation Problems. FOCS'92, JACM, 1998.

[20] S. Axler. Linear Algebra Done Right. Third edition, Springer, 2015.

[21] L. Babai. Monte-Carlo Algorithms in Graph Isomorphism Testing. Technical Report DMS79-10, Département de Mathématique et de Statistique, Université de Montréal, 1979.

[22] L. Babai. Trading Group Theory for Randomness. STOC 1985.

[23] L. Babai. E-mail and the unexpected power of interaction. In Proceedings of the Fifth Annual Structure in Complexity Theory Conference, 31–91. IEEE, 8–11 July 1990.

[24] L. Babai. Graph Isomorphism in Quasipolynomial Time, STOC'16, 684-697, 2016.

[25] L. Babai, L. Fortnow, L. Levin and M. Szegedy. Checking Computation in Polylogarithmic Time. STOC, 1991.

[26] L. Babai, L. Fortnow and L. Lund. Nondeterministic Exponential Time has Two-Prover Interactive Protocols. FOCS 1990.

[27] L. Babai and S. Moran. Arthur-Merlin Games, A Randomized Proof System, and a Hierarchy of Complexity Classes. Journal of Computer and System Sciences, 254-276, 1988.

[28] R. Bar-Yehuda and S. Even. A linear-time approximation algorithm for the weighted vertex cover problem. Journal of Algorithms, 2:198-203, 1981.

[29] D. Beaver and J. Feigenbaum. Hiding Instances in Mutioracle Queries. Proceedings of the 7th Symposium on Theoretical Aspects of Computer Science. Lecture Notes in Computer Science, Vol. 415, pp. 37-48, Springer-Verlag, New York/Berlin, 1990.

[30] R. Beigel, N. Reingold and D. Spielman. PP is Closed under Intersection, STOC, 1-9, 1991.

[31] T. Baker, J. Gill and R. Solovay. Relativizations of the P=?NP question. SIAM Journal of Computing, 4(4):431–442, 1975.

[32] M. Bellare, O. Goldreich and M. Sudan. Free bits, PCPs, and nonapproximability – towards tight results. SIAM J. Comput., 27(3):804–915, 1998.

[33] M. Ben-Or, S. Goldwasser, J. Kilian and A. Wigderson. Multi-Prover Interactive Proofs: How to Remove Intractability Assumptions. STOC 1988.

[34] H. Barendregt. The Lambda Calculus: Its Syntax and Semantics. North-Holland. 1994.

[35] E. Berlekamp. Factoring Polynomials Over Finite Fields. Bell System Technical Journal. 46: 1853–1859, 1967.

[36] L. Berman and J. Hartmanis. On isomorphisms and density of NP and other complete sets, SIAM Journal on Computing, 6 (2): 305–322, 1977.

[37] J. Binet. Mémoire sur un système de formules analytiques, et leur application à des considérations géometriques. *J. Ec. Polyt.* **9**, **16**:280-302, 1812.

[38] M. Blum. A Machine-Independent Theory of the Complexity of Recursive Functions. Journal of ACM, 1967.

[39] M. Blum, M. Luby and R. Rubinfeld. Self-testing/correcting with applications to numerical problems. In Proceedings of the 22nd Annual ACM Symposium on Theory of Computing, 73–83, 1990.

[40] A. Borodin. Computational Complexity and the Existence of Complexity Gaps. Journal of the ACM 19(1):158-174, 1972.

[41] R. Boppana, J. Håstad and S. Zachos. Does co-NP Have Short Interactive Proofs? Information Processing Letters, 25:127-132, 1987.

[42] J. Cai, A. Condon and R. Lipton. On bounded round multi-prover interactive proof systems. In Proceedings, Fifth Annual Conference on Structure in Complexity Theory, 45-54, 1990.

[43] J. Cai, A. Condon and R. Lipton. PSPACE is provable by two provers in one round. In Proceedings of Structures in Complexity Theory Conference, 1991.

[44] J. Cai, A. Condon and R. Lipton. Playing games of incomplete information, Theoretical Computer Science, volume 103, 25–38, 1992.

[45] J. Cai, and R. Threlfall. A note on quadratic residuosity and UP. Information Processing Letters, 92:127-131, 2004.

[46] J. Carter and M. Wegman. Universal Classes of Hash Functions. Journal of Computer and System Sciences. FOCS, 1977.

[47] J. Carter and M. Wegman. Universal Classes of Hash Functions. Journal of Computer and System Sciences. 143-154, 1979.

[48] H. Casanova, A. Legrand and Y. Robert. Parallel Algorithm. CRC Press, 2009.

[49] A. Cauchy. Mémoire sur les fonctions qui ne peuvent obtenir que deux valeurs égales et de signes contraires par suite des transpositions opérées entre les variables qu'elles referment. *J. Ec. Polyt.* **10**, **17**:29-112, 1812.

[50] A. Chandra, D. Kozen and L. Stockmeyer. Alternation. Journal of the ACM, 28(1):114-133, 1981.

[51] V. Chvatal. A greedy heuristic for the set covering problem. Mathematics of Operations Research, 4:233–235, 1979.

[52] H. Chernoff. A measure of asymptotic efficiency for tests of a hypothesis based on the sum of observations. Annals Mathematical Statistic, 23(4):493-507, 1952.

[53] B. Chor and O. Goldreich. On the power of two-point based sampling. Journal of Complexity, 5:96-106, 1989.

[54] F. Chung. Spectral Graph Theory. American Mathematical Society, 1997.

[55] A. Church. An Unsolvable Problem of Elementary Number Theory. American Journal of Mathematics, 58:345-363, 1936.

[56] A. Cobham. The intrinsic computational difficulty of functions. In Proceedings of the 1964 International Congress for Logic, Methodology, and Philosophy of Science, 24–30. Elsevier/North-Holland, 1964.

[57] S. Cook. The complexity of theorem proving procedures. In Proc. 3rd Ann. ACM Symp. Theory of Computing, 151–158. ACM, 1971.

[58] S. Cook. A Hierarchy for Nondetermintstic Time Complexity. Journal of Computer and System Sciences, 1973.

[59] S. Cook. An observation on time-storage trade-offs, STOC'73, 29-33, 1973.

[60] S. Cook. Deterministic CFL's are Accepted Simultaneously in Polynomial Time and Log Squared Space. FOCS'79, 338-345, 1979.

[61] S. Cook and P. Nguyen. Logical Foundations of Proof Complexity. CUP, 2010.

[62] J. Cooley and W. Tukey. An algorithm for the machine calculation of complex Fourier series. Math. Comput., vol. 19, no. 2, 297-301, 1965.

[63] B. Copeland and F. Zhao. Did Turing stand on Gödel's shoulders? The Mathematical Intelligencer, 2022.

[64] T. Cover and J. Thomas. Elements of Information Theory. John Wiley & Sons, 2006.

[65] J. Curtiss. Monte Carlo Method. National Bureau of Standards Applied Mathematics Series, 1951.

[66] G. Dantzig. Maximization of Linear Function of Variables Subject to Linear Inequalities. In: Activity Analysis of Production and Allocation. T. Coopmans (ed.), John-Wiley, 339-347, 1951.

[67] G. Dantzig, G. Ford and D. Fulkerson. A primal-dual algorithm for linear programs. In: Linear Inequalities and Related Systems, H. Kuhn ans A. Tucker (eds.), Princeton University Press, 171-181, 1956.

[68] M. Davis. The Undecidable: Basic Papers on Undecidable Propositions, Unsolvable Problems and Computable Functions. Raven Press, 1965.

[69] I. Dinur. The PCP Theorem by Gap Amplification. J. ACM, 2007. STOC 2006.

[70] I. Dinur and D. Steurer. Analytical approach to parallel repetition, STOC '14: Proceedings of the forty-sixth annual ACM symposium on Theory of computing, ACM, 624–633, 2013.

[71] J. Dodziuk. Difference Equations, Isoperimetric Inequality and Transience of Certain Random Walks. Trans. AMS, 1984.

[72] 堵丁柱、葛可一、胡晓东. 近似算法的设计与分析，高等教育出版社，2011。

[73] R. O'Donnell. Analysis of Boolean Functions. Cambridge University Press, 2014.

[74] R. Durrett. Probability, theory and examples. Cambridge University Press, 2019.

[75] J. Edmonds. Paths, trees, and flowers. Can. J. Math. 17: 449–467, 1965.

[76] P. van Emde Boas. Machine Models and Simulations. In J. van Leeuwen, editor, Handbook of Theoretical Computer Science: Algorithm and Complexity, volume A, Elservier, 65-116, 1990.

[77] P. Erdös. Some Remakrs on the theory of graphs. Bulletin of American Mathematical Society. 1947.

[78] U. Feige. On the success probability of the two provers in one round proof systems. In Proceedings of Structures in Complexity Theory Conference, 1991.

[79] U. Feige. A threshold of $\ln n$ for approximating set cover. Journal of the ACM, 45:634–652, 1998.

[80] U. Feige and L. Lovász. Two-prover one-round proof systems, their power and their problems. In STOC 1992, ACM, New York, 733–744, 1992.

[81] U. Feige, S. Goldwasser, L. Lovász, S. Safra and M. Szegedy. Interactive proofs and the hardness of approximating cliques. J.ACM, 43(2):268–292, 1996. Preliminary version FOCS ' 91.

[82] W. Fernandez de la Vega and G. Lueker. Bin packing can be solved within $1 + \epsilon$ in linear time. Combinatorica, 1:349–355, 1981.

[83] L. Ford and D. Fulkerson. Maximal flow through a network. Canadian Journal of Mathematics, 8:399-404, 1956.

[84] L. Ford and D. Fulkerson. Flows in Networks. Princeton University Press, 1962.

[85] L. Fortnow, J. Rompel and M. Sipser. On the power of multi-prover interactive protocols. In: Proceedings of the Third Annual Conference on Structure in Complexity Theory, June 1988, pp. 156-161. Also in Theoretical Computer Science, **134**:545-557, 1994.

[86] L. Fortnow and M. Sipser. Are there interactive protocols for coNP-languages? Inf. Process. Lett., 28(5):249–251, 1988.

[87] G. Frandsen and P. Miltersen. Reviewing Bounds on the Circuit Size of the Hardest Functions. Information Processing Letters, 2005.

[88] R. Freivalds. Fast probabilistic algorithms. In Proceedings of Symposium on Mathematical Foundations of Computer Science. Lecture Notes in Computer Science, vol. 74. Springer-Verlag, New York, 57–69, 1979.

[89] M. Furst, J. Saxe and M. Sipser. Parity, circuits, andthe polynomial time hierarchy. Mathematical Systems Theory, 17:13–27, 1984. Prelim version FOCS ' 81.

[90] M. Garey and S. Johnson. Computers and Intractability: A Guide to the Theory of NP-Completeness, W. H. Freeman Co., New York, NY, 1979.

[91] G. Gentzen. On the relation between intuitionist and classical arithmetic. Studies in Logic and the Foundations of Mathematics, 1969.

[92] J. Gill. Computational Complexity of Probabilistic Turing Machines. STOC, 91-95, 1974.

[93] J. Gill. Computational Complexity of Probabilistic Turing Machines. SIAM Journal Computing 6(4): 675-695, 1977.

[94] K. Gödel. Über Formal Unentscheidbare Sätze der Principia Mathematica und Verwandter Systeme. Monatshefte für Mathematik und Verwandter Systeme I, 38:173-198, 1931.

[95] O. Goldreich. Computational Complexity, a conceptual perspective. CUP, 2008.

[96] O. Goldreich, S. Micali and A. Wigderson. Proofs that Yield Nothing but Their Validity and a Methodology of Cryptographic Protocol Design. FOCS 1986.

[97] O. Goldreich, S. Micali and A. Wigderson. Proofs that Yield Nothing but Their Validity and a Methodology of Cryptographic Protocol Design. Journal of ACM, 691-729, 1986.

[98] S. Goldwasser, S. Micali and C. Rackoff. The Knowledge Complexity of Interactive Proofs. STOC 1985.

[99] S. Goldwasser and M. Sipser. Private Coins versus Public Coins in Interactive Proof Systems. STOC 1986.

[100] T. Gonzalez. Clustering to minimize the maximum inter-cluster distance. Theoretical Computer Science, 38:293–306, 1985.

[101] R. Graham. Bounds for certain multiprocessing anomalies, Bell System Tech. J. 45, 1563–1581, 1966.

[102] A. Grama, A. Gupta, G. Karypis and V. Kumar. Introduction to Parallel Computing. Second Edition, Addison-Wesley, 2003.

[103] A. Granville. It is easy to determine whether a given integer is prime. Bulletin American Mathematical Society, 3-38, 2005.

[104] C. Grinstead and J. Snell. Introduction to Probability. AMS, 1998.

[105] N. Kahala. Eigenvalues and Expansion of Regular Graphs. Journal fo the ACM, vol. 42, 1091-1106, 1995.

[106] J. Hartmanis, R. Chang, S. Chari, D. Ranjan and P. Rohatgi. Relativization: a Revisionistic Retrospective: Essays and Tutorials. Current Trends in Theoretical Computer Science, 1993.

[107] J. Hartmanis and R. Stearns. On the Computational Complexity of Algorithms. Transactions of AMS, 117:285-306, 1965.

[108] J. Håstad. Almost optimal lower bounds for small depth circuits. Proceedings of the 18th ACM Symposium on Theory of Computing, Association for Computing Machinery, New York, pp. 71–84, 1986.

[109] J. Håstad. Some optimal inapproximability results. J. ACM, 48(4):798–859, 2001. Prelim version STOC ' 97.

[110] M. Heideman, D. Johnson and C. Sydney-Burrus. Gauss and the History of the Fast Fourier Transform. IEEE ASSP Magazine, October, 1984.

[111] F. Hennie and R. Stearns. Two-Tape Simulation of Multitape Turing Machines. Journal of ACM, 13:533-546, 1966.

[112] C. Hoare. Algorithm 64: Qucisort. Communication of ACM, 4(7): 321, 1961. 5: 10-15, 1962.

[113] D. Hochbaum. Approximation Algorithms for NP-hard Problems. PWS Publishing Company, 1997.

[114] D. Hochbaum and D. Shmoys. A unified approach to approximation algorithms for bottleneck problems. Journal of the ACM, 33:533–550, 1986.

[115] D. Hochbaum and D. Shmoys. Using dual approximation algorithms for scheduling problems: theoretical and practical results. Journal of the ACM, 34:144–162, 1987.

[116] T. Holenstein. Parallel Repetition: Simplifications and the No-Signaling Case. Theory of Computing. Volume 5, 141–172, 2009.

[117] 洪加威. On similarity and duality of computation (I). FOCS'80, 348-359, 1980.

[118] 洪加威. On similarity and duality of computation (I). Information and Control, 62:109-128, 1984.

[119] S. Hoory, N. Linial and A. Wigderson. Expander Graphs and their Applications. Bulletin of the AMS, **43**, 439-561, 2006.

[120] J. Hopcroft. Turing machines. Scientific American, 86–98, May 1984.

[121] J. Hopcroft, W. Paul and L. Valiant. On Time versus Space and Related Problems. FOCS, 1975.

[122] O. Ibarra and C. Kim. Fast approximation algorithms for the knapsack and sum of subset problems. Journal of the ACM, 22:463–468, 1975.

[123] R. Impagliazzo and A. Wigderson. P = BPP Unless E has exponential circuits: Derandomizing the XOR Lemma. In STOC, 220–229, New York, 1997.

[124] N. Immerman. Nondeterministic Space is Closed under Complementation. SIAM Journal Computing, 1988.

[125] M. Jerrum, L. Valiant and V. Vazirani. Random generation of combinatorial structures from a uniform distribution. Theoretical Computer Science, 43(2–3):169–188, 1986.

[126] D. Johnson. Approximation algorithms for combinatorial problems. J. Comput. Syst. Sci 9, 256–278, 1974.

[127] N. Johnson and S. Kotz. Urn Models and Their Application: An Approach to Modern Discrete Probability Theory. John Wiley, 1977.

[128] S. Jukna. Boolean Function Complexity: Advances and Frontiers. Springer, 2011.

[129] V. Kabanets and R. Impagliazzo. Derandomizing Polynomial Identity Tests means proving circuit lower bounds, Computational Complexity, 13(1-2), 1-46, 2004.

[130] G. Kalai and M. Safra. Threshold Phenomena and Influence. 2005.

[131] D. Karger. Global Min-cuts in **RNC**, and Other Ramifications of a Simple Min-cut Algorithm. In Proc. 4th Annual ACM-SIAM Symposium on Discrete Algorithms, 21-30, 1993.

[132] N. Karmarkar. A New Polynomial Time Algorithm for Linear Programming. In Proc. 16th Annual ACM-SIAM Symposium on Theory of Computing, 302-311, 1984.

[133] R. Karp. Reducibility among combinatorial problems. In R. E. Miller and J. W. Thatcher, editors, Complexity of Computer Computations, 85–103. Plenum, 1972.

[134] R. Karp. An Introduction to Randomized Algorithms. Discrete Applied Mathematics, 34:165-201, 1991.

[135] R. Karp and R. Lipton. Turing Machines that Take Advice. STOC, 1980.

[136] R. Karp and M. Luby. Monte-Carlo Algorithms for Enumeration and Reliability Problems. Proceedings of the 24-th IEEE Symposium on Foundations of Computer Science, 56-64, 1983.

[137] L. Khachijan. A polynomial algorithm for linear programming. Dokl. A.N. SSSR 244, 1093-1096, 1979.

[138] S. Khot and O. Regev. Vertex Cover Might be Hard to Approximate to within $2-\epsilon$. 18th IEEE Annual Conference on Computational Complexity, 2003.

[139] J. Kilian. Strong Separation Models of Multi Prover Interactive Proofs, DIMACS Workshop on Cryptography, October 1990.

[140] S. Kleene. General Recursive Functions of Natural Numbers. Mathematicsche Annalen, 112:727-742, 1936.

[141] S. Kleene. λ-Definablity and Recursiveness. Duke Mathematical Journal, 2:340-353, 1936.

[142] S. Kleene. Introduction to Metamathematics. Amsterdam, North-Holland, 1952.

[143] S. Kleene. Origin of Recursive Function Theory. Annals of the History of Computing, 3:52-67, 1981.

[144] S. Kleene. The Inconsistency of Certain Formal Logics. Annals of Mathematics, 36:630-636, 1935.

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

[146] R. Ladner. On the structure of polynomial time reducibility. J. ACM, 22(1):155-171, 1975.

[147] R. Ladner. The circuit value problem is log space complete for P, ACM SIGACT News 7, 18–20, 1975.

[148] D. Lapidot and A. Shamir. Fully parallelized multi prover protocols for NEXP-time. In Proceedings of 32nd Annual IEEE Symposium on the Foundations of Computer Science, 13-18, 1991.

[149] D. Lapidot and A. Shamir. A one-round, two-rover, zero-knowledge protocol for NP, in Combinatorica, 15 (1995), pp. 203–214.

[150] C. Lautemann. BPP and the Polynomial Hierarchy. IPL, 1983.

[151] K. de Leeuw, E. Moore, C. Shannon and N. Shapirio. Computability by Probabilistic Machines. Automata Studies, 183-212, Annals of Mathematics Studies, no. 34. Princeton University Press, Princeton, 1956.

[152] L. Levin. Universal sequential search problems. PINFTRANS: Problems of Information Transmission (translated from Problemy Peredachi Informatsii), 9, 265-266, 1973.

[153] D. Levin, Y. Peres and E. Wilmer. Markov Chains and Mixing Times. AMS, 2009.

[154] R. Lipton. New Directions in Testing. In: Distributed Computing and Cryptography. DIMACS Series on Discrete Mathematics and Theoretical Computer Science, Vol. 2, pp. 191-202, Amer. Math. Soc., Providence, RI, 1991.

[155] L. Lovász. On the ratio of optimal integral and fractional covers. Discrete Mathematics, 13:383–390, 1975.

[156] L. Lovász. On determinants, matchings, and random algorithms. In L. Budach, editor, Fundamentals of Computation Theory FCT ' 79, 565–574. Akademie-Verlag, 1979.

[157] C. Lund, L. Fortnow, H. Karloff and N. Nisan. Algebraic Methods for Interactive Proof Systems. FOCS 1990.

[158] C. Lund and M. Yannakakis. On the hardness of approximating minimization problems. Journal of the ACM, 41:960–981, 1994.

[159] O. Lupanov. The Synthesis of Contact Circuits. Dokl. Akad. Nauk SSSR (N.S.) 119:23-26, 1958.

[160] J. Lutz. Almost Everywhere High Nonuniform Complexity. JCSS, 1992.

[161] W. Maass. Quadratic lower bounds for deterministic and nondeterministic onetape turing machines. In STOC, 401–408. ACM, 1984.

[162] S. Mahaney. Sparse complete sets for NP: solution of a conjecture of Berman and Hartmanis. Journal of Computer and System Sciences, 25 (2): 130–143, 1982.

[163] U. Manber. Finding similar files in a large file system. In USENIX Winter, 1–10, 143, 1994.

[164] A. Markov. The Theory of Algorithms. American Mathematical Society Translations, series 2, 15:1-14, 1960.

[165] Y. Matiyasevich. Hilbert's Tenth Problem, MIT Press, Cambridge, Massachusetts, 1993.

[166] G. Miller. Riemann's hypothesis and tests for primality. Journal of Computer and System Sciences, 1976.

[167] R. DeMillo and R. Lipton. A probabilistic remark on algebraic program testing. Information Processing Letters, 193-195, 1978.

[168] H. Minc. Permanents. Encyclopedia of Mathematics and its Applications, G. Rota Editor. Addison-Wesley Publishing Company, 1978.

[169] M. Minsky. Computation: Finite and Infinite Machines. Prentice-Hall, 1960.

[170] M. Mitzenmacher and E. Upfal. Probability and Computing, Randomized Algorithm and Probabilistic Analysis. CUP, 2005.

[171] R. Motwani and P. Raghavan. Randomized algorithms. Cambridge University Press, 1995.

[172] J. von Neumann. Various techniques used in connection with random digits. Applied Math Series, 12:36–38, 1951.

[173] Y. Ofman. On the Algorithmic Complexity of Discrete Functions、。Dokl. Akad. Nauk SSSR (Soviet Math. Dokl.) 145 (1962), 48–51, (in Russian); English translation in Soviet Math. Dokl. 7(7) (1963), 589–591.

[174] M. Nielsen and I. Chuang. Quantum Computation and Quantum Information. Cambridge University Press, 2000.

[175] C. Papadimitriou. Games Against Nature. FOCS, 1983.

[176] C. Papadimitriou. Computational Complexity. Addison-Wesley, 1994.

[177] C. Papadimitriou and K. Steiglitz. Combinatorial Optimization: Algorithms and Complexity. Prentice-Hall, Englewood Cliffs, NJ, 1982.

[178] C. Papadimitriou and M. Yannakakis. Optimization, approximation, and complexity classes. J. Comput. Syst. Sci., 43(3):425–440, 1991. Prelim version STOC ' 88.

[179] C. Papadimitriou and S. Zachos. Two Remarks on the Power of Counting. Lecture Notes in Computer Science 145, 260-276, 1983.

[180] M. Pinsker. On the complexity of a concentrator. In 7th International Telegraffic Conference, 318/1–318/4, 1973.

[181] N. Pippenger. On Simultaneous Resource Bounds. FOCS'79, 307-311, 1979.

[182] E. Post. Formal Reduction of the General Combinatorial Decision Problem. American Jounal of Mathematics, 65:197-215, 1943.

[183] L. Pottier. Minimal Solutions of Linear Diophantine Systems: Bounds and Algorithms. In Proc. RTA' 91, Lecture Notes in Computer Science 488, 162-173. Springer, 1991.

[184] D. Prawitz. Natural deduction: a proof-theoretical study. Almqvist & Wiksell International Republished by Dover Publications, 1965.

[185] M. Rabin. Aprobabilistic algorithm for testing primality. J. Number Theory, 12(1):128–138, 1980.

[186] R. Raz. A parallel repetition theorem. SIAM J. Comput., 27(3):763–803, 1998. Prelim version STOC ' 95.

[187] A. Razborov. Bounded Arithmeticsand Lower Bounds in Boolean Complexity. In: Feasible Mathematics II, Proc. of Workshop (Cornell University, Ithaca, NY, May 28-30, 1992), Birkhauser, Boston, Ma, 1995.

[188] A. Razborov and S. Rudich. Natural proofs. Journal of Computer and System Science, 55(1):24–35, 1997. Preliminary version in STOC ' 94.

[189] O. Reingold. Undirected ST-Connectivity in Log-Space. STOC 2005.

[190] O. Reingold, L. Trevisan and S. Vadhan. Pseudorandom walks in biregular graphs and the RL vs. L problem. Technical Report TR05-022, Electronic Colloquium on Computational Complexity (ECCC), 2005.

[191] O. Reingold, S. Vadhan and A. Wigderson. Entropy Waves, the Zig-Zag Graph Product, and New Constant-Degree Expanders and Extractors. FOCS, 2000.

[192] J. Riordan and C. Shannon. The Number of Two-terminal Series-parallel Networks. Journal of Mathematics and Physics, 21:83-93, 1942.

[193] H. Rogers. Theory of Recursive Functions and Effective Computability. MIT Press, 1987.

[194] Y. Rudich and A. Wigderson. Computational Complexity Theory, American Mathematical Society, 2004.

[195] E. Santos. Probabilistic Turing Machines and Computability. Proc. American Mathematical Society, 22: 704-710, 1969.

[196] E. Santos. Computability by Probabilistic Turing Machines. Trans. American Mathematical Society, 159: 165-184, 1971.

[197] J. Savage. The Complexity of Computing. John Wiley and Sons, New York, 1976.

[198] J. Savage. Models of Computation, Exploring the Power of Computing. Addison-Wesley, 1998.

[199] W. Savitch. Relationships between Nondeterministic and Deterministic Tape Complexities. JCSS, 177-192, 1970.

[200] S. Schmitz. Complexity Hierarchy Beyond Elementary. ACM Transactions on Computation Theory, 2016.

[201] A. Schönhage and V. Strassen. Schnelle Multiplikation grosser Zahlen. Computing 7 (1971), 281–292.

[202] A. Schrijver. Theory of Linear and Integer Programming. John Wiley and Sons. 1986.

[203] J. Schwartz. Fast Probabilistic Algorithms for Verification of Polynomial Identities. Jounral of ACM, **27**:701-717, 1980.

[204] J. Seiferas, M. Fischer and A. Meyer. Separating Nondeterministic Time Complexity Classes. Journal of ACM, 1978.

[205] A. Shamir. IP = PSPACE. FOCS 1990.

[206] C. Shannon. A Symbolic Analysis of Relay and Switching Circuits. Master's thesis, MIT, 1937.

[207] C. Shannon. The Synthesis of Two-Terminal Switching Circuits. Bell System Technical Journal. 28:59-98, 1949.

[208] C. Shannon. Communication theory of secrecy systems. Bell Sys. Tech. J., 28:656–715, 1949.

[209] A. Shen. IP = PSPACE: Simplified Proof. J. ACM, 39(4):878–880, 1992.

[210] J. Shepherdson and H. Sturgis. Computability and Recursive Functions. Journal of Symbolic Logic, 32:1-63, 1965.

[211] J. Simons. On Some Central Problems in Computational Complexity. Cornell University, 1975.

[212] J. Simons. On the Difference between One and Many. ICALP '77, 480-491, 1977.

[213] M. Sipser. A Complexity Theoretic Approach to Randomness. STOC, 1983.

[214] M. Sipser. Introduction to the Theory of Computation. Third edition, Cengage Learning, 2013.

[215] R. Smolensky. Algebraic methods in the theory of lower bounds for Boolean circuit complexity. In STOC, 77–82. ACM, 1987.

[216] M. Snir. Lower Bounds on Probabilistic Linear Decision Trees. Theoretical Computer Science, 38:69-82, 1985.

[217] C. Schnorr. Optimal algorithms for self-reducible problems. Proc. 3rd Internal Coll. on Automata, Languages and Programming (1976) 322-337, 1976.

[218] R. Solovay and V. Strassen. A fast Monte-Carlo test for primality. SIAM J. Comput., 6(1):84–85, 1977.

[219] R. Stanley. Enumerative Combinatorics, vol. 2. 1999. Cambridge Stud. Adv. Math, 1999.

[220] L. Stockmeyer and A. Meyer. The Equivalence Problem for Regular Expressions with Squaring Requires Exponential Space. SWAT'72.

[221] L. Stockmeyer and A. Meyer. Word Problems Requiring Exponential Time. STOC, 1973. Fast Probabilistic Algorithms for Verification of Polynomial Identities. Journal of the ACM, 701-717, 1980.

[222] L. Stockmeyer. The Polynomial-Time Hierarchy. Theoretical Computer Science, 3:1-22, 1976.

[223] L. Stockmeyer. The Complexity of Approximate Counting. STOC 1984.

[224] G. Strang. Introduction to Linear Algebra. Wellesley-Cambridge Press, 2016.

[225] B. Subbotovskaya. Realizations of Linear Functions by Formulas Using $\vee$, &, _. Doklady Akademii Nauk SSSR, 136(3):553-555, 1961.

[226] R. Szelepcsényi. The Method of Forcing for Nondeterministic Automata. Bulletin of EATCS, 1987.

[227] G. Takeuti. Proof Theory. North-Holland, 1987.

[228] M. Tanner. Explicit concentrators from generalized N-gons. SIAM Journal on Algebraic Discrete Methods, 5(3):287–293, 1984.

[229] B. Trakhtenbrot. Turing Computations with Logarithmic Delay. Algebra and Logic 3(4):33-48, 1964. (in Russian)

[230] B. Trakhtenbrot. A survey of Russian approaches to perebor (brute-force search) algorithms. Annals of the History of Computing, 6(4):384–400, 1984.

[231] L. Trevisan, G. Sorkin, M. Sudan and D. Williamson. Gadgets, approximation and linear programming. SIAM J. Comput. 29, 2074–2097, 2000.

[232] A. Turing. On Computable Numbers, with an Application to the Entscheidungsproblem. Proceedings of the London Mathematical Society, 42:230-265, 1936.

[233] A. Turing. On Computable Numbers, with an Application to the Entscheidungsproblem: A Correction. Proceedings of the London Mathematical Society, 43:544-546, 1937.

[234] A. Turing. Computability and λ-Definability. Journal of Symbolic Logic, 2:153-163, 1937.

[235] C. Umans. The Minimum Equivalent DNF Problem and Shortest Implicants. JCSS, 597-611, 2001. Preliminary version in FOCS 1998.

[236] S. Vadhan. Pseudorandomness, 2012.

[237] L. Valiant. Relative Complexity of Checking and Evaluating. Information Processing Letters, 5:20-23, 1976.

[238] L. Valiant. The Complexity of Computing the Permanent. Theoretical Computer Science, 8:189-201, 1979.

[239] L. Valiant. The Complexity of Enumeration and Reliability Problems. SIAM J. Computing 8:410-421, 1979.

[240] L. Valiant. Probably Approximately Correct, nature's algorithms for learning and prospering in a complex world. BASICS BOOKS, 2013.

[241] L. Valiant and V. Vazirani. NP is as Easy as Detecting Unique Solutions. Theoretical Computer Science, 47:85-93, 1986.

[242] V. Vazirani. Approximation Algorithms. Springer, 2003.

[243] O. Verbitsky. Towards the parallel repetition conjecture. Theoretical Computer Science, 157, 277-282, 1996.

[244] C. Wallace. A Suggestion for a Fast Multiplier. IEEE Trans. Computers, 14–17, 1964.

[245] J. Walsh. A closed set of normal orthogonal functions. American Journal of Mathematics, 45(1):5–24, 1923.

[246] I. Wegener. The Complexity of Boolean Functions. John Wiley and Sons Ltd, 1987.

[247] I. Wegener. Complexity Theory. Springer-Verlag Berlin Heidelberg. 2005.

[248] D. Welsh. Randomized Algorithms. Discrete Applied Mathematics, 5:133-145, 1983.

[249] M. Welsh. The End of Programming. Communication of ACM, 66:34-35, 2023.

[250] A. Wigderson. Mathematics and Computation: A Theory Revolutionizing Technology and Science. Princeton University Press, 2019.

[251] B. Wilkinson and M. Allen. Parallel Programming, Techniques and Applications Using Networked Workstations and Parallel Computers. Prentice-Hall, 1999.

[252] D. Williamson and D. Shmoys. The Design of Approximation Algorithms. Cambridge University Press, 2011.

[253] C. Wrathall. Complete Sets and the Polynomial-Time Hierarchy. Theoretical Computer Science. 3:23-33, 1976.

[254] A. Yao. Separating the polynomial-time hierarchy by oracles, Proceedings of the 26th IEEE Symposium on Foundations of Computer Science, IEEE Computer Society Press, Los Angeles, pp. 1–10, 1985.

[255] S. Zák. A Turing Machine Time Hierarchy. Theoretical Computer Science, 1983.

[256] R. Zippel. Probabilistic algorithms for sparse polynomials. Symbolic and Algebraic Computation, Eurosam 79, Marseille, France, June. LNCS 72, 216-226, 1979.