陷门函数的理论和应用*

姚期智 (Andrew C. Yao)

翻译：李晓峰 (cy_lxf@163.com)

译文来自于经典文献翻译项目 https://gitee.com/uisu/InfSecClaT

译者单位：北京联合大学智慧城市学院

2023 年 4 月 3 日

摘要

本文旨在介绍一种新的信息理论并探讨其应用。利用现代计算复杂性，我们研究了信息的概念, 可以在可行计算 (feasible computation) 中使用。

在本文的第 1 部分中，我们建立了理论基础，并建立了密码学和伪随机数分析的框架。在第 2 部分中，我们研究了陷门函数的概念，并研究了此类函数在密码学、伪随机生成和抽象复杂性理论中的应用。

*原始论文信息：A. C. Yao, "Theory and application of trapdoor functions," 23rd Annual Symposium on Foundations of Computer Science (sfcs 1982), Chicago, IL, USA, 1982, pp. 80-91, doi: 10.1109/SFCS.1982.45.

目录

1 第 1 部分：计算信息理论 (computational information theory)

1.1 引言

香农第一定理 [22]. $\lim_{n\to\infty} \frac{L_n}{n} = H(S)$.

香农第二定理 [22]. 对于任何 $R < capacity(C)$，且 $\epsilon > 0$, 当 m 足够大时，存在一种长度为 m 的编码 E 和一种解码规则 f, 满足:
(a)$|E| \geq 2^{Rm}$,
(b)$P(x) < \epsilon$, 对于所有的 $x \in E$.

1.2 有效熵 (effective entropy)

给定一个具有大字母表的源 S，例如在示例 1 中，我们应该如何定义其输出中包含的信息？我们将采用这样的观点，即以计算上可行的方式描述输出所需的最小平均比特数, 这种度量是恰当的。换句话说，我们将把香农第一定理作为一个定义。

我们考虑到以下情况。源有一个字母表，其符号是平均长度为 n（比如 $n \approx 200$）的有限二进制字符串。A 感兴趣的是向 B 传达由 S 的 n^t 符号组成的序列 σ,t 是固定整数，比如 t=3。问题是，A 能在合理的时间内计算出多短的字符串 ρ（比如说，对于某个固定的 k，在时间 n^k 中），这样 B 在接收到 ρ 时，B 能在合理的时间内恢复 σ？为了准确地定义这个概念，我们求助于发展完善的计算复杂性理论。在这个理论中，计算问题的复杂性是通过输入长度变大时算法的渐近行为来衡量的。为了将理论结果应用于特定长度的输入，我们默认该长度足够大，可以使用渐近结果。例如，假设从理论上可以证明某个形式逻辑系统的决策问题的复杂性为 $\Omega(2^{2^n})$，即，对于某个常数 $C_T > 0$，决策问题的任何算法 T 的运行时间 $\geq C_T 2^{2^n}$。然后，我们将考虑到，对于公式大小 $n \approx 1000$，任何合理的算法都必须为一些输入公式使用的时间 $\approx 2^{2^{1000}}$。采用这种方法，我们需要考虑的不是一个源，而是一系列源，并观察感兴趣量的渐近行为。

Definition 1 设 Σ 是一个固定的，有限的字母表，“源”$\mathbf{S}$ 是一个在 Σ^+ 上，概率分布式是 p，具有有限期望长度 $\beta(S) = \sum_x p(x)|x|$。一个 *source ensemble* S 是源 $\mathbf{S}_1, \mathbf{S}_1, \ldots$ 的一个序列，这些源的概率分布是 $p_1, p_2, ...$，对于某一个固定的 $t_2 > t_1 > 0, p_n(y) > 0$，意味着 $n^{t_1} < |y| < n^{t_2}$

Remark: 最后一个假设并不重要，但有助于简化以后的讨论；在我们感兴趣的大多数应用程序中，这个条件是满足的。

在下文中，概率算法意味着总是停止的概率多带图灵机 [9]。人们也可以把它看作是随机访问计算机上的一个程序，它总是停止，因为我们只证明结果是多项式不变量。

符号： 对于任何函数 $f(n)$，给定 t, 其消亡快于 $1/n^t$，我们记为 $O(v(n))$。

下面的定义准确地阐述了 A 如何编码从 S^n 输出的 $n^k(for\ some\ k > 0)$ 个符号序列，以及，B 如何解码他。

Definition 2 给定 t, k,$t, k > 0$，S 的一个 $(t-k)-encoding$ 是一个概率算法 $\mathcal{M} = (M_A, M_B, M_C)$ 三元组 *(triplet)*，满足一下性质：
(a) 给定输入 $\alpha = (n, x_1, x_2, \ldots, x_{n^k})$，对于所有 i,$p_n(x_i) > 0$, 算法 M_A 在时间 $O(n^t)$ 内停止，在 M_A 的输出带上留下一个二进制串 β；β 的概率分布记为 $q_n(\alpha)$。
(b) 随机给定一个输入对 (n, β)，β 按 $q(a)$ 分布，M_B 算法在时间 $O(n^t)$ 内停止，在 M_B 的输出带上以概率 $1 - O(v(n))$ 留下一个二进制串 α。
(c) 给定 b,$b > 0$，给定 n 和任意串 $\beta = \beta_1\beta_2 \ldots \beta_u$, 每一个 β_i 是 M_A 对某个 α_i 的可能输出，并且 $u = O(n^b)$，对某个固定的 b'，算法 M_C 在时间 $O(n^{b'})$ 内停止，并以错误概率 $O(v(n))$ 正确输出 $\beta_1\beta_2 \ldots \beta_u$.

将 $l(a)$ 定义为 β 在 $q_n(a)$ 上的预期长度。设 $p_n(\alpha) = p_n(x_1)p_n(x_2) \ldots p_n(x_{n^k})$。设 $l_n(\mathcal{M}; S) = \sum_\alpha p_n(\alpha) l_n(\alpha)/n^k$, 这是 $\mathcal{M}$ 用于编码 S_n 的输出符号 x 的平均比特数。

Remark:

Definition 3 S 的一个 $(t-k)-entropy$ 序列，是 $w_1, w_2, \ldots$ 序列，存在一个 S 的 $(t-k)-encoding\mathcal{M}$ ，$l_n(\mathcal{M}; S) = w_n$.

只有 w_n 的渐近行为是令人感兴趣的，因为对于任何固定的 n，我们可以选择具有足够状态的 $\mathcal{M}$，使 $w_n = H(S_n)$,S_n 的 Shannon 熵。

Definition 4 我们说有效熵 *(effective entropy)* $H_c(S)$ 小于 $g(n)$,即,$H_c(S) \leq g(n)$, 如果存在 $t, k > 0$ 和 S 的 $(t,k) - entropy$ 序列 $< w_n >$，对于足够大的 n，有 $w_n \leq g(n)$.

Definition 5 真随机数 *ensemble* τ_0 是 *source ensemble* $S_1, S_2, \ldots$，此处，当 $|x| = n$ 时，S_n 的概率分布为 $p_n(x) = 2^{-n}$;$|x| \neq n$ 时, 概率为 *0.*

1.3 可靠传输 (reliable transmission)

Definition 6 设 $S =< \boldsymbol{S}_n >$ 是一个 *source ensemble*，C 是一个有输入-输出字符集 I 和 J 的信道，一个 S 在 C 上的 $(t-k) - coding\ sheme$ 是一个概率算法三元组 $\mathcal{M} = (M_A, M_B, M_C)$，这个算法总是在多项式时间 $O(n^t)$ 内停止。对于任意的 n 和从 $\boldsymbol{S}_n$ 输出的 n^k 长度的字符串 α，编码器 *(encoder)*M_A 随机地计算字符串 $\beta \in I^*$，并且通过信道 C 发送；解码器 *(decoder)*M_B 取结果输出串 $\gamma \in J^*$，并计算串 δ。要求是，当在 α 的概率分布上以及在 M_A, M_B 和 C 的所有随机移动上进行平均时，$\delta \neq \alpha$ 的概率为 $O(v(n))$ 阶。串 γ*(*从信道 C 输出*)* 可通过算法 M_C 唯一解密 *(*如定义 *2* 中所示*)*, 也允许 $O(v(n))$ 的故障概率。

定义 2 可以看做定义 6 的特例，S 的一个 $(t,k) - encoding$ 本质上是在 C 上的 S 的一个 $(t,k) - coding\ scheme$,C 是具有交叉概率 (crossover probability)$q = 0$ 的二进制对称信道。

Definition 7 在前面的定义中，当 M_A 的输入 α 是由源 $\boldsymbol{S}_n$ 概率地生成的，设 $l(\mathcal{M}; S; C)$ 是 $|\beta|/n^k$ 的期望值。

1.4 不可区分性 (indistinguishability)

设源 S, S' 在 Σ^+ 上具有已知的不同的概率分布 p, p'，此处 Σ 是一个固定的字母表。假设有一个模拟其中一个源的盒子给了你，但你没有被告知是哪个源。盒子将在每次请求时发出一个字符串，该字符串根据其底层依赖的概率分布进行分配。你能自信地说出盒子在模拟哪个来源吗？

对于经典源，答案是“是”，因为人们总是可以获得足够的输出，并观察 $p(v) \neq p(v')$ 的任何特定字符串 v 的出现频率。然而，在非经典情况下，这个问题更为复杂。即使 p 和 p' 相差很大，比如 $p(v) = |\Sigma|^{-n}$，对于所有长度的 v，$p'(v) = 1/|T|$，其中 $T \subseteq \Sigma^n$ 和 $|T| = |\Sigma|^{\sqrt{n}}$，没有明显

的办法决定哪种选择是真的（如果我们采用上述经典源使用的方法，将需要天文数字的观测）。我们现在准确地定义了我们所说的两个无法区分的源 (indistinguishable sources) 的含义。

Definition 8 设 $S =< S_n >, S' =< S'_n >$ 是两个 *source ensemble(有翻译为“整体源”的，但是感觉不太好，我们这里暂用英文。)*，一个 (S, S') 的“见证算法”*(witness algorithm,* 也可以翻为“目击算法”“证据算法”*)* M，是一个概率算法，对于固定的 $t, k, \epsilon > 0$，以下属性成立：
(a) 对于任何输入 (n, a)，此处 $a = (x_1, x_2, \ldots, x_n^k)$ 是 S_n 输出的 n^k 序列，算法 M 在 $O(n^k)$ 时间内停止，并且留下一个布尔输出 $M(n, a)$；设 $f_n(M, S)$ 是 $M(n, a) = 1$ 的概率，此处 a 由 S_n 概率生成。
(b) 相似地，设 $f_n(M, S')$ 是 S' 对应的概率；
(c) 这里存在一个无限序列的（不同的）值 $n_1, n_2, \ldots$, 使得

$$|f_n(M, S) - f_n(M, S')| > \epsilon, \ for \ n = n_1, n_2, \ldots$$

Definition 9 当两个 *source ensemble* S 和 S' 不存在“见证算法”时，称 S 和 S' 是不可区分的 *(indistinguishable)*。

请注意，见证算法可能不是决定盒子是模拟源 S 还是 S' 的合适算法，因为条件 (c) 只保证 S 和 S' 在某些 n 值下表现不同[1]。见证算法的定义是为了确保两个不可区分的源在任何测试中表现几乎相同, 当 $n \to \infty$。

存在无法区分的 source ensemble，他们具有非常不同的基础概率分布 (underlying probability distributions)。事实上，示例 2 中定义的 S 和真随机数 ensemble τ_0（定义 5）是不可区分的。原因将在下一节中讲清楚。

[1]译者注：虽然在条件 (c) 中值 n 是无限多个，但是并不能保证是全部，举个例子，整数是一个无限集合，$2n + 1$ 是奇数序列，是无限，但不是全部，因为不包含偶数序列 $2n$。

参考文献

.[1] L. Adleman, "Two theorems on random p o l y n m i a l time," Prac. 19th IEEE Symp. on Foundations of Computer SCIence, Ann Arbor, Michigan, Oct 1978, 75-83.

.[2] L. Adleman, tt Asubexponential algorithm for the discrete logarithm problem with applications to cIJ:ptography," P r . 20th IEEE Symp. on Foundations of Computer Science, Puerto RICO, Oct 1979, 55-60.

.[3] R. Aleliunas, R. M. Karp, R. 1. Lipton, L. Lovasz, .C. Rachoff, "Ran-

dom walks, universal sequences, and the compleXIty of maze p r o b l e " Proc. 20th IEEE Symp. on Foundations of Computer Science, Puerto Rico, Oct 1979, 218-223.
.[4J C. H. Bennett and J. Gill, "Relative to a random oracle, PA = NPA = co-NPA with probability 1," SIAM J. on Computing 10 (1981), 96-113.
.[5] M. Blum and S. Micali, "How to generate cryptographically stron sequences of pseudo random bits," this proceedings.
.[6] G. Chaitin, "A theory of program size fonnally identical to infonnation theory," Journal of ACM 22 (1975), 329-340.
.[7] W. Diffie and M. E. Hellman, "New directions in cryptography," IEEE Trans. on Infonn. Theory IT-22, 6 (1976), 644-654.
.[8] R. Gallager, Infonnation Theory and Reliable Communication, Wiley, New York, 1968.
.[9] J. Gill, "Computational complexity ofprobabilistic Turing machines," SIAM 1. om Computing 6 (1977), 675-695.
.[10] S. Goldwasser and S. Micali, "Probabilistic encryption and how to play mental poker keeping secret all partial infonnation," Proc. 14th ACM Symp. on Theory of Computing, San Francisco, May 1982.
.[11] J. E. Hopcroft and 1. D. Ullman, Introduction -to Automata Theory, Languages, and Computation, Addison-Wesley, Reading, Mass., 1979.
.[12] R. M. Karp and R. 1. Lipton, "Some connections between nonunifonn and unifonn complexity classes," Prac. 12th ACM Symp. on Theory of Computing, Los Angeles, April 1980, 302-309.
.[13] D. E. Knuth, The Art of Computer Programming, Vol.. 2, Addison-Wesley, Reading, Mass., second edition, 1981.
.[14] A. N. Kolmogorov, "Three approaches to the concept of the amount of infonnation," Probl. Pered. Inf. (Probl. of Int: Transm.) 1/1 (1965).
.[15] P. Martin-Lot: "The definition of random sequences," Information and Control 9 (1966), 602-619.
.[16] A. R. Meyer and E. M. McCreight, "Computability complex and pseudorandom zero-one valued functions," in Theory of Machines and Computations, Z. Kohavi and A. Paz, eds., Academic Press, New York 1971, 19-42.
.[17] N. Pippenger, "On simultaneous resource bounds," Prac. 20th IEEE

Symp. on Foundations of Computer Science, Puerto Rico, Oct 1979, 307-31l.

.[18] N. Pippenger and M.. 1. Fischer, "Relations among complexity measures," Journal of ACM 26 (1979), 361- 38l.

.[19] M. O. Rabin, "Digitalized signatures and public-key functions as intractable as factorization," MITILCSITR- 212, 1979.

.[20] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," Communications of ACM 21 (1978), 120-126.

.[21] A. Shamir, presented at Crypto-81, Santa Barbara, 1981.

.[22] C. E. Shannon, "A mathematica theory of communication," Bell System Technical Journal, 27 (1948), Part I, 479-523, Part II, 623-656.

.[23] C. E. Shannon, "Communicatin theory of secrecy systems," Bell System Technical Journal 28 (1949), 656-715,

.[24] L. Valiant, "The complexity of computing the permanent," Theoretical Computer Science 8 (1979), 189-20l.

.[25] A. D. Wyner, "The wire-tap channel," Bell System Technical Journal 54 (1975), 1355-1387.

.[26] 1. Ziv, IEEE Transaction on Information (1965).

.[27] A. K. Zvonkin and L. A. Levin, "The complexity of finite objects and the algorithmic concepts of information and randomness," Uspekhi Mat Nauk (Russian Math. Surveys 25/6 (1970), 83-124.