生成计算问题的可解决实例

Martin Abadi, Eric Allender, Andrei Broder, Joan Feigenbaum, Lane A. Hemachandra

翻译：李晓峰 (cy_lxf@163.com)[‡]

V1.0

2024 年 5 月 10 日

摘要

我们考虑了有效生成计算问题的可解决实例的问题。特别是，我们考虑了不可攻击的生成器 (invulnerable generators)。设 S 是 $(0,1)^*$ 的一个子集，并且 M 是一个接受 S 的图灵机，M 在输入 x 上的接受计算 w 被称为一个“证据”(witness)，$x \in S$。非正式地，一个程序如果在其输入 1^n 上产生实例-证据 (instance-witness) 对 $< x, w >$，其中 $|x| = n$，根据一个分布，任何多项式时间敌手，在给定 x 时，对于无限多个长度 n，至少以概率 α 找不到证据证明 x，$x \in S$，那么这个程序就是一个 α 不可攻击的生成器 (α-invulnerable generator)。

哪些集合具有不可攻击的生成器的问题在理论上具有内在的吸引力，其结果可以应用于启发式算法测试数据的生成和零知识证明系统的理论。不可攻击的生成器的存在性与加密安全单向函数的存在性密切相关。我们证明了三个关于不可攻击性的定理。第一个定理解决了，如果确实存在 NP 集合具有不可攻击生成器的话，NP 集合中哪些集合具有不攻击生成器的问题。第二个解决了这些生成器有多牢不可破的问题。

定理（完备性）：如果 NP 中的任何集合具有率 α 不可攻击生成器，那么 SAT 是一个。

定理（放大）：如果 $S \in NP$，并且存在一个常数 $\beta \in (0,1)$，使得 S 具有 β-不可攻击生成器，那么对于任意常数 $\alpha \in (0,1)$，S 都具有 α-不可攻击生成器。

我们的第三个关于不可攻击性的定理表明，使用相对化的技术无法解决仅凭 $P \neq NP$ 的假设就能证明存在不可攻击生成器的问题。显然，存在这

[*]译者目前为北京联合大学智慧城市学院信息安全老师。

[†]译文来自于经典文献翻译项目 https://gitee.com/uisu/InfSecClaT, 欢迎大家加入经典翻译项目，为更多的人能够获取这些经典文献所传递信息做一点贡献。

样的相对化世界，其中存在不可攻击生成器；在这些世界中，$P \neq NP$。我们通过第三个定理解决的是一个更微妙的问题，即是否存在这样的相对化世界，其中 $P \neq NP$，但不存在不可攻击生成器。

定理（相对化）：存在一个查询机 (oracle)，相对于该查询机，$P \neq NP$，但没有不可攻击生成器。

I 引言

Sanchis 和 Fulk 研究了构建困难问题测试实例的复杂性，以及这种构建与复杂性类结构之间的联系 [20,21]。在本文中，我们考虑了计算问题可解实例的有效生成。例如，如果 $S = \{x : \exists w, p(x, w)\}$ 是 NP 中的集合，我们可能希望根据指定的分布生成实例-证明对 $< x, w >$。生成对 $< x, w >$ 的复杂性与给定 x 的求 w 的复杂性之间的关系在理论上是非常有趣的，它对困难问题的启发式算法的测试和零知识证明系统的可能应用也很重要。

具体地说，我们要问的是: 是否有可能产生我们所说的不可攻击的实例-见证对分布。例如，是否有可能生成对 $< f, \alpha >$，其中 f 是一个布尔公式，α 是一个满足此公式的赋值，将秘密 α 提供给一个用户 A，发布公式 f，并保持合理的信心，多项式时间对手将无法为 f 找到一个满足此公式的赋值 α'，从而冒充 A？Feige、Fiat 和 Shamir 提出使用“零知识身份证明”作为一种安全机制; 他们提出的具体方案是基于二次残差问题 (Quadratic residual Problem, QRP，[6])。即使 QRP 比人们普遍认为的要简单，零知识身份证明仍然是有用的; 此外，即使 QRP 很难，也可以将方案基于另一个问题并实现更高的安全性。因此，有一个复杂性理论框架来考虑生成实例-证明对的方案是否产生安全分布是很重要的。

当 Goldwasser, Micali 和 Rackoff 首次引入零知识证明系统时，他们假设了一个全能的证明者 ([10])。自那时以来，他们和其他人（例如 [3]，[5]）已经考虑一个证明者和验证者具有相同计算资源的模型，证明者的唯一优势是，他恰好知道难题的特定实例 x 的证明 w，这可能是因为他同时构造了 x 和 w。这个模型，连同所有 NP 集合都具有零知识证明 ([4],[11])，构成了将多方协议“编译”为“被验证”协议的基础（[7], [11]）。因此，重要的是要意识到，这个模型只有，有效程序可以生成比验证者能解决的更难的实例时，才有意义。

许多 NP 完全集具有明显的、简单的生成方案。例如，n 个顶点上的哈密顿图可以通过选择一个随机线路，然后以 1/2 的概率独立地添加其他可

能的边来生成。生成一个特定图的概率与它所具有的哈密顿回路的数量成正比。然而，下面的示例表明，生成可解决实例的一些自然方法并不安全。第一种方法由一个非常简单的算法破解; 第二个可以通过复杂的技术来破解。

示例：3SAT。一个 3SAT 实例是一组变量 $U = \{u_1, u_2, \ldots, u_n\}$ 和一组子句 $C = \{c_1, c_2, \ldots, c_m\}$，其中每个子句由三个变量组成。问题是: 是否存在一个真值分配，满足 C。(见 [8] 中的定义)

生成可解决的 3SAT 实例的“自然”方法如下。从 2^n 种可能性中均匀地选择一个真值赋值 t。对于 1 到 m 之间的每个 i，均匀随机选择三个不同的变量; 在与这些变量对应的八组字中，有七组在 t 下为真。从这七组中均匀随机地选择子句 c_i。该方案以相等的概率产生由 t 满足的 m 个子句组成的每个集合 C。

如果子句 m 的数量足够大，一个多项式时间对手可以高概率地重构 t。基本观察是，如果 $t(u_i) = TRUE$，则

$$\frac{Pr(u_i \in c_j)}{Pr(\bar{u_i} \in c_j)} = \frac{4}{3}, \text{对于每个 i 和 j}$$

因此，如果 rn 2 kn In n 对于一个合适的常数 k，那么对于每个 i，以概率 1 - o(1) 同时，文字 ui 出现在 C 中的次数比文字 Ti 多，如果且仅如果 t(u;) = TRUE。

可以尝试通过在每个子句中选择文字，使得至少有一个是 FALSE，至少有一个是 TRUE，来改进这个生成方案。然后，每个子句中文字的期望数量是：标题：Subset Sum 问题的生成方案

正文：

300 个 ui 的出现次数等于 ui 的预期出现次数，对于所有 i。然而，如果 m 1 kn2 Inn 通过观察变量对统计数据，改进的方案可以很容易地被破解。

示例：子集和。子集和实例包括一个有限集合 A = al, a2, ..., an 的正值整数和一个正值整数 M。问题是是否存在一个集合 A C A，其和等于 M。子集和问题的困难在于背包类型公钥论证。

可以生成已解决的子集和实例如下。选择一个零和一组成的向量 e = (el, ..., en)，均匀随机地。固定一个正值整数 B。每个 ai f A 均匀随机地从 1,2, ..., B 中选择。让 A4 = -aiei。

这种生成方案可以用 Lagarias 和 Odlyzko 的算法破解 ([lS])。如果 B 足够大，那么每个实例几乎肯定可以通过他们巧妙地应用 LLL 基础简化算法来解决。

在下面的第 3 节中，我们将精确地定义一个生成方案是不可破解的。然后，我们证明了一个完备性定理，该定理指出，如果 NP 中的任何集合有一个不可破解的生成器，那么 SAT 有一个。特别是，在二次剩余假设、离散对数假设或因子分解假设下，可以生成一个 SAT 的困难分布。这并不令人惊讶。更有趣的是，即使所有这些假设都被证明是错误的，只要能生成 NP 中任何集合的困难分布，仍然可以生成一个 SAT 的困难分布。我们为 SAT 构建的不可破解生成器任何可能的 NP 集合生成器中存在的不可破解性，并不假设它知道不可破解性来自（正如它如果通过乘以不同的素数（如 [6] 等）来构建困难实例，就会假设的那样）。3 节还包含了一个增强定理，展示了如何增强任何可生成的分布的不可破解性，以及一个相对化定理——存在不可破解的生成器显然意味着 $P \neq NP$，但反向不能通过相对化技术来证明。

在第 4 节中，我们简要讨论了哪些集合可以被生成的更一般问题。各种形式的这些假设在密码学文献中无处不在（参见，例如 [l]，[Z]，[9]，[23]），对于这种非正式讨论，不需要精确地陈述它们。对于我们的目的来说，重要的是指出，这些数论问题的实例可以在随机多项式时间内生成，并且广泛地假设，对于这三个问题中的每一个，对于任何常数比例，对于所有足够大的 n，每个多项式时间算法都未能解决该常数比例的实例长度。301 根据哪些分布，考虑一些相关的工作，并提出了未来研究的方向。第 2 部分包含在论文其余部分中广泛使用的术语和符号。为了节省空间，我们推迟了全文的完整证明，尽可能地给出一些关键点的概要。

II 致谢

感谢 Mike Foster、Steve Mahaney、Steven Rudich 和 Mihalisakakis 的有益讨论我们特别感谢 Laura Sanchis。

参考文献

[I) M. Blum and S. Micali. “HOWto Generate Cryptographically Strong Sequences of Pseudo-random Bits,”SIAM J. on Comput. (13), 1984, 850-864.

[2] R. Boppana and R. Hirschfeld. “Pseudorandom Generators and Complexity Classes,” to appear in Advances in Computer Research, Silvio

Micali (ed.),JAI Press (pub.), 1987.

[3] G. Brassard and C. Cripeau. "Non-transitive Transfer of Confidence: A Perfect Zero-Knowledge Interactive Protocol for SAT and Beyond," Proceedings of the 27 th FOCS, IEEE, 1986, 188-195.

[4] G. Brassard and C. Crkpeau. "Zero-KnowledgeSimulation of Boolean Circuits,"Ad- vances in Cqptology -CRYPT086 Proceedings, Andrew Odlyzko (ed.), Springer- Verlag (pub.), 1987, 223-233.

[5] G. Brassard, D. Chaum, and C. CrCpeau. "Minimum Disclosure Proofs of Knowl- edge," to appear.

[6] U. Feige, A. Fiat, and A . Shamir. "Zero Knowledge Proofs of Identity,'' Proceedings of the lgth STOC, ACM, 1987, 210-217.

[7] 2. Galil, S. Haber, and M. Yung. "Cryptographic Computation: Secure Fault- Tolerant Protocols and the Public-Key Model," Advances in Crytology - CRYPT087 Proceedings, Carl Pomerance (ed.), Springer-Verlag (pub.), 1988, 135- 155.

[8] M. Garey and D. Johnson. Computers and Intractability: A Guide to the Theory of N P - Completeness, Freeman, San Francisco, 1979.

[9] S. Goldwasser and S. Micali. "Probabilistic Encryption," JCSS (28), 1984, 270-299.

[10] S. Goldwasser, S. Micali, and C . Rackoff. "The Knowledge Complexity of Interactive Proof Systems," t o appear in SIAM J. on Comput.

[11] 0. Goldreich, S. Micali, and A. Wigderson. "Proofs that Yield Nothing but their Validity and a Method of Cryptographc Protocol Design," Proceedings of the 27 th FOCS, IEEE, 1986, 174-187.

[12] Y. Gurevich. "Complete and Incomplete Randomized N P Problems," Proceedings of the 28th FOCS, IEEE, 1987, 111-117.

[13] J. Hartmanis. "Generalized Kolmogorov Complexity and the Structure of Feasible Computations,"Proceedings of the 24th FOCS, IEEE, 1983, 439445.

[14] M. Jerrum, L. Valiant, and V. Vazirani. ''Fbndom Generation of Combinatorial Structures from a Uniform Distribution," TCS (43), 1986, 169-188.

[15]D. Johnson. "The NP-Completeness Column, An Ongoing Guide,"

JOA (5) , 1984, 284-299.

[16]J. Lagarias and A. Oldlyzko. "Solving Low-Density Subeet Sum Problems," JACM (32), 1985, 229-246.

[17] L. Levin. "Average Case Complete Problems," SIAM J. on Comput. (15), 1986, 285-286.

[18] R. Rardin, C . Tovey, and M. Pilcher. "Polynomial Constructability and Traveling Salesman Problems of Intermediate Complexity," ONR-URI Computational Com- binatorics Report CC-88-2, Purdue University, November, 1988.

[19] S. Rudich, private communication.

[20] L. Sanchis and M. Fulk. "Efficient Language Instance Generation" , University of Rochester Computer Science Department TR 235, 1988.

[21] L. Sanchis. "Test Instance Construction for NP-hard Problems," University of Rochester Computer Science Department TR 206, 1987.

[22] R. Venkatesan and L. Levin "Random Instances of a Graph Coloring Problem are Hard," Proceedings of the 20th STOC, ACM, 1988,217-222.

(231 A. C. Yao. "Theory and Applications of Trapdoor Functions," Proceedings of the 23^{rd} FOCS, IEEE, 1982, 80-91.