

The Tale of One-Way Functions

Leonid A. Levin
Institut Des Hautes Etudes Scientifiques*

*All the king's horses, and all the king's men,
Couldn't put Humpty together again.*

Abstract

The existence of one-way functions (owf) is arguably the most important problem in computer theory. The article discusses and refines a number of concepts relevant to this problem. For instance, it gives the first combinatorial complete owf, *i.e.*, a function which is one-way if any function is. There are surprisingly many subtleties in basic definitions. Some of these subtleties are discussed or hinted at in the literature and some are overlooked. This article attempts a unified approach.

1 Intro I: Inverting Functions.

From time immemorial, humanity has gotten frequent, often cruel, reminders that many things are easier to do than to reverse. When the foundations of mathematics started to be seriously analyzed, this experience immediately found a formal expression.

1.1 An Odd Axiom.

Over a century ago George Cantor reduced all the great variety of math concepts to just one—the concept of sets—and derived all math theorems from just one axiom scheme—Cantor's Postulate.

For each set-theoretical formula $A(x)$ it postulates the existence of a set containing those and only those x satisfying A . This axiom looked a triviality, almost a definition, but was soon found to yield more than Cantor wanted, including contradictions. To salvage its great promise, Zermelo, Fraenkel, and others pragmatically replaced Cantor's Postulate with a collection of its restricted cases, limiting the types of allowed properties A . The restrictions turned out to cause little inconvenience and precluded (so far) any contradictions; the axioms took their firm place in the foundation of math.

In 1904 Zermelo noticed that one more axiom was needed to derive all known math, the (in)famous Axiom of Choice: every function f has an inverse g s.t. $f(g(x)) = x$ for x in the range of f . It was accepted reluctantly; to this day proofs dependent on it are being singled out. Its strangeness was not limited to going beyond Cantor's Postulate—it brought paradoxes! Allow me a simple illustration.

Consider the additive group $\mathbb{T} = \mathbb{R}/\mathbb{Z}$ of reals mod 1 as points $x \in [0, 1)$ on a circle; take its subgroup $\mathbf{Q}_{10} \subset \mathbb{T}$ of decimal fractions $a/10^b$. Let $f(x)$ be the (countable) coset $x + \mathbf{Q}_{10}$, *i.e.*, f projects \mathbb{T} onto its factor group $\mathbb{T}/\mathbf{Q}_{10}$. Any inverse g of f then selects one representative from each coset. Denote by $G = g(f(\mathbb{T}))$ the image of such a g ; then each $x \in \mathbb{T}$ is brought into G by exactly one rational shift $x + q$, $q \in \mathbf{Q}_{10}$. Now I will deviate from the standard path to emphasize the elementary nature of the paradox. One last

*on leave from Boston University, Computer Sci. dept., 111 Cummington St., Boston, MA 02215; email: Lnd@bu.edu. This research was partially conducted by the author for the Clay Mathematics Institute and supported by NSF grant CCR-9820934.

notation: $q' = (10q \bmod 1)$ is $q \in \mathbf{Q}_{10}$, shortened by the removal of its most significant digit.

For a pair $p, q \in \mathbf{Q}_{10}$, I bet 2:1 that $x+p$ rather than $x+q$ falls in G for a random $x \in \mathbb{T}$. The deal should be attractive to you since my bet is higher while conditions to win are completely symmetric under rotation of x . To compound my charitable nature to its extreme, I offer such bets for all $q \in \mathbf{Q}_{10}, p = q'$, not just one pair. If you rush to accept, we choose a random x by rolling dice for all its digits and find the unique $\mathbf{q} \in \mathbf{Q}_{10}$ for which $x+\mathbf{q} \in G$. Then I lose one bet for this \mathbf{q} and win ten (for each q such that $q' = \mathbf{q}$). Generosity pays!

This paradox is not as easy to dismiss as is often thought. Only 11 bets are paid in each game: no infinite pyramids. Moreover, if x is drawn from a sphere S_2 , a finite number of even unpaid bets suffices: [Banach, Tarski, 24] construct 6 pairs, each including a set $A_i \subset S_2$ and a rotation T_i ; betting $x \in A_i$ versus $T_i(x) \in A_i$, they lose one bet and win two for each x . Our $x+p$ and $x+q$ above are tested for the same condition and differ in finitely many digits whose finitely many combinations are equally distributed, given any string of less significant digits of x . One can refuse the thought experiment of rolling the infinite number of digits of x or the question of whether $x+q \in G$, but this amounts to rejecting basic concepts of set theory. It is simpler to interpret the refusal to bet as a hidden disbelief in the Axiom of Choice.

1.2 Finite objects: exhaustive search.

These problems with inverting functions have limited relevance to computations. The latter deal with finite objects which are naturally well-ordered by Induction Axiom, rendering the Axiom of Choice unnecessary. There are other mitigating considerations. Shannon Information theory says a random variable x has as much information about a function $f(x)$ of it as $f(x)$ has about x . Kolmogorov Information theory extended the concept to arbitrary x , not necessarily

random: $I(x : y)$ is the difference between the smallest lengths of programs generating y and of those transforming x to y . Kolmogorov and I proved in 1967 that this quantity is, like Shannon's, symmetric too, albeit approximately [38].

The proof involved a caveat: computationally prohibitive exhaustive search of all strings of a given length. For instance, the product pq of two primes contains as much, i.e. all, information about them as vice versa, but [RSA] and a great many other things in modern cryptography depend on the assumption that recovering the factors of pq is infeasible. Kolmogorov suggested at the time that this information symmetry theorem may be a good test case to prove that for some tasks exhaustive search cannot be avoided (in today's term $P \neq NP$).

The RSA application marked a dramatic twist in the role of the inversion problem: from notorious troublemaker to priceless tool. RSA was the first of the myriad bewildering applications which soon followed. At heart of many of them was the discovery that the hardness of every one-way function $f(x)$ can be focused into a *hard-core* bit, i.e., an easily computable predicate $b(x)$ which is as hard to determine from $f(x)$, or even to guess with any noticeable correlation, as to recover x completely. [Blum, Micali, 82] found the first hard-core for $f(x) = a^x \bmod p$, which was soon followed with hard-cores for RSA and Rabin's function $(x^2 \bmod n)$, $n = pq$, and for "grinding" functions $f^*(x_1, \dots, x_n) = f(x_1), \dots, f(x_n)$ of [Yao 82]¹. [Goldreich, Levin, 89] proved the general case.

The importance of such hard-cores comes from their use, proposed in [Blum, Micali], [Yao] for deterministic generation of an unlimited flow of perfectly random bits from a small random seed s . In the case of permutation f , such generators are straightforward $g_s(i) = b(f^i(s))$; the general case was worked out in [Hastad, Impagliazzo, Levin, Luby, 99]. With the barrier between random and deterministic processes thus broken,

¹See [23] for the proof of Isolation Lemma need for the argument.

many previously unthinkable feats were demonstrated in the 80s. Generic cryptographic results, such as [Blum Goldwasser 82], [Young, Naor, 89], zero-knowledge proofs and implementation of arbitrary protocols between distrusting parties (*e.g.*, card games) as full information games [Goldreich, Micali, Wigderson, 91] are just some of the many famous examples. This period was truly a golden age of Computer Theory brought about by the discovery of the use of one-way functions.

2 Intro II: Extravagant Models.

2.1 The Downfall of RSA.

This development was all the more remarkable as the very existence of one-way (*i.e.*, easy to compute, infeasible to invert) functions remains unproven and subject to repeated assaults. The first came from Adi Shamir himself, the “S” in RSA. [Shamir, 79] proved that factoring (on infeasibility of which RSA depends) can be done in polynomial number of arithmetic operations. This result uses a so-called “unit-cost model” which charges one unit for each arithmetic operation, however long the operands. Squaring a number doubles its length, repeated squaring brings it quickly to cosmological sizes. Embedding a huge array of ordinary numbers into such a long one allows one arithmetic operation to replace a much work, *e.g.*, checking exponentially many factor candidates. The closed-minded cryptographers, however, were not convinced and this result brought a dismissal of the unit-cost model, not RSA:-).

Another, not dissimilar, attack is raging this very moment. It started with the brilliant result of Peter Shor. He factors integers in polynomial time using an imaginary analog device, Quantum Computer (QC), inspired by the laws of Quantum physics taken to their extreme.

2.2 Quantum Computers.

QC has n interacting elements called q-bits. A pure state of each is a unit vector on the complex plane \mathbb{C}^2 . Its projections on the two axes are quantum amplitudes of its two boolean values. A state of the entire machine is a vector in the tensor product of n planes. Its 2^n coordinate vectors are tensor-products of q-bit basis states, one for each n -bit combination. The machine is cooled, isolated from the environment nearly perfectly, and initialized in one of its basis states representing the input and empty memory bits. The computation is arranged as a sequence of perfectly reversible interactions of the q-bits, putting their combination in the superposition of a rapidly increasing number of basis states, each having an exponentially small amplitude. The environment may intervene with errors; the computation is done in an error-correcting way, immune to such errors as long as they are few and of special restricted forms. Otherwise, the equations of Quantum Mechanics are obeyed with unlimited precision. This is crucial since the amplitudes are exponentially small and deviations in remote (hundredth or even millionth) decimal places would overwhelm the content completely. In [Shor, 97] such computers are shown capable of factoring in polynomial time. The exponentially many coordinates of their states can, roughly speaking, explore one potential factor each and concentrate the amplitudes in the one that works.

2.3 Small Difficulties.

There are many problems with such QC-s, though. For instance, thermal isolation cannot be perfect. Tiny backgrounds of neutrinos, gravitational waves, and other exotics, cannot be shielded. Their effects on quantum amplitudes need not satisfy the restrictions on which error-correcting tools depend. Moreover, non-dissipating computing gates, even classical, remain a speculation. Decades past, their exis-

tence was cheerfully proclaimed and even proven for worlds where the laws of physical interaction can be custom-designed. In our world, were the electromagnetic interaction between electrons, nuclei, and photons is about the only one readily available, circuits producing less entropy than computing remain hypothetical. So, low temperatures have limits and even a tiny amount of heat can cause severe decoherence problems. Furthermore, the uncontrollable degrees of freedom need not behave simply like heat. Interaction with the intricately correlated q-bits may put them in devilish states capable of conspiracies which defy imagination.

2.4 Remote Decimals.

All such problems, however, are peanuts. The major problem is the requirement that basic quantum equations hold to multi-hundredth if not millionth decimal positions where the significant digits of the relevant quantum amplitudes reside. We have never seen a physical law valid to over a dozen decimals. Typically, every few new decimal places require major rethinking of most basic concepts. Are quantum amplitudes still complex numbers to *such* accuracies or do they become quaternions, colored graphs, or sick-humored gremlins? I suspect physicists would doubt even the laws of arithmetic pushed that far :-). In fact, we know that the most basic laws cannot all be correct to hundreds of decimals: this is where they stop being consistent with each other!

And what is the physical meaning of 500 digit long numbers? What could one possibly mean by saying “This box has a remarkable property: its many q-bits contain the Ten Commandments with the amplitude whose first 500 decimal places end with 666”? What physical interpretation could this statement have even for just this one amplitude? Close to the tensor product basis one might have opportunities to restate the assertions using several short measurable numbers instead of one long. Such op-

portunities may also exist for large systems, such as lasers or condensates where individual states matter little. But QC factoring uses amplitudes of an exponential number of highly individualized basis states. I doubt anything short of the most generic and direct use of these huge precisions would be easy to substitute. One can make the amplitudes more “physical” by choosing a less physical basis. Let us look into this.

2.5 Too Small Universe.

QC proponents often say they win either way, by making a working QC or by finding a correction to Quantum Mechanics. *e.g.*, in [33] Peter Shor says: “If there are non-linearities in quantum mechanics which are detectable by watching quantum computers fail, physicists will be VERY interested (I would expect a Nobel prize for conclusive evidence of this).”

Consider, however, this scenario. With few q-bits, QC is eventually made to work. The progress stops, though, long before QC factoring starts competing with ordinary PCs. The QC people then demand some noble prize for the correction to the Quantum Mechanics. But the committee wants more specifics than simply a non-working machine, so something like observing the state of the QC is needed. Then they find the Universe too small for observing individual states of the needed dimensions and accuracy. (Raising sufficient funds to compete with paper and pencil factoring may justify a Nobel Prize in Economics :-).

Let us make some calculations. In cryptography the length n of the integers to factor may be a thousand bits (and could easily be millions.) By $\sim n$ I will mean a reasonable power of n . A $2^{\sim n}$ dimensional space H has $2^{2^{\sim n}}$ roughly different vectors. Take a generic $v \in H$. The minimal size of a machine which can recognize or generate v (approximately) is $K = 2^{\sim n}$ —far larger than our Universe. This comes from a cardinality argument: $2^{\sim K}$ machines of K atoms. Let us call such v “mega-states”.

There is a big difference between untested and untestable regimes. Claims about individual mega-states are untestable. I can imagine a feasible way to separate any *two* QC states *from each other*. However, as this calculation shows, no machine can separate a generic QC state from the set of all states more distant from it than QC tolerates. So, what thought experiments can probe the QC to be in the state described with the accuracy needed? I would allow to use the resources of the entire Universe, but *not more*!

Archimedes made a great discovery that digital representation of numbers is exponentially more efficient than analog ones (sand pile sizes). Many subsequent analog devices yielded unimpressive results. It is not clear why QCs should be an exception.

2.6 Metric versus Topology.

A gap in quantum formalism may be contributing to the confusion. Approximation has two subtly different aspects: metric and topology. Metric tells how close is our ideal point to a specific wrong one. Topology tells how close it is to the combination of all unacceptable (non-neighboring) points. This may differ from the distance to the closest unacceptable point, especially for quantum systems.

In infinite dimensions the distinction between 0 and positive separation varies with topologies. In finite dimensions 0-vs.-positive distinction is too coarse: all topologies agree. Since 2^{500} is finite only in a very philosophical sense, one needs a quantitative refinement, some sort of a weak-topological (not metric) *depth* of a neighborhood polynomially related to resources required for precision to a given depth. Then, precision to reasonable depths would be physical, *e.g.*, allow to generate points inside the neighborhood, distinguish its center from the outside, etc.

Metric defines ε -neighborhoods and is richer in that than topology where the specific value of ε is lost (only $\varepsilon > 0$ is assured). However, metric is restricted by the axiom that the in-

tersection of any set of ε -neighborhoods is always another ε -neighborhood. Quantum proximity may require both benefits: defined depth ε and freedom to express it by formulas violating the “intersection axiom”. Here is an example of such violation, without pretense of relevance to our needs. Suppose a neighborhood of 0 is given by a set of linear inequalities $f_i(x) < 1$; then its depth may be taken as $1/\sum_i \|f_i\|$. Restricting x to the unit sphere would render this depth quadratically close to metric depth. A more relevant formula may need preferred treatment of tensor product basis.

2.7 The Cheaper Boon.

QC of the sort that factors long numbers seems firmly rooted in science fiction. It is pity that popular accounts do not distinguish it from much more believable ideas, like Quantum Cryptography, Quantum Communications, and the sort of Quantum Computing that deals primarily with locality restrictions, such as fast search of long arrays. It is worth noting that the reasons why QC must fail are by no means clear; they merit thorough investigation. The answer may bring much greater benefits to the understanding of basic physical concepts than any factoring device could ever promise. The present attitude is analogous to, say, Maxwell selling the Daemon of his famous thought experiment as a path to cheaper electricity from heat. If he did, much of insights of today’s thermodynamics might be lost or delayed.

The rest of the article ignores any extravagant models and stands fully committed to the Polynomial Overhead Church-Turing Thesis: Any computation that takes t steps on an s -bit device can be simulated by a Turing Machine in $s^{O(1)}t$ steps within $s^{O(1)}$ cells.

3 The Treacherous Averaging.

Worst-case hardness of inverting functions may bring no significant implications. Imagine that

all instances come in two types: “easy” and “hard”. The easy instances x take $\|x\|^2$ time. An exponential expected time is required *both* to solve, *and to find* any hard instance. So, the Universe would be too small to ever produce instances that it is too small to solve, and the inversion problem would pose no practical difficulty. It is “generic”, not worst-case, instances that both frustrate algorithm designers and empower cryptographers to do their incredible feats. The definition of “generic,” however, requires great care.

3.1 Las Vegas Algorithms.

First we must agree on how to measure the performance of inverters. Beside instances $x = f(w)$, algorithms $A(x, \alpha)$ inverting one-way functions f can use random dice sequences $\alpha \in \{0, 1\}^N$. They never need a chance for (always filterable) wrong answers. So we restrict ourselves to *Las Vegas* algorithms which can only produce a correct output, abort, or diverge.

For any given instance x , the performance of an algorithm A has two aspects: the volume² V_α of computation (depending on the internal dice α) and the chance p of success. The two measures are not independent: the chance $p \ll 1$ can be always boosted while roughly preserving p/V by simply running A on several independent α . This idea suggests the popular requirement that Las Vegas algorithms be normalized to, say, $p \geq \frac{1}{2}$. The problem with this restriction is that estimating p and the needed number of trials may require exponential volume overhead in the worst case. Thus, only such measures as average volume can be kept reasonable while normalizing the chance. It is important that both are averaged only over A ’s own dice α ; the instance x is chosen by the adversary. In this setting the duplicity of performance aspects does become redundant: p and average volume are freely interchangeable (to shrink the latter,

²I say *volume* rather than *time*, for greater robustness in case of massively parallel models.

one simply runs A with a small chance).

Combining several runs into one lessens the modularity and counting the runs needed does involve some overhead. However, there are more substantial reasons to prefer normalization of average volume to that of the success rate p . In some settings, success is a matter of degree. For instance, different inverses of the same instance of a owf may be of different and hard to compare value. Normalizing the average volume, on the other hand, is robust. This volume bound may be $O(1)$ if the model of computation is very specific. If flexibility between several reasonable models is desired, polynomial bounds, specific to each algorithm, may be preferable. There is one obstacle: the set of algorithms with a restricted expected complexity is not recursively enumerable. We can circumvent this problem by using the following enforceable form of the bound.

Definition 1 *Las Vegas algorithms* $A(x, \alpha)$ *start with a given bound* $b(x)$ *on expected computation volume. We denote this* $A \in LV(b)$, *doubling the meaning of* V *as “Vegas” and “volume”. At any time the algorithm can bet a part of the remaining volume, so that it is doubled or subtracted depending on the next dice. $LV(O(1))$ usually suffices and we will abbreviate it as* L .³

Despite its tight $O(1)$ expected complexity bound, L is robust since any Las Vegas algorithm can be put in this form, roughly preserving the ratio between complexity bound and success rate. The inverse of the latter gives the number of runs required for a constant chance of success, thus playing the role of running time. An extra benefit is that a reader adverse to bothering with the inner workings of computers can just

³Pronounced “Las” algorithms to hint at Las Vegas, the term’s inventor Laszlo Babai, and the Spanish definite article :-). I would like to stress that no YACC (Yet Another Complexity Class) is being introduced here. L is a *form* of algorithms; this is much less abstract than a class of algorithms or, especially, a class of problems solvable by a class of algorithms. Besides, it is not really new, just a slight tightening of the Las Vegas restriction.

accept their restriction to L and view all further analysis in purely probabilistic terms!

3.2 Multi-Median Time.

Averaging over the instance x is, however, much trickier. It is not robust to define generic complexity of an algorithm $A(x)$ running in $t(x)$ steps as its expected time $\mathbf{E}_x t(x)$. A different device may have a quadratic time overhead. For instance, reversing an input string requires quadratic time on a Turing machine with one tape, but only linear time with two tapes. It may be that a similar overhead exists for much slower algorithms, too. Then $t(x)$ may be, say, $\|x\|^2$ for $x \notin 0^*$, while $t(0\dots 0)$ may be $2^{\|x\|}$ for one device and $4^{\|x\|}$ for another. Take x uniformly distributed on $\{0,1\}^n$. Then $\mathbf{E}_x t(x)$ for these devices would be quadratic and exponential respectively: averaging does not commute with squaring. Besides, this exponential average hardness is misleading, since the hard instances would never appear in practice!

More device-independent would be the *median* time, the minimal number of steps spent for the *harder half* of instances. This measure, however, is not robust in another respect: it can change dramatically if its *half* threshold is replaced with, say, a *quarter*.

Fortunately these problems disappear as one of the many benefits of our Las Vegas conventions. One can simply take algorithms in L and measure their chance of success for inputs chosen randomly with a given distribution. The inverse of this chance, as a function of, say, input length is a robust measure of *security* of a one-way function. This measure is important in cryptography, where any noticeable chance of breaking the code must be excluded. A different measure is required for positive tasks aimed at success for almost all instances. We start by considering a combined distribution over all instance lengths.

Definition 2 *We consider an L-distribution of instances, i.e., a distribution of an L-algorithm's*

*outputs on empty input.*⁴ *Now, we run the generator k times (spending, an average time of $O(k)$) and apply the inverter until all generated solvable instances are solved.*⁵ *The number of trials is a random variable depending on the inverter's dice. Its median value $MT(k)$ we call the multi-median time of inverting f by A .*

This measure is robust in many respects. It commutes with squaring of the inverter's complexity and, thus, is robust against variation of models. It does not depend much on the $\frac{1}{2}$ probability cut-off used for median. Indeed, increasing k by a factor of c raises $MT(k)$ as much as does tightening the inverter's failure probability to 2^{-c} .

MT is relevant for both upper and lower bounds. Let $T(x)$ be high for ε fraction of $x \in \{0,1\}^n$. Then $MT(k)$ is as high for $k = n^3/\varepsilon$. Conversely, let $MT(k)$ be high. Then, with overwhelming probability, $T(x_i)$ is at least as high for some of $n = k^2$ random x_1, \dots, x_n (and $\sum_i \|x_i\| = O(n)$).

3.3 Nice Distributions.

So far, we addressed the variance of performance of a randomized algorithm over its variable dice for a fixed input, as well as the issue of averaging it over variable input with a given distribution. Now we must address the variance of distributions. Choosing the right distributions is not always trivial, a fact often dismissed by declaring them uniform. Such declarations are confusing, though, since many different distributions deserve the name.

For instance, consider graphs $G = (V, E \in V^2)$, $\|V\| = n$, where n is chosen with probability $\theta(1)/n^2$. For a given n , graphs G are chosen with two distributions, both with a claim to

⁴If the instance generator is not algorithmic, the definition can be modified to use the output length instead of complexity in the definition of L. The instances of length n should have probabilities combining to a polynomial, e.g., $\theta(1)/(n \log n)^2$.

⁵If the generator can produce unsolvable instances too, the definition ignores them.

uniformity: μ_1 chooses G with equal probability among all 2^{n^2} graphs; μ_2 first chooses $k = \|E\|$ with uniform probability $1/n^2$ and then G with equal probability among all the $C_{n^2}^k$ candidates. The set $\{G : k = n^{1.5}\}$ has then μ_2 probability $1/n^2$, while its μ_1 is exponentially small. In fact, all nice distributions can be described as uniform in a reasonable representation. Let me reproduce the argument sketched briefly in [22] adding an additional aspect I will use later.

Let us use set-theoretic representation of integers: $n = \{0, 1, \dots, n-1\}$. A measure μ is an additive real function of *sets* of integers; $\mu(n) = \mu(\{0\}) + \mu(\{1\}) + \dots + \mu(\{n-1\})$ is its monotone *distribution* function. Its *density* $\mu'(n) = \mu(n) - \mu(n-1) = \mu(\{n\})$ is the probability of $\{n\}$ as a singleton, rather than of a set $n = \{0, 1, \dots, n-1\}$. Let \mathbf{Q}_2 be the set of binary fractions $i/2^{\|i\|} \in [\frac{1}{2}, 1)$. We round the real-valued μ to \mathbf{Q}_2 , keeping only as many binary digits as needed for constant factor accuracy of probabilities.

Definition 3 $\mu : \mathbb{N} \rightarrow \mathbf{Q}_2$ is perfectly rounded if $\mu(x)$ is the shortest fraction within $(\mu(x-1), \mu(x+1))$ interval and $-\log \mu(\{x\}) = O(\|x\|)$.

The last condition is just a convenience and can be met simply by mixing the (monotone) μ with some simple distribution.

Lemma 1 Each computable $\mu : \mathbb{N} \rightarrow \mathbf{Q}_2$ can be uniformly transformed into a perfectly rounded μ_1 computable with at most $\|x\|$ factor slow-down so that $\mu'_1 \geq \mu'/4$ for increasing μ (i.e., if $\mu' > 0$).

Monotonicity is assured by comparing $\mu(x)$ with $\mu(y)$, for prefixes y of $x \in \mathbf{Q}_2$. Then the claim can be achieved by rounding. First, round $\mu(x)$ to the shortest binary p that is closer to it than to any other $\mu(y)$ and call these rounded values *points*. Find all *slots*, i.e., closest to p shorter binary fractions of each binary length. Then, for each slot in order of increased lengths, find the point that fills it in the successive roundings until the slot for x is found.

All perfectly rounded μ have a curious property: both $m(x) = \mu(x)/\mu(\{x\})$ and $-\log \mu(\{x\}) = \|m(x)\|$ are always integers, making $\mu(x) = .m(x) \in \mathbf{Q}_2$. So m is quite uniformly distributed: $2k\mu(m^{-1}(k)) \in [1, 2]$ for $k \in m(\mathbb{N})$. It is also computable in polynomial time, as is m^{-1} (by binary search). So, we can use $m(x)$ as an alternative representation for x in which the distribution μ is remarkably uniform.

Simple distributions are not normally general enough. They may be the ultimate source of the information in the instances x of our problems, but the original information r is transformed into x by some process A that may itself be something like a one-way function. We can assume that A is an algorithm with a reasonable time bound, but not that its output distribution is simple. Such distributions are called *samplable*. [Impagliazzo, Levin, 90] deals with samplable distributions in a similar manner as with those in this section, though through a different trick.

4 Completeness.

4.1 Complete Distributions and Inverters.

Given a function to invert, how would one generate hard instances? There are two aspects of the problem. The first is achieving a significant probability that the instance generated is hard. The second is keeping the probability of easy instances negligible. A number of reductions (with various limitations) exist between these tasks. Let us restrict our attention to the first one.

First, note that Lemma 1 enumerates all distributions computable in time $t(x)$ preserving t within a linear factor. Thus, we can generate the largest of all these distributions by adding them up with summable coefficients, say $1/i^2$. This distribution will be complete for $\text{TIME}(t(x))$ and belong to $\text{TIME}(t(x)\|x\|)$. A nice alternative would be to combine all complexities by translating high times into small probabilities, similarly

to section 3.1. Instead, we will switch to samplable distributions directly.

Definition 4 *Distributions generated by algorithms in L without input we call samplable. If the algorithm has inputs, they are treated as a parameter for a family of samplable distributions.*

Usual versions of this definitions are broader, allowing algorithms closer to $LV(P)$. They give probabilities at most polynomially larger; our definitions limits the generators to L for greater precision.

Proposition 1 *There exists a complete, i.e., largest up to constant factors, family of samplable distributions.*

The lemma follows if we note that L is enumerable and, thus, the complete distribution can be obtained by choosing members of L at random and running them. The generator of this distribution spends $O(1)$ average time per run and has the greatest (up to a constant factor) in L capacity for generating surprises. (Compared to $LV(P)$ algorithms, its chance of a nasty surprise may be polynomially smaller.)

Since the complete distribution makes sense only to within a constant factor, it is robust only in logarithmic scale and defines an objective hardness of “hitting” a set X given x .

Notation 1 *By $Kl(X/x)$, we denote $-\log$ of probability of a set X under the complete distribution family parameterized by x .*

As happens often, a strong attack tool helps inventing a strong defense. Optimal searches were noted, *e.g.*, in [20, 21, 3] but here we get a nice version for free. The complete generator of hard instances can be used as an optimal algorithm for solving them. Since algorithms in L combine time into probability, their performance is measured by their chance of success. The generator of optimal distribution family (parameterized by the instance x) has the highest, up to a constant factor, chance $1/S(f/x) =$

$2^{-Kl(f^{-1}(x)/x)}$ of generating solutions. Its minus logarithm $s(f/x)$ measures the hardness of each individual instance x and is called its *security*. The generator takes an $O(1)$ average time per run and succeeds in expected $S(f/x)$ runs. No other method can do better.

Open Problem. The constant factor in the optimal inversion algorithm may be arbitrarily large. It is unknown whether it can be limited to a fixed constant, say 10, independent of the competing algorithm for sufficiently large instances.

4.2 Inversion Problems and OWFs.

A complete distribution achieves about as high probability of hard instances as is possible. Using it makes the choice of a hard to invert function easy: all NP-complete functions would do equally well. However, the interesting goal is usually to find a function that is tough for some standard, say, uniform distribution of instances. Serendipitously, Lemma 1 transforms any P-time distribution into a uniform one via an appropriate encoding. Combined with this encoding, any NP-complete function becomes hardest to invert. However, the encoding would make the function lose all its “prettiness,” so the problem of combining a nice function with a nice distribution remains.

Of course, while many functions seem hard, none are proven to be such. [22], [Venkatesan, Levin, 88], [Impagliazzo, Levin, 90], [Gurevich, 90], [Venkatesan, Rajagopalan, 92], [Wang, 95], and others proved a number of combinatorial and algebraic problems to be complete on average with uniform distributions, *i.e.*, as hard as any inversion problem with samplable distribution could be.

These results, however, do not quite yield owfs. The difference between owf and complete on average inversion problems can be described in many ways. The simplest one is to define owf as hard on average problems of inverting *length preserving* functions. In this case the choice be-

tween picking at random a witness (crucial for owf-s) or an instance, becomes unimportant.

Indeed, each witness gives one instance, so the uniform probability does not increase if length is preserved. On the other hand, if the witnesses are mapped into much fewer hard instances, they must have many siblings. Then, the function can be modified as follows. Guess the logarithm k of the number of siblings of the witness w and pick a random member a of a universal hash family $h_a(w)$. Output $f(w), k, a, h'_a(w)$, where h' is h truncated to k bits. The extra information in the output (if k was guessed correctly) will be nearly random, and so will not make inversion any easier. However, the siblings will be separated into small groups and the numbers (and, thus, uniform probabilities) of hard instances and their witnesses will become comparable. The converse is also true:

Proposition 2 *Any owf with at least $V(k)$ multi-median of its security $S(x)$ (when w is randomly generated and $x = f(w)$) can be transformed into a length preserving owf with a $1/O(k)$ fraction of instances that have security polynomially related to V .*

First, the fraction of hard instances is boosted as described at the end of section 3.2. If the number of hard instances is much smaller than that of their witnesses, the function still can be made length-preserving without altering its hardness. First, the siblings are separated, as in the previous paragraph. Then, the long outputs (instances) are hashed into strings of the same length as the witnesses. See [Impagliazzo, Levin, 90] for more detailed computations of the results of hashing owf-s.

4.3 Complete Owf: Tiling Expansion.

No combinatorial complete owf has been described yet, though [23] shows the existence of an artificial complete owf. It would be nice to have several complete owf-s that are less artificial, *i.e.*, can be described easily to someone who

does not (and does not want to :-) know the definition of computability. Below, such an example is given as a seed. Hopefully, a critical mass of such examples will be achieved some day providing an arsenal for reductions to more popular owf candidates to show their completeness.

We now modify the Tiling Problem to create a complete combinatorial owf.

Tiles: unit squares with a letter at

each corner; may be joined if the letters match. Expansion: maximal tile-by-tile **unique** (using given tiles) extension of a partial tiling of a square with marked border.

a	x	x	c
e	r	r	z
e	r	r	z
n	s	s	z

Definition 5 *Tiling Expansion is the following function: Expand a given top line of tiles to a square using a given set of permitted tiles; output the bottom line and the permitted tiles.*

Theorem 1 *Tiling Expansion is a owf iff owf-s exist.*

It is an interesting open problem to reduce this owf to other nice combinatorial or algebraic owf-s thus proving their completeness.

The raw owf-s, however are hard to use. Many results, such as, *e.g.*, pseudo-random generators require no other assumptions. Such constructions, however, destroy efficiency almost entirely. To be useful, owf need to be nice, *e.g.*, have low Renyi entropy. (Below, $f(x)+ax$ can be replaced with other hashings.)

Note 1 *Inputs of $g(a, x) = (a, f(x) + ax)$ have ≤ 1 siblings on average for any length preserving f and $a, x \in GF_{2^{\|x\|}}$.*

Conjecture 1 *The above g is one-way, for any owf f , and has the same (within a polynomial factor) security.*

References

- [FOCS] *Proceedings of the Annual IEEE Symposium on Foundations of Computer Science.*
- [STOC] *Proceedings of the Annual ACM Symposium on Theory of Computing.*
- [1] S. Banach, A. Tarski. Sur la decomposition des ensembles de points en parties respectivement congruentes. *Fund. Math.* 6, 244-277, 1924.
 - [2] S. Ben-David, B. Chor, O. Goldreich, M. Luby. On the Theory of Average Case Complexity. [STOC], 1989, pp. 204-216.
 - [3] Charles H. Bennett. Logical Depth and Physical Complexity. in: Rolf Herken, ed. *The Universal Turing Machine— a Half-Century Survey*. Oxford University Press 227-257, (1988).
 - [4] Manuel Blum, Silvio Micali. *How to generate cryptographically strong sequences of pseudo-random bits.* *Sicomp*. 13:850-864 (1984).
 - [5] M. Blum, S. Goldwasser. An Efficient Probabilistic Encryption Scheme Hiding All Partial Information. *Crypto*-1982.
 - [6] W. Diffie, M. E. Hellman. New Directions in Cryptography. *IEEE transactions on Info. Theory*, IT-22:644-654, 1976.
 - [7] Oded Goldreich, Russell Impagliazzo, Leonid A. Levin, Ramarathnam Venkatesan, David Zuckerman. Security Preserving Amplification of Hardness. [FOCS] 1990, pp. 318-326.
 - [8] Oded Goldreich, Leonid A. Levin. A Hard-Core Predicate for any One-Way Function. [STOC] pp. 25-32, 1989.
 - [9] O. Goldreich, S. Micali, A. Wigderson. Proofs that Yield Nothing but their Validity. *J.ACM*, 38(3):691-729, 1991.
 - [10] Yuri Gurevich. Average Case Complexity. *Internat. Symp. on Information Theory, Proc.*, IEEE, 1985.
 - [11] Yuri Gurevich. Complete and Incomplete Randomized NP Problems. [FOCS], 1987, pp. 111-117.
 - [12] Yuri Gurevich. The Challenger-Solver game: Variations on the Theme of $P=?NP$ ". *Bull. Europ. Assoc. for Theor. Comp. Sci.*, Oct. 1989, pp. 112-121.
 - [13] Yuri Gurevich. Matrix Decomposition is Complete for the Average Case. [FOCS], 1990.
 - [14] Johan Hastad, Russell Impagliazzo, Leonid A. Levin, Michael Luby. A Pseudorandom Generator from any One-way Function. *SICOMP* 28(4):1364-1396, 1999.
 - [15] Russell Impagliazzo, Leonid A. Levin. No Better Ways to Generate Hard NP Instances than Picking Uniformly at Random. [FOCS] 1990, pp. 812-821.
 - [16] David S. Johnson. The NP-Completeness Column. *J. of Algorithms* 5:284-299, 1984.
 - [17] Richard Karp. The probabilistic analysis of some combinatorial search algorithms. *Algorithms and Complexity*. (J.F.Traub, ed.) Academic Press, NY 1976, pp. 1-19.
 - [18] Donald E. Knuth. The Art of Computer Programming. v.2 *Seminumerical Algorithms*. Addison-Wesley, 3d ed., 1997. Sec. 3.5.F. Also available on pp. 10, 29-36 of <http://www-cs-faculty.stanford.edu/~knuth/err2-2e.ps.gz>.
 - [19] Andrei N. Kolmogorov, Vladimir A. Uspenskii. Algorithms and Randomness. *Theoria Veroyatnostey i ee Primeneniya = Theory of Probability and its Applications*, 3(32):389-412, 1987.

- [20] Leonid A. Levin. Universal Search Problems. *Problems of Information Transmission*. 9(3):265-266, 1973.
- [21] Leonid A. Levin. Randomness Conservation Inequalities. *Information and Control* 61(1):15-37, 1984.
- [22] Leonid A. Levin. Average Case Complete Problems. *SIAM J. Comput.* 15(1):285-286, 1986.
- [23] Leonid A. Levin. One-way functions and pseudorandom generators. *Combinatorica* 7(4):357-363, 1987.
- [24] Leonid A. Levin. Randomness and Non-determinism. *J. Symb. Logic*, 58(3):1102-1103, 1993.
A less technical version:
International Congress of Mathematicians, Zurich, August 1994.
Proceedings (Invited Addresses), pp. 1418-1419. Birkhauser Verlag, 1995.
- [25] G.L.Miller. Riemann's Hypothesis and tests for Primality, *J. Comp. Sys. Sci.* 13(3):300-317, 1976.
- [26] Ming Li, Paul M.B. Vitányi. Introduction to Kolmogorov Complexity and its Applications. Springer Verlag, New York, 1993.
- [27] M. Naor, M. Yung. Universal One-way Hash Functions and Their Applications. [STOC], 1989, pp. 33-43.
- [28] Michael Rabin. *Digitalized Signatures as Intractable as Factorization*. MIT/LCS/TR-212, 1979.
- [29] M.O. Rabin. Probabilistic Algorithms for Testing Primality. *J. Number Theory*, 12:128-138, 1980.
- [30] Ronald L. Rivest, Adi Shamir, Leonard M. Adleman. A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. *CACM* 21(2):120-126, 1978.
- [31] Adi Shamir. Factoring Numbers in $O(\log n)$ Arithmetic Steps. *Information Processing Letters* 8(1):28-31, 1979.
- [32] Peter W. Shor. Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer. *SIComp*. 26(5):1484-1509 (1997).
- [33] Peter W. Shor. "Re: When will quantum computers become practical?" Moderated usenet group *sci.physics.research* article FrsHL0.ILr@research.att.com, 3/22/2000: <http://groups.google.com/groups?ic=1&selm=FrsHL0.ILr%40research.att.com>
The thread can also be retrieved at <http://www.lns.cornell.edu/spr/2000-03/threads.html#0022485>.
- [34] Ramarathnam Venkatesan, Leonid A. Levin. Random Instances of a Graph Coloring Problem are Hard. *STOC*, 1988.
- [35] Ramarathnam Venkatesan, Sivaramakrishnan Rajagopalan. Average case intractability of Matrix and Diophantine Problems. [STOC], 1992 pp. 632-642.
- [36] J. Wang. Average Case Completeness of a Word Problem for Groups.[STOC], 1995, pp. 325-334
- [37] Andrew C. Yao. Theory and applications of trapdoor functions. [FOCS], 1982, pp. 80-91.
- [38] Alexander K. Zvonkin, Leonid A. Levin. The Complexity of finite objects and the Algorithmic Concepts of Information and Randomness. *UMN = Russian Math. Surveys* 25(6):83-124, 1970.