A history of the PCP Theorem

(This is a brief illustrated take on the history of the PCP Theorem, as inferred by the author, Ryan O'Donnell. My main sources were Babai's article Email and the unexpected power of interaction*, Goldreich's article* A taxonomy of proof systems*, and the original sources. Likely there are several inaccuracies and omissions, and I apologize for these and ask for corrections in advance. Since this note was prepared for a class at the University of Washington, a few details relating to UW have also been emphasized.)*

With the exciting new proof of the PCP Theorem by Irit Dinur (April 2005), a course on the PCP Theorem

Irit Dinur

no longer needs to get into many — if any — of the details involved in the original proof. But this original proof and the seven years of work leading up to it form an interesting history that is certainly worth hearing.

The story of the PCP Theorem begins at MIT in the early 1980s, with a paper that would win the first ever Gödel Prize: *The Knowledge Complexity of Interactive Proof Systems*, by Goldwasser, Micali, and Rackoff. This paper was first published in STOC '85. However drafts of it are said to have existed as early

Shafi Goldwasser

Silvio Micali

Charlie Rackoff

as late '82; indeed, it was supposedly cited in at least one paper from '83. The story also goes that this paper was rejected from FOCS '83, STOC '84, and FOCS '84, although it's not clear what form the paper was in for these rejections.

Goldwasser, Micali, and Rackoff were actually interested in the philosophical notion of what it means to prove something, although the main motivation of their paper was cryptographic. This paper introduced two new notions: interactive proofs, and zero-knowledge proofs.

Definition 1 *In an* interactive proof*, a randomized poly-time verifier with private coin tosses interacts with an all-powerful prover; they send messages back and forth in polynomially many rounds. Correct statements should have proofs accepted with probability 1 ("completeness"), and incorrect statements should be rejected, regardless of the proof, with probability at least* $1/2$ *("soundness").*[1] *We let* IP *denote the class of languages*

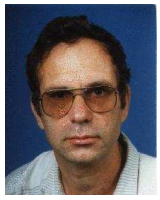
[1] Actually, GMR originally allowed $1 - 2^{-n}$ completeness; this turns out not to matter.

with interactive proofs.

This is the most general notion of efficient proof that GMR could think of; they modeled it on the idea of students in a classroom interacting with a lecturer giving a proof. As for their other notion of zero-knowledge proofs, we won't get into any details here, except to say that whereas in a tradition proof you may "learn" many things about the theorem in addition to the fact that it's true, in an interactive proof it can be possible that you learn "zero additional information" beyond the fact that the theorem is true. GMR's main example was the "quadratic non-residuosity" problem. It is not hard to prove in NP that a number is a quadratic non-residue, by giving the factorization of the modulus as a witness; however this reveals a lot of information. GMR gave a "zero-knowledge" proof of this fact. This is certainly an interesting example of a zero-knowledge proof, but not such an interesting example of an interactive proof, since the problem is already in NP.

Independently of GMR, and published in the same STOC '85, was a paper of Babai, *Trading Group Theory for Randomness*. This paper was later published in journal version as *Arthur-Merlin Games: A Randomized Proof System, and a Hierarchy of Complexity Classes*, with Moran as a coauthor; in fact, this paper shared the first ever Gödel Prize with GMR. Babai had written a previous paper with Szemerédi in

Laci Babai



Shlomo Moran

which he had shown that some certain group theory problems — e.g., for a matrix group over a finite field given by its generators, is its order at most k? — were in NP, subject to some unproven group-theoretic hypothesis. Babai wanted to get an unconditional result, so he independently introduced the notion of

Endre Szemerédi

interactive proofs, albeit with *public* coin tosses, and showed his problem had constant-round interactive proofs. In particular, he gave the following definition:

Definition 2 AM[k] *is the class of interactive proofs that have k rounds, where the verifier speaks first and has public coin tosses. (AM stands for Arthur-Merlin, Arthur being the verifier, Merlin the prover.)*

Babai also showed:

Theorem 1 *For all constant k,* AM[k] = AM[2].

Mike Sipser

The class AM[2] is today known simply as AM. With this definition we see that AM[poly] is very similar to IP; the main difference is in public coins versus private coins. Goldwasser and Sipser soon thereafter (STOC '86) showed that they were the same class. So after this paper, there was a nice, robust class called IP defined, which seemed to capture a liberal notion of languages with efficient proofs.

In fact, the class soon became an intriguing one to complexity theorists, for the following reason: GMR's interactive proof was for something that was already in NP. Babai's proof was for something he suspected was in NP but didn't quite have the group theory to prove. But in FOCS '86 (and actually, the result was known a little before Goldwasser-Sipser), Goldreich, Micali, and Wigerson showed the Graph Non-Isomorphism problem is in IP, and this is a problem people had thought about and tried to put in NP for quite some time.

Definition 3 *Graph Non-Isomorphism is the complement of Graph-Isomorphism: Given are* $G_1 = (V_1, E_1)$ *and* $G_2 = (V_2, E_2)$*, two graphs in adjacency-list format. Are they isomorphic? I.e., is there a renaming of vertices so that they are identical graphs?*

Theorem 2 *(GMW '86) Graph Non-Isomorphism is in IP.*

Proof: The verifier picks $i \in \{1, 2\}$ at random, randomly permutes the vertices of G_i, and presents the resulting graph to the prover. The prover must guess i. For completeness, if the graphs are non-isomorphic then the all-powerful prover can certainly identify i. For soundness, if the graphs are isomorphic then the prover see the same probability distribution on graphs no matter what i is; hence all it can do is guess. □

Oded Goldreich

Avi Wigderson

There weren't any major developments regarding IP for a little while after this, although interactive proofs continued to receive attention in the crypto community. In particular, in STOC '88, to remove

cryptographic assumptions from some results about zero-knowledge proofs, Michael Ben-Or, Goldwasser, Joe Kilian, and Wigderson introduced the notion of multi-prover interactive proofs:

Definition 4 *(BGKW '88.) MIP is the class of interactive proofs with multiple, noncommunicating provers.*

A theorem of BGKW showed that MIP with polynomially many provers is the same as MIP with two provers.


Miki Ben-Or


Joe Kilian

For a little while longer, things stood still with complexity of interactive proofs. Babai had conjectured that IP = AM, and indeed it seems like most people believed that IP (and even MIP) was only a slight randomized extension of NP. From a philosophical point of view, this seems highly reasonable: why should one expect significant additional power from such a reasonable extension of the notion of efficient proof? Fortnow and Sipser in '88 showed that there was an oracle relative to which coNP was not in IP; in the same year Fortnow, Rompel, and Sipser extended this result to MIP. (This paper also gave a redefinition of MIP in terms of proof checking that would prove useful later...) Because of this oracle result, any proof of


Lance Fortnow

???
John Rompel

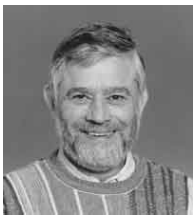
something like, say, coNP $\subseteq$ MIP would require a proof technique never seen before in complexity theory (specifically, a nonrelativizing technique). This is quite an "emotional barrier", as Babai would later write.

So it must have come as quite a surprise when on Nov. 27 1989, Nisan sent an email[2] to some colleagues showing that the Permanent and hence the very large class $P^{\#P} \supseteq PH$ is in MIP.[3] Nisan then decamped to South America for vacation. It should be noted that his paper built on recent work that had been circulating in 1989 by M. Blum and S. Kannan on program checking, by Lipton on random self-reducibility of the Permanent, and by Beaver and Feigenbaum on oracles and algebraic encoding.

Nisan's result was very impressive, but some people questioned the relevance of MIP — while IP sounded pretty plausible as a notion of efficient proof, MIP seemed unclear. Things changed dramatically just two

[2]Email in 1989, mind you. Babai's home country of Hungary didn't even have email until March 1990.
[3]The result $P^{\#P} \supseteq PH$ was proved earlier in 1989 by Toda.

Noam Nisan



Manuel Blum

Sampath Kannan

Dick Lipton

???

Donald Beaver

Joan Feigenbaum

weeks later; on Dec. 13, Fortnow, writing for a group of three at Chicago (Karloff and Lund), sent an email to a few dozen colleagues containing the LaTeX for a proof that Permanent and hence $P^{\#P}$ was in IP. This was definitely very surprising, as it meant that IP was hugely more powerful than people had realized. Not only was coNP was in it, the whole polynomial time hierarchy was in it. A side note about the recipients

Howard Karloff

Carsten Lund

of Fortnow's email: University of Washington professor Martin Tompa was on it, and it seems very likely to me that UW prof Richard Ladner was on it as well. As Babai wrote, notable for not being on the list were Razborov or anyone else from Eastern Europe. Note that the Berlin wall had fallen only a month ago (Nov. 9) and that the USSR still had over a year and a half left. Another side note, about the credits on this result: Lund was made "first author" on the paper, bucking standard practice of alphabetical order, since he apparently came up with the key step in the proof. Fortnow later wrote he thought this was a bad decision.[4] Also, Nisan was added as a coauthor on this paper. Hence the usual credit for this result is:

Theorem 3 *(LFKN '90)* $P^{\#P} \subseteq IP$.

Now it was long known that IP $\subseteq$ PSPACE (this result is usually credited to P. Feldman '86, although I've also seen it credited to Papadimitriou '83 in his paper about "Games Against Nature"); apparently after this email the race was on to try to prove the reverse containment. This was done just two weeks later: Shamir sent out an email on Dec. 26 1989 in which he introduced some new clever techniques to show:

[4] See `http://weblog.fortnow.com/archive/2003_12_07_archive.html`.

Adi Shamir

Theorem 4 *(Shamir '90)* IP = PSPACE.

(Note that the IP = PSPACE result is sometimes credited to LFKN+Shamir.)

Not to be outdone, three weeks later (Jan. 17, 1990) another email was sent out by Babai, Fortnow, and Lund:

Theorem 5 *(BFL '90)* MIP = NEXP*; i.e., anything with an exponential-sized proof can be proven in poly-time with multiple provers.*

This flurry of work produced a bit of a natural stopping point. The theorem IP = PSPACE is nowadays viewed as a classic of complexity theory and an amazing characterization of what can be proven efficient. The MIP = NEXP theorem is today considered somewhat more esoteric, but it actually turned out to inspire almost all of the future development in PCP theory. (Incidentally, this line of work also in some part spurred a lot of future development of derandomization theory, via a paper of Babai, Fortnow, Nisan, and Wigderson.)

Within a year of these results, people started trying to "scale down" the results for NP; i.e., try to put restrictions on the verifier's abilities which would recapture the tradition notion of the provable. One of the earlier restrictions considered was to bound the verifier's use of *space*. Much of the work in this direction was done by Condon, whose 1987 Ph.D. thesis from the University of Washington won the ACM Doctoral Dissertation Award for its study of the computational complexity of games and interactive proofs. One

Anne Condon

result of Condon's from an early '91 STACS paper is of particular interest. In this paper she showed that NP is exactly the class of languages with interactive proofs in which the verifier has logarithmic space and one-way read access to the proof. (A technical improvement to this result was made later by Condon and Ladner.) The main proof tools came from the IP = PSPACE result. But furthermore, the paper showed as a corollary that the MAX-WORD problem for matrices (given vectors u, v, matrices $M_1, \ldots, M_t$, and k, maximize $\langle u, M_{i_1} \cdots M_{i_k} v \rangle$) has no constant-factor approximation algorithm unless NP = P. This was the first ever connection made between interactive proofs and hardness of approximation. Unfortunately,

however, Condon's result did not receive much historical credit, as space-bounded verifiers proved to be not the most fruitful avenue of restriction.

Another restriction considered for verifiers was bounding their *time*. A result of Babai, Fortnow, Levin, and Szegedy from early/mid 1991 showed that if the prover was constrained to write its proof using a certain error-correcting code, then all NP languages could be checked by a verifier using *polylogarithmic time*. BFLS


Mario Szegedy


Leonid Levin

called such proofs "transparent proofs" (or sometimes, "holographic proofs"). Although the possibility of sublinear time proof checking is philosophically quite interesting, verifier time also proved to be not the most fruitful avenue of restriction.

As it happened, the most exciting results come from simultaneously restricting the number of random bits the verifier uses and the number of proof bit accesses it makes. For such verifiers, let us make a definition that was made first by Arora-Safra '92, though the significance of the definition was first made clear in the


Sanjeev Arora


Muli Safra

earlier paper Feige-Goldwasser-Lovász-Safra-Szegedy '91 (FGLSS):


Uri Feige


Laci Lovász

Definition 5 PCP$[r(n), q(n)]$ *is the class of languages provable with a PCP system which uses* $O(r(n))$ *bits of randomness, queries* $O(q(n))$ *bits in the proof, and has completeness 1, soundness* $1/2$.

With this definition, it can be seen that BFL's MIP = NEXP result is equivalent to NEXP $\subseteq$ PCP[poly, poly]. Also, if you look at the BFLS result on polylog time verifiers in the right way, it can be seen as showing NP $\subseteq$ PCP[polylog, polylog]. This latter result was noticed apparently independently (very slightly later) proved by Feige, Goldwasser, Lovász, and Safra (at Princeton). Later Szegedy joined this team and they published an improved result, along with a dramatic application that surprised everyone and set PCP research ablaze for the next couple of years:

Theorem 6 *(FGLSS, FOCS '91)* NP $\subseteq PCP(f(n), f(n))$*, where* $f(n) = \log n \cdot \log\log n$*. Furthermore, as a fairly straightforward consequence, it is impossible to approximate MAX-CLIQUE to within any constant factor, unless* NP $\subseteq DTIME(n^{\log\log n})$.

From this result it seemed clear that NP $\subseteq$ PCP[$\log n, \log n$] must be true; further, there was now huge extra motivation to prove it and improve on these PCP results because of their consequences for hardness of approximating clique. The result was proven in early 1992 (a little over two years after Nisan's email) by Arora and Safra at Berkeley, in a paper that introduced very many technical developments, along with the acronym "PCP" and the PCP[$r(n), q(n)$] notation mentioned earlier. The initials PCP seem to be due to Safra and it was surely not lost on these Berkeley authors that PCP is also the name of a hallucinogen. The name is apparently somehow motivated by an incident at a conference somewhere in California where police came to the conference hotel room where Safra was staying, looking to make a drug (PCP?) bust (not on Safra — they had the wrong room!).

Theorem 7 *(AS '92)* NP $\subseteq$ PCP[$\log n, \log n$]*. In fact,* NP $\subseteq$ PCP[$\log n, (\log n)^{.5+\epsilon}$].

So in fact, the queries can be *sublogarithmic*. In fact, an unpublished (unwritten?) manuscript attributed to Arora, Motwani, Safra, Sudan, and Szegedy notices that basically the same proof gets the queries to be $O((\log\log n)^2)$. Muli then left for Israel for the summer, I think; shortly thereafter was published the final

Rajeev Motwani

Madhu Sudan

improvement.

Theorem 8 *(Arora-Lund-Motwani-Sudan-Szegedy '92)* NP $\subseteq$ PCP[$\log n, 1$]*. (Although it was never explicitly calculated, the number of proof queries used was rumored to be about* 10^6*.)*

This result is now called "The PCP Theorem" and is traditionally credited to both Arora-Safra '92 and ALMSS '92. ALMSS's improvements incorporated ideas from Lapidot-Shamir '91, Feige-Lovász '92, and Blum-Luby-Rubinfeld '90. Both AS and ALMSS appeared in FOCS 1992 — they shared a session with a paper called *Undirected connectivity in* $O(\log^{1.5} n)$ *space* by Nisan, Szemerédi, and Wigderson — although news of the result spread widely in the spring of 1992. Indeed, six months before FOCS, on April 7, the result was written up by Gina Kolata in the Science section of the New York Times ("New Short Cut Found for Long Math Proofs"), and a week after that it was announced that there would be an informal presentation of the results at STOC '92. (This announcement is reproduced verbatim below, as an indicator of how fun STOCs and FOCSes apparently used to be. STOC Follies? Raffles? Sea-kayaking? Native story, ritual, and dancing? Nude bungee jumping?!)

???
Dror Lapidot Mike Luby Ronitt Rubinfled

Although there have subsequently been many improvements to the PCP Theorem of various nature, the result is considered a pinnacle and a crowning jewel of complexity theory. FGLSS '91, AS '92, and ALMSS '92 together shared the 2001 Gödel prize for their work.

The STOC '92 announcement.

Date: Mon, 20 Apr 1992 10:37:07 -0400
Reply-To: Michael Fellows
Sender: TheoryNet List
Subject: STOC '92 update

Update Information on STOC 92, Victoria, May 4-6:

(1) Yes, clothing is optional on the bungee jumping; no, we did not engineer the evening television news story which played across North America as a promotional event for STOC 92, it was just a coincidence.
(2) Discounts are available on Hertz rental cars, when arrangements are made through the United Airlines Convention desk.
(3) Victoria Taxi is the official taxi for STOC 92, and they are guaranteeing a rate of $32 (Can) between the Empress and the Victoria International Airport. Their phone number is 383-7111 in Victoria.
(4) Some phone numbers re: travel to Victoria Lake Union Air (Seattle - Victoria) 800-826-1890 Victoria Clipper (Seattle - Victoria) 604-384-8322 BC Ferries 604-656-0757 Helijet Airways (Vancouver - Victoria) 604-382-6222 Black Ball Ferries (Port Angeles - Victoria) 604-386-2202 Washington State Ferries (Seattle or Anacortes to Victoria) 604-381-1551
(5) Another route to Victoria is via the Anacortes ferry. Anacortes is about one hour's drive north of Seattle; this is a very pretty trip of about 3 hours through the San Juan islands. The ferry from Anacortes runs less frequently, so be sure to check the times with the number above if you choose this route.
(6) Oops! This will not be the first ever STOC follies; there have been two previously, one in 1978, and the last in San Francisco in 1982. If you wish to communicate or coordinate concerning the follies, contact Maria Klawe.
(7) There will be a raffle on Tuesday night, with raffle tickets awarded for submission of a topic in theoretical computer science together with a way that the topic might be presented in problem-solving mode to schoolchildren. For more details about this raffle and the project of assembling a compendium of theoretical computer science topics and presentation strategies for schoolchildren, stay tuned to theorynet.
(8) Sea-kayaking has filled up for Sunday! We are offering also a hike along Finlayson Arm from 10:30 AM until mid afternoon. Let us know if you are interested.
(9) The venue of the banquet on Tuesday night has been changed to the Native Heritage Center of the Cowichan Band, located in Duncan beside the Cowichan River. This is a feast, introduced and presented with native traditional story, ritual and dancing. The Center has several galleries and other displays of native arts, crafts and history. Bus transportation from the Empress will be provided. ONE PAGE ABSTRACTS OF RECENT RESULTS FOR DISTRIBUTION AT THE MEETING ARE ENCOURAGED AND WILL BE ACCEPTED UNTIL APRIL 28 The purpose of this is to encourage informal communication of the most recent results in the field. We are modeling our effort on the similar service offered by the Structures in Complexity meeting.
(10) A number of exciting developments are now scheduled for informal presentation, including the results from Berkeley which were written up in the New York Times last week.