**Event ID:** 2881507
**Event Started:** 3/9/2016 1:48:04 PM ET

Please stand by for realtime captions.

Welcome and thank you for standing by. At this time all participants are in a listen only mode. Today's call is being recorded. You have any objections you can disconnect at this time. I will turn the meeting over. You may now begin.

[ Indiscernible - low volume ] it is a great pleasure to introduce Moshe Vardi [ Indiscernible - low volume ] distinguished professor and computational [ Indiscernible - low volume ] for information technology [ Indiscernible - low volume ] used to be at IBM and then I knew he was moving from IBM I was trying hard to hire him [ Indiscernible - low volume ] acted faster than we could [ Indiscernible - low volume ]. He is truly an imminent researcher he is currently the [ Indiscernible - low volume ] he got many awards, three IBM outstanding awards, IBM [ Indiscernible - low volume ] in the European Community. He wrote over 500 papers and books, he did quite a number of papers. The most impressive thing is the quality of each and every one of those papers. He is truly remarkable in that sense. [ Indiscernible - low volume ] and he is a member of US national Academy of engineering, national Academy of science, American Academy of arts and sciences, the European Academy of science, the European Academy of science, [ Indiscernible - low volume ] which could have been easier if I said [ Indiscernible - low volume ] or something like this. He has several doctorates, for example [ Indiscernible - low volume ] or lands University of France [ Indiscernible - low volume ] a truly eminent researcher in all aspects of computer science. A couple of years ago he gave a talk at Johns Hopkins, a distinguished lecture talk on a slightly different topic, always entertaining and awful type of talks. It is my pleasure to have him here.

[ Applause ]

Thank you for this generous introduction. [ Indiscernible - low volume ] the first one has a footnote under his name and he says an AT&T phone because of Fellowship of the AT&T foundation and the second one is a footnote had fellow with a footnote from the health foundation and the third one has a footnote that says a jolly good fellow.

[ Laughter ]

Is an honor and pleasure and privilege to give the CISE distinguished lecture. Want to tell you about what I consider a true revolution that is happening in computer science, the [ Inaudible ] between the two of them. I want to start with a little bit of introduction which hopefully they'll just be reminding you of something you are all familiar with [ Inaudible ] on big outstanding question [ Indiscernible - low volume ] this is a question that has been that is considered a major course in mathematics and has allocated $1 million for whoever is going to solve this problem. What is it about? It is about the complexity how hard this is to solve social problems. This is not about -- [ Indiscernible - low volume ] he came up with this poster. Quantity now. What is a traditional problem?

For example we are going to start with a graph or network or segments or arcs and there are two very similar problems people asks about [ Indiscernible - low volume ] which is a cycle [ Indiscernible - low volume ] exactly what's. A similar one is [ Indiscernible - low volume ] built every edge exactly what's. We are wanting to find out how many cycles. [ Indiscernible - low volume ] theory [ Indiscernible - low volume ] this is a map and you see [ Inaudible ] is an island and there are seven bridges [ Indiscernible - low volume ] a question came up can you take a walk south from one point, come back and cross every bridge exactly what's? They could figure out how to do it and they had a famous mathematician and they went to him and said [ Indiscernible - low volume ] and then you get the grass. This is where the graph comes about and what was the solution to this problem in [ Indiscernible - low volume ] is named after [ Inaudible ] and this was a particular thing can you have cycle here [ Indiscernible - low volume ] you can visit everyone exactly what's. These are two classical questions in the theory and what we want to know how to do this so very formally we ask [ Indiscernible - low volume ] or does the size of the graph simply consider the number of notes versus the number of edges? We don't really think in terms of two dimensional operations but this is [ Indiscernible - low volume ] any kind of machine operation [ Indiscernible - low volume ] can be solved in the ocean for some consistency in cubes [ Indiscernible - low volume ]. Some problems are easy is the number even, all we have to do is look at the last digit, see if it is even or odd or do it in a Whittier pattern. -- A linear pattern.

[ Indiscernible - low volume ] I suspect this is a matter of age but the oldest people here clearly results [ Indiscernible - low volume ] long division or oblong square in today of course you use a calculator but if you look maybe you have been taught this is actually [ Indiscernible - low volume ] we can go back to the picture and what was produced was [ Indiscernible - low volume ] every note [ Indiscernible - low volume ] every time you into you have to get out, in here we see [ Indiscernible - low volume ]. You cannot have in the ocean we do this and Paul mealtime. We contact all these so this is [ Indiscernible - low volume ] this is a very large number and to do [ Indiscernible - low volume ] if we take a graph [ Indiscernible - low volume ] hundred steps to take the edge of the universe and say 15 billion years old and plug it into your computer and do it operation [ Indiscernible - low volume ] the universe is not old enough to finish [ Indiscernible - low volume ] so this is a fundamental question, can we do it in a very fundamental observation here which is which is due to it goes along edges and a hit every node exactly once. Are many problems but the checking is easy, single factor numbers, we don't know how to factor numbers efficiently of Omak all we have to do is multiplied them and check the number and are tens of thousands of problems in all domains that have essentially you can check solutions in polynomial time. You can check solutions efficiently. The [ Inaudible ] question is a very fundamental mathematical question which is the difficulty of planning solutions also the difficulty of checking solutions. Question we have been now asking [ Indiscernible - low volume ] 1970 [ Indiscernible - low volume ] that's how we think of our life. We talk about finding a needle in a haystack. [ Indiscernible - low volume ] but finding it is hard. [ Indiscernible - low volume ] finding is difficult. It is difficult to come up with proofs -- but we do not know how to prove that solving is harder than checking. We could imagine one universe [ Indiscernible - low volume ] and on one side these are many difficult problems we're not going to be able to solve. On the other hand is going to be safe because [ Indiscernible - low volume ] for example. Many years ago I was working at IBM we had a fist those physicists [ Indiscernible - low volume ] said something about very fundamental said you generally believe [ Indiscernible - low volume ], I said yes. I said [ Indiscernible - low volume ] why would you just accept it and move on? Which is what physicists will do, okay.

[ Laughter ]

Why don't you do that? I told him two reasons, one is because if we don't have the proof, we really do not understand it. The proof is understanding. Secondly [ Indiscernible - low volume ] and then every is, in a say, Chinese NSA, but they are reading our email. We need to know. We can imagine [ Indiscernible - low volume ] scientists at MIT said it beautifully he said [ Indiscernible - low volume ] the world would be a profoundly different place than we usually assumed to be. There will be no special value [ Indiscernible - low volume ] between solving a problem and mobilizing the solution once it sounds. Everyone could appreciates [ Indiscernible - low volume ] everybody can follow step-by-step [ Indiscernible - low volume ] he said this is very unlikely. The good things that are many problems we can solve in polynomial time but it is not safe anymore. Conventional wisdom is [ Indiscernible - low volume ] absolutely. It would take is to discover on clever item and we should remember that most of the complexity of about 50 years old in discovering [ Indiscernible - low volume ] people thought it was not [ Indiscernible - low volume ] it is quite possible. I have come to discuss again the significant of proving on over another.

One of the beautiful scenery that in the early 70s was that -- in a very formal way [ Inaudible ] 1972. Because of the problem [ Indiscernible - low volume ] polynomial time. Is a very tempting target , people probably prove every year in the [ Indiscernible - low volume ] equal are not equal to NP and [ Indiscernible - low volume ] in prison once and for all. Thousands of incomplete problems so we only have to find one of them to solve to prove it is NP or not NP. This has been [ Indiscernible - low volume ] many years. Now I want to give you the history of this. In some senses the early study of [ Indiscernible - low volume ] in the 50s and 60s to realize that all of this difficult problem [ Indiscernible - low volume ] and tried very hard to show it is inevitable finally and 71 [ Indiscernible - low volume ] showed about 20 other a complete problems was an amazingly short paper, the pages at the able to do what's [ Inaudible ] to in one short paper independently, 1971 [ Inaudible ] came out and [ Indiscernible - low volume ] I still have a copy which is falling apart now but it was a beautiful book and it popularized the products but [ Indiscernible - low volume ] to merit an award of $1 million.

I mention [ Indiscernible - low volume ] is the problem of incompleteness. This is the first a complete problem. This goes to -- now we are going to go back to 1847 and had a fantastic insight. And insight [ Indiscernible - low volume ] the previous 2000 years really can be algebra. Here's a paragraph from his book. [ Indiscernible - low volume ] is good, is employed for the description is applicable [ Indiscernible - low volume ] by the combination here I'm using algebraic convention of [ Indiscernible - low volume ] by juxtaposition so X times lie -- Y [ Indiscernible - low volume ] the insight here is that the conjunction and can be [ Indiscernible - low volume ] population and it is an additional operation and suck you have algebra. This is how [ Indiscernible - low volume ] that is how it was born. The question of the viability in the 19th century is usually formalized today in the following manner, this is a modern formalization you can imagine a Boolean expression [ Indiscernible - low volume ] in the question is is there a way to assign zero and one to the baronetcy so it evaluates to on? Here we can see if we take these to be zero and these to be on it becomes [ Indiscernible - low volume ] here it is easy to do there are three variables which is it possible [ Indiscernible - low volume ] to do it in segments imagine what would happen if I had a formula that I had maybe the whole slide it would not be possible to do by inspection anymore. Of the 19th century this was a very important problem and if you do any kind of automated reasoning would have to [ Indiscernible - low volume ] this is the weakest possible Logix of any kind we have to do we have to do with Boolean reasoning.

In the middle of the 19th century before you have any concept of computation they want to know how to do it fast so Boolean [ Indiscernible - low volume ] some relation that we use today [ Indiscernible - low volume ] of the process, the process is Boolean reasoning and the devices which may be adopted for that event resource building the first logic machine [ Indiscernible - low volume ] I could handle for variables so of Omak not very impressive but moving within pieces. If you can do that [ Indiscernible - low volume ].

I'm going to show you a bit later [ Indiscernible - low volume ] a faster method for obtaining these consequences seems to me to be on of the ultimate goals of mathematics and logic. This is the ultimate goal of mathematics and logic to solve this problem which as we know today was shown by of Omak is incomplete. By the conventional wisdom of computer science and [ Indiscernible - low volume ] means hopeless, to waste your time. Were several people who nevertheless wasted their time. In fact, it goes back to the mid-50s so we have to remember that in 1946 in the 1950s computers are just being built, maybe thousands of computers and [ Indiscernible - low volume ] from a computer mathematical [ Indiscernible - low volume ] respond very graciously, 1958 [ Indiscernible - low volume ] founded by the NSA and [ Indiscernible - low volume ] if they are listening.

[ Laughter ]

[ Indiscernible - low volume ] this is relevant to photography. To publish papers in 1960 [ Indiscernible - low volume ] they have given us the basic theory of propositional reasoning in the method that came out of this is called [ Indiscernible - low volume ] which is basically [ Indiscernible - low volume ] normal form, it looks like this and these junctions you can always converted to CNF, and there was one important [ Indiscernible - low volume ] is generated to be one variable and there's nothing more to choose, just take this assignment because you are forced to.

From the early 60s, for the next 30 years a very small group of people [ Indiscernible - low volume ] it is going to be hard and they right problems and can handle some variables and then a few hundred variables, but they mostly thought this was a waste of time, isn't it problem and [ Indiscernible - low volume ] problems. And the something happen in the mid-90s and there was an explosion of the linguistics and linguistics have changed the game dramatically [ Indiscernible - low volume ] I want go to every detail but it means that [ Indiscernible - low volume ] you try to jump up as high as you can instead of going on level of the time [ Indiscernible - low volume ] unit variable just jump at it [ Indiscernible - low volume ]. This is very trivial [ Indiscernible - low volume ] to implement except that people profiling discovered that 80% of the time you are doing this operation of updating because you want to keep of Omak and you are spending 80% of the time uploading [ Indiscernible - low volume ] a data structure to do it and so on and so forth. I want to [ Indiscernible - low volume ] a very important tool that came from Michigan in the mid-90s [ Indiscernible - low volume ] from Princeton and this tool has been adopted and accepted in wide industrial usage [ Indiscernible - low volume ] annual competition and today we solve problems with millions of variables. This happened for 20 years we went from hundreds of variables to millions of variables. Colleague of mine [ Indiscernible - low volume ] decided to take [ Indiscernible - low volume ] and take on benchmark problem and loaded on a 20 submachine. Usually everyone [ Indiscernible - low volume ] a different machine so let's build them to each other. On this benchmark problem that in 2000 that in 2800 seconds in 2012 just one second. [ Indiscernible - low volume ] people are starting to talk about [ Indiscernible - low volume ] which is really kind of a joke, but nobody can really explain these problems. A problem without 20 years ago we thought was an impossible problem and today it is so possible that [ Indiscernible - low volume ] but they have been doing [ Indiscernible - low volume ] said today doing that solving is in reality so we went from a niche academic activity to a mainstream [ Indiscernible - low volume ] all activity Microsoft Corporation is a developed software they have used [ Indiscernible - low volume ] development which is widely known in one reason I'm here is to take it the world is changing in a very dramatic way.

This is the first half of the talk and what a what to do in the second half is saying now that we can do this, what can we do with the? [ Indiscernible - low volume ] I don't know who said it, but if you have a hammer what do you do? [ Indiscernible - low volume ] let's go look for nails. Let's go back to talk about and developments [ Indiscernible - low volume ] is a quarter billion dollar a year industry and [ Indiscernible - low volume ] we talk about people who design systems that will tell you that the 1070% to 80% of the design effort is validation. You designs of the, how do you know that it does what you want to do? This is called functional validation. [ Indiscernible - low volume ] just checking that has been the functionality is a huge undertaking. [ Indiscernible - low volume ] we talk a lot about [ Indiscernible - low volume ] all essentially around [ Inaudible ]. How to find precisely talk to people in industry and asset to look at the person hours invested in this activity and 10% is an enormous estimate. Is some of the more advanced places maybe Microsoft, until, every small software company does nothing but [ Indiscernible - low volume ] they do it the same way [ Indiscernible - low volume ]. Pretty much. This now has a nice name is called [ Inaudible ] NUC where the system under different scenarios and you see that you get the right answer and this is 90% of what takes place in the industry. Let's zoom in a little bit. This is the [ Indiscernible - low volume ] and basically you simulate the system under many different input, possible input and the inputs reflect different scenarios that you want to simulate and then you compare the results to what you get from the simulation and the ideal results NUC the results and the test space is [ Indiscernible - low volume ] one example so that is just one of the most famous in the industry in [ Indiscernible - low volume ] could do floating-point division correctly so everybody now knows today the next time this comes out to the market somebody will lose their job [ Indiscernible - low volume ] happen only once. Imagine the time to verify [ Indiscernible - low volume ] and supposed which I to look for all the values and there are 156 possibilities [ Indiscernible - low volume ] before we're done and everybody knows this is not scalable so we cannot cover the whole test base exhaustively so what do we do? The logical approach is to me to sit down and think really hard to write test cases so [ Indiscernible - low volume ] they write test cases when I was at IBM I was asked to help with the testing program that IBM was developing [ Indiscernible - low volume ] hundred people in IT test cases and it turns out [ Indiscernible - low volume ] 20 per day so that means every day we are generating about 2000 possible testing scenarios, and IBM decided to invest in it [ Indiscernible - low volume ] emulator runs about 100,000 times faster than software simulation and this 2000 cases about 30 seconds and then for the rest of the day [ Indiscernible - low volume ] in some manager had to explain why he spent $5 million on the system that is utilized for 30 seconds. I was asked if I could help. IBM eventually came up with a different approach which has become the de facto industry standard. [ Indiscernible - low volume ] they do not write test cases. Instead they right constraints with scenarios. For example they say the two numbers are both very large or very small one is very large and one is very small [ Indiscernible - low volume ] solutions are test vectors. This has become now the standard approach in the industry it is the [ Indiscernible - low volume ] test generation.

Now we have constraints. We give it to a [ Indiscernible - low volume ] we want to give it all of them to give us solutions [ Indiscernible - low volume ] uniformly. You're looking for the bug. Some of it has its own internal search will be [ Indiscernible - low volume ] there's no reason to believe that the solution will [ Indiscernible - low volume ] I don't know where the bug is. [ Indiscernible - low volume ] are not marked so I should do it randomly. Also [ Indiscernible - low volume ] another part of the space. This gives the following question, given the formula in terms of Boolean formula but he could be produced to Boolean formula. You are given a Boolean formula and you not want to find a solution [ Indiscernible - low volume ] uniformly. How can we do that? [ Indiscernible - low volume ] we want to get uniformly on the solutions. This is the problem that really is important for [ Indiscernible - low volume ] applications. Turns out there are many other applications. This is really [ Indiscernible - low volume ] I talked my colleagues [ Indiscernible - low volume ] people are talking incessantly [ Indiscernible - low volume ] somebody will post the solution. That means you have to generate every assignment, you have to generate hundred thousand different problems. How do you do it? You right constraints, [ Indiscernible - low volume ] you want to generate solutions to formulate at random. Optimization [ Indiscernible - low volume ] jump from there to another place but is still have to satisfy some constraints and you want to do it again [ Indiscernible - low volume ]. And machine learning this is a big thing. You have some initial problems [ Indiscernible - low volume ] you want to condition, steak the evidence and you want to sample after the condition. [ Indiscernible - low volume ] your given the constraints, you want to sample uniformly and unilaterally. [ Indiscernible - low volume ] have been studying it now for 30 years from a uniform distribution [ Indiscernible - low volume ] I won't get into it because it would improve from years later [ Indiscernible - low volume ] and they were able to show how you do it using [ Indiscernible - low volume ] for example in 2011 after I realized this is an important industrial problem in to quote an undergraduate student let's try to implement [ Indiscernible - low volume ] algorithm that is implemented. We implemented it and it scaled to I remember talking to the students and said very nice we put a good effort I have to tell you but cannot [ Indiscernible - low volume ] this is in 2011, people are solving huge problems and we said we could do it for [ Indiscernible - low volume ] said the committee will not do stable laugh at the paper I can imagine [ Indiscernible - low volume ] submission. If we get to 1000 variables may be we can [ Indiscernible - low volume ] workshop but 16 is that even establish. I said it is a very important problem so what do people do in the industry? [ Indiscernible - low volume ] in the industry I can't really explain too much for lack of time on his based on binary decision diagrams [ Indiscernible - low volume ] how many solutions to you have? [ Indiscernible - low volume ] this is a perfectly adequate solution and you hand it off of 2000 variables and then it gets to be too large and the site very useful. There is another technique popular today [ Indiscernible - low volume ] it is a big field, and this is a startup technique in any kind of machine learning [ Indiscernible - low volume ] what you to is built in the space and you know you can [ Indiscernible - low volume ] you will reach what is called [ Indiscernible - low volume ] and then you can sample. The question is how long is the work? [ Indiscernible - low volume ] the work is short, but in general the work has to be proportion to the size [ Indiscernible - low volume ] it is unfeasible. What do you do? You take a short walk it to you lose patience and then you sample but you are not uniform and we can say nothing about no uniformity. The other thing is let's take the public let's choose [ Indiscernible - low volume ] a value at random people have tried to see how uniform and what you get, it is very nonuniform because it depends on the action [ Indiscernible - low volume ] very nonuniform distributions. Even if this report works well [ Indiscernible - low volume ] over the last few years, and actually I should mention all of this work is geared toward [ Indiscernible - low volume ] supporting me in my students at a particular this is the result of an expedition we're in the last year of and [ Indiscernible - low volume ] together with my collaborator [ Indiscernible - low volume ] students we have a new sample that does almost uniform [ Indiscernible - low volume ] it is based on the universal hashing [ Indiscernible - low volume ] it depends on [ Inaudible ] software which is a new idea and I will explain. It can handle millions of variables.

It requires that you spend some time preprocessing and then you [ Indiscernible - low volume ] workstation each one can do its own generating of its own independent samples. It does what it should do for sampling [ Indiscernible - low volume ].

Of course we have to compromise. The compromise here is we cannot do it uniformly which is very difficult we took almost uniformly. What is it me to do almost uniformly? [ Indiscernible - low volume ] solutions then the uniform probability [ Indiscernible - low volume ] we do it you give us an Athlon and we will do it within [ Indiscernible - low volume ] let's suppose it is .1 it means we are 1.1 factor away from the uniform probability [ Indiscernible - low volume ]

What are the ideas here? It reminds me of a very old story purchase how do you catch a line in the desert? [ Indiscernible - low volume ] it was the and one quarter, you keep doing it in eventually you get a piece that is so small [ Indiscernible - low volume ] that is really what we do. We divide the whole solution space [ Indiscernible - low volume ] constraints. We have no idea what the solutions look like. Show you how we delighted divided into [ Indiscernible - low volume ] that we just picked randomly in uniformly with one of the solutions because they are almost equal, they are not exactly equal. This is the basic idea. You find the solution space [ Indiscernible - low volume ] maybe only 100 solutions we can move and enumerate them to choose one of them. The challenge is how do you take a space you know nothing about and position almost uniformly? How do we do that? This is the magic of universal hashing. Hashing is a uniform concept [ Indiscernible - low volume ] much smaller space [ Indiscernible - low volume ] if you go back to the old volumes with hash functions, the is a discussion of [ Indiscernible - low volume ] the hash function should not screw it up [ Indiscernible - low volume ] output. People realize it is not working because we know nothing about [ Indiscernible - low volume ] it could be highly concentrated. Here is the idea of universal hashing, we have the function, you choose one randomly and randomize over the initial distribution and it doesn't matter what the additional distribution you are guaranteed to get [ Indiscernible - low volume ] function at random. The universal family is the one that does this job but it is not enough because remember we do sampling here. There is really not a requirement [ Indiscernible - low volume ] I have on several images of again and again. How do you do it independently? I need a hash function not only to get the uniformly, but also to create independent. Here come the consequent [ Indiscernible - low volume ] this is a perimeter and if you are universal it means that every input are hashed independently. The higher the more independence you have [ Indiscernible - low volume ] more uniform the higher they are. Since we know how to generate high universality [ Indiscernible - low volume ] this is all well understood. [ Indiscernible - low volume ] harder to solve, higher complexity. [ Indiscernible - low volume ] and universality. An example of variables. Even for [ Indiscernible - low volume ] were only to have to use [ Indiscernible - low volume ] polynomials if we go farther back it is not feasible. We have to work hard to show that you can do this with very low universality [ Indiscernible - low volume ] and this is where we get also [ Indiscernible - low volume ] we get almost uniform generation. The mathematical part of the paper was to show if we can do it with very about universality and this enabled us to go from tens of variables to millions of variables.

The other important question is how do we do this [ Indiscernible - low volume ] one of the specifics of the hash function? [ Indiscernible - low volume ] we generate a bunch of additional constraints. Every constraints we take, we choose variables with uniform probability and what I did [ Indiscernible - low volume ] flip the coin is included were not included so we have them available in every equation and we choose 011. This is [ Indiscernible - low volume ] for the solution space and we do them with additional constraints [ Indiscernible - low volume ] whatever the solution space [ Indiscernible - low volume ] we're going to get about half the solutions. The challenge for us is that now we get the problem that consists of the [ Indiscernible - low volume ] but now we also have [ Indiscernible - low volume ]. Notice that the once close up on themselves or is it solved because the linear equation of American high school students should be able to solve them without eliminations [ Indiscernible - low volume ] there are lots of solvers that could do this. We can solve new systems [ Indiscernible - low volume ] it is actually very easy. Now we have this combination [ Indiscernible - low volume ] we can reduce, efficient reduction [ Indiscernible - low volume ] but then we lose the easiness so if we do that [ Indiscernible - low volume ] we try to do it, it doesn't work. Now comes [ Indiscernible - low volume ] SMP solving. Ability model theory, what does it mean? [ Indiscernible - low volume ] more sophisticated automatic reasoning techniques and we combine the Boolean reasoning with let's say [ Indiscernible - low volume ] can we handle these junctions of linear inequalities, for example? We want to combine Boolean reasoning [ Indiscernible - low volume ] is another domain of constraints. This has been very active research for the last 15 years [ Indiscernible - low volume ] solving a combination of Boolean and other type of constraints.

In 2009 [ Indiscernible - low volume ] decided to drive to [ Indiscernible - low volume ] introduce a combination and he combine [ Indiscernible - low volume ] in a very clever way. [ Indiscernible - low volume ] was sitting there waiting for us when we needed to& Evolve -- to solve the serendipity factor [ Indiscernible - low volume ] success in what way [ Indiscernible - low volume ] we started using Google aggressively, found the software and it was like manna from heaven and he cannot be happier because he left academia and went to industry and it was the key for our success. How good is the performance? Difference here between a couple of Mexico I gave a talk on this and I said the rate of difference between [ Indiscernible - low volume ] what we do is we don't just proves that we haven't algorithm we run the algorithm. We want to know how [ Indiscernible - low volume ] we took a formula with 16,000 solution and we generated about 4 million samples. I have 16,000 been [ Indiscernible - low volume ] now I will give different count [ Indiscernible - low volume ] I can look at each count how many times it appears. [ Indiscernible - low volume ] distribution, we don't go to the limit so instead what we did we implemented this universal example and compared it to our sampler, in this is the solution of accounts and the [ Indiscernible - low volume ] what we generate is statistically indistinguishable from uniform probability. What about the performance? We benchmark ourselves against, at the time this was [ Indiscernible - low volume ] the best sample you can get from the community [ Indiscernible - low volume ] it is a sample [ Indiscernible - low volume ] of uniformity's [ Indiscernible - low volume ] based on a combination of, it is based on [ Inaudible ] and we outperform it by [ Indiscernible - low volume ] we get not only guaranteed uniformity, but also fantastic performance. That this such success that we decide to look for another name and the next was counting. We want to count how many solutions there are [ Indiscernible - low volume ] so there are three solutions. This is, again accounting solution [ Indiscernible - low volume ] it is a form of counting, how many solutions to you have for a problem [ Indiscernible - low volume ] incomplete problem. Is known to be actually of much harder problem so while that has kind of become [ Indiscernible - low volume ] what I mean by easy [ Indiscernible - low volume ]. It is a problem has many applications, for example in the context of unknown verification like to have some idea of what is the size of the solution space before we start generating solutions? How long should you go? You need a firm idea of the size of the solution space [ Indiscernible - low volume ] in this is a very hard problem. It is much harder in fact. [ Indiscernible - low volume ]. Again [ Indiscernible - low volume ] approximate counting in this is called [ Indiscernible - low volume ] and this is even before you look at the count but you wanted to be [ Indiscernible - low volume ] certain high probability. It does that have to be [ Indiscernible - low volume ] going back to 1989 they proved [ Indiscernible - low volume ] within into Oracle. By now we understand [ Indiscernible - low volume ] we want to use the same approach. The approach is [ Indiscernible - low volume ] to divided into small cells. In each cell [ Indiscernible - low volume ] for the host of the space simple enough to get an estimate with high enough confidence and I get an algorithm which is [ Indiscernible - low volume ] in place of [ Indiscernible - low volume ] only thousands variable we can compare ourselves against the exact counter, and we use .75 in all the cases we feel the .75 and even though we have the probability to deviate we never had [ Indiscernible - low volume ] accuracy is 4% even though we set the parameter of 75% [ Indiscernible - low volume ] analysis explain why we are getting such a variable with fantastic accuracy and [ Indiscernible - low volume ] it keeps going forward and we can [ Indiscernible - low volume ] have program with hundreds of thousands of variables because we need to do sampling so we can handle hundreds of thousands of variables.

I'm getting to the end of the talk I want to stop it is some reflection on what does this tell us about the [ Indiscernible - low volume ]. I think when I was a freshman student asked if I know the difference between theory [ Indiscernible - low volume ] until they told me the standard cliché which is in theory they are not very different of all Mac very different so there is a huge difference between [ Indiscernible - low volume ] in practice it would do us no good because example everything can be done [ Indiscernible - low volume ] no practical application whatsoever or we could [ Indiscernible - low volume ] but maybe it is not a fixed degree. [ Indiscernible - low volume ] asks us what is the name of [ Indiscernible - low volume ] so we said it is infinity and he said in practice it is about 50. [ Indiscernible - low volume ]

[ Laughter ]

Might be very practical algorithms so it could be that [ Indiscernible - low volume ] still very possible. There might be no practical benefit one way or another, quite possible. We have to accept that this is a possibility. The difference is when I was a graduate students [ Indiscernible - low volume ] was scary is a scary thought. Admits don't touch it, don't even look at it. In the does it might be contaminated by looking at it. Today, it is a hard problem. We can synthetically generate instances with hundreds of variables [ Indiscernible - low volume ] can solve. We are solving that problem with millions of variables of all Mac why some are hard [ Indiscernible - low volume ] we have a fantastic challenge to understand the actual performance. The on that we in general had things easy. What does this now mean for [ Indiscernible - low volume ] what else can we do with the? Me show you for example the problem we considered impossible which now becomes very feasible. What else can we do? [ Indiscernible - low volume ] in fact polynomial time. I think this is the time of really need to [ Indiscernible - low volume ] the standard assumptions in computer science. Thank you very much.

[ Applause ]

[ Indiscernible - low volume ] not all random number generators are created equal [ Indiscernible - low volume ]

This is actually a very good question. What you do is use, typically use behavior to generate [ Indiscernible - low volume ] in the new use this call of all Mac number generator to generate that sequence. Is actually difficult. We start the beginning with [ Indiscernible - low volume ] but then we didn't have enough ways to use them and actually [ Indiscernible - low volume ] so it is actually an interesting question and people [ Indiscernible - low volume ] random for a number of problems we understand the difference. If you really want the balance so there is a certain [ Indiscernible - low volume ] in practice the when can distinguish the pseudo-randomness [ Indiscernible - low volume ].

To you have it into, complete problem, you translated into SAT and use that solver [ Indiscernible - low volume ] on what a complete problems does that work?

Less suppose I wanted to generate a random [ Indiscernible - low volume ] so think about it. Every economic problem privet by showing the reduction is a reduction to SAT which means you can then use it as absolute. A whole variety of problems I can now use it by production or introduction to SAT. In some sense this is one way [ Indiscernible - low volume ] approach and universal hashing to do something in counting. Can you take these ideas to other domains? Can I go for example can I [ Indiscernible - low volume ] and devise some kind of hash function [ Indiscernible - low volume ] ability to solve the hash function to be able to estimates questions [ Indiscernible - low volume ] constraints [ Indiscernible - low volume ]. It is not clear if that is the right approach but it is the general paradigm here which is universal hashing [ Indiscernible - low volume ] can be a very powerful combination, one of the actions we're not looking at is misdirection and we go to other domains [ Indiscernible - low volume ] algorithmic components.

[ Indiscernible - low volume ]

[ Indiscernible - low volume ] are only improving the performance. That is correct. We know mistakes. You can check the final solution. [ Indiscernible - low volume ] the run time. There is a compromise here on the [ Indiscernible - multiple speakers ]

[ Indiscernible - low volume ]

The SAT are found a complete [ Indiscernible - low volume ] that will take too long and you will give up before you have the solution . We are not compromising here. We do get an approximate answer [ Indiscernible - low volume ] but that we're very precise [ Indiscernible - low volume ] guarantee.

[ Indiscernible - low volume ]

For some problems yes, for some problems it is better to move to the domain.

Of all Mac -- [ Inaudible ]

There are some technicalities I don't want to get into one of the things you to [ Indiscernible - low volume ] and that means we are dealing with extra variables so we don't need a sample of all variables [ Indiscernible - low volume ] enable us to deal with [ Indiscernible - low volume ]

Have one question [ Indiscernible - low volume ] if you do find it in one step do it many times [ Indiscernible - low volume ]

We start to now to compare this approach to polynomial time approaches. This has been a major activity in the community now for the past 25 years, and some beautiful, beautiful results have come up [ Indiscernible - low volume ] is in polynomial time and all kinds of things like that. We are starting this comparisons and it is a bit too early but I expect I could be wrong but I expect these measures will perform much better than probably polynomial measures of all Mac [ Indiscernible - low volume ] you could do the calculation [ Indiscernible - low volume ] a huge number. [ Indiscernible - low volume ] as I said we are in the beginning of revising our thinking about algorithms and complexity in secret takes us.

Thank you very much. -- And fever it takes us.

Thank you very much.

[ Applause ]

If you would like to ask a question from the following you compress \*1.

[ Indiscernible - multiple speakers ]

[ Silence ]

That concludes today's conference. You may now disconnect.

[ Event Concluded ]

Actions