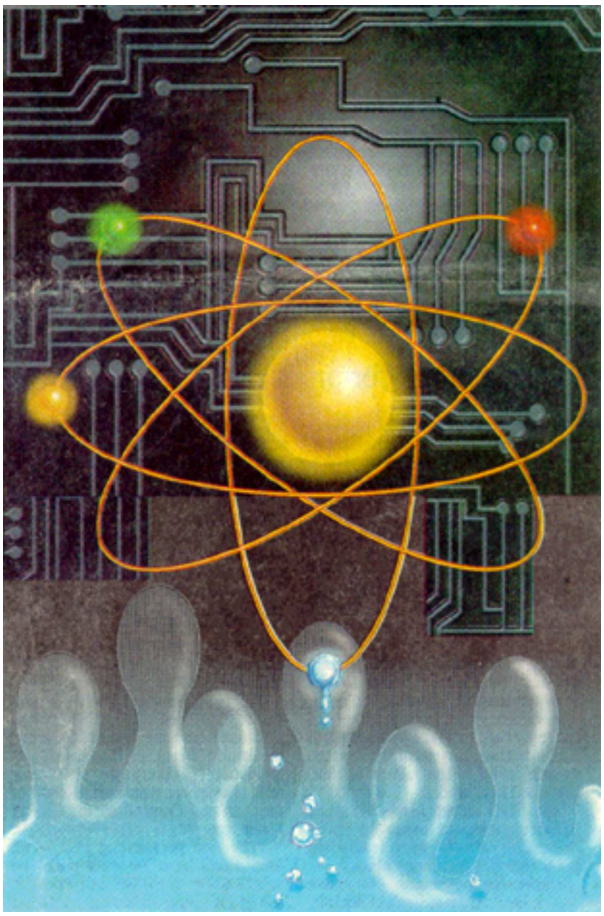


XOOTIC

magazine

July 2003-Volume 10-Number 3

POST-MASTERS PROGRAMME SOFTWARE TECHNOLOGY

Quantum Computing

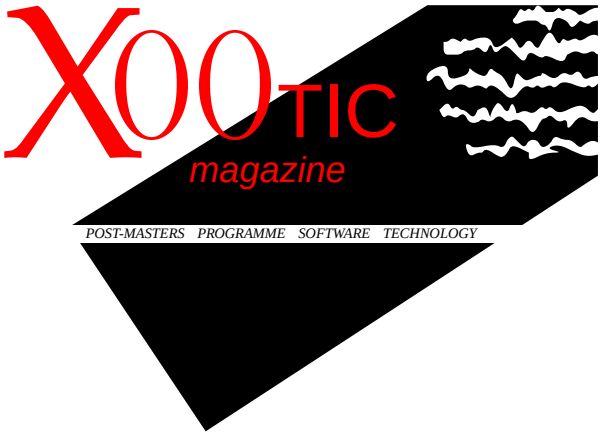
Small Computers

Teleportation

Xootic Survey

Contents

Advertorials



Colofon

XOOTIC MAGAZINE
Volume 10, Number 3
July 2003

Editors
C. Delnooz
N.H.L. Kuijpers
Y. Mazuryk

Address
XOOTIC and XOOTIC MAGAZINE
P.O. Box 6122
5600 MB Eindhoven
The Netherlands
xootic@win.tue.nl
http://www.win.tue.nl/xootic/

Secretariat OOTI
Ms. M.A.C.M. de Wert
Post-masters Programme
Software Technology
Eindhoven University of Technology, HG 6.57
P.O. Box 513
5600 MB Eindhoven
The Netherlands
tel. +31 40 2474334
fax. +31 40 2475895
ooti@win.tue.nl
http://wwwooti.win.tue.nl/

Printer
Offsetdrukkerij De Witte, Veldhoven

Quantum Computing

Editorial Preface

Hello XOOTICS! Before you lies the first XOOTIC MAGAZINEof 2003. Where we usually have themes close to our own fields of employment, especially the embedded software and architecting, this time we ventured a little bit aside these topics. As computer scientists, we are all aware that there are problems which cannot be solved (in polynomial time) by conventional computers. A different side of computer science promises to solve these and other problems: Quantum Computing.

Caltech's Jacob West opens this magazine with a general introduction into the field of Quantum Computing. He will explain some of the differences between conventional computers and the fundamental concepts of quantum computing, such as the qubit and quantum interference.

Next, we anticipated two articles on *Q*uantum Information and *Quantum Cryptography*. Due to various reasons, we are not able to publish these articles.

Samuel Braunstein and Pieter Kok provide us with a look into the, until now science-fiction, world of teleportation. Samuel and Pieter look at the meaning of teleportation in general and the achievements that have already been made. Finally, they speculate about the vast amount of computing power needed to even think about teleporting a living being in a Startrek-like fashion.

We close this magazine with the results of the Xootic Survey held in 2002. The survey committee presented the results recently, and you can all read them at leisure in this magazine.

Enjoy reading this magazine!

Chris Delnooz, editor

Advertorial: Philips

Page 4 (should be even)

The Quantum Computer

Jacob West

What is a Quantum Computer?

Behold your computer. Your computer represents the culmination of years of technological advancements beginning with the early ideas of Charles Babbage (1791-1871) and eventual creation of the first computer by German engineer Konrad Zuse in 1941. Surprisingly however, the high speed modern computer sitting in front of you is fundamentally no different from its gargantuan 30 ton ancestors, which were equipped with some 18000 vacuum tubes and 500 miles of wiring! Although computers have become more compact and considerably faster in performing their task, the task remains the same: to manipulate and interpret an encoding of binary bits into a useful computational result. A bit is a fundamental unit of information, classically represented as a 0 or 1 in your digital computer. Each classical bit is physically realized through a macroscopic physical system, such as the magnetization on a hard disk or the charge on a capacitor. A document, for example, comprised of n-characters stored on the hard drive of a typical computer is accordingly described by a string of $8n$ zeros and ones. Herein lies a key difference between your classical computer and a quantum computer. Where a classical computer obeys the well understood laws of classical physics, a quantum computer is a device that harnesses physical phenomenon unique to quantum mechanics (especially *quantum interference*) to realize a fundamentally new mode of information processing.

In a quantum computer, the fundamental unit of information (called a quantum bit or *qubit*), is not binary but rather more quaternary in nature. This qubit property arises as a direct consequence of its adherence to the laws of quantum mechanics which differ radically from the laws of classical physics. A qubit can exist not only in a state corresponding to the logical state 0 or 1 as in a classical bit, but also in states corresponding to a blend or *superposition* of these classical states. In other words, a qubit can exist as a zero, a one, or simultaneously as both 0 and 1, with a numerical coefficient representing the probability for each state. This may seem counterintuitive because everyday phenomenon are governed by classical physics, not quantum mechanics – which takes over at the atomic level. This rather difficult concept is perhaps best explained through an experiment. Consider Figure 1 below:

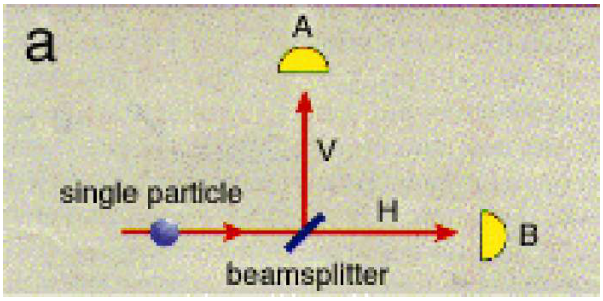


Figure 1: Figure taken from a paper by Deutsch and Ekert.

Here a light source emits a photon along a path towards a half-silvered mirror. This mirror splits the light, reflecting half vertically toward detector A and transmiting half toward detector B. A photon, however, is a single quantized packet of light and cannot be split, so it is detected with equal probability at either A or B. Intuition would say that the photon randomly leaves the mirror in either the vertical *or* horizontal direction. However, quantum mechanics predicts that the photon actually travels *both* paths simultaneously! This is more clearly demonstrated in Figure 2.

In an experiment like that in Figure 1, where a photon is fired at a half-silvered mirror, it can be shown that the photon does not actually split by verifying that if one detector registers a signal, then no other detector does.

With this piece of information, one might think that any given photon travels either vertically or horizontally, randomly choosing between the two paths. However, quantum mechanics predicts that the photon actually travels both paths simultaneously, collapsing down to one path only upon measurement. This effect, known as *single-particle interference*, can be better illustrated in a slightly more elaborate experiment, outlined in Figure 2 below:

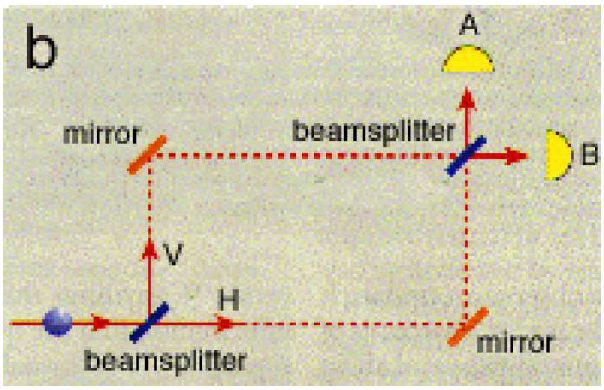


Figure 2: Figure taken from a paper by Deutsch and Ekert.

In this experiment, the photon first encounters a half-silvered mirror, then a fully silvered mirror, and finally another half-silvered mirror before reaching a detector, where each half-silvered mirror introduces the probability of the photon traveling down one path or the other. Once a photon strikes the mirror along either of the two paths after the first beam splitter, the arrangement is identical to that in Figure 1, and so one might hypothesize that the photon will reach either detector A or detector B with equal probability. However, experiment shows that in reality this arrangement causes detector A to register *100%* of the time, and *never* at detector B! How can this be?

Figure 2 depicts an interesting experiment that demonstrates the phenomenon of single-particle interference. In this case, experiment shows that the photon *always* reaches detector A, *never* detector B! If a single photon travels vertically and strikes the mirror, then, by comparison to the experiment in Figure 1, there should be an equal probability that the photon will strike either detector A *or* detector B. The same goes for a photon traveling down the horizontal path. However, the actual result is drastically different. The only conceivable conclusion is therefore that the photon somehow traveled both paths simultaneously, creating an interference at the point of intersection that destroyed the possibility of the signal reaching B. This is known as *quantum interference* and results from the *superposition* of the possible photon *states*, or potential paths. So although only a single photon is emitted, it appears as though an identical photon exists and travels the 'path not taken', only detectable by the interference it causes with the original photon when their paths come together again. If, for example, either of the paths are blocked with an absorbing screen, then detector B begins registering hits again just as in the first experiment! This unique characteristic, among others, makes the current research in quantum computing not merely a continuation of today's idea of a computer, but rather an entirely new branch of thought. And it is because quantum computers harness these special characteristics that gives them the potential to be incredibly powerful computational devices.

The Potential and Power of Quantum Computing

In a traditional computer, information is encoded in a *series* of bits, and these bits are manipulated via *Boolean logic gates* arranged in succession to produce an end result. Similarly, a quantum computer manipulates qubits by executing a series of quantum gates, each a *unitary transformation* acting on a single qubit or pair of qubits. In applying these gates in succession, a quantum computer can perform a complicated unitary transformation to a set of qubits in some initial state. The qubits can then be measured, with this measurement serving as the final computational result. This similarity in calculation between a classical and quantum computer affords that in theory, a classical computer can accurately simulate a quantum computer. In other words, a classical computer would be able to do anything a quantum computer can. So why bother with quantum com-

puters? Although a classical computer can theoretically simulate a quantum computer, it is incredibly inefficient, so much so that a classical computer is effectively incapable of performing many tasks that a quantum computer could perform with ease. The simulation of a quantum computer on a classical one is a computationally hard problem because the correlations among quantum bits are qualitatively different from correlations among classical bits, as first explained by John Bell. Take for example a system of only a few hundred qubits, this exists in a *Hilbert space* of dimension $\sim 10^{90}$ that in simulation would require a classical computer to work with exponentially large matrices (to perform calculations on each individual state, which is also represented as a matrix), meaning it would take an exponentially longer time than even a primitive quantum computer.

Richard Feynman was among the first to recognize the potential in quantum superposition for solving such problems much much faster. For example, a system of 500 qubits, which is impossible to simulate classically, represents a quantum superposition of as many as 2^{500} states. Each state would be classically equivalent to a single list of 500 1's and 0's. Any quantum operation on that system –a particular pulse of radio waves, for instance, whose action might be to execute a *controlled-NOT* operation on the 100th and 101st qubits– would simultaneously operate on all 2^{500} states. Hence with one fell swoop, one tick of the computer clock, a quantum operation could compute not just on one machine state, as serial computers do, but on 2^{500} machine states at once! Eventually, however, observing the system would cause it to collapse into a single quantum state corresponding to a single answer, a single list of 500 1's and 0's, as dictated by the measurement axiom of quantum mechanics. The reason this is an exciting result is because this answer, derived from the massive *quantum parallelism* achieved through superposition, is the equivalent of performing the same operation on a classical super computer with $\sim 10^{150}$ separate processors (which is of course impossible)!!

Early investigators in this field were naturally excited by the potential of such immense computing power, and soon after realizing its potential, the hunt was on to find something interesting for a quantum computer to do. Peter Shor, a research and computer scientist at AT&T's Bell Laboratories in New Jersey, provided such an application by devising the first quantum computer algorithm. Shor's algorithm harnesses the power of quantum superposition to rapidly factor very large numbers (on the order $\sim 10^{200}$ digits and greater) in a matter of seconds. The premier application of a quantum computer capable of implementing this algorithm lies in the field of encryption, where one common (and best) encryption code, known as *RSA*, relies heavily on the difficulty of factoring very large composite numbers into their primes. A computer which can do this easily is naturally of great interest to numerous government agencies that use RSA – previously considered to be "uncrackable" – and anyone interested in electronic and financial privacy.

Encryption, however, is only one application of a quantum computer. In addition, Shor has put together a toolbox of mathematical operations that can only be performed on a quantum computer, many of which he used in his factorization algorithm. Furthermore, Feynman asserted that a quantum computer could function as a kind of simulator for quantum physics, potentially opening the doors to many discoveries in the field. Currently the power and capability of a quantum computer is primarily theoretical speculation; the advent of the first fully functional quantum computer will undoubtedly bring many new and exciting applications.

A Brief History of Quantum Computing

The idea of a computational device based on quantum mechanics was first explored in the 1970's and early 1980's by physicists and computer scientists such as Charles H. Bennett of the IBM Thomas J. Watson Research Center, Paul A. Benioff of Argonne National Laboratory in Illinois, David Deutsch of the University of Oxford, and the late Richard P. Feynman of the California Institute of Technology (Caltech).

The idea emerged when scientists were pondering the fundamental limits of computation. They understood that if technology continued to abide by Moore's Law, then the continually shrinking size of circuitry packed onto silicon chips would eventually reach a point where individual elements would be no larger than a few atoms. Here a problem arose because at the atomic scale the physical laws that govern the behavior and properties of the circuit are inherently quantum mechanical in nature, not classical. This then raised the question of whether a new kind of computer could be devised based on the principles of quantum physics.

Feynman was among the first to attempt to provide an answer to this question by producing an abstract model in 1982 that showed how a quantum system could be used to do computations. He also explained how such a machine would be able to act as a simulator for quantum physics. In other words, a physicist would have the ability to carry out experiments in quantum physics inside a quantum mechanical computer.

Later, in 1985, Deutsch realized that Feynman's assertion could eventually lead to a general purpose quantum computer and published a crucial theoretical paper showing that *any* physical process, in principle, could be modeled perfectly by a quantum computer. Thus, a quantum computer would have capabilities far beyond those of any traditional classical computer. After Deutsch published this paper, the search began to find interesting applications for such a machine.

Unfortunately, all that could be found were a few rather contrived mathematical problems, until Shor circulated in 1994 a preprint of a paper in which he set out a method for using quantum computers to crack an important problem in number theory, namely factorization. He showed how an ensemble of mathematical operations, designed specifically for a quantum computer, could be organized to enable a such a machine to factor huge numbers extremely rapidly, much faster than is possible on conventional computers. With this breakthrough, quantum computing transformed from a mere academic curiosity directly into a national and world interest.

Obstacles and Research

The field of quantum information processing has made numerous promising advancements since its conception, including the building of two- and three-qubit quantum computers capable of some simple arithmetic and data sorting. However, a few potentially large obstacles still remain that prevent us from "just building one", or more precisely, building a quantum computer that can rival today's modern digital computer. Among these difficulties, error correction, decoherence, and hardware architecture are probably the most formidable. Error correction is rather self explanatory, but what errors need correction? The answer is primarily those errors that arise as a direct result of *decoherence*, or the tendency of a quantum computer to decay from a given quantum state into an incoherent state as it interacts, or entangles, with the state of the environment. These interactions between the environment and qubits are unavoidable, and induce the breakdown of information stored in the quantum computer, and thus errors in computation. Before any quantum computer will be capable of solving hard problems, research must devise a way to maintain decoherence and other potential sources of error at an acceptable level. Thanks to the theory (and now reality) of quantum error correction, first proposed in 1995 and continually developed since, small scale quantum computers have been built and the prospects of large quantum computers are looking up. Probably the most important idea in this field is the application of error correction in *phase coherence* as a means to extract information and reduce error in a quantum system without actually measuring that system. In 1998, researches at Los Alamos National Laboratory and MIT led by Raymond Laflamme managed to spread a single bit of quantum information (qubit) across three nuclear spins in each molecule of a liquid solution of alanine or trichloroethylene molecules. They accomplished this using the techniques of nuclear magnetic resonance (NMR). This experiment is

significant because spreading out the information actually made it harder to corrupt. Quantum mechanics tells us that directly measuring the state of a qubit invariably destroys the superposition of states in which it exists, forcing it to become either a 0 or 1. The technique of spreading out the information allows researchers to utilize the property of entanglement to study the interactions between states as an indirect method for analyzing the quantum information. Rather than a direct measurement, the group compared the spins to see if any new differences arose between them without learning the information itself. This technique gave them the ability to detect and fix errors in a qubit's *phase coherence*, and thus maintain a higher level of coherence in the quantum system. This milestone has provided argument against skeptics, and hope for believers. Currently, research in quantum error correction continues with groups at Caltech (Preskill, Kimble), Microsoft, Los Alamos, and elsewhere.

At this point, only a few of the benefits of quantum computation and quantum computers are readily obvious, but before more possibilities are uncovered theory must be put to the test. In order to do this, devices capable of quantum computation must be constructed. Quantum computing hardware is, however, still in its infancy. As a result of several significant experiments, nuclear magnetic resonance (NMR) has become the most popular component in quantum hardware architecture. Only within the past year, a group from Los Alamos National Laboratory and MIT constructed the first experimental demonstrations of a quantum computer using nuclear magnetic resonance (NMR) technology. Currently, research is underway to discover methods for battling the destructive effects of *decoherence*, to develop an optimal hardware architecture for designing and building a quantum computer, and to further uncover quantum algorithms to utilize the immense computing power available in these devices. Naturally this pursuit is intimately related to quantum error correction codes and quantum algorithms, so a number of groups are doing simultaneous research in a number of these fields. To date, designs have involved ion traps, cavity quantum electrodynamics (QED), and NMR. Though these devices have had mild success in performing interesting experiments, the technologies each have serious limitations. Ion trap computers are limited in speed by the vibration frequency of the modes in the trap. NMR devices have an exponential attenuation of signal to noise as the number of qubits in a system increases. Cavity QED is slightly more promising; however, it still has only been demonstrated with a few qubits. Seth Lloyd of MIT is currently a prominent researcher in quantum hardware. The future of quantum computer hardware architecture is likely to be very different from what we know today; however, the current research has helped to provide insight as to what obstacles the future will hold for these devices.

Future Outlook

At present, quantum computers and quantum information technology remains in its pioneering stage. At this very moment obstacles are being surmounted that will provide the knowledge needed to thrust quantum computers up to their rightful position as the fastest computational machines in existence. Error correction has made promising progress to date, nearing a point now where we may have the tools required to build a computer robust enough to adequately withstand the effects of decoherence. Quantum hardware, on the other hand, remains an emerging field, but the work done thus far suggests that it will only be a matter time before we have devices large enough to test Shor's and other quantum algorithms. Thereby, quantum computers will emerge as the superior computational devices at the very least, and perhaps one day make today's modern computer obsolete. Quantum computation has its origins in highly specialized fields of theoretical physics, but its future undoubtedly lies in the profound effect it will have on the lives of all mankind.

References

[1] D. Deutsch, Proc. Roy. Soc. London, Ser. A **400**, 97 (1985).

[2] R. P. Feynman, Int. J. Theor. Phys. **21**, 467 (1982).

[3] J. Preskill, "Battling Decoherence: The Fault-Tolerant Quantum Computer," Physics Today, June (1999).

[4] Shor, P. W., *Algorithms for quantum computation: Discrete logarithms and factoring, in Proceedings of the 35th Annual Symposium on Foundations of Computer Science*, IEEE Computer Society Press (1994).

[5] Nielsen, M., "Quantum Computing," (unpublished notes) (1999).

[6] QUIC on-line, "Decoherence and Error Correction," (1997).

[7] D.G. Cory et al., Physical Review Letters, http://ojps.aip.org/prlo/, 7 Sept 1998.

[8] J. Preskill, "Quantum Computing: Pro and Con," quant-ph/9705032 v3, 26 Aug 1997.

[9] Chuang, I. L., Laflamme, R., Yamamoto, Y., "Decoherence and a Simple Quantum Computer," (1995).

[10] D. Deutsch, A. Ekert, "Quantum Computation," Physics World, March (1998).

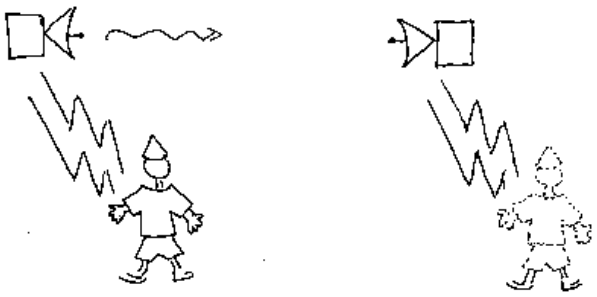
Teleportation: from fantasy to fact and back

Samuel L. Braunstein and Pieter kok

Since a few years, there is a lot of talk about teleportation. And indeed, it has become a reality: researchers have teleported photons, light beams and atoms over distances of up to a few meters. Can this be extended to the type of teleportation we see in the movies, involving people? And if so, when?

First of all, what do we mean with the term "teleportation"? If someone comes up to you saying "Look! I've finally done it: I've discovered how to teleport. . . ," we'd like to be able to decide whether we are even speaking the same language. Now we are all familiar with StarTrek®, so let's take a stab at defining it: *teleportation is some kind of instantaneous "disembodied" transport.*

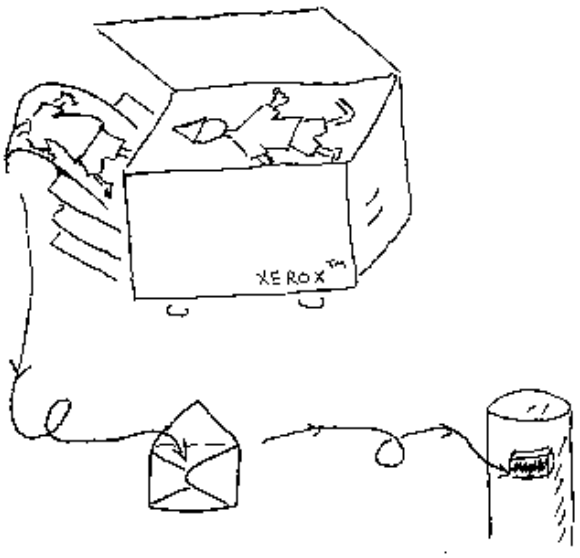
But wait a second! Einstein's theory of relativity — and many decades of experimental evidence back him to the hilt — says that the fastest speed is the speed of light. If we accept this as normative science, then we are going to have to change our definition immediately to: *teleportation is some kind of "disembodied" transport*. This is a little bit better, but we have been rather vague about the "disembodied". Perhaps we should let this figure be our guide to what that might mean:



When you think about this definition for a little while, you realize that we already have lots of examples of teleportation around us every day:

- telephone - transports sound waves as electricity,
- fax - transports an image,
- world wide web - . . .

Does this count as teleportation? They are really copying processes. They leave the sound, image, or what-have-you behind, and send the copy shooting across space in some disembodied way. But is this really the definition of teleportation we are looking for? They don't leave a copy of lieutenant Worf behind in our favorite TV program. Or perhaps that's just what they do: they have some machine that measures the positions and momenta and types of atoms throughout the entire person and then sends that information (for example by radio waves) to the place where the body is reconstructed by another machine. Actually, on TV they're also able to recreate the person from the information apparently without a machine to receive it. One thing at a time, please!



What about the original? Well, maybe the machine that measures all those atoms has to slice the person apart to do that. We guess that would be like a photocopy machine with such a hot flash lamp that it vaporizes the original. This wouldn't be a necessary requirement of teleportation, though: as soon as someone worked out how to build a more gentle copying process they could leave the original behind. Would they want to? Would the soul be copied? Would the copy still have to pay taxes if the original were still around? Surely the destruction of the original would raise all sorts of ethical questions! Of course if we could ever learn how to do this we might find new fields of research like "experimental religion." Who knows?

Just how much information are we talking about anyway? The visible human project by the American National Institute of Health requires about 10 Gigabytes (or about ten CD ROMs) to give the full three-dimensional details of a human, down to one millimeter resolution in each direction. If we forget about recognizing atoms and measuring their momenta and just scale that to a resolution of one-atomic length in each direction, that's about 10^{32} bits. This is so much information that even with the best optical fibers conceivable, it would take over one hundred million centuries to transmit all that information (compare this to approximately a hundred centuries of human civilization)! In fact, that is about as long as the universe is old. It would be easier to walk! If we packed all that information into CD ROMs it would fit into a cube almost 1000 kilometers on a side! Enough said?

"But what about the uncertainty principle" we hear you ask, "can you really measure things that accurately?" Well, quantum mechanics tells us that the precision with which we can measure position and momentum of any particle are limited by a very simple formula:

$$\text{uncertainty in position} \times \text{uncertainty in momentum} \gtrsim \text{Planck's constant}.$$

If we measure each atom to within a typical atomic size, the velocities will be uncertain by about 300 meters per second (if the particle weighs as much as a Hydrogen atom, say). This sounds fast, but it's not so bad. The ordinary jiggling of our atoms due to us being at room temperature is more than three times larger. In other words, the uncertainty principle doesn't appear to be too restrictive in terms of how well we can measure those atoms. Of course, that's not all. What about the "quantum state" of those atoms? Does it matter what energy levels they are all in? Do the chemical reactions need to have this information to work once we reassemble the atoms to make a person?

We don't believe that this is true, and neither do a number of other scientists we've asked. But that's hardly a definitive answer. What tends to convince people that the detailed quantum state is not important to get right, is that people routinely go to hospitals for NMR (nuclear magnetic resonance) and ESR (electron spin resonance) scans to see inside them. These scans mix up the quantum states of at least some large number of atoms and nuclei of the people being scanned — usually in their brain! — yet it doesn't seem to disturb their feeling of who they are, or even upset their appetites! (We should note that there are some eminent physicists and mathematicians, like Eugene Wigner, Roger Penrose and others who are not convinced and hold that consciousness requires quantum mechanics to be fully understood.) Thus here again the quantum nature of our atoms and molecules doesn't appear to rule

out the copying method for teleportation. The sheer amount of information involved is still mind boggling, though. Perhaps we should start with something smaller, like a subatomic particle.

When we want to teleport something like an electron, everything we have talked about so far changes: the amount of information we have to transport is actually rather small, but suddenly we do have to worry about the uncertainty principle. For example, we cannot find out with arbitrarily high precision in which direction the spinning axis of the electron is oriented, and whether the electron is spinning clockwise or counter-clockwise. This is called the "spin state" of the electron. This lack of precision rules out any teleportation scheme based on measuring, sending and recreating an atomic-scale system. It would violate the uncertainty principle and fundamental laws of quantum mechanics themselves. In fact, this prohibition against copying has itself been risen to the status of a law and is called the no-cloning principle. Notwithstanding this strong prohibition it turns out that we can *still* perfectly teleport the spin state of our electron, and this is where it really gets weird.

To see how we can get around no-cloning. Let's recall what teleportation should look like: A sender, whom we will call Alice, is given an electron in a spin state that is unknown to her. After "doing something" to the electron (we will talk about that in a minute), she contacts the receiver, whom we will call Bob, to teleport the electron. Alice can tell Bob anything she wants, but can only use a conventional communication channel, like radio or the telephone or even email. It is then Bob's job to put the spin state of the original electron onto one in his laboratory (he doesn't need to recreate the matter itself, just the information content!).

But there doesn't seem to be anything special about Bob here. Anybody could tap the communication channel that Alice is using, and simply apply the same recreation protocol that Bob is using. They too could create a copy of the state in their own lab. But as we have already argued, this would violate no-cloning. So if it really were to work, there would have to be something singling out Bob as the unique receiver. That special something is shared between himself and Alice and it is called quantum entanglement.

Entanglement is a property of two or more quantum particles, like electrons. So let's think about the entanglement between two electrons: suppose that they always have opposite spin. In other words, whenever the spin state of one electron in any given direction is clockwise, its partner must be spinning counter-clockwise in the same direction. When this is true for all possible spinning axes, the two electrons are called entangled. In fact, there are many kinds of entanglement, but this is the type we're interested in for now.

So we have three electrons: Alice's electron whose spin we want to teleport, and a second electron sitting right next to it in her lab. This second electron has an entangled partner that is waiting in Bob's lab. In principle, there is no limit to how far his lab is away. It might even be in another galaxy!

Now, what is this special "something" that Alice does to her electron? We somehow have to connect the initial electron with Bob's electron, and we can accomplish that by creating *new* entanglement between the two electrons at Alice's site. When we *measure* this new entanglement between the two electrons, we actually force them to have opposite spin states. However, the electron that was part of the quantum channel already had a spin state opposite to Bob's electron, so now the remote electron must be spinning in the same direction as the initial electron.

Hang on! Something is not quite right here. . . , we did not use the radio, the telephone or even email! Without such classical communication, teleportation is instantaneous, and this is forbidden by Einstein's laws. How can this be resolved?

As we said earlier, there are many kinds of entanglement, and the measurement Alice performed can actually give her *four* different outcomes. Every outcome corresponds to a slightly different type of entanglement, which corresponds to a different type of correlation between the entangled spins. Since she has

no way of predicting the measurement result, she has to correct for it at the remote electron. Which means: she has to send the outcome to Bob's lab, where the remote electron is sitting! For that, she uses a conventional communication channel — and in those, the information cannot move faster than the speed of light. Depending on this measurement result, Bob will rotate or flip the electron in a particular way to make the spin axis parallel to the original, and Bob's electron now has the same spin state as Alice's. This is quantum teleportation [1].

What exactly happened here? And what happened to the original electron? According to the no-cloning law, the spin state of the original electron must be destroyed, right? Indeed, by forcing it to become entangled with the electron of the quantum channel, we lost the original spin state. The spin state therefore truly disappears on one end, and it reappears at the remote end with perfect precision!

Another question is: what happened to the information of the spin state when it was teleported? The measurement outcome that we sent to the destination is totally random, so it does not contain any information about the spin state. Somehow, the information appears in Bob's electron instantaneously, but it must be made accessible by the transmission of Alice's measurement result.

The weirdest thing of all is perhaps that nobody needs to know the original spin state of the electron. When the initial electron is itself entangled to a fourth electron, it becomes meaningless to talk about its individual spin state. But the teleportation still works, and afterwards the fourth electron is entangled to Bob's remote electron! We call this *entanglement swapping*, because we start with two entangled pairs of electrons (1,2) and (3,4), and we end up with two entangled electrons (1,4) that have never even seen each other.

You might think this is truly science fiction, but amazingly people have actually done this in the lab. Instead of the spin state of the electron, they used polarization states of photons [2, 3, 4, 5], the quantum state of a light beam [6], and the spin state of a whole atom [7]. In most of these experiments the distance over which the quantum system was teleported was only about one meter (and only nanometers in one case [7]), however, using an optical fiber to share the entanglement, one group managed to perform quantum teleportation over *two kilometers* [4].

Of course, the aim of these experiments is not directed towards the eventual teleportation of people at all. In fact, all this research was carried out in the context of the development of a whole new technology that hopes to take advantage of the weirdness of quantum mechanics. Such technologies include quantum computers, which can do some calculations far more efficiently than the fastest conventional computer ever could. They also include quantum communication which can allow provably secure communication no matter how advanced the technology of an eavesdropper.

Fine, but it's fun to speculate. So let's do just that. Suppose we wanted to simply build a fancy big three-dimensional fax machine which could scan and transmit people to where-ever a receiving machine could rebuild them. We already argued that the best known communication channels would be woefully inadequate to transfer the apparently huge amount of information involved. But technology improves at an incredible rate. Will the limitations to our communication bandwidth always be a barrier to such a feat?

Let's build our speculations on those of others. Back in 1965 Gordon Moore predicted that the complexity and processing power of computer chips would double every 12 to 18 months. Considering that this was shortly after the invention of the transistor it's an amazing prediction. Even more amazing because the semiconductor industry has used this prediction as a roadmap for developing and introducing new technology. This increase in capacity to process information doesn't quite generalize to improved communication bandwidth, which doesn't improve at quite this rate, but let's take this figure as a benchmark for our speculations.

At this rate of doubling, to have a communication channel which could transfer the huge amounts of information we mentioned would take about another 100 years. But don't ex-

pect anything before then unless totally new physics is involved. And all this is a 'shortest' time estimate. It's much more likely we'll be stuck to conventional travel, due to the demise of Moore's law. And then we'd never be able to teleport.

In fact, Moore's law is not expected to last beyond about 2017 when transistors would have shrunk to a size where their switching would be controlled by individual electrons. But maybe we can extend its reach. After all, our computer chips are still primarily two-dimensional. If we could deal with the heating problem (say by devising near reversible computer logic gates) we could conceive of building chips with as much complexity in the third dimension as they currently have in those of the silicon substrate. Even without finding a way of shrinking transistors to be smaller than atoms this could give Moore's law room for another 50 years expansion beyond its predicted end. However, this would still leave us way short of our bandwidth goal!

Maybe we don't really need to transmit all the information about a person. What about some sort of intelligent compression routine? Unfortunately, this routine would have to be really good, offering compression factors of millions of billions (not simply a factor of 10, which we might get when we compress with 'zip'). It could be that future biology will help us understand how much information is really important. However, would you want to have your brain compressed? (Actually, compression might not hurt too much, since most people tend to use only 10% of their brain power anyway. . .)

Perhaps the likes of Wigner and Penrose will turn out to be right after all, in that the quantum state is crucial for successful teleportation of a person. But that's OK, because quantum teleportation tells us how to teleport all that quantum stuff without violating any fundamental laws. Of course, to find out who's right, it looks like we'll have no choice but to wait and see. . .

References

[1] C.H. Bennett, G. Brassard, C. Cr/'epeau, R. Jozsa, A. Peres, and W.K. Wootters, *Teleportation of an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels*, Phys. Rev. Lett. **70**, 1895 (1993).

[2] D. Bouwmeester, J.-W. Pan, K. Mattle, M. Eibl, H. Weinfurter, and A. Zeilinger, *Experimental quantum teleportation*, Nature (London) **390** 575 (1997).

[3] D. Boschi, S. Branca, F. DeMartini, L. Hardy, and S. Popescu, *Experimental realization of teleporting an unknown pure quantum state via dual classical and Einstein-Podolsky-Rosen channels* Phys. Rev. Lett. **80**, 1121 (1998).

[4] I. Marcikic, H. de Riedmatten, W. Tittel, H. Zbinden, and N. Gisin, *Long-distance quantum teleportation of qubits at telecommunication wavelengths*, Nature (London) **421**, 509 (2003).

[5] J.-W. Pan, S. Gasparoni, M. Aspelmeyer, T. Jennewein, and A. Zeilinger, *Experimental realization of freely propagating teleported qubits*, Nature (London) **421**, 721 (2003).

[6] A. Furusawa, J.L. Sorensen, S.L. Braunstein, C.A. Fuchs, H.J. Kimble, and E.S. Polzik, *Unconditional quantum teleportation*, Science **282**, 706 (1998).

[7] M.A. Nielsen, E. Knill, and R. Laflamme, *Complete quantum teleportation using nuclear magnetic resonance*, Nature (London) **396**, 52 (1998).

Professor Braunstein has joined the University of Wales, Bangor, in 1997 and is heading a group in quantum information science. He was born in Melbourne, Australia in 1961. He was awarded a BSc (Honors) and MSc in Physics from the University of Melbroune and received his PhD in Physics from the California Institute of Technology in 1988.

Professor Braunstein is a recipient of the prestigious Royal Society-Wolfson Research Merit Award - a five-year 20m scheme created to attract and retain the best scientific talent in the UK. He was recently awarded the honorary title of 2001 Lord Kelvin Lecturer. Before joining the University of Wales, he held a prestigious German Humboldt Fellowship (spent at the University of Ulm).

He is editor of two books “Quantum Computing” and “Scalable Quantum Computing” and serves on the editorial board of the journal Fortschritte der Physik for which he has prepared two special issues on quantum computation. He has initiated and is a Founding Managing Editor of Quantum Information and Computation – the first journal dedicated specifically to this field. Its first issue appeared in July 2001.

He has over 60 papers published in refereed journals, which have been cited almost two thousand times, including 16 papers in Physical Review Letters, 3 in Nature and 1 in Science. His work on quantum teleportation, quantum computation, quantum lithography and quantum information has received extensive coverage in prestigious scientific venues such as Science, Nature, Physics Today, New Scientist and Optics & Photonics News, as well as on radio, television and daily newspapers (The Independent, The Times, The New York Times and more).

Professor Braunstein’s most cited work on quantum teleportation was chosen among the ‘top ten [scientific] breakthroughs’ of 1998 by the journal Science.

Dr. Pieter Kok is a postdoc in the Quantum Computing Technologies Group at the Jet Propulsion Laboratory in Pasadena, USA. He holds a degree in Foundations of Quantum Theory from the University of Utrecht, and received his Ph.D. in physics from the University of Wales, Bangor. His research interests include quantum teleportation, quantum lithography, optical quantum computers, and the interpretation of quantum mechanics.

XOOTIC Survey 2002

Marinelle van Dongen (on behalf of the survey committee)

In October 2002, the bi-annual XOOTIC *questionnaire was sent out again to all* XOOTIC *members to ask them about their current and future work, and about their opinion of* OOTI *and* XOOTIC*. In the past months, the returned questionnaires have been analysed and the results have been presented to the* XOOTIC *members April 4th 2003. This article presents the survey results.*

Introduction

The XOOTIC survey has become a biannual tradition. It provides valuable feedback to both the OOTI and the XOOTIC board on their program and their activities. Previous surveys were held in 1993, 1994, 1996, 1998, and 2000 (see XOOTIC MAGAZINE September 1993, September 1994, April 1996, October 1999, and April 2001, respectively). The survey committee, Lucian Voinea, Sergei Shumski, and myself set out to organise the survey for 2002. The first thing we did, was to take the previous questionnaire and modify it according to suggestions for improvement that were given during the previous survey and according to our own ideas. That mainly came down to changing the options in the answer-lists of a number of questions: adding and/or deleting options. Also, we added explanations to specific abbreviations.

We had to be careful not to change too much in the questionnaire, because otherwise the results are difficult/impossible to compare with previous surveys. That is why the general look of the questionnaire has been left (more or less) unchanged.

The questionnaire was sent to every XOOTIC member early October 2002. Table 1 shows the number of surveys that were sent out and the number of surveys that were returned this year as well as previous years.

Survey	Nr sent	Nr received	Percentage
1993	22	17	77%
1994	41	24	59%
1996	88	43	49%
1998	155	69	45%
2000	189	88	47%
2002	210	69	33%

Table 1: History of returned questionnaires.

The questionnaire was returned this time by only 69 members. That was amazingly less than expected. As you can see, the number of returned questionnaires was vast growing until this year. That means that, in these results, about every 3% is one person. In 1998 this number was 1.4% and in 2000 even 1.1%!

Figure 1 shows the returned questionnaires per generation. We see that the large decrease of returned forms can mainly be assigned to the generations ”September 1992 - January 1994”, ”September 1992 - March 1996”, and ”September 1996 - April 1998”. An explanation could be, that the older generations feel less involved in the OOTI whereabouts. If this is true, there has to be done something about that!

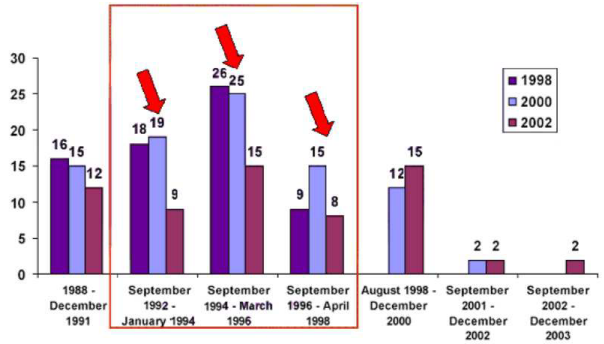


Figure 1: Number of returned questionnaires per generation.

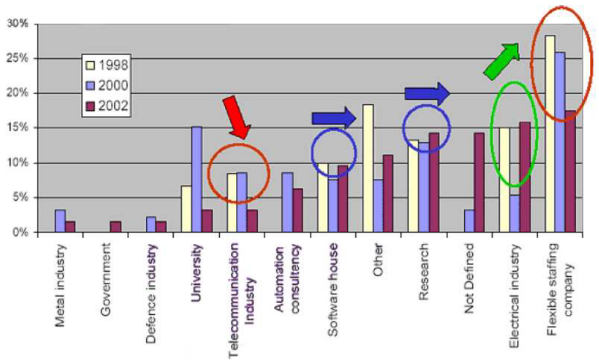


Figure 2: Branch distribution.

Employer

The questions about the current employer are intended to get an impression of the employer where XOOTIC members are working. Figure 2 shows the major branches where ex-OOTIS are working now. Compared to the results of the previous survey, there are some significant changes. The top losers are: *Flexible staffing company*, *Telecommunication industry*, and *University* (less OOTIS filled in the questionnaire). The top gainer is *Electrical industry*, who was the top loser last time.

Further, it looks like there is a trend to switch to a job at a company that is bigger and perhaps more safer in this economic climate. Was in 2000 still upwards of 13% of the members working for a small company (0..25 employees), this time that number is decreased to 6%. The opposite happened at the other side of the list. Large companies (>20.000 employees) are suddenly more popular: 8% this time against a good 2% last time. Apart from that, companies with a size of 100-500 employees are still the most popular (27%).

Figure 3 indicates how many jobs our generations have had since they started the OOTI course. It is striking how many of us are still working for their first employer. The best example for this is the generation Sep '96 - Apr '98. Most of them are still working for their first employer and only a few switched jobs. Another conclusion could be that within 2 years about half of this generation (Sep '96 - Apr '98) will change jobs.

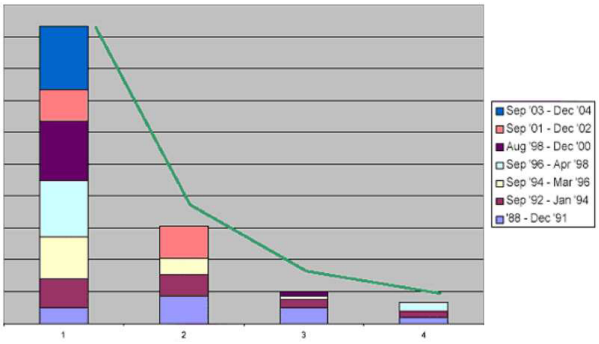


Figure 3: Number of employers.

The main reason why the current employer has been chosen is, like in 2000, *nature of the work*, followed by *geographical location*, *career perspective*, and *company culture*. *Salary* is not such a hot topic any more. Striking is the growth of almost all the options (except *products of the company*). Are we becoming more critical?

Figure 4 shows that the *final project of* OOTI and a direct approach by the company or a person working for the company (ex-OOTI or not) are still successful strategies of recruiting ex-OOTIS (55%). But, this time less OOTIS

found a job via an ex-OOTI and more found a job via a non-ex-OOTI. The *open application*, which became more and more unpopular over the years, gained a few percent this time: the option dropped from 47% in 1996, via 25% in 1998 to 14% in 2000, but climbed to 19% this time.

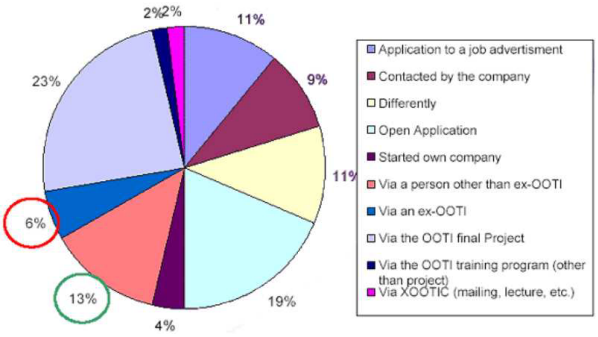


Figure 4: How did we get our current job?

Function

The results of the current & future function and working environment tell us something about our daily work and our expectations. If you look at Figure 5, you will notice that the XOOTIC members currently still have very technical jobs: 71% are *software/system engineer/architect* or *researcher*, compared to 73% in 2000 and 64% in 1998. But there is also a trend in moving to more leadership functions like *board member*, *project leader*, and *team leader*. And again *software architect* is the big winner. Further, this distribution can be found in all generations. It is not true that, the longer we work, the more leading function we get. When we asked which future function the members preferred, the picture looked the same: 29% preferred *software engineer*, 25% *software architect*, 9% *project leader*, and 9% *researcher/scientist*.

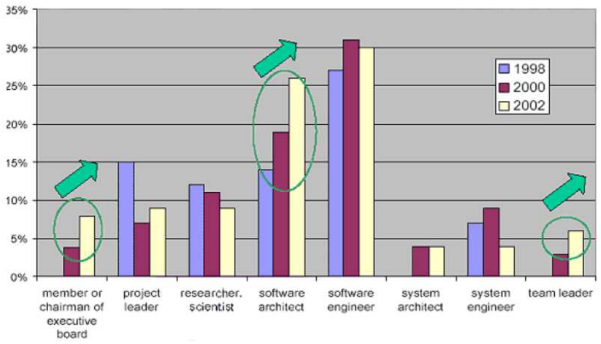


Figure 5: Current functions.

The distribution of disciplines in the current function shows a striking growth in the *computing science* and *information technology* sectors. There is a big shift from related disciplines (*physics*, *logistics*, *telecommunication*, *economics*, *electrical engineering*, and *business engineering*) to pure informatics. In 2000, this trend already started, But now it is extremely more clear.

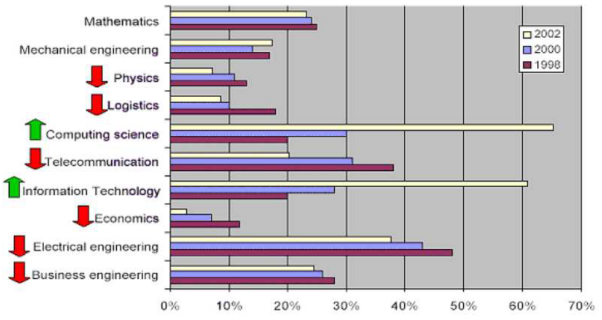


Figure 6: Disciplines of current function.

Skills

There were several questions concerning the tools and methods that are being used around the working place of an ex-OOTI. Like two years ago, **formal methods** are being used: 15% of the returned questionnaires indicated that methods like Chi, Spin, Promela, YAPI, and EXPECT were used in their direct working environment.

We are also happy to see that **design methods** are being used more and more. *Design patterns* grows from 51% (2 years ago) to 67%,

OMT grown from 33% to 48%, and *architectural patterns* from 21% to 43%. Poor *ROOM* is again being used only by one person. But there is also a downside. Design methods do not have our interest any more. The interest in *design patterns* has been halved from 40% to 21% and *architectural patterns* falls from 44% to 33%. *ROOM* is a big winner here: although almost nobody uses it, 21% of the members is interested in it (against 7% 2 years ago)!

The same trend, we observed in the use of and interest in **programming languages**. Languages like *C*, *JAVA*, *Scripting languages*, and *Visual Basic* are used more and more, but we loose our interest in them. The exception to this rule is *C#*. This was, by the way, a new option in the choice-list of this survey. With *C#* there are more people that are interested in it (24%) than use it in the working environment (14%) and that is not the case with any other language.

Windows NT is used most as a host **platform** (88%), directly followed by *Unix* (65%) and *Linux* (44%). The dominant used target platforms are: *Windows NT*, *Unix*, and *Linux*, directly followed by *Java Platform* and *pSOS+*. Note that *Unix* and *Linux* are more than doubling their use in 2 years! (see Figure 7) The answers given show that the interest in platforms is decreasing except for the interest in *Linux* and *Palm OS*.

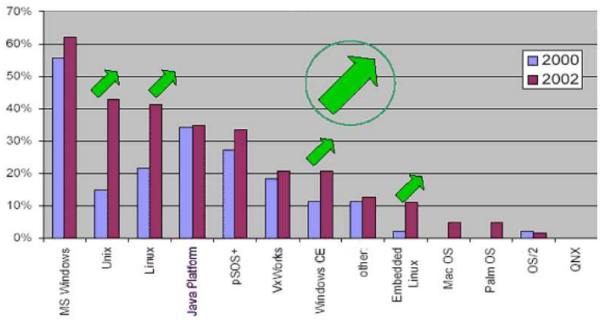


Figure 7: Target platforms used.

XML, *Automated testing*, *Distributed-* and *Component technologies* are very popular on the work floor of ex-OOTIS: on the average 45% uses these **technologies**. But only half of the ex-OOTIS are interested in them. . . The only technology that is popular, is *.NET* (27% is interested and 21% uses it).

The usage of the *waterfall model* is fast growing (58% in 2002 against 34% in 2000) and again the most used **process model**, followed by *Rational Unified Process* (37% in 2002 against 7% in 2000) and *Extreme programming* (30% in 2002 against 19% in 2000). XOOTIC members are, like in 2000, most interested in *Extreme Programming* (40%), so we can conclude that this is not a hype.

Then the big question rises where the interest in **skills** of the XOOTIC members lays. This is a considerable different picture than 2 years ago. See for yourself in Figure 8 what has happened.

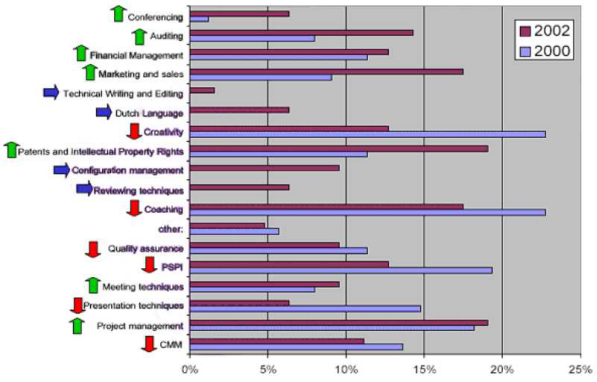


Figure 8: Interesting skills.

Working conditions

This section gives us an indication of the conditions of employment. Table 2 shows the current **salaries** of the 56 ex-OOTIS who filled in the question.

Currently 5 ex-OOTIS (equals approximately to 8%) are **working part-time** and 22 ex-OOTIS (34%) would like to work part-time.

54% of the ex-OOTIS reported to have *no signs* of **RSI**, 35% responded *sometimes*, 5% *quite often* and 6% *very often*. Those numbers are almost the same as last time.

59% of the ex-OOTIS give **guidance** to *1..5 persons*, 25% give guidance to *6..10 persons*, no one gives guidance to *15..50 persons*, and 5% of us guide *more than 50 people*.

Generation	≤ 20	≤ 30	≤ 35	≤ 40	≤ 45	≤ 50	≤ 55	≤ 60	> 60
1988 - Dec 1991						2	4		6
Sep 1992 - Jan 1994					1	3	3	1	1
Sep 1994 - Mar 1996					2	5	4	1	1
Sep 1996 - Apr 1998			1	4	1	1	1		
Aug 1998 - Dec 2000	1	2	3	6	1				1
Dec 2002 - Dec 2003									

Table 2: Salary distribution in EURO 1000 (absolute numbers of ex-OOTIs).

OOTI training program

The questions about the current Software Technology program only have to be filled in by the OOTIs who started their program after August 1994. The current courses were listed and the trainees of OOTI were asked to indicate their value/usefulness of the individual courses and whether they have applied the knowledge from the course during their work. Finally, they were asked to indicate the amount of time OOTI should allocate to each course.

The top 5 of *most useful* courses are:

1. Software Process Improvement (SPI) Basics [2000: not in top5]
2. Technical Writing and Editing [2000: place 4]
3. Workshop Software Engineering [2000: place 2]
4. Industrial Design and Development Project [2000: place 1]
5. System and Software Architecture [2000: place 5]

The top 5 of *least useful* courses are [same order as in 2000]:

1. Workshop on Declarative Method (PVS)
2. Workshop on Constructive Method (SPIN)
3. Formal Methods in the Software Life Cycle
4. Seminars with Industry (FM)
5. Control and System Theory

The top 5 of *most applicable* courses are:

1. Technical Writing and Editing
2. Workshop Software Engineering
3. Industrial Design and Development Project
4. System and Software Architecture
5. Software Process Improvement (SPI) Basics

The top 5 of *least applicable* courses are:

1. Workshop on Declarative Method (PVS)
2. Workshop on Constructive Method (SPIN)
3. Formal Methods in the Software Life Cycle
4. Control and System Theory
5. Seminars with Industry (FM)

XOOTIC

Again, the main reason to be a member of XOOTIC is to *stay in touch with other* XOOTIC *members* (28%). To *stay informed about the TU/e and/or* OOTI (21%) is the second reason. The XOOTIC MAGAZINE (19%) and *lectures* (15%) are the most appreciated XOOTIC activities.

We also asked the members to imagine they were unemployed. We then asked the question if they think XOOTIC could help them find a new job. 32% of the members thought *yes*, 21% thought *no*, and 47% *didn't know* or *wouldn't say*. That's a good score!

Suggestions for lectures are:

- Series of lectures on a single theme, giving room for technical depth and comparison.
- Knowledge transfer sessions about new technologies (e.g. Bluetooth).
- Organize a seminar with a guru (CMG like).
- Lectures on Saturdays, in large cities (Rotterdam, Amsterdam), with lunch.
- Regular lectures about the latest developments in the field of computer science.
- Organize a symposium on embedded sys-

tems.

Suggestions for activities are:

- Company visits/excursions to a company of one of the members.
- Major XOOTIC event.
- Organize study groups with the industry on hot topics.
- Excursions to countries where OOTIs come from.
- More social events like Paintball, BBQ, and midget golf.

Other suggestions are:

- Larger XOOTIC magazine and bring it out more often.
- Advertise MTD (e.g. via logos on t-shirts).
- Lower membership fees.

Conclusion

The results of this survey are very valuable for OOTI and XOOTIC. It allows them to measure the quality of the program, steer the program and verify whether changes to the curriculum have the desired effect. The results can also be used to identify trends and interests of XOOTIC members and to take advantage of this information. This report only gives a summary of the survey results. More detailed results have been given to the OOTI and XOOTIC boards.

The survey committee also received some recommendations:

- Use survey results to build the spending policy.
- Use the survey results to check if ex-OOTIs satisfy the goals of OOTI.
- Use the survey results to check if changes in the curriculum have the intended result.

We would like to pass these recommendations to the XOOTIC Survey 2004 Committee. We would like to thank all XOOTIC members who returned their questionnaire for their cooperation. Without their effort, we could not have presented these results! Also we would like to thank the XOOTIC Survey 1998 and 2000 Committees for their support and useful input. One word of special thanks goes to Harold Weffers.

The XOOTIC Survey 2002 Committee: Lucian Voinea, Sergei Shumski, and Marinelle van Dongen.