cnrs

n° 20
Quarterly
January 2011

international magazine

THE FUTURE OF Computing Science

Gérard Férey

Recipient of the
CNRS 2010 Gold Medal

cnrs
advancing the frontiers

Editorial

© B. WERNER/ ECOLE POLYTECHNIQUE

BY PHILIPPE BAPTISTE,
SCIENTIFIC DIRECTOR OF THE CNRS INSTITUTE
FOR COMPUTER SCIENCES (INS2I)

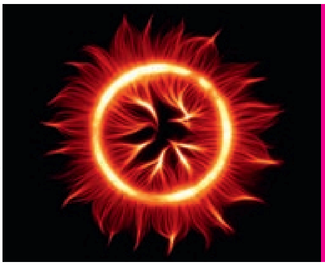
Recent advances in computer and information sciences have triggered a revolution whose spectacular developments have radically transformed our daily lives. Today, CNRS faces new challenges in digital technology, especially in the health and environmental protection sectors.

By founding the Institute for Computer Sciences (INS2I),[1] our national research center has strengthened its position in this highly competitive area. With the primary goal of pushing the boundaries of computer science and information technology, the INS2I is also actively involved in research at the interface of software and hardware, like automatic control, signals, imaging, robotics, and systems-on-chip. This interdisciplinarity, which makes new tools and concepts available in all disciplines, is at the heart of CNRS's agenda. What's more, CNRS welcomes all current and future debates raised by such novel scientific and social practices.

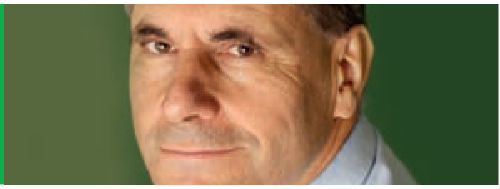
Through the INS2I, CNRS intends to pursue a policy of excellence for the benefit of the scientific community, while encouraging knowledge transfer and enhancement through partnerships with industry. It also intends to develop international collaborations through new international joint laboratories like the Japanese-French Laboratory for Informatics (JFLI), created in 2009 in Tokyo.[2] Similar structures are being developed with Argentina and Canada, both in areas related to the foundations of computer science. They should be operational by 2011.

[01] Institut des sciences informatiques et de leurs interactions.
[02] With the University of Tokyo, Keio University, and the National Institute of Informatics (NII) of Japan.

Contents



© A.-C. REYMANN/CEA



© C. LEBEDINSKY/CNRS PHOTOTHÈQUE

© C. FRESILLON/CNRS PHOTOTHÈQUE ; ESA, HFI ET LFI CONSORTIA

The Future of Computing Science

Information technology has revolutionized all facets of communications, from the personal computer to the latest and trendiest smart phones. Yet it has also given a radical boost to research, lending scientists enormous amounts of computing power to locate distant galaxies, devise climate models, sequence the human genome, or model our organs. And this is still only the beginning. Research laboratories around the world are busy developing a new Internet that will also connect billions of objects together, inventing powerful data processing technologies, and edging closer to the much-awaited quantum computers. CNRS International Magazine reports on the latest bytes, bits, and qubits that make up the bright future of one of the fastest growing fields in science.

A SURVEY BY MATHIEU GROUSSON AND VAHÉ TER MINASSIAN

The Digital **Revolution**

“**It is a fundamental and inevitable revolution,** comparable to the invention of the steam engine, which marked the beginning of the industrial age,[1]” says Gérard Berry, member of the French Academy of Sciences and 2009-2010 Chair of Computing and Digital Sciences at the Collège de France. “Our civilization is going digital. Traditional industries, such as telecommunications, and the dissemination of culture are undergoing drastic changes. Others, such as IT and associated services, are expanding at lightning speed. The Internet has revolutionized communications by eliminating such constraints as distance, time, and volume. In science, computer modeling of any phenomena has become standard.” Twenty-one years after the invention of the World Wide Web—the Internet's main application—it would be both tedious and futile to attempt to list the countless upheavals generated by recent progress in computing. Yet they are comparatively few considering what the future has in store.

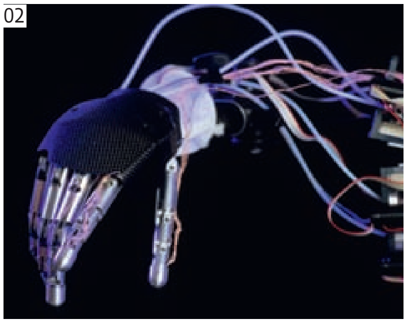
FAST EXPANSION

What will this digital world of the future be like? Difficult to say. New applications shake up the IT industry every week. Nevertheless, specialists predict a spec-

01 The 32 high-definition screens of the Wild platform can display extremely large images. Featured here is one of the most detailed photographs of our galaxy taken to date, 450,000 pixels wide.

© C. FRÉSILLON/CNRS PHOTOTHÈQUE ; ESA, HFI ET LFI CONSORTIA

02



© M. BREGA/LOOKATSCIENCES

02 In the future, electronic prostheses such as that of the Cyberhand project will be directly connected to the nervous system.

tacular expansion of the Internet, which will eventually connect not only people, but also objects near and even inside us. “Today, autonomous computers worldwide are 15 to 20 times more numerous than computers that interact with humans,” explains Berry. For example, the latest car models feature more than 80 microprocessors that control everything from braking to combustion. “Currently, these hundreds of billions of processors scattered all around us are not interconnected. Tomorrow, with the advent of this ‘Internet of Things,’ all these machines will communicate with one another to collectively produce new applications. The road itself will communicate with our vehicles to inform on speed limits, warn about traffic jams, or monitor trajectories to avoid accidents.”

Electronic prostheses will be directly connected to our nervous system, and circuits in patients’ bodies will send information on their health to a hospital’s IT system. Ultimately, it is the physicians who will call their patients in case of remotely detected problems, and not the other way around.

Meanwhile, the way we control the machines designed to receive our instructions will also radically change. Touch screens and motion detectors could soon replace keyboards and mice on desktop computers. Furthermore, progress in the semantic Web will provide intelligent search engines able to find information on the Web based on the meaning of a question rather than on its syntax. “Finally, applications such as Twitter and Facebook, as well as the commercial success of smartphones, have changed the core utility of the Web. It is no longer just a giant repository of information, but also an interactive space where people communicate with one another,” notes Serge Abiteboul, scientist at the LSV[2] and at INRIA[3] Saclay. “In fact, some people are permanently connected to this space via their cell phones,” adds this specialist in the management of the highly disseminated data and knowledge of the present-day Web—where information is accessed via numerous channels (computers, cell phones, websites, social networks, etc.).

© KAKSONEN/INRIA

03

ADAPTING TO THE FUTURE

Such upheavals require major adjustments. “Despite the Internet’s ability to integrate new technologies and applications—a key factor in its success—this evolution also makes it vulnerable,” explains Serge Fdida, professor at the LIP6[4] and coordinator of the European platform OneLab,[5] a European project tackling the future Internet. “Although its basic principle is not threatened, the Internet was not designed to handle demands like mobility, security, and platform diversity on a large scale: the combination of these factors disrupts its current structure. One must remember that the Internet was initially designed for clearly-identified, trustworthy individuals using static devices. This is certainly not the case today. Furthermore, the system has gradually changed to provide numerous services, leading to the development of ad hoc solutions such as security management, mobility, or content distribution using overlays. Yet most of these solutions are poorly integrated, making it very complex to manage the network and ensure its efficiency.”

A selection of **pictures** from the traveling exhibit **A Digital World** can be viewed on the online version of CNRS Magazine
› http://www2.cnrs.fr/en/384.htm

03 Multipoint touch screens used by the iPARLA team at Labri make it possible to manipulate 3-D objects. 04 The proliferation of mobile terminals requires new network architectures, tested here on high-mobility small objects wirelessly connected to one another.

Four or five years ago, this situation prompted several countries including the US, Germany, and Japan to launch ambitious research programs intended to lay the foundations of a more modular Internet for the future. In Europe, the Fire project aims in particular to set up by 2015 an experimental platform for scientists, industry, and small and medium businesses to securely design, deploy, and test new tools and Web services. The OneLab platform is the first step—a test phase of sorts—for this giant undertaking. This prototype, which has been operational for three years, provides access to a restricted network of 1000 interconnected computers worldwide and to other research platforms. It has already made it possible to test several applications in a variety of fields like Internet content distribution (videos, eBooks, music), and allowed the geolocation of IP addresses (the number used to identify every computer connected to the Internet).

Another challenge brought on by the increasing mobility of users is the limits of radio technologies for mobile IT services. "Second-generation mobile phone networks such as GSM were designed to transmit voice, not to send images or videos, or connect to digital television or the Internet," notes Pierre Duhamel, senior researcher at the L2S.[6] As a result, these networks are often close to saturation in large cities. "Several solutions are being investigated, including network coding—where data is sent over a network made up of other cell phones that may act as transmitters, receivers, relays, or routers. In any event, our research teams are allocating most of their time and effort to meet this challenge," he adds. Indeed, since September 2010, Duhamel is coordinating the first major project dedicated to this innovative field of network cooperation, as part of the Digiteo Advanced Thematic Research Networks[7] in the Paris region.

SYSTEMS SECURITY

Security—first and foremost that of people—is also a major concern. The plethora of embedded processors performing a wide variety of functions in our environment, without human intervention, already offer appreciable guarantees in terms of responsiveness, availability, and autonomy. Now engineers no longer hesitate to entrust "mission-critical" processors with tasks where human lives are at risk, such as the control of nuclear power plants, aircraft operation, or computer-assisted surgery. Yet "these systems are very expensive to design," says Joseph Sifakis, CNRS researcher at the Verimag laboratory[8] and 2007 winner of the prestigious Turing Award—the IT equivalent of the Nobel prize. "Writing mission-critical software requires specific development methodologies. This type of program is 1000 times more expensive than regular software, and must be submitted to an international certification authority." And while industrial methods for verifying such embedded systems do exist—current methods involve a type of model checking co-invented by Sifakis—they remain ineffective beyond a certain level of complexity. "This prevents the roll-out of several technologies requiring high availability or responsiveness. This includes medical or vehicle-operation software, but also applications relating to the 'Internet of Things' where an additional step is necessary to enable the cooperation of numerous embedded systems in a non-critical Internet environment, i.e., that offers little security."

04

© C. LEBEDINSKY/INRIA

Faced with these challenges, some scientists, following Sifakis' example, have revisited the theory, hoping to find solutions that would avoid a posteriori verification. "When engineers build a bridge, they use mathematical equations that guarantee that the structure will not collapse," he says. "No such tools are available to programmers: they must build systems first and check operation afterwards. My colleagues and I are trying to identify the theoretical basis that would guarantee that a computer system built from basic components would function properly."

THE HACKING PROBLEM

Finally, the increase in communicating objects makes IT security breaches a growing challenge. Users are often unaware that their computers have been hacked. Mobile phones, credit cards, game consoles, as well as electronic keys or pay TV sets are all potential areas of study for the cryptographers who design security mechanisms, and the cryptanalysts who try to break them. “Today we are sharing more and more personal information, with little or no control over where it ends up. That is why identity theft and the protection of our private lives are among today’s biggest concerns,” says Phong Nguyen, researcher at the LIENS laboratory[9] in Paris. Some researchers on the Crypto team at ENS are working on provable security, i.e., ways to improve security guarantees on cryptographic programs. Others are testing the limits of existing security systems by devising the best types of attack against a given cryptographic scheme. This can go as far as trying to recover data from a smart card by observing its electrical consumption or its electromagnetic radiation… For Nguyen, this cat and mouse game will eventually apply to tomorrow’s technologies such as quantum computers, although “if such a technology sees the light of day, we will have to transform much of today’s cryptography.”

CRYPTOGRAPHY All relevant techniques that ensure the secure transmission of data.

CONTACT INFORMATION:
Serge Abiteboul
› serge.abiteboul@inria.fr
Gérard Berry
› gerard.berry@sophia.inria.fr
Pierre Duhamel
› pierre.duhamel@lss.supelec.fr
Serge Fdida
› serge.fdida@lip6.fr
Phong Nguyen
› phong.nguyen@ens.fr
Joseph Sifakis
› joseph.sifakis@imag.fr

01. Gérard Berry, *Pourquoi et comment le monde devient numérique*, coll. “Leçons inaugurales du Collège de France” (Paris: Collège de France / Fayard, 2008).
02. Laboratoire spécification et vérification (CNRS / ENS Cachan).
03. Institut national de recherche en informatique et en automatique.
04. Laboratoire d’informatique de Paris-6 (CNRS / UPMC).
05. www.onelab.eu
06. Laboratoire des signaux et systèmes (CNRS / Supélec / Université Paris-Sud-XI).
07. Digiteo is a research platform dedicated to science and technology. With a staff of 1200 researchers from six institutes, the platform collaborates on a number of projects.
08. CNRS / Université Joseph-Fourier / Grenoble INP.
09. Laboratoire d’informatique de l’ENS (CNRS / ENS Paris / INRIA).

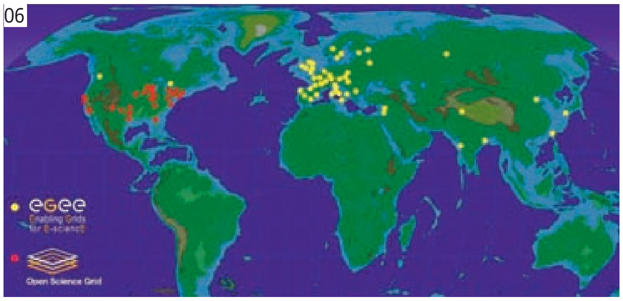
05 In cryptography, data is frequently condensed (or “hashed”). The resulting condensed file makes it possible to generate a digital signature used to authenticate a message sender.

© KAKSONEN/INRIA

Navigating the Datasphere

“**Whether you’re a tourist looking for the cheapest airline ticket,** a physicist analyzing data from a particle accelerator, or an employee at a temp agency sifting through applications, you all have something in common,” says Amedeo Napoli from the IT specialized LORIA[1] laboratory in Vandœuvre-lès-Nancy. “You are trying to extract specific information from a huge amount of data.” In principle, solving this problem couldn’t be simpler: prepare the initial data, feed it to a data mining algorithm, and wait for the system to provide the results in the required format. But in a world where that volume of data is increasing relentlessly, extracting pertinent knowledge becomes a seemingly impossible task.

06



© CERN

06 Location of sites involved in the world’s two largest grid infrastructures: Egee in Europe (in yellow) and OSG in the US (in red).

Looking for a holiday flight, hotel, and rental car, all at the lowest possible price, is a good example. As Michel Beaudouin-Lafon, from the LRI in Orsay[2] puts it: “Mathematically, we know that the complexity of this type of problem makes it impossible to find an exact solution in reasonable time, given the massive amount of input data.” Therefore, in practice, programmers must find clever ways of obtaining the most accurate result within reasonable time. In fact, the burgeoning field of data mining brings together specialists from fields as different as computer science, of course, but also machine architecture, linguistics, and mathematics. These specialists use artificial intelligence, databases, learning techniques, and statistical methods.

OPTIMIZING DATA SIFTING

One thing is certain: every field needs to develop efficient methods to avoid being flooded with unusable data often impossible to store. Take the French Midas project,[3] for example. It brings together, among others, CNRS labs and companies that have to deal with complex sets of data, like the telecommunications company Orange or the French energy provider EDF. Its goal is to develop an algorithm able to condense a large amount of data generated in real time so that it can be stored in a limited central memory for later use. “This is typically the type of situation that France Télécom, EDF, or the French national railway company SNCF have to deal with every day,” says Pascal Poncelet of the LIRMM,[4] in Montpellier. “For example, a TGV high-speed train records 250 data points per carriage every five minutes to anticipate maintenance operations. But such a huge amount of data is impossible to store. Events must therefore be sorted by order of importance, which changes over time.”

Scientists themselves are heavy users of data mining techniques. The LHC, CERN’S giant particle collider in Geneva, is a prime example. When it reaches its full capacity, 40 million proton collisions will occur every second. Yet physicists estimate that just 100 of those will be of interest and will need to be recorded. Such events will have to be selected in real time using specialized algorithms. “These are typically learning algorithms where the computer’s performance improves as it processes the new data to be kept or rejected,” explains Beaudouin-Lafon, whose laboratory is involved with the LAL,[5] to elaborate ways of analyzing the

MAKING PICTURES TALK

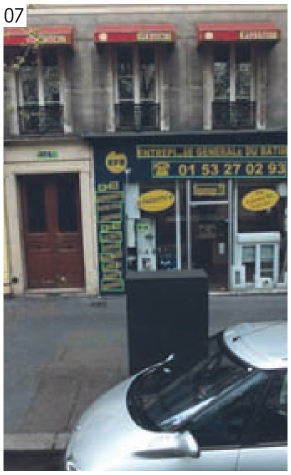
If you think sorting family pictures on your home computer is a hassle, imagine sifting through the largest image databases in existence, which contain millions. Luckily, tools like face recognition software are already available. Yet as Matthieu Cord of the LIP6[1] points out, “the success rate is only 50-60%.” Typically, a specialized algorithm can perfectly handle so-called “low-level” information: color, contrast, or pixel movement vectors in a video stream, for example. It is somewhat trickier to transform this data into high-level information making it possible to positively identify a particular object or event. This has not prevented the emergence of increasingly powerful applications, like the one developed by Jenny Benois-Pineau’s team at the LaBRI,[2] a laboratory near Bordeaux working in conjunction with the French national medical research center (Inserm). “We film Alzheimer patients at home with wearable cameras, and identify behaviors associated with the disease so that doctors can follow a patient’s evolution,” Benois-Pineau explains.

Cord is working on the iTowns project, a digital map of Paris elaborated from photographs, and modeled after Google Street View—but with an accuracy of just one centimeter. “We are developing tools to automatically detect people and cars in order to blur personal data,” he explains. “But we are also working on the recognition of a multitude of objects more or less buried in these images, such as street signs, façades, or vegetation, in order to improve advanced navigation.”

[01] Laboratoire d’informatique de Paris-6 (CNRS / UPMC).
[02] Laboratoire Bordelais de recherche en informatique (CNRS / Université Bordeaux-I / IPB Enseirb-Matmeca Bordeaux / Université Victor-Segalen).

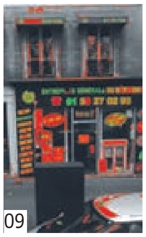
CONTACT INFORMATION:
Jenny Benois-Pineau
› jenny.benois-pineau@labri.fr
Matthieu Cord
› matthieu.cord@lip6.fr

07



08

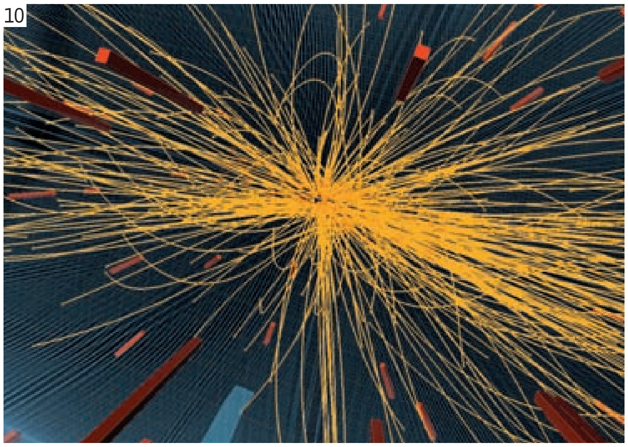
09



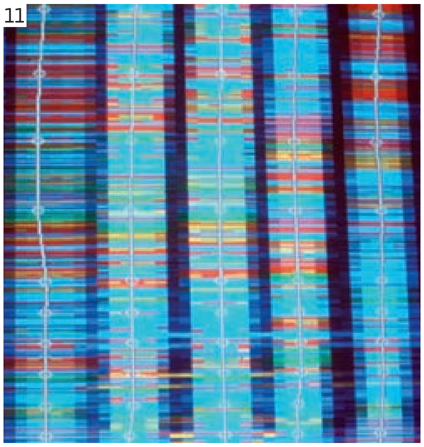
© IGN - STEREOPOLIS

07 08 09 iTowns automatically extracts all types of information contained in an image.

10



11



© CERN ; M. DEPARDIEU/INSERM

12

© C. LEBEDINSKY/INRIA

10 11 Some experiments, such as particle collisions (left) or genome sequencing (right), generate large amounts of data that must be sorted and analyzed.
12 Analyzing scientific data sometimes requires extensive computing resources as well as interconnecting machines through networks, as shown here in the Grid 5000 project.

huge amount of data provided by particle accelerators.

TRIAL AND ERROR

Particle physicists are far from being the only ones to handle large amounts of data. Pascal Poncelet's team, working in collaboration with researchers from the French medical research center Inserm, has developed an algorithm able to single out the genes involved in various types of breast cancer tumors, based on patient data (genetic information, age, weight and size of the tumor, treatment used, and results obtained). "It gives doctors information on the potential evolution of the tumor," the researcher explains.

In a different field, Amedeo Napoli's team has worked with astronomers to develop data mining software applied to information collected in astrophysics. Researchers hope this type of software will reveal particular characteristics or combinations that might have escaped a human operator.

Can data mining work miracles? Not exactly. It is a relatively new field, first explored at the end of the 1980s, and still in full expansion. For Beaudouin-Lafon, "most methods used today are empirical. Parameters are adjusted manually and when something works, it is not really clear why. In many cases, there are no quantitative criteria for judging the quality of information extracted from a database. That is left up to specialists in the field." Napoli adds: "much work still has to be done to handle very large amounts of data. At present, we can manage a few thousand objects with a few hundred attributes. Beyond that, the hardware's physical limits become apparent."

To overcome this obstacle, two complementary approaches are currently used. First, when a single machine does not have enough computing power for a specific task, several computers can be run in parallel. This is the principle of grid computing (*see box*), which LHC has pushed to the limit: it relies on 50,000 PCs located in various research centers worldwide to analyze the 15 millions Gigaoctets of scientific data (the equivalent of a

GRID COMPUTING

Grid computers are virtual infrastructures consisting of a set (or clusters) of computers, including home computers, that are geographically remote but working as a network. These systems, which emerged a few years ago to meet the demands of particle physics experiments, enable research scientists and industrialists to have access to extensive computing resources at lower cost, in sectors ranging from engineering to the study of neurodegenerative diseases or astrophysics. The CNRS's Grids Institute (Institut des grilles) managed by Vincent Breton, has been the leading research center in this field in France for the past three years. Along with Grid 5000, a tool specifically dedicated to grid research, it provides scientists and industry with a production grid comprising around 20,000 processors scattered over some 20 centers at CNRS, CEA,[1] and universities. Last September, this already sizeable system reached new heights with the creation of "France Grilles," involving several research organizations and universities. Its purpose is to coordinate the deployment of a nationwide grid infrastructure, which will eventually be integrated into a European grid. For Breton, who heads the program, its objective is clear-cut: "to double resources and users by 2015."

[1] French Atomic Energy and Alternative Energies Commission.

CONTACT INFORMATION:
Vincent Breton
› vincent.breton@idgrilles.fr

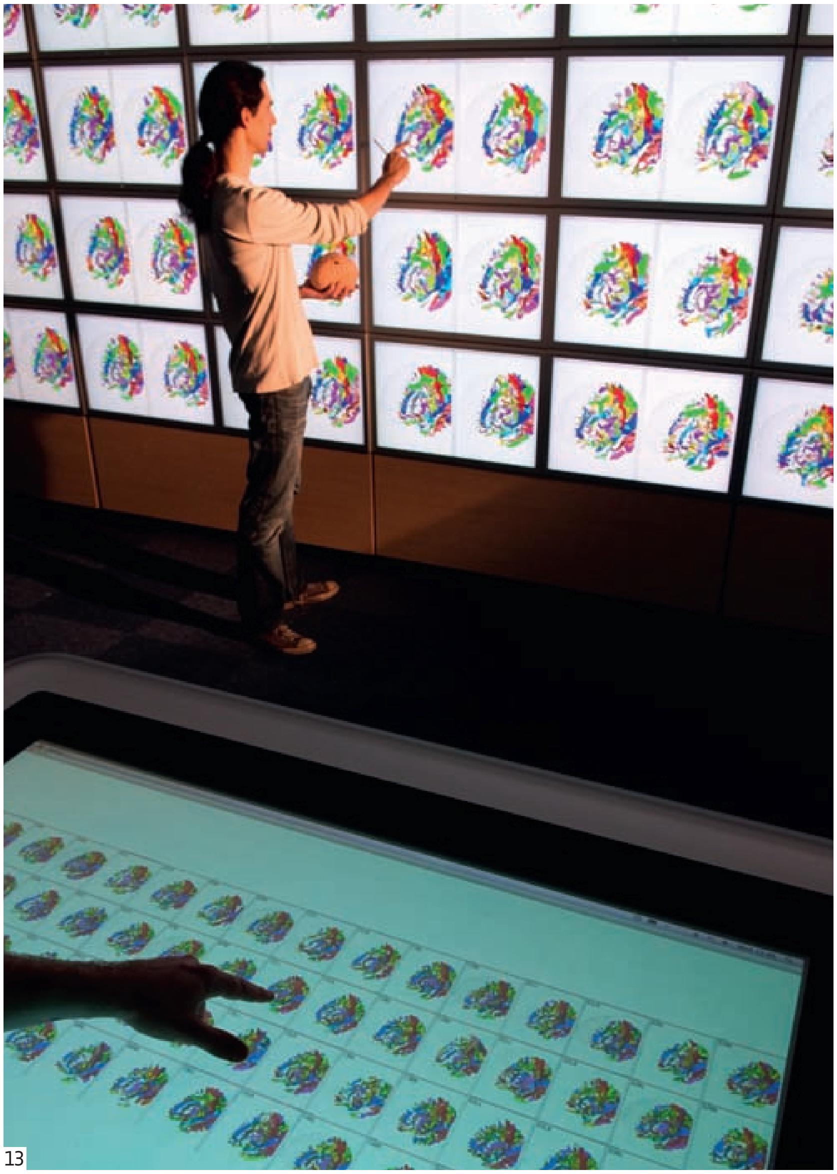
20km-long pile of CDs) that researchers will collect every year. The second approach is based on supercomputers, like the one used since 2008 at CNRS's IDRIS[6]—a monster capable of performing 207 thousand billion FLOPS. "In some cases, such as weather simulation, for which it is difficult to parcel out the data to a network of PCs, supercomputers remain the best solution," explains Beaudouin-Lafon.

FLOPS
FLOPS stands for floating-point operations per second. It is a measurement of a computer's performance. By comparison, an average handheld calculator can perform around 10 FLOPS.

THE HUMAN FACTOR

But developing fast and high-performing computers is not enough. The data they have sorted still need to be understandable to human users. Take Google for example: the search engine can bring up several thousand addresses for a query, but can only display a dozen or so per page. "It is a shame to have sophisticated data retrieval algorithms and yet not be able to display the results comprehensively," says Beaudouin-Lafon. This raises the question of how search results can best be presented.

To answer this question, the LRI has developed a new type of platform called Wild: a wall of 32 computer screens—over 130 million pixels in total—allowing users to grasp a huge amount of information at a glance. "We are working with eight other laboratories from CNRS and the Saclay Campus, on this project," says Beaudouin-Lafon. For neuroscience specialists, Wild can display 64 brain MRIs, "which offers an indisputable advantage when trying to identify a pathology, considering there are significant variations even among healthy brains," he adds. Similarly, in astrophysics, certain observatories now compile images much too large to be displayed on single computer screens. To view an entire image at its highest resolution, Wild-like tools make all the difference. "I am convinced that this type of approach will expand in the future—not only for research, but also for industry," concludes Beaudouin-Lafon. "Indeed, the amount of data is constantly expanding, and the questions asked are both increasingly vague and complex." In other words, everything must be done to prevent today's information society from drowning in this massive quantity of data.


13

© C. FRÉSILLON/CNRS PHOTOTHÈQUE

13 The "Substance Grise" (Grey Matter) application used on the Wild platform allows users to simultaneously compare 3-D reconstructions of 64 patients' brains.

800,000 petabytes*

was the estimated amount of digital data in the world in 2009. This number was expected to rise to 1.2 million in 2010, and experts predict it to grow by 45% each year between now and 2020.

* 10^{15} bytes.

01. Laboratoire lorrain de recherche en informatique et ses applications (CNRS / Université Henri-Poincaré / Université Nancy-II / Inria).
02. Laboratoire de recherche en informatique (CNRS / Université Paris-Sud-XI).
03. Microwave Data Analysis for petascale computers.
04. Laboratoire d'informatique, de robotique et de microélectronique (CNRS / Université Montpellier-II).
05. Laboratoire de l'accélérateur linéaire (CNRS / Université Paris-Sud-XI).
06. Institut du développement et des ressources en informatique scientifique.

CONTACT INFORMATION:
Michel Beaudouin-Lafon
› michel.beaudouin-lafon@lri.fr
Amedeo Napoli
› amedeo.napoli@loria.fr
Pascal Poncelet
› pascal.poncelet@lirmm.fr

14

© IBM

Quantum Computers: **The Ultimate Challenge**

It is every computer scientist's dream: a computer so fast that breaking a code, making long-term weather predictions, or thrashing a chess grandmaster would only take a second. If this is still science-fiction today, it does not prevent mathematicians and physicists from sketching the outlines of how this extraordinary machine might work. Its name: quantum computer. Its underlying structure: to take advantage of the surprising laws of quantum mechanics, which allow a particle, an atom, or a molecule, to exist in two states at once. While today's computers store data as bits equal to either 0 or 1, quantum bits (or qubits) can simultaneously be equal to both 0 and 1. The advantage is the ability to store (in principle) information representing a large number of potential solutions to a given problem in the same memory, and, by applying suitable algorithms, to process all those solutions at once. This would turn today's most powerful computers into stone-age relics overnight.

QUBIT
A quantum bit is a unit of quantum information—the quantum analogue of the classical bit. A qubit has some similarities to a classical bit.

THE LONG ROAD AHEAD

But will such a machine ever make it out of the laboratory? And if so, would it really be able to work wonders? Nothing is less certain. Quantum computers started as a simple idea floated in the 1980s by Richard Feynman, Nobel Prize Laureate in Physics. For Julia Kempe from the LRI[1]—elected Research Woman of the Year in 2010—"Feynman explained that quantum computers would be able to calculate the properties of quantum particles, such as electrons, much faster than a traditional computer. Each electron could be encoded in a qubit, whereas a large number of traditional bits are needed to encode the many states it may be in at the same time. But it was still all just an idea." And a very good one at that. In 1994, Peter Shor, then working at the AT&T Laboratories in the US, formally demonstrated that a quantum computer could factor a number—break it down into a product of prime numbers—in record time. Enough to make cryptographers nervous, since factoring, because it requires lots of computing time, is currently the key to all encrypted codes, whether for credit cards or top-secret documents. Likewise, in 1997, Lov Grover, then also at AT&T, demonstrated that a computer using qubits could considerably increase the effectiveness of algorithms aimed at finding information in databases. Unfortunately, despite mathematicians' and physicists' attempts to demonstrate the advantages of quantum computers at the time, these remained a pipe dream. In fact, to this day, no one knows exactly what a qubit will be made of: atoms, ions, molecules, electrons, superconductor circuits? What's more, the type of medium itself—solid, liquid, or gas—also remains a mystery.

FACTORING The decomposition of a mathematical object (for example, a number, a polynomial, or a matrix) into a product of other objects, or factors, which when multiplied together produce the original.

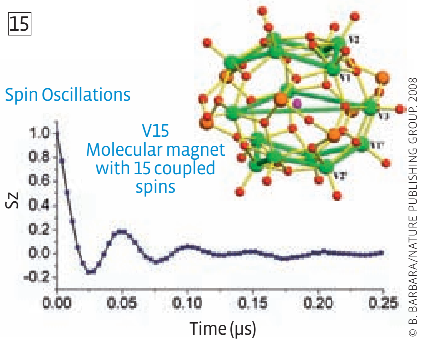
Several teams around the world are currently testing all types of materials that could potentially be used as basic components in future quantum processors. "We are studying qubits whose 0 and 1 states correspond to the spin states (a kind of rotation of the particle around itself) of molecules or ions of certain metals in solid matrices," explains Bernard Barbara, of the Institut Néel[2] in Grenoble.

DECOHERENCE IS THE ENEMY

But physicists are far from proposing a turnkey computer. For now they are trying to understand and, insofar as possible, overcome the major pitfall in the path to quantum computers: something called decoherence. As Barbara points out, "any system in a quantum superposition of various states is extremely fragile. Through interactions with the environment, it can lose in a fraction of a second the properties required for any quantum calculation, and the more qubits it contains, the more unstable it is." At present, the best computing feat performed with qubits is that of Isaac Chuang at the Massachusetts Institute of Technology (US). In 2001, using the spin of molecules with seven effective nuclear spins, the researcher managed to factor 15, showing that the number could be broken down into 3 times 5. "But to be really effective," says Barbara, "a quantum computer needs to include a few thousand qubits, and be able to combine them in order to perform logical calculations."

DECOHERENCE Time during which a quantum system is not corrupted by its external environment.

15



© B. BARBARA/NATURE PUBLISHING GROUP 2008

14 Quantum computers, like the one developed at MIT based on organic molecules, are still very much in the experimental stage.
15 A large molecule containing several hundred atoms, when interacting with its environment, slowly loses its quantum nature: a phenomenon known as decoherence.

For most scientists, two systems currently offer the most interesting perspectives. These include superconductor qubits, or microscopic electronic circuits allowing electric current to flow in both directions at the same time. "They are very easy to manufacture and duplicate and can be laid out in chips with several qubit superconductors," says Barbara. The second and most promising development relates to "gaseous ions trapped by powerful laser beams that provide several minutes of coherence, despite relatively restricted systems."

"Quantum computers are still a long way away," admits Barbara. "But I think they may become a reality within a few decades." Miklos Santha, also at the LRI, is less optimistic: "We might eventually find out that nature prohibits the very possibility of quantum computers..."

If quantum computers ever become a reality, they will still not be the ultimate computing machines, as their time-saving power could only be applied to solving specific problems. "While the benefit is considerable in the case of factoring, it is less obvious when searching through unsorted data, determining the shortest route on a map, or playing a game of chess or Go," notes Santha. "And quantum computers would provide little benefit put to other types of data, like sorted lists for example."

Does this mean research into quantum computers is pointless? Far from it. "Whether or not we build a quantum computer, our research helps us learn how to control quantum laws and understand the fundamentals better," explains Barbara. As for Kempe, she insists on the advantages of developing quantum algorithms: "They represent very powerful mathematical tools for addressing fundamental questions linked to complexity, and also for studying what a traditional computer can and cannot do. Finally, as quantum factoring algorithms threaten classical cryptography, it is essential to develop quantum cryptography, which is already used to exchange secret data." Nobody knows whether quantum computers will ever make it out of the laboratory. But it does not matter. Even if the concept proves unattainable, it remains an endless source of inspiration—and a genuine scientist's dream.

RECENTLY PUBLISHED

The LLL Algorithm, Survey and Applications. Series: Information Security and Cryptography. Phong Q. Nguyen and Brigitte Vallée, Eds. (Berlin: Springer, 2010).

Joint Source-Channel Decoding. A Cross-Layer Perspective with Applications in Video Broadcasting over Mobile and Wireless Networks. Pierre Duhamel and Michel Kieffer (Amsterdam: Academic Press, 2009).

Machine Learning Techniques for Multimedia: Case Studies on Organization and Retrieval. Matthieu Cord and Pádraig Cunningham, Eds. (Berlin: Springer, 2008).

HCI Remixed, Reflections on Works That Have Influenced the HCI Community. Thomas Erickson and David W. McDonald, Eds. (Cambridge: MIT Press, 2008).

[1] Laboratoire de recherche en informatique (CNRS / Paris-XI).
[2] CNRS.

CONTACT INFORMATION:
Bernard Barbara
› bernard.barbara@grenoble.cnrs.fr
Julia Kempe
› julia.kempe@lri.fr
Miklos Santha
› miklos.santha@lri.fr