ASTROPHYSICS

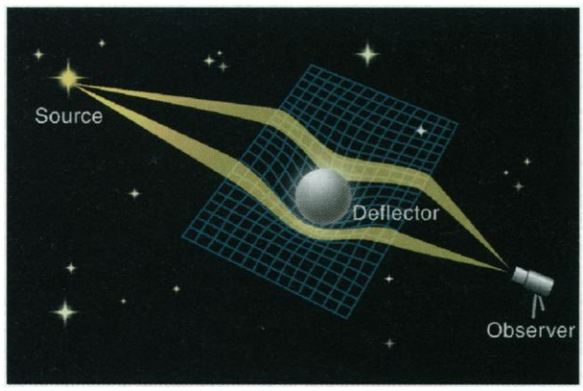
Microlensing Sheds Light on Dark Matter

Paul Hewett and Stephen Warren

It has been known for more than a decade that the mass content of the universe is dominated by dark matter. The first real clue as to its nature may come from the study of gravitational lensing by objects of stellar mass within our own galaxy. This is a very recent possibility, the standard monograph on lensing, published in 1992, states "that lensing of stars by stars in our galaxy is unlikely to be discovered" (*1*). The detection of the first such event occurred the next year (*2*), and further examples are now discovered at the rate of one a week.

Eddington's experimental verification of general relativity, by means of his measurement of the apparent displacement of stars close to the limb of the sun during the solar eclipse in 1919, can be thought of as the first gravitational lens observation. Very close alignments between an observer, a distant object, and an intervening compact mass can result in multiple images of the background source (see figure). The separation images, twice the Einstein radius, is proportional to the square root of the mass of the intervening object. Angular separations of sources at cosmological distances lensed by intervening galaxies with masses ~10^{12} times that of the sun are ~1 arc sec (where the mass of the sun $M_\odot$ = 1.99×10^{30} kg). A second observational consequence is an increase in the apparent brightness of the background source: the sum of the brightness of the multiple images is greater than that of the single unlensed image. The angular scale of image splittings produced by a lens of mass ~1 $M_\odot$ is 10^{-6} arc sec (hence "microlensing"), far below the resolution of conventional optical techniques, and the signature of such an event is confined to a brightness change in the background source.

Dark halos dominate the total mass associated with luminous galaxies, such as our own galaxy, but we know little about their composition. Candidates as different as exotic nonbaryonic particles and failed stars, objects with masses <0.08 $M_\odot$, are possibilities. In 1993, the Massive Compact Halo Object (MACHO) collaboration began monitoring ~2×10^6 stars in the Large Magellanic Cloud (LMC), a satellite galaxy in the far halo of the Milky Way at a distance of 50 kpc. The time history of the apparent brightness of stars in the LMC provides a probe for the presence of compact objects crossing our line of sight. However, even if we assume that the entire mass of the dark halo of our galaxy is made up of compact objects, the probability of observing a lensing-induced brightness fluctuation in a single star is small, ~10^{-6} per year.



Darkness visible. The warped grid represents the distortions in space-time produced by a compact mass. Close alignment between a distant star, a compact object and the observer produces a focusing (gravitational lensing) of radiation from the source. To an observer, this manifests itself as a change in brightness, or even multiple images, of the source. Microlensing experiments look for the characteristic variation in brightness with time as an unseen compact object traverses the line of sight. [Adapted from figure by P. Newbury]

A single event produces a frequency-independent brightening of the background source, reaching a maximum at the minimum impact parameter, followed by a symmetric decline in the brightness to the level prior to the event. The time scale Δt of the event depends on the square root of the mass m of the compact object, the inverse of its distance d from the observer, and the inverse of the velocity v of the object perpendicular to the line of sight: $\Delta t \propto m^{1/2}/vd$. The amplitude of the brightening depends on the minimum impact parameter and the angular size of the background star relative to the Einstein radius. A single event, which lasts typically tens of days, is thus underconstrained, and a well-defined statistical sample is necessary to make progress.

Model predictions—incorporating a halo density profile, mass spectrum, and velocity distribution for the compact objects—must be compared to the statistical distribution of event properties. Analysis of the first year of monitoring, which reaped three events, suggested the fraction of the dark halo in the form of compact objects was small. However, monitoring over 2 years produced eight events and an estimated mass contribution to the halo within 50 kpc of $2.0^{+1.2}_{-0.7} \times 10^{11}$ $M_\odot$ (*3*), about half of the total mass inferred from dynamical considerations but with a large uncertainty.

The likely difficulty of establishing the reality of any signal attributable to compact objects in the halo led the MACHO investigators, and the similarly motivated OGLE collaboration, to monitor "control" fields toward the center of the galaxy. The line-of-sight toward the central bulge of the galaxy, some 8 kpc distant, probes the galactic disc with its (relatively) high space density of stars. The probability of observing a lensing event was calculated to be substantial, but there was surprise when events were observed at a frequency ~3 times greater than predictions based on the (supposedly) known structure of the galaxy and its constituent stellar populations.

Last year alone the MACHO team has detected 41 lensing events toward the galactic bulge. Data acquisition and analysis have become highly automated, and the identification of events within a few days of their onset is routine. Alerted to their existence, other telescopes can obtain higher precision photometric observations with much greater sampling frequencies. Events attributable to binary stars (*4*) have been seen, and a consortium has been established to search for planets (*5*). Jupiter-class planets orbiting the lensing star have a significant probability for detection by means of transient (a few hours) brightenings superimposed on the slowly varying many-day brightness modulation due to the star (*6*).

The bulge-field results have sparked a reassessment of the galaxy's structure. One interpretation increases the number of stars between us and the bulge by postulating the existence of a massive stellar "bar," changing the classification of our galaxy from that of a normal to a barred spiral. However, definitive interpretation of the observations toward the

P. Hewett is at the Institute of Astronomy, University of Cambridge, Madingley Road, Cambridge CB3 0HA, UK. E-mail: phewett@ast.cam.ac.uk. S. Warren is at the Department of Physics, Imperial College of Science and Technology, Prince Consort Road, London, SW7 2BZ, UK. E-mail: s.j.warren@ic.ac.uk

bulge and the LMC is not easy. In particular, the contribution to the observed lensing frequency from stars in our own galactic disc and in the LMC must be established more reliably. The luminous stars in the LMC and the bulge have large radii and thus cannot strictly be treated as point sources, and the distribution of stellar radii in the lensed population is also required. As the statistics improve and the detailed nature of the experiments (MACHO, EROS, OGLE, DUO, and others) become better understood, microlensing in the galaxy should provide unique constraints on the composition of dark matter in the galaxy halos and the structure of our galaxy, and detailed follow-up observations of individual events may reveal more extra-solar planets.

An enhanced version of this Perspective, with live links, can be seen in *Science* Online on the Web at http://www.sciencemag.org/

References

1. P. Schneider, J. Ehlers, E. E. Falco, in *Gravitational Lenses* (Springer-Verlag, New York, 1992), p. 11.
2. C. Alcock *et al.* (The MACHO Collaboration), *Nature* **365**, 621 (1993).
3. ———, *Astrophys. J.* **471**, 774 (1996).
4. D. J. Lennon *et al.*, *ibid.*, p. L23.
5. M. Albrow *et al.*, in *Astrophysical Returns of Microlensing Surveys*, R. Ferlet and J.-P. Maillard, Eds. (Editions Frontieres, Gif sur Yvette, France, in press).
6. A. Gould and A. Loeb, *Astrophys. J.* **396**, 104 (1992).

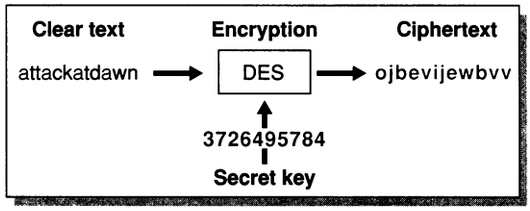
QUANTUM COMPUTING

Searching a Quantum Phone Book

Gilles Brassard

What could be easier than finding someone's phone number in your city's directory, provided you know her name? It would be another matter altogether if you wanted to find the name of a stranger whose phone number you did know. If the directory is available electronically as a simple unstructured file, a computer would have to search through, on average, half of the data to locate the desired entry. It is easily proven that there can be, in general, no shortcuts. No shortcuts, that is, if we stick to computers that obey the rules of classical Newtonian physics. At a conference held in Philadelphia in May 1996, Grover presented his remarkable discovery that a quantum computer could do much better: With the use of inherently quantum-mechanical effects, it could find the desired entry in about square root as much time as its classical counterpart (*1*).

This advantage would not be dramatic for locating information in the phone directory of even a large city; however, the situation changes if we are interested in virtual databases that are so large that they would not fit in the memory of all the world's computers put together. Such databases cannot be built explicitly, of course, but they can be specified by a rule that allows the construction of any required record efficiently on demand. Consider a cryptographic example. One of the most widely used systems to protect the confidentiality of information is the Data Encryption Standard (DES). Encipherment and decipherment are controlled by a 56-bit key, which the legitimate participants must share in secret ahead of time. If an eavesdropper has intercepted matching pairs of clear and enciphered text—a classic scenario in secret intelligence—her goal is to find the key that maps one into the other.



Key (name)	Ciphertext (phone number)
0000000000	sdfngdfjolgj
0000000001	ksngdjslkjdf
⋮	⋮
3726495783	kdhhhkhfushh
3726495784	**ojbevijewbvv**
3726495785	ljkdfmhsodfh
⋮	⋮
9999999998	goihgmoijopw
9999999999	hsidjgehjcuw

Grover's quantum searching algorithm can in principle be used to break classical cryptographic systems such as the widely used Data Encryption Standard. Assume an eavesdropper has intercepted a matching pair of clear text and enciphered text (attackatdawn, ojbevijewbvv). This problem defines a very large virtual phone book that maps each possible key to the result of enciphering "attackatdawn" with that key. Searching for the "name" corresponding to "phone number" ojbevijewbvv yields the desired secret key, 3726495784, that unlocks the remaining text.

This problem can be described by a virtual "phone directory" in which each possible key is a "name" and the enciphered text with that key is the corresponding "phone number" (see figure). Given the intercepted enciphered text, our name-finding problem corresponds to searching for the required secret key to decode the rest of the enciphered text. An exhaustive search would need to try an average of $2^{55} \approx 3.6 \times 10^{16}$ keys before hitting the right one. This would take more than 1 year even if one billion keys are tried every second. By comparison, Grover's algorithm would solve the problem after quantum-DES enciphering the known clear text a mere 185 million times.

Born at the dawn of the 20th century, quantum mechanics has evolved into one of the most successful scientific theories of all time. Nevertheless, information processing is firmly rooted in classical physics. This has prevented us from tapping the full potential of physical reality for computing purposes. About 12 years ago, Deutsch from Oxford University, following the lead of Benioff at Argonne National Laboratory and Feynman at the California Institute of Technology, thought of harnessing some of the strange properties of quantum mechanics to obtain unprecedented parallelism in computation (*2*).

To get a glimpse of Deutsch's insight, consider an atom that has a lone electron on its outermost orbit. By shining light on the atom, it is possible to force this electron to jump to a higher orbit: the atom becomes excited. What happens if you shine the light on an atom in the ground state, but for only half the time needed to excite it? Where will the electron end up, knowing that quantum mechanics forbids it from lying anywhere between the two orbits? The counterintuitive answer is that the electron will find itself simultaneously on both orbits. If we associate the binary value 0 to an atom in its ground state and 1 to an excited atom, we have produced a qubit—the unit of quantum information—that is in a superposition of classical states 0 and 1.

Similarly, two qubits can be in a superposition of the four classical values 00, 01, 10, and 11. More generally, a quantum register composed of n qubits can be in an arbitrary superposition of all 2^n different classical states.

The author is at the Université de Montréal, Département d'informatique et de rechérche opérationnelle, Montréal, Québec, Canada H3C 3J7. E-mail: brassard@iro.umontreal.ca