April 26th

Manuel Blum

Born: April 26, 1938;

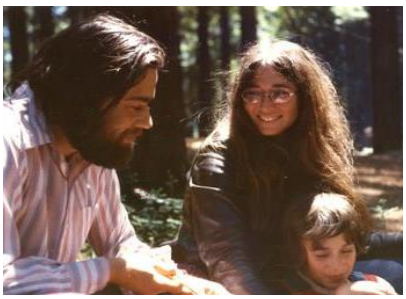
Caracas, Venezuela

Blum's contributions to the foundations of computational complexity include his speedup theorem which states that any algorithm can be sped up exponentially for almost all of its inputs. This can be done repeatedly, leading to an infinite sequence of exponential improvements.

His Blum axioms can be used to determine whether complex problems are even solvable by computer.

Blum Blum Shub is a pseudorandom number generator proposed by Lenore Blum, Manuel Blum, and Michael Shub. Lenore is a noted mathematician, and also Manuel's wife.

His other work includes a protocol for flipping a coin over a telephone (in the information sense, not physically), the Blum-Goldwasser cryptosystem, and CAPTCHAs ("Completely Automated Public Turing test to tell Computers and Humans Apart").



Manuel Blum, Lenore Blum, and their son Avrim (1973).

In the early 2000's, Manuel, Lenore and their son Avrim were all members of Carnegie Mellon's computer science department, with the parents' offices conveniently located on either side of their son's.

The family have collaborated on several projects including ALADDIN (algorithm adaptation dissemination and integration).

A quote: "When you can prove that a proposition is true, and also that the same proposition is false, then you know you are on to something."

Ralph William Gosper, Jr.

Born: April 26, 1943;

USA

Gosper and Richard Greenblatt [Dec 25] are often called the founders of the hacker community surrounding LISP [April 15] at MIT, which developed out of his membership of the Technology Model Railroad Club [Sept 6]. His contributions included HAKMEM, the MacLisp system [Dec 25], and the MACSYMA [July 00] computer algebra package.

HAKMEM is a 1972 tech. report that collects a variety of useful algorithms, pieces of number theory and schematics by various people in the AI lab. Guy L. Steele [Oct 2] has called it, "a bizarre and eclectic potpourri of technical trivia".

Gosper became intensely interested in the "Game of Life" shortly after it was proposed by John Horton Conway [Dec 26]. This included Conway's conjecture of infinitely growing patterns in the game, with a reward for an example. Gosper was the first to find such a pattern, the "glider gun". Gosper also developed the HashLife algorithm to speed up the game by orders of magnitude. Commonly recurring subpatterns are stored in a hash table so they don't have to be recomputed when they arise again.

Gosper is fond of creating packing puzzles, such as the "Twubblesome Twelve", which involves placing twelve disks of various sizes inside a larger disk so that none overlap. He's also responsible for the Gosper space-filling curve (aka the flowsnake) [Nov 20], similar to the dragon and Hilbert curves.

One of his invited talks was entitled "How I find funny looking formulas". Here's one:

$$\lim_{n\to\infty} \prod_{i=n}^{2n} \frac{\pi}{2\tan^{-1} i} = 4^{\frac{1}{\pi}}$$

Harold Abelson

Born: April 26, 1947;

USA

Abelson is lauded for the textbook, "Structure and Interpretation of Computer Programs" (SICP), co-written with Gerald Jay Sussman [Feb 8] and Julie Sussman. It's often called the Wizard book, due to the drawing on the cover. If you read one *serious* computing text, read that one.

The book grew out of Abelson and Sussman's introductory computer science course at MIT which ran from 1980 until 2007. A set of excellent video lectures can be found on YouTube.

His interest in online teaching led to the MIT OpenCourseWare project [May 2], and the development of App Inventor in 2010, a Web-based system for making it easier for novice programmers to write mobile apps.

In March 2015, a copy of Abelson's 1969 Turtle graphics code [Feb 29] was sold at the Algorithm Auction [March 27].

A quote (with some help from Isaac Newton): "If I have not seen as far as others, it is because giants were standing on my shoulders."

STRETCH Announced

April 26, 1960

IBM's 7000 computer series was the company's first to use transistors instead of vacuum tubes. The top of the line model was the 7030, better known as the STRETCH, the fastest

computer in the world when it debuted. It was capable of handling half-million instructions per second, which kept it in the no. 1 spot until 1965 when the CDC 6600 [Sept 00] was released. The STRETCH and the UNIVAC LARC [March 00] are sometimes considered the first supercomputers.

You might say that the computer "STRETCHed" technical state-of-the-art on many fronts: it was the first to employ large, fast disk drives (32 MB), and the first to utilize a generous amount of high-speed core memory (2 MB). Its architectural advances included instruction pipelining and lookahead, multiprogramming, and error-correction. The term "byte" was coined during its development [Oct 24].

The IBM STRETCH maintenance console. Musée des Arts et Métiers, Paris. CC BY-SA 3.0 fr.

Stephen Dunwell initiated the original R&D project, with the goal of building a machine 100-200 times more powerful than anything else, and drew inspiration from Cuthbert Hurd's [April 5] proposal to build a computer for Edward Teller at the Los Alamos Scientific Lab.

The first STRETCH was delivered to Los Alamos in 1961, where it was considered something of a failure because it was only 30-40 times faster than other computers. IBM was forced to drop its asking price to $7.8 million, from $13.5 million, which meant the computer was sold at below cost.

Nine STRETCHs were purchased altogether, mainly by national labs, and a special version, known as HARVEST [Feb 27] (the Model 7950), was developed for the NSA [Oct 24].

It's rumored that the NSA was responsible for the STRETCH's popcount instruction. Short for "population count", it counts the number of bits set in a machine word. Although it may seem fairly useless, it's related to the Hamming weight measure of information content [Feb 11], which is the number of symbols in a string that are different from the zero-symbol of the alphabet. For a binary string, that's exactly the popcount result.

popcount is also useful in chess programming [Nov 22]. Many applications store data using a bitboard representation, which conveniently fits into a 64-bit word. popcount can be used to perform useful chess-related operations on this representation, such as calculating the mobility of a piece.

popcount has had a long history since, appearing in such machines as the CDC 6000 [Sept 00], the Cray-1 [March 4], and various Intel [July 18], AMD [May 1], and ARM [April 26] chips.

Althiough the STRETCH never became a commercial success, its architectural innovations influenced future machines, including IBM's successful 7080 and 7090 lines [Nov 30].

ARM Processor

April 26, 1985

Acorn Computers [Dec 5] had sold over 1.5 million BBC Micros [Dec 1], so funding was available for Acorn engineers Steve Furber [March 21] and Sophie Wilson [?? 1957] to create a 32-bit microprocessor for the next model. They called it the Acorn RISC Machine, or ARM, and it became the first RISC [May 30] processor used in a home computer, the Acorn Archimedes [June 11].

Hermann Hauser, co-owner of Acorn, later joked that, "I gave them two things which National, Intel and Motorola had never given their design teams: the first was no money; the second was no people. The only way they could do it was to keep it really simple."

Furber defined the ARM's architecture while Wilson developed its instruction set. In tests it was able to execute at over 4.5 MIPS, a significant upgrade from 8-bit home computers of the time. It was also small, energy efficient, and easy to program.

Furber later recalled, "At 1pm on April 26, 1985, the first ARM microprocessors arrived back from the manufacturer - VLSI Technology, Inc. They were put straight into the development system which was fired up with a tweak or two and, at 3pm, the screen display is believed to have said: 'Hello World, I am ARM'."

Wilson later recalled the first test of the chip in a computer: "We did 'PRINT PI' at the prompt, and it gave the right answer. We cracked open the bottles of champagne."

After a major investment from Apple in 1990, Acorn spun off its ARM division [Sept 8] The ARM architecture went on to become the dominant 32-bit embedded processor, with over 130 billion produced as of 2019.

CU-SeeMe Seen

April 26, 1993

CU-SeeMe was an Internet video-conferencing client, written by Tim Dorcey at Cornell (hence the "CU" in the name), as part of an NSF funded education project called The Global Schoolhouse.

CU-SeeMe was the first widely used videotelephony service, and was likely the first product to use the term 'video chat'.

Unfortunately, PC hardware wasn't quite fast enough yet to support its needs, and acceptance of CU-SeeMe outside of the schools market was limited by its relatively poor audio/video quality and latency.

For various first's with CU-SeeMe, see [Nov 7] and [Nov 23].

Chernobyl Virus

April 26, 1998

The CIH/Chernobyl virus targeted Windows 9x [Aug 24] by infecting its Portable Executable (PE) files, which allowed it to fill the first 1024K of the host's boot drive with zeros and attack certain kinds of BIOS.

The virus was created by a student in Taiwan, who later claimed to have written it as a challenge for antivirus software developers. He also apologized and co-wrote a freely available antivirus program.

Taiwanese prosecutors couldn't charge the individual because no victims came forward to file a lawsuit. This led to new computer crime legislation to close the loophole.

The virus was christened the "Chernobyl Virus" since it was first observed on this day, the anniversary of the 1986 Chernobyl nuclear disaster.