SIAM Turns Fifty

In this very special year for the Society for Industrial and Applied Mathematics (SIAM)—the year of our fiftieth anniversary—we are pleased to share with you some reflections on our past and visions for our future.

SIAM was founded in 1951 in Philadelphia—not coincidentally the city in which the first programmable digital computer, the ENIAC, was built and tested. Close ties to computing and computational science have complemented deep interests across the spectrum of applied mathematics throughout the fifty years of SIAM's existence. As these fields have grown and evolved over the past half century, so has SIAM.

Many of those associated with the development of the ENIAC became prominent SIAM leaders. ENIAC developer John Mauchly served on the first SIAM Board of Trustees and later became the fourth president of SIAM. John von Neumann, while never an officer of SIAM, lends his name to one of our most prestigious prizes: the John von Neumann Lecture. Grace Hopper, a member of Howard Aiken's Mark I team and later a researcher at the Eckert-Mauchly Corporation, was elected SIAM vice president for planning at a 1952 organizational meeting.

The region around Philadelphia was an early center for the computer industry, as reflected by early lists of SIAM's corporate members. The Burroughs Corporation, IBM, Sperry Rand's Remington Rand Division (a successor of Eckert-Mauchly), and RCA were among our first corporate members. Also well represented among our early corporate sponsors were oil companies, including Standard Oil of California and Socony-Mobil. With the launch of Sputnik came strong representation from the aerospace sector, including Boeing Airplane Company, Hughes Aircraft Company, Lockheed Aircraft Corporation, and the Martin Company. Consistently among our corporate sponsors over the years has been Bell Labs.

Paralleling SIAM's strong ties to industry, with an emphasis on digital computing, were deep roots in applied mathematics and the academic community, through membership and especially through the SIAM journals. The first volume of the *Journal of the Society for Industrial and Applied Mathematics* appeared in 1953 under the leadership of editors I. Edward Block, Philip Davis, Robert Jackson, and Russell Remage. In the early issues, the acquisition and shaping of every paper seemed to be a story in itself. By the early 1960s, though, the journal was on solid enough footing to spin off two specialty journals—on control (1962) and on numerical analysis (1964).

The blend of computing and applied mathematics that has been a consistent hallmark of SIAM can be seen in our leadership over the years. Alston Householder (president, 1963–64), J. Wallace Givens (president, 1966–67), and George Forsythe (trustee, 1970–72) were all important pioneers in numerical analysis and scientific computing. During the same period, Harold Kuhn lent his wisdom and prestige to SIAM as an early president (1954–55); other prominent applied mathematicians elected to leadership positions include Garrett Birkhoff (president, 1965–66) and Joseph LaSalle (president, 1962–63, and a driving force in establishing control as an important SIAM interest). This dual tradition continues today and contributes to the vitality of our community.

From its origins, with just a few hundred members and a single journal, SIAM has grown into an organization with nearly 9,000 members and eleven journals in areas that range from applied mathematics to control, optimization, and scientific computing. Today, SIAM holds eight to ten conferences a year in various areas of applied mathematics and computing and supports twelve activity groups. The activity groups are always a good indication of new emphases within SIAM, from the first (in linear algebra, founded in the early 1980s) to the three newest groups—in life sciences, imaging science, and computational science and engineering—all begun in the past two years. Like much of applied mathematics today, the areas covered by our activity groups are highly interdisciplinary, with exciting new research topics emerging from the intersection of mathematics, computing, and application areas.

The SIAM membership itself is quite interdisciplinary. Only about half of SIAM members, according to a 1995 survey, received their highest degrees from mathematics departments, with another 11 percent from applied mathematics departments. The remainder held degrees in a variety of disciplines, including computer science, engineering, and physics. Roughly two thirds of regular SIAM members work in academia, with the other third divided fairly evenly between industry and government, including a strong representation from national labs.

We believe that the future holds great promise for applied mathematics and computing—and for SIAM. Interdisciplinary mathematics has always played an important role in science and technology, on which the economy is increasingly dependent. New and exciting applications are continually emerging.

Biotechnology, imaging science, and information technology are some of the fields whose recent growth has been driven, in part, by remarkable advances in computational capabilities. As our computational tools have grown in power, mathematics has become even more important. A good case can be made that improvements in our ability to model complex phenomena can be attributed at least as much to advances in algorithms as to advances in hardware. For the coming years, we see applied and computational mathematics continuing to grow with computational technologies.

Traditional areas of applied mathematics—fluid dynamics being one important example—continue to thrive, driven by new problems. At the same time, the emergence of exciting new application areas—large data sets and financial mathematics among them—is driving the development of whole new areas of applied mathematics.

SIAM will celebrate its anniversary at the 2002 SIAM Fiftieth Anniversary and Annual Meeting in Philadelphia this summer (July 8–12). We are planning a special program, one that reflects our roots in both applied mathematics and computing but that is oriented very definitely toward the future. We invite you all to come and celebrate with us. See `http://www.siam.org/meetings/SIAM50/` for details about the conference and related special events.

—Tom Manteuffel, SIAM President
—Jim Crowley, SIAM Executive Director

Letter to the Editor

Digital Millennium Copyright Act

The Digital Millennium Copyright Act (DMCA), promoted by the music and motion picture industries under the banner of protecting intellectual property rights, was passed into law in July 1998. Section 1201(b)(1)(A) of the DMCA prohibits trafficking in "any technology…that is primarily designed or produced for the purpose of circumventing [copyright] protection." Unfortunately, the DMCA is being used to discourage scientific research related to encryption. With no stretch of the imagination, mathematics will be directly and adversely affected, as the fields of computer security and data encryption already are.

The names of Edward Felten and Dmitry Sklyarov are associated with events of interest to mathematicians. As part of a public challenge issued by the Secure Digital Music Initiative (SDMI), Felten's team broke several "watermarking" technologies for digital music, then rejected a monetary prize in favor of publication. The SDMI and the Recording Industry Association of America (RIAA) warned Felten that publication would "subject [Felten's] team to enforcement actions under the DMCA and possibly other federal laws." After negotiating with the recording industry, Felten's team presented its results at the Tenth Annual USENIX Security Symposium, but the wording of subsequent public announcements by the SDMI and RIAA leads us to believe that the recording industry's seeming acquiescence represents merely their perception of current public opinion.

The second case concerns a Russian software developer and cryptography student named Dmitry Sklyarov. As an employee of the Russian software firm ElcomSoft, Sklyarov authored a commercial program to circumvent password protection on Adobe eBook files. This software is legal outside the United States and has legitimate applications that are not provided by Adobe's own software. Sklyarov was also an invited speaker at the Def Con security conference held in Las Vegas in July 2001. Acting on a motion filed by Adobe Software, the FBI arrested Sklyarov on July 16, charging him with violating Section 1201(b)(1)(A) of the DMCA. In response to strong negative public reaction, Adobe dropped its complaint, but the Department of Justice is pursuing the case. On August 30, Sklyarov was charged with five counts, each carrying a maximum penalty of five years imprisonment and a fine of $500,000.

Sklyarov's case is relevant to academics because he was in the United States as a conference participant, not as a representative of ElcomSoft. However, all such cases are important to research mathematicians: Many commercial "content protection technologies" are currently at the level of Rot-13 (an involution of the Roman alphabet), Fermat's little theorem, and mod 2 linear algebra, relying on public ignorance for their effectiveness. To criminalize publication of work that *could be used* to thwart such measures is misguided. A mathematician whose work has cryptographic applications could run afoul of the DMCA. We do not believe criminal charges would be upheld in such a case, but find it unacceptable that the DMCA contains provisions for raising these charges at all.

The chilling effect of the DMCA on academic research has not been emphasized in media accounts, but it is extant and will only get worse as the entertainment industry pushes for more enforcement of the DMCA. In July, Alan Cox (the maintainer of the stable Linux kernel) stated that he would boycott conferences held in the United States and urged others to do the same. In August, Dutch cryptographer Neils Ferguson (a co-designer of the Twofish encryption algorithm) announced that he had broken the encryption used in Intel's High-bandwidth Digital Content Protection (HDCP). Because he visits the United States regularly, Ferguson has declined to discuss the details of his findings, even with Intel, since that could constitute "trafficking" under the DMCA.

Readers can find up-to-date information on legal aspects of the Sklyarov and Felten cases at the Electronic Frontier Foundation: `http://www.eff.org/`.

Technical and practical aspects of encryption are engagingly discussed at David Touretzky's Carnegie-Mellon University site. His gallery of DVD descramblers pointedly illustrates the fact that source code—a form of mathematical expression—is speech that should be protected by the First Amendment. See `http://www.cs.cmu.edu/~dst/`.

Two undergraduates broke the weak encryption used by Mattel's *Cyber Patrol 4* Internet blocking software. Information about this case and subsequent events can be found at: `http://www.ansuz.sooke.bc.ca/cpbfaq.html`.

—George S. Avrunin
UMass Amherst
—Anders Buch
MIT
—Andrew D. Hwang
College of the Holy Cross
—Frank Sottile
UMass Amherst

(Received November 9, 2001)

The *Notices* invites readers to submit letters and opinion pieces on topics related to mathematics. Electronic submissions are preferred; see the masthead for addresses. Opinion pieces are usually one printed page in length (about 800 words). Letters are normally less than one page long, and shorter letters are preferred.