

Cryptography and Alan Turing

Computer scientists, mathematicians and inquisitive laymen are interested in fast and comprehensive information about publications in Computer Science. In this chapter we illustrate the helpfulness of the databases ZMATH and io-port.net for this purpose.

Enzo Rossi

Within a few decades, Computer Science has evolved from a branch of mathematics into a self-contained field of science. The importance of Computer Science today is great and considerably increasing. For more and more specialists, scientists and laymen comprehensive and up-to-date information about new publications is essential. FIZ Karlsruhe offers two databases which accommodate these demands.

The informatics portal io-port.net (<http://www.io-port.net>) provides centralised access to a literature database of more than two million bibliographical records in computer science and related areas. It unifies information from several (all important German) scientific databases:

- Parts of ZMATH (see below),
- DBLP (Digital Bibliography & Library Project, University of Trier, www.informatik.uni-trier.de/~ley/db/),
- LEABiB (Bibliographic database of the Lehrstuhl für Effiziente Algorithmen of the Technical University of Munich, www.mayr.informatik.tu-muenchen.de/leabib/index.html.de),
- CCSB (The Collection of Computer Science Bibliographies, University of Karlsruhe, <http://iinwww.ira.uka.de/bibliography/>)).

The database contains references to articles of journals, reports, dissertations, books and proceedings. Every reference includes the bibliographic information, in many cases also keywords, classification (ACM Computing Classification System, CCS) or abstracts. Books are frequently reviewed by subject specialists. io-port.net also offers links to electronic full-texts if available and full-text ordering systems. In cooperation with publishing companies and libraries fast delivery is guaranteed.

Additionally, io-port.net is complemented by further content and services such as personalised services and semantic tools. Basic information, like the display of author and title, is free; the full version is available to subscribers only.

The bibliographical database ZMATH contains records from "Zentralblatt für Mathematik" (1931 to date) and from "Jahrbuch über die Fortschritte der Mathematik" (1868 to 1942) (for more information see the first three chapters of this brochure). The database ZMATH provides information not only on mathematics but also on Computer Science, in particular on Theoretical Informatics. A free demo version is available on the internet (three hits are displayed); subscribers - among them almost all mathematical faculties in Germany - can access all data.

In this chapter we want to show how search results from both databases complement each other in various respects. We take the subject Cryptography and scientist Alan Turing as examples. In ZMATH and io-port.net much information can be gained about these subjects and in particular about Alan Turing, the "father" of Theoretical Informatics and Artificial Intelligence. Cryptography (coming from the Greek words *kryptós*, "secret", and *gráphein*, "written") is the science of encoding and decoding data. Alan Turing made an important contribution to this theory by deciphering the code of the German "Enigma" machine during World War II.

Quick search for Alan Turing

A simple search for the author "Turing, A*" in ZMATH gives 33 hits (Fig. 23). It is remarkable that all of Turing's works have been re-published during the last years: Nearly on top of the results list are four volumes

of "Collected works". Three reasons for this can be taken from the reviews of these collections:

1. Turing wrote "classical" papers which are still trend-setting and interesting for mathematicians and computer scientists.
2. For secrecy reasons, Turing's papers on the Enigma were not published before the 1990s.
3. Many of Turing's papers, especially those from the last years of his life, have remained incomplete or unpublished.

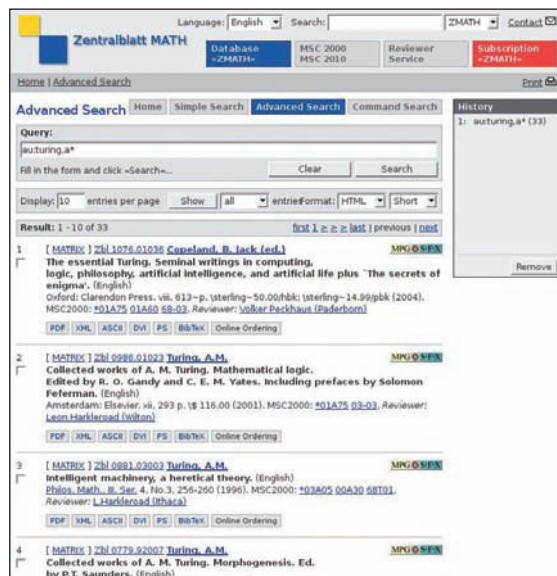


Fig. 23: Searching for author "Turing, A*" in ZMATH gives 33 hits.

A search for "turing" (Advanced Search for author) in io-port.net gives 54 publications. Whenever possible, entries from different providers concerning the same publication were unified; references to the original entries are maintained.

Biographies on Alan Turing can be found in ZMATH by searching for "Alan Turing" in the Basic Index and the classification "01*" (History and Biography). One of the first and most famous biographies is the one by Andrew Hodges: "Alan Turing: The Enigma", published in 1983 (Zbl 0541.68001). It was re-published several times and is now also available in German (Zbl 0834.68023).

First research activities

From 1931 to 1938, Turing studied mathematics in Cambridge and Princeton. He showed particular interest in mathematical logic and in the writings by Russell, Whitehead, Gödel, Hilbert and Neumann.

The Jahrbuch database (included in ZMATH) lists seven publications by Turing from this period with contemporary reviews in German (e.g. JFM 62.1059.03, Fig. 24). In ZMATH a detailed review in English of this ground-breaking paper can be found: "On computable numbers, with an application to the Entscheidungsproblem" (Zbl 0016.09701). In this paper, Turing introduced a machine known today as the "Turing machine". It was the first mathematical model of a computer and the basis for many experiments on decidability, computability and the theory of algorithms. With this model, Turing also succeeded in demonstrating that there is no solution to Hilbert's so-called "Entscheidungsproblem".

The fact that a search for "turing mach*" in ZMATH (Basic Index) gives 2,342 hits shows that the theory of Turing machines is still topical. A whole sub-section of the Mathematics Subject Classification is dedicated to papers on such models: "68Q05, Models of computation (Turing machines, etc.)".



Fig. 24: Review in the Jahrbuch of one of Turing's most famous articles.

Turing's activities during WW II

At the outbreak of World War II, in 1939, the English secret service invited Turing to join them at Bletchley Park and to support them in deciphering the code of the "Enigma" (evolving from the Greek word for "riddle"), an encoding machine used by the German forces. The Enigma was designed in order to keep the radio communication between the military units of the "Wehrmacht" secret from the allied forces. The Enigma was an extremely complex apparatus consisting of five rotors and thousands of different settings, and its code was considered unbreakable. Turing largely contributed to the code-breaking. Since all this work had been kept secret, the essential role Turing had played in it became only known in the 1970s. According to historians, the deciphering of radio transmissions during the submarine war has played a decisive role in the war.

It is therefore not surprising that a search for "enigma turing" in the Basic Index of the ZMATH database finds only papers published after 1983. The "Collected Works" contain articles on the work in Bletchley Park, the cryptographical methods used, and excerpts from Turing's report on the Enigma (Zbl 0986.01023). The whole Enigma report was first published in 1996.

A search for "enigma turing" in io-port.net gives 26 papers. The article "Turing's Treatise on Enigma" (Fig. 25) provides a link to the website of a digitalisation project which offers full-texts of Turing's works and other publications on this topic:
<http://cryptocellular.org/Turing/>.

Post-war period spent in Teddington and Manchester

After the war, Turing was engaged in designing the first computers, the "ACE" (Automatic Computing Engine) and "Mark I", and did some theoretical work in the field of Artificial Intelligence. In his paper "Computing machinery and intelligence" (Mind, October 1950) he suggested to carry out an experiment, the so-called "Turing Test", to find out whether machines are capable of thinking. This paper is accessible via <http://cogprints.org/499/>.



Fig. 25: Citation in io-port.net of the article: "Turing's Treatise on Enigma".

Today the theme "Turing test" is still topical. Publications on the Turing test can be found by searching for "turing test" in io-port.net: At present, 335 publications are contained, almost 90 of which were published during the last five years.

From 1952 until his death in 1954 Turing worked on programmes for a chess computer and on mathematical biology. One of the relevant papers to be found in io-port.net is the article "Digital computers applied to games". His important paper "The chemical basis of morphogenesis" of 1952 is also available via io-port.net. Again, the new theory was named after Turing: the "Turing Mechanism".

A prosecution for homosexuality put an end to Turing's career and his life. On June 7, 1954 Turing committed suicide with a cyanide-poisoned apple.

Conclusion

These examples show that with the help of the portal io-port.net and the ZMATH database searched together it is possible to get comprehensive information about different computer science themes and scientists. The databases complement one another, and give references to further print and electronic sources – not only for specialists, but also for teachers, students and laymen.