Kryptographie und Turing-Maschinen

Informatiker, Mathematiker und interessierte Laien sind an schnellen und umfassenden Informationen über Veröffentlichungen auf dem Gebiet der Informatik interessiert. In diesem Artikel zeigen wir, wie die Datenbank ZMATH und das Portal io-port.net dabei behilflich sein können.

Enzo Rossi

Innerhalb weniger Jahrzehnte hat sich die Informatik von einem Teilgebiet der Mathematik zu einem eigenständigen Fach entwickelt. Die Bedeutung dieses Faches ist heute enorm und wächst ständig. Für eine immer größer werdende Anzahl von Wissenschaftlern und interessierten Laien ist eine schnelle und umfassende Information über Veröffentlichungen auf diesem Gebiet eine Notwendigkeit.

Im April 2006 wurde das Portal io-port.net (www.io-port.net) mit dem Ziel ins Netz gestellt, eine Datenbank für die Informatik anzubieten, welche die oben angesprochenen Bedürfnisse befriedigen kann. Sie enthält die meisten der für die Informatik relevanten Datensätze aus der Datenbank ZMATH (ausgenommen die Daten aus dem „Jahrbuch über die Fortschritte der Mathematik“ (JFM)) und die Inhalte aus drei anderen deutschen Datenbanken

- DBLP (Digital Bibliography & Library Project, Universität Trier, www.informatik.uni-trier.de/~ley/db/),
- LEABiB (Bibliographische Datenbank des Lehrstuhles für Effiziente Algorithmen der Technischen Universität München, www.mayr.informatik.tu-muenchen.de/leabib/index.html.de)
- CCSB (The Collection of Computer Science Bibliographies, Universität Karlsruhe, http://liinwww.ira.uka.de/ bibliography/)].

Zur Zeit enthält io-port.net über 2 Mio. Referenzen auf Zeitschriften, Reports, Dissertationen, Bücher und Konferenzbeiträge und wird monatlich mit ca. 15.000 Dokumentationseinheiten aktualisiert. Jede Referenz enthält die bibliographischen Daten der Originalliteratur und, wenn diese Literatur zu den Kerngebieten der Informatik gehört, auch Klassifikationen (gemäß dem ACM-Klassifikationsschema), Schlagwörter und eine Zusammenfassung. Bücher werden meistens von Fachreferenten besprochen.
io-port.net bietet als weiteren wichtigen Dienst die Volltextvermittlung an. Die Mitwirkung von Verlagen und Bibliotheken ermöglicht dem Benutzer, bei einem Großteil der Referenzen schnell und unkompliziert zu der Originalliteratur zu gelangen.

Die Datenbank ZMATH (siehe Beitrag von O. Ninnemann in diesem Heft) speichert die Daten aus dem „Zentralblatt für Mathematik” (1931 bis heute) und die Daten aus dem „Jahrbuch über die Fortschritte der Mathematik” (1868 bis 1942).

Anhand eines Beispiels können wir das Ineinandergreifen von io-port.net und der Datenbank ZMATH verfolgen.

Das Beispiel Alan Turing

Nehmen wir an, dass ein Benutzer sich für Kryptographie und für Turing-Maschinen interessiert. Kryptographie von griechisch: kryptós, „verborgen“, und gráphein, „schreiben“ ist im ursprünglichen Sinne die Wissenschaft der Verschlüsselung von Informationen. Als erste Annäherung an das Thema kann man nach dem Forscher Alan Turing recherchieren, denn Alan Turing war ein Pionier auf den Gebieten der Berechenbarkeit und Kryptographie. Eine einfache Suche in ZMATH nach dem Autor „Turing, A” führt auf 33 Dokumente (Abb. 23). Auffällig ist, dass in den letzten Jahren alle Werke von Turing neu aufgelegt wurden: Vier „Collected works” findet man gleich am Anfang der Ergebnisliste. Schon das erste Referat deutet drei Gründe für diese Auflagen an:

1. Turing hat „klassische” Arbeiten geschrieben, die heute noch richtungsweisend und interessant für Informatiker und Mathematiker sind.

2. Turings Enigma-Arbeiten wurden aus Geheimhaltungsgründen erst in den neunziger Jahren veröffentlicht.

3. Turing hat vor allem aus seinen letzten Lebensjahren viele unveröffentlichte oder unvollendete Schriften hinterlassen.

Abb. 23: Eine einfache Suche in ZMATH nach dem Autor „Turing, A" führt auf 33 Dokumente.

In io-port.net findet man mit dem Stichwort „turing" im Autorenfeld 54 Arbeiten. Einträge verschiedener Provider zur gleichen Arbeit sind – wo immer dies eindeutig möglich war – zu einem Eintrag zusammengeführt; dabei bleiben die Verweise auf die Original-Einträge erhalten. Bei manchen Dubletten war dies allerdings nicht möglich.

Insgesamt erhält man mit Hilfe der beiden Datenbanken ZMATH und io-port.net eine umfangreiche Werkliste von Turing:

Arbeiten sowohl in ZMATH
als auch in io-port.net: 16
Arbeiten nur in ZMATH: 8
Arbeiten nur in io-port: 19

Lebensbeschreibungen von Alan Turing findet man in ZMATH durch eine Recherche nach „Alan Turing" im Basic Index und der Klassifikation „01*" (History and Biography). Eine der ersten und bekanntesten Biographien ist die von Andrew Hodges „Alan Turing: The Enigma" 1983 (Zbl 0541.68001). Sie wurde vielfach aufgelegt und ist inzwischen auch auf Deutsch erschienen (Zbl 0834.68023).

Jugend und erste Forschungsarbeiten

Alan Mathison Turing wurde am 23. Juni 1912 in London geboren. Schon früh zeigte er Interesse an Mathematik und Naturwissenschaften, las Einsteins Relativitätstheorie und Arbeiten zur Quantenmechanik.

Von 1931 bis 1938 studierte Turing Mathematik in Cambridge und Princeton. Er las Werke von Russell, Whitehead, Gödel, Hilbert und von Neumann - wandte sein Interesse also der mathematischen Logik zu.

In der Jahrbuch-Datenbank findet man sieben Arbeiten von Turing aus diesem Zeitabschnitt mit zeitgenössischen Referaten auf Deutsch. Für die bahnbrechende Arbeit „On computable numbers, with an application to the Entscheidungsproblem" (JFM 62.1059.03, Abb. 24) gibt es auch im Zentralblatt ein ausführliches Referat auf Englisch (Zbl 0016.09701). In dieser Arbeit definierte Turing eine Maschine, heute „Turing-Maschine" genannt. Diese Turing-Maschine stellt das erste mathematische Modell für einen Computer dar. Sie ist die Grundlage für viele Untersuchungen über Entscheidbarkeit, Berechenbarkeit und Algorithmentheorie. Mit Hilfe dieser Maschine gelang es Turing auch zu zeigen, dass es keine Lösung für das sogenannte „Entscheidungsproblem" von Hilbert gibt.

Wie aktuell die Theorie der Turingmaschinen noch heute ist, sieht man daran, dass eine Recherche in ZMATH (basic index) mit dem Stichwort „turing mach*"

Abb. 24: JFM 62.1059.03

2278 Arbeiten anzeigt. Zudem enthält ein ganzes Teilgebiet der Mathematics Subject Classification Arbeiten über solche Modelle: „68Q05, Models of computation (Turing machines, etc.)“; man findet dort zur Zeit über 4200 Dokumente.

Arbeiten im 2. Weltkrieg

Bei Kriegsausbruch 1939 wurde Turing vom englischen Geheimdienst nach Blechtley Park berufen, um an der Entschlüsselung der „Enigma“ mitzuwirken. Die „Enigma“ (von dem griechischen Wort für „Rätsel“) war eine Verschlüsselungsmaschine, die das deutsche Militär verwendete, um die Funksprüche zwischen den verschiedenen militärischen Einheiten vor den Alliierten geheim zu halten. Als eine Apparatur mit 5 Walzen und Tausenden von verschiedenen Einstellungen, war die Enigma eine äußerst komplexe Maschine, die für unentschlüsselbar gehalten wurde. Turing wirkte maßgeblich an der Dechiffrierung mit. Da alle Arbeiten unter strengster Geheimhaltung ausgeführt wurden, ist erst im Laufe der 70er Jahre bekannt geworden, welchen großen Beitrag Turing hierzu lieferte. Nach Einschätzung von Historikern hat die Entschlüsselung der Funksprüche, die den U-Boot-Krieg betrafen, mit eine kriegsentscheidende Rolle gespielt.

Aufgrund dieser Tatsachen ist es also verständlich, dass man bei der Recherche in der Datenbank ZMATH mit den Schlagworten „enigma turing“ erst Arbeiten ab 1983 findet. Es gibt Artikel über die Arbeit des Teams in Blechtley Park, die verwendeten Methoden der Kryptographie und den Abdruck von Teilen eines Enigma-Reports von Turing in den „Collected works“ (Zbl 0986.01023). Der Enigma-Report wurde erst 1996 öffentlich gemacht.

Mit einer Recherche in io-port.net nach „enigma turing“ erhält man 26 Arbeiten. Der Artikel „Turings Treatise on Enigma“ (Abb. 25) führt auf die Internetadresse eines Digitalisierungsprojektes: http://home.cern.ch/~frode/crypto/Turing/index.html unter der man Volltexte von Turing und weitere Arbeiten zum Thema findet.

Andere – nicht geheime – Arbeiten über weitere Probleme der mathematischen Logik aus dem Zeitraum 1939-1945 findet man in ZMATH mit der Suche nach dem Autor „turing, a“ und dem Zeitraum 1939-45.

Abb. 25: Der Artikel „Turing's Treatise on Enigma“

Nachkriegszeit in Teddington und Manchester

In der Zeit nach dem Krieg beschäftigte sich Turing einerseits mit dem Aufbau der ersten Computer, der „ACE (Automatic Computing Engine)“ und Mark I, und andererseits mit theoretischen Arbeiten auf dem Gebiet der Künstlichen Intelligenz. In der Arbeit „Computing machinery and intelligence“ (Mind, Oktober 1950) schlug er einen Test vor - heute "Turing-Test" - genannt, der sich mit der Frage "Können Maschinen denken?" befasst. Diese Arbeit findet man über io-port.net als Volltext unter der Adresse: http://cogprints.org/499/. In manchen Quellen ist sie auch mit dem Untertitel als Titel angegeben.

Viele neuere Arbeiten zum Turing-Test findet man in io-port.net mit einer Recherche mit dem Stichwort „turing test“ : 335 Arbeiten werden zur Zeit angezeigt, fast 90 aus den letzten 5 Jahren.

Wenn wir die Ergebnisse der Recherche zusammenfassen, können wir sagen, dass der Benutzer mit Hilfe von ZMATH und io-port.net umfassende Informationen über das Werk und einige Hinweise über das Leben von Alan Turing bekommen hat. Somit hat er einige Antworten auf seine Frage nach Kryptographie und Turing-Maschinen und Anregungen für weitere Recherchen auf diesem Gebiet bekommen.

Enzo Rossi
FIZ Karlsruhe, Abteilung Mathematik und Informatik,
Editor Zentralblatt Math