Zeitschrift: Visionen : Magazin des Vereins der Informatik Studierenden an der ETH Zürich

Herausgeber: Verein der Informatik Studierenden an der ETH Zürich

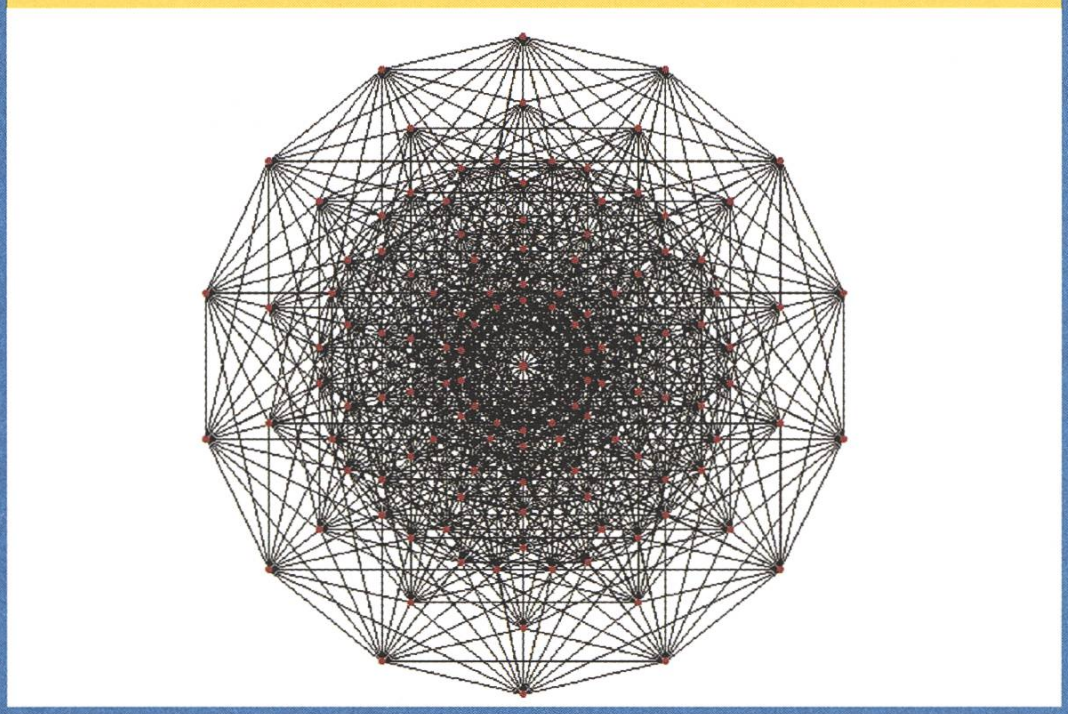
Band: - (2004)

Heft: 2

Heft

Visionen
Praktisches Lehrbuch

TI



Ein Standardwerk in sechs Bänden
Band 2
Jahrgang 2004

Ausgabe 02/2004

Magazin des Vereins der Informatik Studierenden an der ETH Zürich (VIS)

Erscheinungsweise: 6x jährlich
Auflage: 1500
Jahresabonnement: SFr. 25.-
Redaktion, Konzept & Realisation:
Alex de Spindler, Jonas Wäfler

Mitarbeiter an dieser Ausgabe

Prof. Hans Hinterberger, Prof. Angelika Steger, Prof. Robert Stärk, Krzysztof Pietrzak, Robert Berke, Melanie Rämi, Martin Marciniszyn, Konstantinos Panagoton, Andreas Weissl, Thomas Bruderer, Mathias Payer, Sacha Bäbler, Andrea Francke, Bettina Polasek, Daniel Markwalder, Michael Grossniklaus, Alex de Spindler

Anschrift, Verlag & Redaktion

Verein der Informatik Studierenden (VIS)
ETH Zentrum, RZ F17.1
CH-8092 Zürich
Tel.: 01 / 632 72 12
Fax: 01 / 632 16 20

Präsenzzeiten: Mo. bis Fr. 12:15 bis 13:00
Email: **visionen@vis.ethz.ch**
http://www.visionen.ethz.ch/
Postkonto: 80-32779-3

Inserate

1/1 Seite, schwarz/weiss	SFr.	750.–
1/1 Seite, s/w + 1 Farbe	SFr.	1000.–
1/1 Seite, 4-farbig	SFr.	1500.–

Andere Formate auf Anfrage.

Druck

Binkert Druck AG
Baslerstrasse 15
5080 Laufenburg
062 869 79 79

Editorial

ALEX - SCHREIBT DAS EDITORIAL SCHON MONATE IM VORAUS

Der VIS wurde am 26. April 1984 gegründet, also vor bald 20 Jahren. Das ist ein runder Geburtstag! Wir haben uns Verschiedenes ausgedacht, um dieses Jubiläum im Verlaufe dieses Jahres gebührend zu würdigen. Das erste Projekt besteht darin, die diessemestrige Mitgliederversammlung auf das Geburtsdatum zu verschieben. Das tönt jetzt einfach, aber das ist auch nicht alles. Mehr möchten wir an dieser Stelle nicht verraten - lasst euch überraschen.

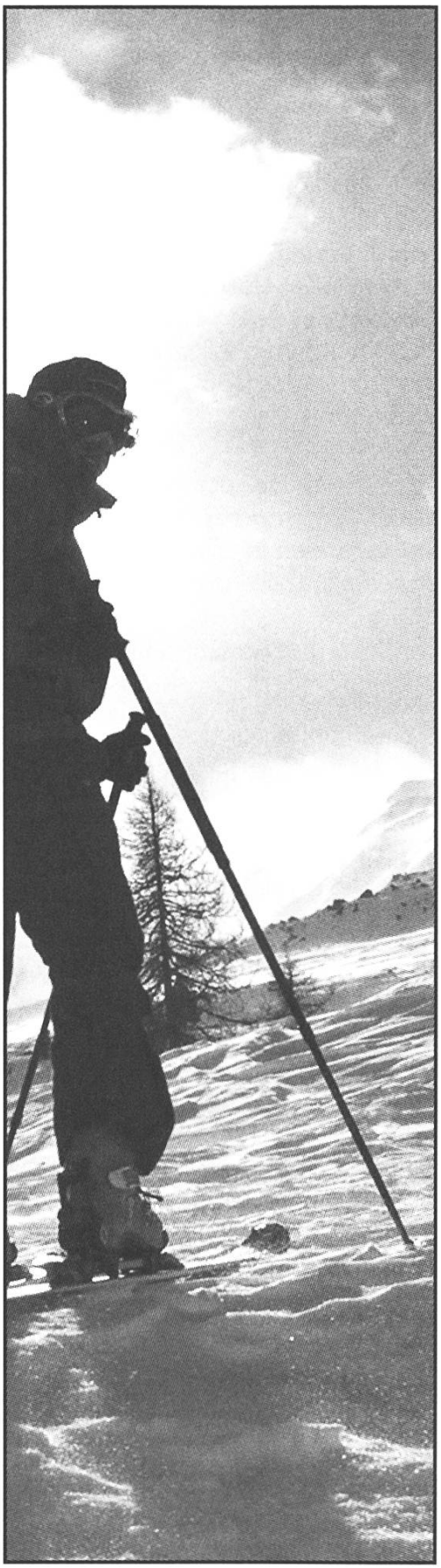
Aus gegebenem Anlass haben wir die erste Ausgabe der Visionen ausgegraben und ich möchte hier den damaligen Departementsvorsteher Prof. N. Wirth zitieren, der zur Gründung des VIS folgendes geschrieben hat:

„Ein studentischer Fachverein hat eine zweifache Aufgabe. Einmal soll er die fachlichen Interessen der Studenten wahrnehmen und dazu beitragen, die Studienzeit interessant und anregend zu machen. Anderseits hat er auch einen sozialen Auftrag: er soll die zwischenmenschlichen Kontakte fördern. Ich hoffe gerne, dass diese Kontakförderung sich auch auf Assistenten und Dozenten erstrecken möge. Das Publikationsorgan (Anm. d. Red: die Visionen) dient der Information, wobei sich diese durch Qualität eher als Quantität auszeichnen möge. [...]“

Die heutigen Visionen beinhalten einiges mehr an Quantität als die erste Ausgabe, wir hoffen, dass auch die Qualität mitgewachsen ist. Das aktuelle Konzept der Vorstellung von Forschungsgebieten aus Sicht der Dozierenden, Assistenten und Studierenden ist ein weiterer Schritt, den Auftrag zur Förderung der zwischenmenschlichen Kontakte zu erfüllen.

Titelbild: 7-D Hypercube

Inhalt



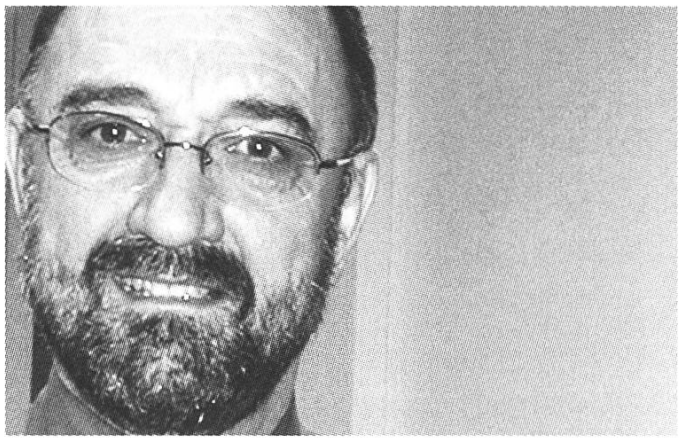
vom Departement

Fernweh

PROF. HANS HINTERBERGER - AKADEMISCHER REISEBERATER

Das folgende Zitat aus den Richtlinien für die koordinierte Erneuerung der Lehre an den universitären Hochschulen der Schweiz im Rahmen des Bologna-Prozesses (Bologna-Richtlinien) vom 4. Dezember 2003, bestimmt das Thema des Departements in diesen Visionen:

«... mit der Zielsetzung, dass im Rahmen dieses Reformprozesses ..., die Mobilität der Studierenden in allen Phasen des Studiums erweitert, ... werden soll, ...».



Vertikale und horizontale Mobilität

Erwirbt eine Studentin oder ein Student ein Bachelordiplom an der Universität A und wechselt zur Universität B für ein weiterführendes Studium (Master oder Doktorat), dann spricht man von vertikaler Mobilität. Im Gegensatz dazu verwendet man den Begriff horizontale Mobilität, wenn ein Teil des Studiums an einer anderen Universität absolviert wird, ohne dass dies zu einem Abschluss an der Gastuniversität führt.

Wenn die europäischen Bildungsminister und andere Entscheidungsträger im Bildungswesen heutzutage von Mobilität sprechen, dann beziehen sie sich in der Regel auf die vertikale Mobilität. Was ist aber gemeint, wenn sie sagen, die Mobilität soll erweitert werden? Im Wesentlichen beziehen sie sich dann auf:

a) Die Universitäten vereinheitlichen die Benennung ihrer Studienabschlüsse und
b) äquivalente Bachelordiplome werden für die Zulassung zum Masterstudium gleich behandelt (vgl. Visionen Januar 2004).

Vertikale Mobilität

Wie unterstützt Sie nun die ETH in der vertikalen Mobilität? Obwohl die Implementation des Bologna-Modells bei weitem noch nicht abgeschlossen ist, gibt es bereits erste Ansätze den internationalen Austausch zwischen kooperierenden Universitäten zu fördern. So wurden beispielsweise studiengangbezogene Arbeitsgruppen innerhalb der IDEA-League gebildet, in denen z.B. Qualifikationsprofile für die Bachelor- und Masterstudiengänge ausgearbeitet werden. Die IDEA-League ist eine strategische Allianz zwischen Imperial College London, TU Delft, ETH Zürich und RWTH Aachen.

Dieses Jahr zum ersten Mal verleiht jede IDEA-League Hochschule drei Masterstudium-Stipendien – je eine für Studierende der anderen Partner-Hochschulen. Es ist vorgesehen, dass diese 12 Stipendien jährlich vergeben werden und dazu beitragen Studierende in einem Masterstudiengang zu unterstützen. Zu beachten ist, dass das Masterdiplom von der Gastuniversität verliehen wird und die Studiengänge von unterschiedlicher Dauer sind. Ungleiche Studiengebühren und

Lebenshaltungskosten führen dazu, dass die Beträge der Stipendien verschieden hoch sind.

Jede Gastuniversität wird ihre eigenen Zulassungsverfahren anwenden. Leider ist die Anmeldefrist für 2004 bereits abgelaufen, aber vielleicht fassen Sie dieses Angebot fürs kommende Jahr ins Auge

Horizontale Mobilität

Viele möchten natürlich ein Austauschsemester oder Austauschjahr absolvieren und trotzdem ein Diplom der Heimuniversität erhalten. Mit den gestuften Studiengängen ist dies leider ohne eine Verlängerung der Studiendauer fast nicht zu schaffen. Denn im Masterstudiengang bedeutet bereits schon ein Austauschsemester, dass man die Hälfte der Vorlesungen auswärts gehört hat und im Bachelorstudiengang ist höchstens ein Semester im 3. Studienjahr halbwegs realistisch.

Trotzdem sollte man es sich überlegen, ob es sich lohnen würde, das Studium zugunsten eines Austauschs um ein oder zwei Semester zu verlängern. Ich denke, im Zeitalter der Globalisierung könnte es sich durchaus bezahlt machen. Deshalb hier einige Hinweise, herausgegeben von der Mobilitätsstelle der ETH Zürich, wo Sie auch weitere detaillierte Informationen erhalten können [1].

Als erstes sollten Sie sich entscheiden, ob Sie eine andere Hochschule entweder in der Schweiz, in Europa oder den USA besuchen möchten. Das Schweizerische Mobilitätsprogramm wurde als Gegengewicht zum europäischen Mobilitätsförderungsprogramm ERASMUS ins Leben gerufen. Die zugrunde liegende Philosophie ist dieselbe, so wie auch der Abwicklungsmodus ähnlich ist. Es sind Studierende angesprochen, die in der französischsprachigen oder in der italienischsprachigen Schweiz ein Mobilitätssemester oder Mobilitätsjahr absolvieren möchten.

SOCRATES ist eines der Bildungsprogramme der EU, das auch die EWR-Staaten einschliesst. Offiziell nimmt die Schweiz seit 1996 nicht mehr daran teil; sie konnte sich aber im Status eines «silent partner» mit vielen Hochschulen über eine Durchführung der Mobilität im Sinne von SOCRATES einigen. Ein Bestandteil von SOCRATES ist ERASMUS. Auf der Mobilitätswebseite finden Sie die für die Informatik in Frage kommenden Partnerhochschulen. Das Bestehen des 2. Vordiploms ist die Voraussetzung für eine Teilnahme am Programm. Daher wird das Erasmus-Studium vorwiegend im 3. Studienjahr absolviert und dauert im Normalfall ein oder zwei Semester. Die monatlichen Stipendien sind je nach Gastland wie folgt festgesetzt (Änderungen vorbehalten): AT, BE, DE, ES, FR, GB, IT, NL: Fr. 200,-; DK, FI, GR, IE, PT, SE: Fr. 250,-; NO: kein Stipendium. Der Anmeldetermin ist jeweils der 1. Mai für einen Aufenthalt im darauf folgenden Studienjahr. Je nach Gasthochschule können auch spätere Anmeldungen berücksichtigt werden.

Das Ausbildungs- und Forschungsinstitut EURECOM ist 1992 gemeinsam von der ENST Paris und der EPF Lausanne gegründet worden. Vor diesem Hintergrund ist an der ETH Lausanne das Departement «Systèmes de Communication» entstanden, von welchem ein Grossteil der Studierenden ihr letztes Studienjahr in Sophia Antipolis verbringt. Studierenden der ETH Zürich steht es (in begrenzter Zahl) offen, eben da eine

anwendungsorientierte Vertiefungsausbildung von 2 Semestern im Bereich der Kommunikationssysteme zu absolvieren, mit eventuell anschliessender Diplomarbeit.

Studierende der Departemente D-INFK und D-ITET können vom Doppelabkommen TIME (Top Industrial Managers for Europe) profitieren. Das Programm sieht ein zweijähriges Studium an einer ausländischen Universität vor (z.Zt. nur Ecole Centrale Paris), mit anschliessendem Studienabschluss an der Heimhochschule. Für das erfolgreiche Absolvieren des Programms wird das Diplom sowohl der Gast- als auch der Heimhochschule erteilt. Das Doppeldiplomstudium dauert ca. ein Jahr länger als ein reguläres ETH-Studium. Berücksichtigt werden nur Studierende mit sehr guten Studienleistungen.

UNITECH International ist ein Netzwerk von führenden europäischen technischen Universitäten und multinationalen Unternehmen. Das UNITECH Programm ermöglicht Top-Studierenden, ihre ausgezeichnete Ingenieursausbildung durch internationale akademische und berufliche Erfahrungen zu ergänzen.

Seit einigen Jahren baut die ETH Zürich mit amerikanischen Hochschulen Austauschbeziehungen auf. Es gelten dieselben Grundsätze wie bei einem sonstigen Mobilitätsaufenthalt. Informationen über Schulgeld und evtl. Stipendium finden Sie bei den einzelnen Angeboten. Es stehen i.d.R. so viele Plätze zur Verfügung, wie Studierende der jeweiligen Partnerhochschulen an die ETH kommen.

TASSEP ist ein loses Netzwerk einiger US-amerikanischer, kanadischer und europäischer Hochschulen zum Austausch von Studierenden. Im Sinne des Programms stehen den ETH-Studierenden die beteiligten Hochschulen jenseits des Atlantiks, d.h. in den USA und Kanada, offen, nicht jedoch die anderen europäischen Partner. Eine Liste aller beteiligten Hochschulen finden Sie auf der TASSEP-Webseite.

Praktikum im Ausland

Vielleicht möchten Sie nicht an einer anderen Hochschule Vorlesungen besuchen, sondern lieber ein Praktikum im Ausland absolvieren. Dabei unterstützen Sie an der ETH unter anderem die folgenden zwei Programme.

IAESTE:

International Association for the Exchange of Students for Technical Experience. IAESTE ist eine nicht politische, unabhängige Nichtregierungsorganisation, die aus Nationalkomittees in über 80 Ländern besteht. Die ETH Zürich ist einer der Partner von IAESTE Switzerland.

StudEx:

StudEx beteiligt sich im Auftrag des Bundesamtes für Bildung und Wissenschaft (BBW) am EU-Bildungsprogramm Leonardo da Vinci. StudEx vermittelt und unterstützt Auslandpraktika für in- und ausländische Studierende, Studien- und Lehrabgänger/-innen.

Ich beantworte gerne Ihre Fragen falls ich Ihren akademischen Reisehunger geweckt habe und Sie mehr Wissen möchten.

Links:

[1]: http://www.mobilitaet.ethz.ch/

interact

McKinsey sucht Persönlichkeiten mit ausgezeichnetem Hochschulabschluss und vertieften Kenntnissen in Informatik. Als **IT-CONSULTANT** unseres Business Technology Office unterstützen Sie bedeutende Unternehmen dabei, mit durchdachten Informatiklösungen im Wettbewerb zu punkten. Dabei spielen Sie das ganze Repertoire strategischer, technologischer und operativer Überlegungen aus. Ihre Einsatzbereitschaft und Freude an Teamwork sind deshalb genauso gefragt wie Ihre analytischen und fachlichen Stärken. Weil Sie international tätig sein werden, sind Sprachkenntnisse unerlässlich. Erfolgsfördernd ist zudem grosse Eigenständigkeit, die Sie im Studium oder ausseruniversitär bewiesen haben. Damit Sie in Ihrer Karriere rasch vorwärtskommen, fördern wir Ihre Talente durch interne Entwicklungsprogramme und gezieltes Coaching. Möchten Sie mehr über die unvergleichlichen Chancen im Topmanagement-Consulting wissen? **www.mckinsey.ch**

McKinsey & Company
Sophie Brunner
Alpenstrasse 3
8065 Zürich
Telefon 01 - 876 8000
Fax 01 - 876 9000
btozurec@mckinsey.com

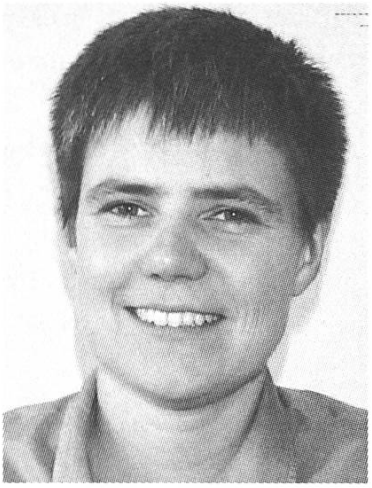
McKinsey&Company

vom Departement

Angelika Steger stellt sich vor

PROF. ANGELIKA STEGER - NEU AM DEPARTEMENT

Meine Stelle ist am Institut für Theoretische Informatik angesiedelt. Ich bin also – Theoretikerin. Ich weiss nicht welche Assoziationen dies bei Ihnen weckt. Bislang ist mir allzu häufig eine seltsame Mischung aus Mitleid und Bewunderung begegnet. Und so möchte ich diesen Artikel auch nutzen um zu schildern, warum ich eine begeisterte und überzeugte Theoretikerin bin, und warum Theorie viel mit Anwendung zu tun hat.



Zur Person

Studiert habe ich Mathematik an den Universitäten Freiburg, Heidelberg und an der State University of New York at Stony Brook. Dort habe ich nicht nur 1985 mein Studium mit dem Master of Science abgeschlossen, die Zeit in den USA war darüber hinaus für mich in vielerlei Hinsicht spannend und prägend. Zurück in Deutschland habe ich in Bonn am Forschungsinstitut für Diskrete Mathematik promoviert und habilitiert. Nach kurzer Wanderzeit trat ich 1996 eine Professur für Theoretische Informatik an der Technischen Universität München an. Dort gefiel es mir ganz ausgezeichnet: die TU München ist eine hervorragende Universität, München eine phantastische Stadt und die Berge sind nah. So gab es auch nur eine Universität, an die es mich wirklich reizte zu wechseln: Im Oktober 2003 habe ich es getan.

Zur Forschung

Die Theoretischen Informatik überschneidet sich mit der Mathematik und Physik und neuerdings verstärkt auch mit der Biologie. Eine Attraktion dieses Gebietes ist es, dass es noch unzählige offene Probleme gibt, die sich allgemeinverständlich stellen lassen, deren Lösungen aber alles andere als einfach sind. Man denke hier beispielsweise an das so genannte Rundreiseproblem:

Zu einer gegebenen Menge von Städten bestimme man eine kürzeste Tour durch alle Städte.

Ganz offenbar ist das Problem leicht zu lösen: Man probiert einfach alle möglichen Touren aus. Aber geht dies auch effizient?

Das Teilgebiet der Theoretischen Informatik, das mich zurzeit am meisten beschäftigt, lässt sich unter dem Stichwort „Average-Case-Analyse" zusammenfassen. Von vielen Problemen weiss man inzwischen, dass sie NP-schwer sind. Oft sind diese Probleme auch nicht approximierbar, d.h. es gibt keinen Algorithmus, der in polynomieller Zeit eine Lösung findet, die beispielsweise mindestens halb so gut ist wie das Optimum. Ein prominenter Vertreter der nicht-approximierbaren Probleme ist neben

dem oben bereits erwähnten Rundreiseproblem das Graphenfärbungsproblem: Gegeben sei ein Graph, finden Sie die kleinste Anzahl von Farben, die man benötigt, um die Knoten des Graphen so zu färben, dass benachbarte Knoten unterschiedliche Farben erhalten. Wenn man zeigt, dass ein Problem NP-schwer oder nicht-approximierbar ist, interessiert man sich für die Laufzeit des Algorithmus, für die bösartigste Instanz. Im Gegensatz dazu interessiert man sich bei der Average-Case-Analyse für die typische bzw. durchschnittliche Laufzeit. Leider gibt es hier bislang erst sehr wenige Resultate. Das bekannteste ist die Analyse des Sortieralgorithmus Quicksort, für den erst die Average-Case-Analyse bestätigt, was man aus der Praxis weiss, nämlich dass der Algorithmus meistens schneller eine Lösung findet, als zum Beispiel Mergesort oder Heapsort. Bei genauerem Hinsehen beruht die Analyse von Quicksort auf einer Aussage über Zahlensequenzen: Nimmt man ein zufälliges Element einer Folge, so ist es mit hoher Wahrscheinlichkeit ein gutes Pivotelement. Um zum Beispiel für Graphenalgorithmen ähnliche Aussagen treffen zu können, muss man also Eigenschaften kennen, die ein zufälliger Graph mit hoher Wahrscheinlichkeit besitzt. Dies führt zu der Theorie der zufälligen Graphen, die Sie nächstes Semester im Rahmen der Vorlesung „Random Graphs" studieren können (siehe auch den Abschnitt Lehre).

Neben der Average-Case-Analyse beschäftige ich mich noch mit zahlreichen anderen Problemkomplexen aus der Theoretischen Informatik. Hier möchte ich nur noch auf ein weiteres eingehen: das Problem der Lastbalancierung. In einem Netzwerk möchte man Jobs möglichst gleichmässig auf die vorhandenen Rechner verteilen. Modellieren kann man dieses Problem durch eine Menge von Bällen (Jobs) und einer Menge von Körben (Rechner) auf die die Bälle so verteilt werden sollen, dass alle Körbe möglichst die gleiche Anzahl Bälle enthalten. Stellt man das Problem so, ist es natürlich einfach, die Schwierigkeit kommt daher, dass man in dem Netzwerk die Kommunikationskosten niedrig halten möchte. Daher soll sich jeder Ball einen Korb aussuchen, ohne in alle Körbe zu sehen. Eine nahe liegende Strategie in diesem Szenario ist es, jedem Ball einen Korb zufällig zuzuweisen. Wie wir zeigen konnten ist es jedoch viel besser, dass sich jeder Ball zufällig zwei Körbe sucht und sich dann in denjenigen platziert, der aktuell weniger Bälle enthält. Auf diese Weise kann man das System beliebig lange laufen lassen, ohne dass ein Ungewicht in der Lastverteilung entsteht.

Zur Lehre

Eine reine Forschungsstelle anzunehmen, könnte ich mir nur sehr schwer vorstellen. Die Interaktion mit engagierten, talentierten und aufgeschlossenen Studenten und Doktoranden ist eine Herausforderung, die mir immer wieder sehr viel Freude bereitet. Ich versuche möglichst oft die Brücke zwischen Forschung und Lehre zu schlagen, zum Beispiel indem aktuelle Forschungsergebnisse in (Spezial-) Vorlesungen behandelt werden, oder im Rahmen von Diplomarbeiten und studentischen Projekten. Das bisher schönste und interessanteste Projekt in dieser Richtung hatte die Entwicklung eines Prototypen für eine IT-basierte Rekonstruktion zerrissener Stasi-Akten zum Thema. Hierüber berichten zwei ehemalige Teilnehmer des Projektes, Martin Marciniszyn und Andreas Weißl, ausführlich an anderer Stelle in dieser Ausgabe der Visionen. An der ETH habe ich im letzten Semester die Vorlesung „Random Graphs" gehalten. Aufgrund meines kurzfristigen Wechsels von München nach Zürich, wurde sie allerdings sehr spät angekündigt, so dass sie ausschliesslich von Doktoranden und meinen aus München „importierten" Diplomanden besucht wurde. Auf Wunsch einiger Studenten wird die Veranstaltung im nächsten Semester

deswegen von Stefanie Gerke, einer Oberassistentin in meiner Gruppe, noch einmal angeboten. Ich selbst werde im nächsten Sommer die Vorlesung „Graphalgorithmen“ halten und im Herbst die beiden Veranstaltung „Randomisierte Algorithmen“ und die Grundstudiumsvorlesung „Algorithmen und Komplexität“ für die Mathematiker lesen.

Ich würde mich sehr freuen, Sie in der einen oder anderen Vorlesung demnächst kennen zu lernen. Gerne steht ich auch für Fragen nach Themen für Semester- oder Diplomarbeiten zur Verfügung. Einen ersten Eindruck über das mögliche Themenspektrum finden Sie auf unseren Webseiten [1].

Links:

[1]: www.ti.inf.ethz.ch/as/


visionen

Herausgegeben vom Verein der Informatikstudenten an der ETH Zürich (VIS)
erscheint monatlich während des Semesters Auflage 800 Ex.

Hier hätte unser Signet stehen sollen. Leider ist das gültige Original im Fotolabor verschollen, so dass wir hier nur einen unvollkommenen Vorentwurf zeigen können.

18. Mai 1984 Erster Jahrgang Nr. 1

Visionen

Das Bild oben war die Titelseite der ersten Visionen. Vieles hat sich seither verändert. Wer neben dieser Auswahl von Titelbildern noch mehr sehen will, geht auf:
www.vis.ethz.ch -> Anlässe -> Photos -> 2000-09 AlleVisionenTitelbilder.
Dort finden sich bisherige Titelbilder.


visionen

TI

Theoretische Informatik

PROF. ROBERT STÄRK - KANN THEORETISCH JEDES PROBLEM LÖSEN

Die Theoretische Informatik befasst sich mit mathematischen, logischen und formalen Konzepten der Informatik. Das Ziel der Theoretischen Informatik ist die Natur der Berechnung besser zu verstehen und als Konsequenz daraus, effizientere Methoden und Algorithmen zu entwickeln. Die Theoretische Informatik wird oft in zwei grössere Gebiete unterteilt.

Das erste Gebiet „Algorithmen, Automaten, Komplexität und Spiele" umfasst das Studium der Algorithmen und ihrer Komplexität mit Hilfe von analytischen, kombinatorischen und probabilistischen Methoden. Es schliesst auch die abstrakte Komplexitätstheorie mit ein (das berühmte „P = NP" Problem) sowie die Automaten- und Sprachtheorie und geometrische (graphische) Anwendungen.

Das zweite Gebiet „Logik, Semantik und Theorie der Programmierung" ist den formalen Methoden gewidmet. Es geht um die Semantik von sequentiellen und parallelen Programmen -- oder allgemeiner Computersystemen -- und wie man deren Eigenschaften formal beweist. Die Entwicklung und Erweiterung von Kalkülen zur Spezifikation von Prozessen und komplexen Systemen steht im Zentrum der Untersuchungen.

Am Institut für Theoretische Informatik ist das Gebiet der Algorithmik vertreten durch Prof. Bläser (Komplexitätstheorie und Algorithmen), Prof. Steger (Kombinatorische Strukturen und Algorithmen), Prof. Welzl (Theorie der kombinatorischen Algorithmen) und Prof. Widmayer (Algorithmen, Datenstrukturen und Anwendungen). Die Gruppe „Informationssicherheit und Kryptographie" von Prof. Maurer gehört ebenfalls zum Institut für Theoretischen Informatik, da ihre Forschungsthemen auf mathematischen Methoden basieren. Ausserhalb des Institutes stehen mehrere Forschungsgruppen der Algorithmik nahe wie etwa Prof. Wattenhofer (Verteilte Systeme) und Prof. Hromkovic (Informationstechnologie und Didaktik). Es gibt Verbindungen zu Operations Research (Optimierung) und auch zur Theorie von alternativen Berechnungsmodellen (neuronale Netze, genetische Algorithmen, Quantencomputer).

Die Theoretische Informatik an unserem Departement hat sich immer als Brücke zwischen Anwendung und Theorie verstanden und nicht als unabhängige Einheit. Sobald man sich wis-

senschaftlich mit einem Problem befasst, braucht man eine klare mathematische und theoretische Grundlage. Man sollte sich dann aber nicht in der reinen Theorie verlieren, sondern die Anwendungen immer im Auge behalten.

Meine eigene Forschungsgruppe „Formale Spezifikation, Verifikation und Validierung von Systemen" ist Teil des Gebietes „Logik, Semantik und Theorie der Programmierung" und hat ‹berschneidungen mit Software Engineering und mathematischer Logik. Das Hauptinteresse liegt zur Zeit bei den „Abstract State Machines" einer Methode zur Spezifikaton und Analyse von komplexen Systemen.

Der Ursprung der „Abstract State Machines" (ASMs) liegt in einer Kritik der These von Church und Turing. Die These sagt, dass jeder Algorithmus auf einer Turing-Maschine simuliert werden kann. Für praktische Probleme sind Turing-Maschinen aber unbrauchbar. Man stelle sich nur einen einfachen Graphalgorithmus vor, der als Bestandteil eines Rechenschrittes überprüfen muss, ob zwei Knoten des Graphen durch eine Kante verbunden sind. Eine Turing-Maschine muss dazu ihren Lese/Schreibkopf über weite Distanzen des Speicherbandes bewegen und ihren internen Kontrollzustand mehrmals ändern. In den meisten Graphalgorithmen geht man aber davon aus, dass diese Operation in einem einzigen Schritt erledigt werden kann.

Yuri Gurevich hat die Church-Turing-These darum 1985 verschärft zur ASM-These:

Jeder Algorithmus/jedes Computersystem kann auf seiner natürlichen Abstraktionsstufe Schritt für Schritt durch eine „Abstract State Machine" (ASM) simuliert werden.

Die Betonung liegt dabei auf der Schritt-für-Schritt-Simulation. Das heisst, dass ein Schritt des Algorithmus genau ein Schritt auf der abstrakten Maschine erfordert. Die ASM-These umfasst zudem nicht nur Algorithmen sondern beliebige Computersysteme wie paralle, nebenläufige, und verteilte Systeme und auch Kommunikationssysteme.

Die Zustände einer ASM sind (endliche oder unendliche) algebraische Struktuern, wie sie in der Mathematik und der Logik schon seit bald 100 Jahren benutzt und untersucht werden. Die Strukturen werden als eine Art abstraktes Memory aufgefasst. Ein mathematischer Term f(x + f(y)) entspricht einem Ausdruck mem[x + mem[y]]. Die Funktion f ist dynamisch und kann ihre Werte ändern. Der Wert f(x) ist der Inhalt der Funktion f an der Lokation x, so wie mem[x] der Inhalt der Speicherzelle mit Adresse x bezeichnet.

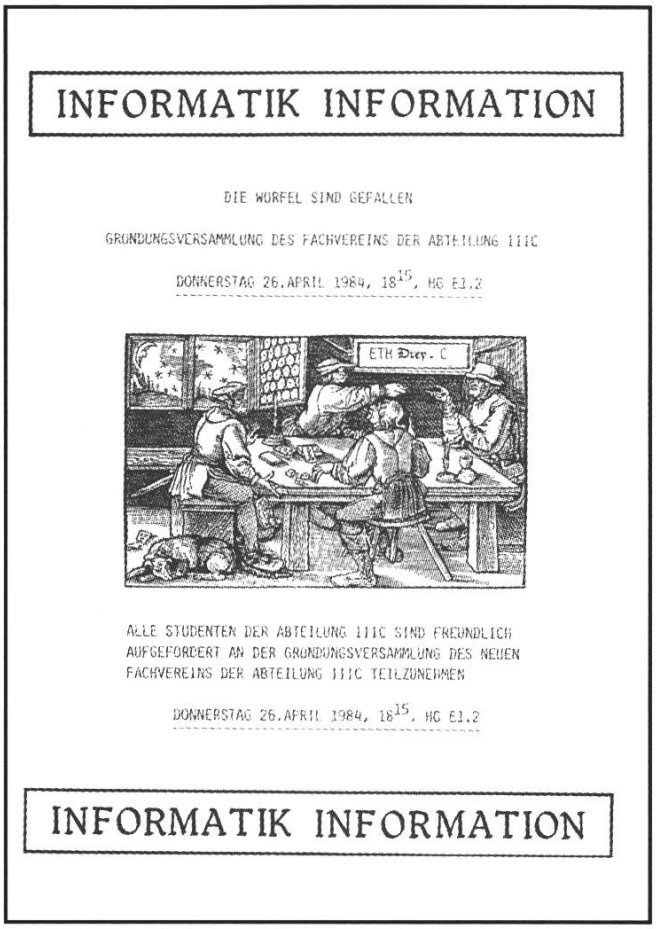
Um ein System Schritt für Schritt simulieren zu können, muss eine ASM mehrere Lokationen von dynamischen Funktionen gleichzeitig (parallel) aktualisieren können. Die parallele Komposition spielt darum bei den ASMs eine wichtigere Rolle als die sequenzielle Komposition, an die wir uns von den imperativen Programmiersprachen so sehr gewöhnt haben. Die Übergangsrelation einer ASM wird im wesentlichen durch eine parallele Komposition von bedingten Updates beschrieben. Gurevich hat 2001 bewiesen, dass unter bestimmten Postulaten, dies zumindest für sequenzielle Algorithmen genügt.

Die ASM-Methode ist erfolgreich eingesetzt worden in der Industrie (Beispiel: Siemens, FALKO, Simulation der Untergrundbahn der Stadt Wien, 1998) und wird in der Gruppe

„Foundations of Software Engineering“ bei Microsoft Research verwendet. The ITU Standard für die Spezifikations- und Beschreibungssprache SDL-2000 hat ein ASM-Modell als offizielle Definition akzeptiert. Im Buch „Java and the Java Virtual Machine:

Definition, Verification, Validation“ (R. Stärk, J. Schmid, E. Börger, Springer-Verlag, 2001) haben wir ASMs zur vollständigen Spezifikaton der Programmiersprache Java, der JVM, eines Compilers und der Bytecode-Verifikation verwendet. Beim Versuch, die Korrektheit zu beweisen, haben wir Lücken in den Konzepten von Java festgestellt, wie Programme, die zwar ohne Fehler compiliert werden, aber dann nachher vom Bytecode-Verifier abgelehnt werden und auf der JVM nicht ausgeführt werden können. Andere Forschungsgruppen, die sich mit anderen Methoden zu tief in der Formalisierung von Java begeben haben und die richtige Abstraktionsstufe verloren haben, fanden solche Programm nicht.

Die Vorteile der ASM-Methode sind: Präzision (einfache klare mathematische Semantik), Direktheit (keine unnötige Kodierung, direkte Modellierung von Systemen), Verständlichkeit (jeder Programmierer kann ASM-Code lesen), Ausführbarkeit (Tests und Experimente sind auf der Spezifikationsstufe möglich), Skalierbarkeit (Spezifikation auf beliebigen Abstrationsstufen, Verfeinerung), Allgemeinheit (sequenzielle, parallele, verteilte Systeme mit Echtzeit oder abstrakter Zeit, endlichem oder unendlichem Zustandsraum und echter Nebenläufigkeit). Eine Übersicht findet man in dem Buch „Abstract State Machines: A Method for High-Level System Design and Analysis“ (E. Börger und R. Stärk, Springer-Verlag, 2003).


INFORMATIK INFORMATION

DIE WÜRFEL SIND GEFALLEN

GRÜNDUNGSVERSAMMLUNG DES FACHVEREINS DER ABTEILUNG IIIC

DONNERSTAG 26.APRIL 1984, 18^{15}, HG E1.2

ALLE STUDENTEN DER ABTEILUNG IIIC SIND FREUNDLICH AUFGEFORDERT AN DER GRÜNDUNGSVERSAMMLUNG DES NEUEN FACHVEREINS DER ABTEILUNG IIIC TEILZUNEHMEN

DONNERSTAG 26.APRIL 1984, 18^{15}, HG E1.2

INFORMATIK INFORMATION

WLAN im ETH-Bus

Der ETH-Pendelbus wird im Sommersemester testweise mit Wireless LAN ausgeruestet. Der Betrieb startet am 30. Maerz und dauert bis zum 2. Juli. Er wird durch eine Projektpartnerschaft der ETH Zuerich mit sunrise und den VBZ ermoeglicht.
Der Datenverkehr wird von der Wireless-LAN-Basisstation ueber GPRS ins Mobilnetz von sunrise geleitet (2 Kanaele mit insgesamt bis zu 48 kbps). Die Nutzerinnen und Nutzer muessen diese begrenzte Bandbreite teilen, weshalb nur eine kleine Datenrate moeglich ist.
Vom 13. bis 19. April und vom 21. bis 27. Juni findet zudem eine Umfrage statt. Zu gewinnen gibt es 120 sunrise pronto Prepaid-Karten im Wert von je CHF 48.-!

happy birthday vis

MV Ankuendigung

BETTINA - IM VIS VORSTAND

Vor 20 Jahren war es soweit. Ein Grüppchen eifriger Studenten sah ein, dass es an der Zeit war, sich zu organisieren und einen Verein zu gründen! Endlich ein legitimer Grund Feste zu feiern!

Aber ich denke, das war nur einer der Gründe, warum Pascal Faivre am 26. April 1984 die Informatiker und ein paar Informatikerinnen zusammenrief. Die Möglichkeiten als Fachverein die Studierenden im Departement zu vertreten, aktiv an Unterrichtskommissionen teilzunehmen und praktische Dienstleistungen zu erbringen, wurde anscheinend schon damals als wichtig erachtet.

Interessant wäre noch zu erwähnen, dass damals auch über den Namen abgestimmt wurde. In die Endauswahl gelangten:

VIP - Verein der Informatikstudenten am Poly
VIS - Verein der Informatikstudenten an der ETH

Der Vorschlag VIS wurde mit 27 zu 17 Stimmen angenommen. Sonst wären wir wohl heute noch der VIP. Und die **Vis**ionen hiessen wohl **V**oll **I**nteressantes **P**rospekt oder so ähnlich...

Was würde wohl heute bei dieser Abstimmung rauskommen? Um solche wichtige Meilensteine des VIS nicht zu verpassen und selber mitbestimmen zu können darf man an der MV nicht fehlen.

Der damalige Vorstand bestand aus sieben Studenten, Fredi war unser erster Präsident, dann waren da noch Josef, Beat, Stefan, Urs, Alex und Martin. Sie waren unser erster offiziell gewählter VIS-Vorstand. Und jetzt müsst ihr euer Wahlrecht wahrnehmen und den VIS-Vorstand fürs Sommersemester 2004 wählen!

Ganze 50 Nasen fanden sich an der Gründungsversammlung zusammen, ja! Und wir hoffen, dass ihr mindestens so zahlreich zu der 20-Jahre-VIS-MitgliederVersammlung erscheint wie damals! Natürlich relativ gesehen, das entsprach damals nämlich ca. 10% der Informatikstudierenden! Also hopp! Natürlich feiert man Geburtstag nicht nur mit Mineralwasser, wir werden gebührend auf 20 Jahre VIS anstossen können!

Vormerken:

Wann?
Montag 26. April 2004, 18.00 Uhr
Was?
VIS MV, mit anschliessender 20 Jahre VIS Geburtstagsfeier
Wer?
Alle Mitglieder des VIS

TI

Kryptographie

KRZYSZTOF PIETRZAK - TI ASSISTENT

„Gentlemen do not read each others mail"
-- Henry Lewis Stimson

Für viele Probleme gibt's eine einfache und elegante Lösung. Leider funktioniert die oft nur so lange wie sich alle ans Protokoll halten. Sobald wer betrügt wird's kompliziert. Das ist der Grund wieso wir fancy Banknoten und nicht bunte Kieselsteine als Zahlungsmittel verwenden. Das Aufkommen von Computern hat die Problematik nochmals verschärft. Daten werden heute digital verarbeitet und übertragen. Klassische Werkzeuge wie Siegel oder Schlösser welche früher für Geheimhaltung und Integrität von Informationen gesorgt haben sind hier nicht mehr anwendbar.

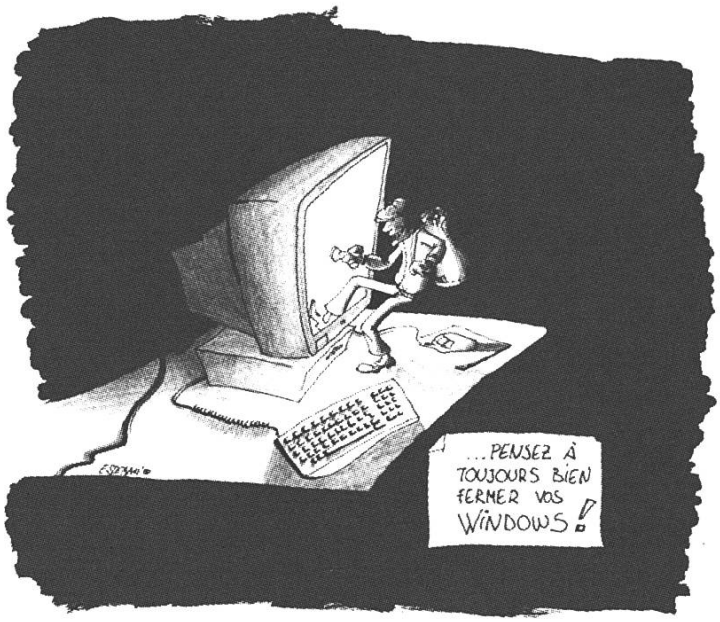
Und hier kommt Krypto ins Spiel! Die Kryptographie befasst sich mit Protokollen welche selbst dann noch funktionieren sollen, wenn sich wer wo nicht an die Regeln hält. Krypto gab's natürlich schon bevor es Computer gab. Früher war das mehr so eine Art Kunst. Die „Kryptologen" haben Codes zum Verschlüsseln von Nachrichten erfunden und andere haben die auch gleich wieder gebrochen. Im letzten Jahrhundert hat sich die Kryptographie weg von einer Kunst zu einer Wissenschaft entwickelt in welche Gebiete wie die Informationstheorie, Komplexitätstheorie, Zahlentheorie, Kombinatorik und Quantenmechanik einfliessen.

Informationstheoretische und Komplexitätstheoretische Krypto

Vorlesungen: Information und Kommunikation, Informationssicherheit und Kryptographie

Claude Shannon, der Erfinder der Informationstheorie, hat 1949 den ersten richtigen Beweis für die Sicherheit eines Verschlüsselungsverfahren, des One-Time-Pads, gegeben. Der One-Time-Pad ist absolut nicht zu brechen, das Chiffrat enthält, wenn man des geheimen Schlüssel nicht kennt, schlicht keine Information über die darin Verschlüsselte Nachricht. Leider muss beim One-Time-Pad der geheime Schlüssel mindestens so lange sein wie die Nachricht die man verschlüsseln will, und wie der Name schon sagt, darf dieser Schlüssel nur ein einziges mal verwendet werden!

Die Sicherheit von der meisten „praktikablen" Kryptosysteme kann leider nicht so rigoros (also informationstheoretisch) bewiesen werden wie



„Evil will always triumph, because good is dumb."
(Rick Moranis in Space Balls, directed by Mel Brooks)

die des One-Time-Pads. Vielmehr basiert die Sicherheit auf der Annahme, dass ein möglicher Gegner, welcher einen geheimen Schlüssel nicht kennt und nur über beschränkte Rechenresourcen verfügt, ein bestimmtes Problem nicht in vernünftiger Zeit lösen kann.

So richtig was zu beweisen dürfte hier jedoch schwierig sein: jeder Beweis, dass ein solches Problem wirklich nicht effizient lösbar ist, würde P ungleich NP implizieren, also das wichtigste offene der Problem der Komplexitätstheorie beantworten.

Public-Key Kryptographie

Vorlesung: Informationssicherheit und Kryptographie, Kryptographische Protokolle

Wenn man jetzt also an die Schwierigkeit von gewissen Problemen glaube, können zwei Parteien, welche einen kurzen gemeinsamen geheimen Schlüssel besitzen, bereits recht viel machen, z.B. beliebig viele Nachrichten geheim hin- und austauschen.

1976 haben Diffie und Hellman die wohl bedeutendste Entdeckung in der Kryptogeschiche gemacht, die Public-Key Kryptographie. Mit dem Diffie-Hellman Protokoll können sich zwei Parteien „aus dem nichts" einen geheimen Schlüssel generieren (Ellis und Cocks vom Britischen Geheimdienst haben das schon sechs Jahre früher rausgefunden, die durften aber nicht damit angeben).

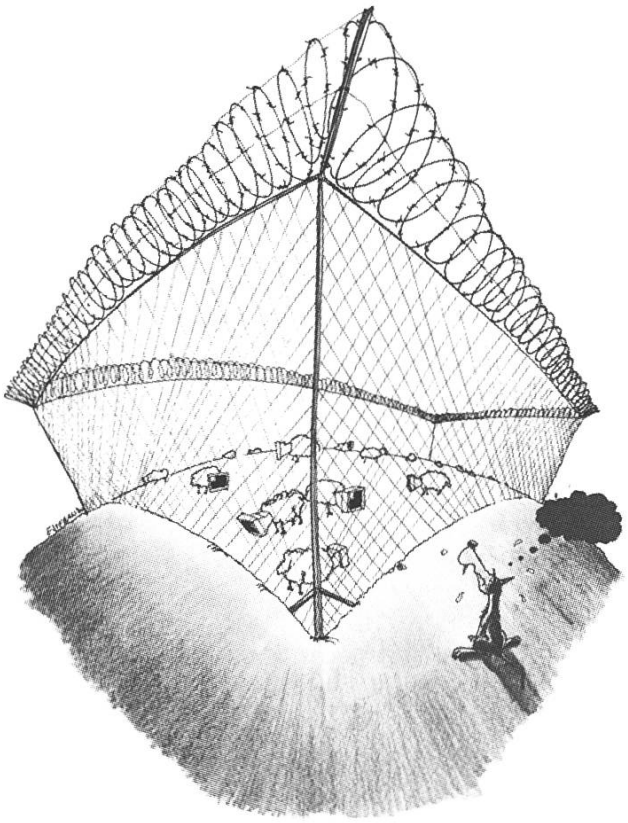
Damit war es nun für zwei Parteien plötzlich möglich, über völlig unsichere Kanäle (z.B. das Internet) geheim zu kommunizieren, ohne sich vorher auf einen geheimen Schlüssel einigen zu müssen.

Im Gegensatz zur klassischen Kryptographie, wo man sich die „schwierigen Probleme" mehr oder weniger beliebig zusammenbasteln konnte, müssen die „schwierigen Probleme" auf welchen die Public-Key Kryptographie beruht sehr viel Struktur besitzen. Probleme aus der Zahlentheorie, wie das Faktorisieren, haben sich da als besonders geeignet erwiesen. Man kann wohl sagen, dass die Zahlentheorie dank der Public-Key Kryptographie in den letzten Jahrzehnten ein regelrechtes Revival erlebt hat.

Mehr als nur Verschlüsseln

Vorlesung: Kryptographische Protokolle

Historisch versteht man unter Kryptographie das Entwerfen von Codes für die geheime übermittlung von Nachrichten. Heute fällt vieles was im weitesten Sinne was mit der Geheimhaltung oder Integrität von Daten zu tun hat, in den Kryptotopf. So wurden in den letzten Jahrzehnten neue, zum Teil paradox scheinende Kryptographische



Protokolle entdeckt. Zero-Knowledge Beweise sind ein schönes Beispiel.

Bei einem Zero-Knowledge Beweis überzeugt ein Spieler A einen Spieler B von einer Aussage (z.B. „Die Zahl n hat genau drei Primfaktoren"). Und zwar so, dass am Ende des Beweises B überzeugt ist, dass die Aussage stimmt, ansonsten jedoch absolut nichts neues erfährt (für obige Aussage also insbesondere keine Ahnung hat welches die drei Primfaktoren jetzt sind).

Kryptographie in der Quantenwelt

Vorlesung: Introduction to Quantum Computation

Wie gesagt, Public-Key Kryptographie basiert heutzutage fast ausschliesslich auf der Schwierigkeit von Zahlentheoretischen Problemen. Insbesondere dem Faktorisieren und dem sog. Diskreten Logarithmus Problem. Alle Vorschläge von Public-Key Kryptosystemen welche auf anderen Problemen beruhen sind entweder extrem ineffizient oder wurden gebrochen (meist beides). Aber ist ja egal, seit Jahrmillionen suchen Mathematiker nach effizienten Faktorisierungsalgorithmen, und es sieht nicht danach aus, als ob man hier in naher Zukunft mit einem ultimativen Durchbruch rechnen müsste. Doch vor zehn Jahren erwuchs plötzlich Gefahr aus einem ganz unerwarteten Ecke, der Realität, denn die ist bekanntlicht Quantenmechanisch. 1994 publizierte Peter Shor einen effizienten Algorithmus zum Faktorisieren und für das Diskrete Logarithmus Problem. Shors Algorithmus läuft jedoch nur auf einem sogenannten Quantencomputer, und es ist nicht klar, ob es überhaupt möglich ist einen solchen zu bauen. Aber wenn... ja wenn, dann muss man sich was einfallen lassen um weiterhin Public-Key Krypto zu betreiben. Aber die Quantenrealität ist nicht nur das Problem, sondern bietet auch gleich eine elegante Lösung. Während jedes klassische Public-Key Kryptosystem auf einem einem „schwierigen Problem" basieren muss, ist dies in der Quantenwelt nicht mehr der Fall. Quanteninformation wird durch blosses „betrachten" unwiederrufbar verändert!

Diese Tatsache kann man sich zu nutze machen, um heraus zufinden, ob jemand einen Kanal abhorcht.

„We can factor the number 15 with quantum computers. We can also factor the number 15 with a dog trained to bark three times."

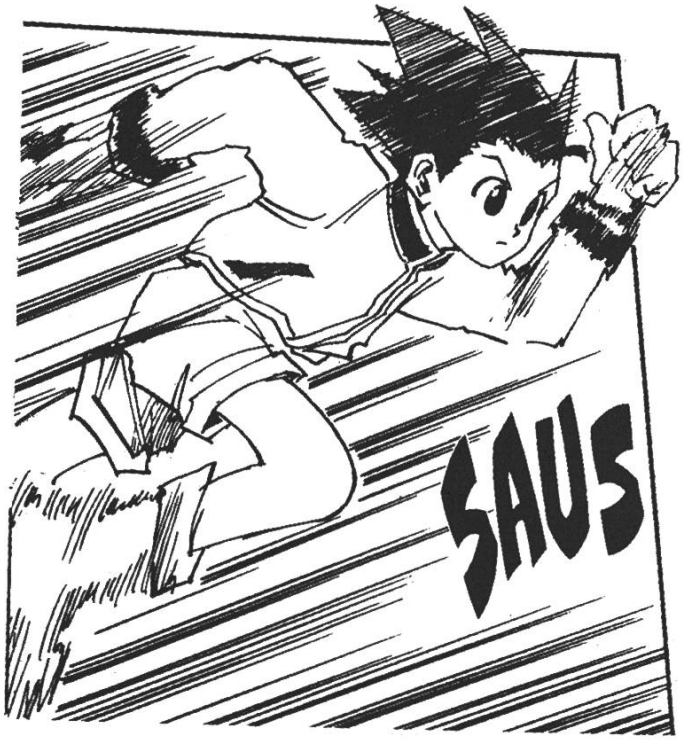
-- Robert Harley, 5/12/01, Sci.crypt.

TI

If you do it then do it fast

ROBERT BERKE - INFORMATIKER IM SAUSESCHRITT

Ähnlich wie in dem entsprechendem Artikel in der letzten Ausgabe der Visionen wage ich nicht zu behaupten, dass es möglich ist, Forschung in der Theoretischen Informatik zu betreiben, ohne ein Flair für die Mathematik zu haben. Wobei (so hoffe ich doch) ein Informatik-Studium an der ETH doch ausreichen sollte. Ganz anders denke ich aber verhält es sich mit dem Verständnis vieler Probleme aus der Theoretischen Informatik. Oft handelt es sich hier um sehr einfache Ideen - zumindest im Nachhinein. Die Schwierigkeit besteht darin die richtige Abstraktionsebene zu finden.



In diesem Artikel werde ich über einen nahen Verwandten des berühmten SAT Entscheidungs-Problem schreiben.

Ein Algorithmus für k-SAT

Gegeben ist eine erfüllbare logische Formel F mit n Bool'schen Variablen in konjunktiver Normalform (siehe Logik im 1. Semester) deren Klauseln höchstens k Literale (Variable oder deren Negation) enthalten.

Das Problem und dessen Lösung wurden kürzlich von Professor Emo Welzl in der Vorlesung, *Erfüllbarkeit logischer Formeln* vorgestellt und sind Gegenstand aktueller Forschung in der Theoretischen Informatik.
Wie schwierig ist dieses Problem denn überhaupt? Natürlich könnte man per Brute-Force alle 2^n Belegungen auf Erfüllbarkeit mit F testen. Ausserdem wissen wohl alle Informatiker, dass SAT für k>=3 die Mutter aller NP-vollständigen Probleme

$$F = (x \vee y \vee z) \wedge (x \vee \bar{y} \vee \bar{z}) \wedge (\bar{x} \vee y \vee \bar{z}) \wedge (\bar{x} \vee \bar{y} \vee z) \quad \text{with } n = 3, k = 3$$

Ziel: Finde schnellstmöglich eine Belegung der boolschen Variablen welche F erfüllt.

ist. Ein polynomieller Algorithmus der eine erfüllbare Belegung für F findet, würde zugleich

einen polynomiellen Algorithmus um SAT zu entscheiden liefern. Dies ist aber unmöglich (ausser P=NP). Deshalb geben wir uns bescheidener und suchen Algorithmen deren Laufzeit $O(c^n \text{ poly}(n))$ mit $c<2$ ist, wobei poly(n) alle polynomiellen Faktoren schluckt.

Wie sieht solch ein *schneller* Algorithmus denn aus? Nun viel kürzer als der folgende Algorithmus rfb(F), wobei F die gegebene Formel ist, scheint wohl fast unmöglich zu sein.
An jeder Stelle an der eine schwierige Entscheidung ansteht trifft der Algortihmus seine Wahl entweder zufällig, oder beliebig (wobei hier zufällig als gleichverteilt auf allen Möglichkeiten gemeint ist). Die eigentlich schwierige Arbeit, nämlich die Laufzeitanalyse steht uns aber noch bevor. Ausserdem fehlt dem Algorithmus noch eine kleine, aber äusserst wichige Zutat, wie sogleich klar werden wird.

1: function **rfb**(F)
2: $\alpha \underbrace{\longleftarrow}_{randomly}$ in $\{0,1\}^n$;
3: **loop**
4: **if** α satisfies F **then** return 1;
5: $C \underbrace{\longleftarrow}_{some}$ unsatisfied clause in F;
6: $x \underbrace{\longleftarrow}_{randomly}$ variable in C;
7: flip assignment for x in α;
8: **end loop**

Betrachten wir den Algorithmus nachdem wir eine zufällige Belegung der Variablen gewählt haben (2. Zeile). Wir starten die Loop-Schleife und überprüfen, ob die Formel F bereits erfüllt ist (4. Zeile). Hat uns dazu aber das Quäntchen Glück gefehlt ändern wir den Wahrheitswert einer Variablen x welche zufällig aus einer unerfüllten Klausel C gewählt wurde (Zeilen 5/6/7) (Wichtiges Detail: Die Klausel wurde beliebig, nämlich ohne Zufall aus allen unerfüllten Klauseln, darauf die Variable zufällig, ohne jegliches Belieben aus der Klausel gewählt). Die Schleife iteriert und es wird erneut getestet, ob nun die Belegung die Formel F erfüllt, wobei sich die alte und die neue Belegung natürlich nur in einer Position unterscheiden.

Da eine Klausel aus höchstens k-1 Disjunktionen von Variablen besteht, darf unter der Belegung kein Literal der unerfüllten Klausel zu wahr evaluieren. Die Wahrscheinlichkeit in einer Iteration einer erfüllbaren Belegung einen Schritt näher zu kommen ist deshalb mindestens 1/2^k.

Der Algorithmus merkt sich nicht welche Belegungen der Variablen er bereits geändert hat. Daher kann es durchaus sein, dass gewisse Schritte rückgängig gemacht werden - dies ist bei zuvor schlechter Wahl sinnvoll und wohl einer der Stärken randomisierter Algorithmen. Problematisch ist der Fall, wenn der Algorithmus sich lange in Zyklen befindet und/oder nur sehr gelegentlich Fortschritte macht. In der Tat ist die erwartete Anzahl Schritte bis wir eine erfüllbare Belegung erreichen unendlich.

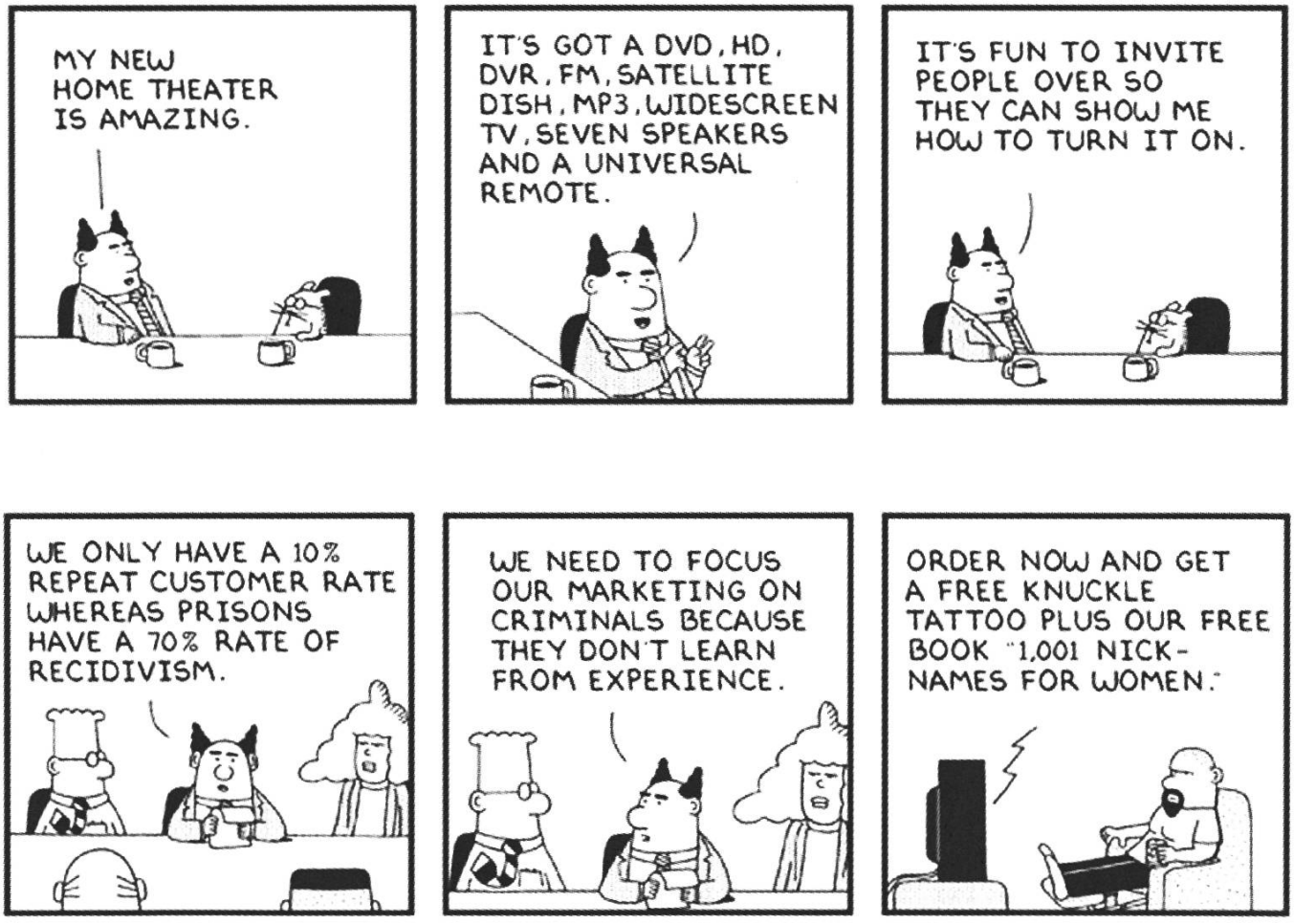
Aber aus dieser Misere gibt es einen Ausweg. Wie uns eine genauere Analyse zeigen würde, benötigt rfb(F) zwar oft (abhängig von der Wahl der Zufälligkeiten in den Zeilen 2/6) sehr lange bis er eine erfüllbare Belegung der Variablen findet und manchmal schafft er dies sogar gar nicht. Andererseits existiert jedoch eine für uns ausreichend hohe Anzahl an ‚Instanzen' von rfb(F), welche sehr schnell zu unserem Ziel gelangen. Es liegt nun auf der Hand, gemäss IF YOU DO IT THEN DO IT FAST, den Algorithmus rfb(F) nach nur kurzer Zeit abzubrechen (z.B. nach 3n vielen Iterationen der Loop-Schleife) und unser

Glück mit einem weiteren Aufruf von rfb(F) erneut herauszuforden.

Somit sind wir nun an der erwarteten Anzahl Schritte interessiert unter der Bedingung, dass dies höchstens endlich viele sind. Ausserdem kann eine untere Schranke für die Wahrscheinlichkeit, dass ein Aufruf von rfb(F) eine erfüllbare Belegung für F nach der vorgegebenen Anzahl Iterationen der Loop-Schleife gefunden wird, gegeben werden.

Dieses Resultat stammt von Uwe Schöning, dessen optimale Wahl der Anzahl Iterationen der Loop-Schleife und der Anzahl Aufrufe von rfb(F) für z.B. k=3 zu einer erwarteten Gesamtlaufzeit von $O((4/3)^n \text{ poly}(n))$ führt - so schnell wie (fast) kein anderer bekannter Algorithmus.

Nun ja, das war ein sehr kurzer Überblick über das Problem und dessen Lösung, wobei viele Einzelheiten unter dem Teppich verschwinden mussten (I did it and I was forced to do it fast...). Der Algorithmus ist in „Uwe Schöning: A probabilistic algorithm for k-SAT based on limited local search and restart, Algorithmica 32 (2002) 615-623" erschienen und wird wohl erneut im nächsten Wintersemester in der oben erwähnten Vorlesung in seiner vollen Pracht erklärt werden.



TI

TI-Master

MELANIE-StudenTIn

Nachdem ich letztes Mal versucht habe, euch mein Nebenfach näher zu bringen, werde ich dieses Mal über den TI-Master berichten.

Die Kryptofächer, die ich im Nebenfach hatte, werden nicht nochmals vorgestellt, obwohl sie auch Fokusfächer des TI-Masters sind. Da mir die Fragen vorgegeben sind, führe ich jetzt eine Art Selbstinterview:

Melanie Raemy: Wieso hast Du den TI-Master gewählt?
Melanie Raemy: Ich habe nicht wie andere (vgl. letzte Visionen) die Begründung in meiner Kindheit gesucht..

Im Grundstudium habe ich darauf geachtet, welche Vorlesungen ich am liebsten mag, von welchen Dozenten ich noch mehr hören möchte und mich dann informiert, was die sonst noch so tun. Diese Dozenten waren Welzl, Maurer und Widmayer; womit meine Entscheidung erklärt wäre.

Trotzdem möchte ich noch eine andere Methode aufzeigen, die ich sehr zuverlässig finde: Man nehme ein Vorlesungsverzeichnisheft von Herrn Dubach und streiche alles rot an, was man unbedingt nehmen will und alles gelb, was noch interessant klingt. Dann übertrage man die Farben auf die Mastervertiefungslisten und nehme den farbigsten Master.

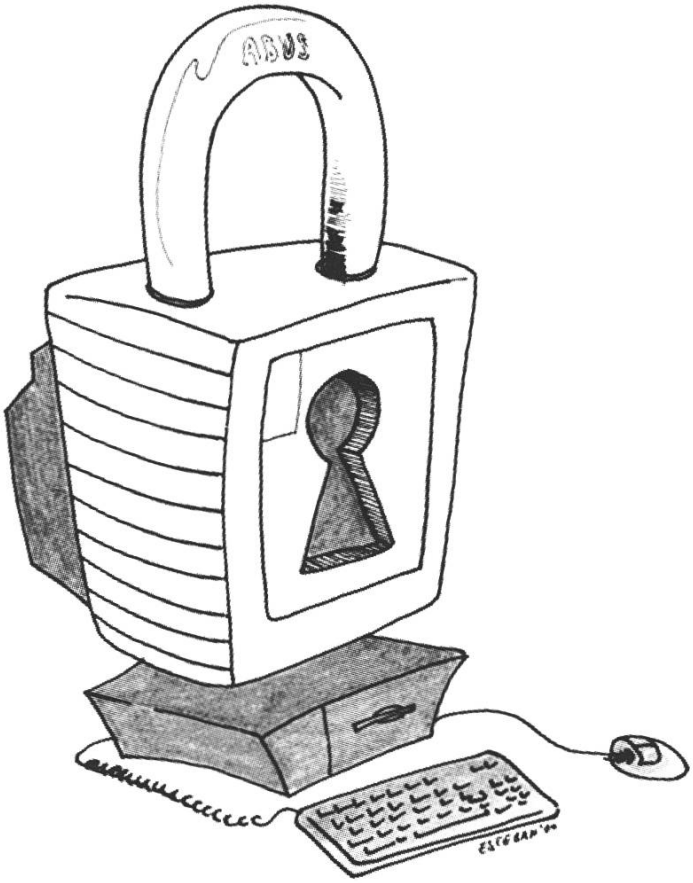
Welche TI-Fächer hast Du belegt, wirst Du belegen?
M. R.: Vertiefungen: Graph Theory, Randomized Algorithms, Approximationsalgorithmen, Erfüllbarkeit logischer Formeln, Abstract State Machines, Web-Algorithmen, Graphenalgorithmen.

Seminare: TI-Mittagsseminar, Krypto, Extremal Combinatorics.

Semesterarbeit: Approximation Algorithms for Matroids.

Wie beurteilst Du das Gebiet?
M. R.: Wie letztes Mal verweigere ich eine Aussage über die Schwierigkeit, denn das ist objektiv nicht beurteilbar. Was ich sehr schätze, ist das breite Fächerangebot und die vielen Seminarmöglichkeiten.

Von der Zeit, bzw. Arbeitsaufwand wollte ich nicht noch mehr Fächer nehmen, aber es gäbe noch viele Fächer, die mich reizen würden, die ich leider nicht nehmen konnte. Cool finde ich auch, dass man als Student Themen zu Gesicht bekommt, die zur Zeit die Forschung beschäftigt und die aktuell sind.



Somit habe ich eine Vorstellung davon bekommen habe, was man in TI nach dem Studium noch machen kann.

Du tendierst also Richtung Forschung?
M.R.: Ja das würde ich gern, entweder Forschung in der Industrie oder Doktorieren. Aber ich werde mir das in einem Jahr konkreter überlegen, dann gehe ich alle Möglichkeiten durch.

Was war ein Highlight in Deinem Studium und wieso?
M.R.: Als ich im Mittagsseminar das Paper „Primes Is In P" vorgestellt hatte ein paar Monate nach Veröffentlichung, fand ich das extrem aufregend, weil ich gerade eben in den Zeitungen davon gelesen hatte und dann dieses präsentierte.

Mir war nicht bewusst, wie viele sich dafür interessierten, bis ich meinen zahlreichen Zuhörern gegenüber stand.

Gewählt hatte ich dieses Paper weil ich Lust auf Zahlentheorie hatte und mich wirklich auf diesem Gebiet tief einarbeiten musste.

Noch eine letzte Frage: hat es viele Frauen in TI?
M.R.: Ich finde nicht, dass die Anzahl Frauen die Masterwahl beeinflussen sollte. Meistens bin ich mir der Anzahl auch nicht bewusst. Viel mehr empfinde ich als wichtig, wie viele ich kenne.

Bin ich in einem Raum, wo ich niemanden kenne, fühle ich mich anders als wenn ich fast alle kenne. Aber die Frauenquote hat keinen Einfluss darauf, wie ich mich in einem Raum fühle.

Aber um die Frage zu beantworten: ja es hat schon einige Frauen, was unter anderem daran liegt, dass die TI-Fächer auch von Mathematikerinnen besucht werden...

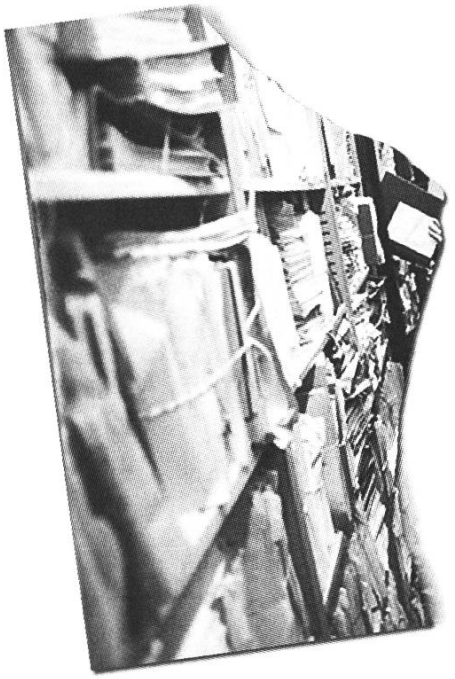
Vielen Dank für das Interview.
M.R.: Gern geschehen. Ich hoffe, das hat euch geholfen, sonst fragt jederzeit, wenn ihr noch was wissen wollt.

TI

E-Jigsaw: Rekonstruktion zerrissener Stasi-Unterlagen

MARTIN MARCINISZYN, KONSTANTINOS PANAGIOTOU, ANDREAS WEISSL
- PUZZLE FREAKS

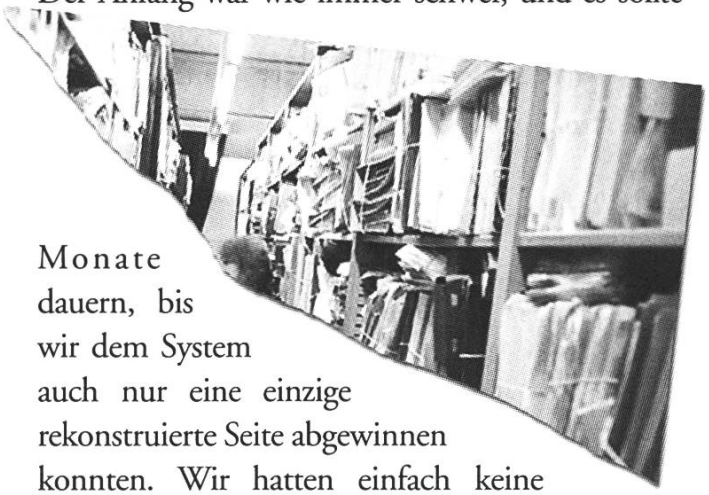
Als ich meine heutige Doktormutter Angelika Steger Anfang 2002 nach einem Thema für eine Diplomarbeit fragte, konnte ich nicht ahnen, worauf ich mich einliess. Schliesslich bezeichnet sie sich selbst gern als Theoretikerin. Ich war also darauf gefasst, das nächste halbe Jahr mit Papier, Bleistift und tonnenweise Büchern über Kombinatorik im stillen Kämmerlein zu verbringen. Klar gab es auch solche Themen, doch am Ende unseres Gespräches erfuhr ich von einem studentischen Projekt, das Frau Steger damals noch an der TU München durchführte. Es sei jedoch geheim, und ich müsse die Katze daher im Sack kaufen. Ich spielte mit, und das nächste Jahr sollte zum spannendsten meines Studiums werden.



Zur Vorgeschichte: Während der Wende in Deutschland hat die Stasi einen grossen Teil ihrer Akten vernichtet. Nachdem sämtliche verfügbaren Reisswölfe wegen der Papiermassen ihren Geist aufgegeben hatten, zerriss man die Akten einfach per Hand, bis Bürgerrechtsbewegungen der DDR diese Vernichtungsaktionen stoppen konnten. Man packte die Schnipsel in Säcke und brachte diese schließlich zur neu gegründeten Behörde der Bundesbeauftragten für die Unterlagen des Staatssicherheitsdienstes (BStU, «Birthler-Behörde»). Dort lagern sie heute eingemottet in etwa 17.000 Säcken à 20.000 Schnipsel. Seit Jahren bemüht man sich, diese Unterlagen von Hand wieder zusammenzusetzen, doch das ist eine nahezu endlose, frustrierende Aufgabe - ein ganzes Jahr braucht eine Person durchschnittlich pro Sack. In unserem Projekt wollten wir ein System bauen, das dieses gigantische Puzzle automatisch wieder zusammensetzen kann.

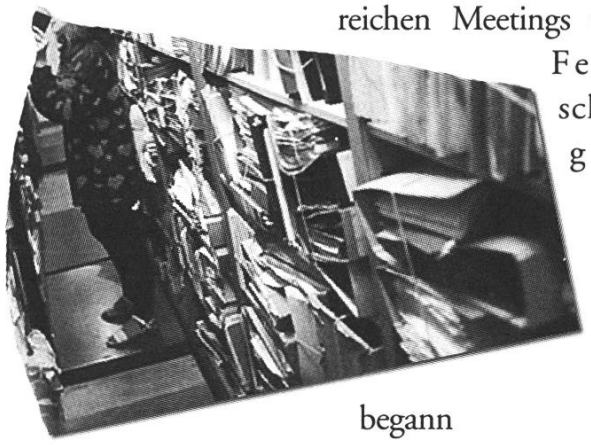
Angefangen haben wir mit einer bescheidenen Ausstattung. Ein gewöhnlicher Flachbettscanner und einige mittelmässige PCs mussten fürs erste ausreichen, denn es ist nicht ganz einfach, Geld für ein Projekt aufzutreiben, wenn man nicht verrät,

was man vorhat. Um dem politischen Anspruch des Projektes gerecht zu werden, zerrissen wir das Grundgesetz und scannten die Schnipsel in tagelanger Schichtarbeit auf unserer lahmen Kiste ein. Der Anfang war wie immer schwer, und es sollte



Monate dauern, bis wir dem System auch nur eine einzige rekonstruierte Seite abgewinnen konnten. Wir hatten einfach keine Ahnung, welche Dimensionen diese Aufgabe annehmen sollte, an der sich schon vorher einige Firmen die Finger verbrannt hatten.

Im Groben war der Ablauf der Rekonstruktion von Beginn an klar. Die Schnipsel werden gescannt, die Bilder von der Software analysiert und anschliessend mit passenden Gegenstücken zusammengefügt. Klingt ganz leicht, doch wie findet man das richtige Gegenstück, und welchen Aufwand darf man sich dabei erlauben? Nach zahlreichen Meetings und Fehlschlägen



begann sich endlich eine vernünftige Strategie dafür herauszukristallisieren. Bei der Bildanalyse konzentrierten wir uns hauptsächlich auf die geometrischen Eigenschaften der Schnipsel. Das System extrahiert deren Kontur und lokalisiert darauf die Eckpunkte, die sich zwischen verschiedenen Risskanten befinden. Diese werden vermessen und möglichst eindeutig durch Attribute wie Länge, Krümmung, Winkel zum Seitenrand usw. charakterisiert. Falls sich wenigstens auf einer Seite des Schnipsels Text befindet, wird es automatisch in die richtige Lage gedreht, und die Bilder beider Seiten werden in Korrelation zueinander gesetzt. Wir hofften durch die Auswahl geeigneter Merkmale, zusammengehörende Schnipsel einfach und effizient aus der Datenbank herausfischen zu können. Um das Projekt nicht völlig in die Bildverarbeitungs- und Datenbankecke abgleiten zu lassen, implementierten wir in Form eines speziell auf unsere Bedürfnisse zugeschnittenen Tries eine Indexstruktur, mit der sich die Merkmale zigtausender Risskanten flott miteinander vergleichen liessen. Auf keinen Fall möchte man alle möglichen Paarungen betrachten, denn diese Realisierung würde selbst auf Hochleistungsmaschinen Jahre für die Rekonstruktion benötigen. Es gibt zwar nur n^2 viele Kombinationen, doch bei n = 100.000 muss man schon viel Zeit mitbringen.

Nachdem wir zahlreiche Kombinationen von Objektmerkmalen getestet hatten, wurden unsere Hoffnungen endlich erfüllt. Für einen Grossteil der Schnipsel schaut das System nur einmal in den Trie, identifiziert wenige potentielle Gegenstücke und entscheidet sich nach eingehender Analyse, dem so genannten Hypothesentest, für die richtige Paarung. Es klebt diese zwei Schnipsel zusammen und wirft das neu entstandene wieder in den Rekonstruktionsprozess hinein, bis es mit anderen zu einer vollständigen Seite zusammengebaut wurde. Wie üblich sind es einige wenige Ausnahmen, die für schlechte Laune sorgen, da man ihretwegen viel Rechenzeit verbrät. Dies ist wohl

unvermeidbar, da kleine Stücke ohne Schrift und mit fast schnurgeraden Risskanten nun mal an fast jeder Stelle ins Puzzle passen. Wir haben viel Aufwand betrieben, um mit diesen Erscheinungen fertig zu werden. Das System beherrscht einen Mechanismus zur Aussortierung dieser Ausnahmefälle, und geht besonders sorgsam mit ihnen bei der Auswahl passender Gegenstücke um. Ausserdem verteilt es seine Aufgaben inzwischen via CORBA auf einen Linux-Cluster, so dass immer genügend Rechenkapazität vorhanden ist.

Als E-Jigsaw 20 Seiten in annehmbarer Zeit rekonstruieren konnte, stellten wir es der Birthler-Behörde vor. Dort war man davon sehr angetan und ermutigte uns zur Weiterarbeit. Kurze Zeit darauf wurde zum zweiten Mal eine Studie ausgeschrieben, in der die Machbarkeit der elektronischen Rekonstruktion der Stasi-Unterlagen untersucht werden sollte. Die vorangegangene Studie war ergebnislos eingestellt worden, da zum damaligen Zeitpunkt die Leistung der Computer nicht ausreichte. Die zweite Studie ging an das Fraunhofer Institut in Berlin, das ebenfalls ein System entwickelt hat und leider für kompetenter als ein studentisches Team gehalten wurde, die Frage der Realisierbarkeit und Finanzierung zu beantworten.

Als vorläufigen Abschluss des Projektes sollte E-Jigsaw seine Leistungsfähigkeit an einem Sack selbst zerrissener Unterlagen unter Beweis stellen. 1.700 Seiten wurden jeweils in 10 - 20 Teile gerissen. Insgesamt entstanden 20.709 Schnipsel, die mit freundlicher Unterstützung der Münchner Firma MFM innerhalb einer Woche mit einem Hochleistungsscanner abgelichtet wurden. Erwartungsgemäss traten haufenweise Bugs auf, als wir das System mit dieser Datenmenge konfrontierten, doch bald lief es wieder rund und rekonstruierte 88% der Seiten innerhalb von etwa einer Woche vollständig. Auf unserer Homepage [1] kann man sich jede einzelne davon ansehen.

Die Machbarkeitsstudie wurde im Herbst 2003 abgeschlossen, und als Ergebnis gab die Birthler-Behörde in ihren Pressemitteilungen bekannt, die Rekonstruktion und Grobsichtung der Unterlagen aus 600 Millionen Schnipseln sei innerhalb von fünf Jahren möglich. Dazu benötige die Behörde pro Haushaltsjahr eine einstellige Millionensumme zusätzlich. In anderen Presseberichten kursierte auch die Summe von 60 Millionen Euro. Konkrete Angaben über die Dauer und die Erfolgsquote einer allfälligen Rekonstruktion von einem Sack Schnipsel im Rahmen dieser Studie nennen weder die BStU noch das Fraunhofer-Institut, das eigens zu diesem Projekt einen Film produziert hat. Es ist völlig offen, ob der deutsche Bundestag die Gelder für dieses Projekt bewilligen wird.

Mit Kombinatorik habe ich mich in meiner Diplomarbeit nicht viel beschäftigt, ich durfte jedoch miterleben, wie ein visionäres Projekt Realität wird. In unserem 20-köpfigen Team mit wechselnder Besetzung hatten wir eine Menge Spass, und daraus sind enge Freundschaften hervorgegangen. Diese Erfahrung möchten wir gerne als Betreuer von Studienarbeiten weitergeben und schreiben hiermit einen Kasten Bier für den besten Vorschlag für das Projekt E-Jigsaw II aus.

Links:

[1]: www.e-jigsaw.de

TechTeam

Erfahrungsbericht: WinXP-64

THOMAS BRUDERER - NEU MIT ERWEITERTEM HORIZONT

Seit ein paar Monaten schon gibt es von AMD die neuen 64bit Prozessoren für den Heim Bereich. Da es bei mir sowieso einen neuen Rechner brauchte, hab ich mich dazu entschlossen denn AMD Athlon 64, damals den 3200+, mir auf mein Board zu holen. Damit dachte ich, bin ich zumindest mal für die unmittelbare Zukunft gewappnet.

Zum Verkaufsstart vom neuen Chip mit dem neuen x86-64 Befehlssatz gab es nur zwei Möglichkeiten, 32 Bit oder ein aktuelles SuSe 9.0. Windows hat zwar angekündigt Windows XP zu portieren, aber das scheint in Redmond etwas zu dauern. Seit ein paar Wochen nun aber gibt es eine Public Beta für WinXP-64. Und da dachte ich mir: lieber eine public beta als die Fähigkeiten des Rechners ganz brach liegen zu lassen.

Step 1: Installation

Das ganze funktioniert wie bei einer ganz normalen WinXP Installation und auch die Multibootmöglichkeit funktioniert tadellos. Zwei kleinere Hacken gab es dann aber leider doch noch.

1. SATA: Meine 200 GB SATA Platte wird von XP-64 nicht erkannt, der Treiber ist nicht vorhanden. Der Mitgelieferte 32bit Treiber des Plattenherstellers war natürlich auch total nutzlos. Diese Platte kann ich also momentan überhaupt nicht benutzen und für XP-64 aktualisierte Treiber wird es womöglich bei einem offiziellen Start schnell geben, im Moment aber hoffnungslos.
2. WinXP 64 trägt sich als Windows XP Professional ins Bootmenu ein. Wenn ihr also ein richtiges WinXP Professional habt, gibt es zwei gleich lautende Einträge. (In X:\boot.ini lässt sich das aber korrigieren)

Step 2: Erster Start:

Es fällt kaum ein Unterschied auf, zwar wird man aufmerksam gemacht das man eine Beta benutzt in Build 3790, aber sonst scheint sich nichts verändert zu haben. Netzwerkkarte funktioniert sofort, man kommt also flott ins Internet, Updates oder so gab es aber seit der public beta keine. Software läuft... Mozilla startet, auch sonstige Standardsoftware tut anstandslos seinen Dienst.

Step 3: System Steuerung

Microsoft Windows XP; 64Bit Edition, Version 2003, AMD Athlon @ 2.00 GHz, 1.00 GB of RAM.

Doch dann kam die Hardware: was im Moment wegen Fehlender Treiber (32 Bit Treiber können nicht benutzt werden) noch nicht funktioniert:

Logitech Webcam, OnBoard Gigabit Ethernet Controller (100mbit Controller wurde wie gesagt erkannt), Lexmark Drucker an USB, OnBoard Sound Controller, Raid Controller.

Step 4: Intensiv Test

Games:
Ich kann nicht mal sagen ob DirectX drauf ist. Soundkarte läuft ja gar nicht, und für die Radeon 9800 gibts noch keine offiziellen Treiber. Ich hab mal Counter Strike gestartet, und es läuft. Bei einem 2 GHz Rechner sogar flüssig, aber es ist trotzdem nur möglich mit Software Rendering zu Gamen ich denke dann lass ich den Test mit UT2k4Demo mal bleiben.

Rechenintensives:
Rendern von Videos, und sonst CPU belastendes konnte ich nur mit 32bit Software testen. Die scheint ohne Probleme in der 64bit Umgebung zu laufen. Weder schneller noch langsamer. Hier gilt es also auf neue Software zu warten.

Alte Programme:
16bit Software wird nicht mehr unterstützt. Und ich fand kein Programm, das ich in letzter Zeit gebraucht habe, das sich nicht starten liess unter WinXP-64. Aber natürlich wird es Software geben die jetzt nicht mehr laufen wird. Besonders DOS und Win 3.11 Programme werden wohl gar nicht mehr oder nur noch eingeschränkt laufen.

Zum experimentieren ist es schön und gut, aber mehr ist leider noch nicht möglich mit der Beta Version. Vor allem an den Treibern happert es noch, sonst scheint das OS aber reif für einen Start in die 64 Bit Welt.

Honigtöpfe

Oder wie die Blackhats, Script Kiddies und Möchtegerns kleben bleiben

MATHIAS PAYER - SCHLECKMAUL

Traditioneller Schutz von Servern geschieht defensiv. Firewalls, IDS (Intrusion Detection System), VPN, Verschlüsselungstechniken usw. werden benutzt um einen Rechner abzusichern. Von nun an liegt die Initiative bei einem Angreifer.

Falls dieser Angreifer in das System eindringen kann und dort sein Unwesen treibt, ist es im nachhinein ziemlich schwer, nachzuvollziehen von wo der Angriff kam und nach welchem Schema er statt gefunden hat, d.h. welcher Dienst wurde kompromittiert, welche Lücken wurden ausgenutzt usw. Eine weitere Schwierigkeit ist, die Daten zu retten, da man nicht weiss, was wo geändert wurde (in gewissem Sinne können Checksummen und Backups helfen, aber das ist Nebensache).

Wie allen klar sein wird, ist es sehr peinlich, wenn ein Server durch einen Einbruchsversuch vom Netz genommen werden muss und es zeugt nicht von einer guten Administration. Aber wie kann ein Administrator erkennen, was für Techniken eingesetzt werden, um in einen Server einzudringen? Wie können diese Angriffsmuster aufgezeichnet werden?

Hier kommen die Honigtöpfe, oder besser bekannt *Honeypots* ins Spiel. Bei diesen Systemen wird der Spiess umgedreht, Blackhats können beobachtet werden, welche Schritte sie unternehmen und wie sie sich einem System nähern. Honeypots

simulieren auf einem Hostrechner beliebig viele andere Systeme, mit laufenden Servern. Der Hostrechner protokolliert dann alle Zugriffe auf diese Gastrechner und kann somit auch mögliche Angriffe aufzeichnen.

Durch diese Aufzeichnungen erkennt man die Muster nach denen die Blackhats vorgehen. Neue Tools werden erkannt und z.B. auch Backdoors sind einfach zu erkennen und zu analysieren.

Diese Honeypots haben natürlich keine geschäftskritischen Daten auf ihren Systemen, liefern aber einem Angreifer trotzdem (Pseudo-) Informationen, so dass diese meist nicht erkennen, dass sie sich auf einem virtuellen Rechner befinden.

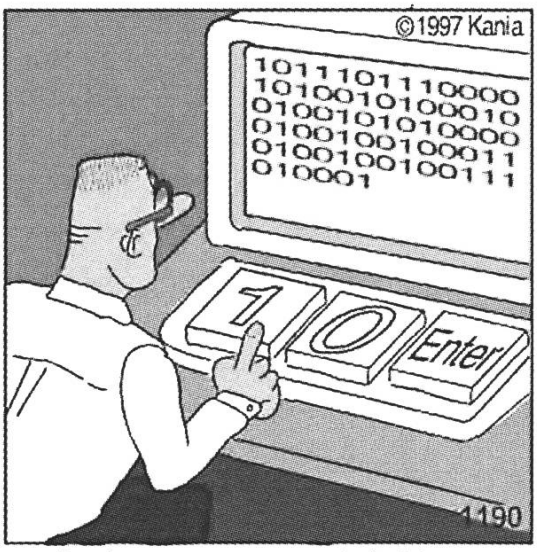
Im Normalfall legt man einen Honeypot hinter einer Firewall an. Sobald sich ein Angreifer am Rechner zu schaffen macht, erkennt man dies durch die Logfilter bei der Firewall und wird alarmiert. Ab dann kann man zuschauen, wie er sich am System zu schaffen macht (oder kläglich scheitert ;-)). Sobald er root-Zugriff hat und alle seine Backdoors usw. installiert hat, nimmt man den Honeypot vom Netz und startet ihn neu, setzt ihn neu auf (und schliesst die ausgenutzten Sicherheitslücken) und hängt ihn wieder ans Netz und wartet dann auf den Nächsten.

Damit die gehackte Box nicht für irgendwelche böswilligen Dinge (DDOS & Co) verwendet werden kann, werden einige zusätzliche Regeln bei der Firewall geschrieben, welche den ausgehenden und kommenden Datenverkehr auf dem Honeypot beschränken.

Nachdem man seine Honigtöpfe aufgesetzt hat muss man nur noch warten, bis der erste anbeisst. Irgendwie ist das wie Fischen, nur viel spannender und nerdiger :)

Links:

http://rootprompt.org/article.php3?article=210
http://project.honeynet.org
http://project.honeynet.org/papers/honeynet
http://www.honeyd.org
http://www.cti.umich.edu/u/provos/honeyd



Real programmers code in binary.

VIS-Aktiv

Bericht zur Kontaktparty 2004

SACHA - PRÄSIDENTSSCHAFTSKANDIDAT

Die diesjährige Kontaktparty ist vorbei und wahrscheinlich werden schon bald die ersten Studenten ihre Praktika und Stellen antreten, die sie aufgrund der dort gemachten Bekanntschaften erhalten haben. Eigentlich so, wie es jedes Jahr abläuft. Dennoch hat es dieses Mal zwei Premieren gegeben...

Zum einen ist da das Seminar der Firma MLP. Am Freitag vor der Kontaktparty hatten der VIS und MLP Studenten zu einem Seminar eingeladen, an welchem Tipps dazu gegeben wurden, wie die Studenten am besten auf die Firmen zugehen sollten. Das Interesse war grösser als wir erwartet hätten. Ich konnte mir anfangs nicht genau vorstellen, was MLP wohl vortragen würde, musste dann aber eingestehen, dass sie doch einige nützliche Hinweise gegeben hatten. Gerade den Studenten, die noch nie ein Bewerbungsgespräch geführt oder noch keinen Lebenslauf geschrieben haben, kann ich dieses Seminar sehr empfehlen. So werden wir uns darum bemühen, dass so ein Seminar auch im nächsten Jahr im Rahmen der Kontaktparty wieder stattfinden wird.

Eine weitere Neuerung war die Fernsehpräsenz am und um den Anlass, was wir der Firma google zu verdanken hatten. Google lässt sich ja, wie fast nicht zu überhören war, in Zürich nieder. Dies war auch der Grund, warum in der Woche zuvor der welsche Fernsehsender TSR bei uns im IFW war um einige Videoaufnahmen zu machen. Wir hatten eingewilligt, für Fernsehaufnahmen Schauspieler und Örtlichkeiten zur Verfügung zu stellen und erhofft, dass dafür die Kontaktparty im Bericht erwähnt würde. Leider war dem nicht so und wir hatten uns somit vergebens ins Zeug gelegt. So hätten wir es auch besser wissen sollen, als uns das SFDRS Team, das an der Kontaktparty selber Filmaufnahmen machte, zusicherte, sie würden unseren Event im Bericht erwähnen. Im Beitrag des Fernsehens, der abends in 10vor10 erschien, war wiederum von der Kontaktparty selber keine Rede. Sich darüber aufzuregen lohnt jedoch nicht, da wir nicht geplant hatten, im Fernsehen Werbung zu machen. Es wäre bloss eine willkommene Möglichkeit gewesen, die

Kontaktparty einem grösseren Publikum bekannt zu machen.

Um die Gunst der Studenten, für die wir diese Dienstleistung erbringen, müssen wir jedenfalls nicht buhlen. Wir sind zufrieden, dass auch dieses Jahr ca. 300 Studenten da waren, darunter auch einige von anderen Hochschulen. Auf der anderen Seite, bei den Firmen, ist nun endlich eine erfreuliche Wende eingetroffen. In den *goldenen Jahren* 2000 / 2001 waren so viele Firmen zur Kontaktparty angemeldet, dass die ganze Mensa an zwei Tagen gefüllt werden und das Begleitheft zur Kontaktparty schon fast als Index der schweizerischen Informatikbranche durchgehen konnte. In den zwei folgenden Jahren jedoch wurde die Zahl der Firmen zweimalig fast halbiert. Dieses Jahr wurde der Abwärtstrend aber endlich gestoppt. Nach 30 Firmen im letzen Jahr, dem absoluten Minimum, waren es diese Jahr schon wieder fast 40. Und will man den Antworten auf den Fragebogen zur Kontaktparty 2004 glauben, so sollten beinahe alle Firmen dieses Jahres im 2005 *sicher* oder zumindest *wahrscheinlich* wieder dabei sein. Generell war das Feedback sowohl der Studenten als auch der Firmenvertreter positiv. Bis auf wenige Kleinigkeiten, die wir nächstes Jahr besser machen wollen, war man mit allem zufrieden.

Was immer wieder erwähnt wird, und was einem auch auffällt, wenn man die Firmenvertreter und Studenten um 17 Uhr aus ihren Gesprächen aufschrecken lassen und sie regelrecht aus der Mensa vertreiben muss, ist die mit drei Stunden recht knapp bemessene Zeit. Oft reicht dies den Studenten nicht, um mit allen interessanten Firmen ins Gespräch zu kommen, da es auch immer wieder Wartezeiten gibt, bis andere Studenten die Firmenvertreter *freigeben*. Leider können wir gegen diesen Missstand nichts tun, da die Mensa ihre Öffnungszeiten nicht ändern kann. An einen anderen Ort möchten wir den Anlass auch nicht verlegen, da die zentrale Lage von allen Teilnehmern geschätzt wird. Wir wollen aber dafür sorgen, dass nächstes Jahr die Firmen über die ganze Mensa verteilt sind, um so die Platzverhältnisse weniger eng zu gestalten und damit mehr Studenten gleichzeitig mit den Firmenvertretern zusammensitzen können.

In diesem Sinne ist es auch ein Glück, dass

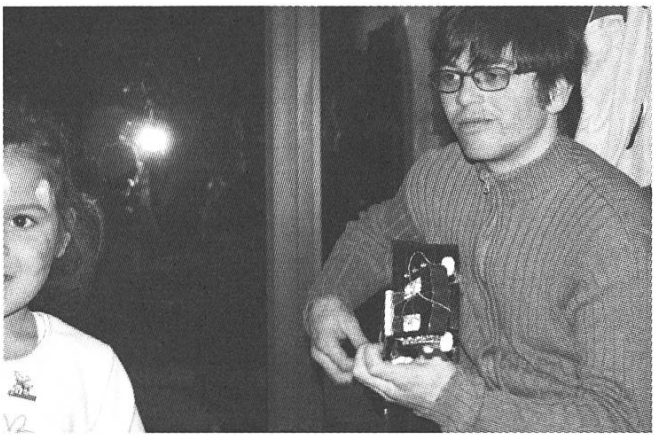
nicht mehr so viele Firmen teilnehmen, wie 3 Jahre zuvor. Auf diesen interessanten Aspekt der kleineren Firmenzahl machte mich ein Firmenvertreter in einem kurzen Gespräch aufmerksam. Er erwähnte, dass dieses Jahr die bessere Kontaktparty gewesen sei als im 2001, denn da wären so viele Firmen dagewesen, dass es manchen an Studenten gemangelt habe und sie lange Zeit gar keine Gespräche mit Studenten führen konnten. Er erwähnte ebenfalls, dass die Vorbereitung der Studenten dieses Jahr unerwartet gut gewesen sei. Dies hängt wohl damit zusammen, dass es heutzutage nicht mehr selbstverständlich ist, als Informatiker sofort eine Anstellung zu finden.

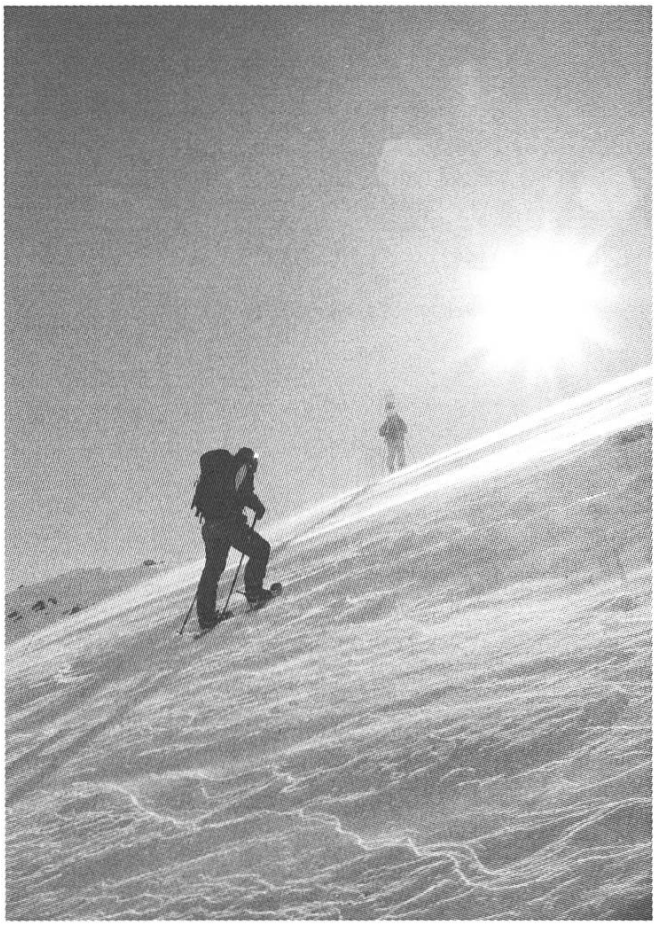
Abschliessend möchte ich allen Helfern für ihre Mitarbeit danken. Ich bin sehr zufrieden mit der Kontaktparty 2004 und erwarte gespannt die Entwicklungen für das nächste Jahr.

VIS-Aktiv

Snowdayz

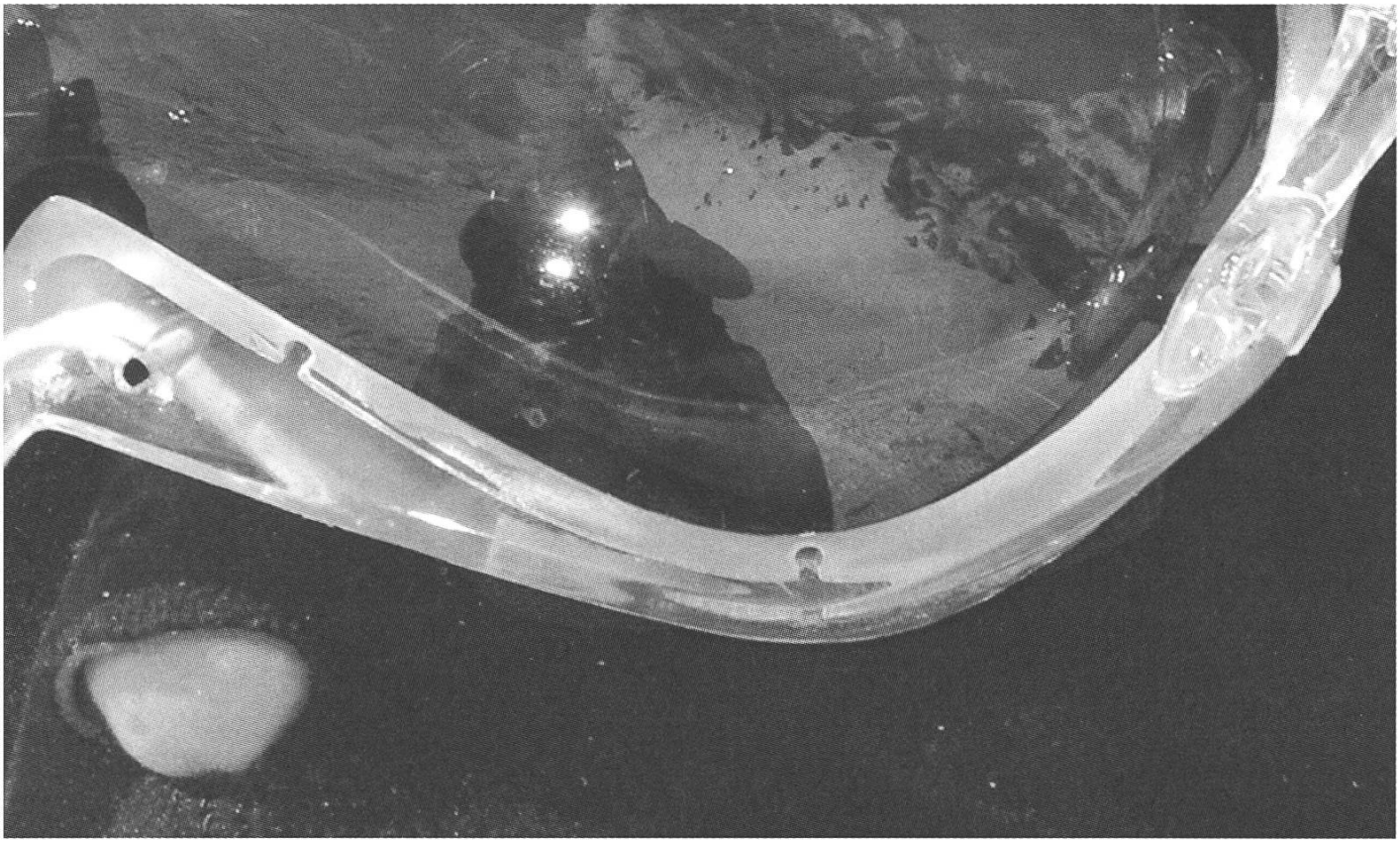
ALEX - SNOWDAYZ VETERAN

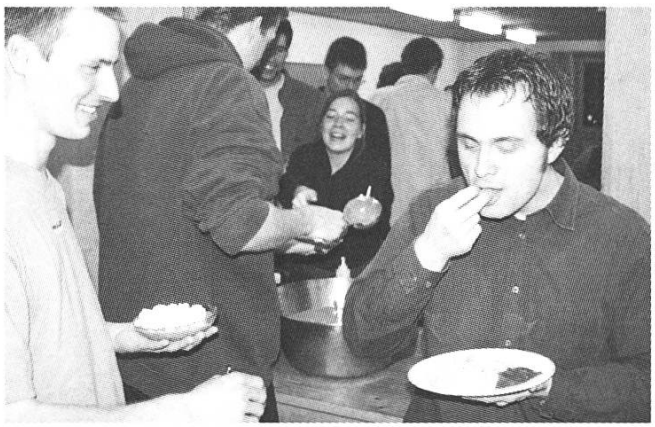


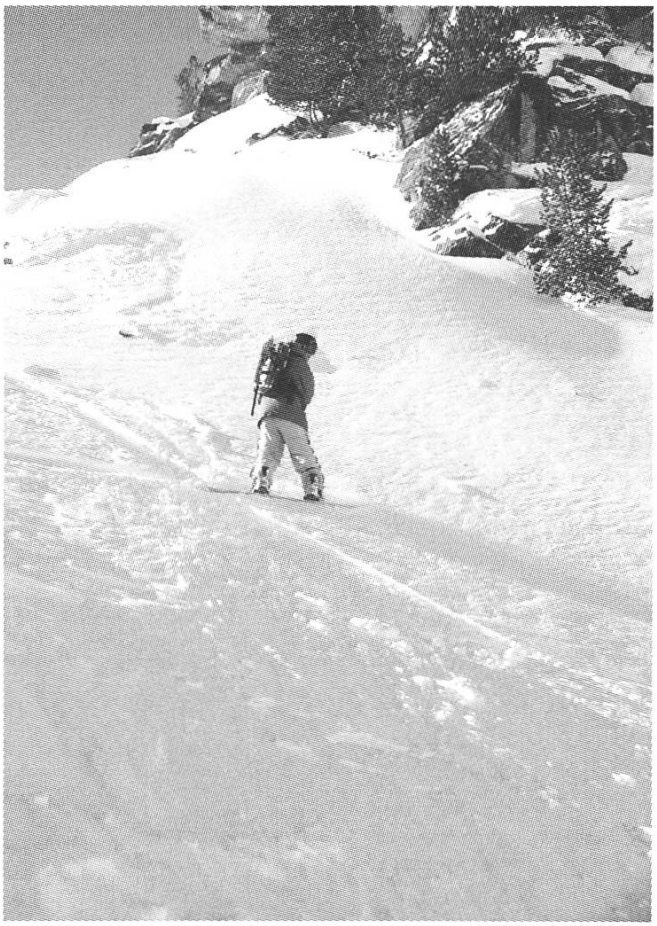


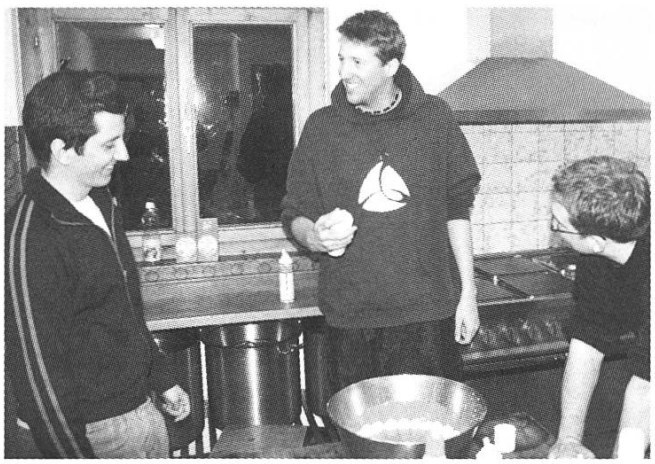
Zum ersten mal seit Enstehung der Snowdayz fand dieses mal ein richtiges Skilager statt. Eine Woche lang stand ein Lagerhaus in Tschierv, Val Müstair, den Teilnehmern ganz zur Verfügung. 60 VIS-Mitglieder nahmen die ersten drei Tage lang teil und 30 blieben die ganze Zeit über oben. Wir lassen die Bilder für sich selber sprechen...

Wir möchten im nächsten Jahr wieder ein einwöchiges Lager anbieten, wofür wir noch zwei bis drei Freiwillige suchen, die Lust haben, dafür ein Organisationskomitee zu bilden. Wer interessiert ist, kann eine Mail an vis@vis.ethz.ch schreiben oder an der Mitgliederversammlung erscheinen.









VIS-Aktiv

Videosessions im Sommer-semester

ANDREA - DEPARTEMENT FÜR VIDEOSESSION

Schon zum zwölften Mal gibts im bevorstehenden Semester Videosessions. Es bleibt alles wie gehabt: Ort ist jeweils IFW A 36, Zeit 19.00, und bis 17.00 lassen sich für 15.- im VIS-Büro Pizzen bestellen.

Abteilung für Gleichberechtigung:

7. April 2004: Whale Rider
präsentiert von der Frauenförderung
Neuseeland, 2002
Sprache: englisch mit deutschen Untertiteln

Pai Apirana kommt in der Zeit zur Welt, in der das Volk der Whangara die Geburt eines Erben ihres Stammvater Paikea erwartet. Pai besitzt die richtige Herkunft, und, wie sich herausstellt, offensichtlich auch das Talent, um die Nachfolge ihres Grossvaters als Stammesführer anzutreten. Was sie nicht hat, ist das richtige Geschlecht: als Frau ist sie traditionell von der Stammesführung ausgeschlossen.

Von Stammesgründer Paikea wird gesagt, dass er einst auf dem Rücken eines Wals von Hawaii nach Neuseeland kam. Trotz unzähliger vorausgehender Könnensbeweise ist es dann auch erst die Wiederbegegnung mit diesem Mythos, als eine Herde Wale an der Küste strandet und Pai deren Schicksal unter Einsatz ihres Lebens zu wenden vermag, die die Meinung des Grossvaters ändern kann.

Abteilung für Nostalgie:

28. April 2004: Tron
USA, 1982
Sprache: englisch mit deutschen Untertiteln

Dem Programmierer Kevin Flynn wird von seinem ehemaligen Mitarbeiter Dillinger der Programmcode für ein Spiel geklaut. Beim Versuch, sich Zugang zum Netzwerk seines ehemaligen Arbeitsgebers zu verschaffen, um diesen Diebstahl zu beweisen, wird Flynn vom „Master Control Program" des Systems, kurz MCP, mittels Laserkanone ins System „hineingebeamt" und wird vom User zum Programm. Die Welt der Programme wird vom MCP, einem aufgemotzten Schachprogramm, das Ambitionen hegt, die Welt zu beherrschen, tyrannisiert. In dieser Welt versucht Flynn zusammen mit einem ehemaligen Versicherungsprogramm, das MCP zu bekämpfen und es durch TRON, ebenfalls ein Programm, das auf Seite der User steht, zu ersetzen, zwecks Rettung der Computer- sowie der realen Welt.

Natürlich mag Tron mit den graphischen Ansprüchen an aktuelle Filme nicht mithalten, aber hat doch viel Würdigung verdient als ein Film, der

seinerzeit in Sachen computeranimierte Filme neue Massstäbe gesetzt hat. Tron hat vermutlich die Vorstellungen über virtuelle Realitäten und künstliche Intelligenzen nachhaltig geprägt und ist alleine schon aus Nostalgiegründen sehenswert!

Abteilung für Bill Murray:

12. Mai 2004: Groundhog Day
USA 1993. 101 Minuten.
Sprache: englisch mit englischen Untertiteln

Phil Connors (Bill Murray, Lost In Translation) ist ein sarkastischer Wettermann bei einem kleinen Lokalsender in den Vereinigten Staaten. Punxsutawney Phil ist ein Murmeltier, dem nachgesagt wird, dass es voraussehen kann, ob der Winter bald endet oder aber noch weiter andauert. Die beiden treffen sich jedes Jahr am 2. Februar, am Groundhog Day, zur Liveübertragung des tierischen Wetterberichtes. Nur dieses Jahr endet Groundhog Day nicht und überlässt das Feld dem 3. Februar. Dieses Jahr ist Phil Connors gezwungen seinen schlimmsten Tag wieder und wieder zu erleben. Zusammen mit seiner Produzentin Rita (Andie McDowell, Four Weddings And A Funeral) und seinem Kameramann Larry (Chris Elliott, There's Something About Mary) sitzt er im provinziellen Pennsylvania fest, doch nur er scheint die tägliche Endlosschleife zu bemerken...
Harold Ramis (Analyze This) Film über einen frustrierten Menschen, der verucht sein Leben ins Positive zu wenden, ist schwer in ein Genre zu verweisen. Aspekte der Komik und Romantik mischen sich mit tragischen Elementen, aus Fantasy wird Phil-osophie.

Abteilung für Demokratie:

9. Juni 2004: Wunschfilm
Wegen relativ abenteuerlichen Liefer-Routen für „Serial Lover" findet in diesem Semester die Demokratie-Videosession nicht wie üblich am Semesterende statt, sondern mittendrin. Alles andere bleibt (fast) wie gehabt: Sendet uns Vorschläge für Filme auf videosessions@vis.ethz.ch! Aus allen vorgeschlagenen Filmen werden wir einige auswählen, die dann auf der VIS-Webseite zur Wahl stehen - der Meistgewählte wird am neunten Juli gezeigt. Vorschläge könnt ihr ab sofort abschicken, wann die Abstimmung beginnt und alles weitere folgt per Mail.

Abteilung für schwarzen Humor:

30. Juni 2004: Serial Lover
Frankreich, 1998
Sprache: voraussichtlich französisch mit englischen Untertiteln

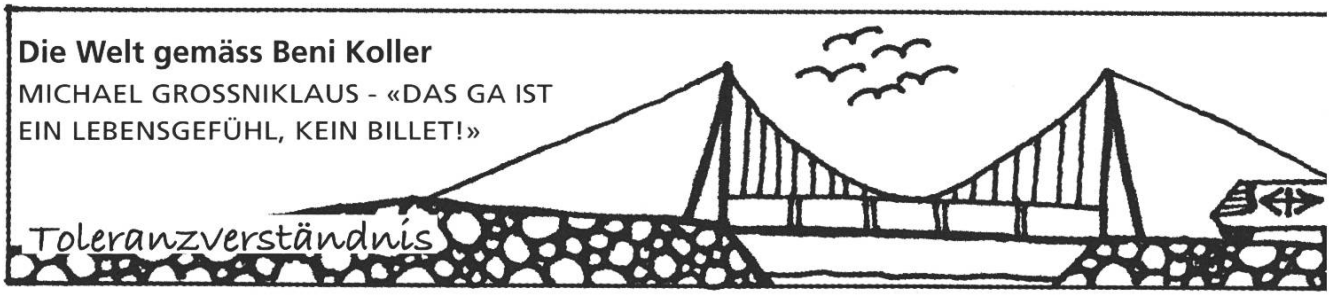
Die Hauptfigur dieses Filmes hört auf den Namen Claire und beschliesst anlässlich ihres bevorstehenden 35. Geburtstages, ihr Single-Leben aufzugeben und zu heiraten. Unklar ist jedoch noch, welcher ihrer drei Liebhaber der Glückliche sein soll, und um dieses Problem aus der Welt zu schaffen, lädt Claire am Vorabend ihres Geburtstags alle drei zum vermeintlichen tête-à-tête ein.

Besagtes Problem wird am Nachtessen zu fünft auf relativ unerwartete Weise einfacher, als Liebhaber Nummer eins in der Küche einen fatalen Unfall mit einem Messer hat. Auch Liebhaber Nummer zwei und drei erreilt bald ein ähnliches Schicksal, des weiteren mischen sich auch noch die Polizei, Claires Schwester mit einer Überraschungsparty, zwei Einbrecher und ein weiteres Messer ein. Das alles ergibt eine Mischung mit viel schwarzem Humor, die auf www.filmtext.com als „Tarantino meets Almodovar meets Splatter goes France" beschrieben wird.

Gewinne eine Pizza --> Seite 46

Die Welt gemäss Beni Koller

MICHAEL GROSSNIKLAUS - «DAS GA IST EIN LEBENSGEFÜHL, KEIN BILLET!»



Beni Koller sitzt im Zug der ihn nach hause nach Zürich bringt. Er fährt gerne Zug, denn er schätzt die tolerante Atmosphäre, die in den Zügen der Schweizerischen Bundesbahnen herrscht. Der immer neue Mix von Leuten mit verschiedensten Hintergründen, fasziniert ihn auf jeder Reise. Wäre anstatt der Zauberformel, der Verwaltungsrat der SBB im Bundesrat, so glaubt Beni, wäre Kiffen und die gleichgeschlechtliche Ehe schon lange legal. Diese tolerante Haltung der SBB wirkt sich auch auf die Menschen aus, die mit ihr fahren. Häufig sprechen sie im Zug offener über ihre Sorgen und Wünsche und jeder der sich in Hörweite befindet, kann daran teilhaben. Auf Pendlerzügen bilden sich sogar richtige Gemeinschaften, die sich jeden Morgen wieder im gleichen Wagen treffen, sodass mit der Zeit alle Wagen ihren eigenen Charakter entwickeln.

Lebhaft kann sich Beni Koller noch an die Geschichte mit der Frau erinnern, die im vollen Pendlerzug darauf bestanden hat, dass auch ihr Hund einen Platz bezahlt habe und ihr deshalb der Sitz gegenüber auch zustehe. Oder jene Fahrt, als ein junger Mann im Nachtzug darauf bestand, dass man ihn nicht mit 80 Franken büssen könne, weil er keinen Zuschlag gelöst hatte. Diese Busse, so argumentierte er, sei nur anwendbar, falls ein Passagier ohne gültigen Fahrausweis erwischt werde und ein solchen hatte er als Besitzer eines Generalabonnements. Für Beni Koller ist deshalb im Zug immer für Unterhaltung gesorgt und es wird ihm auch nach jahrelangem Befahren der gleichen Strecke nicht langweilig. Die Landschaft mag jeden Tag die gleiche sein, die Gesellschaft im Zug ist es nicht.

Natürlich sind solche Verhältnisse nicht jedermanns Sache, das weiss auch Beni Koller. Als toleranter Mensch akzeptiert er auch, dass es Fahrgäste gibt, die lieber in Ruhe die Fahrt geniessen oder

die Zeit zum arbeiten nutzen möchten. Für diese Leute gibt es ja auch Ruhewagen, in denen nicht geredet, telefoniert und Musik gehört werden darf. Beni Koller aber bringt so leicht nichts aus der Ruhe. Seine Toleranz, für die er sich oftmals rühmt, geht soweit, dass er auch mit drei schreienden Kindern im Abteil, einem fremden Hund auf dem Schoss und einem alten Herrn, der ihm Räubergeschichten aus dem Zweiten Weltkrieg erzählt, gelassen reisen kann. Auch der mit Mohawk gestylte SBB-Lehrling, der kürzlich eine Wandergruppe von pensionierten Senioren in Aufregung versetzte, bringt ihn nicht aus dem Gleichgewicht. Man muss, so findet Beni, lernen, andere Leute und ihre Meinungen zu akzeptieren oder eben zu tolerieren.
Klar, dass auch die Toleranz ihre Grenzen hat. Beni würde zum Beispiel Gewalt oder Diskriminierung nie tolerieren. Gegen solche Dinge, so ist er überzeugt, muss man sich mit allem Nachdruck wehren. Und in Fällen, wo die Toleranz abhängig von der Stärke der Nerven ist, gibt es ja auch die Möglichkeit des Ausweichens. So zum Beispiel als ein junger Herr eines Morgens seinen Orangensaft über Benis Rucksack ausleert und nicht mehr aufhören kann, sich zu entschuldigen. Diskret begibt sich Beni in einen anderen Wagen, wo er seinen Kopfhörer gemütlich wieder aufsetzt und weiter döst. Nach einiger Zeit spürt er ein Zupfen an seinem Ärmel. Es ist sein Abteilsgenosse, der ihn freundlich darauf aufmerksam macht, dass sein Natel schon etliche Male geklingelt hat. Gleichzeitig bittet er Beni höflich, seine Musik auszumachen, damit er die anderen Leute im Ruhewagen nicht stört. Erbost über diese Kleinlichkeit fügt sich Beni seinen Bitten. Das Einzige, was Beni Koller wirklich nicht tolerieren kann, sind intolerante Menschen.

Alles was Recht ist ...

Somebody's knocking at your door...

DANIEL MARKWALDER - ANKLOPFER

Wie (l)egal ist es, bei jemandem ein bisschen an die virtuelle Tür zu klopfen? Ist ein Portscan – also der Versuch mit einem Port eines anderen Rechners Kontakt aufzunehmen – überhaupt ein Anklopfen? Oder vielleicht eher erst ein Anschauen? Die Diskussion darüber führt in gewissen Foren regelmässig zu erbitterten Glaubenskriegen... Hier kommen meine fünf Cents zum Thema.

Neuer Wein in alten Schläuchen

Gesetze hinken der (Computer-) Zeit zwangsläufig hinterher. Das Strafrecht beispielsweise trat 1942 in Kraft! Natürlich hat es seither diverse Änderungen und Anpassungen erfahren. Bis aber eine neue Norm durchs Parlament und - noch schlimmer - eine computerspezifische Norm durch die Köpfe der Parlamentarier ist, vergehen schnell mal ein paar Jährchen...

Man versucht deshalb oft, eine alte Vorschrift auf eine neue Tat anzuwenden; neuen Wein in alte Schläuche zu füllen. Oder etwas juristischer formuliert: Einen neuen Tatbestand unter eine geltende Norm zu subsumieren.

Portscan = ?

Mit was für einer Handlung ist ein Portscan im realen Leben vergleichbar? Da gibt es diverse kreative Vorschläge:

- Man geht zu einem Haus (=einer IP-Nummer) und drückt bei allen Türen die Klinke runter um festzustellen, welche Türen offen sind. (Alternativvorschlag: Man schliesst das Schloss auf und wieder zu).
- Man geht einer Mauer entlang und tastet ab, wo es in der Mauer überhaupt Türen hat (ohne Klinkendrücken).
- Man schleicht auf einem Parkplatz rum und schaut durch die Fenster, welche Autos unverschlossen sind.
- Man betrachtet eine Strasse auf der Suche nach offenen Läden.

Für und gegen das eine oder andere Beispiel gibt es durchaus Argumente. Tatsache ist, dass man einen Portscan nicht so ohne weiteres aufs Real-Life übertragen kann: Im virtuellen Leben ist das Sehen nicht so unproblematisch, denn im Netz sieht man mit Päckchen. Ein Päckchen ist nur schon deshalb nicht 1:1 mit einem Blick zu vergleichen, weil Päckchen Verkehr generieren...

Eventuell ist es aber gar nicht so wichtig, wie der Vergleich zum Real-Life ist? Einige Leute behaupten, ein Portscan sollte schon deshalb illegal sein, weil es schlicht keine lauteren Motive für dessen Anwendung gebe!

Nulla poena sine lege

Wer argumentiert, dass ein Portscan verboten ist/sein sollte, weil keine ehrlichen Motive ersichtlich seien, sagt letzlich: Alles wofür es nicht gute Gründe gibt, soll verboten sein. Grundsätzlich verbieten und ausnahmsweise erlauben! Die Idee des Strafrechts ist aber (zum Glück!) genau die Gegenteilige: Alles, was nicht ausdrücklich verboten ist, ist erlaubt. Keine Strafe ohne Gesetz! Artikel 1 StGB. Punkt.

Der zweite Einwand ist, dass es tatsächlich legitime Gründe für einen Portscan geben kann (die laufenden Dienste erfahren)...

Portscans unter Strafe zu stellen, resp. als solche unter einen bestehenden Artikel zu subsumieren würde das Ziel völlig verfehlen. Es wäre dasselbe, wie wenn man beispielsweise das Schneiden unter Strafe stellen möchte, ohne gross darüber nachzudenken, ob sich das Schneiden auf eine Tomate oder eine Halsschlagader bezieht...

Zurück zum Thema: Einen Rechner mit „ping" ansprechen dürfen gehört zu den Grundspielregeln des Internets, und es käme wohl auch niemand auf die Idee, dies zu verbieten. Aber schon ein harmloses „ping" kann verheerende Auswirkungen haben, wenn man beispielsweise eine fette Leitung hat und mit „ping –f" einen Rechner mit langsamerer Leitung in die Knie zwingt... Es kommt immer auf den Zusammenhang und die Motivation des „Täters" an!

Auf den Zusammenhang kommt's an

Dasselbe muss auch für Portscans gelten: Es darf nur darauf ankommen, in welchem Zusammenhang, wie und mit welcher Absicht er gemacht wird! Wenn jemand einen Server lahm legen will und mit „nmap" potentielle Einfallstore ausmacht, so *könnte* damit die Grenze der straflosen Vorbereitungshandlung zum strafbaren Versuch überschritten sein. Wen's interessiert, die Grenze ist gemäss Bundesgericht wie folgt definiert:

„Zur Ausführung (also zum strafbaren Versuch) gehört schon jede Tätigkeit, die nach dem Plan, den sich der Täter gemacht hat, auf dem Weg zum Erfolg den letzten entscheidenden Schritt darstellt, von dem es in der Regel kein Zurück mehr gibt, es sei denn wegen äusserer Umstände, die eine Weiterverfolgung der Absicht erschweren oder verunmöglichen" (z.B. in BGE 118 IV 396).

Im Real-Life gilt Auskundschaften des Hauses noch als Vorbereitungshandlung; der Versuch beginnt in etwa mit dem Aufbrechen, resp. sich zu schaffen machen an der Türe...

Ein Portscan dürfte wohl eher nicht als Aufbrechen der Türe gelten und noch weniger als der „letzte entscheidende Schritt, von dem es in der Regel kein Zurück mehr gibt"!

Aber nochmals: Es kommt auf die Vorstellung des Täters an. Wenn er einbrechen will und den Portscan als seinen ersten Schritt betrachtet, könnte es unter Umständen der Beginn eines Versuches sein. Ein bluttes „nmap" einfach so zur Freude ist dagegen allemal straflos.

Zivilrecht

Nun gibt es neben dem Strafrecht bekanntlich unter anderem auch das Zivilrecht. Es ist sehr gut möglich,

dass etwas zwar strafrechtlich nicht unter Strafe steht, aber trotzdem zivilrechtliche Folgen hat. Ein Beispiel dafür ist die fahrlässige Sachbeschädigung, die nicht unter Strafe steht, aber natürlich in aller Regel eine Schadenersatzpflicht auslöst.

Schadenersatz durch Portscan?

Es ist denkbar, dass einem Server mein Portscan sauer aufstösst und ein Schaden entsteht. Ein solcher Schaden kann beispielsweise in Arbeitszeit bestehen, die entsteht, um hysterische User zu beruhigen, deren Personal-Firewall Alarm geschlagen hat...

Um schadenersatzpflichtig nach Art. 41 OR zu werden, braucht es neben dem Schaden (und dem Verschulden und der Widerrechtlichkeit) einen adäquaten Kausalzusammenhang zwischen dem Verschulden und dem Schaden. Adäquatkausal ist nach der Formel des Bundesgerichts eine Tat die *„nach allgemeiner Lebenserfahrung und dem allgemeinen Lauf der Dinge dazu geneigt ist, einen Schaden in der Art des eingetretenen hervorzurufen"*. Herrlich präzise Formel! ;-) Jedenfalls geht es um ein Abwägen, ob der Verursacher mit einem solchen Schaden hätte rechnen müssen oder nicht.

Wenn der Schaden wie oben beschrieben in Arbeitszeit besteht, wird man diese Frage wohl bejahen müssen (zumal das Bundesgericht seine „Formel" recht extensiv auslegt). Wenn er dagegen in einem Serverabsturz besteht, ist sie zu verneinen. Dies ist nun wirklich nicht mehr der allgemeine Lauf der Dinge!

Vertrag mit Provider

Bleibt noch darauf hinzuweisen, dass in den AGBs mancher Internet-Provider Portscans ausdrücklich untersagt werden. Wer über einen solchen Provider ins Netz geht, hat die von ihm zugestimmten Regeln einzuhalten...

Und last but not least noch die Anmerkung, dass es nicht unbedingt nett ist, jemanden mit Portscans „abzuklopfen" (Stichwort Netiquette).

Fazit:

Strafrechtlich sollte es mit einem Portscan keine Probleme geben, es sei denn, man habe „gröberes" vor (aber dann ist der Portscan wohl nicht mehr das Problem...). Etwas wahrscheinlicher könnten zivilrechtliche Probleme oder Zoff mit dem Provider sein.

Für solche Fälle rate ich mit Ghandi: *„Wenn Du im Recht bist, kannst Du es Dir leisten, die Ruhe zu bewahren, und wenn Du im Unrecht bist, kannst Du Dir nicht leisten, sie zu verlieren."*

Links:

statt vieler: http://groups.google.ch
http://www.admin.ch/ch/d/sr/c311_0.html - StGB
http://www.admin.ch/ch/d/sr/c220.html - OR

Beispiel (intern):

```
> nmap 192.168.0.30
Starting nmap V.3.00 ( www.insecure.org/nmap/ )
Interesting ports on (192.168.0.30):
(The 1595 ports scanned but not shown below are in state: closed)
Port       State       Service
21/tcp     open        ftp
22/tcp     open        ssh
23/tcp     open        telnet
111/tcp    open        sunrpc
139/tcp    open        netbios-ssn
6000/tcp               open        X11

nmap run completed – 1 IP address (1 host up) scanned in 2 seconds
```

Werden Sie Junior-Berater/-in für Technologie bei Accenture.

_ Accenture ist ein weltweit tätiger Management- und Technologiedienstleister mit mehr als 86.000 Mitarbeitern in 48 Ländern. Mit ausgewiesenem Branchenwissen und umfassender Erfahrung im Beratungs- und Outsourcing-Geschäft arbeiten wir zusammen mit unseren Kunden daran, Innovationen umzusetzen.

_ Wir bieten Ihnen das richtige Umfeld, Ihre Fähigkeiten unter Beweis zu stellen und an herausfordernden Aufgaben zu wachsen. Arbeiten Sie gemeinsam mit unseren Kunden daran, Ideen in Resultate zu verwandeln. Bewerben Sie sich bei uns als Junior-Berater/-in für Technologie.

_ Ihre Aufgaben:
- umfassende und individuelle Beratung unserer Kunden in allen IT-Themen
- Entwicklung und Programmierung von technisch- oder SAP-orientierten Geschäftslösungen in Grossprojekten
- Realisierung innovativer IT-Architekturen und -Anwendungen von der Analyse über Design bis zum Test oder Entwicklung und Implementierung von anspruchsvollen Konzepten und Lösungen im SAP-Umfeld

_ Wir suchen Mitdenker wie Sie!

_ Sie besitzen:
- ein überdurchschnittlich abgeschlossenes Hochschulstudium (Uni, FH)
- fundierte IT-Kenntnisse oder erste SAP-Kenntnisse
- qualifizierte praktische Erfahrungen in den Bereichen Anwendungsentwicklung, Internet, IT-Architekturen, Infrastrukturaufbau, Microsoft-architekturen, EAI, Datawarehousing oder SAP
- Persönlichkeit und Kommunikationsstärke
- ausgeprägte Teamfähigkeit und hohe Belastbarkeit
- Flexibilität und Engagement
- hohe Kundenorientierung
- sehr gute Englischkenntnisse

Mobilität sowie Freude an Reisen und internationalem Teamwork runden Ihr Profil ab.

Wir entwickeln Lösungen gemeinsam mit unseren Kunden aus folgenden Bereichen:

Telekommunikation, Elektronik und High Tech, Medien und Unterhaltung, Banken und Versicherungen, Kapitalmärkte, öffentliche Verwaltungen, Regierungen und regierungsnahe Organisationen, Automobilindustrie, Fluggesellschaften, Fracht und Logistik, Handel, Investitionsgüter, Konsumgüter, Personen- und Güterverkehr, Pharmazie, Medizin und Gesundheitswesen sowie Touristik, Energieversorgung, chemische Industrie, Öl- und Grundstoffindustrie.

Interessiert? Dann machen Sie den ersten Schritt in Ihre berufliche Zukunft mit Accenture. Bewerben Sie sich!

Accenture
Recruiting
Monika Dammert
Fraumünsterstrasse 16
CH-8001 Zürich
Tel.: +41 1 219 98 89
recruiting.switzerland@accenture.com

Weitere Informationen unter

www.entdecke-accenture.com

accenture
High performance. Delivered.

• Beratung • Technologie • Outsourcing

CREDIT SUISSE

Eine Karriere braucht eine Vision. Und die Wahl des richtigen Partners.

Wir suchen Nachwuchstalente, die anspruchsvolle Aufgaben mit viel Enthusiasmus und Engagement angehen und ihre Karriere durch ein hohes Mass an Selbstverantwortung vorantreiben möchten. Mit einem überdurchschnittlichen Studienabschluss, Ihrer überzeugenden Persönlichkeit und ausgeprägten sozialen Kompetenzen bringen Sie die besten Voraussetzungen für Ihre Karriere bei uns mit. Attraktive Career Start Opportunities bei der CREDIT SUISSE, der CREDIT SUISSE FIRST BOSTON und der CREDIT SUISSE ASSET MANAGEMENT erwarten Sie. Sind wir Partner?

www.credit-suisse.com/careerstart

Liebe Studierende

Auch schon in der Informatik-Bibliothek gestanden und gesucht? Lost in hyperspace kann man zwar schlecht sagen inmitten der Regale, trotzdem sind bibliographische Informationen heute oft erst nach einer erfolgreichen Suchanfrage zu greifen. Dazu braucht man zuerst zu wissen, WO gesucht werden soll, und dann WIE das geschieht. Und zuletzt spielt noch eine Rolle, WER überhaupt ausleihen darf.

Wir bieten eine

Einführung in die Bibliothek und den NEBIS-Katalog

Mittwoch, 14. April 04, 18.30 – 19.30 h
Dienstag, 4. Mai 04, 18.30 – 19.30 h

an, um das Zurechtfinden in der Leihbücherwelt zu erleichtern. Folgende Punkte sollen angesprochen werden:

- Was ist wo in der Informatik-Bibliothek? Aufbau, Struktur
- Wie findet man ein Buch (Lehrbuch zur Vorlesung, Fachbuch), wie einen Zeitschriftenartikel?
- Wie funktioniert der NEBIS-Katalog?
- Welche Zusatzinfos findet man via ETH-Netz? (Neuerwerbungen, e-Texte, elektronischer Dokulieferdienst)
- Elektronische Dokumentenbestellung von anderen Anbietern
- Anschaffungsvorschläge

Interessierte schicken bitte ein Email an bibliothek@inf.ethz.ch
mit dem Vermerk „Anmeldung zur Einführung am xx.y.04 "
und dem Vornamen, Namen, der Studienrichtung und des Studiensemesters.

Wir freuen uns auf Euren Besuch
das Bibliotheksteam, Floris Tschurr

vis-à-vis

Alex, abtretender VIS-Präsident

ANONYMER FEIGLING

Beschreib uns einen typischen Tag

Für mich gibt es ungefähr drei verschiedene Tage. Der eine könnte man Sonntag nennen, was aber nicht heisst, dass er einmal in der Woche vorkommt. Ich wache immer (relativ) früh auf. Seit dem zweiten Vordiplom bin ich nicht mehr fähig, auszuschlafen. Ich stehe also auf und stelle alles auf den Tisch, was ich in der Küche finde. Ich frühstücke mich ins Koma. Dann kann ich wieder schlafen. Ein paar Stunden später stehe ich auf und wiederhole das ganze mit dem Mitagessen.

Ein anderer Tag wäre eine Art Samstag. Entweder ich bin in den Ferien, also irgendwo am Meer, oder ich bin mit dem Velo auf einem (Uetli-)Berg unterwegs, fahre Rollbrett oder Snowboard. Am Abend gehe ich dann häufig aus.

Zu guter letzt gibt es noch Mittwoche. Die verbringe ich von Anfang an und konsequent im RZ/IFW. Ich mag die Atmosphäre da und ich liebe es zu arbeiten (z.B. programmieren, schreiben, Papers lesen).

Was ist das Unglaublichste, was Dir widerfahren ist?

Dass ich jetzt hier bin und das tue was ich tue. Ich weiss nicht, wieso ich vor einer Woche nicht beim Escher-Wyss-Platz von einem Lastwagen überfahren wurde. Das war dermassen knapp und lag extrem nicht in meiner Macht. Ueberhaupt, mein Lebensverlauf. Zum Beispiel als ich zwei Wochen vor der Aufnahmeprüfung ins Gymnasium von einem Freund erfuhr, dass in einem anderen Schulhaus fünf-Tage-Woche ist. Ich habe mich umgemeldet, er hat die Prüfung nicht bestanden und so habe ich halt statt der Neusprach- die Wirtschaftsmatur gemacht. Und fünf-Tage-Woche gab es doch nicht. Jetzt ist mir total unvorstellbar, dass ich meine Freunde, die ich dort kennengelernt habe, nicht hätte.

Mein ganzes Leben scheint von Zufällen bestimmt zu sein: Ich habe am D-INFK begonnen, weil ich wärend dem Psychologiegrundstudium(?) zufällig eine Hilfsassistenz für HTML/JavaScript(??!) bekommen hatte, ich bin in den VIS gekommen, weil ich den Samichlaus

gefragt hatte, ob es in jenem Jahr einen Skitag gäbe usw. Ich habe aufgegeben, mein Leben in diesem Sinne in eine Richtung lenken zu wollen. Ich konzentriere mich darauf, ein guter Mensch zu sein und Sachen zu tun, bei denen ich alles um mich herum vergesse.

Was sind für Dich die grössten Fortschritte/ Errungenschaften in der Geschichte der Informatik?

Ja, also, so ganz offensichtlich natürlich die weltweite Vernetzung mit der (potentiellen) Demokratisierung vieler Lebensbereiche. Das ist aber eine etwas abgedroschene Aussage, nicht? Subtiler und meines Erachtens von Anfang an verkannt sind: copy & paste, undo und printscreen. Das sind Dinge, die einem immer wieder auf ganz simple Art aus der tiefsten Patsche helfen können. Diese Funktionen verändern die Arbeitsweise auf sehr grundlegende Art und deren Fehlen (z.B. im realen Leben) kann sehr frustrierend sein (eben weil es so einfach wäre, nur einmal ctrl-z....bittebitteeee!). Man stelle sich ein SMS an den falschen Empfänger vor: weniger als 160 Zeichen und man ist alleine im Leben. Du siehst den „sending progress bar" und hast nicht mal Zeit, den Akku weg zu reissen!

Was ist das Dümmste, was Du gesehen hast?

Ich weiss nicht mehr, welche Windowsversion das war, aber einmal gab es so einen ‚shut down'-Dialog, da konnte man ‚herunterfahren', ‚neu starten' usw. wählen und dann entweder ja, nein oder abbrechen sagen! Davon hatte ich fast ein Tourettesyndrom entwickelt, weil ich immer wieder spontan das Bedürfnis hatte, meinen Rechner nicht herunter zu fahren. Gab es das, oder hab ich das geträumt? Jetzt ist es nicht mehr so. Aber irgendwie wäre das eine Art später Abschluss der französischen Revolution. Die gesamte Errungenschaft der Freiheit und des Individualismus ganz konkret angewendet. Das ist etwa so, wie wenn ich in die Migros gehe, einen Vitaminsaft aus dem Gestell nehme, ihn an der Kasse aufs Förderband lege und dann dem Kassierenden sage, dass ich den Saft gerne nicht kaufen möchte. Alles andere bleibt gleich: ich stehe Schlange, wir begrüssen und verabschieden uns. Ist es sinnvoller, eine Kinderüberaschung zusammen zu bauen?

Alles ist Sinnlos? Das klingt doch auch abgedroschen...

Nein. Alles was je erreicht wurde, ist, dass immer noch Leben existiert. Sinnlos wäre alles dann, wenn dies nicht ewig so bleiben würde. Aber die Evolution ist vielleicht gerade dabei, einen Sprung zu vollziehen. Bisher fanden die Innovationen in der Entwicklung der Arten statt, also nicht zu Lebzeiten eines Lebewesens. Das Leben selbst diente nur als Test, ob die letzte genetische Neukombination oder Mutation einen Fortschritt bedeutete. So betrachtet macht die Kinderüberaschung nicht mehr Sinn als seinen Rechner nicht herunter zu fahren. Der Mensch hat aber nun die Möglichkeit, auch zu Lebzeiten Probleme zu lösen, die bisher nur durch genetische Anpassung gelöst werden konnten. Das finde ich total faszinierend!

Somit haben wir einen klaren Sinn im Leben: unseren Beitrag zur ewigen Erhaltung von Leben zu leisten - weil wir es können. Es gibt viele Probleme zu lösen, z.B. dass in vier Milliarden Jahren die Sonne ein für allemal untergeht und bis dann irgend eine Form von Leben ganz weit weg aus unserem Sonnensystem heraus gelangen muss.

Gibt es eine Frage, die Dich gerade brennend interessiert?

Wie kann man strukturelle Informationen aus Daten berechnen? Was ist der Unterschied zwischen Peppermint und Spearmint?

Pizza zu gewinnen!

Die DVD-Preise sinken, aber das Videosessions-Budget bleibt vorerst konstant! Um das zu kompensieren, gibts in diesem Semester ein Preisrätsel, bei dem es dreimal eine Pizza nach Wahl an einer Videosession (ebenfalls nach Wahl) zu gewinnen gibt.
Folgende Zeilen bilden jeweils ein Rätsel, dessen Lösung eine Filmfigur ist. Man nehme von jeder Figur den ersten Buchstaben des Namens und reihe alle so erhaltenen Buchstaben aneinander und erhält so das Lösungswort, das übrigens ein Filmtitel ist. Die ersten drei, die eine vollständige Lösung, d.h. eine, die das Lösungswort sowie alle Personennamen enthält, an videosessions@vis.ethz.ch senden, oder aber die drei vollständigsten Lösungen, die wir bis zum 26. April erhalten, gewinnen je eine Pizza.

1. Bürger mit Krückstock
2. palindromische Ballerina
3. Strahl mich rauf
4. bestimmt übers Käferleben
5. Quentin Tarantino in „au revoir les enfants“
6. lauwarmer Engel zu Fuss
7. U.S.-Bundesstaat, ehemals mit Zuhälter
8. nicht Elmo und nicht Fabio
9. barbarische Kanone, verdreht
10. begeisterter Teppichbesitzer

AZB
PP/Journal
CH - 8092 Zürich

Falls unzustellbar bitte zurück a
Verein der Informatik Studieren
RZ F17.1
ETH Zentrum
CH 8092 Zürich

Agenda

April

07. April:	Videosession: Whale Rider
14. April:	Einführung in die Bibliothek
26. April:	Mitgliederversammlung VIS
28. April:	Videosession: Tron
29. April:	SSD-Expo im GEP Pavillon halbjährliche Produkteausstellung

Mai

04. Mai:	Einführung in die Bibliothek
12. Mai:	Videosession: Groundhog Day