Interview mit Prof. Johannes Buchmann

Innerhalb weniger Monate ist mit Prof. Dr. Johannes Buchmann ein zweiter neuer Professor an den Fachbereich Informatik berufen worden. Das Inforz sprach mit ihm über seine ersten Eindrücke, Interessen und Zukunftspläne.

Inforz: Herr Buchmann, Sie sind seit dem Sommersemster in der Nachfolge Tzschach hier am Institut für Theoretische Informatik dieses Fachbereiches tätig. Wie sind Ihre ersten Eindrücke? Haben Sie sich schon eingelebt?

Buchmann: Die Eindrücke sind dadurch bestimmt, daß ich erstens eine Vorlesung über Kryptographie halte, zweitens meinen Lehrstuhl hier am Fachbereich installiere, drittens ein Haus gekauft habe, das gerade umgebaut wird, und viertens meine Familie noch in Saarbrücken wohnt, so daß ich noch ein bißchen hin und her pendle. Habe ich mich schon eingelebt? Nein, daß kann man nicht sagen. Ich habe aber eine sehr kompetente Sekretärin, Frau Skrobic, die sehr viel organisiert hat. Eine Reihe von Mitarbeitern, die ich aus Saarbrücken mitgebracht habe, sind sehr engagiert dabei, alles aufzubauen. In meiner Vorlesung sitzen 30 Studenten, die auch sehr gut mitarbeiten. Alles in allem glaube ich daher, daß wir schon ganz gut angefangen haben und hoffe darauf, daß wir auch noch sehr gut weiterarbeiten werden. Ich habe ein bißchen wenig Platz. Aber ich will mich auch nicht beschweren. Der Fachbereich hat sich ziemlich ins Zeug gelegt bei meiner Berufung. Außerdem leidet der Gesamtfachbereich darunter, daß die räumliche Situation so miserabel ist.

Inforz: Wir würden uns gerne ein Bild von Ihrer Person machen. Wo und was haben Sie studiert? Wie verlief Ihr weiterer Werdegang, bevor Sie nach Darmstadt gekommen sind?

Buchmann: Aufgewachsen bin ich in Köln, habe dort Mathematik und Physik mit dem Ziel Lehramt studiert. 1982 habe ich in Köln im Bereich der Zahlentheorie promoviert. Dann ist mein Doktorvater verstorben und ich hing etwas in der Luft. Es ist ja bekannt, daß es im wissenschaftlichen Bereich nicht schlecht ist, "Sponsoren" zu haben. Von 1983 bis 1984 bin ich in den Referendardienst gegangen und habe mein zweites Staatsexamen in Mathematik und Physik abgelegt. Dann war ich ein Jahr auf einer Assistentenstelle in Köln (der Professor wurde anschließend emeritiert). Ein weiteres Jahr verbrachte ich anschließend in den USA, an der Ohio State University. Dort habe ich mich sehr stark mit wissenschaftlichem Rechnen im Bereich Algebra und Zahlentheorie beschäftigt. Ich habe große Programmpakete geschrieben und mich mit Algorithmen und Berechnungsverfahren im Bereich Zahlentheorie beschäftigt. Ich bin viel herumgereist, war auf vielen Konferenzen, habe viele Kollegen kennengelernt und habe angefangen, mich für die Schnittstelle zwischen Informatik und Mathematik zu interessieren, also Komplexität zahlentheoretischer Algorithmen, Komplexität von Algorithmen im Bereich der Computeralgebra einerseits, und Anwendungen der Zahlentheorie auf die Kryptographie andererseits. Da bestehen Bezüge: Schwierige zahlentheoretische Probleme sind Grundlage der Sicherheit kryptographischer Verfahren: Das Stichwort hier ist Public-Key-Kryptographie. Ich habe angefangen in diesem Bereich zu publizieren. 1988 habe ich mich in Düsseldorf mit einer Arbeit über Komplexität von Algorithmen im Bereich der algebraischen Zahlentheorie habilitiert. Dann habe ich mich in Saarbrücken beworben auf eine Stelle für Mathematik, wo ich aber nicht genommen wurde. Daraufhin sind die Informatiker auf mich aufmerksam geworden und haben mich auf eine C4-Stelle berufen. Anschließend war ich fast siebeneinhalb Jahre in Saarbrücken. Ich habe angefangen, mich für effiziente Implementierungen von Faktorisierungsalgorithmen für natürliche Zahlen zu interessieren, Implementierungen, die viel Rechenzeit benötigen. Dann haben wir angefangen, ein System zu bauen, das einem die ungenutzte Rechenzeit in einem riesigen Workstationnetz zugänglich macht. Wir haben auf ca. 240 Rechnern mit dem System LIPS gerechnet, welches also unsere Anwendungen immer aus der Versenkung hervorholt, wenn der eigentliche Besitzer der Workstation gerade nicht mit dem Rechner arbeitet. Wir haben also im Bereich der verteilten Systeme gearbeitet. Als wir festgestellt haben, daß im Bereich der Zahlentheorie viel für den Mülleimer programmiert wird, haben wir 1994 angefangen, eine C++-Klassenbibliothek namens LIDIA für diese Probleme zu bauen, die auch schon einen beträchtlichen Umfang angenommen hat und frei erhältlich ist. Es gibt sie auch schon in Darmstadt. Dann haben wir begonnen, eine C++-Klassenbibliothek für kryptographische Probleme zu bauen.

Inforz: Warum haben Sie sich für die TH Darmstadt entschieden?

Buchmann: Die Sache hat einen persönlichen und einen beruflichen Aspekt. Beginnen wir mit dem persönlichen Aspekt: Meine Frau und ich wollten wieder in einem Ballungsgebiet leben. Das Saarland ist eher ruhig, beschaulich, da kann man auch ganz schön leben, aber es ist halt begrenzt. Es liegt etwas am Rande der Republik. Darmstadt liegt in einem Ballungsraum, mit Frankfurt, Heidelberg usw. Beruflich gibt es für mich hier ein ganz interessantes Umfeld. Es gibt eine Reihe von Forschungsinstitutionen, die sich hier mit kryptographischen Problemen beschäftigen. Zum Beispiel hat die GMD hier eine Arbeitsgruppe und hier gibt es das Forschungszentrum der Telekom. Im kryptographischen Bereich ist man hier also sehr gut aufgehoben.

Inforz: Sie haben bereits gesagt, daß Sie sich viel mit Kryptographie und algebraischer Zahlentheorie beschäftigt haben. Entspricht das also auch Ihren Spezialgebieten?

Buchmann: Kryptographie sicherlich. Und auch Algorithmen im Bereich der Algebra und Zahlentheorie, und wie gesagt haben wir noch dieses Projekt, das verteilte System zu machen.

Inforz: Welche Erfahrungen haben Sie bisher mit den Lehrveranstaltungen hier gesammelt?

Buchmann: Ich halte eine Kryptographievorlesung, die nicht im Vorlesungsverzeichnis angekündigt war. Trotzdem nehmen erfreulich viele Studierende teil. Ich muß sagen, daß die mathematischen Grundkenntnisse vielleicht noch eine Spur besser sein dürften, ansonsten finde ich die Studierenden aber sehr engagiert. Sie fragen viel und diskutieren auch. Die Zahlentheorievorlesung, die ich auch noch halte, ist eine Spezialvorlesung; da sitzen nur meine Mitarbeiter drin und zwei bis drei andere, das ist auch okay.

Inforz: Wieviel Lehrerfahrung, vor allem auch in der Grundlehre, bringen Sie aus Saarbrücken mit?

Buchmann: In Saarbrücken habe ich beispielsweise die Informatik I bis IV einmal komplett durchgelesen, allerdings sind die Schwerpunkte dort etwas anders als hier. Dann habe ich Algorithmen und Komplexität I und II, Kryptographie und Zahlentheorie gelesen. Im Wintersemester werde ich hier die Vorlesung Grundzüge der Informatik III halten.

Inforz: Wir kommen nun zu etwas allgemeineren Fragen. Die Informationstechnik spielt eine immer wichtiger werdende Rolle in der Gesellschaft. Wie kann man Ihrer Meinung nach gewährleisten, daß die Informatik der Verantwortung, die diese Entwicklung mit sich bringt, gerecht wird?

Buchmann: Das ist eine wichtige Frage. Zu allererst habe ich den Auftrag, die Wissenschaft zu vermitteln, von der ich etwas verstehe. Die wissenschaftlichen Disziplinen, die sich mit Technikfolgenabschätzung beschäftigen, vertrete ich nicht und kann sie insofern auch nicht unterrichten. Der andere Aspekt ist der verantwortliche Umgang mit Ressourcen. Das ist für einen Wissenschaftler eine wichtige Frage. Das ist natürlich auch für mich ein Thema, obwohl es im alltäglichen Wissenschaftsbetrieb leicht untergeht. Zum Beispiel kann man in diesem Zusammenhang die Frage diskutieren, wie man unsere Daten vor unerlaubten Zugriffen schützen kann. Die Kryptographie kann man einerseits benutzen, um militärische Geheimnisse zu transportieren, man kann sie aber auch im Gegenteil dazu benutzen, den einzelnen in den Stand zu versetzen, Kontrolle über seine persönlichen Daten zu behalten. Mit der Kryptographie kann man gewährleisten, daß man Kontrolle darüber behählt, ob mit seinen Daten erlaubte oder unerlaubte Dinge gemacht werden. In der Kryptographievorlesung spreche ich solche Dinge auch an. Ich hoffe natürlich auch sehr, daß die Studierenden sich selbst mit diesen Fragen beschäftigen und Lehrveranstaltungen der Fachbereiche besuchen, die damit zu tun haben. So etwas gibt es hier ja auch.

Ich bin gerne bereit, solche Fragen zu diskutieren, werde aber nicht anfangen, Vorlesungen über Technikfolgenabschätzung zu halten.

Inforz: Welche Empfehlungen geben Sie jetzigen Studierenden im Bezug auf die Wahl von Schwerpunkten, Nebenfächern und außeruniversitären Tätigkeiten?

Buchmann: Ich denke, das Wichtigste ist, daß man im Studium das tut, was einen interessiert. Um herauszufinden, was einen interessiert, muß man sich nur bereit genug umschauen. Die Beobachtungen aus meiner eigenen Studentenzeit zeigen mir, daß der Studienweg leider ganz schön vom Zufall bestimmt ist. Man sollte wirklich selbst aktiv sein und die Professoren ansprechen. Das heißt, man sollte aktiv sein bei der Auswahl und sich fragen, was man für Interessen hat. Eine andere Sache ist zu erwägen, auch mal ins Ausland zu gehen. Das ist immer eine enorme Erweiterung des Horizonts, auch wenn man glaubt, daß man die Kontinuität des eigenen Studiums stark durchbricht. Die andere Sache ist auch, sich zu bemühen, zügig zu studieren. Ich glaube, einige Studierende studieren einfach zu lange.

Inforz: Wie beurteilen Sie den Ruf der TH Darmstadt und speziell des Fachbereichs Informatik unter Ihren Kollegen außerhalb der TH?

Buchmann: Bei den deutschen Hochschulen gibt es bis jetzt keine direkte Konkurrenz. Es gibt überall in deutschen Hochschulen Bessere und Schlechtere. Ich glaube, der Fachbereich Informatik an der TH Darmstadt ist ein solider Informatik-Fachbereich, der eine Menge Potential hat. Eine Menge Potential durch die Leute, die hier tätig sind und eine Menge Potential vom Umfeld und Einzugsgebiet. Ich persönlich meine, daß man die Informatik noch verstärken könnte, wenn sie einen Standort bekäme.

Ich finde, die Studierenden sollten ruhig auch hingehen und Fachbereiche verschiedener Universitäten vergleichen. Wir – die Professoren – können das schlecht.

Inforz: Sie haben jetzt ja schon mehrere Universitäten kennengelernt. Die Studierenden sehen aber in der Regel aber nur eine.

Buchmann: Sie müssen als Studierender nur herausfinden, wo das stattfindet, was für Sie geeignet ist. Dann gibt es eine Abstimmung mit den Füßen und dann wird sich zeigen, welche Fachbereiche gut sind. Ich glaube, daß die Studierenden hier von den amerikanischen Studenten lernen sollten, etwas mehr Mobilität zu zeigen. Es gibt genügend Möglichkeiten, sich zu informieren. Machen sie das ruhig.

Inforz: Herr Buchmann, wir bedanken uns für das Gespräch.

(Das Gespräch führten Andreas Hiepe und Felix Gärtner)