

GESELLSCHAFT FÜR INFORMATIK E.V.

G



C 2014

**DIE
GRAND CHALLENGES
DER INFORMATIK**

Impressum

Gesellschaft für Informatik e.V. (GI)

Wissenschaftszentrum

Ahrstraße 45 · 53175 Bonn

Telefon 0228 / 302 – 145

Telefax 0228 / 302 – 167

grandchallenges@gi.de · www.gi.de

Redaktion: Simone Rehm & Cornelia Winter

Konzeption & Gestaltung: www.mehrwert.de

© 2014, Gesellschaft für Informatik e.V.

Bildnachweis: Seite 7: Shutterstock.com/Ollyy, Showcake, Dubova, Hayati Kayhan, BigLike Images, Verticalarray, Pavel Ignatov, Africa Studio · Seite 9: Shutterstock.com/Botnarenco Stas, singkam, Panachai Cherdchuheep, extradeda, DenisNata, onair, Kwanjitr, idesygn, rook76, dny3d, Milos Dizajn, Jag_cz · Seite 11: Shutterstock.com/TsuneoMP, Alex Mit, mtkang, Jorg Hackemann, etraveler, Franck Boston, Peshkova, Macrovector, Jozsef Bagota, ArtisticPhoto · Seite 13: Shutterstock.com/Syda Productions, Photology1971, Sergey Nivens, Rawpixel, Sayid, VLADGRIN, Arcady, Turbo Vector · Seite 15: Shutterstock.com/ imageshunter, Kekyllaynen, hkeita, megainarmy, Zurijeta, Stepan Kapl, Neveshkin Nikolay, Maksim Kabakou, gradi1975, Denys Prykhodov, Darq





Vorwort

Vor welchen großen Herausforderungen steht die Informatik in den kommenden Jahren und Jahrzehnten? Mit dieser Frage hat sich die Gesellschaft für Informatik e.V. (GI) im Rahmen der Initiative „Grand Challenges der Informatik“ beschäftigt. Gesucht waren grundsätzliche und schwierige Fragestellungen, deren Lösung mithilfe der Informatik einen deutlich spürbaren Fortschritt in wirtschaftlicher, sozialer oder gesellschaftlicher Hinsicht für die Allgemeinheit bedeutet.

Die Sprecher der Fachbereiche, GI-Fellows und interessierte Fachleute waren eingeladen, „ihre“ Grand Challenge bei der GI einzureichen. Die Vorschläge wurden gesichtet, verdichtet und nach verschiedenen Kriterien bewertet. Fünf davon wurden im Januar 2014 dem GI-Präsidium vorgestellt und als herausragend identifiziert. Im Folgenden stellen wir sie einem breiteren Publikum vor.

Warum fiel die Wahl gerade auf diese fünf? Mit dem Entstehen der Informatik hat man Zeichen binär codiert. Auf diese Weise konnte man Zeichen, denen eine Bedeutung innewohnt, eine digitale Repräsentation geben. Somit hat man die Möglichkeit geschaffen, die Bedeutung von Zeichenfolgen (z.B. die Bedeutung eines Worts) und die Zeichenfolge selbst (z.B. das Wort) von seiner Repräsentation in der realen Welt zu trennen. Was früher mit Tinte auf Papier geschrieben wurde, lässt sich heute in Bits und Bytes erfassen. Binär codierte digitale Symbole genügen. Die Information wird entmaterialisiert und kann als elektronische Post in Sekundenschnelle ans andere Ende der Welt gelangen, wo der Empfänger die Information entschlüsselt und ihre Bedeutung sofort versteht. In der allseitigen Verfügbarkeit wie auch in der

Vielfalt der repräsentierten Inhalte liegt gerade der Vorteil digitaler Medien.

Was für viele Menschen ein Segen ist und das Aufblühen des modernen, digitalen Zeitalters erst ermöglichte, stellt uns Informatiker heute vor immense Herausforderungen:

Wie bewahren wir digitale Informationen für unsere Nachwelt auf? Bücher, Bilder und Tonträger lassen sich ins Museum stellen. Sie lassen sich sogar digitalisieren und digitalisiert für lange Zeit archivieren. Wie aber bewahrt man einen Video-Clip, der digital erstellt und nur im Internet veröffentlicht wird, für die nachfolgenden Generationen auf?

Wie erkennen wir beim Versenden einer digitalen Information, ob sie auf dem Weg zum Empfänger unbemerkt gelesen wurde? An einem versiegelten Briefumschlag sah man, ob das Siegel gebrochen war. Eine digitale Information kann unbemerkt kopiert, aber auch sehr einfach manipuliert worden sein. Wie sichern wir dann Integrität und Vertraulichkeit im Netz?

Eine digitale Information kann mit beliebig vielen anderen Informationen verbunden werden. Es entstehen dabei vernetzte Systeme, die in ihrer Komplexität kaum fassbar, geschweige denn beherrschbar sind. Wie schaffen wir es, die daraus entstehenden Risiken einzudämmen und zu beherrschen?

Ist es schon schwer, sich in einem Irrgarten zurechtzufinden, wo Wege im Nichts enden, wie schwer finden sich Menschen

im virtuellen Raum zurecht? Wie kann die allgegenwärtige Mensch-Computer-Interaktion künftig so gestaltet werden, dass alle Bürger sich in der gemischt digitalen und physischen Welt souverän bewegen können?

Und nicht zuletzt: Wenn Software unsere Welt regiert, unsere Autos und Flugzeuge steuert und unsere medizinischen Instrumente dirigiert, wie schaffen wir es zu beweisen, dass die Software genau das tut, was sie soll?

Die GI hat diese fünf Fragestellungen als große Herausforderungen der Informatik identifiziert, weil sie damit zum Ausdruck bringen möchte, dass die Informatik sich zuallererst um die von der Informatik selbst geschaffenen Probleme kümmern muss. Die Auswahl spiegelt sowohl die Kompetenz der Informatik zur Definition dieser Fragestellungen als auch ihre Verantwortung für die Gestaltung der Zukunft wider. Es werden Forschungs- und Entwicklungsthemen benannt, die in der Fortentwicklung der Informatik als Schlüsselfelder gelten und Potenziale für künftige Anwendungen, Dienste oder Produkte beinhalten. Die Grand Challenges-Initiative soll Aufmerksamkeit bei Fachleuten und Interessenten in Wissenschaft, Politik, Gesellschaft schaffen, Ressourcen zur Lösungsfindung bündeln sowie den Nachwuchs motivieren.

So notwendig die Fokussierung ist, so sehr reduziert sie auch das Spektrum der interessanten Gebiete und lässt manchen wichtigen Aspekt ganz unbeachtet. Dies ist uns bewusst. Deshalb sehen wir die Initiative als fortlaufende Aktivität. Uns ist ebenfalls

bewusst: Es existieren noch viele große Herausforderungen für die Informatik in allen Bereichen der Gesellschaft wie z.B. Energie, Umwelt, Medizin, Biologie, Transportwesen, um nur einige zu nennen. Wir stehen also nicht am Ende, sondern ganz am Anfang von Diskussion und Erforschung der Grand Challenges.

Unser herzlicher Dank für die Erarbeitung der ersten fünf Grand Challenges richtet sich an Simone Rehm (Leitung), Wolfgang Coy, Jörg Desel, Maximilian Eibl, Albert Endres, Gregor Engels, Torsten Eymann, Hannes Federrath, Michael Goedicke, Michael Herczeg, Michael Koch, Agata Królikowski, Heinz-Günter Kuper, Jens-Martin Loebel, Peter Mertens, Dirk Nowotka, Harald Reiterer, Gunter Saake, Patrick Stoll, Wolfgang Thomas, Thomas Wilke.

Weitere Informationen sowie die Langfassungen der Grand Challenges mit Beispielen finden Sie unter <http://www.gi.de/themen/grand-challenges-der-informatik.html>.

Ihre Gesellschaft für Informatik



Digitales Kulturerbe

Die Digitalisierung hat längst auch unsere Kultur erfasst. Das birgt Chancen, denn digitalisiert sind analoge Artefakte wie Bücher einem größeren Interessenten-Kreis zugänglich. Gleichzeitig verändert sich der Gegenstand jedoch, er verliert beispielweise seine Haptik. Damit verbunden sind zwei zentrale Herausforderungen: Wie können virtuelle Objekte angemessen präsentiert und zugänglich gemacht werden? Und es stellt sich die Frage nach der Langzeitarchivierung: Wie lässt sich das digitale Kulturerbe dauerhaft bewahren?

Neben den digitalisierten analogen Artefakten haben wir es mittlerweile aber auch mit vielen alltäglichen digitalen Kulturgütern wie Fotos, Filmen, Musik oder E-Mails zu tun. Nicht zu vergessen sind auch die so genannten Born Digitals wie Programme oder Spiele, die überhaupt keine analoge Entsprechung mehr haben. Im Gegensatz zu analogen Datenträgern wie Steintafeln verfügen digitale Datenträger allerdings nur über wenige Jahre Halbwertszeit. Problematisch sind zudem proprietäre Systeme und Formate, denn damit sind Daten von der Interpretation durch eine bestimmte Software abhängig. Rechtliche Fragen im Zusammenhang mit Urheberrechtsschutz, Digital Rights Management und Cloud Computing erschweren die Langzeitarchivierung zusätzlich. Insgesamt droht so der Verlust digitaler Kulturgüter. Und was die Präsentation betrifft, so stehen Konzepte für die Verschmelzung digitaler Kultursammlungen mit den Möglichkeiten physikalischer Gedächtnisorganisationen wie Archive, Museen oder Bibliotheken noch am Anfang ihrer Entwicklung.

Lösungen zur Bewahrung des digitalen Kulturerbes müssen neben rechtlichen Aspekten viele fachspezifische und technische Anforderungen berücksichtigen, was die Konsensfindung erschwert. Auch ist Langzeitarchivierung aus technischer Sicht kein einmaliger Vorgang, sondern eine dauerhafte Aufgabe: Datenbestände müssen kopiert, umformatiert und emuliert werden. Am sinnvollsten geschieht dies mithilfe offener Standards und Open-Source-Software, um Nachvollziehbarkeit und langfristige Nutzung zu sichern. Doch wie zuverlässig sind Methoden der Langzeitarchivierung überhaupt? Hier stehen Testverfahren aus.

Mit ersten Ansätzen, die dem Paradigma Blended Interaction folgen, entstehen auch neue Interaktionskonzepte für die Präsentation digitaler Kulturgüter; die interaktive Wissensvermittlung erfolgt hier durch die Kombination von realweltlicher Ausstellung und digitaler Präsentation. Zugang und Bewahrung des digitalen Kulturerbes lassen sich nicht mit einem einzigen Ansatz lösen. Die große Herausforderung ist die Entwicklung von Best Practices in einem längerfristigen und interdisziplinären Prozess.

Mit Strategien zur Langzeitarchivierung können wir unser digitales Kulturerbe erhalten und ein „Zeitalter ohne Gedächtnis“ vermeiden. Ohne nachhaltige Langzeitbewahrung ist das digitale Kulturerbe unwiederbringlich verloren. Deshalb benötigen wir Konzepte, um diese Kulturgüter auch für künftige Generationen begreifbar und erlebbar zu machen. <





Das Internet der Zukunft

sicher, frei,
vertrauens-
würdig

In den 40 Jahren seines Bestehens hat das Internet stetig an Bedeutung gewonnen – gesellschaftlich, politisch, wirtschaftlich. Seine technische Basis ist jedoch weitgehend unverändert geblieben. Insbesondere die Sicherheit im Internet hat mit seiner gewachsenen Bedeutung nicht mithalten können. Daher ist die technische Weiterentwicklung zu einem sicheren, freien und vertrauenswürdigen Internet der Zukunft eine besondere Herausforderung der Informatik.

Eine Grundfrage der Sicherheit betrifft den Konflikt von Privatsphäre und Eindeutigkeit bei der Internet-Kommunikation. Einerseits sollen Internet-Nutzer ihre Identität geheim halten können, andererseits sollte der Sender einer Nachricht auf Wunsch des Empfängers auch eindeutig zu identifizieren sein. Ein anderer Aspekt ist die Zweckbindung sensibler und persönlicher Daten. Wie ist sichergestellt, dass beispielsweise eine digitale Krankenakte nur vom behandelnden Arzt, nicht aber von der Versicherungswirtschaft verwendet wird? Wie lassen sich kriminelle Handlungen wie Spam, Cybermobbing oder Identitätsdiebstahl verhindern, ohne zugleich die Offenheit der Kommunikation einzuschränken? Verlässlichkeit und Vertrauenswürdigkeit sind Kerneigenschaften des Internets der Zukunft!

Zweifellos gibt es zu allen Einzelproblemen bereits viele Lösungsansätze. Und obwohl die Komplexität und Interdependenz der Fragen eine Gesamtbetrachtung erfordern, steht diese noch aus. Hier muss die Informatik mit ihren technischen und methodischen Kompetenzen eine Vorreiterrolle einnehmen, Experten

aller Fachrichtungen und Tätigkeitsbereiche zusammenbringen und den Erneuerungsprozess des Internets federführend mitgestalten. So verfolgt das Konzept der mehrseitigen Sicherheit etwa das Ziel, Kommunikationssysteme technisch so zu entwerfen, dass die Sicherheitsanforderungen aller Nutzer berücksichtigt werden und sich widersprüchliche Anforderungen auflösen lassen.

Auf übergeordneter Ebene könnte man das existierende Internet technisch erweitern oder parallele neue Netze aufbauen, mit Schnittstellen zum existierenden Internet. Um den Anforderungen des digitalen Zeitalters gerecht zu werden, sind Dienste mit garantierten Eigenschaften notwendig, zum Beispiel mit verschlüsselter Datenübertragung, Werbefreiheit und physischer Identifizierung. Bei Bedarf kann der Informationsaustausch anonym oder pseudonym stattfinden. Pseudonymität wahrt die Privatsphäre, die Nutzer sind jedoch – falls erforderlich – nachträglich identifizierbar. Mit verschlüsselten mobilen Endgeräten in der Hand haben Nutzer einen sicheren und freien Zugang zum Internet.

Das Internet der Zukunft muss offen gestaltet sein und den Austausch von Daten und Gütern ohne Beschränkung der Kommunikationsformen erlauben. Das Internet der Zukunft genießt zudem Vertrauen, denn seine Kommunikationsinfrastruktur ist nicht nur abhörsicher, sondern ermöglicht insbesondere bei rechtlich relevanter Kommunikation die Nachvollziehbarkeit und reduziert damit auch signifikant die Möglichkeiten krimineller Handlungen. <





Systemische Risiken in weltweiten Netzen

Wirtschaftssysteme, Unternehmen, Maschinen und Haushalte sind enger vernetzt als je zuvor. Die Methoden, eine Übertragung von Schocks durch das gesamte System zu identifizieren und einzuschränken, haben mit dieser Entwicklung jedoch nicht Schritt gehalten: Systemische Risiken werden auch in komplexen und dynamischen Netzwerken durch starre Trennlinien, fixe Puffer und personelle Überprüfung gemanagt. Die Herausforderungen an die Informatik: Entwicklung differenzierter Interventionssysteme.

Beispiel Finanzkrise: Ausfälle US-amerikanischer Hypothekendarlehen haben erst US-amerikanische Banken, dann europäische Institute und zuletzt ganze Staaten in den Ruin geführt. Die Unterstützung für betroffene Unternehmen und Staaten erfolgte nach dem Gießkannenprinzip, statt die systemischen Knotenpunkte des Netzwerks zu identifizieren und dort gezielt tätig zu werden. Andere Netzwerke wie elektronische Börsen sind durch Schnelligkeit und hohen Automatisierungsgrad attraktiv. Auf Ausfälle reagieren sie aber besonders unflexibel: bei Kurseinbrüchen wird der Handel automatisch eingestellt, denn maßgeschneidertes Eingreifen ist wegen der hohen Übertragungsgeschwindigkeit und der Datenmengen nach heutigen technischen Standards unmöglich.

Hier ist die Informatik gefordert, den wirtschaftlichen und gesellschaftlichen Bedarf nach differenzierten Interventionssystemen zu decken. Nötig sind vier Schritte: Im ersten Schritt werden abstrakte Netzwerk-Modelle entwickelt, die auf unterschiedlichste

reale Probleme anwendbar sind. Um übertragbar zu sein, müssen die Modelle mit speziellen Datensätzen umgehen können und viele Stellschrauben enthalten. Im zweiten Schritt werden umfangreiche Simulationen notwendig. Diese erlauben es, an Knotenpunkten des Netzwerks Schocks auszulösen. Je nachdem in welche Richtung sich ein Schock ausbreitet, wie stark sein Effekt auf das Netzwerk ist und wie lange und intensiv er spürbar ist, lässt sich der Knotenpunkt als mehr oder weniger wichtig einteilen. Im dritten Schritt gilt es die Ergebnisse der Simulationen zu interpretieren. Das geschieht aufgrund der hohen Datenmengen nicht personell, sondern automatisiert mit Methoden aus der Künstlichen-Intelligenz-Forschung. Doch auch die beste Schlussfolgerung ist ohne zielgruppengerechte Kommunikation wertlos. Politiker und Aufsichtsbehörden interessieren sich für andere Kennzahlen als Führungskräfte aus der Wirtschaft. Angemessene Kommunikationsstrategien bilden daher den vierten und letzten Lösungsschritt.

Und dann? Dann können knappe Ressourcen wie Eigenkapital, Ersatzteillager oder Versicherungen an kritischen Stellen eingesetzt werden, statt sie undifferenziert an allen eventuellen Schwachstellen vorzuhalten. Es können von Interessengruppen gesteuerte wirtschaftliche oder politische Schreckensszenarien wissenschaftlich zuverlässig auf ihren Wahrheitsgehalt überprüft werden. Gezielte Interventionen ersetzen Maximallösungen, die auf Kosten der Allgemeinheit gehen. ◀





allgegenwärtige Mensch-Computer Interaktion

In unserer immer mehr von digitalen Kommunikations- und Informationsangeboten bestimmten Welt entscheidet die wirkungsvolle Nutzung von Computern – insbesondere die Interaktion zwischen Mensch und Computer – zunehmend über persönlichen Erfolg und gesellschaftliche Teilhabe. Wie kann die Informatik bei der Gestaltung von Interaktion und Benutzungsschnittstellen dazu beitragen, dass Menschen möglichst aller Altersstufen, körperlicher und geistiger Verfassung, Bildungsabschlüsse, kultureller Hintergründe, gesellschaftlicher Funktionen und ökonomischer Möglichkeiten gleichermaßen von der Informationstechnologie profitieren können?

Mit der Weiterentwicklung interaktiver und multimedialer Anwendungssysteme steigt auch deren Komplexität. Anwender haben inzwischen eine Vielzahl unterschiedlicher Interaktionsgeräte zur Verfügung: private mobile Geräte, Tablets, interaktive Tische, öffentliche Interaktionswände und vieles mehr. Wie lässt sich sicherstellen, dass Einzelpersonen oder Gruppen diese Geräte intuitiv erfolgreich nutzen können? Niemand möchte für jedes Gerät eine ausführliche Gebrauchsanweisung studieren. Außerdem werden immer mehr Dienste über diese Geräte angeboten und genutzt. Die Dienste und ihre Verknüpfungen untereinander sind heute oft nicht verständlich. Eine benutzergerechte Gestaltung der Mensch-Computer-Interaktion bezieht daher auch die genutzten Dienste ein und integriert sie in ein transparentes und verständliches Gesamtkonzept. Ein wichtiger Aspekt ist dabei die Absehbarkeit von Folgen. Da Menschen bei der Interaktion mit Computern vielfach Aktionen wie den Abschluss eines Vertrages

oder die Übermittlung persönlicher Daten auslösen, sollten sie bereits vor der Interaktion die Konsequenzen ihres Handelns verlässlich einschätzen können.

Eine unmittelbar verständliche oder selbsterklärende Nutzung ist ein wichtiges Teilziel bei der Senkung der Zugangsvoraussetzungen. Neben Fragen der Software-Ergonomie spielt dabei die Fähigkeit zur kontextgerechten Konfiguration und Adaption eine wichtige Rolle. Der Anspruch adaptiver Informationssysteme ist es, sich automatisch und intelligent an den Nutzerkontext anzupassen, um Interaktion einfach, wirkungsvoll und individuell zu machen. Neue Interaktionswege – etwa die Verarbeitung natürlicher Sprache oder das Erkennen von Gesten – setzen wenn möglich direkt bei den natürlichen Fähigkeiten des Menschen an. Trotz beachtlicher Fortschritte in den letzten Jahren gibt es große Herausforderungen und Chancen gerade bei der transparenten Integration auf verschiedenen Ebenen. Interdisziplinarität und Zusammenarbeit von Experten aus Informatik, Psychologie, Design und anderen Fachgebieten sind gefragt.

Angemessen gestaltete Mensch-Computer-Interaktion soll es Menschen aller Alters- und Bildungsstufen künftig erlauben, die inzwischen allgegenwärtigen Kommunikations- und Informationsangebote mühelos zu nutzen und an gesellschaftlichen Prozessen in Bildung, Kultur und Politik teilzunehmen. Idealerweise schaffen Interaktionssysteme während der Nutzung ein Bewusstsein für die Folgen der Interaktion sowie für die Verantwortung des Nutzers für sich und andere. <





Verlässlichkeit von Software

Software ist heute allgegenwärtig und kommt im täglichen Leben überall zum Einsatz: in der Kommunikation, der Unterhaltungselektronik, im Haushalt, in der Medizintechnik und in sicherheitskritischen Bereichen. Umso überraschender, dass es keine durchgängigen Methoden und Werkzeuge gibt, um die Verlässlichkeit von Software zu garantieren. Dieser Herausforderung muss sich die Informatik in den kommenden Jahren stellen.

Verlässlichkeit umfasst dabei nicht nur die Frage, ob Software ihre funktionalen Anforderungen erfüllt. Auch Datenschutz und schnelles Erkennen von Fehlfunktionen sind wichtige Aspekte. Für Entwickler etwa wäre die Garantie, dass von ihnen entwickelte Softwaresysteme sensible Daten schützen, ein Qualitätsmerkmal. Anwender, die Software im privaten und industriellen Bereich einsetzen und von Software generierte Ergebnisse zur Grundlage von Entscheidungen machen, können durch Vermeiden oder frühzeitige Fehlererkennung hohe Kosten vermeiden – etwa bei Rückrufaktionen in der Automobilindustrie. Die Verlässlichkeit von Software lässt sich allerdings nicht vollständig automatisiert überprüfen und garantieren. Softwaresysteme werden für unklare Einsatzfelder und -bedingungen entworfen. Unterschiedliche Entwickler ändern sie im Laufe der Zeit, entwickeln sie weiter und vernetzen sie mit anderen Systemen. Schließlich setzen Nutzer mit verschiedenen Anforderungen sie ein. So entstehen Softwaresysteme von einer Größe, Komplexität und Vielzahl voneinander abhängiger Qualitäten. Deren Verlässlichkeit lässt sich nur durch eine Kombination von automatisierter Verifikation und weiteren Methoden wie Anwenderstudien garantieren.

In vielen Teilen der Informatik – beispielsweise Algorithmenentwicklung und -analyse, formale Spezifikationssprachen, automatische Verifikation, Semantik- und Simulationstechniken, Entwicklungs-, Architektur- und Testmethoden, Mensch-Maschine-Schnittstellenunterstützung – gibt es bereits umfangreiche Vorarbeiten zur Verlässlichkeit von Software. Diese Vorarbeiten müssen durch Zusammenarbeit der Fachleute mit Spezialisten in Hardware-nahen Disziplinen und in den Anwendungsdisziplinen zusammengeführt werden. Dadurch kann – im mittelfristigen Zeitraum innerhalb eingegrenzter Domänen und Nutzungskontexte, längerfristig auch für vernetzte Anwendungen – das Verhalten von Software präzise vorhergesagt werden. Auf Basis nachvollziehbarer und automatisch auswertbarer Dokumentationen können Softwaresysteme dann sowohl bei der Entwicklung als auch im Betrieb automatisiert zertifiziert werden. Auf Fehler kann das Softwaresystem dann auch mit selbstheilenden Mechanismen reagieren, so dass bei lokalen Ausfällen die Stabilität des gesamten Systems nicht beeinträchtigt wird.

Verlässliche Software steigert das Vertrauen der Nutzer, führt zu einem effizienteren Einsatz knapper Ressourcen und verhindert Katastrophen in sicherheitskritischen Bereichen sowie in der Infrastruktural.



Gesellschaft für Informatik e.V. (GI)

Wissenschaftszentrum
Ahrstraße 45 · 53175 Bonn
Telefon 0228 / 302 – 145
Telefax 0228 / 302 – 167
gs@gi.de · www.gi.de

