HOL, ML

Sinds een tiental jaren hou ik me intensief bezig met het onderwerp 'bewijsassistenten'.
Bewijsassistenten zijn programma's waarmee wiskunde door de computer op correctheid kan worden gecontroleerd. Dat wil zeggen: mits op de juiste wijze gecodeerd. Zulke gecodeerde wiskunde heet 'een formalisatie' en ziet er in de huidige systemen uit als volslagen onbegrijpelijke computercode. Er zijn vandaag de dag een viertal bewijsassistenten waarmee serieus wiskunde 'geformaliseerd' wordt: Mizar, HOL, Isabelle en Coq. Mijn onderzoeksterrein is het ontwikkelen van technologie om deze systemen *beter* te maken.
Er zijn nog niet veel hedendaagse wiskundigen die een helder beeld van bewijsassistenten hebben. Laat ik daarom eerst een tweetal misverstanden over bewijsassistenten uit de weg ruimen. Ten eerste worden bewijsassistenten *niet* gebruikt om de wiskunde verder te helpen, om nieuwe resultaten te bereiken. Je mag al blij zijn als je wiskunde die je door en door begrijpt met een heleboel werk voor een bewijsassistent verteerbaar kunt maken. Ten tweede zijn bewijsassistenten iets totaal anders dan systemen voor computer algebra en ook iets totaal anders dan automatische stellingenbewijzers. Deze drie soorten software hebben momenteel niets met elkaar te maken.
Het *aardige* van bewijsassistenten is dat als je je wiskunde eenmaal 'geformaliseerd' hebt, en het systeem zegt dat het klopt, dat je dan ook *volkomen* zeker kan zijn dat het inderdaad klopt. Over hoe zeker dat 'volkomen zeker' is kun je een hoop woorden vuil maken, maar laten we zeggen: een heel stuk zekerder dan op welke andere wijze dan ook bereikbaar is. De *enige* ruimte voor 'fouten' bij formalisatie is dat je denkt dat er wat anders staat dan er staat, dus dat je intuïtieve begrip niet overeenkomt met wat je in werkelijkheid hebt gedefinieerd en bewezen. Maar *wat* er staat is zo zeker als wat. En dat heeft iets heel moois. Een formalisatie is als een volkomen feilloze diamant.
Twee van de meest indrukwekkende formalisaties die ik ken zijn allebei gemaakt door John Harrison. Voor deze formalisaties gebruikte hij de mooiste van de vier bovengenoemde bewijsassistenten, zijn eigen versie van het HOL systeem. In zijn werk bij Intel gebruikt hij dit om floating point processors correct te bewijzen. Formalisatie van wiskunde doet hij er in zijn vrije tijd bij, voor de aardigheid.
De eerste van deze formalisaties bewijst de correctheid van de *kernel* van zijn HOL systeem. Het laat zien dat je er zeker van kan zijn dat dit programma geen 'bugs' bevat waardoor per ongeluk incorrecte bewijzen als correct worden geaccepteerd. Nu kun je morren dat hier een kip en ei probleem is (de checker kan fout zijn en daarom de formalisatie accepteren terwijl die niet klopt), of over hoe het dan zit met Gödels tweede onvolledigheidsstelling, maar dat zijn bezwaren die geen hout snijden. Wat wel een serieus bezwaar is, is dat de formalisatie momenteel alleen het 'moeilijke' stuk van de HOL kernel behandelt (het deel dat te maken heeft met het hernoemen van variabelen bij substitutie). Als evenwel binnenkort de *hele* HOL kernel correct bewezen is, zal er een heel interessant punt bereikt zijn!
De tweede formalisatie is een vertaling van het bewijs van de priemgetalstelling uit de analytische getaltheorie. Hierbij wordt door beschouwing van de nulpunten van de Riemann zeta-functie bewezen dat de verhouding tussen het aantal priemgetallen $\leq n$ en $n/\ln n$ in de limiet van n naar oneindig gelijk is aan één. Het analytische bewijs van deze stelling was een paar jaar geleden door de verzamelingstheoreticus Bob Solovay als uitdaging aan de bewijsassistentengemeenschap gegeven. Zijn verwachting was dat het nog decennia zou duren voor de technologie zo ver zou zijn dat dit bewijs in de praktijk geformaliseerd kon worden. Maar toen kwam John Harrison die in één maand tijd, naast zijn gewone werk bij Intel, een bestand van 4.314 regels HOL code produceerde waarin hij een vijftal pagina's uit een boek van Donald J. Newman formaliseerde. (Die HOL code blijkt ongeveer *acht* keer zo groot als de LaTeX van Newmans bewijs: dit heet de *de Bruijn factor*.) Hij deed dit voor het *Festschrift* voor zijn promotor die dat jaar zestig was geworden. Het controleren van deze formalisatie – inclusief het checken van alle gebruikte basiswiskunde – kost de computer ongeveer twintig minuten. Gedurende die tijd construeert het HOL systeem een gerichte acyclische graaf met 22.882.354 punten, die loopt van drie beginpunten voor de drie axioma's van het HOL systeem aan de ene kant, naar een eindpunt dat correspondeert met de priemgetalstelling.
De reden dat John Harrison dergelijke indrukwekkende dingen met zijn HOL systeem kan doen is omdat hij één van de beste *bibliotheken* van geformaliseerde wiskunde heeft die er zijn. Het is een aantrekkelijke gedachte (een soort wiskundige versie van het 'human genome-project') om een dergelijke bibliotheek te maken voor *alle* wiskunde die je als algemeen ontwikkeld wiskundige hoort te kennen. Dat is dus ongeveer de wiskunde die vroeger in het kandidaats- en nu in het bachelors-programma wordt behandeld. Ik heb ooit uitgerekend dat het ongeveer 140 man-jaar zal kosten om dat allemaal te formaliseren. Een interessante dagdroom is om je af te vragen of dat er ooit van zal komen. En zo ja: wanneer dan, en in welke vorm.