Foutverbeterende codes

Begeleider: Raymond van Bommel

In digitale communicatie komen berichten soms niet goed aan. Zo kan een radiosignaal door interferentie niet goed aankomen of kan data op een harde schijf ontoegankelijk worden door fysieke beschadiging. Een manier om dit probleem op te lossen is door gebruik te maken van foutverbeterende codes.

Voorbeeld 1. *De 128 ASCII-karakters worden bijvoorbeeld gecodeerd met zeven bits (0 of 1) en daaraan wordt vaak één pariteitsbit toegevoegd, op zo een manier dat de som van alle 8 bits even is. Ten hoogste één fout in de communicatie kan dan gedetecteerd (maar niet verbeterd) worden.*

Voorbeeld 2. *Een andere foutverbeterende code is de volgende: stuur het bericht drie keer. Als de ontvanger dan ten minste twee keer hetzelfde bericht ziet, kan hij aannemen dat dat het verstuurde bericht is en kunnen alle fouten in het derde bericht verbeterd worden.*

Dit zijn voorbeelden van foutverbeterende codes over het eindige lichaam $\mathbb{F}_2$. In het algemeen bestaan er ook foutverbeterende codes over grotere eindige lichamen $\mathbb{F}_q$. Het eerste voorbeeld heeft als voordeel dat er niet zo heel veel extra data verstuurd hoeft te worden. De code kan echter maar één fout detecteren (en geen eens iets verbeteren). Het tweede voorbeeld kan veel meer fouten verbeteren, maar is heel inefficiënt: er moet drie keer zoveel data verstuurd worden.

Onderzoeksvraag 1. *Stel dat we uitgaan van een foutkans van* $0 < p < 0.5$ *per verstuurde bit en dat we willen dat ons bericht met* $(100-\varepsilon)\%$ *zekerheid goed uitkomt. Welke code kan dit met zo min mogelijk extra data?*

Onderzoeksvraag 2. *Stel dat er in Voorbeeld 1 een fout is opgetreden, maar je weet niet waar. Dan zou je de verzender kunnen vragen om het hele karakter opnieuw op te sturen. Dat betekent wel 8 extra bits aan communicatie. Dit kan misschien wel efficiënter. Wat is er al bekend over* interactieve foutverbeterende codes*? Kunnen bestaande protocollen op een makkelijke manier uitgebreid worden?*

Onderzoeksvraag 3. *Er zijn foutverbeterende codes die geconstrueerd worden met behulp van algebraïsche krommen. Het efficiënt coderen van een bericht is betrekkelijk eenvoudig, maar het decoderen van een bericht met een fout erin is ingewikkelder. Hoe werkt dit? Kunnen deze algemene methodes verbeterd worden, bijvoorbeeld in het geval dat de algebraïsche kromme een elliptische kromme is?*

De student kan één van de vragen kiezen als startpunt voor de scriptie, maar hij of zij mag ook zelf een vraag voorstellen over foutverbeterende codes.

Vereiste voorkennis: Algebra 3 (eindige lichamen), Lineaire Algebra 1 & 2.

Andere voorkennis die van pas zou kunnen komen: Kansrekening en/of Besliskunde A (voor onderzoeksvragen 1 & 2), Curves over Finite Fields en/of Elliptic Curves (voor onderzoeksvraag 3).