Decoding Codes from Curves and Cyclic Codes

Iwan M. Duursma

Decoding Codes from Curves and Cyclic Codes

Proefschrift

ter verkrijging van de graad van doctor aan de Technische Universiteit Eindhoven, op gezag van de Rector Magnificus, prof. dr. J.H. van Lint, voor een commissie aangewezen door het College van Dekanen in het openbaar te verdedigen op maandag 13 September 1993 om 16.00 uur

door

Iwan Maynard Duursma

geboren te Bussum

Dit proefschrift is goedgekeurd door de promotoren
prof. dr. J. H. van Lint
en
prof. dr. H. Stichtenoth

copromotor: dr. G. R. Pellikaan

CIP-GEGEVENS KONINKLIJKE BIBLIOTHEEK, DEN HAAG

Duursma, Iwan Maynard

Decoding codes from curves and cyclic codes / Iwan Maynard
Duursma. – Eindhoven : Technische Universiteit Eindhoven
Proefschrift Eindhoven. – Met lit. opg.
ISBN 90-386-0212-X
Trefw. : coderingstheorie / algebraïsche meetkunde.

Stellingen behorende bij het proefschrift

DECODING
CODES FROM CURVES
AND CYCLIC CODES

van Iwan M. Duursma

I.

Het projectieve vlak over het lichaam $GF(8)$ bevat 73 rationale punten. Hieronder bevinden zich acht drietallen van de vorm $\{(X : Y : Z)$, $(X^2 : Y^2 : Z^2)$, $(X^4 : Y^4 : Z^4)\}$ met de eigenschap dat de drie punten niet op een lijn liggen. De overige 49 punten liggen op de zeven lijnen gedefinieerd over het lichaam $GF(2)$. De automorfismengroep van de acht drietallen en de automorfismengroep van de zeven lijnen zijn identiek (als ondergroep van de automorfismengroep van het projectieve vlak). Het zijn $L_2(7)$, respectievelijk $L_3(2)$.

II.

Zij k een lichaam van karakteristiek 2. Zij $S_i, T_i \in k[X, Y, Z]$ gedefinieerd door $S_i = X^i + Y^i + Z^i$ en $T_i = S_i + (S_1)^i$, voor $i > 0$. Zij q en r machten van 2. Er geldt

$$T_{q+1}^{r+1} + T_{r+1}^{q+1} = T_{qr+1}\, T_{q+r}.$$

III.

Zij K de Klein kromme, gedefinieerd door $K : X^3Y + Y^3Z + Z^3X = 0$ over het lichaam der rationale getallen. De 24 flexpunten van K bevinden zich in de doorsnijding met de kromme $H : X^5Z + Y^5X + Z^5Y - 5X^2Y^2Z^2 = 0$. Zij K^* de duale kromme van K. Na reductie modulo $p = 2$, factoriseert het morfisme $K \longrightarrow K^*$ als

$$K \overset{sep}{\longrightarrow} H \overset{insep}{\longrightarrow} K^*.$$

(In [Ha,p.305] wordt opgemerkt dat na reductie modulo $p = 3$, het morfisme $K \longrightarrow K^*$ volledig inseparabel is.)

[Ha] Hartshorne, R., Algebraic geometry. New York: Springer-Verlag, 1977.

IV.

De kromme met affiene vergelijking $y^2 + y = x^5$ over het lichaam $GF(16)$ heeft 32 eindige rationale punten en een punt P_∞ in oneindig. De ondergroep van de Picard groep voortgebracht door de divisoren van graad nul is elementair abels van orde 625. De elementen van de vorm $[P - P_\infty]$ en hun tweevouden, met P een eindig rationaal punt, vormen een klasse in een partitie design van regulariteit vier. Dit impliceert voor algebraïsch-meetkundige codes gedefinieerd met de kromme en de 32 rationale punten, dat ten hoogste zes verschillende gewichtsverdelingen optreden bij codes van een gegeven dimensie.

[Ca] Camion, P., Courteau, B., and Delsarte, P.,
On r-partition designs in Hamming spaces,
Applicable Algebra in Eng., Commun. and Comput., vol.2, pp.147-162, 1992.

V.

De Fermat kromme van graad m over het lichaam $GF(q^2)$ bevat ten hoogste $q^2 + 1 + (m-1)(m-2)q$ rationale punten. Het maximum wordt bereikt als $m \mid q+1$. Een elementair bewijs wordt gegeven in [We]. De classificatie van supersinguliere Fermat variëteiten [Sh] laat zien dat de voorwaarde $m \mid q+1$ noodzakelijk is voor het bereiken van het maximum. Een elementair bewijs van de noodzakelijkheid wordt gegeven in [Du]. De tabel in [Se] van maximale Fermat krommen van graad $m \leq 7$ blijkt bij toetsing aan het criterium $m \mid q+1$ niet compleet. De versie van dezelfde tabel in [Go, p.130] bevat enkele krommen die niet maximaal zijn.

[We] Weil, A., Numbers of solutions of equations in finite fields, Bull. Am. Math. Soc., vol.55, pp.497-508, 1949.

[Sh] Shioda, T., and Katsura, T., On Fermat varieties, Tôhoku Math. J., vol.31, pp.97-115, 1979.

[Du] Duursma, I.M., Afstudeerverslag, Universiteit van Amsterdam, 1989.

[Se] Segre, B., Arithmetische Eigenschaften von Galois-Räumen I, Mathematische Annalen, vol.154, pp.195-256, 1964.

[Go] Goppa, V.D., Geometry and Codes. Dordrecht: Kluwer, 1988.

VI.

Zij $\pi : Y \longrightarrow X$ een Galois overdekking met groep G van krommen over een eindig lichaam k. Voor een ondergroep H van G beschouwen we de kromme Y/H. Zij $Pic_0(Y/H)$ het homogene deel van de Picard groep van een kromme Y/H. Zij

$$\{\ ,\ \}_{H,m}\ :\ Pic_0(Y/H)_m \times Pic_0(Y/H)/mPic_0(Y/H) \longrightarrow k/k^m$$

de Tate paring, gedefinieerd als in [Fr]. De groep $Pic_0(Y)$ wordt op de groep $Pic_0(Y/H)$ afgebeeld door restrictie. Op $Pic_0(Y)_m \times Pic_0(Y)/mPic_0(Y)$ definieren we een samengestelde afbeelding

$$\langle\ ,\ \rangle_{H,m} = \{\ ,\ \}_{H,m} \cdot (Res, Res).$$

Zij $\epsilon_H \in Q[G]$ de idempotent van een ondergroep H van G, gedefinieerd als in [Ka]. Laat een relatie op de idempotenten gegeven zijn door $\sum_H a_H \epsilon_H = 0$. Er geldt

$$\prod_H \langle\ ,\ \rangle_{H,m}^{a_H}\ =\ 1.$$

[Fr] Frey, G., and Rück, H., A Remark Concerning m-Divisibility and the Discrete Logarithm in the Divisor Class Group of Curves. Essen: Institut für Experimentelle Mathematik, 1991.

[Ka] Kani, E., and Rosen, M., Idempotent relations and factors of Jacobians, Mathematische Annalen, vol.284, pp.307-327, 1989.

VII.

Het is bekend dat de zeta functie $Z_2(t)$ van een kromme gedefinieerd over een kwadratisch eindig lichaam factoriseert als $Z_2(t^2) = Z_1(t)Z_1(-t)$. De kromme met affiene vergelijking $y^2 = x^p - x + 1$ over het lichaam $GF(p^2)$, p een oneven priemgetal, heeft zeta functie

$$Z(t) = \frac{(1 \pm p^p t^p)/(1 \pm pt)}{(1-t)(1-p^2 t)}.$$

Het plusteken geldt als $p \equiv 3 \pmod 4$ en het minteken als $p \equiv 1 \pmod 4$. De factorisatie van $Z(t^2)$ is een speciaal geval van een Aurifeuillian factorisatie.

[Sc] Schinzel, A., On primitive factors of $a^n - b^n$,
Proc. Cambridge Philos. Soc., vol.58, pp.555-562, 1962.

[St] Stevenhagen, P., On Aurifeuillian factorizations,
Proc. Kon. Ned. Akad. van Wetenschappen, vol.90, pp.451-468, 1987.

VIII.

Zij $f = (X - \alpha_1)(X - \alpha_2)(X - \alpha_3)(X - \alpha_4) \in k[X]$ een deler van $X^{41} - 1$, met $k = GF(2^{20})$. Zij $S_i = \alpha_1^i + \alpha_2^i + \alpha_3^i + \alpha_4^i$, $i \geq 0$. Het is bekend dat f volledig wordt bepaald door de waarde van S_1. Met $S_0 = 0$, $S_{2i} = {S_i}^2$ en $S_{i+41} = S_i$ zijn alle elementen in de volgende matrix te berekenen, met uitzondering van S_3.

$$\begin{pmatrix} S_0 & S_{31} & S_{37} & S_{23} & S_1 \\ S_8 & S_{39} & S_4 & S_{31} & S_9 \\ S_{20} & S_{10} & S_{16} & S_2 & S_{21} \\ S_9 & S_{40} & S_5 & S_{32} & S_{10} \\ S_2 & S_{33} & S_{39} & S_{25} & S_3 \end{pmatrix}$$

Singulariteit van de matrix en regulariteit van de minor buiten S_3 geeft een vergelijking voor S_3. Een alternatieve berekening van S_3 wordt gegeven in [Re].

[Du] Duursma, I.M., and Kötter, R., Error-locating pairs for cyclic codes.
Eindhoven-Linköping: preprint, 1993.

[Re] Reed, I.S., Truong, T.K., Chen, X., and Yin, X.,
The algebraic decoding of the [41,21,9] quadratic residue code,
IEEE Trans. Inform. Theory, vol.IT-38, pp.974-986, 1992.

IX.

Zij gegeven een nevenklasse $\mathbf{y} + C$ van een algebraïsch-meetkundige code C. De oplossingsruimte van het basis decodeeralgoritme bevat functies die nul zijn op de support van een element uit de nevenklasse. Laat de nevenklasse een tweetal vectoren $\{\mathbf{e}_1, \mathbf{e}_2\}$ bevatten met de eigenschap dat het gezamenlijke aantal coördinaten dat verschilt van nul gelijk is aan de ontwerp minimumafstand van de code. De oplossingen van het basis decodeeralgoritme zijn dan te schrijven als lineaire combinatie van een functie die nul is op de niet-nul coördinaten van de eerste vector en een functie die nul is op de niet-nul coördinaten van de tweede vector. In de notatie van dit proefschrift: $K(F) = L(F - Q_1) + L(F - Q_2)$.

Samenvatting

Het proefschrift beschrijft de resultaten van mijn onderzoek aan decodeeralgoritmen voor lineaire codes. De algoritmen worden toegepast bij het corrigeren van fouten die onbedoeld optreden bij het verzenden of opslaan van informatie.

Algebraïsch-meetkundige codes (in de zin van Goppa) kennen een eenvoudig te bepalen ondergrens voor het aantal fouten dat gecorrigeerd kan worden. Deze ondergrens wordt de ontwerpcapaciteit genoemd. Bij aanvang van het onderzoek waren twee nauw verwante algoritmen beschikbaar: het basis algoritme en het gemodificeerde algoritme. Beide algoritmen zijn in het algemeen niet in staat om fouten te corrigeren tot de ontwerpcapaciteit van de code. De gemodificeerde versie corrigeert meer fouten maar is slechts toepasbaar op een beperkte klasse van codes. Voor het gemodificeerde algoritme is een formulering gevonden die het toepasbaar maakt op alle algebraïsch-meetkundige codes. Voor de gevallen waarbij de herformulering het algoritme niet wezenlijk verandert wordt bewezen dat de prestaties van het algoritme in feite beter zijn dan aanvankelijk was aangetoond. Gedurende het onderzoek suggereerden Feng en Rao een wezenlijke verbetering van de bestaande algoritmen. Hiermee kunnen fouten worden gecorrigeerd tot de ontwerpcapaciteit. In een voorpublikatie lichten zij dit toe aan de hand van een voorbeeld en ontbreekt een bewijs. Uitwerking van hun idee heeft geresulteerd in een algemeen toepasbaar algoritme met een volledig bewijs. Het huidige bewijs van Feng en Rao gaat uit van een beperkt toepasbaar algoritme, dat een groter beslag legt op computergeheugen en rekentijd.

In samenwerking met R. Kötter, werkzaam aan de universiteit van Linköping, zijn resultaten bereikt voor het decoderen van cyclische codes. Algemene stellingen worden gegeven voor het construeren van decodeeralgoritmen voor deze codes. In het bijzonder worden algoritmen gegeven die meer fouten corrigeren dan het Berlekamp-Massey algoritme als de optredende eenheidswortels verdeeld zijn over een beperkt aantal grote conjugatieklassen. De complexiteit is die van het Berlekamp-Massey algoritme. Toetsing van de stellingen aan binaire codes van lengte kleiner dan 63 leert dat alle codes op vier na gedecodeerd kunnen worden tot de werkelijke capaciteit.

Curriculum vitae

Iwan Maynard Duursma was born on April 19, 1963, in Bussum. He attended the rijksscholengemeenschap Schoonoord in Zeist and completed the gymnasium in 1980. From September 1980 till August 1986, he studied aerospace engineering at the Technische Hogeschool Delft and graduated with the minor thesis: Satellite orbit perturbations due to tidal forces (cum laude, professor K.F. Wakker). From September 1983 till February 1989, he studied mathematics at the Universiteit van Amsterdam and graduated with the minor thesis: Some remarks on Goppa codes (cum laude, professor G. van der Geer).
During his study, he was appointed as student assistant (for September 1985 – April 1987, by professor H.W. Lenstra jr., and for January 1988 – November 1988, by A.M. Cohen). While applying for a position as a Ph.D. student, he was a full-time teacher of mathematics at the Instituut Blankestijn in Utrecht. Since September 1990, he has worked in the Discrete Mathematics group at the Technische Universiteit Eindhoven, with support from the Netherlands Organization for Scientific Research.