

Fejlkorrigerende koder
Toriske varieteter, specielt Hirzebruch flader

Johan P. Hansen,
matjph@imf.au.dk
Matematisk Institut, Aarhus Universitet

Trondheim, den 18. Oktober 2002

Informationsoverførsel. Et problem? **JA** En løsning? **JA**

Binær symmetrisk kanal: Sandsynligheden for korrekt overførsel af 1 bit er p , $0 \leq p \leq 1$.

	0	1
0	p	$1 - p$
1	$1 - p$	p

Hvis $p = \frac{999}{1000}$, så overføres 10000 bits korrekt med sandsynligheden $\left(\frac{999}{1000}\right)^{10000} = 0,0000452$. **Ubrugeligt** - modtageren ved end ikke, om der er opstået fejl.

Blok kode strategi:

- del budskabet op i blokke af længde k
- til hver blok knyttes ekstra kontrolbits, så blokken vokser til længde N
- send blokkene af længde N
- udnyt den ekstra information til af afsløre og rette fejl

Blok kode eksempel - Paritetscheck. $k = 7$. En ekstra bit, der er summen af de øvrige 7 tilføjes, så $N = 8$. Kan afsløre op til 1 fejl i et kodet ord (længde 8)

Sandsynligheden for 0 fejl i et kodeord er

$$\left(\frac{999}{1000}\right)^8 = 0,992028.$$

Sandsynligheden for 1 fejl i et kodeord er

$$8 * \left(\frac{999}{1000}\right)^7 * \left(\frac{1}{1000}\right) = 0,007944.$$

Sandsynligheden for højst 1 fejl (altså ingen ikke opdagede fejl) i et kodeord er således

$$0,992028 + 0,007944 = 0,999972$$

Sandsynligheden for ingen ikke opdagede fejl i budskabet på 10000 bits

$$0,999972^{\frac{10000}{7}} = 0,960942.$$

Prisen: send 8 bits for hver 7 bits af budskabet. **Merprisen mindre end 15%.**

Shannon

<http://www.ams.org/notices/200201/fea-shannon.pdf>

<http://www.ams.org/notices/200201/fea-berlekamp.pdf>

I 1948 lagde Shannon det matematiske grundlag for informationsteori. Han knyttede til enhver kanal en *kapacitet C* og viste, at *ved passende kodning kan kanalen transmittere med $\frac{k}{N}$ vilkårlig tæt på C og vilkårlig lav fejlsandsynlighed.*

For den binære symmetriske kanal er

$$C(p) = 1 + p \log_2 p + (1 - p) \log_2(1 - p).$$

I eksemplet med $p = \frac{999}{1000}$ bliver kapaciteten $C(p) = 0,988592$. Ved passende kodning kan der altså transmitteres med $\frac{k}{N}$ tæt på 0,988592 med vilkårlig lav fejlsandsynlighed.

$$\frac{N}{k} = \frac{1}{0,988592} = 1,011539,$$

merprisen er mindre end 2%!

Lineære koder

\mathbb{F} legeme med l elementer.

$$V \subset \mathbb{F}^N$$

Længde N

Dimension $k = \dim V$

Minimumsafstand d : to ord er forskellige i mindst d positioner.

Singleton grænsen

$$\frac{k}{N} + \frac{d}{N} \leq 1 + \frac{1}{N} \quad (1)$$

Reed-Solomon koden er billedet $\phi(L_m) \subset \mathbb{F}^l$ af evalueringsafbildningen:

$$\begin{aligned} \phi : L_m := \text{Span}\{1, x, x^2, \dots, x^m\} &\rightarrow \mathbb{F}^l \\ f &\mapsto (f(a_1), \dots, f(a_l)), \quad \mathbb{F} = \{a_1, \dots, a_l\} \end{aligned}$$

fra \mathbb{F} vektorrummet af polynomier af grad højst m .

- Har effektive afkodningsalgoritmer (Berlekamp)
- burst-error kapacitet
- utallige anvendelser (CD,DVD, computer hukommelse, deep-space kommunikation)
- special tilfælde af [Goppa koder](#), som kommer fra algebraisk geometri

Reed-Solomon koder - parametre

Koden $\phi(L_m)$, $m < l$ har kendte parametre:

- **længde** $N = l$
- **dimensionen** $k = m + 1$
- **minimumsafstanden** $d = l - m$

(Anvend, at antallet af rødder i et polynomium højst er lig med polynomiets grad).

Vi rammer altså netop **singleton grænsen**

$$\frac{k}{N} + \frac{d}{N} = 1 + \frac{1}{N} \quad (2)$$

Bedre kan det ikke gøres, men koden er **ikke** lang.

Kurver, genus og punktantal - definitioner

Lad \mathbb{F} være et endeligt legeme med l elementer.

En *kurve* C over \mathbb{F} er defineret ved ligninger:

$$f(X_1, \dots, X_n) = 0, \quad (3)$$

hvor $f(X_1, \dots, X_n) \in \mathbb{F}[X_1, \dots, X_n]$ er polynomier i flere variable med koefficienter i \mathbb{F} .

- g - kurvens *genus*. Kan bestemmes ud fra ligningerne (3) på en normalt ikke simpel måde. En linie har genus 0.
- N - *punktantallet* (over \mathbb{F}) på kurven - altså antallet (talt rigtigt) af n -tupler

$$(x_1, \dots, x_n),$$

der er løsninger til (3) med $x_i \in \mathbb{F}$. En (affin) linie defineret over \mathbb{F} har l punkter (over \mathbb{F}), den (projektive) linie har $1 + l$.

Goppa gav omkring 1981 en konstruktion af koder udfra algebraiske kurver - der er en generalisering af Reed-Solomon koder.

Funktionerne i et \mathbb{F} -vektorum L af (polynomier/rationale) funktioner evalueres i punkterne P_1, \dots, P_N på en kurve C med koordinater i \mathbb{F} :

$$\begin{aligned}\phi : L &\rightarrow \mathbb{F}^N \\ f &\mapsto (f(P_1), \dots, f(P_N))\end{aligned}$$

Goppa koden er billedet:

$$\phi(L) \subset \mathbb{F}^N$$

Koden har *længde* N . Ved passende valg af L kan kodens *dimension* k og *minimumsafstand* d bestemmes/vurderes (Riemann-Roch) så

$$1 + \frac{1}{N} - \frac{g}{N} \leq \frac{k}{N} + \frac{d}{N} \leq 1 + \frac{1}{N} \quad (4)$$

- hvis $g = 0$ får vi lighedstegn (Reed-Solomon koder, jvf. (2))
- hvis $\frac{g}{N}$ er lille ($\frac{N}{g}$ stor), så får vi koder, der er næsten ligeså gode
- Lange koder, hvis N er stor, altså kurven har mange punkter over \mathbb{F}

Find kurver med mange punkter i forhold til genus!

Eks.: Hermite kurven $l = q^2$

Kurven har ligning:

$$y^q + y = x^{q+1}$$

Genus $g = \frac{q^2 - q}{2}$ og punktantallet $N = q^3$.

L_m er vektorrummet af funktioner med basis

$$x^i y^j,$$

hvor

$$0 \leq i, 0 \leq j \leq q - 1, iq + j(q + 1) \leq m.$$

Koden $\phi(L_m)$ har kendte parametre. Er for eksempel $q^2 - q \leq m < q^3$, så er:

- dimensionen $m - g + 1$
- minimumsafstanden $N - m$

Vi rammer altså netop undergrænsen i estimatet (4).

Forholdet mellem g og N .

Hasse-Weil siger, at N cirka er $1 + l$:

$$1 + l - 2g\sqrt{l} \leq N \leq 1 + l + 2g\sqrt{l}$$

Det indebærer, at for fast g er der en øvre grænse for N . Skal vi have kurver med stort N , må g altså tillades at vokse. Af Hasse-Weil følger direkte, at

$$\lim \frac{N}{g} \leq 2\sqrt{l}.$$

Det er langt fra optimalt. Denne øvre grænse er faktisk dobbelt for stor.

Drinfeld-Vladut siger nemlig, at for $l = q^2$ er

$$\lim \frac{N}{g} \leq \sqrt{l} - 1 = q - 1,$$

hvilket er meget bedre. Faktisk kan det gøres bedre.

Tsfasman, Vladut og Zink - Ihara viste i 1981/1982, at for $l = q^2$ er

$$\lim \frac{N}{g} = \sqrt{l} - 1 = q - 1 \quad (5)$$

beviset beror på meget abstrakt algebraisk geometri. De indgående familier af kurver er såkaldt modulære kurver. Konstruktionen er **ikke** eksplicit.

Garcia og Stichtenoth konstruerede imidlertid i 1995 eksplicit en familie af kurver, så (5) realiseres. Ligningerne:

$$\begin{aligned} (x_1^{q-1} + 1)(x_2^q + x_2) &= x_1^q \\ (x_2^{q-1} + 1)(x_3^q + x_3) &= x_2^q \\ &\dots \\ (x_{n-1}^{q-1} + 1)(x_n^q + x_n) &= x_{n-1}^q \end{aligned}$$

definerer en sådan familie af kurver C_n over \mathbb{F} , hvor $l = q^2$.

JPH, *Toric Varieties Hirzebruch Surfaces and Error-Correcting Codes*, AAEECC (Applicable Algebra in Engineering, Communication and Computing), Springer-Verlag 2002, to appear.

Resumé

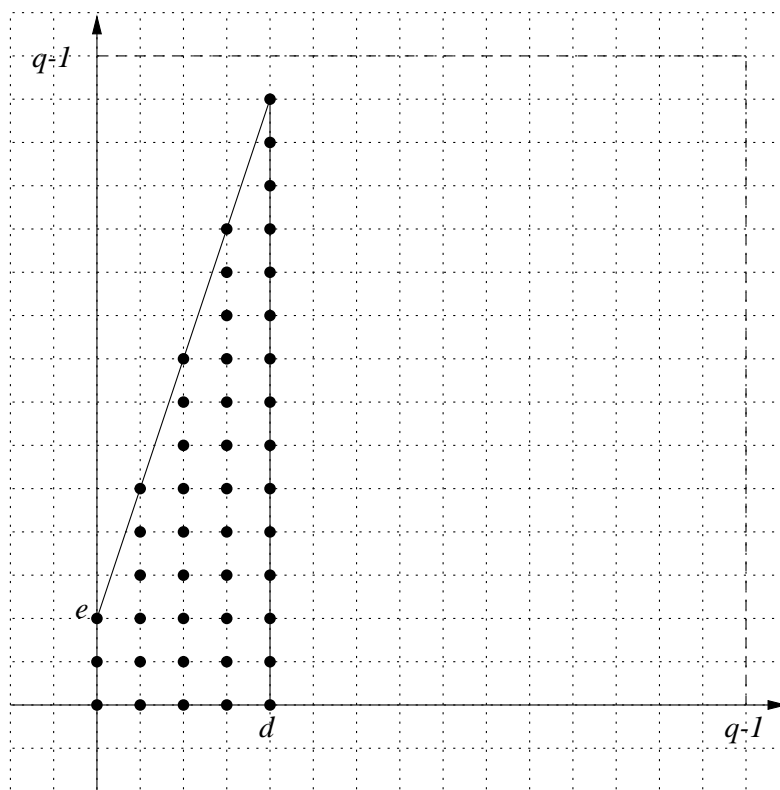
For any integral convex polytope in \mathbb{R}^2 there is an explicit construction of an error-correcting code of length $(q - 1)^2$ over the finite field \mathbb{F}_q , obtained by evaluation of rational functions on a toric surface associated to the polytope. The dimension of the code is equal to the number of integral points in the given polytope and the minimum distance is determined using the cohomology and intersection theory of the underlying surfaces. In detail we treat Hirzebruch surfaces.

Toriske koder

Lad $M \simeq \mathbb{Z}^2$ være en \mathbb{Z} -modul af rank 2 over de hele tal \mathbb{Z} .

Lad \square være en integral konveks polytop i $M_{\mathbb{R}} = M \otimes_{\mathbb{Z}} \mathbb{R}$.

Eks. Polytop med hjørner $(0, 0)$, $(d, 0)$, $(d, e + rd)$, $(0, e)$.



Toriske koder

$\xi \in \mathbb{F}_q$ et primitivt element.

$$P_{ij} = (\xi^i, \xi^j) \in \mathbb{F}_q^* \times \mathbb{F}_q^*.$$

m_1, m_2 være en \mathbb{Z} -basis for M .

For $m = \lambda_1 m_1 + \lambda_2 m_2 \in M \cap \square$:

$$\mathbf{e}(m)(P_{ij}) = (\xi^i)^{\lambda_1} (\xi^j)^{\lambda_2}.$$

Den toriske kode C_\square er den lineære kode af længde $n = (q - 1)^2$ frembragt af:

$$\{(\mathbf{e}(m)(P_{ij}))_{i=0, \dots, q-1; j=0, \dots, q-1} \mid m \in M \cap \square\}.$$

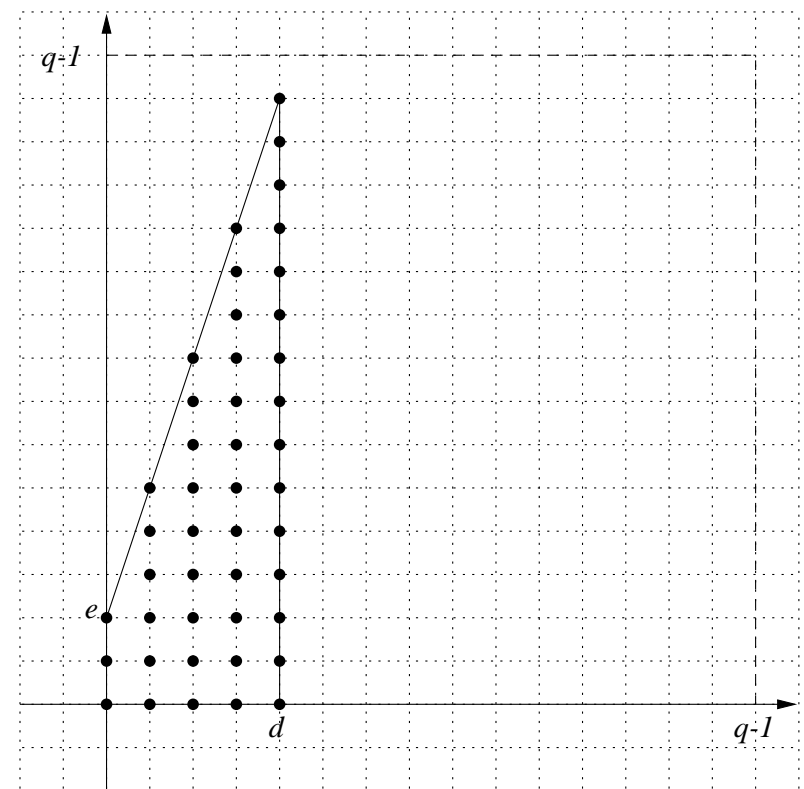
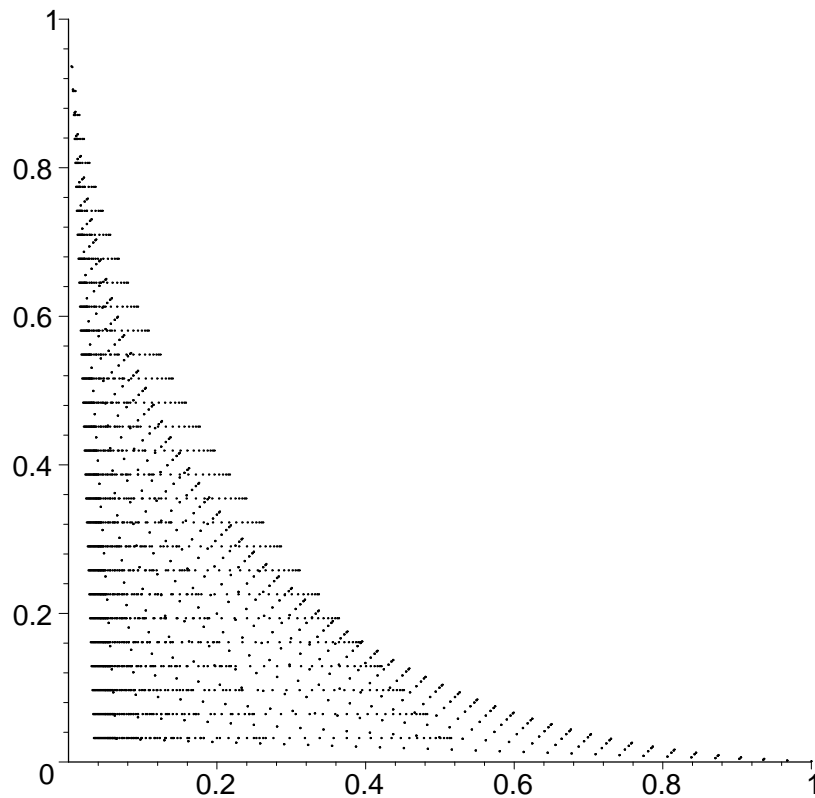
Funktionerne i et \mathbb{F} -vektorummet $L = \text{Span}\{\mathbf{e}(m) \mid m \in M \cap \square\}$ evalueres i punkterne P_{ij} , $i = 0, \dots, q - 1; j = 0, \dots, q - 1$ på en torus $\mathbb{F}_q^* \times \mathbb{F}_q^*$:

$$\begin{aligned} \phi : L = \text{Span}\{\mathbf{e}(m) \mid m \in M \cap \square\} &\rightarrow \mathbb{F}^{(q-1)^2} \\ f &\mapsto (f(P_{ij}))_{i=0, \dots, q-1; j=0, \dots, q-1} \end{aligned}$$

(7)

Sætning

Polytopen \square i $M_{\mathbb{R}}$ med hjørner $(0, 0)$, $(d, 0)$, $(d, e + rd)$, $(0, e)$. Antag $d < q - 1$, $e < q - 1$ og $e + rd < q - 1$. Den toriske kode C_{\square} har **længde** $(q - 1)^2$, **dimension** $\#(M \cap \square) = (d + 1)(e + 1) + r \frac{d(d+1)}{2}$ (antallet af gitterpunkter i \square) og **minimums afstanden** $\text{Min}\{(q - 1 - d)(q - 1 - e), (q - 1)(q - 1 - e - rd)\}$.



$$x = \frac{\text{dimension}}{\text{length}}, y = \frac{\text{minimal distance}}{\text{length}}, (q = 32)$$

Toriske varieteter - støttefunktion

M heltalsgitter $M \simeq \mathbb{Z}^2$.

$N = \text{Hom}_{\mathbb{Z}}(M, \mathbb{Z})$ det duale gitter med \mathbb{Z} - bilinear parring
 $\langle \cdot, \cdot \rangle: M \times N \rightarrow \mathbb{Z}$.

\square en 2-dimensional integral konveks polytop i $M_{\mathbb{R}} = M \otimes_{\mathbb{Z}} \mathbb{R}$.

Støttefunktionen

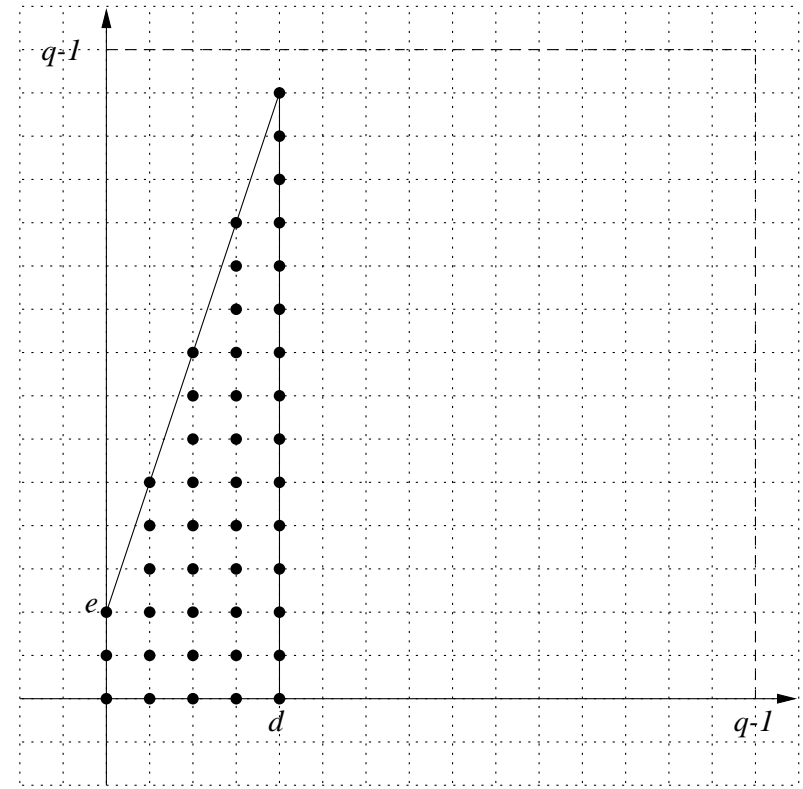
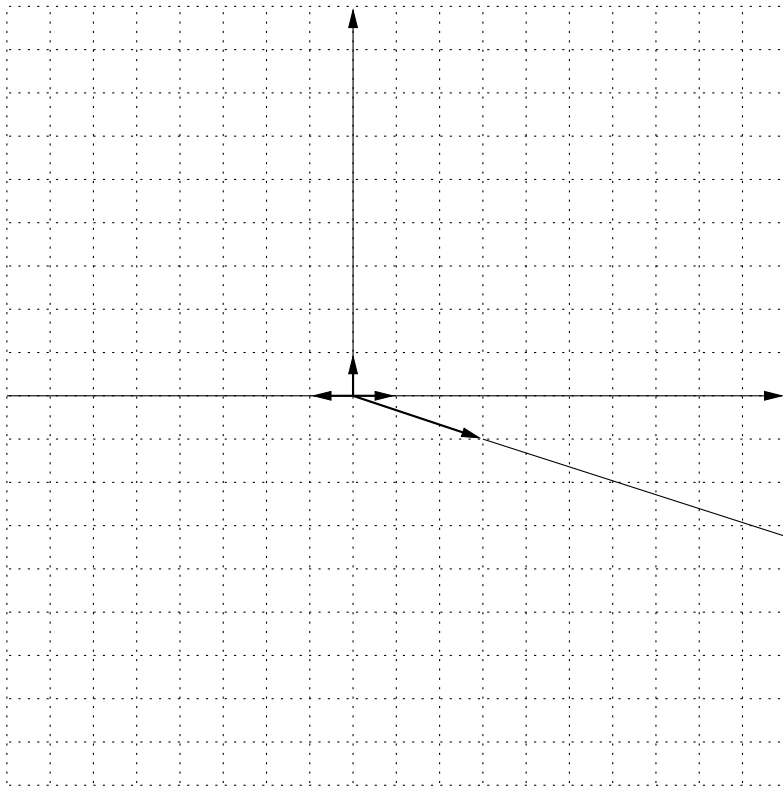
$$h_{\square} : N_{\mathbb{R}} = N \otimes_{\mathbb{Z}} \mathbb{R} \rightarrow \mathbb{R}$$

$$h_{\square}(n) := \inf\{\langle m, n \rangle \mid m \in \square\}$$

og \square kan rekonstrueres:

$$\square_h = \{m \in M \mid \langle m, n \rangle \geq h(n) \quad \forall n \in N\}.$$

Støttefunktionen er stykkevis lineær i den forstand, at $N_{\mathbb{R}}$ er foreningen af endelig mange polyhedrale kegler i $N_{\mathbb{R}}$ og h_{\square} er lineær på hver kegle.



Frembringere for de 1-dimensionale kegler:

$$n(\rho_1) = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, n(\rho_2) = \begin{pmatrix} 0 \\ 1 \end{pmatrix}, n(\rho_3) = \begin{pmatrix} -1 \\ 0 \end{pmatrix}, n(\rho_4) = \begin{pmatrix} r \\ -1 \end{pmatrix}$$

Torisk varietet - definition

$T_N := \text{Hom}_{\mathbb{Z}}(M, \overline{\mathbb{F}}_q^*) \simeq \overline{\mathbb{F}}_q^* \times \overline{\mathbb{F}}_q^*$ er en 2-dimensional **algebraisk torus**.

$\mathbf{e}(m) : T \rightarrow \overline{\mathbb{F}}_q^*$, $m \in M$ defineret som $\mathbf{e}(m)(t) = t(m)$ for $t \in T_N$ er en **multiplikativ karakter**.

Den **toriske flade** X_{\square} knyttet til \square er

$$X_{\square} = \cup_{\sigma \in \Delta} U_{\sigma}$$

U_{σ} er de $\overline{\mathbb{F}}_q$ -valued punkter på det affine schema $\text{Spec}(\overline{\mathbb{F}}_q[S_{\sigma}])$, altså

$$U_{\sigma} = \{u : S_{\sigma} \rightarrow \overline{\mathbb{F}}_q \mid u(0) = 1, u(m + m') = u(m)u(m') \forall m, m' \in S_{\sigma}\},$$

hvor S_{σ} is the additive undersemigruppe af M

$$S_{\sigma} = \{m \in M \mid \langle m, y \rangle \geq 0 \forall y \in \sigma\}.$$

X_{\square} er irreducibel, (glat) og komplet.

T_N virker algebraisk på X_\square . På $u \in U_\sigma$ virker $t \in T_N$ således

$$(tu)(m) := t(m)u(m) \quad m \in S_\sigma$$

For $\sigma \in \Delta$

$$\text{orb}(\sigma) := \{u : M \cap \sigma \rightarrow \overline{\mathbb{F}}_q^* \mid u \text{ is a group homomorphism}\}$$

er en T_N bane X_\square . $V(\sigma)$ defineres til at være aflukningen $\text{orb}(\sigma)$ in X_\square .

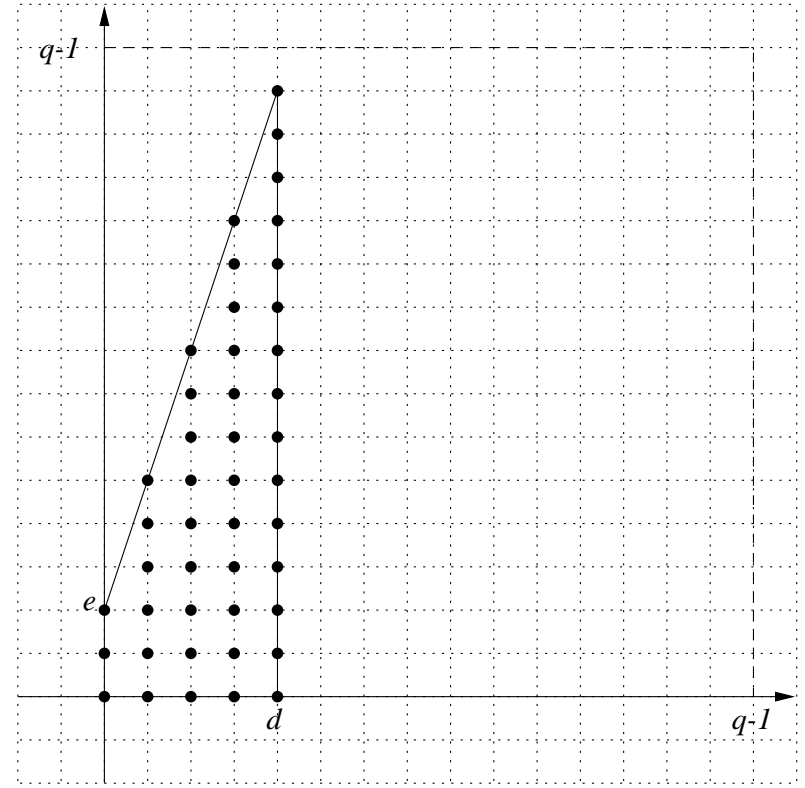
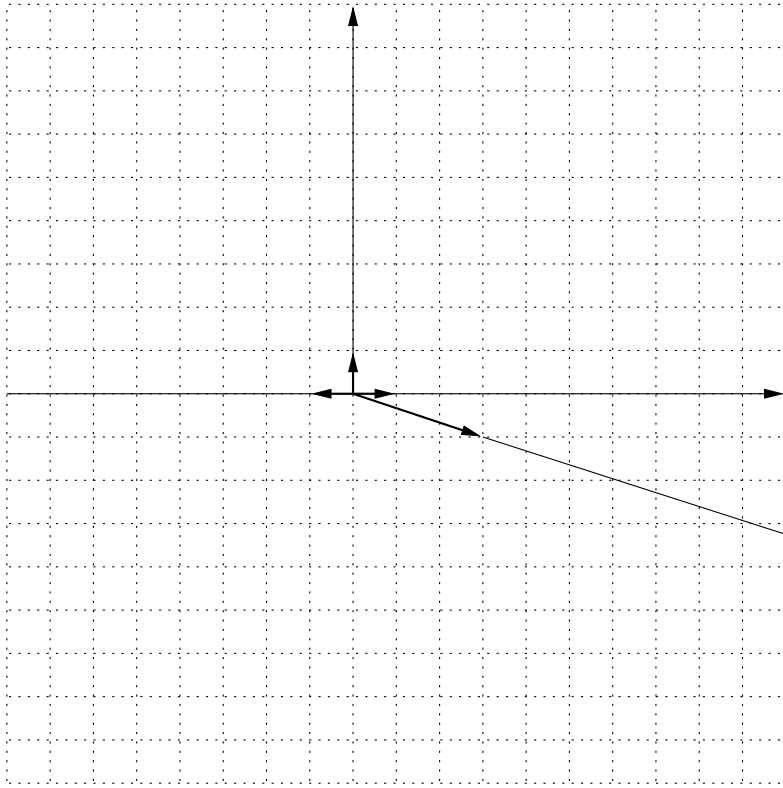
En Δ -lineær støttefunktion h giver anledning til en **Cartier divisor** D_h :

$$D_h := - \sum_{\rho \in \Delta(1)} h(n(\rho)) V(\rho).$$

$$D_m = \text{div}(\mathbf{e}(-m)) \quad m \in M.$$

hvor $\Delta(1)$ er de 1-dimensionale kegler i Δ .

Lemma 1. *Vektorrummet $H^0(X, O_X(D_h))$ af globale sektioner af $O_X(D_h)$, har dimension $\#(M \cap \square_h)$ og $\{\mathbf{e}(m) \mid m \in M \cap \square_h\}$ er en basis.*



$$D_h := - \sum_{\rho \in \Delta(1)} h(n(\rho)) V(\rho) = dV(\rho_3) + eV(\rho_4)$$

$$\dim H^0(X, O_X(D_h)) = (d+1)(e+1) + r \frac{d(d+1)}{2}.$$

Toriske flader - Snitteori

Lad D_h være en Cartier divisor og lad \square_h være den tilhørende polytop. Så er

$$(D_h; D_h) = 2 \operatorname{vol}_2(\square_h),$$

hvor vol_2 er det normaliserede Lesbesgue-mål.

I vort eksempel bliver [snit-tabellen](#)

	$V(\rho_1)$	$V(\rho_2)$	$V(\rho_3)$	$V(\rho_4)$
$V(\rho_1)$	$-r$	1	0	1
$V(\rho_2)$	1	0	1	0
$V(\rho_3)$	0	1	r	1
$V(\rho_4)$	1	0	1	0

Bestemmelse af parametre

For $t \in T \simeq \overline{\mathbb{F}}_q^* \times \overline{\mathbb{F}}_q^*$, rationale funktioner i $H^0(X, O_X(D_h))$ kan evalueres

$$\begin{aligned} H^0(X, O_X(D_h)) &\rightarrow \overline{\mathbb{F}}_q^* \\ f &\mapsto f(t). \end{aligned}$$

$H^0(X, O_X(D_h))^{\text{Frob}}$ de Frobenius invariante funktioner i $H^0(X, O_X(D_h))$ (funktioner som er \mathbb{F}_q -linearkombinationer af $(\mathbf{e})(m)$).

Evaluering i samtlige punkter i $T(\mathbb{F}_q)$ giver koden C_{\square} :

$$\begin{aligned} H^0(X, O_X(D_h))^{\text{Frob}} &\rightarrow C_{\square} \subset (\mathbb{F}_q^*)^{\#T(\mathbb{F}_q)} \\ f &\mapsto (f(t))_{t \in T(\mathbb{F}_q)} \end{aligned}$$

og frembringere for koden er billederne af basen:

$$\mathbf{e}(m) \mapsto (\mathbf{e}(m)(t))_{t \in T(\mathbb{F}_q)}.$$

Lad $m_1 = (1, 0)$. De \mathbb{F}_q -rationale punkter på $T \simeq \overline{\mathbb{F}}_q^* \times \overline{\mathbb{F}}_q^*$ ligger på $q - 1$ linier på X_\square givet ved $\prod_{\eta \in \mathbb{F}_q} (\mathbf{e}(m_1) - \eta) = 0$.

Lad $0 \neq f \in H^0(X, O_X(D_h))$ og antag, at f er (identisk) nul netop på a af disse linier. Da $\mathbf{e}(m_1) - \eta$ og $\mathbf{e}(m_1)$ har samme pol-divisor, har de ækvivalente nulpunktsdivisorer, så

$$(\operatorname{div}(\mathbf{e}(m_1) - \eta))_0 \sim (\operatorname{div}(\mathbf{e}(m_1)))_0.$$

Derfor er

$$\operatorname{div}(f) + D_h - a(\operatorname{div}(\mathbf{e}(m_1)))_0 \geq 0$$

eller ækvivalent

$$f \in H^0(X, O_X(D_h - a(\operatorname{div}(\mathbf{e}(m_1)))_0)).$$

Det indebærer, at $a \leq d$ ifølge Lemma 1 om cohomology.

På enhver af de øvrige $q - 1 - a$ linier er antallet af nulpunkter for f højst snittallet:

$$(D_h - a(\operatorname{div}(\mathbf{e}(m_1)))_0; (\operatorname{div}(\mathbf{e}(m_1)))_0).$$

Beregnes let ved hjælp af snittabellen ovenfor og observationen $(\operatorname{div}(\mathbf{e}(m_1)))_0 = V(\rho_1) + rV(\rho_4)$. Vi får

$$(D_h - a(\operatorname{div}(\mathbf{e}(m_1)))_0; (\operatorname{div}(\mathbf{e}(m_1)))_0) = e + (d - a)r.$$

Da $0 \leq a \leq d$ er det totale antal (rationale) nulpunkter for f højst

$$a(q - 1) + (q - 1 - a)(e + (d - a)r) \leq \max\{d(q - 1) + (q - 1 - d)e, (q - 1)(e + dr)\}.$$

Derfor er

$$\begin{aligned} H^0(X, O_X(D_h))^{\operatorname{Frob}} &\rightarrow C_{\square} \subset (\mathbb{F}_q^*)^{\#T(\mathbb{F}_q)} \\ f &\mapsto (f(t))_{t \in T(\mathbb{F}_q)} \end{aligned}$$

og dimension og nedre grænsen for minimumsafstanden som angivet i sætningen.

Sande minimumsafstand

Lad $b_1, \dots, b_{e+rd} \in \mathbb{F}_q^*$ være parvis forskellige elementer. Funktionen

$$x^d(y - b_1) \cdots (y - b_{e+rd}) \in H^0(X, O_X(D_h))^{\text{Frob}}$$

er nul i de $(q - 1)(e + rd)$ punkter

$$(x, b_j), x \in \mathbb{F}_q^*, \quad j = 1, \dots, e + rd$$

and giver et kodeord af vægt

$$(q - 1)^2 - (q - 1)(e + rd) = (q - 1)(q - 1 - (e + rd)).$$

Lad $a_1, \dots, a_d \in \mathbb{F}_q^*$ være parvis forskellige elementer og lad $b_1, \dots, b_e \in \mathbb{F}_q^*$ være parvis forskellige elementer. Funktionen

$$(x - a_1) \cdots (x - a_d)(y - b_1) \cdots (y - b_e) \in H^0(X, O_X(D_h))^{\text{Frob}}$$

er nul i de $d(q - 1) + (q - 1)e - de$ points

$$(a_i, y), (x, b_j), \quad x, y \in \mathbb{F}_q^*, i = 1, \dots, d, j = 1, \dots, e$$

og giver et kodeord af vægt $(q - 1 - d)(q - 1 - e)$.

Litteratur

- [1] W. Fulton, “Introduction to Toric Varieties, @, Princeton University Press, 1993.
- [2] W. Fulton, “Intersection theory” *Ergebnisse der Mathematik und ihrer Grenzgebiete, 3. Folge, Springer Verlag, 1998.*
- [3] J. P. Hansen, “Toric Surfaces and Error-correcting codes,” in Coding theory, cryptography and related areas (Guanajuato, 1998), 132-142, Springer, Berlin, 2000
- [4] J. P. Hansen, “Hirzebruch surfaces and Error-correcting Codes, @
- [5] Hansen, Søren Have, “Error-correcting codes from higher-dimensional varieties,” *Finite Fields Appl.*; no 7, 2001, 531–552
- [6] Joyner, David, “Toric codes over finite fields,” Preprint, Aug. 2002, <http://front.math.ucdavis.edu/math.AG/0208155>
- [7] T. Oda, “Convex Bodies and Algebraic Geometry, An Introduction to the Theory of Toric Varieties, @, Springer Verlag, 1985.