$$= \max \; p^n \hat{a}(0)$$

$$\hat{a}(z) \geq 0 \quad , \quad z \in \mathbb{F}_p^n$$

$$\sum_z \hat{a}(z) = 1$$

$$\sum_z \hat{a}(z) \chi_z(x) = 0 \quad , \quad \text{falls } w(x) \in \{1, \dots, d-1\}$$

2. Schritt Dualisiere LP

$$A_p(n,d) \leq \min \alpha_0$$

$$\alpha_0, \alpha_x \in \mathbb{R} \quad x \in \mathbb{F}_p^n, \; w(x) \in \{1, \dots, d-1\}.$$

$$\alpha_0 + \sum_x \alpha_x \geq p^n$$

$$\alpha_0 + \sum_x \alpha_x \chi_z(x) \geq 0 \quad , \quad z \in \mathbb{F}_p^n \setminus \{0\}.$$

3. Schritt Fasse Variablen zusammen → LP linear groß

Für $k = 1, \dots, d-1$ setze $\beta_k = \alpha_x$ für alle x mit $w(x) = k$, $\beta_0 = \alpha_0$.

Dann

$$A_p(n,d) \leq \min \beta_0$$

$$\beta_0, \beta_1, \dots, \beta_{d-1}$$

$$\beta_0 + \sum_{k=1}^{d-1} (p-1)^k \binom{n}{k} \beta_k \geq p^n$$

$$\beta_0 + \sum_{k=1}^{d-1} \beta_k \underbrace{\sum_{w(x)=k} \chi_z(x)}_{=?} \geq 0 \quad , \quad z \in \mathbb{F}_p^n \setminus \{0\}.$$

Def.: Krawtchouk-Polynom

$$K_k(x) = \sum_{j=0}^{k} (-1)^j \binom{x}{j} \binom{n-x}{k-j} (p-1)^{k-j},$$

wobei $\binom{x}{j} = \frac{x(x-1)\cdots(x-j+1)}{j!}$

Lemma Sei $z \in \mathbb{F}_p$. Für $k = w(z)$ gilt

$$K_k(k) = \sum_{\substack{x \\ w(x)=k}} \chi_z(x)$$

Bew.: → Aufgabe (ähnlich zum Beweis der MacWilliams-Identität)

Zusammen:

Theorem (Delsarte, LP-Schranke)

$$A_p(n,d) \leq \min \beta_0$$

$$\beta_0, \dots, \beta_{d-1} \in \mathbb{R}$$

$$\beta_0 + \sum_{k=1}^{d-1} (p-1)^k \binom{n}{k} \beta_k \geq p^n$$

$$\beta_0 + \sum_{k=1}^{d-1} \beta_k K_k(i) \geq 0, \quad i = 1, \dots, n.$$

Etwas mehr zu den Krawtchouk-Polynomen

Bsp.: $K_0(x) = 1$

$$K_1(x) = \binom{x}{0}\binom{n-x}{1}(p-1)^1 - \binom{x}{1}\binom{n-x}{0}(p-1)^0$$

$$= (n-x)(p-1) - x = -px + n(p-1) \overset{(p=2)}{=} -2x + n$$

$$K_2(x) = \binom{x}{0}\binom{n-x}{2}(p-1)^2$$

$$- \binom{x}{1}\binom{n-x}{1}(p-1)^1$$

$$+ \binom{x}{2}\binom{n-x}{0}(p-1)^0$$

$$\overset{(p=2)}{=} \frac{(n-x)(n-x-1)}{2} - x(n-x) + \frac{x(x-1)}{2}$$

$$= 2x^2 - 2nx + \binom{n}{2}$$

Lemma (Orthogonalitätsrelation von Krawtchouk-Polynomen)

$$\sum_{i=0}^{n} \underbrace{\binom{n}{i}(p-1)^i}_{\text{Gewicht}} K_k(i) K_\ell(i) = \delta_{k\ell}\binom{n}{k}(p-1)^k p^n$$

Bew: → Aufgabe

```
// MAGMA Code zur Berechnung von Krawtchouk Polynomen
//
// MAGMA Online Calculator: http://magma.maths.usyd.edu.au/calc/
//

Q := RationalField();
P<x,q,n> := PolynomialRing(Q,3);

function binom(p,j)
  out := P!1;
  for i := 0 to j-1 do
    out := out*(p-i);
  end for;
  return out/Factorial(j);
end function;

Krawtchouk := [];

m := 2;
for k := 0 to m do
  K := P!0;
  for j := 0 to k do
    K := K + (-1)^j * binom(x,j) * binom(n-x,k-j) * (q-1)^(k-j);
  end for;
  Append(~Krawtchouk,K);
end for;

Krawtchouk;
```

Anwendung der LP-Schranke

→ Exakte Bestimmung von $A_q(n,d)$ für kleine Werte von q, n, d.

Siehe Tabelle von Andries Brouwer (Eindhoven)

www.win.tue.nl/~aeb/codes/binary-1.html

Hier: Nur der Fall $A_2(11,6) = 12$

→ Alternativer Beweis der Plotkin-Schranke

→ Beste bekannte asymptotische Schranken

von den "four Americans":

McEliece, Rodemich, Rumsey, Welch (1977)

(möglicher Seminarthema)

 (von Andries Brouwer)

1. Table of general binary codes

The table below gives upper and lower bounds for $A_2(n,d)$, the maximum number of vectors in a binary code of word length n and with Hamming distance d.

If $d > n$ then this maximum is 1.
Otherwise, if $3d/2 > n$ then this maximum is 2.
If $d = 1$ then this maximum is 2^n.
If $d = 2$ then this maximum is $2^{(n-1)}$.
Furthermore, $A_2(n-1,2e-1) = A_2(n,2e)$.

Thus, in the table below we may restrict ourselves to even d, between 4 and $2n/3$. Horizontally we give d, vertically n.

	d=4	d=6	d=8	d=10	d=12	d=14	d=16
6	4	2	1	1	1	1	1
7	8	2	1	1	1	1	1
8	16	2	2	1	1	1	1
9	20	4	2	1	1	1	1
10	40	6	2	2	1	1	1
11	72	12	2	2	1	1	1
12	144	24	4	2	2	1	1
13	256	32	4	2	2	1	1
14	512	64	8	2	2	2	1
15	1024	128	16	4	2	2	1
16	2048	256	32	4	2	2	2
17	2816-3276	256-340	36	6	2	2	2
18	5632-6552	512-673	64-72	10	4	2	2
19	10496-13104	1024-1237	128-135	20	4	2	2
20	20480-26168	2048-2279	256	40	6	2	2
21	40960-43688	2560-4096	512	42-47	8	4	2
22	81920-87333	4096-6941	1024	64-84	12	4	2
23	147456-172361	8192-13674	2048	80-150	24	4	2
24	294912-344308	16384-24106	4096	128-268	48	6	4
25	2^{19}-599184	16384-47538	4096-5421	192-466	52-55	8	4
26	2^{20}-1198368	32768-84260	4104-9275	384-836	64-96	14	4
27	2^{21}-2396736	65536-157285	8192-17099	512-1585	128-169	28	6
28	2^{22}-4792950	131072-291269	16384-32151	1024-2817	178-288	56	8

Satz Es gilt $A_2(10,5) = A_2(11,6) = 12$.

Bew: 1) $A_2(10,5) = A_2(11,6)$

Bew: Sei C ein $(10, A_2(10,5), 5)$-Code.

Dann besitzt der **erweiterte Code**

$$\overline{C} = \{ (x_1, \dots, x_{11}) \in \mathbb{F}_2^{11} : (x_1, \dots, x_{10}) \in C, \sum_{i=1}^{11} x_i = 0 \}$$

Minimaldistanz 6. D.h. $A_2(10,5) \leq A_2(11,6)$.

Sei umgekehrt C ein $(11, A_2(11,6), 6)$-Code.

Dann besitzt der **punktierte Code**

$$\dot{C} = \{ (x_1, \dots, x_{10}) \in \mathbb{F}_2^{10} : \exists\, x_{11} \in \mathbb{F}_2 : (x_1, \dots, x_{11}) \in C \}$$

Minimaldistanz ≥ 5. D.h. $A_2(10,5) \geq A_2(11,6)$.

Insbesondere können wir annehmen, dass bei einem optimalen $A_2(11,6)$-Code keine ungeraden Abstände zwischen Codewörtern auftreten.

2) $A_2(11,6) \geq 12$

Bew.: durch Angabe einer Konstruktion.

Def.: Eine Matrix $H \in \{-1,+1\}^{n \times n}$ heißt Hadamard-Matrix, falls $H H^T = nI$ gilt.

Bsp. $H_1 = (1)$, $H_2 = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$

$$H_{2n} = \begin{pmatrix} H_n & H_n \\ H_n & -H_n \end{pmatrix}$$

Wissen: Falls H_n eine Hadamard-Matrix ist, dann ist $n = 1, 2$, oder n ist ein Vielfaches von 4.

Vermutung: Falls $4 \mid n \Rightarrow$ Hadamard-Matrix der Größe $n \times n$ existiert.

Stimmt bis $n < 668$. (Wikipedia)

Def.: Sei H_n eine normalisierte Hadamard-Matrix (d.h. erste Zeile und erste Spalte enthält nur +1 Einträge). Definiere den Code $A_n \subseteq \mathbb{F}_2^{n-1}$ wie folgt

Ersetze in der Matrix H_n die $+1$-Einträge durch 0, die -1-Einträge durch 1. Die Elemente von $\mathcal{A}_n$ sind die Zeilen 1 bis n, wobei die erste Koordinate nicht übernommen wird.

Klar: $\mathcal{A}_n$ ist ein binärer $(n-1, n, \frac{n}{2})$-Code.
(im Allgemeinen ist $\mathcal{A}_n$ nicht-linear)

Bsp: $\mathcal{A}_{12}$ ist $(11, 12, 6)$-Code

$\mathcal{A}_{12} =$

$$\begin{bmatrix}
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
1 & -1 & 1 & -1 & 1 & 1 & 1 & -1 & -1 & -1 & 1 & -1 \\
1 & -1 & -1 & 1 & -1 & 1 & 1 & 1 & -1 & -1 & -1 & 1 \\
1 & 1 & -1 & -1 & 1 & -1 & 1 & 1 & 1 & -1 & -1 & -1 \\
1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 & 1 & 1 & -1 & -1 \\
1 & -1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 & 1 & 1 & -1 \\
1 & -1 & -1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 & 1 & 1 \\
1 & 1 & -1 & -1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 & 1 \\
1 & 1 & 1 & -1 & -1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 \\
1 & 1 & 1 & 1 & -1 & -1 & -1 & 1 & -1 & -1 & 1 & -1 \\
1 & -1 & 1 & 1 & 1 & -1 & -1 & -1 & 1 & -1 & -1 & 1 \\
1 & 1 & -1 & 1 & 1 & 1 & -1 & -1 & -1 & 1 & -1 & -1
\end{bmatrix}$$