Vortrag zum Artikel „Error probabilities for bounded distance decoding“

Autoren des Artikels

Andreas Faldum, Julio Lafuente, Gustavo Ochoa, Wolfgang Willems

Vorraussetzungen

Die Codewörter werden durch einen q-nären symmetrischen Kanal übertragen mit einer Symbolfehlerwahrscheinlichkeit von $p \leq \frac{q-1}{q}$. Jedes Codewort wird mit der gleichen Wahrscheinlichkeit übertragen. Die Symbole werden mit Wahrscheinlichkeit $\frac{p}{q-1}$ zu einem anderen (bestimmten) Symbol während der Übertragung durch den Kanal verfälscht. Die zugrundeliegenden Codes C und C' sind $[n,k,d]$ bzw $[n,k,d']$ Codes über dem Körper Γ_q mit q Elementen. In diesem Artikel geht es nur um Decodierfehlerwahrscheinlichkeiten, wenn bis zu $t \leq \frac{d-1}{2}$ Fehler decodiert werden. Der Fall „decoding failure“ wird außer Acht gelassen.

Ziel

Ein Ziel ist es, für gegebene Fehlerwahrscheinlichkeit, Codes mit minimaler Fehlerwahscheinlichkeit zu finden und verschiedene Codes mit Hilfe ihrer Fehlerwahrscheinlichkeiten zu vergleichen um den geeigneteren zu bestimmen.

Einleitung

Es werden zwei Übertragunswahrscheinlichkeiten betrachtet. Für den Sender ist die Wahrscheinlichkeit $P_{ue}(C,t,p)$ interessant. Das ist die Wahrscheinlichkeit dass ein Wort w empfangen wird, welches zu c' decodiert wird, aber $c \in C$ gesendet wurde.
D.h. für $B_t(c) = \{w | w \in \Gamma_q,\ d(c,w) \leq t\}$ ist $P_{ue}(C,t,p) = P(Y \in \bigcup_{c \neq c'} B_t(c) | X = c)$,wobei
X= Zufallsvariable dass Codewort c gesendet wurde
Y= Zufallsvariable dass ein Wort aus der Umgebung von c empfangen wurde.

Bemerkung. P_{ue} hängt nicht vom gesendeten Codewort c ab (da alle $c \in C$ gleichwahrscheinlich sind und C linear ist). Also kann man auch

$$P_{ue}(C,t,p) = P(Y \in \bigcup_{c \neq 0} B_t(c) | X = 0)$$

schreiben.
Dann gilt

$$\begin{aligned} P_{ue} &= \sum_{0\neq c\in C} \sum_{v\in B_t(c)} P(Y=v|X=0) \\ &= \sum_{0\neq c\in C} \sum_{v\in B_t(c)} P(Y=-c+v|X=-c) \\ &= \sum_{0\neq c\in C} \sum_{w\in B_t(0)} P(Y=w|X=-c) \\ &= (|C|-1)\cdot(P(Y\in B_t(0)|X\in C\setminus\{0\}. \end{aligned}$$

Für den Empfänger ist die Wahrscheinlichkeit $P_{fd}(C,t,p)$ interessant. Das ist die Wahrscheinlichkeit, dass $c'\in C\setminus\{c\}$ übermittelt wurde, unter der Bedingung dass w mit $d(w,c)\leq t$ empfangen wird. $P_{fd}(C,t,p)=P(X\in C\setminus\{c\}|Y\in B_t(c))$

Da wir von Gleichverteilung auf C ausgehen.

$\implies P_{fd}(C,t,p)=P(X\in C\setminus\{0\}\colon Y\in B_t(0))$.

Dann folgt

$$\begin{aligned} P(Y\in B_t(0))\cdot P_{fd}(C,t,p) &= P(X\in C\setminus\{0\}|Y\in B_t(0))\cdot P(Y\in B_t(0)) \\ &= P(X\in C\setminus\{0\}, Y\in B_t(0)) \\ &= \sum_{0\neq c\in C}\sum_{w\in B_t(0)} P(X=c,Y=w) \\ &= \sum_{0\neq c\in C}\sum_{w\in B_t(0)} P(Y=w|X=c)\cdot P(X=c) \\ &= \frac{1}{|C|}\sum_{0\neq c\in C}\sum_{w\in B_t(0)} P(Y=w|X=c) \\ &= \frac{1}{|C|}P_{ue}(C,t,p) \end{aligned}$$

Man sieht die direkte Abhängigkeit von P_{ue} und P_{fd}.

Beide Fehlerwahrscheinlichkeiten sind gleich gut, wenn es darum geht, einen optimalen $[n,k,d]$ Code zu finden, in Bezug auf die Decodierfehlerwahrscheinlichkeit. Dabei sind n,k fest. In beiden Fällen folgt, dass für hinreichend kleine p's die Qualität eines Codes nur eine Frage der "weight distribution" ist, so lange nur bis $t\leq(d-1)/2$ decodiert wird.

Wir betrachten nun das „Verhalten" der Wahrscheinlichkeit falsch zu decodieren als Funktion, die von p und t abhängt.

Vergleich von P_{fd} und P_{ue}

Die Wahrscheinlichkeiten P_{fd} und P_{ue} sind unterschiedlich, aber wenn es darum geht, die Fehlerwahrscheinlichkeiten für $[n,k]$-Codes zu minimieren, sind P_{fd} und P_{ue} gleich gut.

Theorem 1. *Sei C ein $[n,k,d]$ Code, $t \leq (d-1)/2$. Dann ist*

$$P_{fd}(C,t,p) = \frac{P_{ue}(C,t,p)}{P_{ue}(C,t,p) + \sum_{i=0}^{t} \binom{n}{i} p^i (1-p)^{n-1}}$$

Beweis. Es gilt

$$\begin{aligned}
\frac{P_{ue}(C,t,p)}{P_{fd}(C,t,p)} &= |C| P(Y \in B_t(0)) \\
&= |C| \sum_{c \in C} P(Y \in B_t(0) | X = c) P(X = c) \\
&= P(Y \in B_t(0) | X = 0) + \sum_{0 \neq c \in C} P(Y \in B_t(0) | X = c) \\
&= \sum_{i=0}^{t} \binom{n}{i} p^i (1-p)^{n-i} + P_{ue}(C,t,p).
\end{aligned}$$

□

Es gilt

$$|C|\, P(Y \in B_t(0)) = \sum_{c \in C} P(Y \in B_t(c)).$$

Daher folgt:

Korollar 1. *Sei C ein $[n,k,d]$ Code, $t \leq (d-1)/2$.*

a) $P_{ue}(C,t,p) \leq P_{fd}(C,t,p)$

b) $P_{ue}(C,t,p) = P_{fd}(C,t,p)$ g. d. w. C perfekt ist und $t = (d-1)/2$.

Beweis. a) $\frac{P_{ue}(C,t,p)}{P_{fd}(C,t,p)} = \sum_{c \in C} P(Y \in B_t(0)) \leq 1 \implies P_{ue}(C) \leq P_{fd}(C)$.

b) C perfekt und $t = (d-1)/2 \overset{\text{Def.}}{\implies} \sum_{c \in C} P(Y \in B_t(c)) = 1 \implies P_{ue} = P_{fd}$. Andere Richtung genauso.

□

Korollar 2. *Seien C und C' $[n,k,d]$ bzw. $[n,k,d']$-Codes. Für die Fehlerwahrscheinlichkeit gilt $0 < p < q - 1/q$ und für festes $t \leq \min\{(d-1)/2, (d'-1)/2\}$ sind äquivalent*

(a) $P_{fd}(C,t,p) < P_{fd}(C',t,p)$

(b) $P_{ue}(C,t,p) < P_{ue}(C',t,p)$

Beweis. Nach Theorem 1 gilt

$$P_{fd}(C,t,p) = \frac{P_{ue}(C,t,p)}{P_{ue}(C,t,p)+A} = 1 - \frac{A}{P_{ue}(C)+A}$$

mit konstantem A.

$$\begin{aligned}
&\implies P_{ue}(C) < P_{ue}(C') \\
&\iff P_{ue}(C) + A < P_{ue}(C') + A \\
&\iff \frac{1}{P_{ue}(C)+A} > \frac{1}{P_{ue}(C')+A} \\
&\iff \frac{A}{P_{ue}(C)+A} > \frac{A}{P_{ue}(C')+A} \\
&\iff 1 - \frac{A}{P_{ue}(C)+A} < 1 - \frac{A}{P_{ue}(C')+A} \\
&\iff P_{fd}(C) < P_{fd}(C')
\end{aligned}$$

□

Die Wahrscheinlichkeit $P_{ue}(C,t,p)$

Sei C ein $[n,k,d]$ Code über $\mathbb{F}_q$ mit Gewichtspolynom

$$A(x) = \sum_{i=1}^{n} A_i x^i.$$

Weiterhin sei $t \in \mathbb{N}_0$ mit $t \leq (d-1)/2$.

Theorem 2. *Es gilt*

$$P_{ue}(C,t,p) = \sum_{i=1}^{n} A_i \sum_{j=0}^{t} \sum_{s=0}^{j} \left[\binom{i}{s} \left(\frac{p}{q-1}\right)^{i-s} \left(1 - \frac{p}{q-1}\right)^{s} \binom{n-i}{j-s} p^{j-s} (1-p)^{n-i-j+s} \right]$$

Beweis. Wir wissen dass $P_{ue}(C,t,p) = P(Y \in \bigcup_{0 \neq c} B_t(c) | X = 0)$. Sei $c \in \mathbb{F}_q^n$ mit $\mathrm{wt}(c) = i > 0$. Es wird $0 \in C$ übertragen. Empfangen wird $w \in B_t(c)$ mit Wahrscheinlichkeit

$$\sum_{j=0}^{t} \sum_{s=0}^{j} \left[\binom{i}{s} \left(\frac{p}{q-1}\right)^{i-s} \left(1 - \frac{p}{q-1}\right)^{s} \binom{n-i}{j-s} p^{j-s} (1-p)^{n-i-j+s} \right]$$

Bemerkung.

- $\binom{n-i}{j-s} = 0$ für $j - s > n - i$
- $i \geq d > t \geq s$

- die Wahrscheinlichkeit ist die selbe für alle $c \in C$ mit $\mathrm{wt}(c) = i$
  $\Longrightarrow A_i \sum_{j=0}^{t} \sum_{s=0}^{j} \binom{i}{s} \left(\frac{p}{q-1}\right)^{i-s} \left(1 - \frac{p}{q-1}\right)^{s} \binom{n-i}{j-s} p^{j-s}(1-p)^{n-i-j+s}$
  für alle $c \in C$ mit $\mathrm{wt}(c) = i$
  $\Longrightarrow \sum_{i=1}^{n} A_i \sum_{j=0}^{t} \sum_{s=0}^{j} \binom{i}{s} \left(\frac{p}{q-1}\right)^{i-s} \left(1 - \frac{p}{q-1}\right)^{s} \binom{n-i}{j-s} p^{j-s}(1-p)^{n-i-j+s} \ \forall c \in C.$

(Dieses Theorem wurde in der Vorlesung Angewandte Diskrete Mathematik schon bewiesen.) □

Um zwei $[n,k]$ Codes C und C' miteinander zu vergleichen, kann $P_{ue}(C)$ und $P_{ue}(C')$ nach Theorem 2 berechnet werden. Für sehr kleine p's gibt es einen einfacheren Weg.

Definition 1. *Seien f und f' mit $f(x) = \sum_{i=0}^{n} a_i x^i$ bzw. $f'(x) = \sum_{i=0}^{n} a'_i x^i$ Polynomfunktionen mit a_i, $a'_i \in \mathbb{R}_0^+$. Wir schreiben $f(x) \prec f'(x)$, wenn $(a_0, \ldots, a_n) \prec (a'_0, \ldots a'_n)$. d. h. $s \in \{0, 1, \ldots, n\}$ ex., sodass $a_i = a'_i$ für $i < s$, aber $a_s < a'_s$. Dann ist $f(x) \preceq f'(x)$, wenn $f(x) \prec f'(x)$ oder $f(x) = f'(x)$.*

Theorem 3. *C und C' $[n,k,d]$ und $[n,k,d']$ Codes mit Gewichtspolynomen $A(x)$ und $A'(x)$. Sei $t \leq \min\{(d-1)/2, (d'-1)/2\}$. Ist p klein genug, so sind folgende Bedingungen äquivalent:*

a) $P_{fd}(C) \leq P_{fd}(C')$

b) $P_{ue}(C) \leq P_{ue}(C')$

c) $A(x) \preceq A'(x)$

Beweis. a) $\Longleftrightarrow$ b) gilt nach Korollar 2. Also reicht es *b)* $\Longleftrightarrow$ *c)* zu zeigen.
Angenommen $A(x) \neq A'(x)$ (da sonst $C \cong C'$). Sei l der kleinste Wert an dem die Gewichtspolynome von C und C' verschieden sind.
Betrachte $f(p) = P_{ue}(C', t, p) - Pue(C, t, p) =^{Theoremoben} \sum_{i=l}^{n} (A'_i - A_i) f_i(p)$,
wobei $f_i(p) = \sum_{j=0}^{t} \sum_{s=0}^{j} \binom{i}{s} \left(\frac{p}{q-1}\right)^{i-s} \left(1 - \frac{p}{q-1}\right)^{s} \binom{n-i}{j-s} p^{j-s}(1-p)^{n-i-j+s}$ ist.
Wegen $0 \leq j \leq t < l$ folgt, dass für $i \geq l$ gilt $f_i(p)$ hat die Form $f_i(p) = \binom{i}{l} \frac{1}{q-1}^{i-t} p^{i-t} +$ Terme in p^r, mit $r > i - t$.
$\Rightarrow f(p) = (A'_l - A_l)\binom{l}{t} \frac{1}{q-1}^{l-t} p^{l-t} +$ Terme in p^r mit $r > l - t$.
($l - t$ ist der untere Teil der Summe, alle anderen Terme sind $\Delta \cdot p^{r+k}$ für $k > 0$, also $O(p^r)$)
Also gilt für sehr kleine p:
$f(p) > 0 \Leftrightarrow A_l < A'_l$
$\Rightarrow P_{ue}(C, t, p) < P_{ue}(C', t, p) \Leftrightarrow A(x) \preceq A'(x)$ □

Proposition 4. *Seien C und C' $[n,k,d]$ bzw. $[n,k,d']$ Codes über Γ_q, mit Gewichtsverteilung $(A_0, \ldots, A_n)$ und $(A'_0, \ldots, A'_n)$.*
Angenommen:

$$\sum_{i=0}^{j} A_i \leq \sum_{i=0}^{j} A'_i \forall j = 0, \ldots n \text{ mit } \sum_{i=0}^{j_0} A_i < \sum_{i=0}^{j_0} A'_i \text{ für ein } j_0 \in \{0, \ldots, n\}$$

Dann ist $P_{ue}(C, t, p) < P_{ue}(C', t, p)$ $\forall 0 < p < \frac{q-1}{q}$ und $t \leq \min\left\{\frac{d-1}{2}, \frac{d'-1}{2}\right\}$.

Beweis. Um zu zeigen, dass $P_{ue}(C,t,p) < P_{ue}(C',t,p)$ müssen wir zeigen, dass

$$\sum_{i=0}^{n} A_i f_i(p) < \sum_{i=0}^{n} A'_i f_i(p)$$

mit

$$f_i(p) = \sum_{j=0}^{t}\sum_{s=0}^{j}\left[\binom{i}{s}\left(\frac{p}{q-1}\right)^{i-s}\cdot\left(1-\frac{p}{q-1}\right)^{s}\binom{n-1}{j-s}p^{j-s} - (1-p)^{n-i-j+s}\right]$$

Wir nehmen an, dass $f_{i+1}(p) < f_i(p)$ für $i = 0,\dots,n$, wobei $f_{n+1}(p) = 0$ schon gezeigt wurde. Betrachte dann

$$\begin{aligned} f(p) &= \big(P_{ue}(C',t,p) - P_{ue}(C,t,p)\big) \\ &= \sum_{i=0}^{n}(A'_i - A_i)\cdot f_i(p) \\ &= \sum_{j=0}^{n}(f_j(p) - f_{j+1}(p))\cdot \underbrace{\sum_{i=0}^{j}(A'_i - A_i)}_{\geq 0} \\ &> 0, \text{ da } f_j(p) - f_{j+1}(p) > 0 \end{aligned}$$

$$\Rightarrow f(p) > 0 \text{ für } 0 < p < \frac{q}{q-1} \Rightarrow P_{ue}(C,t,p) < P_{ue}(C',t,p)$$

Es bleibt zu zeigen, dass $f_{i+1}(p) < f_i(p)$.

- $f_i(p)$ hängt nur vom Gewicht der Codewörter c, mit $wt(c) = i$ ab, jedoch nicht vom Codewort selbst.
- $f_n(p) > f_{n+1}(p) = 0$ Klar.

$\Rightarrow$ Angenommen $i < n$:

- $f_i(p) = P(Y \in B_t(c) | X = 0)$ mit $c \in C$ und $wt(c) = d(c,0) = i$.
  $f_i(p)$ hängt dabei nur vom Gewicht von c ab, aber nicht von c selbst.

OBdA sei

$$c = \underbrace{1,\dots,1}_{i\text{-mal}},0,\dots,0;\ \hat{c} = c + e;\ e = 0,\dots,0,1$$

$$\Rightarrow f_i(p) = \sum_{w\in B_t(c)} P(Y = w|X = 0) \text{ und } f_{i+1}(p) = \sum_{v\in B_t(\hat{c})} P(Y = v|X = 0)$$

Wir stellen fest, dass $\forall w \in B_t(c)$ gilt:

$$d(w,\hat{c}) \leq d(w,c) + d(c,\hat{c}) \leq t + 1.$$

Also gilt für

$$w \in B_t(c) \setminus B_t(\hat{c}) : d(w,c) = t \text{ und } d(w,\hat{c}) = t+1 \Rightarrow w = (w_1,\dots,w_{n-1},0)$$

Betrachte nun die Bijektion:

$$\begin{aligned}
&\varphi : B_t(c) \to B_t(\hat{c}) \\
&\varphi(w) = w, \text{ wenn } w \in B_t(c) \cap B_t(\hat{c}) \\
&\varphi(w) = w + e, \text{ wenn } w \in B_t(c) \setminus B_t(\hat{c}) \\
&\Rightarrow d(w,0) \leq d(\varphi(w),0) \ \forall w \in B_t(c)
\end{aligned}$$

Weiterhin gilt (da $p < \frac{q-1}{q}$)

$$P(Y = w|X = 0) \geq P(Y = \varphi(w)|X = 0)$$

wobei die echte Ungleichung gilt für $w \in B_t(c) \setminus B_t(\hat{c}) \neq \emptyset$

$$\begin{aligned}
\Rightarrow f_i(p) &= \sum_{w \in B_t(c)} P(Y = w|X = 0) \\
&> \sum_{w \in B_t(c)} P(Y = \varphi(w)|X = 0) \\
&= \sum_{v \in B_t(\hat{c})} P(Y = v|X = 0) \\
&= f_{i+1}(p)
\end{aligned}$$

□