The Asymptotic Theory of Error-Correcting Codes

Harald Niederreiter

RICAM Linz and University of Salzburg

— Error-correcting codes

— Global function fields

— Algebraic-geometry codes

— Asymptotic theory of codes

— The TVZ bound

— Improving the TVZ bound globally

— Further improvements

Error-correcting codes

An error-correcting code (or simply a code) is a scheme for detecting and correcting transmission errors in noisy communication channels. A code operates by adding redundant information to messages. As the signal alphabet we use $\mathbb{F}_q$, the finite field with q elements (q prime power).

For integers $1 \leq k \leq n$, an $[n, k]$ code over $\mathbb{F}_q$ is a k-dimensional linear subspace C of $\mathbb{F}_q^n$.

For $\mathbf{a}, \mathbf{b} \in \mathbb{F}_q^n$, define the Hamming metric $d(\mathbf{a}, \mathbf{b})$ to be the number of coordinates in which $\mathbf{a}$ and $\mathbf{b}$ differ. Define the minimum distance

$$d(C) = \min \{d(\mathbf{a}, \mathbf{b}) : \mathbf{a}, \mathbf{b} \in C, \ \mathbf{a} \neq \mathbf{b}\}.$$

Note that C adds $n-k$ redundant symbols to k information symbols for error correction. It is well known that C can correct up to $\lfloor (d(C) - 1)/2 \rfloor$ transmission errors in each coded message block of length n.

The aim of coding theory is to construct $[n, k]$ codes C over $\mathbb{F}_q$ with large minimum distance $d(C)$ for given n and k, or with a large relative minimum distance $\frac{d(C)}{n}$ for a given information rate $\frac{k}{n}$.

The above defines a linear code. A general code of length n is a subset C of $\mathbb{F}_q^n$ with $|C| \geq 2$. The minimum distance $d(C)$ is defined as before. We have the same result about the error-correction capability for general codes C.

Global function fields

Let $F/\mathbb{F}_q$ be a global function field with full constant field $\mathbb{F}_q$. This means:
(i) F is an algebraic function field with constant field $\mathbb{F}_q$;
(ii) $\mathbb{F}_q$ is algebraically closed in F.

A place of F is an equivalence class of valuations of F.

ν_P = normalized valuation belonging to the place P.

A divisor of F is a formal sum $\sum_P n_P P$ with $n_P \in \mathbb{Z}$ and all but finitely many $n_P = 0$.

The divisors of F form a free abelian group generated by the places of F.

The principal divisor of $f \in F^*$ is

$$\operatorname{div}(f) = \sum_P \nu_P(f) P.$$

$F/\mathbb{F}_q$ global function field of genus g.
G divisor of F.

The Riemann-Roch space

$$\mathcal{L}(G) = \{f \in F^* : \mathrm{div}(f) + G \geq 0\} \cup \{0\}$$

is a finite-dimensional vector space over $\mathbb{F}_q$.
Write $\ell(G) = \dim(\mathcal{L}(G))$.

By the Riemann-Roch theorem

$$\ell(G) \geq \deg(G) + 1 - g,$$

with equality if $\deg(G) \geq 2g - 1$.

Def. A place of $F/\mathbb{F}_q$ is rational if it has degree 1, i.e., if its residue class field is $\mathbb{F}_q$.

Put

$N(F) =$ number of rational places of F,

$g(F) =$ genus of F.

Weil bound:

$$N(F) \leq q + 1 + 2g(F)q^{1/2}.$$

Def. For any prime power q and any integer $g \geq 0$, let

$$N_q(g) = \max \ N(F),$$

where max. over all $F/\mathbb{F}_q$ with $g(F) = g$.

Remark. $N_q(g)$ is also the max. number of $\mathbb{F}_q$-rational points that a projective, smooth, absolutely irreducible algebraic curve over $\mathbb{F}_q$ of genus g can have.

Algebraic-geometry codes

Introduced by Goppa (1977–81). We use the language of global function fields.

- $F/\mathbb{F}_q$ global function field of genus g.
- $P_1, \ldots, P_n$ distinct rational places of F.
- G divisor of F with $P_i \notin \operatorname{supp}(G)$ for $1 \leq i \leq n$.

For $f \in \mathcal{L}(G)^*$ we have by definition

$$\operatorname{div}(f) + G \geq 0,$$

hence $\nu_{P_i}(f) \geq 0$ for $1 \leq i \leq n$. This holds trivially for $f = 0$ as well. Thus, f lies in the valuation ring O_{P_i} of P_i. The residue class of f modulo the maximal ideal of O_{P_i} is in the residue class field $\mathbb{F}_q$ and denoted by $f(P_i)$.

An algebraic-geometry code is defined as the image of the $\mathbb{F}_q$-linear map

$$f \in \mathcal{L}(G) \mapsto (f(P_1), \ldots, f(P_n)) \in \mathbb{F}_q^n.$$

If $g \leq \deg(G) < n$, get linear $[n, k]$ code C over $\mathbb{F}_q$ with

$$k = \ell(G) \geq \deg(G) + 1 - g,$$
$$d(C) \geq n - \deg(G).$$

Thus

$$k + d(C) \geq n + 1 - g.$$

Note that by the Singleton bound we always have

$$k + d(C) \leq n + 1.$$

Example. Let $F = \mathbb{F}_q(x)$ be the rational function field over $\mathbb{F}_q$. We have genus $g = 0$ in this case.

Let P_∞ be the infinite place of F, i.e., P_∞ corresponds to the negative degree map.

For any integer $k \geq 1$, put

$$G_k = (k-1)P_\infty.$$

Then $\mathcal{L}(G_k)$ consists exactly of all polynomials over $\mathbb{F}_q$ of degree $\leq k-1$, and so $\ell(G_k) = k$.

Consider the algebraic-geometry code C with $G = G_k$. The rational places $P_1, \ldots, P_n$ of F correspond to distinct elements $a_1, \ldots, a_n$ of $\mathbb{F}_q$, thus must assume $n \leq q$. We also assume $1 \leq k \leq n$. The code C is the image of the injective $\mathbb{F}_q$-linear map

$$f \in \mathcal{L}(G_k) \mapsto (f(a_1), \ldots, f(a_n)) \in \mathbb{F}_q^n.$$

This is called a Reed-Solomon code. It is a linear $[n, k]$ code over $\mathbb{F}_q$ with $k + d(C) = n + 1$, and so it meets the Singleton bound.

Asymptotic theory of codes

C code over $\mathbb{F}_q$.

$n(C) =$ length of C,

$|C| =$ size of C,

$d(C) =$ minimum distance of C.

Def. $U_q =$ set of pairs $(\delta, R) \in [0,1]^2$ such that $\exists$ sequence $C_1, C_2, \ldots$ of codes over $\mathbb{F}_q$ with $n(C_i) \to \infty$ as $i \to \infty$ and

$$\delta = \lim_{i \to \infty} \frac{d(C_i)}{n(C_i)}, \quad R = \lim_{i \to \infty} \frac{\log_q |C_i|}{n(C_i)}.$$

Known: $\exists$ function α_q on $[0,1]$ such that

$$U_q = \{(\delta, R) : 0 \leq R \leq \alpha_q(\delta),\ 0 \leq \delta \leq 1\}.$$

α_q is nonincreasing with $\alpha_q(0) = 1$ and $\alpha_q(\delta) = 0$ for $(q-1)/q \leq \delta \leq 1$.

The values of $\alpha_q(\delta)$ for $0 < \delta < (q-1)/q$ are not known.

Basic problem of coding theory:

find good lower bounds on α_q in the interval $(0, (q-1)/q)$.

For $0 < \delta < 1$ define the q-ary entropy function by

$$H_q(\delta) = \delta \log_q(q-1) - \delta \log_q \delta - (1-\delta) \log_q(1-\delta).$$

Put

$$R_{\mathrm{GV}}(q, \delta) = 1 - H_q(\delta).$$

Gilbert-Varshamov bound (1950s):

$$\alpha_q(\delta) \geq R_{\mathrm{GV}}(q, \delta) \qquad \forall \delta \in \left(0, \frac{q-1}{q}\right).$$

The TVZ bound

For any q put

$$A(q) = \limsup_{g \to \infty} \frac{N_q(g)}{g}.$$

From Weil bound get $A(q) \leq 2q^{1/2}$.

Ihara (1981): $A(q) \geq q^{1/2} - 1$ for squares q.

Vlăduţ-Drinfeld (1983): $A(q) \leq q^{1/2} - 1 \ \ \forall q$.

Garcia-Stichtenoth (1995): if q is a square, then $A(q) = q^{1/2} - 1$ can be achieved by an explicit tower of global function fields.

Serre (1983): $A(q) \geq c \log q$ for all q with abs. constant $c > 0$.

Xing-Yeo (2007): $A(2) \geq \frac{97}{376} = 0.2579\ldots$.

Tsfasman-Vlăduţ-Zink bound (1982). $\forall \delta \in [0,1]$

$$\alpha_q(\delta) \geq R_{\mathrm{AG}}(q,\delta) := 1 - \frac{1}{A(q)} - \delta.$$

Sketch of proof. From def. of $A(q)$ get sequence $F_1, F_2, \ldots$ of global function fields over $\mathbb{F}_q$ such that $g_i := g(F_i)$ and $n_i := N(F_i)$ satisfy

$$\lim_{i\to\infty} g_i = \infty, \qquad \lim_{i\to\infty} \frac{n_i}{g_i} = A(q).$$

Obtain sequence $C_1, C_2, \ldots$ of AG codes with

$$k_i + d_i \geq n_i + 1 - g_i$$

and $n(C_i) = n_i \to \infty$ as $i \to \infty$. Divide by n_i.

Pass to a subsequence, if necessary, and let $i \to \infty$. Then we get $(\delta, R) \in U_q$ with

$$R + \delta \geq 1 - \frac{1}{A(q)}.$$

Thus

$$\alpha_q(\delta) \geq R \geq 1 - \frac{1}{A(q)} - \delta. \qquad \text{QED}$$

Big triumph of AG codes: for suitable q we have

$$R_{\mathrm{AG}}(q, \delta) > R_{\mathrm{GV}}(q, \delta)$$

on a subinterval of $(0, (q-1)/q)$ containing $(q-1)/(2q-1)$.

Tsfasman-Vlăduţ-Zink (1982): for all squares $q \geq 49$.

Zink (1985), Bezerra-Garcia-Stichtenoth (2005): for all sufficiently large cubes q.

H.N.-Xing (1998): for sufficiently large composite non-squares q.

The proofs are based on $A(q) = q^{1/2} - 1$ (TVZ) and on lower bounds on $A(q)$.

H.N.-Xing, *Rational Points on Curves over Finite Fields: Theory and Applications*, Cambridge Univ. Press, 2001.

Improving the TVZ bound globally

Local improvements on the TVZ bound, i.e., improvements on small intervals of δ-values, were already obtained by Vlăduţ (1987), Elkies (2001), and Xing (2001). Global improvements, i.e., improvements for all $\delta \in [0, 1]$, were achieved only recently.

Xing (2003): $\forall \delta \in [0,1]$

$$\alpha_q(\delta) \geq 1 - \frac{1}{A(q)} - \delta + \sum_{i=2}^{\infty} \log_q \left(1 + \frac{q-1}{q^{2i}}\right).$$

The proof is nonconstructive.

H.N.-Özbudak (2004): $\forall \delta \in [0,1]$

$$\alpha_q(\delta) \geq 1 - \frac{1}{A(q)} - \delta + \log_q \left(1 + \frac{1}{q^3}\right).$$

It is an easy exercise to verify that the NÖ bound is always better than the Xing bound.

The proof of the NÖ bound is constructive on an interval of the form $[0, c_q]$ with $c_q \to 1$ as $q \to \infty$.

Stichtenoth-Xing (2005): NÖ bound by simpler construction. Consider

$$\phi : f \in \mathcal{L}(G) \mapsto (f(P_1), \ldots, f(P_n)) \in \mathbb{F}_q^n$$

in the definition of an AG code. Nonlinearity is created in two ways:

(i) ϕ is restricted to a subset S of $\mathcal{L}(G)$ which is not necessarily an $\mathbb{F}_q$-linear subspace;

(ii) if P_i is in the support of an aux. divisor, the coordinate $f(P_i)$ is changed to 0.

The code is $C = \psi(S) \subseteq \mathbb{F}_q^n$, where ψ is the modified version of ϕ.

The NÖ bound is obtained by using a sequence of function fields with $g_i \to \infty$ and $n_i/g_i \to A(q)$.

Further improvements

H.N.-Özbudak (Finite Fields Appl., 2007)

- $F/\mathbb{F}_q$ global function field.
- $P_1, \ldots, P_n$ distinct rational places of F.
- G divisor of F with $P_i \notin \mathrm{supp}(G)$ for $1 \leq i \leq n$.

In addition to $\phi : \mathcal{L}(G) \to \mathbb{F}_q^n$, consider

$$\phi_1 : f \in \mathcal{L}(G) \mapsto (f'(P_1), \ldots, f'(P_n)) \in \mathbb{F}_q^n,$$

where $f'(P_i)$ is the coefficient of the linear term in the local expansion of f at P_i.

Let $B(\mathbf{c}; r) \subseteq \mathbb{F}_q^n$ be the Hamming ball with center $\mathbf{c}$ and radius r. The code is

$$C = \phi_1(\phi^{-1}(B(\mathbf{c}; r))) \subseteq \mathbb{F}_q^n.$$

A major effort in the construction is expended on finding a distinguished divisor G of F which has a prescribed degree and satisfies

$$\mathcal{L}(G - D) = \{0\}$$

for a (large) finite family of positive divisors D of F.

This divisor is then used in the above construction together with suitable choices of $\mathbf{c}$ and r. As usual, the construction is applied to a sequence of function fields with $g_i \to \infty$ and $n_i/g_i \to A(q)$.

The final result is

$$\alpha_q(\delta) \geq 1 - \frac{1}{A(q)} - \delta + \log_q \left(1 + \frac{q-1}{q^4}\right) + h_q(\delta)$$

with a complicated nonnegative function h_q.

This yields local improvements on the old NÖ bound from 2004.

Example 1. $q = 64$, $\delta \approx 0.2988$. The new NÖ bound beats the old NÖ bound by about $1.6 \cdot 10^{-6}$ and the GV bound by about $2.6 \cdot 10^{-3}$.

Example 2. $q = 49$, $\delta \approx 0.6089$. The new NÖ bound

beats the old NÖ bound by about $5 \cdot 10^{-10}$ and the GV bound by about $2 \cdot 10^{-3}$.

Example 3. $q = 2^{21}$, $\delta \approx 0.0104$. The new NÖ bound beats the old NÖ bound by about $1.3 \cdot 10^{-18}$ and the GV bound by about $3.2 \cdot 10^{-8}$.

Maharaj (2007): refined the Stichtenoth-Xing approach and obtained several local improvements on the new NÖ bound.

H.N.-Özbudak (SIAM J. on Discrete Math., 2007)

Combined for the first time three major tools:

(i) distinguished divisors;
(ii) local expansions of arbitrary length;
(iii) averaging arguments.

This leads to local improvements on all previous bounds, at the cost of considerable complications in the analysis. This approach yields also improved bounds in the asymptotic theory of linear codes.

Yang-Qi (to appear)

Extend method in H.N.-Özbudak (Finite Fields Appl., 2007).

The basic approach is the same, but instead of ϕ_1 they work with the map

$$\phi_2 : f \in \mathcal{L}(G) \mapsto (f''(P_1), \ldots, f''(P_n)) \in \mathbb{F}_q^n,$$

where $f''(P_i)$ is the coefficient of the quadratic term in the local expansion of f at P_i.

This yields

$$\alpha_q(\delta) \geq 1 - \frac{1}{A(q)} - \delta + \log_q\left(1 + \frac{2}{q^3}\right) + \log_q\left(1 + \frac{q-1}{q^6}\right)$$

for sufficiently large q and certain ranges of δ.

Problem. The proofs of the TVZ bound and its improvements use only rational places of suitable global function fields. We know general constructions of AG codes (NXL, XNL) that use places of higher degrees as well. Do these constructions lead to improvements on the bounds discussed here?