AN ASYMPTOTIC GILBERT-VARSHAMOV BOUND FOR (T,M,S)-NETS

Jürgen Bierbrauer
Department of Mathematical Sciences, Michigan Technological University, Houghton, Michigan 49931, USA
jbierbra@mtu.edu

Wolfgang Ch. Schmid[1]
Department of Mathematics, University of Salzburg, 5020 Salzburg, Austria
wolfgang.schmid@sbg.ac.at

Received: , Accepted: , Published:

Abstract

(t, m, s)-nets are point sets in Euclidean s-space satisfying certain uniformity conditions, for use in numerical integration. They can be equivalently described in terms of ordered orthogonal arrays, a class of finite geometrical structures generalizing orthogonal arrays. This establishes a link between quasi-Monte Carlo methods and coding theory. In the present paper we prove an asymptotic Gilbert-Varshamov bound for linear nets and compare it to the algebraic-geometric net construction.

1. Introduction

(t, m, s)-**nets** (short: nets) were defined by Niederreiter [13] in the context of quasi-Monte Carlo methods of numerical integration. Close connections with various combinatorial and algebraic structures were obvious right from the start. Linear nets (usually known as digital nets) can be described in terms of **ordered orthogonal arrays** (OOA), a family of objects that contain linear **orthogonal arrays** as a subclass. As linear orthogonal arrays are the duals of linear error-correcting codes this establishes a link with algebraic coding theory. These connections were described and systematically exploited by many authors, see [7, 8, 9, 10, 11, 12, 14, 17, 18]. In [4] we proved a finite Gilbert-Varshamov bound for linear nets, thus generalizing a classical result from coding theory. In the present paper we prove an asymptotic Gilbert-Varshamov bound for linear nets. Basic definitions and the statement of the theorem are in the next section. In Section 3 we prove a version of the asymptotic GV-theorem for nets. In Section 4 we finish the proof of

[1] partially supported by the Austrian Science Foundation (FWF), projects no. S8311 and P17022

our main result and give parametric examples. In the final Section 5 we compare the GV-bound with the asymptotic bound derived from the algebraic-geometric net construction.

2. Definitions and results

Definition 1. *Let $\mathcal{A} \subset \mathbb{F}_q^s$ be a linear subspace of dimension m. The* **strength** *k of $\mathcal{A}$ is the maximal number such that the projection from $\mathcal{A}$ to any set of k coordinates is surjective.*
The **rate** *is $R = 1 - \frac{m}{s}$, the* **relative strength** *is $\delta = \frac{k}{s}$.*

Such subspaces are also known as linear q-ary **orthogonal arrays** (OA) of strength k. As $\mathcal{A}$ has strength k if and only if its dual $\mathcal{A}^\perp$ has minimum distance $k+1$, the theory of linear OA is equivalent with the theory of linear error-correcting codes. We have chosen terminology in Definition 1 in accordance with established terminology in coding theory.

Definition 2. *Let q be a prime-power and $0 \leq \delta, R \leq 1$. We say that (δ, R) is* **asymptotically reachable** *by linear q-ary orthogonal arrays if there is an infinite series of such arrays of length s_i, dimension m_i, and strength k_i whose rates have a limit $\geq R$ and whose relative strengths have a limit $\geq \delta$.*

Terminology has been chosen in Definition 2 such that (δ, R) is **asymptotically reachable** by linear q-ary OA if and only if (δ, R) can be asymptotically reached by linear q-ary codes in the theory of error-correcting codes, where R is the rate and δ is the relative minimum distance of the code. The classical asymptotic Gilbert-Varshamov theorem from coding theory can be formulated as follows (see for example [3]):

Theorem 1. *The q-ary code entropy function is defined as*

$$H_q(\delta) = \log_q(2) \cdot h(\delta) + \delta \cdot \log_q(q-1),$$

where

$$h(x) = -x \cdot \log_2(x) - (1-x) \cdot \log_2(1-x)$$

is the binary Shannon entropy function.

If $R \leq 1 - H_q(\delta)$, then (δ, R) is asymptotically reachable by linear q-ary OA.

(t, m, s)-nets are subsets of Euclidean $s-$space. As mentioned before, they can be described equivalently in terms of certain finite combinatorial structures, **ordered orthogonal arrays.** We take this equivalent description as the definition and concentrate on the linear case.

Definition 3. *Let $\Omega = \Omega^{(T,s)}$ be a set of Ts elements, partitioned into s* **blocks** *B_i, $i = 1, 2 \ldots, s$, where $B_i = \{\omega_1^{(i)}, \ldots, \omega_T^{(i)}\}$. Each block carries a total ordering:*

$$\omega_1^{(i)} < \omega_2^{(i)} < \cdots < \omega_T^{(i)}.$$

This gives Ω the structure of a partially ordered set, the union of s totally ordered sets of T points each. We consider Ω as a basis of a $Ts-$dimensional vector space $\mathbb{F}_q^{(T,s)}$. An **ideal** *in Ω is a set of elements closed under predecessors. An* **antiideal** *is a subset closed under followers. Antiideals are precisely the complements of ideals.*

We visualize $x = \left(x_j^{(i)}\right) \in \mathbb{F}_q^{(T,s)}, i = 1, \ldots, s; j = 1, \ldots, T$ as matrices with T rows and s columns. The interpretation of $x \in \mathbb{F}_q^{(T,s)}$ as a point in the $s-$dimensional unit cube is obtained by reading the $x_j^{(i)}$ for fixed i as the T first digits of the $q-$ary expansion of a real number between 0 and 1. Here is some more helpful terminology:

Definition 4. *The* **breadth** *$b = b(x)$ of a vector $x \in \mathbb{F}_q^{(T,s)}$ is the number of blocks $B_i, i = 1, 2, \ldots, s$ where x has a nonzero entry. The ideal $K = K(x)$ generated by x is the smallest ideal containing the support of x. The breadth of K is the breadth of x. Let $n = |K|$ be the* **size** *of K. The* **type** *$\pi = \pi(K)$ is the partition of n, where the multiplicity f_i of i as a part of π is the number of blocks, which intersect K in i points. The breadth $b(\pi)$ of a partition is the number of its nonzero parts. If $\pi = \pi(K(x))$, then $b(\pi) = b(x)$.*

Definition 5. *A linear subspace $\mathcal{C} \subseteq \mathbb{F}_q^{(T,s)}$ has* **strength** *$k = k(\mathcal{C})$ if k is maximal such that the projection from $\mathcal{C}$ to any ideal of size k is surjective. We also call such a subspace an* **ordered orthogonal array** *OOA, which is $q-$linear, has* **length** *s,* **depth** *T,* **dimension** *$m = dim(\mathcal{C})$, and strength k.*

Definition 6. *We define a linear $(m-k, m, s)_q$-net (usually: digital $(m-k, m, s)$-net over $\mathbb{F}_q$) as an $m-$dimensional linear OOA of length s, strength k, and depth k.*

Observe that linear OOA of depth 1 are precisely linear orthogonal arrays. It follows that the existence of a linear $(m-k, m, s)_q$-net implies the existence of a linear OA of length s, dimension m, and strength k. For $m \leq s$ this is equivalent with the existence of an $[s, s-m, k+1]_q$-code. The asymptotic parameters are the following:

Definition 7. *The* **rate** *of a linear $(m-k, m, s)_q$-net is $R = 1 - \frac{m}{s}$, its* **relative strength** *is $\delta = \frac{k}{s}$.*

Definition 8. *Let q be a prime-power, $0 \leq \delta < \infty$ and $-\infty < R \leq 1$. We say that (δ, R) is* **asymptotically reachable** *by linear q-ary nets if there is an infinite series of linear $(m_i - k_i, m_i, s_i)_q$-nets whose rates have a limit $\geq R$ and whose relative strengths have a limit $\geq \delta$.*

Here $0 \leq \delta < \infty$ and $-\infty < R \leq 1$. The terminology has been chosen to facilitate comparison with the asymptotics of linear OA and linear error-correcting codes. The relative strength may be arbitrarily large, whereas in the case of OA the relative strength is ≤ 1 and correspondingly the relative minimum distance of a code is ≤ 1. Also, negative rates do not occur in the case of codes and OA, but they do make sense for OOA and nets. A linear $(m-k, m, s)_q$-net has negative rate if and only if $m > s$.

Our main theorem is the following analogue of Theorem 1.

Theorem 2. *If $R \leq 1 - F_q(\delta)$, then (δ, R) is asymptotically reachable by linear q-ary nets. Here $F_q(\delta)$, the q-ary net entropy function, is defined as follows:*

$$F_q(\delta) = \delta - 1 + \log_q\left(\frac{q-1+\alpha}{\alpha}\right) - \delta \cdot \log_q(1-\alpha) \ ,$$

where $\alpha = \dfrac{\sqrt{q-1}\sqrt{1+6\delta+\delta^2} - (q-1)(1+\delta)}{2\delta}$.
Equivalently α is defined by $\delta = \dfrac{(q-1)(1-\alpha)}{(q-1)\alpha+\alpha^2}$.

3. Proof of the main theorem

In this section we prove Theorem 2 in the following equivalent form:

Theorem 3. *If $R \leq 1 - F_q(\delta)$, then (δ, R) is asymptotically reachable by linear q-ary nets. Here*

$$F_q(\delta) = \max_{0 \leq \alpha \leq \min(1, 1/\delta)} F_q(\alpha, \delta),$$

where

$$F_q(\alpha, \delta) = \log_q(q-1)\alpha\delta + \delta - \alpha\delta + \log_q(2)h(\alpha\delta) + \log_q(2)\delta h(\alpha)$$

and $h(x)$ is the binary Shannon entropy function.

The fact that Theorem 3 is the same as Theorem 2, equivalently that the two expressions for the net entropy function $F_q(\delta)$ coincide, will be proved in Section 4. The present section provides a proof of Theorem 3.

We start from the finite GV-bound for nets as given in [4]:

Theorem 4. *A linear $(m-k, m, s)_q$-net exists if the following is satisfied for all $T = 1, 2, \ldots, k-1$:*

$$\sum_{\pi} B(\pi) < q^m \ .$$

Here π varies over all partitions of numbers $l \leq k - T$ with maximal part at most T, the partition is described by the numbers $f_1, f_2, \ldots, f_T$ where f_i is the number of times *number i is used, $b(\pi) = f_T + f_{T-1} + \cdots + f_2 + f_1 \leq s-1$ is the number of parts of π and finally*

$$B(\pi) = (q-1)^b q^{l+T-1-b} \binom{s-1}{f_T, f_{T-1}, \ldots, f_2, f_1, s-1-b} .$$

The asymptotic GV-theorem is obtained by taking base q logarithms, dividing by s and taking the limit of the result for $s \longrightarrow \infty$ on both sides of the equation in the statement of Theorem 4. Denote the value of this limit as the **asymptotic contribution.** The right side's asymptotic contribution is $m/s = 1-R$. We need to make sure that the asymptotic contribution of the left side is less than that.

As a first step we simplify the left side. Denote by $p(k)$ the number of partitions of k. It follows from the famous Hardy-Ramanujan-Rademacher approximation for the partition function $p(k)$ (see [1]) that $\lim_{k\to\infty} \log(p(k))/k = 0$. This implies that instead of the sum it suffices to use the maximal value $B(\pi)$, where π varies over the partitions of $k-T$. This leads to the number $B'(\pi)$, which is asymptotically equivalent to $B(\pi)$.

Definition 9.

$$B'(\pi) = (q-1)^b q^{k-b} \binom{s-1}{f_T, f_{T-1}, \ldots, f_2, f_1, s-1-b} .$$

We need to show that under the conditions of Theorem 3 the asymptotic contribution of $B'(\pi)$ is less than $1-R$, where we can choose π to be a partition of k with a maximal value of $B'(\pi)$.

Recall that k/s approaches δ. We can assume $k/s = \delta$. Rewrite the multinomial in Definition 9 as

$$\binom{s-1}{f_T, \ldots, f_1, s-1-b} = \binom{s-1}{b} \binom{b}{f_1, f_2, \ldots, f_T}.$$

Next we use a famous link between multinomials and Shannon entropy:

Lemma 1. *Let $n, m_i \to \infty$ such that $m_1 + m_2 + \cdots + m_k = n$ and $\lim(m_i/n) = p_i$. Then*

$$\lim \frac{\log_2 \binom{n}{m_1, m_2, \ldots, m_k}}{n} = H(p_1, p_2, \ldots, p_k) .$$

Introduce the parameter $\alpha = b/k$, the relative number of parts of the partition. We continue under the assumption that the value of α is fixed. Recall that by definition $\alpha\delta \leq 1$ as $b \leq s-1$. The asymptotic contribution of $\binom{s-1}{b}$ is the limit of $\log_q(2)h(b/(s-1))$, which is $\log_q(2)h(\alpha\delta)$. The asymptotic contributions of the powers of q and of $q-1$ are obvious. They are $\delta - \alpha\delta$ and $\log_q(q-1)\alpha\delta$, respectively. Only the asymptotic contribution of the multinomial

$$\binom{b}{f_1, f_2, \ldots, f_T} = \binom{f_1 + f_2 + \cdots + f_T}{f_1, f_2, \ldots, f_T}$$

is in doubt. Recall that we are fixing $\alpha = b/k$. This means $k = \sum i f_i = b/\alpha$.

Lemma 2.
$$\sum_{j=1}^{T} j x^{j-1} = \frac{1-x^{T+1}}{(1-x)^2} - \frac{(T+1)x^T}{1-x} \ .$$

Proof. Let $f(x) = \sum_{j=0}^{T} x^j = (1-x^{T+1})/(1-x)$. Then
$$f'(x) = \sum_{j=1}^{T} j x^{j-1} = \frac{1-x^{T+1}-(1-x)(T+1)x^T}{(1-x)^2} \ .$$
□

By Lemma 1 maximizing the multinomial under the side condition $\sum i f_i = b/\alpha$ is the same as maximizing the entropy $H(p_1, p_2, \dots)$, where the p_i describe a probability distribution, under the side condition $\sum i p_i = 1/\alpha$. The solution to this optimization problem is known in information theory, see Chapters 11 and 12 of Cover/Thomas [5].

Proposition 1. *Let a natural number T and a positive real number α be given. The maximal value of the entropy function $H(p_1, p_2, \dots, p_T)$ under the side condition $\sum_i i p_i = 1/\alpha$ is achieved when $p_i = p_1 c^{i-1},\ i = 1, \dots, T$, where $p_1 = (1-c)/(1-c^T)$ and $0 < c < 1$ is the solution of the equation*
$$\frac{1-c^{T+1}}{1-c^T}\frac{1}{1-c} - \frac{(T+1)c^T}{1-c^T} = \frac{1}{\alpha} \ . \tag{1}$$

The corresponding maximal value of the entropy function is
$$-\log_2(p_1) - \frac{c\log_2(c)}{1-c} + \frac{Tc^T\log_2(c)}{1-c^T} \ . \tag{2}$$

Proof. We quote from Cover/Thomas [5] that H is maximized by a choice $p_i = p_1 c^{i-1}$ for a constant $0 < c < 1$. The value of p_1 as a function of c follows from the condition $\sum_i p_i = 1$. The value of c follows from the side condition $\sum_i i p_i = 1/\alpha$:
$$1/\alpha = p_1 \sum_{i=1}^{T} i c^{i-1} = \frac{1-c}{1-c^T}\left(\frac{1-c^{T+1}}{(1-c)^2} - \frac{(T+1)c^T}{1-c}\right) =$$
$$= \frac{1-c^{T+1}}{1-c^T}\frac{1}{1-c} - \frac{(T+1)c^T}{1-c^T} \ .$$
With these values for c, p_1 the entropy is
$$H(p_1, p_1 c, \dots, p_1 c^{T-1}) = -\sum_{i=1}^{T} p_1 c^{i-1}\log_2(p_1 c^{i-1}) \ .$$

The terms containing $\log_2(p_1)$ contribute $-\log_2(p_1)$, the remaining terms yield

$$-p_1 \log_2(c)\left(c + 2c^2 + \cdots + (T-1)c^{T-1}\right) .$$

Factoring out c, using Lemma 2 and substituting $p_1 = \frac{1-c}{1-c^T}$ the claim is obtained. $\square$

Recall that in Proposition 1 the quantities $c = c(T)$ and $p_1 = p_1(T) = \frac{1-c(T)}{1-c(T)^T}$ depend on T.

Lemma 3. *We have* $\lim_{T\to\infty} c(T) = 1-\alpha$ *and* $\lim_{T\to\infty} p_1(T) = \alpha$.

Proof. Equation 1 shows $\lim_{T\to\infty} c(T) = 1-\alpha$. The statement concerning p_1 follows. $\square$

Equation 2 yields the maximal asymptotic value of the entropy for the fixed value of α. It is

$$-\log_2(\alpha) - \frac{(1-\alpha)\log_2(1-\alpha)}{\alpha} = \frac{h(\alpha)}{\alpha} .$$

The asymptotic contribution of $\binom{b}{f_1, f_2, \ldots, f_T}$ is therefore the maximum over all α of $\lim(\log_q(2)\frac{l}{s}h(\alpha)/\alpha) = \log_q(2)\delta h(\alpha)$. Adding up the asymptotic contributions of the left side we arrive at $F_q(\alpha, \delta)$. This completes the proof of Theorem 3.

4. The net-entropy function

The value $\alpha = 1$ in $F_q(\alpha, \delta)$ corresponds to the case of codes. Not surprisingly the corresponding function $F_q(1, \delta) = H_q(\delta)$ is precisely the q-ary entropy function of coding theory, see Theorem 1. The maximum of $H_q(\delta)$ is 1. The condition $F_q(1, \delta) < 1 - R$ is therefore always satisfied when $R < 0$. This is in consonance with the fact that depth 1 can always be reached when $m > s$. In the other extremal case $\alpha = 0$ we obtain $F_q(0, \delta) = \delta$.

We want to show that Theorem 3 is equivalent with Theorem 2. An exercise in basic calculus yields the following:

Lemma 4.

$$\frac{\partial F_q}{\partial \alpha} = \delta \cdot \left(\log_q\left(\frac{(q-1)(1-\alpha)(1-\alpha\delta)}{\alpha^2\delta}\right) - 1\right) .$$

The derivative $\partial F_q/\partial\alpha$ approaches ∞ for $\alpha \longrightarrow 0$ and $-\infty$ for $\alpha \longrightarrow 1$. In case $\delta > 1$ we have $\alpha \leq 1/\delta$ and $\partial F_q/\partial\alpha$ approaches $-\infty$ for $\alpha \longrightarrow 1/\delta$. It follows that none of the extremal values at $\alpha = 0$ and $\alpha = \min(1, 1/\delta)$ is the maximal value of

F_q. The maximum occurs when the fraction under the logarithm equals q, which means $(q-1)(1-\alpha\delta)(1-\alpha) = q\alpha^2\delta$, equivalently

$$\delta = \frac{(q-1)(1-\alpha)}{(q-1)\alpha + \alpha^2} \ .$$

Definition 10. $d_q(x) = \dfrac{(q-1)(1-x)}{(q-1)x + x^2}$.

Observe that $d_q(x)$ is decreasing for $0 < x < 1$, $\lim_{x\to 0} d(x) = \infty$, and $d(1) = 0$. We have seen that for every δ the maximum of $F_q(\alpha, \delta)$ is reached when α is chosen such that $\delta = d_q(\alpha)$, in other words

Proposition 2.

$$F_q(\delta) = F_q(\alpha, \delta)$$

where $\delta = d_q(\alpha)$, *equivalently* $\alpha = \dfrac{\sqrt{q-1}\sqrt{1+6\delta+\delta^2} - (q-1)(1+\delta)}{2\delta}$.

The form given in Theorem 2 is obtained when we use the definition of the entropy function and the relations

$$\alpha\delta = \frac{(q-1)(1-\alpha)}{q-1+\alpha} \quad \text{and} \quad 1 - \alpha\delta = \frac{q\alpha}{q-1+\alpha} \ .$$

This concludes the proof of Theorem 2.

It is interesting to see when the existence of nets of rate 0 can be guaranteed. This corresponds to $(m-k, m, m)_q$-nets. In the binary case let δ_0 be defined by $F_2(\delta_0) = 1$. We have $\delta_0 \approx 0.263103$. In particular, linear $(0.737m, m, m)_2$-nets exist for large m.

We illustrate with another parametric example for $q = 2$. Choose $\delta = 8/105$. The maximum happens at $\alpha = 7/8$ (check: $\alpha\delta = 7/105 = 1/15$, so the above equation is $(1/15)(7/8) + 1/15 + 7/8 - 1 = 0$). In this case we have

$$F_2(\delta) = F_2(8/105) = 1/105 + h(1/15) + (8/105)h(1/8) \approx 0.40 \ .$$

The asymptotic GV-bound predicts the existence of linear $(\frac{17}{21}m, m, \frac{5}{2}m)_2$-nets for large enough m.

5. Comparison with the AG-construction

The Niederreiter-Xing construction (see [17]) shows that linear $(g, m, s)_q$-nets exist for every $m \geq g$ if there is an algebraic curve defined over $\mathbb{F}_q$ of genus g and with at least s rational points. This leads back to a much-studied question, the optimal ratio of the genus and the maximal number of rational points.

Definition 11. *Let $A(q) = \limsup_{g\to\infty} N_q(g)/g$ over all curves defined over $\mathbb{F}_q$, where g is the genus and $N_q(g)$ is the maximal number of rational points.*

The Drinfeld-Vladut bound [6] shows $A(q) \le \sqrt{q} - 1$. It is known that this bound is achieved with equality when q is a square (see [19]). For cubic fields the lower bound $A(q^3) \ge 2(q^2 - 1)/(q + 2)$ is known (see [2]). The best known lower bound in the binary case appears to be $A(2) \ge 81/317 \approx 0.2555$, see Niederreiter/Xing [15, 16].

The AG-construction shows that (δ, R) is asymptotically reachable by linear q-ary nets if $\delta = (m - g)/s = (1 - R) - g/s \le 1 - R - 1/A(q)$. It follows that the line of slope -1 through $(0, 1 - 1/A(q))$ is asymptotically reachable. A comparison of those asymptotic bounds reveals that the AG-bound is better for large values of δ. In fact, the GV-bound shows that any rate less than R_{GV} can be reached, where $R_{GV} = 1-F_q(\delta)$. The corresponding AG-bound is $R_{AG} = 1 - 1/A(q) - \delta$. We have $R_{AG} \ge R_{GV}$ if $\delta + 1/A(q) \le F_q(\delta)$. This is equivalent with $\log_q((q - 1 + \alpha)/\alpha) - \delta \log_q(1 - \alpha) \ge 1 + 1/A(q)$ and with

$$\frac{q - 1 + \alpha}{\alpha} \frac{1}{(1 - \alpha)^\delta} \ge q^{1+1/A(q)} \ .$$

As the first factor on the left side goes to ∞ for $\alpha \longrightarrow 0$ and the second factor is ≥ 1, this is satisfied when δ is large enough. Using the lower bound of $81/317$ for $A(2)$ this happens when $\delta > 9.6745$ in the binary case. Should the upper bound $A(2) \le \sqrt{2} - 1$ be achieved with equality the point of intersection moves to $\delta \approx 2.64$.

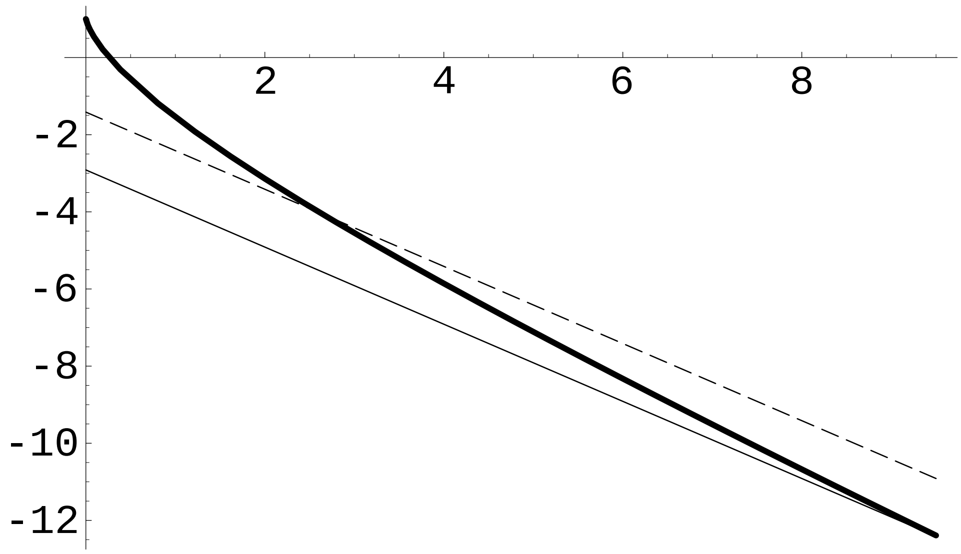

Figure 1: GV-bound and AG-bound

In Figure 1 we compare the bounds in the binary case. δ is on the horizontal axis, R on the vertical. The straight lines represent two versions of the AG-bound, the lower corresponding to the pessimistic value $81/317$, the upper to the optimistic value of $\sqrt{2}-1$ for $A(2)$.

References

[1] G. Andrews: *The Theory of Partitions, Encyclopedia of Mathematics and Its Applications, Addison-Wesley* 1976.

[2] J. Bezerra, A. Garcia and H. Stichtenoth: *An explicit tower of function fields over cubic finite fields and Zink's lower bound.* Submitted, 2004.

[3] J. Bierbrauer: *Introduction to Coding Theory*, Chapman & Hall/CRC, Boca Raton, FL, 2005.

[4] J. Bierbrauer, Y. Edel and W. Ch. Schmid: *Coding-theoretic constructions for (t,m,s)-nets and ordered orthogonal arrays, J. Combin. Designs* **10** (2002), 403–418.

[5] T. M. Cover and J. A. Thomas: *Elements of Information Theory,* Wiley 1991.

[6] V. G. Drinfeld and S. G. Vladut: *Number of points of an algebraic curve, Functional Anal. Appl.* **17** (1983), 53-54.

[7] Y. Edel and J. Bierbrauer: *Construction of digital nets from BCH-codes.* In H. Niederreiter et al., editors, *Monte Carlo and Quasi-Monte Carlo Methods 1996, Lecture Notes in Statistics* **127**, Springer 1998, 221–231.

[8] Y. Edel and J. Bierbrauer: *Families of ternary (t,m,s)-nets related to BCH-codes, Monatsh. Math.* **132** (2001), 99–103.

[9] K. M. Lawrence: *A combinatorial characterization of (t,m,s)-nets in base b, J. Combin. Designs* **4** (1996), 275–293.

[10] W. J. Martin: *Linear Programming bounds for ordered orthogonal arrays and (t,m,s)-nets.* In H. Niederreiter and J. Spanier, editors, *Monte Carlo and Quasi-Monte Carlo Methods 1998, Springer 2000,* 368–376.

[11] W. J. Martin and D. R. Stinson: *Association schemes for ordered orthogonal arrays and (t,m,s)-nets, Canadian Journal of Mathematics* **51** (1999), 326–346.

[12] G. L. Mullen and W. Ch. Schmid: *An equivalence between (t,m,s)-nets and strongly orthogonal hypercubes, J. Combin. Theory A* **76** (1996), 164–174.

[13] H. Niederreiter: *Point sets and sequences with small discrepancy, Monatsh. Math.* **104** (1987), 273–337.

[14] H. Niederreiter and G. Pirsic: *Duality for digital nets and its applications, Acta Arith.* **97** (2001), 173–182.

[15] H. Niederreiter and C. P. Xing: *Towers of global function fields with asymptotically many rational places and an improvement on the Gilbert-Varshamov bound, Math. Nachr.* **195** (1998), 171–186.

[16] H. Niederreiter and C. P. Xing: *Rational points on curves over finite fields: Theory and Applications,* Cambridge University Press, Cambridge 2001.

[17] H. Niederreiter and C. P. Xing: *Digital nets, duality and algebraic curves.* In H. Niederreiter, editor, *Monte Carlo and Quasi-Monte Carlo Methods 2002, Springer 2004*, 155–166.

[18] M. M. Skriganov: *Coding theory and uniform distributions, St. Petersburg Math. J.* **13** (2002), 301–337, translated from *Algebra i Analiz* **13** (2001), 191–239.

[19] M. A. Tsfasman, S. G. Vladut, Th. Zink: *Modular curves, Shimura curves and Goppa codes better than the Varshamov-Gilbert bound, Math. Nachr.* **109** (1982), 21–28.