Weakly biased arrays, weakly dependent arrays and error-correcting codes

Jürgen Bierbrauer
Department of Mathematical Sciences
Michigan Technological University
Houghton, Michigan 49931 (USA)

September 7, 2000

1 The bias and a direct link to codes

We study certain classes of structures, which are being widely used in computer science and cryptography. These structures comprise $\epsilon-$biased arrays, t-wise $\epsilon-$biased arrays and t-wise $\epsilon-$dependent arrays. A link between $\epsilon-$biased arrays and error-correcting codes will be exhibited. This paper is not designed to be published. Rather we make an effort to collect all the pertinent theory, including loose ends.

Definition 1. *An $(n, m)_q-$array is an array with n rows and m columns, where the entries are taken from a set with q elements.*

Definition 2. *Let p be a prime, $v = (v_1, v_2, \ldots, v_n) \in \mathbb{F}_p^n$. For every $i \in \mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ let $\nu_i(v)$ be the frequency of i as an entry of v and let $\delta_i(v)$ be defined by $\nu_i(v) = \frac{n}{p} + \delta_i(v)$. Let ζ be a primitive complex $p-$th root of unity. The* **bias** *of v is defined as*

$$bias(v) = \frac{1}{n}|\sum_{i\in F_p} \delta_i(v)\zeta^i| = \frac{1}{n}|\sum_{i\in F_p} \nu_i(v)\zeta^i|$$

Observe that $\sum_{i\in F_p} \delta_i(v) = 0$. We see that $0 \leq bias(v) \leq 1$ for every vector v. It is also clear that $bias(v) = 1$ if and only if v is a constant vector and that $bias(v) = bias(v+i)$ for every $i \in \mathbb{F}_p$. It is a more serious matter that $bias(v)$ depends on the choice of the root of unity ζ. However, we will always consider the bias of $\mathbb{F}_p-$linear spaces. As the change of root of unity corresponds to the consideration of a multiple of the vector, we see that the bias of an $\mathbb{F}_p-$vector space, defined as the maximum bias of its nonzero members, is defined with no ambiguity, and the result is independent of the choice of the p-th root of unity.

Definition 3. *Let $0 \leq \epsilon < 1$. An $(n,k)_p-$array is $\epsilon-$**biased** if every nontrivial linear combination of its columns has bias $\leq \epsilon$.*

Definition 2 shows that we should consider the linear code $\mathcal{C}$ generated by the columns of our $(n,k)_p-$array $\mathcal{A}$. If $dim(\mathcal{C}) < k$, then the 0-word is a nontrivial linear combination of the columns of $\mathcal{A}$. This shows that $\mathcal{A}$ cannot have a bias < 1. We can therefore assume that $\mathcal{C}$ is an $[n,k]_p-$code. Array $\mathcal{A}$ is the transpose of a generator matrix of $\mathcal{C}$ and the bias of $\mathcal{A}$ is the maximum bias of code-words of $\mathcal{C}$. Remains to understand the relationship between these two parameters, the **bias** and the **minimum distance.** The relationship is very easy to understand in the binary case: the binary word of length n and weight w has bias $|1-\frac{2w}{n}|$. The following is an easy consequence:

Theorem 1. *Let $0 \leq \epsilon < 1$. The following are equivalent:*

- *An $(n,k)_2$-array, which is $\epsilon-$biased.*
- *A binary linear code $\mathcal{C}$ of length n and dimension k, whose minimal distance d and maximal distance D satisfy*

$$Min\{\frac{d}{n}, \frac{n-D}{n}\} \geq \frac{1-\epsilon}{2}$$

- *A binary linear code $\mathcal{C}$ of length n and dimension k, all of whose nonzero words have weights w such that*

$$\frac{1-\epsilon}{2} \leq \frac{w}{n} \leq \frac{1+\epsilon}{2}$$

Let $\mathcal{C}' = \langle \mathcal{C}, \mathbf{1} \rangle$ be the $(k+1)-$dimensional code generated by $\mathcal{C}$ and $\mathbf{1}$. It is obvious that the minimum distance of $\mathcal{C}'$ is precisely $Min\{d, n-D\}$. This gives us the possibility to express the defining property of binary $\epsilon-$biased arrays in terms of the minimum distance of binary linear codes, as follows:

Theorem 2. *Let $0 \leq \epsilon < 1$. The following are equivalent:*

- *An $(n,k)_2$-array, which is $\epsilon-$biased.*
- *A binary linear code $\mathcal{C}'$ of length n and dimension $k+1$, which contains $\mathbf{1}$ and whose minimal distance d satisfies*

$$\frac{d}{n} \geq \frac{1-\epsilon}{2}$$

The quantity d/n is known as the **relative minimum distance.** We have seen that the relationship between bias and minimum distance is very tight in the binary case. For general p things get more complicated, but the following generalization is true:

Theorem 3. *Let p be a prime and $\mathcal{C}'$ a linear code $[n,k+1]_p$, which contains a word m of weight n. Let D be the maximum weight among the words not contained in $\langle m\rangle$. Let $\mathcal{C} \subset \mathcal{C}'$ be a hyperplane avoiding $\langle m\rangle$ (and hence a code $[n,k]_p$ with maximum weight D). The transpose of a generator matrix of $\mathcal{C}$ is an $(n,k)_p-$ array with bias $\epsilon \leq p\frac{D}{n}-(p-1)$.*

Proof. Let $0 \neq v \in \mathcal{C}$. The definition of D and the presence of m show that $\nu_i(v) \geq n-D$ for all $i \in \mathbb{F}_p$. Define $\mu_i(v) \geq 0$ by $\nu_i(v) = n-D+\mu_i(v)$. As the sum over all powers of ζ vanishes we have

$$\sum_i \delta_i(v)\zeta^i = \sum_i \nu_i(v)\zeta^i = \sum_i \mu_i(v)\zeta^i$$

and

$$|\sum_i \delta_i(v)\zeta^i| \leq \sum_i \mu_i(v) = \sum_i \nu_i(v) - p(n-D) = n-p(n-D) = pD-(p-1)n.$$

We conclude $bias(v) \leq p\frac{D}{n}-(p-1)$. ∎

In order to be on the safe side let us check that the upper bound on ϵ given in Theorem 3 is non-negative, as it should be. In fact, let $\mathcal{C}'$ be as in the theorem. Consider the array with all the codewords of $\mathcal{C}'$ as rows. Every column has precisely $(p-1)p^k$ nonzero entries. Counting all nonzero entries we obtain the inequality $n(p-1)p^k \leq (p-1)n + (p^{k+1}-p)D$. Solving for D yields $D \geq \frac{p-1}{p}n$. In particular we see that in the case of equality the array constructed in Theorem 3 is a two-weight code, equivalently $d=D$.

Here is a direct generalization of Theorem 2 from the binary to the $p-$ary case.

Theorem 4. *Let $\mathcal{C}'$ be a linear code $[n, k+1, d]_p$ containing a word m of weight n and $\mathcal{C}$ a maximal subcode not containing m. The transpose of a generator matrix of $\mathcal{C}$ is an $(n, k)_p-$ array with bias $\epsilon \leq (p-1) - p\frac{d}{n}$.*

Proof. Let $0 \neq v \in \mathcal{C}$. The definition of d shows $\nu_0(v) \leq n-d$. We can assume that m is the all-1-word. The presence of m shows that $\nu_i(v) \leq n-d$ for all i. Define $\kappa_i(v) = n-d-\nu_i(v) \geq 0$. As the sum of the roots of unity vanishes we have

$$|\sum_i \nu_i(v)\zeta^i| = |\sum_i \kappa_i(v)\zeta^i| \leq \sum_i \kappa_i(v) = p(n-d) - n = (p-1)n - pd.$$

We conclude $bias(v) \leq (p-1) - p\frac{d}{n}$. ■

Observe the following trivial example of an unbiased array ($\epsilon = 0$): The set of all $k-$tuples as rows is an unbiased $(p^k, k)_p-$array. If we fix p, k and ϵ we wish to minimize n such that an $\epsilon-$biased $(n, k)_p-$array exists.

The following construction is closely related to the **Powering construction** from [4]. A generalization is in Theorem 15

Theorem 5. *Let p be a prime and $\mathcal{C}$ a code $[n, k, d]_p$. Then there is an array $(pn, k)_p$, which is $(1-\delta)-$biased. Here $\delta = d/n$ is the relative minimum distance.*

Proof. Let G' be the transpose of a generator matrix of $\mathcal{C}$. Our array $\mathcal{A}$ is obtained by replacing every entry e of G' by a column $(0, e, 2e, \ldots, (p-1)e)^T$. Let $0 \neq v \in \mathcal{C}$ and $\tilde{v}$ the corresponding linear combination of columns of $\mathcal{A}$. Every nonzero entry of v leads to a string of p entries of $\tilde{v}$, where each element of $\mathbb{F}_p$ occurs once. This gives no contribution to the bias. Each entry 0 in v gives a string of p zeroes in $\tilde{v}$. We obtain $bias(v) = \frac{1}{pn}(n-w)p = 1 - \frac{w}{n}$, where $w = wt(v)$. ■

The Reed Solomon code $[p, k, p-k+1]_p$ has $\delta = 1 - \frac{k-1}{p}$.

Theorem 6. *Application of Theorem 5 to Reed-Solomon codes yields $(p^2, k)_p-$arrays, which are $\frac{k-1}{p}-$ biased, for every prime p and $k \leq p$.*

We can use the Gilbert-Varshamov bound (see [9]):

Theorem 7. *Let $V_p(n, i) = \sum_{j=0}^{i} \binom{n}{j}(p-1)^j$. If $V_p(n-1, d-2) < p^{n-k}$, then a code $[n, k, d]_p$ exists. By Theorem 5 it follows that a $(1-\delta)-$ biased array $(pn, k)_p$ exists.*

The asymptotic version is as follows:

Theorem 8. *Let $\delta \leq (p-1)/p, R \leq 1 - H(\delta) - \delta log_p(p-1)$. Then there is a family of $(1-\delta)-$ biased $(pn_i, k_i)_p-$arrays such that $lim(k_i/pn_i) \geq R/p$. Here $H(\delta) = -\delta log_2(\delta) - (1-\delta)log_2(1-\delta)$ is the entropy function.*

The drawback of this theorem is that it is not constructive. The most fruitful construction idea is the **randomizing** idea used in Theorem 6. We will meet it again. It is the same idea that led to the Justesen construction of explicitly described asymptotically nontrivial families of codes.

2 Limited bias and weak dependency

We define the notions that we are most interested in.

Definition 4. *Let $0 \leq \epsilon < 1$. An $(n, k)_p-$array is t-**wise** $\epsilon-$**biased** if every nontrivial linear combination of at most t of its columns has bias $\leq \epsilon$.*

Definition 5. *Let $0 \leq \epsilon < 1$. An $(n, k)_p-$array $\mathcal{A}$ is t-**wise** ϵ **-dependent** if for every set U of $s \leq t$ columns and every $a \in \mathbb{F}_p^s$ the frequency $\nu_U(a)$ of rows of $\mathcal{A}$, whose projection onto U equals a satisfies*

$$|\frac{\nu_U(a)}{n} - 1/p^s| \leq \epsilon.$$

Definition 6. *An $(n, N)_p-$array $\mathcal{A}$ is an $(n, N, t)_p-$ **covering array** if every projection of $\mathcal{A}$ to a set of t columns contains every t-tuple from $\mathbb{F}_p^t$.*

Both the notions of t-wise ϵ -dependent array and of a $t-$covering array generalize the notion of an orthogonal array of strength t. An array is t-wise independent (=0-dependent) if and only if it is an orthogonal array of strength t.

The standard construction of t-wise $\epsilon-$biased arrays is essentially from [32].

Theorem 9. *Let the following be given:*

- *An $(n, k)_p-$array B, which is $\epsilon-$biased.*
- *A linear code $[N, N-k, t+1]_p$.*

Then we can construct an $(n, N)_p-$array, which is t-wise $\epsilon-$biased.

Proof. Let H be a check matrix of the code, hence an $(k, N)_p$-array each t columns of which are linearly independent. Our array is the product $\mathcal{A} = BH$. Denote by r_i the rows of B, by c_j the columns of H, $i = 1, \ldots, n; j = 1, \ldots, N$. The entries of BH are the dot products $r_i \cdot c_j$. Let $0 \neq \lambda = (\lambda_1, \ldots, \lambda_N)$ of weight $\leq t$. The corresponding linear combination of columns of $\mathcal{A}$ has entry $v_i = r_i \cdot (\sum_j \lambda_j c_j)$ in row i. The defining property of H shows that $\sum_j \lambda_j c_j \neq 0$. Vector $v = (v_i)$ is therefore a nontrivial linear combination of the columns of B, hence has bias $\leq \epsilon$. ■

3 Fourier transform

Let $G = \mathbb{F}_p^k$ be the elementary abelian group of order $g = p^k$. Consider the space $L^2(G)$ of complex-valued functions on G, with scalar product $\langle , \rangle$, where

$$\langle f, g \rangle = \frac{1}{g} \sum_{x \in G} f(x) \cdot \overline{g(x)}.$$

Here $x = (x_1, x_2, \ldots, x_k) \in G$. As is generally known the characters of G form an orthonormal basis of $L^2(G)$. This is in fact easily checked. Let ζ be a primitive complex $p-$th root of unity. Every element $z = (z_1, z_2, \ldots, z_k)$ yields a character ϕ_z, where

$$\phi_z(x) = \zeta^{\sum x_i \cdot z_i} = \zeta^{x \cdot z}.$$

Definition 7. *Let $f \in L^2(G)$. Express $f(x)$ in terms of the characters in the form*

$$f = \sum_{z \in G} \hat{f}(z) \phi_z.$$

The complex numbers $\hat{f}(z)$ are known as the **Fourier coefficients** *of f. The* **mass** *of f is defined as*

$$mass(f) = g\langle f, 1 \rangle = g\hat{f}(0) = \sum_{x \in G} f(x).$$

Finally we define the **bias** *of $z \in G$ with respect to function f by*

$$bias_f(z) = \frac{g}{mass(\mid f \mid)} |\hat{f}(z)|$$

Observe that because of the orthonormality of the characters the Fourier coefficients are given by

$$\hat{f}(z) = \langle f, \phi_z \rangle = \frac{1}{g} \sum_{x \in G} f(x) \zeta^{-x \cdot z}.$$

Definition 8. *Let $\mathcal{A}$ be an $(n,k)_p-$array with entries in $I\!F_p$. The characteristic function $f(x) = \chi_{\mathcal{A}}(x)$ counts with which multiplicity x occurs as a row of $\mathcal{A}$. We define the Fourier transform $\hat{\mathcal{A}}(z)$, the mass and the bias of $\mathcal{A}$ by identifying $\mathcal{A}$ with its characteristic function and applying Definition 7. Observe $mass(\mathcal{A}) = n$.*

Let us compare the bias in Definition 8 with the combinatorial notion from Definition 3. So let $f = \chi_{\mathcal{A}}$ be the characteristic function of the $(n,k)_p-$array $\mathcal{A}$. As $f = |f|$ and $mass(f) = n$ we see that the bias of z in the sense of Definition 7 coincides with the bias of vector v, the linear combination of columns of $\mathcal{A}$ with z as vector of coefficients, in the sense of Definition 2.

Lemma 1. *Let $f = \chi_{\mathcal{A}}$ be the characteristic function of an $(n,k)_p-$array $\mathcal{A}$ and $z \in G = I\!F_p^k$. Then $bias_f(z)$ in the sense of Definition 7 is the same as $bias(v)$ in the sense of Definition 3, where v is the linear combination of the columns of $\mathcal{A}$ with z as vector of coefficients.*

The following characterization of t-wise ϵ -biased arrays in terms of their Fourier transform follows directly from Definition 7 and Lemma 1

Theorem 10. *An $(n,k)_p-$array $\mathcal{A}$ is t-wise ϵ -biased if and only if its Fourier coefficients $\hat{\mathcal{A}}(z)$ satisfy*

$$|\hat{\mathcal{A}}(z)| \leq \frac{n}{g}\epsilon \textit{ for } 0 < wt(z) \leq t.$$

4 The relation between dependency and bias

Definition 9. *Let $\mathcal{A}$ be an $(n,k)_p-$array, $f \in L^2(G)$. The* **expectation** *$E_{\mathcal{A}}(f)$ with respect to $\mathcal{A}$ is defined as the statistical expected value of f when the rows of $\mathcal{A}$ are used as a probability space with uniform distribution:*

$$E_{\mathcal{A}}(f) = \sum_{x \in G} \frac{\chi_{\mathcal{A}}(x)}{n} f(x)$$

The following lemma was inspired by [13]:

Lemma 2. *Let $\mathcal{A}$ be an $(n,k)_p-$array. Then the following are equivalent:*

- *$\mathcal{A}$ is t-wise $\epsilon-$dependent.*
- *for every subset U of $l \leq t$ columns and every $f \in L^2((\mathbb{F}_p)^U)$ the following holds:*

$$|E_U(f) - mass(f)/p^l| \leq \epsilon \cdot mass(|f|).$$

Here the expectation $E_U(f)$ is with respect to the restriction of $\mathcal{A}$ to the columns in U.

Proof. If f runs through the characteristic functions $\chi_a, a \in (\mathbb{F}_p)^U$, then the second condition expresses the definition of t-wise $\epsilon-$dependent arrays. So one direction of the equivalence is clear. Assume therefore $\mathcal{A}$ is t-wise $\epsilon-$dependent, fix U and denote by $\nu_U(a)$ the multiplicity of a as a row in the restriction to U. Consider a general function $f = \sum_a c_a\chi_a$. Because of the linearity of the expectation and the mass, we get $|E_U(f) - \frac{mass(f)}{p^l}| = |\sum_a c_a(\frac{\nu_U(a)}{n} - \frac{1}{p^l})| \leq \sum_a |c_a| \cdot \epsilon = \epsilon \cdot mass(|f|)$. ■

Lemma 3. *Let $\mathcal{A}$ be an $(n,k)_p-$array. Then the following are equivalent:*

- *$\mathcal{A}$ is t-wise $\epsilon-$biased.*
- *For every set U of $l \leq t$ columns and every $0 \neq z \in G$ with support in U, the restriction g_z of the character ϕ_z to $\mathbb{F}_p^U$ satisfies*

$$|E_U(g_z)| \leq \epsilon$$

Proof. We have $|E(g_z)| = |\sum_{x \in F_p^U} \frac{\nu_U(x)}{n}\zeta^{-x \cdot z}|$. Comparison with Definition 2 shows that $\mid E(g_z) \mid$ is the bias of the linear combination of columns of $\mathcal{A}$ with $-z$ as set of coefficients. ■

After these preparations we can start comparing bias and dependency.

Theorem 11. *Let $\mathcal{A}$ be a $p-$ary array, which is t-wise ϵ -dependent. Then $\mathcal{A}$ is i-wise $p^i\epsilon$-biased for all $0 < i \leq t$*

Proof. Lemma 2 gives a characterization of weak dependency in terms of a property, which all complex-valued functions defined on $(\mathbb{F}_p)^U$ have to satisfy, where U is a set of $i \leq t$ columns. Let U be given. Let g_z be the restriction to $(\mathbb{F}_p)^U$ of the character ϕ_z, where $0 \neq z \in (\mathbb{F}_p)^U$. Apply Lemma 2, observing $mass(g_z) = 0, mass(|g_z|) = p^i$. We get $|E(g_z)| \leq p^i \epsilon$. Apply Lemma 3. ∎

Theorem 12. *Let $\mathcal{A}$ be a $p-$ary array, which is i-wise δ_i-biased $(i = 1, 2, \dots, t)$. Then $\mathcal{A}$ is t-wise ϵ -dependent, where $\epsilon = (\sum_{i=1}^{t} \binom{t}{i} (p-1)^i \delta_i)/p^t$.*

Proof. Let $|U| = l \leq t, g_z$ as above, $h = p^l, a \in \mathbb{F}_p^U$. It is easy to check that $\chi_a = \frac{1}{h} \sum_z \zeta^{-a \cdot z} g_z$. By assumption $|E(g_z)| \leq \delta_{wt(z)}, z \neq 0$. Thus $|E(\chi_a) - \frac{1}{h}| = \frac{1}{h} |\sum_{z \neq 0} \zeta^{-a \cdot z} E(g_z)| \leq \frac{1}{h} \sum_{i=1}^{l} \binom{l}{i} (p-1)^i \delta_i$. The δ_i form by definition a non-decreasing series. It is easily seen that the last expression increases with l. This leads to the statement of the theorem. ∎

Two special cases deserve being mentioned.

Corollary 1. *Let $\mathcal{A}$ be a p-ary array. If $\mathcal{A}$ is $(t-1)$-wise 0-biased (equivalently: is an orthogonal array of strength $t-1$) and t-wise ϵ -biased, then $\mathcal{A}$ is t-wise $(\frac{p-1}{p})^t \epsilon$-dependent.*

Theorem 13. *Let $\mathcal{A}$ be a p-ary array. If $\mathcal{A}$ is t-wise ϵ -biased, $\epsilon > 0$, then $\mathcal{A}$ is t-wise ϵ'-dependent for some $\epsilon' < \epsilon$.*

Proof. If $\mathcal{A}$ is t-wise $\epsilon-$biased, then it is also i-wise $\epsilon-$biased for all $1 \leq i < t$. We can apply Theorem 12 with $\delta_i = \epsilon, i = 1, 2, \dots, t$. It follows that $\mathcal{A}$ is t-wise ϵ'-dependent, where $\epsilon' = \epsilon(\sum_{i=1}^{t} \binom{t}{i} (p-1)^i)/p^t = \epsilon(p^t - 1)/p^t < \epsilon$. ∎

Theorem 13 can be applied to the construction of covering arrays.

Theorem 14. *Let $\mathcal{A}$ be an $(n, N)_p-$array, which is t-wise p^{-t}-biased. Then $\mathcal{A}$ is an $(n, N, t)_p-$ covering array.*

Proof. Theorem 13 shows that $\mathcal{A}$ is $t-$wise ϵ'-dependent for some $\epsilon' < p^{-t}$. It follows right from Definition 5 that $\mathcal{A}$ must be $t-$covering. ∎

5 The basic reduction

The most interesting of our structures from the point of view of applications are probably $t-$wise ϵ-dependent arrays. Theorem 13 shows that it suffices to construct $t-$wise ϵ-biased arrays. Theorem 9 reduces this to the construction of ϵ-biased arrays. We concentrate on the following versions of the construction problem:

Problem 1. *Given ϵ, for which $a > 0$ can we find asymptotic constructions for $\epsilon-$biased $(n,k)_p-$arrays such that $n \leq (\frac{k}{\epsilon})^a$?*

Problem 2. *Given ϵ, for which $b > 0$ can we find asymptotic constructions for $\epsilon-$biased $(n,k)_p-$arrays such that $n = O(\frac{k}{\epsilon^b})$?*

Moreover we are interested in efficient constructions, not just proofs of existence.

It has been proved in the final version of [4] that $b \geq 2$. A nonconstructive argument in [6] shows that $b = 2$. This yields the complete answer to Problem 2: $b = 2$. Our main result will be that there are efficient constructions for every $a > 1$ in Problem 1 and for every $b > 2$ in Problem 2.

6 The Weil-Carlitz-Uchiyama construction

The celebrated Weil-Carlitz-Uchiyama bound [11] may be understood as a limit on the bias of dual BCH-codes. More precisely, let (a_j) be a basis of $\mathbb{F}_{p^f}|\mathbb{F}_p$ and $Tr : \mathbb{F}_{p^f} \longrightarrow \mathbb{F}_p$ the trace. Consider the array $\mathcal{A}$ whose rows are indexed by the elements $\alpha \in \mathbb{F}_{p^f}$ and whose columns are indexed by a_jX^i, where $i \leq n$ and i is not a multiple of p. The corresponding entry is $Tr(a_j\alpha^i)$. The WCU bound asserts that this $(p^f, f(n - \lfloor n/p \rfloor))_p-$array has bias $\leq (n-1)p^{-f/2}$.

7 The basic construction

The Weil-Carlitz-Uchiyama construction from Section 6 implies that $a = 2$ can be reached in Problem 1. Three relatively simple constructions of weakly biased arrays have been described in [4]. They all yield the same asymptotic statement $a = 2$ as the WCU construction. In fact, the WCU construction (the exponential sum method) yields somewhat better parameters. Nevertheless the constructions from [4] are very interesting because of their simplicity and because they invite generalizations.

Our basic construction is a generalization of what was called the **Powering construction** in [4].

Theorem 15. *Let $\mathcal{C}$ be a code $[n,k,d]_q$, where $q=p^m$. Let $v(1),\dots,v(k)$ be a basis of $\mathcal{C}$. Construct a $(qn,k)_p$-array $A(\mathcal{C})$ as follows: the columns are indexed by the basis elements $v(j)$, the rows are indexed by pairs (i,u), where i is a coordinate of the ambient space $\mathbb{F}_q^n$ containing the code $\mathcal{C}$ and $u\in\mathbb{F}_q$. The entry in row (i,u) and column j is*

$$tr(uv(j)_i).$$

Here $v(j)_i$ is the entry of $v(j)$ in coordinate i and $tr:\mathbb{F}_q\longrightarrow\mathbb{F}_p$ is the trace. Then $A(\mathcal{C})$ has bias $\leq 1-\frac{d}{n}$.

Proof. Let $\alpha=(\alpha_1,\dots,\alpha_k)\neq(0,\dots,0)$. Let c be the corresponding linear combination of the columns of $A(\mathcal{C})$. The entry of c in row (i,u) is

$$\sum_{j=1}^k\alpha_j tr(uv(j)_i)=tr((\sum_j\alpha_j v(j)_i)u)=tr(v_iu).$$

Here $0\neq v=\sum_j\alpha_jv(j)\in\mathcal{C}$. We imagine the rows of the array as being subdivided in n segments according to the value of i. If $v_i\neq 0$, then the corresponding segment of c is unbiased. If $v_i=0$, then the corresponding segment is 0. We obtain

$$bias(c)\leq\frac{(n-d)q}{nq}=1-\frac{d}{n}.$$

■

8 Efficient construction of codes

In order to make the most of Theorem 15 we need efficiently constructed families of extremly good codes. These are provided by algebraic-geometric codes.

Theorem 16. *Let q be a prime-power and $e\geq 1$ a rational number. Then there is an infinite set $\mathcal{M}$ of natural numbers such that em is a natural number for all $m\in\mathcal{M}$ and for every $m\in\mathcal{M}$ there is an algebraic curve $\mathcal{K}_m$ defined over $\mathbb{F}_{q^m}$ with more than q^{em} rational points and genus g_m, such that $lim_{m\in\mathcal{M}}\frac{g_m}{q^{em}}=0$.*

The basic mechanism of algebraic-geometric codes yields the following:

Theorem 17. *Let an algebraic curve (equivalently: a function field) with genus g be defined with $\mathbb{F}_q$ as field of constants, and with N rational points. Then for every $k < N-1$ we can construct a linear code with parameters $[N-1, k, N-k-g]_q$ (the minimal distance can actually be even higher).*

Theorem 16 yields codes $\mathcal{C}_m$ with parameters

$$[q^{em}, Rq^{em}, (1-R)q^{em} - g_m]_{q^m}.$$

The codes from Theorem 16 can be used to obtain efficient constructions for good $\mathbb{F}_q-$linear codes via the Justesen mechanism as well. Let $H(x) = H_2(x) = -xlog(x) - (1-x)log(1-x)$ be the binary entropy function ($0 \leq x \leq 1$) and

$$H_q(x) = \frac{1}{log(q)}(H(x) + xlog(q-1))$$

the q-ary entropy function. The **Zyablov bound** [38] states that the line $R = (1 - H_q(\mu))(1 - \frac{\delta}{\mu})$ is asymptotically reachable for all $0 \leq \mu \leq (q-1)/q$ by codes, which are obtained by standard concatenation with a Reed-Solomon code as an outer code and a code reaching the Gilbert-Varshamov bound as inner code. This bound may be called semi-constructive and is not terribly interesting in itself. A first constructive lower bound was obtained by Justesen [25]. We can use Justesen's idea and algebraic-geometric codes to show that the Zyablov bound is efficiently constructible.

Choose $\mathbb{F}_q-$linear injective mappings as follows:

$$\alpha : \mathbb{F}_{q^m} \longrightarrow \mathbb{F}_q^m, \beta : \mathbb{F}_{q^m} \longrightarrow \mathbb{F}_{q^{em}}, \gamma : \mathbb{F}_{q^{em}} \longrightarrow \mathbb{F}_q^{em}.$$

Let $\mathbb{F}_{q^{em}} = \{u_i\}$. Also, let $s \leq em$ and let $\pi : \mathbb{F}_q^{em} \longrightarrow \mathbb{F}_q^{em-s}$ be a projection. We define an $\mathbb{F}_q$-linear code $\tilde{\mathcal{C}}_m$ by concatenation and projection, as follows: let $(v_i) \in C_m$. The corresponding codeword of $\tilde{\mathcal{C}}_m$ is obtained by mapping the entry v_i to

$$\tilde{v_i} = (\alpha(v_i), \pi(\gamma(u_i\beta(v_i)))) \in \mathbb{F}_q^{m(e+1)-s}$$

The original Justesen construction is obtained in the special case when $e = 1, q = 2, \mathcal{C}_m$ is a Reed-Solomon code, and $s = 0$. In that case π is the identity and $\tilde{v_i} = (\alpha(v_i), \gamma(u_i\beta(v_i))) \in \mathbb{F}_2^{2m}$. Consider the case when $s = 0$. The basis for Justesen's construction is the following observation, which obviously is true: whenever $i \neq j$ and $v_iv_j \neq 0$, then the $m(e+1)-$tuples $\tilde{v_i}$ and $\tilde{v_j}$ are different. In the general case we are led to the following:

Lemma 4 (Justesen's observation). *Let $0 \neq (v_i) \in \mathcal{C}_m$. Then for every $x \in \mathbb{F}_q^{m(e+1)-s}$ there are at most q^s indices i such that $\tilde{v}_i = x$.*

Theorem 18. *The generalized Justesen construction as applied to codes $\mathcal{C}_m$ yields families of linear $q-$ary codes, which show that the line $R = (1 - H_q(\mu))(1 - \frac{\delta}{\mu})$ is asymptotically reachable for all $0 \leq \mu \leq H_q^{-1}(\frac{e}{e+1})$. This is the line in the $(\delta, R)-$plane through points $(0, 1 - H_q(\mu))$ and $(\mu, 0)$.*

The original (binary) Justesen construction led to the line through $(0, 1/2)$ and $(h^{-1}(1/2), 0)$, showing that all points on and below that Justesen line can be efficiently constructed.

It should be checked if an application of the basic construction Theorem 15 to codes meeting the Zyablov bound has some effect on Problem 2.

9 Construction of weakly biased arrays

Use the codes obtained from the curves in Theorem 16 in Theorem 15.

Theorem 19. *For every prime p, every rational number $e \geq 1$ and $0 < \epsilon < 1$ there is a family of $(n_i, k_i)_p-$arrays, which are ϵ_i- biased such that $lim_i \epsilon_i = \epsilon$ and*

$$lim_i(\frac{n_i}{(k_i/\epsilon_i)^{(e+1)/e}}) = 1.$$

This produces families of $\epsilon-$biased $(n, k)_p-$arrays, where asymptotically $n = (\frac{k}{\epsilon})^a$, for every $a > 1$. Here $a = (e+1)/e$ in the terminology of Theorem 19. Each family from Theorem 19 for a fixed value of e yields an exponent $a = (e+1)/e$ in Problem 1. Moreover these constructions are explicit. The usefulness of this construction is determined by how efficient the AG-codes are, which are used as ingredients. The Reed-Solomon codes are obtained from the projective line ($g = 0$). They yield $e = 1$, hence $a = 2$. This corresponds to the original powering construction from [4].

The first layer in the construction of [19] are the Hermitian curves. These satisfy the assumptions of Theorem 16 for $e = 1.5$ and therefore yield $a = 5/3$ in Problem 1.

We remark that Theorem 19 is best possible in the sense, that it is impossible to replace the exponent a, which is arbitrarily close to 1, but fixed, by $a = 1$. In fact, consider the binary case. A family of binary codes such that $n \sim k/\epsilon$ would give as point in $(\delta, R)-$space, which is asymptotically reachable by binary linear codes and meets the asymptotic Plotkin bound with equality. This is impossible as it contradicts the JPL-bound (for the original bound in the binary case see [30]). Still it is unsatisfactory that in Theorem 19 the dimension of the code appears with an exponent > 1. We can further generalize Theorem 15.

Theorem 20. *Let $\mathcal{C}$ be a code $[n,k,d]_q$, where $q = p^m$ and $\mathcal{B}$ an $(n_0,m)_p$-array of bias ϵ_0. We can construct an $(nn_0,km)_p-$array with bias $\epsilon = 1 - \delta + \delta\epsilon_0 < 1 - \delta + \epsilon_0$, where $\delta = d/n$ is the relative distance of code $\mathcal{C}$.*

Proof. Fix a basis $\{a_r \mid r = 1,\dots,m\}$ of $\mathbb{F}_q \mid \mathbb{F}_p$ and denote the columns of $\mathcal{B}$ by $b_r, r = 1,\dots,m$. Construct an $(nn_0,km)_p$-array $A(\mathcal{C},\mathcal{B})$ as follows: the columns $s(j,r)$ are indexed by pairs of basis elements $v(j)$ of the code and basis elements a_r of $\mathbb{F}_q \mid \mathbb{F}_p$. Let $v_i(j) = \sum_{r=1}^m \lambda_r^{(i,j)} a_r$. The rows come in sections of length n_0, the sections being indexed by the coordinates $i = 1,2\dots,n$. Section i of column $s(j,r)$ is $\lambda_r^{(i,j)} b_r$. We want to show that this array $A(\mathcal{C},\mathcal{B})$ has bias $\leq 1-\delta+\delta\epsilon_0$.

Let $s = \sum_{j,r}\mu(j,r)s(j,r)$ be a linear combination of the columns, where $\mu(j,r) \in \mathbb{F}_p$, not all zero. Every section of s is a linear combination of columns of $\mathcal{B}$, and hence either is 0 or has bias $\leq \epsilon_0$. It will suffice to show that there are at most $n-d$ indices i such that $s_i = 0$. We have

$$s_i = \sum_{j,r}\mu(j,r)\lambda_r^{(i,j)}b_r = \sum_r(\sum_j \mu(j,r)\lambda_r^{(i,j)})b_r.$$

It follows that $s_i = 0$ if and only if $\sum_{j=1}^k \mu(j,r)\lambda_r^{(i,j)} = 0$ for all r.

Consider the codeword $w^{(r)} = \sum_{j=1}^k \mu(j,r)v(j) \in \mathcal{C}$. As not all the coefficients $\mu(j,r) \in \mathbb{F}_p$ vanish we must have $w^{(r)} \neq 0$ for some r. If we expand the entry $w_i^{(r)}$ with respect to the basis a_r we obtain

$$w_i^{(r)} = \sum_r(\sum_{j=1}^k \mu(j,r)\lambda_r^{(i,j)})a_r.$$

Comparison shows that $s_i = 0$ if and only if $w_i^{(r)} = 0$. Choose r such that $w^{(r)} \neq 0$. It follows that at least d segments have $s_i \neq 0$. The bound on the bias follows from the following innocent Lemma 5, which is trivial. ∎

Lemma 5. *Let $v = (v_1,v_2,\dots,v_n)$, where $v_i \in \mathbb{F}_p^m$ and $bias(v_i) \leq \epsilon_i$. Then*

$$bias(v) \leq \frac{\sum_{i=1}^n \epsilon_i}{n}$$

Observe that Theorem 20 is both a generalization and a strengthening of Theorem 15. In fact, let $\epsilon_0 = 0$ in Theorem 20. We obtain an $(nn_0, km)_p-$array of bias $1-\delta$, whereas the basic construction Theorem 15 yields only an array with k columns and the same bias.

Apply Theorem 20 with Reed-Solomon codes $[p^m, Rp^m, (1-R)p^m]$ as outer codes. A first application of the basic construction to Reed-Solomon codes has provided us with arrays solving Problem 1 with $a=2$. There are therefore $(n_0, m)_p-$ arrays such that $n_0 \leq (m/\epsilon_0)^2$. Choose $R = \epsilon_0 = \epsilon/2$. Theorem 20 yields an $\epsilon-$biased $(N, K)_p-$array, where $N = n_0 p^m, K = km = Rmp^m$. For which exponent a' will it be true that

$$N = n_0 p^m = \frac{4m^2}{\epsilon^2} p^m \leq (K/\epsilon)^{a'} = (mp^m/2)^{a'}?$$

This will be true for every $a' > 1$ when m is large enough. We have a second construction showing that every exponent $a > 1$ in Problem 1, and the second construction does not involve complicated AG-codes.

10 Block covering systems

An analysis of the constructions in [32] and [2] suggests the introduction of the following concept.

Definition 10. *A* **block covering system** $BCS(n, l, b, \gamma, \epsilon)$ *is a family* $\mathcal{B}$ *of* l*-element subsets of a fixed* $n-$*set* Ω*, where* $|\mathcal{B}| = b$ *and the following holds: whenever* $W \subset \Omega, \mid W \mid = w$ *such that* $1 - \frac{w}{n} \leq \gamma$*, then*

$$\frac{\textit{number of blocks avoiding } W}{b} \leq \epsilon.$$

Here it is permitted that a point occurs in a block with multiplicity more than 1. It is also permitted that different blocks are made of the same set of points, even with the same multiplicities. Clearly, we are interested in $BCS(n, l, b, \gamma, \epsilon)$ with small l, small b and small ϵ.

In the language of graphs we can describe a BCS as a bipartite graph with n vertices on the left, $b \geq n$ vertices on the right, where each right vertex has precisely l neighbours. The defining property says that every sufficiently large set W of vertices on the left has as set of neighbours almost all vertices on the right. Here the sizes are measured with respect to the size of the underlying set. Set W must satisfy that a random choice of a left vertex lands in W with probability at least $1-\gamma$. Likewise a random choice among reight vertices lands in $\Gamma(W)$ with probability $\geq 1-\epsilon$. This notion is clearly closely related to concepts like **expanders** and **dispersers,** which are often used in theoretical computer science, see the survey [34]. In fact, a BCS can be seen as some kind of a disperser. The main differences are the following: in a disperser the dispersion is from the large set of vertices to the small set. Typically dispersers are very unbalanced. In BCS the dispersion happens the other way around, from the small set to the large set. Also, the assumption of regularity is on starting end for dispersers, on the receiving end for BCS. More importantly, in BCS the sizes of the subsets are measured relative to the size of the underlying set.

The family of all $l-$tuples (a **complete design**) is a $BCS(n,l,\binom{n}{l},1-\binom{w}{n},\binom{n-w}{l}/\binom{n}{l})$ for every w. Let $\mathcal{B}$ be a design $t-(n,l,\lambda)$, and fix W. The number of blocks intersecting W trivially is at most $\binom{n-w}{t}\lambda/\binom{l}{t}$. Dividing this by the number of all blocks we obtain

Lemma 6. *A design $t-(n,l,\lambda)$ is a $BCS(n,l,\binom{n}{t}\lambda/\binom{l}{t},1-\frac{w}{n},\binom{n-w}{t}/\binom{n}{t})$. Observe that $\epsilon=\binom{n-w}{t}/\binom{n}{t}\leq\gamma^t$.*

Another source for BCS are orthogonal arrays. The result of Gopalakrishnan and Stinson [23] may be expressed in our terminology as follows:

Theorem 21. *The rows of an $OA_1(2,l,q)$ form a*

$$BCS(q,l,q^2,\gamma,\frac{\gamma}{1+(1-\gamma)(l-1)}).$$

Observe that $OA_1(2,l,q)$ can be obtained by projecting from 2-dimensional Reed-Solomon codes.

An often used construction idea for BCS are walks in expander graphs. As a preparation we study Eigenvalues of induced subgraphs.

10.1 Eigenvalues of induced subgraphs

The following theorem was apparently first proved in [26]. A proof is also in [27].

Theorem 22. *Let Γ be a graph on n vertices, which is connected and regular of valency Δ. Let λ_1 be the second-largest Eigenvalue of the adjacency matrix A of Γ. Let W be a subset of w vertices and A_1 the adjacency matrix of the graph induced on the vertices not in W. Let $\gamma = 1 - \frac{w}{n}$.*

Then the maximal Eigenvalue of A_1 is at most $\gamma\Delta + (1-\gamma)\lambda_1$.

Proof. For every real vector $v = (v_1, \dots, v_n) \in \mathbb{R}^n$ denote $Q(v) = vAv^T$. Here Q is the quadratic form associated with A. Denote by P the orthogonal projection onto $V \setminus W$ with W as kernel. We have then $PAP = \begin{pmatrix} A_1 & 0 \\ 0 & 0 \end{pmatrix}$. Clearly A is a real symmetric matrix. Its Eigenvalues are therefore real. Denote these Eigenvalues by $\lambda_0 > \lambda_1 \geq \dots \lambda_{n-1}$. The largest Eigenvalue is $\lambda_0 = \Delta$, of multiplicity 1, with $\mathbf{1} = (1, 1, \dots)$ as Eigenvector. We want a bound on the maximum Eigenvalue of A_1, equivalently of PAP. We have $\lambda_0(PAP) = max_v \frac{vPAPv^T}{vv^T}$. As $vP = (v_1, 0)$ and P is symmetric, the numerator is $Q((v_1, 0))$. For fixed v_1 the denominator is minimal when $v = (v_1, 0)$. We have seen

$$\lambda_0(PAP) = max_x Q((x,0))/\|x\|^2, \text{ where } x \in \mathbb{R}^{n-w}.$$

For every vector z denote $\sigma(z) = z \cdot \mathbf{1}$, the sum of the entries of z. Write $(x, 0) = \frac{\sigma(x)}{n}\mathbf{1} + v$. Then $\sigma(v) = 0$ and $v = (v_1, -\frac{\sigma(x)}{n}\mathbf{1}_2)$ and $\sigma(v_1) = \frac{\sigma(x)}{n}w$. This shows that the set of all $(x, 0)$ can be described equivalently as the set of all $\mu\mathbf{1} + (z, -\mu\mathbf{1}_2)$, where $\sigma(z) = \mu w$. We have $\|\mu\mathbf{1} + (z, -\mu\mathbf{1}_2)\|^2 = \mu^2 n + \mu^2 w + \|z\|^2$. Also $Q(\mu\mathbf{1} + (z, -\mu\mathbf{1}_2)) = Q(\mu\mathbf{1}) + Q(v) = \mu^2 n\Delta + Q(v)$, where $v = (z, -\mu\mathbf{1}_2)$. As v is orthogonal to $\mathbf{1}$ we have $Q(v) \leq \lambda_1\|v\|^2$. This is where the second Eigenvalue of A comes into play. Observing $\|v\|^2 = \|z\|^2 + \mu^2 w$ we obtain the following bound:

$$\lambda_0(PAP) \leq max_{\mu,z} \frac{\mu^2 n\Delta + \lambda_1(\mu^2 w + \|z\|^2)}{\mu^2(n+w) + \|z\|^2},$$

where the maximum is over all $\mu \in \mathbb{R}$ and all $z \in \mathbb{R}^{n-w}$ satisfying $\sigma(z) = \mu w$. Equivalently we can take the maximum over all vectors $z \neq 0$ and calculate $\mu = \sigma(z)/w$. Our expression is

$$\frac{\sigma(z)^2 n\Delta/w^2 + \lambda_1(\sigma(z)^2/w + \|z\|^2)}{\sigma(z)^2(n+w)/w^2 + \|z\|^2}.$$

It is invariant under scalar multiples of z. We can therefore assume $\|z\| = 1$. The resulting expression is increasing as a function of $\sigma(z)$. By the Cauchy-Schwartz inequality the maximum value of $\sigma(z)$ is $\sqrt{n-w}$. With this value we obtain

$$\lambda_0(PAP) \leq \frac{\lambda_1 n/w + (n-w)n\Delta/w^2}{1 + \frac{n-w}{w^2}(n+w)}.$$

Multiply numerator and denominator by w^2. The denominator is then n^2. After simplification of the numerator we obtain $\lambda_0(PAP) \leq (1-\frac{w}{n})\Delta + \frac{w}{n}\lambda_1$. ■

10.2 BCS from graphs

The constructions to be discussed in this subsection are also used to obtain dispersers. This underlines the similarity of the concepts.

Definition 11. *Let Γ be a graph defined on the set V of vertices, $|V| = n$. Denote by $T_l = T_l(\Gamma)$ the set of all ordered l-tuples $(P_0, P_1, \dots, P_{l-1})$ of vertices, where P_i and P_{i+1} are adjacent, $i = 0, \dots, l-2$. Observe that when Γ is regular of valency Δ, then $|T_l(\Gamma)| = n\Delta^{l-1}$.*

As we are only interested in the set of points covered by a walk we can divide this number by 2 as each (ordered) walk yields the same set of points, including multiplicities, as the walk back.

Theorem 23. *Let Γ be a graph on n vertices, which is connected and regular of valency Δ. Let λ_1 be the second-largest Eigenvalue of Γ. The family $T_l(\Gamma)$ leads after identification of inverse walks to a $BCS(n, l, \frac{1}{2}n\Delta^{l-1}, \gamma, \gamma(\gamma + (1-\gamma)\frac{\lambda_1}{\Delta})^{l-1})$.*

Proof. Fix a set $W \subset V$ of w vertices, fix length l, let $\gamma = 1 - \frac{w}{n}$ and denote by $b_0 = b_0(W)$ the number of walks in $T_l(\Gamma)$, all of whose vertices are outside W. We aim at bounding b_0 in terms of λ_1. Use the terminology of Subsection 10.1. We have

$$b_0 = \mathbf{1}_1 A_1^{l-1} \mathbf{1}^T.$$

Here $\mathbf{1}_1$ is the all-1 vector of length $n-w$. Because of Theorem 22 we have $b_0 \leq (\gamma\Delta + (1-\gamma)\lambda_1)^{l-1}(n-w)$. Comparing with the number of all walks of length l we get $\frac{b_0}{b} \leq \frac{n-w}{n}(\gamma + (1-\gamma)\frac{\lambda_1}{\Delta})^{l-1}$. Identifying pairs of inverse walks does not change this ratio. ■

Theorem 23 can be found in [3].

A different and in a way dual method of obtaining BCS from graphs is to use the family of neighbours of vertices. The following basic result by Alon/Milman [5] can be used to determine the parameters:

Theorem 24. *Let Γ be a graph on n vertices, which is connected and regular of valency Δ. Let λ_1 be the second-largest Eigenvalue of Γ and $W \subset V$ a subset of w vertices, $\gamma = 1 - \frac{w}{n}$. For some $\rho > 1$ let B be the set of vertices at distance $\geq \rho$ from W. Then*

$$\frac{|B|}{n} \leq \frac{\gamma}{1 + \rho^2(1-\gamma)(1-\lambda_1/\Delta)}$$

In fact, this is just the special case of the corresponding lemma in [5] when the graph is regular. Another bound is proved in [2].

Theorem 25. *[quadratic bound] Let Γ be a graph on n vertices, which is connected and regular of valency Δ. Let λ_1 be the second-largest Eigenvalue of Γ and $W \subset V$ a subset of w vertices, $\gamma = 1 - \frac{w}{n}$. For some $\rho > 1$ let B be the set of vertices at distance $\geq \rho$ from W. Then*

$$\frac{|B|}{n} \leq \frac{\gamma}{1-\gamma}(\frac{\lambda_1}{\Delta})^2.$$

The quadratic bound is better than what follows from Theorem 24 when $\frac{\lambda_1}{\Delta}$ is small.

Let $\mathcal{B}$ be the family of all $i^\perp, i \in V$. Then $b = n$, the blocksize is Δ and the number b_0 of blocks avoiding W is precisely the number of vertices i at distance ≥ 2 from W. Application of Theorem 24 in case $\rho = 2$, and of Theorem 25 yields the following:

Theorem 26. *Let Γ be a graph on n vertices, which is connected and regular of valency Δ. Let λ_1 be the second-largest Eigenvalue of Γ. The family $\mathcal{B} = \{i^\perp \mid i \in V\}$ is a $BCS(n, \Delta, n, \gamma, Min\{\frac{\gamma}{1+4(1-\gamma)(1-\lambda_1/\Delta)}, \frac{\gamma}{1-\gamma}(\frac{\lambda_1}{\Delta})^2\})$.*

It is natural to generalize this by using as blocks the sets $N_r(i) = \{P \mid 0 < d(i,P) \leq r\}$. Again we can use Theorem 24 and obtain the following:

Theorem 27. *Let Γ be a graph on n vertices, which is connected and regular of valency Δ. Let λ_1 be the second-largest Eigenvalue of Γ. For $i \in V$ let $N_r(i) = \{P \mid 0 < d(i,P) \leq r\}$. The family $\mathcal{B} = \{N_r(i) \mid i \in V\}$ is a $BCS(n, \Delta(\Delta-1)^{r-1}, n, \gamma, \frac{\gamma}{1+(r+1)^2(1-\gamma)(1-\lambda_1/\Delta)})$.*

10.3 BCS, codes and $\epsilon-$biased arrays

Theorem 28. *Assume the following exist:*

- *A linear code $\mathcal{C}$ with parameters $[n,k,d]_q$*
- *A $BCS(n,l,b,1-\frac{d}{n},\epsilon)$ for some l.*

Then we can construct a q^l- ary $\mathbb{F}_q-$linear code $\tilde{\mathcal{C}}$ of length b, with just as many codewords as $\mathcal{C}$ and minimum distance (equal to minimum weight) $\geq (1-\epsilon)b$.

Proof. Let $v \in \mathcal{C}$. The corresponding codeword of $\tilde{\mathcal{C}}$ is $\tilde{v} = (\tilde{v}_B)$, where B varies through the blocks. Here $\tilde{v}_B = (v_i)_{i \in B}$. Observe that we interpret $\tilde{\mathcal{C}}$ as defined over $V(l,q)$, the vector space of dimension l over $\mathbb{F}_q$. Clearly $\tilde{\mathcal{C}}$ is linear over the ground field $\mathbb{F}_q$. This shows that minimum weight and minimum distance agree. Let $v \neq 0$. Then $\tilde{v}_B = 0$ if and only if $B \cap supp(v) = \emptyset$. The definition of a BCS shows that the number of such blocks is at most $\epsilon \cdot b$. ■

The output of Theorem 28 is a code, which is q^l-ary and $\mathbb{F}_q-$linear. We can use concatenation with any linear $q-$ary code of dimension l as inner code and produce a q-ary linear code.

Theorem 29. *Assume the following exist:*

- *A linear code $\mathcal{C}$ with parameters $[n,k,d]_q$*
- *A $BCS(n,l,b,1-\frac{d}{n},\epsilon)$ for some l.*
- *A linear code $\mathcal{D}$ with parameters $[n_0,l,d_0]_q$.*

Then we can construct a linear $q-$ary code

$$[n_0 b, k, (1-\epsilon)bd_0]_q.$$

The result in [2] is an application of Theorem 29 with the neighbours of points (see Theorem 26) as BCS. We remark that codes, which are q^l-ary but only $q-$linear (also known as **additive codes**) have recently found renewed interest. In [16, 24] the mechanism of BCH-codes is extended to cover also additive codes, in [17] use is made of this generalization of BCH-codes to construct quantum codes. We can use the method of Theorem 29 for the construction of weakly biased arrays as well. All we need to know is the bias of the inner code.

Theorem 30. *Assume the following exist:*

- *A binary linear code $\mathcal{C}$ with parameters $[n, k, d]_2$.*
- *A $BCS(n, l, b, 1 - \frac{d}{n}, \epsilon)$ for some l.*
- *An ϵ_0-biased $(n_0, l)_2-$array.*

Then we can construct an $(n_0 b, k)_2-$array, which is $\{\epsilon+\epsilon_0(1-\epsilon)\}-$biased.

Proof. As mentioned before the construction is the same as in Theorem 29. Denote the resulting code (after application of Theorem 28 and concatenation) as $\mathcal{C}'$. We need to control the bias of an arbitrary codeword v'. If $B \cap supp(v) = \emptyset$, then v'_B is a 0-tuple of length n_0. By definition of a BCS there are at least $(1 - \epsilon)b$ blocks B such that $B \cap supp(v) \neq \emptyset$. Each corresponding section v'_B is a nonzero codeword of the inner code, hence of bias $\leq \epsilon_0$. It follows that v'_B can have at most $\epsilon_0 n_0$ more zeroes than ones. The total surplus of zeroes in v' is therefore limited by $\epsilon b n_0 + (1-\epsilon) b \epsilon_0 n_0$. Division by the length bn_0 yields the desired upper bound on the bias. ∎

The construction of weakly biased binary arrays as given in [32] is an application of Theorem 30 in the binary case, where the inner code is the Simplex code $[2^l, l, 2^{l-1}]$ of bias $\epsilon_0 = 0$ and the BCS is the family of walks (see Theorem 23). We remark that the family of codes constructed in [32] and used in the role of code $\mathcal{C}$ in Theorem 30 is not interesting. In fact, the use of 2-dimensional Reed-Solomon codes makes sure that the family has to be asymptotically trivial.

Apply Theorem 30 with the following ingredients: Code $\mathcal{C}$ belongs to a family of asymptotically nontrivial codes with relative minimum distance δ. The BCS is derived from Ramanujan graphs (see [29]) on n vertices with valency Δ via Theorem 26. It has parameters $BCS(n, \Delta, n, 1-\delta, \frac{1-\delta}{\delta}\frac{4}{\Delta})$. The weakly biased array are derived from Theorem 19, an ϵ_0-biased $(n_0, \Delta)_p-$ array, where $n_0 = (\Delta/\epsilon_0)^{(e+1)/e}$. Choose $\epsilon_0 = \epsilon/2$ and Δ such that $\frac{1-\delta}{\delta}\frac{4}{\Delta} \leq \epsilon/2$. We obtain an $\epsilon-$biased $(N, K)_p-$ array, where $N = O(K/\epsilon^{2(e+1)/e})$.

We reach the promised conclusion: every exponent $b > 2$ in Problem 2 is reachable with an effective construction.

11 Constructions of weakly dependent arrays and covering arrays

We use Theorem 9 with the weakly biased arrays constructed in Section 9 and in Section 10.3 as one ingredient. Primitive BCH-codes have parameters $[p^i-1, p^i-1-it, t+1]_p$. The following is obtained:

Theorem 31. *Let p be a prime. For every natural number t and $a > 1$ there are efficient constructions for infinite families of t-wise $\epsilon-$ biased $(n,N)_p-$arrays, where asymptotically*

$$n \leq (\frac{tlog_p(N)}{\epsilon})^a$$

For every natural number t and $b > 2$ there are efficient constructions for infinite families of t-wise $\epsilon-$ biased $(n,N)_p-$arrays, where asymptotically

$$n = O(tlog_p(N)/\epsilon^b).$$

Theorem 13 shows that we can replace the term *t-wise $\epsilon-$ biased* in Theorem 31 by *t-wise $\epsilon-$ dependent.*

Theorem 14 implies the following:

Corollary 2. *There exist efficient constructions for $(n,N,t)_p-$covering arrays such that asymptotically $n = O(tlog_p(N)p^t)^a$ for every $a > 1$, and likewise there exist efficient constructions such that $n = O(tlog_p(N)p^{tb})$ for every $b > 2$.*

11.1 A problem in coding theory

As one of the ingredients for the derivation of Theorem 31 we used primitive BCH-codes. An attempt to optimize the code contribution leads to the following highly nontrivial problem in coding theory.

Definition 12. *Fix q and t. Denote by $n_{t,q}(k)$ the maximal length n of a code $[n, n-k, t+1]_q$, equivalently the largest length of a linear orthogonal array of dimension k and strength t. Define*

$$l(t,q) = lim\ inf_{k\rightarrow\infty}\frac{k}{log_q(n_{t,q}(k))}$$

The primitive $BCH-$codes show $l(t,q)\leq t$. This is what we have used in the derivation of Theorem 31. The Gilbert-Varshamov bound seems to give the same bound $l(t,q)\leq t$ as the BCH-codes. The general statement is as follows:

Theorem 32. *Let p be a prime. Assume there is an efficient construction for families of codes achieving $l(t,q)$. Then there are efficient constructions for the following:*

- *$t-$wise $\epsilon-$ biased $(n,N)_p-$arrays, where asymptotically*
$$n\leq (\frac{l(t,p)\cdot log_p(N)}{\epsilon})^a \text{ for } a>1,$$
- *t-wise $\epsilon-$ biased $(n,N)_p-$arrays, where asymptotically*
$$n=O(l(t,p)\cdot log_p(N)/\epsilon^b) \text{ for } b>2,$$
- *$(n,N,t)_p-$covering arrays such that asymptotically*
$$n=O(l(t,p)\cdot log_p(N)p^t)^a \text{ for } a>1,$$
- *$(n,N,t)_p-$covering arrays such that asymptotically*
$$n=O(l(t,p)\cdot log_p(N)p^{tb}) \text{ for } b>2.$$

Ludo Tolhuizen observes that the function $l(t,q)$ has been studied by Dumer in [15]. The sphere packing bound implies $l(t,q)\geq\lfloor t/2\rfloor$. We have
$$\lfloor t/2\rfloor\leq l(t,q)\leq t,$$
showing that we cannot improve on the $BCH-$code method by more than a factor of 2. Still, this is an interesting coding problem.

Let $t=1$. Clearly $n_{1,q}(k)=q^k-1$, hence $l(1,q)=1$. Clearly we have $l(t,q)\geq l(t-1,q)$ in general. When $t=2$ the maximum N such that a code $[N,N-k,3]_p$ exists is of course $N=(p^k-1)/(p-1)$. This yields $l(2,q)=1$.

Theorem 33. *If there is an $\epsilon-$biased $(n,k)_p-$array, then there is a 2-wise $\epsilon-$biased $(n,\frac{p^k-1}{p-1})_p-$array. In particular for every $a>1$ there are efficient constructions for infinite families of 2-wise $\epsilon-$ biased $(n,N)_p-$arrays, where asymptotically*
$$n\leq (\frac{log_p(N)+1}{\epsilon})^a$$
and for $(n,N,2)_p-$covering arrays, where asymptotically $n=O(p^2(1+log_pN))^a$.

Also, in the binary case we have $l(t,2) = \lfloor t/2 \rfloor$. To see this just use primitive $BCH-$codes with defining interval $[1, t/2]$ if t is even and $[0,(t-1)/2]$ if t is odd. In case $t = 3$ we obtain a question on caps. The $(q^2+1)-$caps in $PG(3,q)$ are known as ovoids. A product construction [31], when applied to the affine part of an ovoid, yields $q^{2i}-$caps in $PG(3i,q)$. This shows $l(3,q) \leq 3/2$. For general q the bound $l(3,q) \leq 3/2$ is the best bound known. It is an open general question on caps if $l(3,q) = 1$. The ternary case is special, too. It follows from a construction [10] based on the Hill cap that $l(3,3) < 1/log_3(2.21)$. Dumer claims having proved

$$l(4,q) \leq 7/3 \text{ and } l(5,q) \leq 3.$$

12 Authentication codes

An $(N,m)_p-$array is $(\delta,t)-$**almost strongly universal** (short $(\delta,t)-$ASU) if for every set $U = U_0 \cup \{u\}$ of t columns and every $a' \in \mathbb{F}_p^{t-1}, x \in \mathbb{F}_p$ the frequencies $\nu_{U_0}(a')$ and $\nu_U(a',x)$ satisfy

$$\mid \nu_U(a',x)/\nu_{U_0}(a') \mid \leq \delta.$$

This means that when we authenticate t messages using the same key, the opponent's conditional probability of guessing the authenticator for message number t based on his knowledge of the authenticators of the preceding $t-1$ messages is still bounded by δ. The following obvious fact was proved in [28]:

Theorem 34. *A t-wise $\epsilon-$ dependent array is $(\delta,t)-$ASU, where*

$$\delta = \frac{p^{-t}+\epsilon}{p^{-(t-1)}-\epsilon}.$$

Because of Theorem 12 we see that t-wise $\epsilon-$biased arrays yield authentication codes $(\delta,t)-$ASU. As an example start from $\epsilon-$biased arrays constructed out of Hermitian codes via Theorem 15. Consider the Hermitian code of dimension $k \sim \frac{1}{2}p^m$ defined over $\mathbb{F}_{p^m}$, where m is even (see Section 14). The parameters of the code are $[p^{3m/2}, \frac{1}{2}p^m, p^{3m/2}-p^m]$. Theorem 15 yields an $\epsilon-$ biased $(p^{5m/2}, \frac{1}{2}p^m)_p-$array, where $\epsilon = p^{-m/2}$. Apply Theorem 9 with the code $[p^{2i}, p^{2i}-3i, 4]_p$, obtained by the product construction (see [31]) from the affine part of the ovoid. Here $k \sim \frac{1}{2}p^m \sim 3i$. The result is a

$$3\text{-wise } p^{-m/2}- \text{ biased } (p^{5m/2}, p^{\frac{1}{3}p^m})_p - \text{array}.$$

In case $m = 6$ we obtain a $(p^{15}, p^{\frac{1}{3}p^6})_p-$array, which is $(\delta, 3)-$ASU, where $\delta \sim 2/p$. This can be used to authenticate a source with $\frac{1}{3}p^6 log(p)$ bits with $15 log(p)$ key bits, where the same authenticator is used for 3 consecutive messages. Choose for instance $p \sim 2^{41}$. The opponent's probability of success is limited by 2^{-40} in this case. We can authenticate a source of up to 2^{249} bits, using 615 key bits. The method of [28] would require more than 750 bits of key in this situation. Further improvements can be achieved by using Theorem 20 and more sophisticated AG-codes.

13 Covering arrays

Consider $(n, N, t)_p-$covering arrays.

Definition 13. *Consider $(n, N, t)_q-$covering arrays. Define*

$$c_q(t) = lim\ inf_N \frac{n}{log_q(N)} \text{ where } N \longrightarrow \infty.$$

It follows from Corollary 2 that $c_p(t)$ exists. Moreover we have effective constructions for families, which yield $c_p(t) = O(tp^{tb})$ for every $b > 2$. A non-constructive upper bound is in [21].

In case of strength $t = 2$ the mechanism of **Sperner capacity** solves the asymptotic problem completely, for all q. The result in [20] is

$$c_q(2) = \frac{q log_2 q}{2} \text{ for all } q.$$

A general construction principle for covering arrays involves perfect hash families.

Definition 14. *An $(N, n)_q-$array is* **perfectly $t-$hashing** *if for every set of t columns there is a row such that the entries in this set of columns are different. We use the notation $PHF(N; n, q, t)$. The most suggestive interpretation is obtained when we interpret the array as a family of N mappings from an n-set to a $q-$set. The defining property says then that for every set of t elements in the domain we can find a function whose restriction to these t points is injective.*

Theorem 35. *If a set of n_1 functions from an N-set to an $m-$set is perfectly $t-$hashing and a set of n_2 functions from the $m-$set to a q-set is t-covering, then the composition is a set of $n_1 n_2$ functions from an N-set to a $q-$set, which is again t-covering, hence an $(n_1 n_2, N, t)_q-$covering array.*

This has been formulated in the language of mappings, where the statement is indeed obvious. In order to apply Theorem 35 we need perfect hash families and small covering arrays. The only effective construction of perfect hash families seems to follow from the following remark of Alon [1], which makes use of codes again.

Lemma 7 (Alon). *Let $\mathcal{C}$ be a q-ary code of length N with minimum distance d and n codewords. Write the codewords as columns of an array. Then a $PHF(N; n, q, t)$ is obtained if t is chosen such that*

$$\frac{d}{N} > 1 - 1/\binom{t}{2}.$$

Proof. Almost trivial. Assume there is a t-set of columns (codewords) not satisfying the PHF-property. Calculate the sum of the distances between these codewords. This sum certainly is $\geq \binom{t}{2}d$. Looking at the coordinates and using that some entry is repeated in each row, we get an upper bound of $N \cdot (\binom{t}{2} - 1)$. Comparing these bounds we get $\frac{d}{N} \leq 1 - 1/\binom{t}{2}$. ∎

The main construction in [14] is an application of Theorem 35, our friends the AG-codes from Section 8 furnishing the perfect hash families. Intersecting codes are used in order to construct small covering arrays to which to apply the construction.

Definition 15. *A binary code $[n, k]_2$ is t-wise intersecting if for any t linearly independent codewords there is a coordinate, which is common to all the supports.*

The link with covering arrays (Theorem 4.3 in [14]) is as follows:

Theorem 36. *Assume the following exist:*

- *A binary code $[n, k]_2$, which is t-wise intersecting.*
- *A binary code $[N, N - k, t + 2]_2$.*

Then we can construct a $(2n + 2, N, t + 1)_2-$covering array.

Proof. This is a nice little combinatorial proof. Let B be a check matrix of the long code. This is a $(k, N)-$matrix of strength $t + 1$. Also, let T be the transpose of a generator matrix of the intersecting code. This is an $(n,k)-$matrix. The covering array is defined as follows: the first two rows are the 0-vector and the 1-vector of length N. Next comes TB (an $(n,N)-$matrix) followed by its complement. We have to show that for every non-constant binary $(t+1)-$tuple and any $t+1$ columns of TB either the tuple itself or its complement appears as a row of the corresponding projection of TB. To fix notation consider the first $t+1$ columns of TB. Because of the strength of B the columns $h_0,\dots,h_t$ of this projection are $t+1$ linear independent words of the intersecting code. Also, let the $(t+1)-$tuple in question be 1 in the first w coordinates, 0 in the remaining coordinates. Here comes the nice little idea: consider the following linear combinations:

$$y_1 = h_w + h_1, y_2 = h_w + h_2, \dots, y_{w-1} = h_w + h_{w-1},$$

$$y_w = h_0 + h_w, y_{w+1} = h_0 + h_{w+1}, \dots, y_t = h_0 + h_t.$$

These t elements are linearly independent again. By the t-intersecting property there is a coordinate i such that $y_j(i) = 1$ for all $j = 1,\dots,t$. The definition of the y_j shows that

$$h_0(i) = h_1(i) = \dots = h_{w-1}(i) \neq h_w(i) = \dots = h_t(i).$$

If $h_0(i) = 1$ this is the desired tuple, if $h_0(i) = 0$ it is the complement. ∎

Finally we must have constructions for t-wise intersection codes. Long intersecting codes can be constructed by concatenation out of codes over larger alphabets and short intersecting codes as inner codes.

Theorem 37. *Let the following be given:*

- *A code* $[N,K,D]_q$*, where* $q = 2^k$ *and* $1 - \frac{D}{N} < 2^{1-t}$*, and*
- *a* t*-wise intersecting* $[n,k]_2-$*code.*

Then the concatenation, a $[nN,Kk]_2-$*code, is* $t-$*wise intersecting.*

Proof. Let $\tilde{x_1},\tilde{x_2},\dots,\tilde{x_t}$ be linearly independent words of the concatenated code. Their preimages $x_i, i = 1,2,\dots,t$ in the q-ary code are $\mathbb{F}_2-$linearly independent. Concentrate on the 2^{t-1} binary linear combinations of the x_i with odd weight. As they are all nonzero and because of the asumptions on the relative minimum distance of the code there is some coordinate i, where they are all nonzero. This gives us t codewords $c_1,\dots,c_t$ of the inner (binary) code with the property that every binary linear combination of odd weight of these is nonzero. We want to show that there is some coordinate, where none of the c_i vanishes. Let $S \subseteq \{1, 2 \dots t\}$ be maximal such that the $c_i, i \in S$ are linearly independent. Because of the t-wise intersecting property there is some coordinate j such that $c_i(j) = 1$ for all $i \in S$. Let $i \notin S$. Because of the maximality of S we have that c_i is a binary linear combination of some of the $c_s, s \in S$. If the weight of this linear combination was even, we would have a vanishing sum of an odd number of the c_i, which is not the case. It follows that c_i is sum of an odd number of $c_s, s \in S$, hence $c_i(j) = 1$. ■

Let us see how these basic constructions are put together in [14] to produce efficient asymptotic constructions of binary covering arrays Here we do not worry about absolute constants. Start from a Reed-Solomon code $[2^u, t, 2^u - t]$ defined over $\mathbb{F}_{2^u}$. In order to meet the requirements of Theorem 37 (large relative distance) we must have u large enough, about $u = t + log(t)$. The Simplex code, of parameters roughly $[2^u, u, 2^{u-1}]_2$ is u-wise intersecting, in particular t-wise intersecting. Theorem 37 produces by concatenation $[2^{2u}, ut]_2$, which is t-wise intersecting. A relatively short covering array is produced by Theorem 36. BCH-codes yield $[N, N - ut, t + 1]_2$ (roughly), where $N = 2^u$. We have a covering array $(2^{2u+1}, 2^u, t)_2$. In the functional notation we have 2^{2u+1} functions from size $q = 2^u$ to size 2. Finally use the perfect hash construction Theorem 35, with AG-codes yielding the outer functions: $[2^{eu}, R2^{eu}, (1 - R)2^{eu}]_q$. The condition from Lemma 7 implies that $R \sim 1/t^2$, hence $k \sim 2^{eu}/t^2$. We obtain a $(2^{eu+2u}, 2^{u2^{eu}/t^2}, t)_2-$covering array. If we compute $n/log(N)$, the term 2^{eu} drops out, and we are left with $2^{2u}t^2/u$. Remembering $u = t + log(t)$ we obtain the promised value of $O(2^{2t}t^3)$.

Theorem 38. *There is an efficient construction for families of binary covering arrays showing $c_2(t) = O(t^3 2^{2t})$.*

The difference to the binary case of our mechanism is that the exponential part is 2^{2t}, whereas we are limited to 2^{bt}, where $b > 2$.

14 Hermitian codes for the user

An important ingredient in our constructions are AG-codes. The effeciency of these constructions hinge upon the effectiveness of the description of the AG-codes used. The first layer of the construction in [19] are the Hermitian codes. We describe how to obtain generator matrices for the Hermitian codes. A comparison with the Reed-Solomon codes shows that Hermitian codes are just as effectively described.

Consider the field extension $\mathbb{F}_{q^2} \mid \mathbb{F}_q$ and the corresponding trace tr and norm N, where $tr(x) = x + x^q, N(x) = x^{q+1}$. Our codes are defined over $\mathbb{F}_{q^2}$ and have length q^3.

The coordinates are parametrized by the pairs (α, β), where $N(\alpha) = tr(\beta)$. So we need to calculate traces and norms of all elements in the field and to list all these pairs in some order. There are q^3 such pairs.

The general build-up: We construct a $(q^3 - g, q^3)-$ matrix G with entries from $\mathbb{F}_{q^2}$. Here $g = \binom{q}{2}$. The first k rows of G generate the $k-$dimensional Hermitian code. It has parameters

$$[q^3, k, q^3 - k + 1 - g]_{q^2}.$$

The pole-order test: For $n = 0, 1, 2, \dots$ we have to decide if n is a **pole-order** or not. If n is a pole-order we determine its **coordinate vector** (i, j). This is done as follows: Let r be the remainder of n mod q, where $0 \leq r \leq q - 1$ and $-s$ the (negative) remainder of n mod $q + 1$, where $0 \leq s \leq q$. Then n is a pole-order if and only if

$$x = \frac{n - r}{q} \geq \frac{n + s}{q + 1} = y.$$

If $n \geq 2g$, then the pole-order test does not need to be performed. Every such number is a pole-order. If n is a pole-order, then $n = (q+1)i + qj$, where $i = (x - y)q + r, j = s$. The coordinate vector of n is (i, j).

Constructing the rows of G **:** Let $u_1 = 0, u_2 = q, u_3 = q + 1 \dots$ be the first pole-orders. If u_k has coordinate-vector (i, j), then the entry of row k of G in coordinate (α, β) is $\beta^i \alpha^j$.

We conclude that the use of Hermitian codes requires the usual field arithmetic, just as Reed-Solomon codes.

References

[1] N.Alon: *Explicit construction of exponential sized families of k-independent sets,* Discrete Mathematics **58**(1986),191-193.

[2] N.Alon,J.Bruck,J,Naor,M.Naor,R.Roth: *Construction of asymptotically good low-rate error-correcting codes through pseudo-random graphs,* IEEE Transaction on Information Theory **38**(1992),509-516.

[3] N.Alon,U.Feige,A.Wigderson,D.Zuckerman: *Derandomized graph products,* Computational Complexity(1995),60-75.

[4] N.Alon,O.Goldreich,J.Håstad,R.Peralta: *Simple constructions of almost k-wise independent random variables,* Random Structures in Algorithms **3**(1992), prelim. version Symposium 31st FOCS 1990,544-553.

[5] N.Alon and V.D.Milman: λ_1, *isoperimetric inequalities for graphs, and superconcentrators,* JCTB **38**(1985),73-88.

[6] Y Azar, R. Motwani and J. Naor: *Approximating probability distributions using small sample spaces,* Combinatorics **18**(1998), 151-171.

[7] C.H.Bennett,G.Brassard and J-M.Roberts: *Privacy amplification by public discussion,* SIAM J.Comput. 17,2(1988),210-229.

[8] J.Bierbrauer: *Bounds on orthogonal arrays and resilient functions,* Journal of Combinatorial Designs **3** (1995),179-183.

[9] J.Bierbrauer and Y.Edel: *Lengthening and the Gilbert-Varshamov bound,* IEEE Transaction on Information Theory **43**(1997),991-992.

[10] A.R.Calderbank and P.C.Fishburn: *Maximal three-independent subsets of* $\{0,1,2\}^n$, Designs, Codes and Cryptography **4** (1994),203-211.

[11] L.Carlitz and S.Uchiyama: *Bounds for exponential sums,* Duke Mathematical Journal **24** (1957),37-41.

[12] J.L.Carter and M.N.Wegman: *Universal Classes of Hash Functions,* J.Computer and System Sci. 18(1979), 143-154.

[13] B.Chor,O.Goldreich,J.Håstad,J.Friedman, S.Rudich and R.Smolensky: *The bit extraction problem or t-resilient functions,* Proc. 26th Symp. on Foundations of Computer Science (1985),396-407.

[14] G.D.Cohen and G.Zémor: *Intersecting codes and independent families,* IEEE Transaction on Information Theory **40**(1994),1872-1881.

[15] Ilya Dumer: *Nonbinary double-error-correcting codes designed by means of algebraic verieties,* IEEE Transactions on Information Theory **41**(1995),1657-1666.

[16] Y.Edel and J.Bierbrauer: *Twisted BCH-codes,* Journal of Combinatorial Designs **5** (1997), 377-389.

[17] Yves Edel and J.Bierbrauer: *Quantum twisted codes,* Journal of Combinatorial Designs, to appear.

[18] O.Gabber and Z.Galil: *Explicit construction of linear sized superconcentrators,* Journal on Computer and System Science **22**(1981),407-420.

[19] A.Garcia and H.Stichtenoth: *A tower of Artin-Schreier extensions of function fields attaining the Drinfeld-Vladut bound,* Inventiones Mathematicae **121**(1995),211-222.

[20] L. Gargano, J. Körner and U. Vaccaro: *Sperner Capacities,* Graphs and Combinatorics **9**(1993),31-46.

[21] A.Godbole, D.E.Skipper and R.A.Sunley: *t-Covering arrays: upper bounds and Poisson approximations,* Combinatorics, Probability and Computing **5**(1996),105-118.

[22] O.Goldreich and A.Wigderson: *Tiny families of functions with random properties: a quality-size trade-off for Hashing,* Proceedings STOC 1994, 574-583.

[23] K.Gopalakrishnan and D.R.Stinson: *A simple analysis of the error probability of two-point based sampling,* Information Processing Letters **60**(1996),91-96.

[24] M.Hattori,R.J.McEliece and G.Solomon: *Subspace subcodes of Reed-Solomon codes,* IEEE Transactions on Information Theory **44**(1998),1861-1880.

[25] J.Justesen: *A class of asymptotically good algebraic codes, IEEE Transactions on Information Theory* **18**(1972),652-656.

[26] N.Kahale : *Better expansion for Ramanujan graphs, Proc. 33rd FOCS 1992,* 398-404.

[27] N.Kahale : *Eigenvalues and expansion of regular graphs, Journal of the ACM* **42** (1995), 1091-1106.

[28] K.Kurosawa, T.Johansson and D.Stinson: *Almost k-wise independent sample spaces and their cryptologic applications, Lecture Notes in Computer Science* **1233**(1997),409-421 (Advances in Cryptology, Eurocrypt 97).

[29] A.Lubotzky, R.Phillips and P.Sarnak: *Explicit expanders and the Ramanujan conjectures, Proceedings 18th ACM Symposium Theory of Computing 1986,* 240-246.

[30] R.J.McEliece, E.R.Rodemich, H.Rumsey, L.R.Welch: *New upper bounds on the rate of a code via the Delsarte-MacWilliams inequalities, IEEE Transactions on Information Theory* **23**(1977),157-166.

[31] A.C. Mukhopadhyay: *Lower bounds on $m_t(r,s)$, Journal of Combinatorial Theory A* **25**(1978),1-13.

[32] J.Naor and M.Naor: *Small-bias probability spaces: efficient constructions and applications, SIAM Journal on Computing* **22**(1993),838-856, preliminary version: Proceedings STOC 1990, 213-223.

[33] M.Naor and O.Reingold: *On the construction of pseudo-random permutations:Luby-Rackoff revisited,* Proceedings STOC 29(1997),189-199,
complete version under
http://theory.lcs.mit.edu/ tcryptol/homepage.html

[34] N. Nisan: *Extracting randomness: How and Why - A Survey, Complexity 96.*

[35] B.Z.Shen: *A Justesen construction of binary concatenated codes that asymptotically meet the Zyablov bound for low rate, IEEE Transaction on Information Theory* **39**(1993),239-242.

[36] V.Vazirani: *Randomness, adversaries and computation,* Ph.D. Thesis, University of California, Berkeley (1986).

[37] M.N.Wegman and J.L.Carter: *New Hash Functions and Their Use in Authentication and Set Equality,* J.Computer and System Sci. 22(1981),265-279.

[38] V.V.Zyablov: *An estimate of the complexity of constructing binary linear cascade codes,* Problems in Information transmission **7**(1971),3-10.