CODING THEORY SEMINAR, SPRING 1996

I. Introduction to Code Division Multiple Access systems

I.1. The configuration.

Let us suppose that a physical channel is shared by several users. The realization of sharing can be done in many ways, for example:

- Time division: Each user is given a certain period of time to use the channel and the turn shifts to the next user.
- Frequence division: In the case of radio channel each user is given a frequence level to use. This corresponds to the situation that each user has a channel of his own.
- Code division (CDMA): The messages of the users are coded together to form a single message which is sent to the channel.

Let us now concentrate to the last situation. One can easily invent trivial methods to encode messages together so that the receiver can effectively compute the "partial message" of a single sender. For example, suppose that k users send a message from binary alphabet $\{0,1\}$. All these messages are composed together to form a binary sequence $a_1a_2\dots a_k$ of lenght k, whose i:th component is the message of the i:th user, or a special empty symbol if the i:th user is not sending. Then this sequence is sent to the channel. It is obvious that this naive method works, but now rises the question whether there exist better methods.

We shall now introduce the basic ideas behind a CDMA system. Here we consider only the case where the alphabet is $\{0,1\}$, *binary* alphabet. The i:th user is given a characteristic binary vector, say $\mathbf{s}_i = (s_i(0), s_i(1), \dots s_i(n-1))$ (These are later referred as sequences). This corresponds to a unique complex vector $\mathbf{c}_i = (c_i(0), c_i(1), \dots, c_i(n-1))$, where $c_i(t) = (-1)^{s_i(t)}$ for all $t \in \{0, 1, \dots, n-1\}$. In other words, all zeros in the original vector are transformed to 1:s and 1:s are transformed to -1:s. Then each user encodes his message into a complex vector of length n as follows:

$$\begin{cases} 0 \longrightarrow +\mathbf{c}_i, \\ 1 \longrightarrow -\mathbf{c}_i, \\ \text{silence} \longrightarrow \mathbf{0}, \end{cases}$$

where $\mathbf{0} = (0, 0, \dots, 0)$ denotes the origin. After this all the messages are added together in $\mathbb{C}^n$ in the natural way, and the resulting vector, say $\mathbf{r}$ is sent to the channel. We can immediately see that the absolute value of any component of $\mathbf{r}$ can not be greater than the number of the users, say N.

Typeset by $\mathcal{A}\mathcal{M}\mathcal{S}$-TEX

We shall now consider how the receiver acts. For simplicity, we suppose that he recieves the vector $\mathbf{r}$ correctly. To find the message sent by the i:th user the reciever computes the hermitian inner product in the space $\mathbb{C}^n$:

$$\mathbf{c}_i \cdot \mathbf{r} = \mathbf{c}_i \cdot (\pm\mathbf{c}_1 + \pm\mathbf{c}_2 \pm \ldots \pm \mathbf{c}_N) = \pm n + \sum_{j \neq i} \mathbf{c}_i \cdot (\pm\mathbf{c}_j).$$

The receiver decides, that 0 was sent, if $\mathbf{c}_i \cdot \mathbf{r} > 0$ and 1 was sent if $\mathbf{c}_i \cdot \mathbf{r} < 0$. To guarantee that this system really works, we must be sure that the absolute value of the remainder

$$\sum_{j \neq i} \mathbf{c}_i \cdot (\pm\mathbf{c}_j)$$

is always less than n, the length of the vectors. This means that we have to require the vectors $\mathbf{c}_k$, $k \in \{1, 2, \ldots, N\}$ to be as orthogonal-like as possible. On the other hand, it would be convinient to find very large sets of such vectors to offer an opportunity to use the channel for a very large set of users. In practice, it can be assumed that the number of active senders is small, but the system is built to sustain a large number of *potential users.*

Let us now define *the even crosscorrelation* of vectors $\mathbf{c}_i$ and $\mathbf{c}_j$.

$$\mathbf{C}_{ij} = \mathbf{c}_i \cdot \mathbf{c}_j = \sum_{k=0}^{n-1} c_i(k) c_j(k) = \sum_{k=0}^{n-1} (-1)^{s_i(k)} \cdot (-1)^{s_j(k)} = \sum_{k=0}^{n-1} (-1)^{s_i(k) - s_j(k)}$$

In general, the messages of different users need not to be in the same phase, but there is some shift, so we define *the shift map* S to be

$$S(c_0, c_1, c_2, \ldots, c_{n-1}) = (c_1, c_2, \ldots, c_{n-1}, c_0),$$

and *the even shifted crosscorrelation* by

$$\mathbf{C}_{ij}(t) = S^t \mathbf{c}_i \cdot \mathbf{c}_j = \sum_{k=0}^{n-1} (-1)^{s_i(k+t) - s_j(k)},$$

where the sum $k + t$ is counted modulo n. Even shifted crosscorrelations will also be called even crosscorrelations. If $i = j$ above, we talk about *autocorrelation* instead of crosscorrelation. It may also happen that a negated vector $-\mathbf{c}_i$ overlaps with original one, so we define a negacyclic shift N by

$$N(c_0, c_1, c_2, \ldots, c_{n-1}) = (c_1, c_2, \ldots, c_{n-1}, -c_0),$$

and *odd crosscorrelation* by

$$\overline{\mathbf{C}}_{ij}(t) = N^t \mathbf{c}_i \cdot \mathbf{c}_j = \sum_{k=0}^{n-t-1} (-1)^{s_i(k+t) - s_j(k)} - \sum_{k=n-t}^{n-1} (-1)^{s_i(k+t) - s_j(k)}.$$

We conclude that we should require to all even and odd crosscorrelations to be small when compared to n. In practice, the sequences used are very long, and finding effectively large sets of sequences with good crosscorrelation properties turns out to be very diffucult problem. Several problems arise:

- Find effective constructions for sets of sequences as large as possible and similary having good correlation properties.
- Find theoretical upper bounds for the cardinality of sequence set having crosscorrelations at most a given value.
- Develop theoretical methods to estimate correlations without consuming too much computation time.

It has turned out that one can find good methods for a construction of sequence sets, and good theorethical tools to estimate the even crosscorrelations. Usually, the odd crosscorrelations are much more difficult to estimate, and generally they are simply calculated by computer. However, there is lot of space between known sequence sets and known theoretical bounds.

I.2. Elementary tools.

In this text $\mathbb{F}_q$ always means a finite field with q elements. It is known that the multiplicative group of a finite field is always cyclic. By a *primitive element* of $\mathbb{F}_q$ we mean a generator of the multiplicative group $\mathbb{F}_q^*$.

If not stated othewise, $q = 2^m$ for some $m \geq 1$, so $\mathbb{F}_q = \mathbb{F}_{2^m}$ is a finite extension of degree m of prime field $\mathbb{F}_2$. The automorphism group $\mathrm{Gal}(\mathbb{F}_{2^m}/\mathbb{F}_2)$ of field extension $\mathbb{F}_{2^m}/\mathbb{F}_2$ is known to be a cyclic group of order m, generated by *Frobenius-automorphism* $\sigma : \mathbb{F}_{2^m} \longrightarrow \mathbb{F}_{2^m}$, $\sigma(\alpha) = \alpha^2$. Therefore, the $\mathbb{F}_2$-conjugates of a given element $\alpha \in \mathbb{F}_{2^m}$ are

$$\alpha, \alpha^2, \alpha^{2^2}, \dots, \alpha^{2^{m-1}}.$$

Now we can define the *trace* of α to be the sum of its conjugates, namely,

$$T_{\mathbb{F}_2}^{\mathbb{F}_{2^m}}(\alpha) = \alpha + \alpha^2 + \alpha^{2^2} + \ldots + \alpha^{2^{m-1}}.$$

If there is no danger of confusion, we use a simple notation $T(\alpha)$. It not very difficult to show that T is a $\mathbb{F}_2$-linear mapping from $\mathbb{F}_{2^m}$ *onto* $\mathbb{F}_2$. Therefore, excatly half of elemets of $\mathbb{F}_{2^m}$ has trace 0 and half of them trace 1.

I.3. Connection to the character sums.

Let us now fix γ, a generator of $\mathbb{F}_{2^m}^*$. Suppose now that we have a set P of polynomials in $\mathbb{F}_{2^m}[X]$. Let us define for each $f \in P$ a binary vector $\mathbf{s}(f)$ of length $2^m - 1$ by

$$\mathbf{s}(f) = (T(f(\gamma^0)), T(f(\gamma^1)), T(f(\gamma^2)), \dots, T(f(\gamma^{2^m-2}))).$$

Then the corresponding complex vector, discussed before, will be

$$\mathbf{c}(f) = ((-1)^{T(f(1))}, (-1)^{T(f(\gamma))}, (-1)^{T(f(\gamma^2))}, \dots, (-1)^{T(f(\gamma^{2^m-2}))}).$$

If we now denote $e(\alpha) = (-1)^{T(\alpha)}$, where $(-1)^{T(\alpha)}$ is interpreted in an obvious way, we find out that e is a *character* of the additive group of $\mathbb{F}_{2^m}$, i.e. a mapping

$e : \mathbb{F}_{2^m} \to \mathbb{C}^*$ satisfying $e(\alpha+\beta) = e(\alpha)e(\beta)$. Complex vector $\mathbf{c}(f)$ can now be written as

$$\mathbf{c}(f) = (e(f(1)), e(f(\gamma)), e(f(\gamma^2)), \ldots, e(f(\gamma^{2^m-2})))$$

Suppose now that the set P of polynomials is an additive subgroup of $\mathbb{F}_{2^m}[X]$. Let us compute the correlation of $\mathbf{c}(f_1)$ and $\mathbf{c}(f_2)$, where f_1 and f_2 are in P. then $f = f_1 + f_2 \in P$, too.

$$\begin{aligned}\mathbf{C}_{f_1,f_2} = \mathbf{c}(f_1)\cdot\mathbf{c}(f_2) &= \sum_{i=0}^{2^m-2} e(f_1(\gamma^i))e(f_2(\gamma^i)) = \sum_{i=0}^{2^m-2} e(f_1(\gamma^i)+f_2(\gamma^i))\\ &= \sum_{i=0}^{2^m-2} e(f(\gamma^i)) = \sum_{x\in\mathbb{F}_{2^m}^*} e(f(x))\end{aligned}$$

We say that the sequence set $S(P) = \{\mathbf{s}(f) \mid f \in P\}$ is induced by P. As we saw, the question of determinig the correlations of $S(P)$ turns into a question of estimating the character sums. Well-known result of Weil, Carlitz and Uchiyama states that if a non-constant polynomial f is not of form g^2+g+b for all $g \in \mathbb{F}_{2^m}[X]$ and $b \in \mathbb{F}_{2^m}$ (This can be guaranteed for example requiring that f is of odd degree), then

$$\left|\sum_{x\in\mathbb{F}_{2^m}} e(f(x))\right| \le (\deg f - 1)\sqrt{2^m}.$$

In general, this result can not be improved, but in some cases we may find a polynomial group P of special type, and have a better upper bound for this special group.

I.4. Generalisation into larger alphabets.

There is an evident way to generalize this setup into the situation where the alphabet used is of prime number cardinality. Let us assume that the size of our alphabet is the prime field $\mathbb{F}_p$, and $\mathbb{F}_{p^m}$ an extension of $\mathbb{F}_p$. Similary, we can then define the trace mapping $T : \mathbb{F}_{p^m} \to \mathbb{F}_p$ to be

$$T(\alpha) = \alpha + \alpha^p + \alpha^{p^2} + \ldots + \alpha^{p^{m-1}},$$

and the character of the additive group of $\mathbb{F}_{p^m}$ by

$$e(\alpha) = \mathrm{e}^{\frac{2\pi i}{p}T(\alpha)}.$$

Here $\mathrm{e}^{\frac{2\pi i}{p}}$ is a *primitive p:th root of unity.*

The Carlitz-Uchiyama -bound takes now form:

$$\left|\sum_{x\in\mathbb{F}_{p^m}} e(f(x))\right| \le (\deg f - 1)\sqrt{p^m},$$

if f is non-constant polynomial and $f \neq g^p + g + b$ for all $g \in \mathbb{F}_{p^m}[X]$ and $b \in \mathbb{F}_{p^m}$.

I.5 Theoretical bounds for correlations.

The aim is to introduce some bounds for a parameter while the other parameters remain fixed. Assume that S if a set of sequences of length n. We define the *maximum correlation of* S to be

$$\mathbf{C}_{\max}(S) = \max\{|\mathbf{C}_{ij}(t)| \mid 1 \le i, j \le m, 0 \le t \le n-1, i \ne j \text{ if } t = 0\}.$$

It is now however natural to require that all the sequences in S cyclically distinct, i.e. one cannot transform any sequence in S into an other by cyclic shifts. Then we define S' to be the set of the elements of S and their cyclic shifts. Let us now agree on further terminology. We say that a set of sequences, S', is an (n, M, θ)-code, if its length is n, the size of S' is M and $\mathbf{C}_{\max}(S) \le \theta$. This means that the cardinality of the set is counted assuming that all the cyclic shifts of sequences are included, but the maximum correlation is counted with only one representative from each class of cyclic shifts. The maximal number of cyclically distinct sequences is denoted by $m(n, \theta)$. The number $m(n, \theta)$ can be trivially estimated by inequality

$$m(n, \theta) \le \frac{M(n, \theta)}{n}.$$

Furthermore, we define

$$M(n, \theta) = \max\{M \mid \text{ an } (n, M, \theta)\text{-code exists}\}$$

and

$$\theta(n, M) = \min\{\theta \mid \text{ an } (n, M, \theta)\text{-code exists}\}.$$

The purpose is now to find good upper bounds for $M(n, \theta)$ and good lower bounds for $\theta(n, M)$. An interesting parameter will also be the *mean-square* correlation of a (n, M, θ)-code S defined to be

$$\mu_{ms} = \frac{1}{M(M-1)} \sum_{\mathbf{c}_i \in S'} \sum_{\substack{\mathbf{c}_j \in S' \\ \mathbf{c}_i \ne \mathbf{c}_j}} |\mathbf{C}_{ij}|^2 .$$

We have now the terminology needed to state a classical result:

Proposition I.5.1 (Welch). *Let k be a nonnegative integer. The maximum correlation of an (n, M, θ)-code S' is bounded by*

$$\mathbf{C}_{\max}(S')^{2k} \ge \frac{1}{M(M-1)} \left(\frac{n^{2k} M^2}{\binom{k+n-1}{k}} - M n^{2k} \right).$$

Solving M from the Welch bound we obtain

$$M(n, \theta) \le \frac{n^{2k} - \theta^{2k}}{\frac{n^{2k}}{\binom{k+n-1}{k}} - \theta^{2k}},$$

if the denominator is positive.

For the proof, and the proofs missing after this, see: Sami Koponen: On the Correlation of Sequences.

Also a famous result, usually better than Welch bound, was obtained by Sidelnikov. This bound will not however be introduced here.

Better bounds than these two classical ones are obtained by the means of *linear programming.* To mention one, let us first define *Krawtchouk polynomials* $K_k(x) = K_k(n, x)$ (n is usually thought to be fixed) by the equation

$$\sum_{k=0}^{\infty} K_k(n,x)z^k = (1+z)^{n-x}(1-z)^x.$$

The very first ones are $K_0(x) = 1$, $K_1(x) = n - 2x$ and $K_2(x) = \frac{1}{2}(K_1(x)^2 - n)$. Krawtchouk polynomials are one single case of *orthogonal polynomials*, and many nice properties of Krawtchouk polynomials can be proven under general theory. One of them is

Proposition I.5.2. *Krawtchouk polynomial $K_k(x)$ has k distinct zeros in the interval $(0, n)$. If ξ_i and ξ_{i+1} are two consequtive ones, then K_{k-1} has exactly one zero in (ξ_1, ξ_{i+1}).*

We will denote the smallest zero of $K_k(x)$ by ξ_k.

The following theorem is due to Levenshtein and independently to Tarnanen and Lahtonen.

Proposition I.5.3 (LP-bound). *Assume that $r \leq \frac{n-2}{2}$ is a positive integer, $\theta = n - 2a$ and $\xi_{r+2} < a < \xi_r$. Then*

$$M(n,\theta) \leq \binom{n}{r} \frac{((n-r)(n-r-1)+\rho)^2}{(n^2-\theta^2)\rho},$$

Where $\rho = -\frac{(r+1)(r+2)K_{r+2}(a)}{K_r(a)}$.

It is often convinient to investigate the ultimate behaviour of known bounds when n tends to infinity. Then we speak about *Asymptotic bounds.* One of the reasons to this is the simplier form of bounds and another is that long sequences will permit a CDMA system to have many potential users.

To obtain some terminology, we introcude a notion: Assume that at least $g(n)$ is positive. Then $f(n) \lesssim g(n)$ means that $f(n) \leq g(n)(1 + a_n)$, where a_n is a sequence that tends to 0 as n tends to infinity. It also turns out to be convinient first to investigate $M(n, a\sqrt{n})$ as a function of a and then let n tend to infinity. For example, the asymptotical behaviour of LP-bound is given by

Proposition I.5.4. *Let r be a positive integer and $\zeta_r < b < \zeta_{r+2}$. then*

$$M(n, b\sqrt{n}) \lesssim -\frac{H_r(b)}{r!H_{r+2}(b)} n^{r+1},$$

where $H_r(x)$ is r:th Hermite polynomial and ζ_r the largest zero of $H_r(x)$

Hermite polynomials can be defined by recurrence formula

$$H_{k+1}(x) = xH_k(x) - kH_{k-1}(x)$$

with $H_0(x) = 1$ and $H_1(x) = x$.

I.6 Examples of constructions.

Consider field $\mathbb{F}_{2^m}$, choose $n = 2^m - 1$, and $1 \leq t \leq 2^{\frac{m}{2}-1}$. Set

$$P = \{\sum_{j=1}^{t} a_j x^{2j-1} \mid a_j \in \mathbb{F}_{2^m}\}.$$

Set P is straightforwardly seen to be an additive subgroup of $\mathbb{F}_{2^m}[X]$. Then define the code S to be

$$S(P) = \{\mathbf{s}(f) \mid f \in P\}$$

with notations as in I.3. Now we can estimate the maximum correlation of S to obtain

$$\left|\sum_{k=0}^{n-1} e(f(\gamma^k)) + 1\right| \leq (\deg f - 1)2^{\frac{m}{2}} \leq (t-1)2^{\frac{m}{2}+1}$$

by the Carlitz-Uchiyama bound. It can be observed that the sequence set obtained is the dual code of a t-error correcting binary BCH code. Furthermore, this construction yields $(2^m)^t$ sequences of length $n = 2^m - 1$, but they are not cyclically distinct. The number of cyclically distinct codewords is given by $(2^m)^{t-1}$, and the maximum correlation is bounded above by $2(t-1)2^{\frac{m}{2}} + 1$.

Assume that we have constructed such a set of sequnces of length $2^m - 1$. If we, for example can put $t = 3$, we have $(2^m)^2$ potential users, and the maximum correlation is then given by $4 \cdot 2^{\frac{m}{2}} + 1$. So in theory, there could be approximately $2^{\frac{m}{2}}$ active users simultaneously, but in practice, the correlations cancel each other, and the number of active users can be larger.

Let now $m = 2k$ be even. Then there lies an intermediate field $\mathbb{F}_{2^k}$ in between $\mathbb{F}_{2^m}$ and $\mathbb{F}_2$, and we can choose an element $\varepsilon \in \mathbb{F}_{2^m} \setminus \mathbb{F}_{2^k}$. Choose now a set of polynomials

$$P = \{x + \sum_{j=0}^{t} \beta_j x^{2^{k-j}+1}\},$$

where $\beta_0 \in \varepsilon\mathbb{F}_{2^k}$, $\beta_i \in \mathbb{F}_{2^m}$ when $i > 1$. Then form $S(P)$ as before and choose representatives which are cyclically disjoint. It can be shown that this construction yields a set of sequencies with cardinality $q^{t+\frac{1}{2}}$ and maximum correlation at most $2^t \cdot 2^{\frac{m}{2}} + 1$. These sets are called *Kasami sets.* When $t = 0$, the set is called *small or ordinary Kasami set*, with $t = 1$ we speak about *large Kasami set*, and for $t \geq 2$ the set is said to be *very large Kasami set.*

It should be emphasized, that the method described here is not the original method how ordinary Kasami set was invented. Some of the classical methods for finding good sets of sequencies are linear recurrence and combinig known sequences.

I.7 Constructions using ring arithmetics.

Here we speak only about commutative rings. Furthermore, it is assumed that any ring is equipped with the unit element. An ideal I of ring R is said to be maximal, if it is not contained in any other proper ideal.

By a *local ring* we understand a ring with unique maximal ideal. It can be shown that the residue class ring $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$ is local if and only if $n = p^m$ is a prime power. Rings $\mathbb{Z}_{p^m}$ are called *prime rings.* Let us then investigate the extensions of prime rings.

Suppose that the prime ring $\mathbb{Z}_{p^m}$ is a subring of ring S. Then we say that $S/\mathbb{Z}_{p^m}$ is a *ring extension* and that S is an *extension ring* of $\mathbb{Z}_{p^m}$.

If the ring extension is regular enough, we can observe that S is a local ring too. Even more, we have automorphims group of extension $S/\mathbb{Z}_{p^m}$ cyclic as in the case of field extensions. Such regular extensions of prime rings are called *Galois rings.* In a Galois ring S we can define trace mapping from S to $\mathbb{Z}_{p^m}$ and using constructions similar as before, we can form sequences with entries in $\mathbb{Z}_{p^m}$.

Assume now that $p = m = 2$. Our prime ring is then $\mathbb{Z}_4$. Suppose that we have, using an extension of $\mathbb{Z}_4$, constructed sequences whose componentes are in $\mathbb{Z}_4$, but our intrest is in binary sequences. We can then convert sequences in $\mathbb{Z}_4^n$ into complex vectors as mentioned in I.4, and estimate their correlations. If we have a sequence set with good correlation properties, it would be convinient to covert it into binary set preserving correlation properties. This can be done by *Gray encoding*, mapping a $\mathbb{Z}_4$-sequence of length n into a binary sequence of length $2n$ by mapping $0 \mapsto 00$, $1 \mapsto 01$, $2 \mapsto 11$ and $3 \mapsto 10$.