Communication Complexity and Orthogonal Polynomials

Ulrich Tamm
Dept. of Mathematics, Univ. of Bielefeld, Germany

Let $D_0, \dots, D_n$ be a collection of $\{0,1\}$-matrices forming an association scheme. Since $\sum_{k=0}^n D_k$ is the all-one matrix, a linear combination $\sum_{k=0}^n c_k D_k$ can be regarded as the matrix $(f(x,y))_{x,y}$ representing the function f defined by $f(x,y) = c_k$ if (x,y) is in relation corresponding to matrix D_k. As an example, consider the Hamming distance d_H arising for the matrices of the Hamming association scheme with the choice of $c_k = k$ for all $k = 0, \dots, n$. Parameters of functions thus obtained may now be studied exploiting properties of the association scheme.
One such parameter is the communication complexity $C(f)$, which is the number of bits that two persons have to exchange in order to evaluate $f(x,y)$, when initially one person only knows x and the other person only knows y. Communication complexity, as introduced by Yao in 1979, turned out to be an important topic in Computer Science, especially in the derivation of bounds for area-time tradeoff in VLSI-layout and for depth of circuits, decision trees and branching programs.
Lower bounds for $C(f)$ are obtained from the matrices $M_z(f) = (a_{xy})_{x,y}$ defined by $a_{xy} = \begin{cases} 1 & \text{if } f(x,y) = z \\ 0 & \text{if } f(x,y) \neq z \end{cases}$, namely

$$C(f) \geq \log_2 \sum_z \text{rank} M_z(f).$$

These bounds are tight if all the matrices have full rank. Now let us discuss the following two scenaria.
1) All the c_k's are different. Then the matrices $M_z(f)$ are just the matrices of the association scheme. In order that all of them have full rank, all their eigenvalues must be different from 0. These eigenvalues are orthogonal polynomials. For the Hamming association scheme the problem is to show that the Krawchouk polynomials have only very few integral zeros. This way the communication complexity of the binary Hamming distance can be determined up to one bit. For alphabet size $q \geq 3$, it is still an open problem to derive the same result (at least using the above rank lower bound, for $q = 4, 5$ $C(d_H)$ has been determined up to one bit using a different approach).
2) $c_k = c_l$ for several pairs $k \neq l$. In this case one might exploit the simultaneous diagonalizability of the matrices $D_0, \dots, D_n$ in order to study the eigenvalues of the matrices $M_z(f) = \sum_{k: c_k = z} D_k$. These eigenvalues then will be linear combinations of the orthogonal polynomials arising as eigenvalues for the matrices of the association scheme. We shall present two such functions obtained from the Hamming association scheme.
The first one is defined by $f(x,y) = \begin{cases} 1 & \text{if } d_H(x,y) \leq t \\ 0 & \text{if } d_H(x,y) > t \end{cases}$ and yields the matrices $M_1 = \sum_{k=0}^t D_k$, $M_0 = \sum_{k=t+1}^n D_k$ whose eigenvalues are Lloyd polynomials important in the study of perfect codes. Another such function is the Hamming distance modulo 2 with matrices $M_1 = \sum_{k \text{ even}} D_k$, $M_0 = \sum_{k \text{ odd}} D_k$ whose eigenvalues can be shown to be all different from 0 (for alphabet size $q > 3$) by the identity for Krawchouk polynomials, where w is the number of 1's in the binary expansion of i.

$$\sum_{k \equiv z (\text{mod } 2)} K_k(i,q,n) = \begin{cases} \frac{1}{2}(q^n + (-1)^z (2-q)^n) & i = 0 \\ (-1)^z 2^{n-w-1} (2-q)^w & i = 1, \dots, n \end{cases}$$