The Generalized Goppa Codes and Related Discrete Designs from Hermitian Varieties*

I.M. Chakravarti

University of North Carolina,

Chapel Hill

Abstract

A short description is first given of the fascinating use of Hermitian curves and normal rational curves by Goppa in the construction of linear error correcting codes and estimation of their transmission rate (k/n) and error correcting power (d/n) by invoking Riemann-Roch theorem and the subsequent discovery by Tsfasman, Vladut and Zink of a sequence of linear codes in q symbols, which performs better than those predicted by the Gilbert-Varshamov bound for $q \geq 49$.

Next, several new codes which have been constructed by embedding the non-degenerate Hermitian surface $x_0^3 + x_1^3 + x_2^3 + x_3^3 = 0$ of PG(3,4), in a PG(9,4) via monomials and weight-distributions of these codes are presented.

Using the geometry of intersections of a non-degenerate Hermitian surface in PG(3,s^2), by secant and tangent hyperplanes, a family of two-weight projective linear codes have been derived. For s=2, it is shown that the strongly regular graph of this code gives rise to the Hadamard difference sets $v = 2^8$, $k = 2^7-2^3$, $\lambda = 2^6-2^3$ and $v = 2^8$, $k = 2^7 + 2^3$, $\lambda = 2^6 + 2^3$. In fact, the author has now shown that this construction can be extended to derive the Hadamard difference sets $v = 2^{2N+2}$, $k = 2^{2N+1}-2^N$, $\lambda = 2^{2N}-2^N$, $v = 2^{2N+2}$, $k = 2^{2N+1}+2^N$, $\lambda = 2^{2N}+2^N$. This will be reported in another paper.

*Some of these results were presented at the 3ème Colloque International Théorie des Graphes et Combinatoire, Marseille-Luminy, 23-28 Juin 1986 and at the International Conference on Information Processing and Management of Uncertainty in Knowledge-based Systems, Paris, June 30-July 4, 1986.

Introduction.

A code C is a subset of an n-dimensional vector space $V_n(q)$ over a finite field GF(q). The Hamming weight of a code vector $w(\underline{a})$, $\underline{a} = (a_1,\dots,a_n)$, a_i in GF(q), is the number of non-zero symbols in $\underline{a}$. The Hamming distance $d_H(\underline{a},\underline{b})$ between two codewords $\underline{a}$ and $\underline{b}$ is the number of positions i, $1 \leq i \leq n$, in which they differ. Let d be the minimum of the distances between pairs of codewords of C, $d = \min_{\underline{a},\underline{b}\in C} d(\underline{a},\underline{b})$ and let $|C| = M$ = number of codewords in C. Then the code C has the parameters (n,M,d). n is called the length of a codeword . If C is a subspace of dimension k, of $V_n(q)$, C is a linear (n,k,d) code, $M = q^k$. For a linear code d is the same as the minimum of the weights of non-zero codewords. A code C with minimum distance d can correct up to [(d-1)/2] errors. Let $G_{k,n} = (g_{ij})$ be a basis of the linear code C(n,k,d). Then G is called a generator matrix of the code. Let $H_{r,n} = (h_{ij})$ be a basis of the null space C the dual linear code $C^{\perp}$ of C, $H G^T = 0$. Then H is called a parity check matrix of C.

For a given positive integer q, q-ary symmetric channel is a discrete memoryless channel with input and output alphabet $\{0,1,\dots,q-1\}$ and channel probabilities $p(i|i) = 1-\beta,$, $p(j|i) = \beta/(q-1)$, $i \neq j$. The capacity C of such a channel is $C = \log q + (1-\beta)\log(1-\beta) + \beta \log \beta - \beta \log(q-1)$.

Given a symmetric discrete memoryless channel with capacity $C > 0$ and a positive number $R < C$, there exists a sequence of q-ary linear codes (n_i,k_i,d_i), $i = 1,2,\dots$ where $n_1 < n_2 < \dots$, $R \leq \frac{k_i}{n_i} < C$ with the maximum probability of error λ_i (of the ith code) tending to zero. (See, for instance, Ash (1965), pp. 110-127)). Ash (1965, p. 130) has argued that if we could synthesize binary linear codes meeting the Gilbert-Varshamov bound, then such codes could be used to maintain any transmission rate up to $1 - H(2\beta, 1-2\beta)$ (which is close to the capacity of a binary symmetric channel for $\beta < \frac{1}{4}$), with an arbitrary small probability of error. Ash's analysis and discussion in the context of binary linear codes can be extended with suitable modification to q-ary linear codes. This explains why coding theorists are so keen on constructing algebraically, sequences of q-ary linear codes which perform better than the Gilbert-Varshamov bound. However, it is known that there does not exist an infinite sequence of primitive BCH codes of length n over GF(q) ($n = q^m-1$) with δ and R tending to non-zero limits (see, for instance, MacWilliams and Sloane, 1977) ($\delta = \frac{d}{n}$).

Using the idea of concatenated codes, Delsarte and Piret (1982), have given an algebraic construction of codes with feasible encoding/decoding algorithm, which simultaneously attain channel capacity and have probability of erroneous decoding tending to zero. This is, however, possible only because the requirement of a least d has been dropped. In Goppa's approach based on algebraic geometry and the subsequent work by Tsfasman, Vladut and Zink (1982), this assumption is not made.

<u>Goppa codes from algebraic curves</u>

Let X be a smooth (non-singular) irreducible projective curve of genus g in the N-dimensional projective space over $\overline{GF}(q)$ (the algebraic closure of GF(q)) and let Q, $P_1, \ldots, P_n$ be n+1 rational points (with coordinates in GF(q)) on X. Let t be an integer such that $2g-2 < t < n$. The linear space L(tQ) with respect to the divisor tQ is the set of rational functions f such that the order f in Q is $\geq -t$. The codewords of the linear code C(n,k,d) over GF(q) are then defined by $(f(P_1), \ldots, f(P_n))$, f in L(tQ). From Riemann-Roch theorem, it follows that $k = t - g + 1$ and $d \geq n-t$. Hence $R = \frac{k}{n} \geq 1 - \gamma = g/n$ and $\delta = \frac{d}{n}$. (See, for instance, Goppa (1984), Vladut, Katsman and Tsfasman (1984.)

Let the functions $f_o = 1$, $f_2, \ldots, f_{k-1}$ be a basis of the space L(tQ) and let $g_{ij} = f_i(P_j)$, $i = 0,1,\ldots k-1$, $j = 1, \ldots, n$. Then $G = (g_{ij})$ is a generator matrix of the linear code C (n,k,d). Let $s = t-2g+1$. Then one can show that every set of s columns of G has rank $k-g = (t-g+1)-g = s$. Thus the dual C' of C, has minimum distance $C' \geq s+1$ and has dimension $k' = n-k$. It follows then $R' = \frac{k}{n} \geq 1 - \frac{g}{n} - \frac{d'}{n} = 1-\gamma-\delta'$. The dual codes {C'} can be shown to be the same as the codes {C*} constructed by Goppa (1981, 1982), now known as generalized Goppa codes. The code vectors were defined as vectors of residues of differentials in the linear space $\Omega(\Sigma\ P_i-tQ)$ which is isomorphic to $L(K + \Sigma\ P_i-tQ)$, where K is a canonical divisor of degree 2g-2 and dimension g.

The linear codes {C} constructed above are natural generalizations of Reed-Solomon codes which are maximum distance separable (mds) codes or equivalently orthogonal arrays of index unity (see, Bush (1952), Chakravarti (1963), Singleton (1964) and MacWilliams and Sloane (1977), ch. 11).

Higher the ratio of the number of rational points on the curve X to its genus, better is the performance of the code. Vladut and Drinfel'd (1983) have shown that the limit of this ratio A(q) as the genus tends to infinity, does not exceed $\sqrt{q}-1$ and for $q = p^{2\ell}$ there are families of curves over GF(q) with $A(q) = \sqrt{q}-1$ (Ihara (1982), Tsfasman, Vladut and Zink (1982)). For $q = p^2$ then, $\lim\sup_{n\to\infty} R = \alpha^q(\delta) \geq 1 - (\sqrt{q}-1)^{-1} - \delta$. The asymptotic form of the Gilbert-Varshamov bound states that there exists a sequence of codes such that

$$\lim\sup_{n\to\infty} R = \alpha_q(\delta) \geq 1 - \delta \log_q(q-1) + \delta \log_q \delta + (1-\delta)\log_q(1-\delta).$$

For $\delta_1 < \delta < \delta_2$, where δ_1 and δ_2 are the roots of the equation

$$\delta \log_q(q-1) - \delta \log_q \delta - (1-\delta)\log_q(1-\delta) - \delta = (\sqrt{q}-1)^{-1}),$$

the first lower bound lies above the Gilbert-Varshamov bound. This equation has roots for $q \geq 49$ ($p \geq 7$, $\ell = 1$) (Tsfasman, Vladut and Zink (1982), Tsfasman 1982).

If the sequence of linear codes {C} exceeds the Gilbert-Varshamov bound, the corresponding sequence of dual codes {C'} also does the same.

Goppa (1982) has defined a class of codes called <u>normal</u> codes determined from a pair of divisors $D = \Sigma P_i$ and $G = \Sigma m_Q Q$, where P_i are rational points on a normal curve F and the carriers of the two divisors are disjoint. If Q belongs to some extensions field of GF(q), then both $m_Q Q$ and $m_Q \sigma Q$ lie on the divisor G, where σQ is the Frobenius transform of Q. A normal (D,G) code has the parameters $|n - (q+1)| \leq 2g\sqrt{q}, r = \deg G - g + 1$, $d \geq \deg G - 2g+2$. The length n of the code does not exceed the number of rational points on F, for which the well known Hasse-Weil estimate is $|n - (q+1)| \leq 2g\sqrt{q}$, where g is the genus of F. In particular, of special interest are curves on which the upperbound $n = q+1 + 2g\sqrt{q}$ is attained.

For every $q = p^{2h}$, p a prime, the curve $x_o^{\sqrt{q}+1} + x_1^{\sqrt{q}+1} + x_2^{\sqrt{q}+1} = o$ over PG(2,q), called a Hermitian curve has genus $g = (q - \sqrt{q})/2$ and n = number of rational points $= q\sqrt{q}+1$. Hence it satisfies the Hasse-Weil bound. The geometries of Hermitian curves in projective planes and Hermitian surfaces in higher dimensional projective spaces have been extensively studied by Bose (1963, 1971), Bose and Chakravarti (1966), Chakravarti (1970, 1971) and Segre (1965, 1967).

Goppa (1981, 1982, 1984) has used the Hermitian curves $x_o^{s+1} + x_1^{s+1} + x_2^{s+1} = o$ over $PG(2,s^2)$ to construct new linear codes. Each one of these codes and their duals are equivalent to certain orthogonal arrays which are extremely useful as designs with a wide range of applications and also as building blocks for other designs such as resolvable and affine resolvable balanced incomplete block designs, and balanced arrays which can be also used as equidistant codes with maximum distance, balanced codes and uniformly packed codes.

If h is any element of $GF(s^2)$, where s is a prime or a power of a prime, then $\bar{h} = h^s$ is defined to be conjugate to h and h is conjugate to h since $h^{s^2} = h$. A square matrix $H = (h_{ij})$, $h_{ij} = \bar{h}_{ji}$, i, j = 0,1,...,N is called a Hermitian matrix. The set of all points in $PG(N,s^2)$ whose row vectors $\underline{x}^T = (x_0,x_1,\ldots,x_N)$ satisfy the equation $\underline{x}^T H x^{(s)} = o$, are said to form a Hermitian variety V_{N-1} if H is Hermitian; $\underline{x}^{(s)}$ is the column vector whose transpose is $(x_o^s, \ldots, x_N^s)$. The variety V_{N-1} is said to be non-degenerate if H has rank N+1 and its equation can be taken in the canonical form $x_o^{s+1} + \ldots + x_N^{s+1} = o$. If H has rank r+1, then $\underline{x}^T$ H $\underline{x}^{(s)}$ can be reduced by a non-singular linear transformation, to the canonical form $y_o\bar{y}_o + \ldots + y_r\bar{y}_r$. The number of points in a non-degenerate Hermitian variety V_{N-1} is $(s^{N+1} - (-1)^{N+1})(s^N - (-1)^N)/(s^2-1)$ and the number of points with exactly r non-zero coordinates in V_{N-1} is $\binom{N+1}{r}[(s-1)^{n-1} - (-1)^{n-1}](s+1)^{r-1}/s$. (Bose and Chakravarti, 1966). If N = 2t+1 or 2t+2, then a non-degenerate Hermitian variety V_{N-1} contains flat spaces of dimension t and no higher. The number of u-flats, $o \le u \le [(N-1)/2]$ were derived by Chakravarti (1971).

There exists an extensive literature on the three classical geometries - symplectic, orthogonal and unitary geometries andd their associated classical groups (see, for instance, Dembowski, 1968). Geometry of quadric surfaces in projective spaces (orthogonal geometry) have been used by Bose (1961), Robillard (1969), Hill (1978) and Wolfmann (1977) for constructing linear codes. Delsarte and Goethals (1975) have used symplectic geometry (geometry of alternating forms) to construct linear codes. Further connections between Reed-Muller codes and symplectic forms are now well-known (see, for instance, MacWilliams and Sloane, 1977). Goppa (1981) seems to be the first one to have used a Hermitian curve $x_o^3 + x_1^3 + x_2^3 = o$ over PG(2,4) to construct a new linear code.

Codes better than Gilbert-Varshamov bound.

The original construction due to Tsfasman, Vladut and Zink (1982) of generalized Goppa codes based on certain modular curves over GF(q) $q = p^{2h}$, which lie above Gilbert-Varshamov bound, was further analyzed by Vladut, Katsman and Tsfasman (1984). The curve considered is associated with elliptic Drinfel'd moduli. For $q = r^2$, they consider a ring of polynomials A = GF(r)[T] over GF(r) and a prime ideal $I = (P_I)$ generated by a polynomial P_I in A, that is irreducible over GF(r), of degree $p_I = m_I = m$ where m is odd and $(m,r-1) = 1$. The description of the smooth absolutely irreducible curve X of genus $g = g_I$ over GF(r) is, however, in the abstract language of algebraic geometry. This curve has $n = (r^m+1)/(r+1)$ rational points over $GF(r^2)$ and that as $m \to \infty$ $\lim_{m_I \to \infty} {}^{n}I/g_I = r-1$. The divisor G is then defined as aQ, where Q is one of the two cusps of the curve X (and distinct from P_i's $i = 1,\ldots,n$) and a is a non-negative integer. The code is then defined as the mapping "value at points $P_1,\ldots,P_n$" of the functions of the linear space L(G). The parameters of the resultant code C are n, $k \geq a \quad - g+1$, $d \geq n-1$. This sequence of codes lie asymptotically on the segment $R = 1-(r-1)^{-1}-\delta$. The authors have shown that these codes have polynomial complexity of construction.

One of the objectives of this research program is to find an elementary construction of the algebraic curves or surfaces in projective spaces which provide sequences of codes that perform better than the Gilbert-Varshamov bound.

The construction due to Vladut, Katsman and Tsfasman resembles to a great extent (except for the bit on schemes) construction by Bose and Chakravarti (1966) and Chakravarti (1971) of strongly regular graphs and designs from Hermitian varieties in $PG(N,r^2)$ and constructions by Segre (1967) of non-oval complete arcs in $PG(2,q)$ for $q \geq 7$ using the conic $xy = z^2$ for $q = 4\ell+3$ and constructions of non-oval arcs from cubic curves $yz^2 = x^3$ with a cusp or with double points by Segre and D. Comite (see, Segre, 1967).

Link between quadrics and Hermitian varieties in projective spaces.

Bose (1972) made a special study of the Hermitian variety $x_o^3 + x_1^3 + x_2^3 + x_3^3 = o$ in $PG(3,2^2)$ and derived a representation of $PG(3,3)$ in terms of external points, secant planes and self-conjugate tetrahedra with respect to the Hermitian variety. This representation is very interesting because of the natural change of the characteristic from 2 to 3. Further study of this represention and its generalization will most probably provide a natural way to change characteristics in the Galois arithmetic needed in computation in connection with the combinatorics of codes and designs.

A correspondence between the non degenerate Hermitian variety $x_o^{s+1} + \ldots + x_N^{s+1} = o$ in $PG(N,s^2)$ and a non-degenerate elliptic (hyperbolic) quadric in $PG(2N+1),s)$ when $N = 2k(N=2k-1)$ was established by Heft (1971). This provides a vital link in the investigation of n-sets of type k (n-caps, n-arcs etc.) and associated codes and designs. This link needs to be exploited since the author feels that this will lead to some powerful methods based on both orthogonal and unitary (algebraic) geometries of construction of codes and designs.

New codes, symmetric designs, Hadamard difference sets from Hermitian varieties.

As we move from algebraic curves in projective planes to algebraic surfaces in projective spaces of higher dimensions, the applicable part of algebraic geometry to the construction of codes and related designs, become rather complex. In order to be able to construct codes and designs and calculate their parameters, based on say, quadric hypersurfaces, Hermitian varieties and symplectic forms, one has to find out properties of such geometrical objects or, if feasible, use a computer. The geometry of quadric hypersurfaces in PG(r,q) has been studied by Primrose, Segre, Ray-Chaudhuri, Barlotti, Tallini, Panella, Hirschfeld (for references see for instance, Barlotti (1965), Dembowski (1968) and Segre (1967)). The geometry of Hermitian varieties in $PG(N,q^2)$ has been studied by Segre (1965, 1967) Bose (1963, 1971), Bose and Chakravarti (1966), Chakravarti (1971) and others (see, for instance, Dembowski, 1968).

We have just constructed a linear code C(n=45, k=35, d=4) on q=4 symbols. A parity check matrix of the form 10 x 45, was constructed from a Hermitian surface $x_o^3 + x_1^3 + x_2^3 + x_3^3 = 0$ in PG(3,4). The columns of the matrix were labelled by the 45 points on the surface and the rows were labelled by the 10 monomials x_o^2, x_1^2, x_2^2, x_3^2, x_ox_1, x_ox_2, x_ox_3, x_1x_2, x_1x_3, x_2x_3 and the entries were the values of the monomials at the points. A computer program written by Mr. R. Tobias, a graduate student, generated the matrix and also found that every set of 3 columns were linearly independent but that there were sets of 4 columns which were dependent. The parity check matrix generates then an orthogonal array $(4^{10},45,4,3)$. Its parameters as a linear code $C^{\perp}$ orthogonal to the former C, are n=45, k=10. Using programs for a personal computer, written by Paul P. Spurr (1986) in his Master's project, the weight distribution of this code has been found. It is $A_0=1$ $A_{22}=2160$, $A_{24}=2970$, $A_{26}=4320$, $A_{28}=40,500$, $A_{30}=122,976$, $A_{32}=233,415$, $A_{24}=285,120$, $A_{36}=233,400$, $A_{38}=97,200$, $A_{40}=20,574$, $A_{42}=4320$, $A_{44}=1620$, with all other A_i equal to zero. (A_i is the frequency of codewords of weight i). The code has minimum distance 22 and hence corrects all error patterns of weight 10 or less. It is an even weight code (that is all its codewords have even weights) although it is not a self-orthogonal nor a formally self-orthogonal code. (A code C is called formally self-orthogonal if C and its orthogonal $C^{\perp}$ have the same weight enumerator. C is weakly self orthogonal if $C \subset C^{\perp}$ and (strictly) self orthogonal if $C = C^{\perp}$.

MacWilliams et al. (1978) have studied codes over GF(4) which have even weights and have the same weight distribution as the orthogonal code $C^{\perp}$. These codes are of considerable interest because some of them attain the Gilbert-Varshamov bound. They have also derived several 3 - and 5 - designs from these codes.

We have worked out the weight distributions of three other codes: C_1 (n=18, k=10, d=3), its orthogonal $C_1^{\perp}$ (n=18, k=8, d=6) and C_2(n=27, k=10, d=8) over GF(4). The columns of the 10 x 18 generator matrix of C_1 corresponds to the 18 points of the Hermitian surface V_2: $x_o^3 + x_1^3 + x_2^3 + x_3^3 = 0$ in PG(3,4), which have at least one coordinate equal to zero and the rows correspond to the 10 monomials of degree 2: x_0^2, x_1^2, x_2^2, x_3^2, $x_o x_1$ $x_o x_2$, $x_o x_3$, $x_1 x_2$, $x_1 x_3$, $x_2 x_3$. Its weight distribution is $A_0 = 1$, $A_1=A_2=0$, $A_3=18$, $A_4= A_5=0$, $A_6=540$, $A_7=810$, $A_8=2295$, $A_9=17,238$, $A_{10}=40,581$, $A_{11}=84,078$, $A_{12}=152,658$, $A_{13}=204,660$, $A_{14}=221,022$, $A_{15}=185,382$, $A_{16}=100,278$, $A_{17}=31,590$, $A_{18}=7425$. Thus the minimum distance is 3 and C_1 is a single-error correcting code. Its orthogonal $C_1^{\perp}$ (n=18, k=8) has the weight distribution $A_o=1$, $A_1=A_2=A_3=A_4=A_5=0$, $A_6=144$, $A_7=0$, $A_8=459$, $A_9=672$, $A_{10}=2196$, $A_{11}=6264$, $A_{12}=6750$, $A_{13}=11,016$, $A_{14}=17,388$, $A_{15}=12,744$, $A_{16}=5022$, $A_{17}=194,490$, $A_{18}=216$. This code has minimum distance 6 and corrects all error patterns of weight 2 or less. This code resembles to a certain extent the code S_{18} of MacWilliams et al. (1978) who were able to derive certain 5-designs from S_{18}.

The columns of the 10 x 27 generator matrix of C_2 corresponds to those 27 points of the Hermitian surface V_2 in PG(3,4), which have every coordinate non-zero and the 10 rows correspond to the 10 monomials of degree 2 in the coordinate variables (x_0,x_1,x_2,x_3). Its weight distribution is $A_0=1$, $A_1=A_2=A_3=A_4=A_5=A_6=A_7=0$, $A_8=3$, $A_9=45$, $A_{10}=24$, $A_{11}=141$, $A_{12}=717$, $A_{13}=2031$, $A_{14}=5325$, $A_{15}=14{,}910$, $A_{16}=31{,}605$, $A_{17}=61{,}803$, $A_{18}=105{,}714$, $A_{19}=152{,}484$, $A_{20}=182{,}193$, $A_{21}=179{,}745$, $A_{22}=146{,}529$, $A_{23}=95{,}226$, $A_{24}=48{,}585$, $A_{25}=16{,}392$, $A_{26}=4104$, $A_{27}=999$. This code has minimum distance 8 and hence corrects all error patterns of weight 3 or less.

A non-degenerate Hermitian variety V_2: $x_0^{s+1} + x_1^{s+1} + x_2^{s+1} + x_3^{s+1} = 0$ in PG$(3,s^2)$ has $(s^3+1)(s^2+1)$ points. It is known (Bose and Chakravarti, 1966) that a plane of PG$(3,s^2)$ meets V_2 either in a non-degenerate V_1 which consists of (s^3+1) points of the plane or in a degenerate V_1 of rank 2 which consists of s^3+s^2+1 points of the plane. In the former case, the plane may be called a secant plane and in the latter case the plane is called a tangent plane. Thus the code generated by the 4 x $(s^3+1)(s^2+1)$ matrix whose columns correspond to the $(s^3+1)(s^2+1)$ points of V_2 and rows to the four coordinates, is a two-weight projective linear code over GF(s^2) with $n = (s^2+1)(s^3+1)$ and $w_1=(s^2+1)(s^3+1) - (s^3+s^2+1) = s^5$ and $w_2 = (s^2+1)(s^3+1) - (s^3+1) = s^5+s^2$ and the frequencies $A_{w_1} = (s^3+1)(s^4-1)$ and $A_{w_2} = (s^4-1)(s^4-s^3)$. The set of points $\bar{V}_2$ complementary to V_2 in PG$(3,s^2)$ also gives rise to a two-weight projective linear code over GF(s^2) with $n = s^3(s^3-s^2+s-1)$, $w_1=s^5(s-1)$, $w_2=s^2(s^4-s^3-1)$ $A_{w_1} = (s^3+1)(s^4-1)$ and $A_{w_2}=(s^4-1)(s^4-s^3)$.

Thus for s=2, we get two two-weight projective linear codes over GF(4). The parameters of the code C_3 corresponding to the 45 points of the Hermitian surface V_2 are n=45, k=4, d=32 and the frequency distribution of the weights of this code is $A_0=1$, $A_{32}=135$, $A_{36}=120$ and all other $A_i=0$. The graph on $v=4^4=256$ vertices corresponding to this code is strongly regular and its adjacency matrix $A=B_2-B_1$ has the eigenvalues $\rho_0=-15$, $\rho_1=17$, $\rho_2=-15$. As a two-class association scheme its parameters are $n_1=135$, $n_2=120$, $p^1_{11}=70$, $p^1_{12}=64$, $p^2_{11}=72$, $p^2_{12}=63$, $p^1_{22}=p^2_{22}=56$. This last equality implies that B_2 (the association matrix of the second associates) is the incidence matrix of a symmetric BIB design ($v=256$, $k=120$, $\lambda=56$) and $2\ B_2-J$ is a Hadamard matrix of order 2^8 which corresponds to the Hadamard difference set $v=2^8$, $k=2^7-2^3$, $\lambda=2^6-2^3$. Note that $I + B_1$ is the incidence matrix of the complementary symmetric BIB design ($v=256$, $k=136$, $\lambda=72$).

The code $\bar{C}_3$ corresponding to the 40 points of $\bar{V}_2$ the set complementary to V_2 in PG(3,4) has the parameters $n=40$, $k=4$, $d=28$ and the weight-distribution $A_0=1$, $A_{28}=120$, $A_{32}=135$, and all other $A_i=0$. The adjacency matrix $\bar{A}=\bar{B}_2-\bar{B}_1$ of the strongly regular graph on $v=256$ vertices associated with this code has the eigenvalues $\rho_0=15$, $\rho_1=15$, $\rho_2=-17$. $\bar{B}_1$ (the association matrix of the first associates in this 2-class association scheme is the incidence matrix of the symmetric BIB design ($v=256$, $k=120$, $\lambda=56$) and $I + \bar{B}_2$ is the incidence matrix of the SBIB ($v=256$, $k=136$, $\lambda=72$).

Since a projective (n,k) code over GF(s^r) with weights w_i $i=1 \dots s$ determines a projective (n',k') code over GF(s) with weights w_i' $i=1,\dots s$, $n' = n(s^r-1)/(s-1)$, $k'=kr$, $w_i'=s^{r-1}w_i$, $i=1,\dots s$, (Delsarte, 1972), the two projective two-weight codes C_3 and $\bar{C}_3$ over GF(4) give rise to two projective binary two-weight codes C_4 and $\bar{C}_4$ (say) respectively. The two-weight binary code C_4 corresponding to C_3, has the parameters $n'=135$, $k'=8$, $w_1'=64$, $w_2'=72$, $A_0=1$, $A_{64}=135$, $A_{72}=120$. Then the strongly regular graph associated with this code C_4 has the same parameters as these of the graph of C_3. Consider the 120 code-vectors each of weight 72, which are non-adjacent to (second associates of) the null code-word. Then since $p_{22}^1 = p_{22}^2 = 56$, it follows that these 120 code-vectors form a difference set, $v = 2^8$, $k = 2^7-2^3$, $\lambda = 2^6-2^3$. On the other hand the 135 code vectors each of weight 64 which are adjacent to (first associate of) the null codeword , together with the null vector gives rise to the difference set ($v = 2^8$, $k = 2^7+2^3$, $\lambda = 2^6+2^3$) since $2+p_{11}^1 = p_{11}^2 = 72$.

The author has now generalized the above construction to the case of the intersections of a non-degenerate Hermitian variety V_{N-1} by the hyperplanes of $PG(N,2^2)$ for every $N > 1$. This construction provides the sequence of two-weight linear codes over GF(4) with parameters $n = (2^{2N+1} + (-2)^N)/3$, $k = N+1$, $w_1 = 2^{2N-1}$, $w_2 = 2^{2N-1} + (-2)^{N-1}$, $A_{w_1} = n_1 = 2^{2N+1} + (-2)^{N+1} + (-2)^N-1$, $A_{w_2} = n_2 = 2^{2N+1} + (-2)^N$.

Using the associated strongly regular graph one gets the incidence matrices of the sequence of symmetric BIB designs with $v = 2^{2(N+1)}$, $k = 2^{2N+1}-2^N$, $\lambda = 2^{2N}-2^N$ and the corresponding sequence of Hadamard matrices $H_{4^{N+1}}$. For N even the $2^{2N+1}-2^N-1$ binary codewords of weight 2^{2N} together with the null codeword form a Hadamard difference set $v=2^{2(N+1)}$, $k = 2^{2N+1} - 2^N$, $\lambda=2^{2N}-2^N$ and the $2^{2N+1}+2^N$ binary codewords of weight $2^{2N}+2^N$ form a difference set $v = 2^{2N+2}$, $k = 2^{2N+1}+2^N$, $\lambda = 2^{2N}+2^N$. For odd N, the $2^{2N-1}-2^N$ binary codewords each of weight $2^{2N}+2^N$ form a Hadamard difference set $v=2^{2(N+1)}$, $k=2^{2N+1}-2^N$, $\lambda = 2^{2N}-2^N$ and the $2^{2N+1}+2^N-1$ codewords each of weight 2^{2N} together with the null codeword form a difference set $v = 2^{2N+2}$, $k = 2^{2N+1}+2^N$, $\lambda = 2^{2N}+2^N$.

These results together with proofs will be reported in another communication.

References

Ash, R.B. (1966) Information Theory, Interscience Publishers, John Wiley and Sons, New York.

Barlotti, A. (1965) Some Topics in Finite Geometrical Structures, Lecture Notes, Chapel Hill (Inst. of Statistics Mimeo Series no. 439).

Bose, R.C. (1961) On some connections between the design of experiments and information theory. Bull. Intern. Statist. Inst. 38, 257-271.

Bose, R.C. (1963) Some ternary error correcting codes and fractionally replicated designs. Colloques. Inter. CNRS, Paris, no. 110, 21-32.

Bose, R.C. (1971) Self-conjugate tetrahedra with respect to the Hermitian variety $x_o^3 + x_1^3 + x_2^3 + x_3^3 = 0$ in $PG(3,2^2)$ and a representation of PG(3,3). Proc. Symp. on Pure Math. 19 (Amer. Math. Soc. Providence, R.I.), 27-37.

Bose, R.C. and Chakravarti, I.M. (1966) Hermitian varieties in a finite projective space $PG(N,q^2)$, Canad. J. Math. 18, 1161-1182.

Bush, K.A. (1952) Orthogonal arrays of index unity. Ann. Math. Statist. 23, 426-434.

Chakravarti, I.M. (1963) Orthogonal and partially balanced arrays and their application in Design of Experiments, Metrika 7, 231-343.

Chakravarti, I.M. (1971) Some properties and applications of Hermitian varieties in $PG(N,q^2)$ in the construction of strongly regular graphs (two-class association schemes) and block designs. Journal of Comb. Theory, Series B, 11(3), 268-283.

Delsarte, P. (1972) Weights of linear codes and strongly regular normed spaces. Discrete Mathematics, 3, 47-64.

Delsarte, P. and Goethals, J.M. (1975) Alternating bilinear forms over GF(q). J. Combin. Theory, 19A,

Delsarte, P. and Piret, P. (1982) Algebraic constructions of Shannon codes for regular channels. IEEE Trans. Inf. Th., IT-28, 593-599.

Dembowski, P. (1968) Finite Geometries, Springer-Verlag 1968.

Goppa, V.D. (1983) Algebraico-geometric codes. Math. USSR Izvestiya, 21(1), 75-91.

Goppa, V.D. (1984) Codes and information. Russian Math. Surveys., 39(1), 87-141.

Heft, S.M. (1971) Spreads in Projective Geometry and Associated Designs, Ph.D. dissertation submitted to the University of North Carolina, Dept. of Statistics, Chapel Hill.

Hill, R. (1978) Packing problems in Galois geometries over GF(3), Geometriae Dedicata, 7, 363-373.

MacWilliams, F.J., Odlyzko, A.M., Sloane, N.J.A. and Ward, H.N. (1978) Self-dual codes over GF(4). J. Comb.Th., A25, 288-318.

MacWilliams, F.J. and Sloane, N.J.A. (1977) The Theory of Error-Correcting Codes, North Holland.

Robillard, P. (1969) Some results on the weight distribution of linear codes. IEEE Trans. Info. Theory 15, 706-709.

Segre, B. (1965) Forme e geometrie hermitiane, con particolare riguardo al caso finito. Ann. Math. Pure Appl., 70 1, 202.

Segre, B. (1967) Introduction to Galois Geometries, Atti della Acc. Nazionale dei Lincei, Roma, 8(5), 137-236.

Singleton, R.C. (1964) Maximum distance q-nary codes. IEEE Trans. Info. Theory, 10, 116-118.

Tsfasman, M.A. (1982) Goppa codes that are better than the Varshamov-Gilbert bound. Problems of Info. Trans., 18, 163-165.

Tsfasman, M.A., Vladut, S.G. and Zink, T. (1982) Modular curves, Shimura curves and Goppa codes, better than Varshamov-Gilbert bound. Math. Nachr., 104, 13-28.

Vladut, S.G. and Drinfel'd, V.G. (1983) Number of points of an algebraic curve. Functional Anal. Appl. 17, 53-54.

Vladut, S.G., Katsman, G.L. and Tsfasman, M.A. (1984) Modular curve and codes with polynomial complexity of construction. Problems of Info. Transmission 20, 35-42.

Wolfmann, J. (1977) Codes projectifs à deux poids, "caps" complets et ensembles de différences. J. Combin. Theory, 23A, 208-222.