МАТЕМАТИКА И МАТЕМАТИЧЕСКО ОБРАЗОВАНИЕ, 2003
MATHEMATICS AND EDUCATION IN MATHEMATICS, 2003
Proceedings of the Thirty Second Spring Conference of
the Union of Bulgarian Mathematicians
Sunny Beach, April 5–8, 2003

QPLUS – A COMPUTER PACKAGE FOR CODING THEORY RESEARCH

Galina T. Bogdanova, Stojan N. Kapralov, Vihren H. Todorov, Teodor S. Parvanov

A shared computer tools QPlus for coding theory studying is presented. The system offers computations over $Z_q = \{0, 1, \ldots, q-1\}$ ($q < 256$) and includes modular arithmetic, elementary number theory, vectors and matrices arithmetic and an environment for research on q-ary codes – linear, constant-weight and equidistant codes. Optimal ternary constant-weight codes, binary and ternary equidistant codes have been constructed by our computer methods. QPlus includes a DLL library package that implements coding theory algorithms.

1. Introduction. The main subject of the research in this work are the optimal q-ary codes. We consider several classes of codes – linear codes, constant-weight codes, constant-composition codes and equidistant codes.

Let us introduce some basic notations which we need to describe the results. Let Q be an alphabet of $q \geq 2$ elements. We consider the set Q^n, consisting of ordered n-tuples of elements of Q. The *Hamming distance* between two n-tuples of Q^n is defined as the number of coordinates, in which they differ. We call any subset of Q^n a *q-ary code of length n* or simply a *code* over the alphabet Q. The elements of a code are called codewords. An important parameter of each code is its minimum distance – the smallest possible Hamming distance between two different codewords. An *$(n, M, d)_q$-code* is a q-ary code of length n containing M codewords, and of minimum distance d.

The alphabet Q can consist of the elements of the set $Z_q = \{0, 1, \ldots, q-1\}$. If q is a prime power and the alphabet $Q = GF(q)$ is a finite field of q elements then $GF^n(q)$ is an n-dimensional vector space.

In this paper a set of computer tools for coding theory research is presented. The system offers computations over $Z_q = \{0, 1, \ldots, q-1\}$, $q < 256$ (modular arithmetic, elementary number theory, calculations with vectors, matrices), environments for research on q-ary codes (linear, constant-weight, equidistant) and a DLL library (Delphi's components). By the help of QPlus optimal ternary constant-weight codes, binary and ternary equidistant codes have been constructed.

2. Some classes of codes. In this work we consider the linear codes, constant-weight codes and equidistant codes.

We call any linear subspace of $GF^n(q)$ a q-ary *linear code*. If C is a linear code of length n, dimension k and minimum distance d we say that C is an $[n, k, d]$-code over

$GF(q)$, or an $[n,k,d]_q$-code. Each linear $[n,k,d]_q$-code has q^k codewords, i.e. it is an $(n,q^k,d)_q$-code. Let C be an $[n,k,d]_q$-code. Every $m \times n$ matrix of rank k, whose rows are vectors of C is called a generator matrix of the code. For an $[n,k,d]_q$-code we define its dual code, denoted by $C^\perp$, as the set of vectors of $GF^n(q)$ which are orthogonal to every codeword of C. $C^\perp$ is an $(n-k)$ dimensional subspace of $GF^n(q)$ i.e. an $[n,n-k,d]_q$-code. Every generator matrix of $C^\perp$ is called parity check matrix for C. We say that the generator matrix G is in systematic form if $G = (I_k \ P)$ where I_k is the identity matrix of order k and P is a $k \times (n-k)$ matrix. If C is a code with generator matrix G then the matrix $H = (-P^T \ I_{n-k})$ is a parity check matrix for C. Every code is equivalent to a code with a systematic generator matrix. The sequence $A_0, A_1, \ldots, A_n$, where A_w is the number of the codewords of weight w is called a spectrum of the code. The MacWilliams' identities ([7], p.129) give the relation between the spectrum of a code C and the spectrum of its dual code $C^\perp$.

The *Hamming weight* of an n-tuple of Z_q^n or $GF^n(q)$ is defined as the number of its nonzero coordinates. We call *a constant-weight code* the (n,M,d)-code in which every codeword has a Hamming weight w. The ternary constant-weight codes for which the exact number w_1 of ones and w_2 of twos is specified, are called *constant-composition codes*.

An $(n,M,d)_q$ *equidistant code* is a set of M codewords of length n over the alphabet $\{0,1,\ldots,q-1\}$, such that any two codewords differ in d positions.

One of the fundamental problems in Coding Theory is to find $A_q(n,d)$ – the largest value of M for which there exists an $(n,M,d)_q$-code.

Codes with parameters $(n, A_q(n,d), d)_q$ are called *optimal*. In a similar manner we consider the function $A_q(n,d,w)$ for constant-weight codes and the function $B_q(n,d)$ for equidistant codes.

The results in this area are described in surveys which contain tables [7, 3, 10, 2] etc. The aim of the computer systems related to the research in Coding Theory is to facilitate some routine work in the q-ary codes research. The idea of using a computer for this purpose is not a new one. Among the computer systems in this area is the program package for research on linear codes GUAVA [9]. The program system GFQ for calculations over finite fields with its modifications – an object-oriented library $GF2$ for calculations over finite fields with characteristics 2 were developed at the Applied Mathematics and Informatics Laboratory [1]. In [8] the system LinCoR for the study of binary linear codes is presented. The system QLC for studying q-ary linear codes [6] represents a development of BLC [4, 5]. The QCC is program for finding q-ary constant-weight codes from other codes [11].

In this next section a new program system QPlus (Q-ary Codes Tools) for research on q-ary codes is presented on an improved Windows version of GFQ, QLC and QCC.

3. Features of the system. The program system QPlus offers an integrated environment: the possibility of computations over Z_q and some environments for investigation of q-ary codes.

The program system consists of six units:

A Modular Arithmetic and Elementary Number Theory;
B Vectors;
C Matrices;
D Linear codes;
E Constant-weight codes;
F Equidistant codes.

For that purpose the following tools have been developed: the form A for computations over $Z_q = \{0, 1, \ldots, q-1\}$ ($q < 256$), forms B and C (over finite fields, q is prime power) and the forms D, E, F for research of q-ary codes, the objects (q-ary vectors, matrices and codes) and the corresponding classes, the editors of the q-ary objects, processing modules and input/output modules, the algorithms for generation of codes with good parameters.

Form A ($q < 256$) includes:
- Calculator;
- The N-th power;
- The N-th root;
- The greatest common divisor.

Form B offers the following calculations with vectors for $q < 256$:
- The sum of two vectors;
- The scalar product of two vectors;
- Multiplication of a vector by scalar.

The form C is designed for calculations with matrices for $q < 256$:
- Addition of matrices;
- Multiplication of a matrix by a scalar;
- Multiplication of a vector by a matrix;
- Multiplication of matrices;
- The determinant of a square matrix.

Form D offers an environment for research of q-ary linear codes ($q < 256$):
- The code dimension and the code basis;
- A systematic generator matrix;
- The spectrum of the code;
- A parity check matrix;
- The spectrum of the dual code.

The main object in forms C, D, E and F is a q-ary matrix of m rows and n columns. For linear codes this is a generator or parity check matrix of a linear code over $GF(q)$. The elements of the matrix can be entered by the keyboard or read from a data file (observing of a fixed data-file format is recommended). The dimensions of the matrix can be changed during the work. The data on the screen can be written into a data file or printed. While the older similar programs only realized calculations over $GF(q)$ where $q \leq 16$, the present project provides the opportunity to work up to $q = 256$ (q is a prime power). The code spectrum calculation may turn out to be a time-consuming work because in the general case it is necessary to generate all $\frac{q^k-1}{q-1}$ non-proportional linear combinations.

The form E is designed for finding q-ary constant-weight and constant-composition codes.

The form F offers algorithms for finding equidistant codes:

– Binary equidistant codes;
– Ternary equidistant codes.

Some methods for the construction of codes used in form E and F are:

1 An exhaustive search;
2 Constructing codes from other codes;
3 Some standard constructions.

QPlus includes a DLL library package that implements coding theory algorithms. QPlus has been written in Delphi 6.

One of the main advantages of QPlus is that there is no need for the user to have any programming skills. The system can be used for solving practical problems of Algebraic Coding Theory or for making calculations even by people not familiar with the coding theory. In addition to scientific research the program can be successfully used in the teaching process in an auditorium as well as individually. To make the program more useful for educational purposes the user can change the current parameters $(q, n, M, w, k \ldots)$ and some features of objects.

QPlus aims at the integration and upgrade of the design and functions of similar already existing systems. The system QPlus offers significant improvements including faster calculations, a convenient and easy to use graphic Windows-based interface compared to GFQ and QLC which have certain limitations. In addition to all this, the new version introduced the possibility to construct and study nonlinear codes (constant-weight, equidistant codes) and to determine the equivalence of codes.

4. Some results obtained by QPlus. We use QPlus for research of binary and ternary codes. The research of ternary constant-weight codes of length up to 10 was done with the help of Form E and methods 2 and 3. Many of the constructed

Table 1. Optimal binary equidistant codes for $n \leq 15$.

	$d=2$	$d=4$	$d=6$	$d=8$	$d=10$
n	M / #	M / #	M / #	M / #	M/#
2	2 / 1				
3	4 / 1				
4	4 / 2	2 / 1			
5	5 / 1	2 / 2			
6	6 / 1	4 / 1	2 / 1		
7	7 / 1	8 / 1	2 / 1		
8	8 / 1	8 / 3	2 / 1	2 / 1	
9	9 / 1	8 / 3	4 / 1	2 / 1	
10	10 / 1	8 / 3	6 / 1	2 / 1	2 / 1
11	11 / 1	8 / 3	12 / 1	2 / 1	2 / 1
12	12 / 1	8 / 3	12 / 8	4 / 1	2 / 1
13	13 / 1	8 / 3	13 / 1	4 / 2	2 / 1
14	14 / 1	8 / 3	13 / 1	8 / 4	2 / 1
15	15 / 1	8 / 3	14 / 2	16 / 5	4 / 1

denote the number of inequivalent equidistant codes

Currently, the tools and its library package will be sent to you upon request (galina@moi.math.bas.bg).

codes coincide with optimal codes. By the help of Form D some ternary linear codes are studied. Properties of binary and ternary equidistant codes related to the size of the code are obtained in Form F.

Optimal ternary constant-weight codes and binary and ternary equidistant codes have been constructed by our computer methods. Some of the results (tables, codes) are presented in the following Internet site http://www.moi.math.bas.bg/galina.

Example: Binary equidistant codes of length $n \leq 20$ are researched by QPlus, form F. For codes of small size we can apply combinatorial reasoning. For example, it is easy to prove that $B_2(n,d) = 2$ precisely when d is odd. For the rest of the values of M we use computer algorithm based on exhaustive search (form F, method 1), which is of exponential complexity. All of the binary equidistant codes obtained are optimal. The exact values of the bounds on $B_2(n,d)$ for $n \leq 15$ and $d \leq 10$ are displayed in Table 1.

Acknowledgment. The authors would like to thank Prof. D. Sci. S. Dodunekov, Prof. Dr. R. Daskalov, Prof. Dr. I. Boukliev and all colleagues from the Department of Mathematical Foundations of Informatics for the all-round help and for their useful advices.

REFERENCES

[1] Ts. Baicheva, G. Bogdanova, S. Ilieva, Sv. Topalova. Object-oriented C++ library for computations in and over finite fields of characteristic 2. *Mathematics and Education in Mathematics* **23**, Stara Zagora, April 1-4, (1994), 227–230.

[2] G. Bogdanova, T. Yorgova. Bounds for Ternary Equidistant Constant Weight Codes. *Mathematics and Education in Mathematics*, **31**, Borovec, April 3-6, (2002), 131–135.

[3] A. E. Brouwer. Bounds on the minimum distance of linear codes. <www.win.tue.nl/math/dw/personalpages/aeb/voorlincod.html>, Eindhoven University of Technology, Eindhoven, the Netherlands.

[4] St. Kapralov, P. Petrov. Program tool for binary linear codes researches. Proceedings of the Conference of the TU, Gabrovo, 1992.

[5] St. Kapralov, P. Petrov, Pl. Christov. QLC – Program tool for q-ary linear codes research. *Mathematics and Education in Mathematics*, **23**, Stara Zagora, April 1-4, (1994), 271–227.

[6] S. Kapralov, P. Christov, G.Bogdanova. The New Version of QLC – a Computer Program for Linear Codes Studying. Proc. of the International Workshop on Optimal Codes and Related Topics, Sozopol, Bulgaria, 1995, 11–14.

[7] F. J. MacWilliams, N. J. A. Sloane. The Theory of Error-Correcting Codes. Amsterdam, North-Holland, 1977.

[8] K. N. Manev. LINCOR – A System for Linear Codes Researches. *Mathematics and Education in mathematics*, **26** (1987), 500–503.

[9] J. Simonis. GUAVA, A computer algebra package for coding theory. *Proceedings of Fourth International Workshop on Algebraic and Combinatorial Coding Theory*, Novgorod, Rusia, 1994, 165–167.

[10] M. Svanstrom, P. R. J. Ostergard, G. T. Bogdanova. Bounds and Constructions for Ternary Constant-Composition Codes. *IEEE Trans. Inform. Theory*, **48**, No 1 (2002), 101–111.

[11] V. Todorov. QCC – Constructing codes from other codes. Student's Section of the Spring Conferences of the Bulgarian Mathematicians, Borovec, April 3-6, 2001.

Galina Todorova Bogdanova
P.O.Box 323
5000 V. Tarnovo, Bulgaria
e-mail: galina@moi.math.bas.bg

Stoyan Nedkov Kapralov
Technical University
Gabrovo, Bulgaria
e-mail: kapralov@tugab.bg

Vihren Hristov Todorov
Pliska 5 V
5000 V. Tarnovo, Bulgaria
e-mail: vih@top.bg

Teodor Sashev Parvanov
Hr. Smirnenski 6
5000 V. Tarnovo, Bulgaria
e-mail: ats@infotel.bg

QPLUS – ПРОГРАМЕН ПАКЕТ ЗА ИЗСЛЕДВАНИЯ В ТЕОРИЯ НА КОДИРАНЕТО

Галина Т. Богданова, Стоян Н. Капралов, Вихрен Хр. Тодоров, Теодор С. Първанов

Представя се програмна система в областта на теория на кодирането. Създадени са модули за пресмятания с вектори и матрици над крайно поле, калкулатор ($q < 256$) и среда за изследване на q-ични кодове – линейни, константно-тегловни и еквидистантни. Оптимални троични константно-тегловни кодове, двоични и троични еквидистантни кодове са конструирани с помощта на създадените алгоритми. QPlus съдържа DLL библиотеки от компоненти. При реализацията на QPlus се използват предимствата на обектно-ориентираното програмиране (Delphi 6).