



Finding Minimum Distance and Decoding Linear Error-correcting Codes with Groebner Bases

Ruud Pellikaan* and Stanislav Bulygin**

* Department of Mathematics and Computer Science, Eindhoven
University of Technology, The Netherlands

** Department of Mathematics, Technical University of Kaiserslautern,
Germany

Work in progress

Linz, May, 2006



Groebner Bases and Linear Codes

- Cyclic codes: Newton identities of syndromes - Augot, Bardet, Faugere
- Cyclic codes: Power sums - Cooper, Helleseth et.al., Sala, and others
- (General) linear codes: generalization of the power sum method - Lax, Fitzgerald
- (General) linear codes: key equation - O'Keefe, Fitzpatrick, and others



Preliminaries and Notation I

- Let F be a field. Let \overline{F} be the algebraic closure of F . Let b_1, \dots, b_n be a basis of F^n . Now let B be the $n \times n$ matrix with b_1, \dots, b_n as rows. The (*unknown*) *syndrome* $u(B, e)$ of a word e w.r.t B is the column vector $u(B, e) = Be^T$. It has entries $u_i(B, e) = b_i \cdot e$ for $i = 1, \dots, n$. We abbreviate $u(B, e)$ by $u(e)$.
- (*Coordinatewise*) *Star Product* of two vectors $x * y := (x_1 y_1, \dots, x_n y_n)$. Then we have $b_i * b_j = \sum_{l=1}^n c_{ijl} b_l$, for some c_{ijl} which are called *structure constants* of the basis b_1, \dots, b_n .
- Let b_1, \dots, b_n be a basis of F^n . Let B_r be the $r \times n$ matrix with b_1, \dots, b_r as rows. We say that b_1, \dots, b_n is an *MDS basis* and B is an *MDS matrix* if all the $t \times t$ submatrices of B_t have rank t for all $t = 1, \dots, n$.

Preliminaries and Notation II

- W.l.o.g we assume that after a finite extension of the field F_q we have $n \leq q$. We also assume that matrix B is an MDS matrix.
- Let C be an $[n, k, d]$ F_q - linear code with a check matrix H , whose rows are h_1, \dots, h_r , $r = n - k$ the redundancy. We can express $h_i = \sum_{j=1}^n a_{ij} b_j$.
- Let $r = c + e$ be a *received word*, $c \in C$ the codeword, e the *error vector*. Then $h_i \cdot c = 0$ for all $i = 1, \dots, r$. Thus we have $s_i(r) := h_i \cdot r = h_i \cdot e = s_i(e)$.
These can be rewritten as $s_i(r) = \sum_{j=1}^n a_{ij} u_j(e)$.
- The ideal $J(r)$ in the ring $F_q[U_1, \dots, U_n]$ is generated by the elements

$$\sum_{l=1}^n a_{jl} U_l - s_j(r), \text{ for } j = 1, \dots, r.$$

The ideal $I(t, U, V)$ in the ring $F_q[U_1, \dots, U_n, V_1, \dots, V_n]$ is generated by the elements (here $U_{ij} = \sum_{l=1}^n c_{ijl} U_l$).

$$\sum_{j=1}^t U_{ij} V_j - U_{it+1}, \text{ for } i = 1, \dots, n.$$



Main Theorem

- We use the above notation. Suppose that the weight of e is at most $(d(C) - 1) / 2$. Let $I(t, r)$ be an ideal (equations) generated by $J(r)$ and $I(t, U, V)$. Suppose also that $r \notin C$. Let t be the smallest positive integer such that $I(t, r)$ has a solution (u, v) over \overline{F}_q . Then $t = wt(e)$ and the solution is unique; it satisfies $u_i = u_i(e)$ for all $i = 1, \dots, n$.
- Advantages:
 - **NO** field equations;
 - nevertheless, **solution is unique**, and lies in the ground field;
 - all equations have degree **at most 2**;
 - after solving the system, **decoding is simple**:

$$e^T = B^{-1} B e^T = B^{-1} u(e).$$



Other Problems that can be Solved

- Other problems that can be solved by applying ideas that lie behind the Main Theorem include:
 - Finding minimum weight of the code;
 - Finding weight distribution of the code;
 - Nearest codeword decoding, when for a received vector all codewords closest to this vector are found (when distance from the received word to the code exceeds error capacity).



Things to be Done

- There is still some work to be done:
 - Applying this method to cryptanalysis of McEliece and Niederreiter cryptosystems;
 - Gaussian elimination approach to solving the system above;
 - More simulations/experiments and benchmarks against known methods of decoding (with Groebner bases).