Department of Mathematical Sciences
Clemson University

http://www.ces.clemson.edu/ keyj/

Information sets for the generalized Reed-Muller codes

J. D. Key

keyj@ces.clemson.edu

Abstract

We produce a simple rule that will give information sets for the generalized Reed-Muller codes over any finite field, and use these information sets to obtain new bases of minimum-weight vectors for the codes of the designs of points and hyperplanes over prime fields.

Joint work with T. P. McDonough and V. C. Mavron of the University of Wales, Aberystwyth, [KMM].

October 26, 2004

Coding theory terminology

- A q-ary **linear code** of length n is a subspace of the n-dimensional vector space $\mathbb{F}_q^n$ over the finite field $\mathbb{F}_q$.
- The (Hamming) **distance** between two vectors $u, v \in \mathbb{F}_q^n$ is the number of coordinate position in which they differ.
- The **weight** of a vector is the number of non-zero coordinate entries. If a code has smallest non-zero weight d then the code can correct up to $t = \lfloor \frac{d-1}{2} \rfloor$ errors by nearest-neighbour decoding, i.e. if at most t errors occur in transmission then the nearest codeword to the received vector is the one that was sent.
- If a code C over a field of order q is of length n, dimension k, and minimum weight d, then we write $[n, k, d]_q$ to show this information.
- A **generator matrix** G for C is a $k \times n$ matrix made up of a basis for $C = [n, k, d]_q$. The set of coordinate positions corresponding to a set of k linearly independent columns of G is an **information set** for C.

Coding theory terminology continued

- The **dual** code $C^\perp$ is the orthogonal to C under the standard inner product $(,)$, i.e. $C^\perp = \{v \in F^n | (v, c) = 0 \text{ for all } c \in C\}$.
- A **check** matrix for C is a generator matrix H for $C^\perp$.
- Two linear codes of the same length and over the same field are **isomorphic** if they can be obtained from one another by permuting the coordinate positions.
- An **automorphism** of a code C is an isomorphism from C to C.
- Any code is isomorphic to a code with generator matrix in **standard form**, i.e. the form $[I_k \,|\, A]$; a check matrix then is given by $[-A^T \,|\, I_{n-k}]$. The first k coordinates are the **information symbols** and the last $n - k$ coordinates are the **check symbols**.
- **Encoding** of a data-set vector $x = (x_1, \ldots, x_k)$ is by matrix multiplication, i.e. xG, where G is a generator matrix. Decoding methods vary for different codes.

Generalized Reed-Muller codes

Let $q = p^t$, p a prime, and $V = \mathbb{F}_q^m$ with standard basis. The codes are q-ary codes of length q^m in the function space $\mathbb{F}_q^V$, with the usual basis of characteristic functions of the vectors of V.

Denote the elements $f \in \mathbb{F}_q^V$ by functions of the m-variables denoting the coordinates of a variable vector in V, i.e. if $\mathbf{x} = (x_1, x_2, \ldots, x_m) \in V$, then $f \in \mathbb{F}_q^V$ is given by $f = f(x_1, x_2, \ldots, x_m)$ and the x_i take values in $\mathbb{F}_q$. The codeword defined by f will have $f(\mathbf{v})$ at the coordinate position corresponding to $\mathbf{v} = (v_1, v_2, \ldots, v_m) \in V$.

Every $f \in \mathbb{F}_q^V$ can be written as a polynomial given uniquely as a linear combination of the q^m monomial functions

$$\mathcal{M} = \{x_1^{i_1} x_2^{i_2} \ldots x_m^{i_m} \,|\, 0 \leq i_k \leq q-1, \text{ for } 1 \leq k \leq m\}.$$

The degree ρ of a monomial is the total degree, i.e. $\rho = \sum_{k=1}^{m} i_k$ and $0 \leq \rho \leq m(q-1)$.

Definition 1 *Let $V = \mathbb{F}_q^m$, $m \geq 1$, over $\mathbb{F}_q$, where $q = p^t$ and p prime. For $0 \leq \rho \leq m(q-1)$, the* **ρ^{th}-order generalized Reed-Muller code** $\mathcal{R}_{\mathbb{F}_q}(\rho, m)$ *is the subspace of $\mathbb{F}_q^V$ (with basis the characteristic functions of vectors in V) of all m-variable polynomial functions (reduced modulo $x_i^q - x_i$) of degree at most ρ. Thus*

$$\mathcal{R}_{\mathbb{F}_q}(\rho, m) = \langle x_1^{i_1} x_2^{i_2} \cdots x_m^{i_m} \mid 0 \leq i_k \leq q-1, \text{ for } 1 \leq k \leq m, \sum_{k=1}^{m} i_k \leq \rho \rangle.$$

The codes have length q^m and the codewords are obtained by evaluating the m-variable polynomials in the code at all the points of the vector space V.

Further $\mathcal{R}_{\mathbb{F}_q}(\rho, m)^{\perp} = \mathcal{R}_{\mathbb{F}_q}(\mu, m)$ for $\rho < m(q-1)$ and where $\rho + \mu + 1 = m(q-1)$.

[For more about the generalized Reed-Muller codes, see [AK98] or [AK92].]

Some properties of GRM codes

- $\mathcal{R}_{\mathbb{F}_q}(\rho, m) = [q^m, f_{\rho,m,q}, d_{\rho,m,q}]_q$ where

$$f_{\rho,m,q} = \sum_{i=0}^{m} (-1)^i \binom{m}{i} \binom{m+\rho-iq}{m} \text{ and } d_{\rho,m,q} = (q-b)q^{m-a-1},$$

  where $\rho = a(q-1)+b$, $0 \leq b < q-1$.

- $\mathrm{Aut}(\mathcal{R}_{\mathbb{F}_q}(\rho, m)) = AGL_m(\mathbb{F}_q)$ for $0 \leq \rho \leq m(q-1)$.

- $\mathcal{R}_{\mathbb{F}_q}(\rho, m)^*$ is the **punctured** GRM, of length $q^m - 1$, and is cyclic with $GL_m(\mathbb{F}_q)$ as automorphism group.

- With $m = 1$, $\mathcal{R}_{\mathbb{F}_q}(\rho, 1)^*$ is the Reed-Solomon code and $\mathcal{R}_{\mathbb{F}_q}(\rho, 1)$ the extended Reed-Solomon code, i.e.

$$\mathcal{R}_{\mathbb{F}_q}(\rho, 1) = \langle x^i \mid 0 \leq i \leq \rho \rangle,$$

  where $\rho \leq q-1$ and $d_{\rho,1,q} = (q-\rho)$, so the code is $[q, \rho+1, q-\rho]_q$ and is an MDS code.

If $\rho = r(q-1)$, the minimum distance of $\mathcal{R}_{\mathbb{F}_q}(r(q-1), m)$ is q^{m-r} and the minimum words are the incidence vectors of the subspaces of dimension $(m-r)$ and their cosets (the $(m-r)$-flats), e.g.

$$p(x_1, \ldots, x_m) = \prod_{i=1}^{r} (1 - x_i^{q-1}) \in \mathcal{R}_{\mathbb{F}_q}(r(q-1), m)$$

is the incidence vector of the subspace of V given by the equations

$$X_1 = X_2 = \cdots = X_r = 0$$

of dimension $m - r$.

The incidence (characteristic) vector of a point (vector) $\mathbf{w} = (w_1, \ldots, w_m) \in V$ is

$$\chi_{\mathbf{w}} = v^{\mathbf{w}} = \prod_{i=1}^{m} (1 - (x_i - w_i)^{q-1}).$$

Information sets

The coordinate set of the codes are the vectors $(v_1, v_2, \ldots, v_m) \in V$, where $v_i \in \mathbb{F}_q$, and the vectors can be ordered in any way. For a generator matrix to be in standard form, we want the first k positions to form an information set, where k is the dimension of the code.

The set of monomial functions of degree at most ν,

$$\mathcal{B} = \{x_1^{i_1} x_2^{i_2} \ldots x_m^{i_m} \mid 0 \leq i_k \leq q-1, \text{ for } 1 \leq k \leq m, \sum_{k=1}^{m} i_k \leq \nu\},$$

is an $\mathbb{F}_q$-basis of $\mathcal{R}_{\mathbb{F}_q}(\nu, m)$. A subset $S \subseteq V = {\mathbb{F}_q}^m$ will be an information set of the code if, and only if, the subspace of ${\mathbb{F}_q}^S$ spanned by the restriction of $\mathcal{B}$ to S has dimension $|\mathcal{B}|$.

Theorem 1 *Let $V = \mathbb{F}_q^m$, where $q = p^t$ and p is a prime, and $\mathbb{F}_q = \{\alpha_0, \ldots, \alpha_{q-1}\}$, and*

$$\mathcal{S} = \{[i_1, i_2, \ldots, i_m] \mid i_k \in \mathbb{Z},\ 0 \leq i_k \leq q-1,\ 1 \leq k \leq m\}.$$

Let $\leq$ denote the partial order defined on S by $[i_1, i_2, \ldots, i_m] \leq [j_1, j_2, \ldots, j_m]$ if and only if $i_k \leq j_k$ for all k such that $1 \leq k \leq m$.

Let $\mathcal{X} \subseteq \mathcal{S}$ have the property

$$x \in \mathcal{X} \Rightarrow ((y \in \mathcal{S}) \wedge (y \leq x) \Rightarrow y \in \mathcal{X}).$$

and let

$$C = \langle x_1^{i_1} x_2^{i_2} \cdots x_m^{i_m} \mid [i_1, i_2, \ldots, i_m] \in \mathcal{X} \rangle.$$

Then the set of vectors

$$\mathcal{I} = \{(\alpha_{i_1}, \ldots, \alpha_{i_m}) \mid [i_1, i_2, \ldots, i_m] \in \mathcal{X}\}$$

is an information set for C.

In particular,

$$\mathcal{I} = \{(\alpha_{i_1}, \ldots, \alpha_{i_m}) \mid \sum_{k=1}^{m} i_k \leq \nu,\ 0 \leq i_k \leq q-1\}$$

is an information set for $\mathcal{R}_{\mathbb{F}_q}(\nu, m)$, and if $q = p$ is a prime,

$$\mathcal{I} = \{(i_1, \ldots, i_m) \mid i_k \in \mathbb{F}_p,\ 1 \leq k \leq m,\ \sum_{k=1}^{m} i_k \leq \nu\}$$

is an information set for $\mathcal{R}_{\mathbb{F}_p}(\nu, m)$, by taking $\alpha_{i_k} = i_k$.

Examples

$q=3$		0	0	0	1	1	2	1	2	2
$m=2$		0	1	2	0	1	0	2	1	2
1	[0,0]	1	1	1	1	1	1	1	1	1
x_2	[0,1]	0	1	2	0	1	0	2	1	2
x_2^2	[0,2]	0	1	1	0	1	0	1	1	1
x_1	[1,0]	0	0	0	1	1	2	1	2	2
x_1x_2	[1,1]	0	0	0	0	1	0	2	2	1
x_1^2	[2,0]	0	0	0	1	1	1	1	1	1

Figure 1: $\mathcal{R}_{\mathbb{F}_q}(\rho, m) = \mathcal{R}_{\mathbb{F}_3}(2,2)$

$$\mathcal{B} = \{x_1^{i_1} x_2^{i_2} \mid 0 \leq i_k \leq 2, i_1 + i_2 \leq 2\}.$$

		0	0	0	0	1	1	1	w	w	w^2	1	w	w	w^2	w^2	w^2
		0	1	w	w^2	0	1	w	0	1	0	w^2	w	w^2	1	w	w^2
1	[0,0]	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
x_2	[0,1]	0	1	w	w^2	0	1	w	0	1	0	w^2	w	w^2	1	w	w^2
x_2^2	[0,2]	0	1	w^2	w	0	1	w^2	0	1	0	w	w^2	w	1	w^2	w
x_2^3	[0,3]	0	1	1	1	0	1	1	0	1	0	1	1	1	1	1	1
x_1	[1,0]	0	0	0	0	1	1	1	w	w	w^2	1	w	w	w^2	w^2	w^2
x_1x_2	[1,1]	0	0	0	0	0	1	w	0	w	0	w^2	w^2	1	w^2	1	w
$x_1x_2^2$	[1,2]	0	0	0	0	0	1	w^2	0	w	0	w	1	w^2	w^2	w	1
x_1^2	[2,0]	0	0	0	0	1	1	1	w^2	w^2	w	1	w^2	w^2	w	w	w
$x_1^2x_2$	[2,1]	0	0	0	0	0	1	w	0	w^2	0	w^2	1	w	w	w^2	1
x_1^3	[3,0]	0	0	0	0	1	1	1	1	1	1	1	1	1	1	1	1

Figure 2: $\mathcal{R}_{\mathbb{F}_4}(3,2)$, $\mathbb{F}_4 = \{\alpha_0, \alpha_1, \alpha_2, \alpha_3\} = \{0, 1, w, w^2\}$

Example

The extended Reed-Solomon code,

$$\mathcal{R}_{\mathbb{F}_q}(\rho, 1) = \langle x^i \mid 0 \leq i \leq \rho \rangle,$$

where $\rho \leq q-1$ and $d_{\rho,1,q} = (q-\rho)$, is a $[q, \rho+1, q-\rho]_q$. Taking

$$\{\alpha_0, \ldots, \alpha_{q-1}\} = \{0, 1, w, w^2, \ldots, w^{q-2}\}$$

where w is a primitive element for $\mathbb{F}_q$, then our information set is the usual set

$$\{0, 1, w, w^2, \ldots, w^{\rho-1}\}$$

giving the usual generating matrix as for BCH codes (puncturing first at 0).

The proof puts $\mathcal{X}$ in lexicographic order by $\prec$, i.e. $x = [i_1, \ldots, i_m] \prec y = [j_1, \ldots, j_m]$ if, and only if, for some k with $1 \leq k \leq m$, $i_k < j_k$ and $i_\ell = j_\ell$ for $\ell < k$. So $\preceq$ is a total order consistent with the partial order $\leq$.

It is then shown that the $|\mathcal{X}| \times |\mathcal{X}|$ matrix M with

$$M_{x,y} = \alpha_{j_1}^{i_1} \alpha_{j_2}^{i_2} \ldots \alpha_{j_m}^{i_m}$$

is the product of two matrices, one lower triangular, one upper triangular, whose determinant is easy to find.

Illustration (not GRM)

Let $\mathcal{X} == \{[0,0],[0,1],[0,2],[1,0],[1,1],[1,2]\}$, $q \geq 3$ and $\mathbb{F}_q = \{\alpha_0, \alpha_1, \ldots, \alpha_{q-1}\}$.

$$L = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ \alpha_0 & 1 & 0 & 0 & 0 & 0 \\ {\alpha_0}^2 & \alpha_0 + \alpha_1 & 1 & 0 & 0 & 0 \\ \alpha_0 & 0 & 0 & 1 & 0 & 0 \\ {\alpha_0}^2 & \alpha_0 & 0 & \alpha_0 & 1 & 0 \\ {\alpha_0}^3 & (\alpha_0 + \alpha_1)\,\alpha_0 & \alpha_0 & {\alpha_0}^2 & \alpha_0 + \alpha_1 & 1 \end{bmatrix},$$

$$R = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & \alpha_1 - \alpha_0 & \alpha_2 - \alpha_0 & 0 & \alpha_1 - \alpha_0 & \alpha_2 - \alpha_0 \\ 0 & 0 & (\alpha_2 - \alpha_0)(\alpha_2 - \alpha_1) & 0 & 0 & (\alpha_2 - \alpha_0)(\alpha_2 - \alpha_1) \\ 0 & 0 & 0 & \alpha_1 - \alpha_0 & \alpha_1 - \alpha_0 & \alpha_1 - \alpha_0 \\ 0 & 0 & 0 & 0 & (\alpha_1 - \alpha_0)^2 & (\alpha_2 - \alpha_0)(\alpha_1 - \alpha_0) \\ 0 & 0 & 0 & 0 & 0 & (\alpha_2 - \alpha_0)(\alpha_2 - \alpha_1)(\alpha_1 - \alpha_0) \end{bmatrix}$$

For $x = [i_1, \ldots, i_m]$ and $y = [j_1, \ldots, j_m]$ then

$$M_{x,y} = \alpha_{j_1}^{i_1} \alpha_{j_2}^{i_2} \ldots \alpha_{j_m}^{i_m}$$

and

$$M = LR = \left[\begin{array}{c|cccccc} & (\alpha_0,\alpha_0) & (\alpha_0,\alpha_1) & (\alpha_0,\alpha_2) & (\alpha_1,\alpha_0) & (\alpha_1,\alpha_1) & (\alpha_1,\alpha_2) \\ \hline 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ x_2 & \alpha_0 & \alpha_1 & \alpha_2 & \alpha_0 & \alpha_1 & \alpha_2 \\ x_2^2 & {\alpha_0}^2 & {\alpha_1}^2 & {\alpha_2}^2 & {\alpha_0}^2 & {\alpha_1}^2 & {\alpha_2}^2 \\ x_1 & \alpha_0 & \alpha_0 & \alpha_0 & \alpha_1 & \alpha_1 & \alpha_1 \\ x_1x_2 & {\alpha_0}^2 & \alpha_0\alpha_1 & \alpha_0\alpha_2 & \alpha_0\alpha_1 & {\alpha_1}^2 & \alpha_1\alpha_2 \\ x_1x_2^2 & {\alpha_0}^3 & \alpha_0{\alpha_1}^2 & \alpha_0{\alpha_2}^2 & {\alpha_0}^2\alpha_1 & {\alpha_1}^3 & \alpha_1{\alpha_2}^2 \end{array}\right]$$

Design theory background

An incidence structure $\mathcal{D} = (\mathcal{P}, \mathcal{B}, \mathcal{I})$, with point set $\mathcal{P}$, block set $\mathcal{B}$ and incidence $\mathcal{I}$ is a t-(v, k, λ) design, if $|\mathcal{P}| = v$, every block $B \in \mathcal{B}$ is incident with precisely k points, and every t distinct points are together incident with precisely λ blocks.

E.g. A 2-$(n^2 + n + 1, n + 1, 1)$ is a projective plane of order n;
a $2 - (16, 6, 2)$ is a biplane.

The code C_F of the design $\mathcal{D}$ over the finite field F is the space spanned by the incidence vectors of the blocks over F, i.e. the row span over F of an incidence matrix.

For any finite field $\mathbb{F}_q$ of order q, the set of points and r-dimensional subspaces (respectively flats) of an m-dimensional projective (respectively affine) geometry forms a 2-design which we will denote by $\boldsymbol{PG_{m,r}(\mathbb{F}_q)}$ (respectively $\boldsymbol{AG_{m,r}(\mathbb{F}_q)}$). The **automorphism groups**, $P\Gamma L_{m+1}(\mathbb{F}_q)$ or $A\Gamma L_m(\mathbb{F}_q)$, respectively, of these designs (and codes) are the full projective or affine semi-linear groups, and always 2-transitive on points.

If $q = p^e$ where p is a prime, the codes of these designs are over $\mathbb{F}_p$ and are subfield subcodes of the generalized Reed-Muller codes. The dimension and minimum weight is known in each case.

In particular, the code $\mathcal{R}_{\mathbb{F}_p}((m-r)(p-1), m)$ is the p-ary code of the affine geometry design $AG_{m,r}(\mathbb{F}_p)$.

Projective geometry

We can construct information sets for the code $C_p(PG_{m,r}(\mathbb{F}_p))$ using what we have found for the affine case:

if $\mathcal{I}$ is an information set for $C_p(AG_{m,m-1}(\mathbb{F}_p))$, then

$$\{(0,\ldots,0,1)\} \cup \{(1,x_1,\ldots,x_m) \mid (x_1,\ldots,x_m) \in \mathcal{I}\},$$

is an information set for $C_p(PG_{m,m-1}(\mathbb{F}_p))$.

More generally, if $\mathcal{I}$ is an information set for $C_p(AG_{m,r}(\mathbb{F}_p))$ and $\mathcal{J}$ is an information set for $C_p(PG_{m-1,r}(\mathbb{F}_p))$, then $\mathcal{I}^* \cup \mathcal{J}^\dagger$ is an information set for $C_p(PG_{m,r}(\mathbb{F}_p))$, where

$$\mathcal{I}^* = \{(1,x_1,\ldots,x_m) \mid (x_1,\ldots,x_m) \in \mathcal{I}\},$$

$$\mathcal{J}^\dagger = \{(0,x_1,\ldots,x_m) \mid (x_1,\ldots,x_m) \in \mathcal{J}\}.$$

Using this inductive construction, we get

$$\{(0,\ldots,0,1)\} \cup \bigcup_{1\leq i\leq r} \mathcal{K}_i$$

is an information set for $C_p(PG_{m,r}(\mathbb{F}_p))$, where $\mathcal{K}_i$ is the set of vectors

$$\{(\underbrace{0,\ldots,0}_{r-i},1,\underbrace{a_{r-i+1},\ldots,a_m}_{m-r+i})|0\leq a_j\leq p-1, r-i+1\leq j\leq m, \sum_{j=r-i+1}^{m} a_j \leq i(p-1)\}.$$

As a by-product of this construction of information sets for the projective geometry designs, in the case of the design of points and hyperplanes we can use homogeneous coordinates to obtain a set of hyperplanes whose incidence vectors will form a basis for the code in the prime case.

This construction can be compared with the basis found in [GK98], where a basis of hyperplanes for the affine prime case was constructed and this then applied to the projective case.

Here the dimension of the code is

$$f_{q-1,m,q} = \binom{m+q-1}{m}$$

in the affine case, and $f_{q-1,m,q} + 1$ in the projective case.

Proposition 2 *If $C = C_p(PG_{m,m-1}(\mathbb{F}_p))$, where p is a prime and $m \geq 2$, then, using homogeneous coordinates, the incidence vectors of the set*

$$\{(1, a_1, \ldots, a_m)' \mid a_i \in \mathbb{F}_p, \sum_{i=1}^{m} a_i \leq p-1\} \cup \{(0, \ldots, 0, 1)'\}$$

of hyperplanes form a basis for C.

Similarly, a basis of hyperplanes for $C_p(AG_{m,m-1}(\mathbb{F}_p))$ for $m \geq 2$, p prime is the set of incidence vectors of the hyperplanes with equation

$$\sum_{i=1}^{m} a_i X_i = p-1$$

with

$$\sum_{i=1}^{m} a_i \leq p-1,$$

where $a_i \in \mathbb{F}_p$ for $1 \leq i \leq m$, and not all the a_i are 0, along with the hyperplane with equation $X_m = 0$.

Example

A basis of minimum-weight vectors for $C_3(PG_{2,1}(\mathbb{F}_3))$.

	0	1	1	1	1	1	1	1	1	1	0	0	0
	0	0	0	0	1	1	2	1	2	2	1	1	1
	1	0	1	2	0	1	0	2	1	2	0	1	2
$(0,0,1)'$	0	1	0	0	1	0	1	0	0	0	1	0	0
$(1,0,0)'$	1	0	0	0	0	0	0	0	0	0	1	1	1
$(1,0,1)'$	0	0	0	1	0	0	0	1	0	1	1	0	0
$(1,0,2)'$	0	0	1	0	0	1	0	0	1	0	1	0	0
$(1,1,0)'$	1	0	0	0	0	0	1	0	1	1	0	0	0
$(1,1,1)'$	0	0	0	1	0	1	1	0	0	0	0	0	1
$(1,2,0)'$	1	0	0	0	1	1	0	1	0	0	0	0	0

Figure 3: $C_3(PG_{2,1}(\mathbb{F}_3))$

Example

A basis of minimum-weight vectors for $\mathcal{R}_{\mathbb{F}_3}(2,2) = C_3(AG_{2,1}(\mathbb{F}_3))$.

	0 0	0 1	0 2	1 0	1 1	2 0	1 2	2 1	2 2
$X_2 = 0$	1	0	0	1	0	1	0	0	0
$X_2 = 2$	0	0	1	0	0	0	1	0	1
$X_2 = 1$	0	1	0	0	1	0	0	1	0
$X_1 = 2$	0	0	0	0	0	1	0	1	1
$X_1 + X_2 = 2$	0	0	1	0	1	1	0	0	0
$2X_1 = 2$	0	0	0	1	1	0	1	0	0

Figure 4: $\mathcal{R}_{\mathbb{F}_3}(2,2) = C_3(AG_{2,1}(\mathbb{F}_3))$

Compare with the generator matrix using the polynomial basis 1.

References

[AK92] E. F. Assmus, Jr and J. D. Key. *Designs and their Codes*. Cambridge: Cambridge University Press, 1992. Cambridge Tracts in Mathematics, Vol. 103 (Second printing with corrections, 1993).

[AK98] E. F. Assmus, Jr and J. D. Key. Polynomial codes and finite geometries. In V. S. Pless and W. C. Huffman, editors, *Handbook of Coding Theory*, pages 1269–1343. Amsterdam: Elsevier, 1998. Volume 2, Part 2, Chapter 16.

[GK98] S. Gao and J. D. Key. Bases of minimum-weight vectors for codes from designs. *Finite Fields Appl.*, 4:1–15, 1998.

[KMM] J. D. Key, T. P. McDonough, and V. C. Mavron. Information sets and partial permutation decoding of codes from finite geometries. Submitted.